# BEZPEČNOSŤ IT

## ÚVOD

Toto je prvá metodika zo série 3 metodík, ktoré sú venované problematike bezpečnosti IT. Táto problematika je veľmi zložitý problém, ktorého znalosť sa týka všetkých ľudí používajúcich IT. Tieto metodiky predstavujú všeobecné zásady používania IT, prácu s počítačovou sieťou a zásadami s jej používaním[1].

V metodike sa používa voľne šíriteľný softvér **HashCalc**[2], ktorý odporúčame nainštalovať na učiteľský počítač a v rámci metodiky použiť formou frontálnej ukážky, nakoľko program nefunguje pod užívateľským kontom, len pod kontom administrátora.

Žiaci majú k dispozícii pracovný list, ktorý obsahuje zadania úloh, miesto na žiacke riešenie a miesto pre poznámky.

## PRIEBEH VÝUČBY

Osnova vyučovacej hodiny (podľa modelu 5E):

- **Zapojenie (5 minút)** – motivačný rozhovor so žiakmi
- **Skúmanie (5 minút)** – riešenie úlohy z pracovného listu formou práce vo dvojiciach (úloha 1)
- **Vysvetlenie (12 minút)** – zhrnutie výsledkov úlohy z pracovného listu, analýza ďalších príkladov pomocou videí a úloh z pracovného listu (úlohy 2 a 3) a ukážka práce s hašovacím programom
- **Rozpracovanie (10 minút)** – práca vo dvojiciach, vyhľadávanie na internete pomocou úlohy z pracovného listu (úloha 4)
- **Hodnotenie (8 minút)** – porovnanie a odprezentovanie zistení z úlohy 4, sebahodnotiaca rubrika

### ZAPOJENIE (CCA 5 MIN.):

Hodinu začneme rozhovorom so žiakmi na tému: hrozba, zraniteľnosť a riziko, bezpečnosť na počítačovej sieti. Vo virtuálnom svete na nás neustále útočia, my si to vôbec neuvedomujeme.

---

[1] Metodika nepokrýva celú oblasť bezpečnosti IT v takej podobe, ako by ju mal ovládať učiteľ (nie žiak), preto pre hlbšie štúdium problematiky je možné odporúčať ďalšie študijné materiály, napr. https://www.csirt.gov.sk/doc/MFSRVzdelavanie/02Vzdelavanie2014/Studijne_materialy/Stud_2014_02_IT_IB_ucitelia.pdf

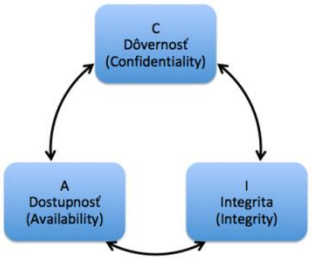
[2] Stiahnuteľný zo stránky https://hashcalc.soft112.com

Útočníci chcú mať prístup k nášmu majetku a údajom. Organizácie si musia chrániť svoje databázy, je to pre nich veľmi dôležité. Pretože vlastnia údaje tisícov a tisícov svojich zákazníkov a ich nemôžu sklamať. Naše údaje sú osobné, súkromné a nechceme si ich nechať ukradnúť a zneužiť napríklad na reklamnú kampaň, alebo pri volebnej kampani alebo aby si niekto z nás robil posmech.

Na ukážku môžeme využiť problém prístupov k hodnoteniu žiaka:

- známky žiaka nie sú sprístupnené iným osobám ako sú oprávnené osoby (napr. učitelia, rodičia)
- známky žiaka nemôže nikto modifikovať mimo učiteľa, ktorý má právo toho hodnotenie udeľovať
- zabezpečenie prístupu k známkam žiaka vtedy, keď je potrebné uzavrieť školský rok

Všetky tieto spomínané problémy chceme zabezpečiť pri hodnotení žiaka. Ako by sme ich mohli nazývať všeobecne? Nechajme žiakov, aby sami v nasledujúcom skúmaní objavili a priradili ku príkladom jednotlivé ciele a definície informačnej bezpečnosti. **Dôvernosť**, **integrita** a **dostupnosť**, známa ako trojica **CIA**, sú základné požiadavky pre bezpečnosť informácií (aj v prípade spomínaného hodnotenia žiakov). Dôvernosť zabezpečuje súkromie údajov obmedzením prístupu prostredníctvom šifrovania autentifikácie. Integrita zaručuje, že informácie sú presné, nezmenené a dôveryhodné. Dostupnosť zaručuje, že informácie sú prístupné len oprávneným osobám a v danom čase. V ďalších častiach hodiny budeme tieto tri požiadavky skúmať v rôznych prípadoch zo života.




## SKÚMANIE (CCA 5 MIN.):

Žiaci pracujú v 3-4členných skupinách s pracovným listom – cieľom je oboznámiť sa bližšie s pojmami dôvernosť, integrita a dostupnosť, ktoré boli uvedené v predchádzajúcej časti hodiny. Žiakov môžeme upozorniť, že úloha v pracovnom liste nie je test, teda môže sa stať, že v niektorých prípadoch si nebudú úplne istí odpoveďou, čo si môžu do pracovného listu poznačiť a k výsledkom sa vrátime v ďalšej časti hodiny, kde si budú môcť overiť ich správnosť. V tejto etape záznamy žiakov nevyhodnocujme ani nekomentujme.

***Úloha 1*** *a) Posúďte a pri popisoch vyberte, či sa jedná o dôvernosť, integritu alebo dostupnosť:*

| ***Popis*** | ***Bezpečnostná požiadavka*** *(vyberte správnu podľa popisu)* |
|---|---|
| ***zdroje systému sú k dispozícii oprávnenej osobe**, napr. počítačové siete, hardvérové vybavenie a dáta sú k dispozícii oprávneným používateľom, teda napr. vďaka údržbe a opravám zariadení, aktualizovaniu operačných systémov a softvéru a vytváraniu záloh* | ***?*** ***Dôvernosť*** ***Integrita*** ***Dostupnosť*** |
| ***informáciu obsiahnutú v správe (dokumente) sa nedozvedia nepovolané osoby**, teda údaje musia byť zabezpečené (napr. šifrovaním, používateľským menom* | ***?*** ***Dôvernosť*** ***Integrita*** |

| | |
|---|---|
| *a heslom**)** pred zobrazovaním neoprávneným osobám* | ***Dostupnosť*** |
| ***údaje nie je možné zmeniť bez toho, aby to ich vlastník alebo adresát nemohol zistiť**, teda údaje musia byť počas presunu nezmenené a nesmú sa meniť neoprávnenými subjektmi* | ***?*** <br> ***Dôvernosť*** <br> ***Integrita*** <br> ***Dostupnosť*** |

b) *Posúďte a pri príkladoch vyberte, či sa jedná o dôvernosť, integritu alebo dostupnosť:*

| ***Príklad*** | ***Bezpečnostná požiadavka*** *(vyberte správnu podľa príkladu)* |
|---|---|
| *V škole: zabezpečenie hodnotení žiaka tak, aby ich **nemohol nikto zmeniť mimo učiteľa**, ktorý má právo toto hodnotenie udeľovať* | ***?*** <br> ***Dôvernosť*** <br> ***Integrita*** <br> ***Dostupnosť*** |
| *V škole: aby známky žiaka **neboli sprístupnené iným osobám ako sú oprávnené osoby** (napr. učitelia, rodičia).* | ***?*** <br> ***Dôvernosť*** <br> ***Integrita*** <br> ***Dostupnosť*** |
| *V škole: **zabezpečenie prístupu k známkam žiaka len vtedy, keď sa známky udeľujú**, ale potom už nie (teda počas aktuálneho školského roka, nie minulého).* | ***?*** <br> ***Dôvernosť*** <br> ***Integrita*** <br> ***Dostupnosť*** |

## VYSVETLENIE (CCA 12 MIN.):

Postupne vyzveme jednotlivé skupiny, aby predstavili ostatným svoje výsledky z úlohy 1. Na základe kontroly správnosti budeme v dvoch ďalších dvoch úlohách spoločne analyzovať, k porušeniu ktorej z troch základných bezpečnostných požiadaviek v danej situácii došlo. Každú úlohu najprv žiakom predstavíme a formou diskusie vedieme žiakov k prezentovaniu ich názorov a argumentov. Výsledky si následne poznačia do pracovných listov. Následne im premietneme frontálne doplnkové video k úlohe.

***Poznámka:***

Doplnkové videá sú v anglickom jazyku, nakoľko tematicky vhodné videá v slovenčine (ani s titulkami) v čase prípravy tejto metodiky neboli dostupné. Stredoškoláci (metodika je odporúčaná pre tretí ročník gymnázia) by mali mať už dostatočnú znalosť anglického jazyka, aby týmto videám porozumeli. Pokiaľ učiteľ usúdi, že jazykové znalosti žiakov nebudú postačujúce, je dobré, aby požiadal niektorého zo žiakov (s lepšou znalosťou angličtiny), aby prerozprával obsah videa ostatným, prípadne to môže urobiť aj učiteľ.

***Úloha 2*** *Soňa sa zastavila vo svojej obľúbenej kaviarni, aby si vypila popoludňajšiu kávu. Pokiaľ sa pripravoval jej obľúbený nápoj, tak sa cez telefón pripojila na otvorenú wifi sieť, ktorá sa zdala, že je sieťou tejto kaviarne. Vytvoril ju však hacker, ktorý tak napadol jej internetovú komunikáciu. Soňa sa napojila na svoj internet banking a tým pádom sa hacker dostal k údajom jej bankového účtu. Ktorá požiadavka na informačnú bezpečnosť nebola splnená?* _____

*Pozrite si nasledujúce video, ktoré ukazuje podobnú situáciu na stanici v Utrechte:* https://youtu.be/zcmmFQGxMNU.

***Úloha 3*** *Vladimír, zamestnanec vo finančnom oddelení významnej verejnoprávnej spoločnosti, dostane e-mail od výkonného riaditeľa spoločnosti s priloženým PDF. PDF sa týka zárobku spoločnosti v treťom štvrťroku. Vladimír si nepamätá názov oddelenia, kde pracuje riaditeľ a ktoré vytvorilo PDF. Jeho zvedavosť vrcholí, takže otvára prílohu. Rovnaký scenár sa odohrá v celej organizácii, pretože desiatky ďalších zamestnancov sú úspešne nalákaní, aby klikli na prílohu. Po otvorení súboru PDF sa na počítačoch zamestnancov nainštaluje ransomvér[3] a začne proces zhromažďovania a šifrovania firemných údajov. Cieľom útočníkov je finančný zisk, pretože si uchovajú údaje spoločnosti a hrozia zašifrovaním diskov zamestnancov až do zaplatenia výkupného. Ktorá požiadavka na informačnú bezpečnosť nebola splnená?* _____

*Pozrite si dramatizáciu spôsobu, ako mohol tento útok ransomvéru nastať:* https://youtu.be/668mc-_kJBM

Položme žiakom otázku, kto podniká útoky na dáta a siete – počuli už o nejakých prípadoch?

- Môžu to byť amatéri, tiež známi ako skriptanti, ktorí majú len malú alebo žiadnu zručnosť. Často používajú existujúce nástroje alebo pokyny nájdené na internete na spustenie útokov.
- Hacktivisti protestujú proti organizáciám alebo vládam prostredníctvom uverejňovania článkov a videí.
- Hackeri sú motivovaní finančným ziskom. Títo kybernetickí kriminálnici chcú získať prístup k našim bankovým účtom, osobným a ďalším údajom, čo môžu zneužiť napríklad na prenesenie peňažných tokov na svoju stranu.
- Národné štáty sa tiež zaujímajú o využívanie kybernetického priestoru na priemyselnú špionáž. Krádež duševného vlastníctva môže krajine priniesť významné výhody v medzinárodnom obchode.

**Internet vecí** je všade okolo nás a rýchlo sa rozširuje. Ako sú tieto zariadenia zabezpečené? V októbri 2016 útok proti spoločnosti Dyn zničil mnoho webových stránok. Útok pochádzal z webových kamier, rekordérov, smerovačov a iných zariadení internetu vecí, ktoré boli ohrozené škodlivým softvérom. Tieto zariadenia vytvorili „botnet" - sieť robotov, ktorá bola kontrolovaná hackermi a použila sa na vytvorenie obrovského útoku, ktorý zakázal základné internetové služby.

Ak dôjde k poškodeniu údajov, musí byť k dispozícii ich záloha. Na kontrolu integrity údajov, teda či nedošlo k ich pozmeneniu, sa používa zašifrovaný (zahašovaný) kontrolný súčet počas prenosu údajov cez sieť. **Hašovací program** možno teda použiť na overenie toho, či sa údaje zmenili, alebo nie. Hašovací program vykoná hašovanie na údajoch alebo súboroch a vráti nejakú (zvyčajne oveľa kratšiu) hodnotu. Existuje mnoho rôznych hašovacích algoritmov, niektoré veľmi jednoduché a niektoré veľmi zložité. Keď sa rovnaký hašovací algoritmus vykoná na rovnakých údajoch, vrátená hodnota je vždy rovnaká. Ak dôjde k akejkoľvek zmene údajov, tak vrátená hodnota haš bude iná.

[3] typ škodlivého softvéru, ktorý blokuje počítačový systém alebo šifruje dáta v ňom zapísané, a potom požaduje od obete výkupné za obnovenie prístupu

Na učiteľskom počítači ukážeme frontálne pomocou dataprojektora žiakom prácu s hašovacím programom **HashCalc**. Vytvorme jednoduchý textový súbor v poznámkovom bloku a nazvime ho ***skuska.txt***. Využime hašovací program **HashCalc**, aby sme zistili integritu údajov v súbore. Pomocou hašovacieho algoritmu **MD5** zistíme hodnotu haš nášho súboru. Skopírujme ju a zapíšme do iného textového dokumentu. Súbor ***skuska.txt*** zmeňme (napr. zmažme nejakú medzeru alebo urobme iný drobný zásah) a súbor uložme. Znova pomocou hašovacieho algoritmu **MD5** vytvorme hodnotu haš súboru ***skuska.txt***. Skopírujme hodnotu haš a porovnajme s predchádzajúcou hodnotou. Sú rovnaké?

## ROZPRACOVANIE (CCA 10 MIN.):

Žiaci pracujú vo dvojiciach – každej dvojici pridelíme jeden z príkladov útoku z úlohy 4 v pracovnom liste. Nakoľko v úlohe sú 3 rôzne príklady, viacero dvojíc bude nezávisle pracovať na analýze toho istého príkladu a na konci si svoje zistenia porovnajú.

***Úloha 4***

*Riešte podľa pokynov učiteľa*

*Pomocou vyhľadávacieho nástroja vyhľadajte informácie o každom z nižšie uvedených kybernetických útokov. Vaše vyhľadávanie pravdepodobne prinesie viac výsledkov, od spravodajských článkov až po technické články. Vyhľadajte informácie, kedy sa útok odohral a aké mal ciele, alebo aké škody napáchal. Vyplňte nasledujúcu tabuľku:*

| ***Popíšte následky:*** | ***Realizované útoky*** | | |
|---|---|---|---|
| | ***Porušenie bezpečnosti kariet Target (Target Credit Card Breach)[4]*** | ***Stuxnet Virus*** | ***Prelomenie bezpečnosti firmy Sony Pictures Entertainment (Sony Pictures Entertainment Hack)*** |
| ***Aké boli obete útoku?*** | | | |
| ***Aké technológie boli použité na útok?*** | | | |
| ***Kedy sa útok stal?*** | | | |
| ***Aká bola motivácia útočníkov? Čo dúfali, že dosiahnu?*** | | | |
| ***Aký bol výsledok útoku? (ukradnuté údaje, výkupné, poškodenie systému atď.)*** | | | |

[4] https://www.nbcnews.com/technology/massive-target-credit-card-breach-new-step-security-war-hackers-2D11778083

| | | | |
|---|---|---|---|
| ***Kto boli útočníci*** | | | |

## HODNOTENIE (CCA 8 MIN.):

Dvojice žiakov, ktoré pracovali na rovnakom type útoku, vytvoria spoločnú skupinu a porovnajú si zistené výsledky. Následne jeden žiak z každej skupiny odprezentuje v krátkosti ostatným skupinám informácie o nimi analyzovanom útoku

Na evalváciu slúži sebahodnotiaca rubrika, pomocou ktorej žiaci zaškrtnutím sami zhodnotia úroveň osvojenia vedomostí a zručností, ako aj splnenie cieľov hodiny. Zároveň rubrika slúži na zhrnutie základných poznatkov a zručností, ktoré si žiaci na hodine mali osvojiť.

*Sebahodnotiaca rubrika*

| **ČO SOM SA NAUČIL/NAUČILA...** | |
|---|---|
| Vymenovať základné bezpečnostné požiadavky (**CIA**) | **VIEM / VIEM S POMOCOU / NEVIEM** |
| Vysvetliť vlastnými slovami/na príklade, čo jednotlivé bezpečnostné požiadavky znamenajú | **VIEM / VIEM S POMOCOU / NEVIEM** |
| Vysvetliť, na čo slúži hašovací program | **VIEM / VIEM S POMOCOU / NEVIEM** |
| Uviesť príklady na rôzne typy útokov, pri ktorých môže dôjsť k porušeniu bezpečnosti IT | **VIEM / VIEM S POMOCOU / NEVIEM** |