TYPY ÚTOKOV NA IT

ÚVOD

Toto je druhá metodika zo série troch metodík, ktoré sú venované problematike bezpečnosti IT. Táto problematika je veľmi zložitá. Pochopenie spôsobu infiltrácie sa škodlivého softvéru, útokov na siete a podobne je znalosť, ktorá sa týka všetkých ľudí používajúcich IT. Tieto metodiky predstavujú všeobecné zásady bezpečného a zodpovedného používania IT, pre prácu s počítačovou sieťou a počítačmi vôbec.

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 (10 minút)** – motivačný rozhovor so žiakmi na tému škodlivého softvéru a útokov na sieť, skupinová práca s pracovným listom (úloha 1) a predstavenie mapy digitálnych útokov
- **Skúmanie (5 minút)** – riešenie úlohy z pracovného listu formou práce vo dvojiciach (úloha 2)
- **Vysvetlenie (10 minút)** – zhrnutie výsledkov úlohy z pracovného listu, úvod do sociálneho inžinierstva
- **Rozpracovanie (12 minút)** – práca vo dvojiciach s pracovným listom (úloha 3)
- **Hodnotenie (3 minúty)** – sebahodnotiaca rubrika

ZAPOJENIE (CCA 10 MIN.):

Hodinu začneme rozhovorom so žiakmi. Položíme im otázku, či už mali svoj počítač napadnutý malvérom, škodlivým softvérom. Aké to malo príznaky? V odpovediach žiakov by mali byť spomenuté tieto príznaky:

zvyšuje sa využitie procesora, rýchlosť počítača klesá, počítač často zamrzne alebo havaruje, rýchlosť prehliadania webových stránok klesá, vyskytujú sa nevysvetliteľné problémy so sieťovými pripojeniami, nejaké súbory sú upravené, niektoré súbory sú odstránené, vyskytujú sa neznáme súbory, programy alebo ikony na pracovnej ploche, sú spustené neznáme procesy, programy sa vypínajú alebo sa znovu konfigurujú, bez vedomia alebo súhlasu používateľa sa odosiela e-mail, a pod.

Následne sa žiakov vyzveme, či by vedeli vysvetliť, čo je to škodlivý softvér. Mali by sme dospieť ku konštatovaniu, že je to akýkoľvek program, ktorý možno použiť na ukradnutie údajov, obchádzanie kontrol prístupu alebo spôsobenie poškodenia alebo ohrozenia systému.

Keďže v praxi existuje veľké množstvo rôznych druhov škodlivého softvéru, pokúsime sa pozrieť na niektoré jeho druhy. Žiakov rozdelíme do 3-4členných skupín, v ktorých budú spoločne riešiť úlohu 1 z pracovného listu.

Poznámka:

V úlohe 1 je spomenutých pomerne veľa rôznych odborných termínov. Odporúčame žiakom ešte pred začatím riešenia vysvetliť, že **nie je potrebné, aby sa všetky pojmy učili (aj s definíciami)** – pojmy sú tu spomenuté skôr len na ilustráciu veľkej rozmanitosti škodlivého kódu, aj keď predpokladáme, že niektoré z týchto pojmov už niekde počuli. Niektoré môžu vyskúšať priradiť na základe diskusie v ich skupine, prípadne ak si nie sú istí, tak môžu si k zložitejším termínom dať otáznik a v diskusii po ukončení práce na úlohe sa k týmto pojmom vrátime.

Úloha 1 *Priraďte typy škodlivých programov k ich popisom. Pracujte v skupinách. Svoj výber zdôvodnite.*

Typy malvéru	***Popis***
MitMO (Man-In-the-Mobile)	*1. Malvér vytvorený na automatické spúšťanie akcií obvykle online*
Vírus	*2. Malvér vytvorený na zablokovanie počítačového systému alebo dát, ktorý obsahuje výzvu na zaplatenie*
Trojský kôň	*3. Malvér určený na modifikovanie OS za účelom vytvorenia zadných vrátok (backdoor)*
Ransomware	*4. Malvér, ktorý sa často sa viaže na legitímny softvér, tento malvér je určený na sledovanie aktivity používateľa*
Bot	*5. Škodlivý spustiteľný kód, ktorý je priložený k iným spustiteľným súborom, často sú to legálne programy*
Scareware	*6. Malvér, ktorý robí škodlivé operácie pod pláštikom nejakých normálnych požadovaných operácií*
Adware	*7. Malvér niekedy zviazaný s iným softvérom a je určený na automatické spúšťanie reklám*
Červ	*8. Malvér na prevzatie kontroly nad mobilným zariadením*
Spyware	*9. Malvér, ktorý je určený na presvedčenie používateľa, aby urobil určitú akciu na základe jeho strašenia, strachu*
MitM (Man-In-The-Middle)	*10. Umožňuje útočníkovi prevziať kontrolu nad zariadením bez vedomia používateľa a zachytiť informácie o používateľovi predtým, ako ho odovzdá do určeného cieľa*
Rootkit	*11. Škodlivý kód, ktorý sa replikuje (vytvára svoje kópie) pomocou nezávislého využívania bezpečnostných dier v počítačovej sieti*

Žiaci pracujú 5 minút, potom spoločne zrekapitulujeme správne odpovede a položíme otázku, či sa s niektorými názvami, použitými v úlohe 1, už predtým stretli. Taktiež sa ich spýtame, či – okrem škodlivého softvéru – sa stretli aj s inými formami útokov na IT - nemusí to byť ich osobná skúsenosť, ale pravdepodobne počuli alebo čítali o útokoch na sieť, kedy boli napadnuté napr. servery vládnych alebo iných inštitúcií a pod. O tom, že tieto útoky nie sú zriedkavosťou, svedčí aj mapa digitálnych útokov (http://www.digitalattackmap.com/), ktorá zachytáva práve prebiehajúce útoky a ktorú žiakom ukážeme pomocou dataprojektora:

Objasneniu podstaty týchto útokov sa budeme venovať v nasledujúcej aktivite v rámci skúmania.

SKÚMANIE (CCA 5 MIN.):

Žiaci pracujú vo dvojiciach na počítačoch alebo tabletoch s pracovným listom (úloha 2) s krátkym článkom, ktorý im predstaví základnú podstatu DoS a DDoS útokov, pričom si do pracovným listov zaznačia vysvetlenia najdôležitejších pojmov. Žiakov upozorníme, že nie je potrebné čítať celý článok, ale zameriame sa len na jeho prvé dve časti venované **DoS** a **DDoS útokom**. V tejto etape záznamy žiakov nevyhodnocujme ani nekomentujme.

Úloha 2 *V prehliadači načítajte stránku* http://preventista.sk/info/spustite-siet-2-ked-sa-vam-sluzba-odoprie/ *a prečítajte si úvodné dve časti venované* ***DoS*** *a* ***DDoS útokom****. Na základe prečítaného zodpovedzte v stručnosti nasledovné otázky:*

a) Čo znamená skratka ***DoS*** *(po anglicky, po slovensky)?* _____

b) Čo môže mať za následok útok na server? _____

c) V čom sa líši útok ***DDoS*** *od útoku* ***DoS****?*

_____

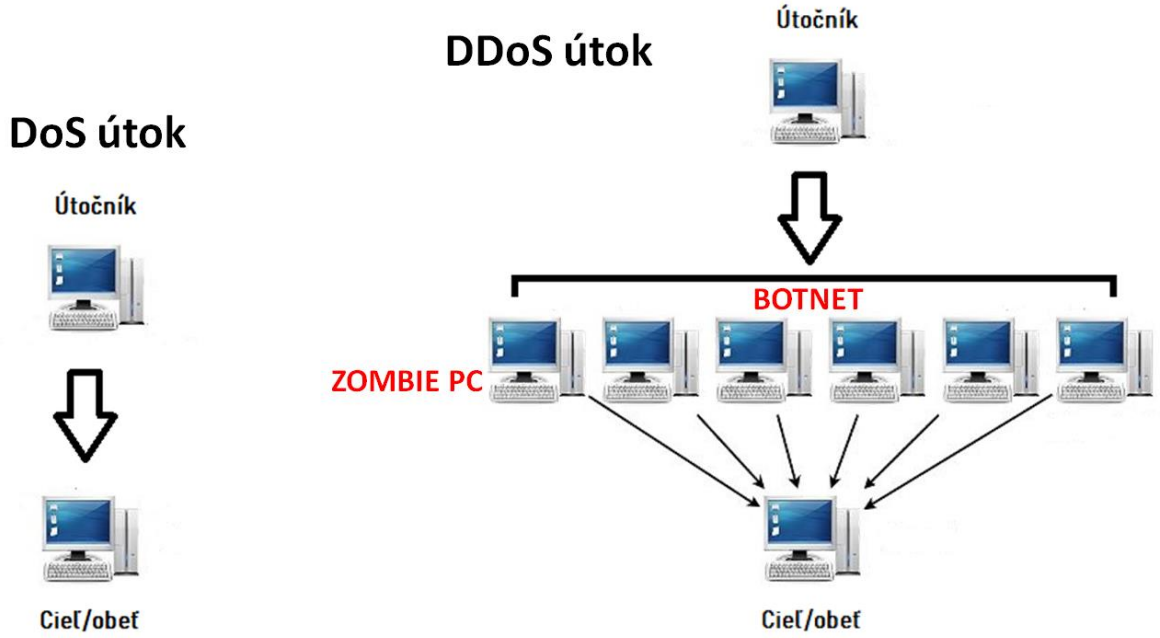
d) Ako získa útočník kontrolu nad iným počítačom? _____

e) Čo je to ***zombie*** *počítač?* _____

f) Čo je to ***botnet****?* _____

VYSVETLENIE (CCA 10 MIN.):

Postupne vyzývame žiakov, aby pomocou odpovedí z úlohy 2 objasnili základnú podstatu **DoS** a **DDoS** útokov, pričom na vysvetlenie môžeme využiť sprievodnú prezentáciu (snímka 2), kde žiaci sa pokúsia vysvetliť podstatu týchto útokov aj na pripravených obrázkoch:



Poznámka:

Pre učiteľa zaujímavé video na rozšírenie problematiky a ako pomoc pri vysvetľovaní môže byť napr. https://www.lupa.cz/clanky/jan-hruska-o2-ddos-utoky/. Toto video žiakom z časových dôvodov v rámci hodiny nepustíme, ale môžeme im ho odporučiť ako domácu úlohu.

Pravdepodobne sa niektorí žiaci dočítali (pri riešení úlohy 2) aj o tom, že botnety sú predmetom obchodovania na čiernom trhu – môžeme ich vyzvať, aby to ostatným objasnili, čo sa o tom dozvedeli. Položme žiakom otázku, čo môže byť obsahom útokov, resp. ako môže vyzerať priebeh takéhoto útoku u obete – spravidla je výsledkom, napr.:

- spotreba zdrojov stroja, napr. „zaplavením“ prevádzky náhodnými dátami, ktoré zabraňujú toku skutočných dát , extrémnym zaťažením cieľového procesora, alebo zahltením pamäte, dokonca až poškodenie fyzických sieťových komponentov,
- prekážanie na komunikačnom médiu medzi určenými užívateľmi tak, že im znemožní adekvátne komunikovať, narušenie stavu komunikácie,
- vloženie chybných konfiguračných informácii, ...

Napokon žiakov vyzveme, aby navrhli, ako by mohli doma ochrániť svoj počítač, aby sa nestal obeťou (ani súčasťou) takéhoto útoku. Žiaci by mali spomenúť:

- **antivírusový systém** - počítač sa infiltráciou trójskym koňom nestane „zombie“ počítačom,

- **firewall** – jeho úlohou je prepúšťať len komunikáciu, o ktorú sme žiadali, alebo ktorú sme posielali,
- **e-mailové filtre** – na obmedzenie nechcenej komunikácie.

Tieto tri myšlienky sú zhrnuté aj v sprievodnej prezentácii (snímka 3).

Posledným typom útokov, ktorým sa v rámci hodiny budeme venovať, sú **metódy sociálneho inžinierstva,** čo sú postupy, ktoré sa zameriavajú na manipuláciu bežných spôsobov ľudského správania a existuje tu len obmedzená množina technických (alebo softvérových) opatrení na ochranu pred týmito útokmi a preto je nevyhnutné zvyšovanie bezpečnostného povedomia používateľov IT. Príkladom je **baiting**, pri ktorom útočník nastraží infikované fyzické dátové médium (napr. USB kľúč, DVD apod.) na mieste, kde ho obeť určite nájde. V prípade DVD alebo CD médií sa dôveryhodnosť tohto média zvyšuje jeho atraktívnym označením. Napr.: „návrh miezd na rok 2016“ alebo „plán prepúšťania zamestnancov“. Útočník následne počká, kým obeť pripojí nastražené médium k svojej pracovnej stanici a škodlivý kód sa nainštaluje. Iná podoba je online reklama a webové stránky. Poznávacím znakom môže byť to, že tieto stránky ponúkajú niečo, čo je príliš dobré na to, aby to bola pravda. My sa špecificky zameriame na inú, veľmi rozšírenú metódou sociálneho inžinierstva - **phishingové útoky**. Položme teda žiakom najprv otázku, či sa stretli s pojmom **phishing**. Je to spôsob útoku, pri ktorom sa útočník pokúša získať citlivé informácie prostredníctvom elektronických komunikácií (napr. e-mailom) vydávaním sa za dôveryhodnú entitu (napr. za banku alebo inú všeobecne známu organizáciu), pričom využíva manipuláciu človeka a klamstvo na to, aby od používateľa vylákal prihlasovacie údaje, údaje o kreditných kartách alebo nakazil jeho počítač škodlivým kódom. Ako ukážku môžeme žiakom ukázať dva phishingové e-maily zo sprievodnej prezentácie (snímka 4 a 5).

Poznámka:

Napriek tomu, že sa jedná o veľmi ľahko odhaliteľné phishingové e-maily, sú to reálne príklady a stále sa nájdu používatelia, ktorí na ne zareagujú – možno sa so žiakmi zamyslieť, čo vedie týchto používateľov k tomu, aby na ne zareagovali alebo položiť aj trochu „provokatívnu“ otázku – ako by zvýšili „presvedčivosť“ a „dôveryhodnosť“ týchto predložených e-mailov, aby boli ťažšie odhaliteľné. Pri tejto otázke však je potrebné byť opatrný, aby žiaci nebrali takýto postup ako „navádzanie“ na tvorbu phishingových e-mailov; treba zdôrazniť, že tu ide o uvedomenie si prvkov, ktoré aj útočníci využívajú pri svojich postupoch.

ROZPRACOVANIE (CCA 12 MIN.):

Rozlíšiť phishingový e-mail od pravého (nepodvodného) je niekedy problém, čo si žiaci budú môcť odskúšať na phishingovom teste[1], ktorý budú samostatne riešiť v úlohe 3 z pracovného listu na počítačoch alebo tabletoch.

[1] test je prístupný na stránke **Vládnej jednotky pre riešenie počítačových incidentov v Slovenskej republike, CSIRT (Computer Security Incident Response Team Slovakia)** na adrese https://www.csirt.gov.sk/, kde je možné nájsť aj ďalšie informácie v časti **Bezpečnostná študovňa**, napr. aj k téme sociálneho inžinierstva (https://www.csirt.gov.sk/socialne-inzinierstvo-812.html)

Úloha 3 *Vyskúšajte si* ***phishingový test*** *na stránke* https://www.csirt.gov.sk/osvedcene-postupy/navody-a-odporucania/phishingovy-test-871.html.

Phishingový test

Náš phishingový test Vám poskytne možnosť otestovať sa v odhaľovaní falošných e-mailov, ktorých cieľom je získanie informácii a často aj spustenie škodlivého kódu na zariadení príjemcu takejto správy.

Test sa skladá celkovo zo 17 testovacích otázok. Vašou úlohou bude rozhodnúť či zobrazený e-mail, ktorý prijal Chuck Norris (chucknorris@gmail.sk), je **legitímny** alebo **podvrhnutý útočníkom**.

Test spustíte kliknutím tlačidla ***Spustiť test***.

Prajeme Vám veľa úspechov.

Spustiť test

HODNOTENIE (CCA 3 MIN.):

V krátkosti prediskutujeme so žiakmi výsledky, ktoré dosiahli vo phishingovom teste a pri ktorých e-mailoch mali najväčšie problémy.

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...	
Uviesť niekoľko príkladov na malvér	**VIEM / VIEM S POMOCOU / NEVIEM**
Vlastnými slovami vysvetliť, ako prebieha DoS a DDos útok	**VIEM / VIEM S POMOCOU / NEVIEM**
Vysvetliť, čo je to phishing	**VIEM / VIEM S POMOCOU / NEVIEM**
Identifikovať niektoré znaky phishingového e-mailu	**VIEM / VIEM S POMOCOU / NEVIEM**

ALTERNATÍVY METODIKY

Na základe skúseností z praxe je možné, že žiakov táto téma zaujme a rozprúdi sa na hodine živá diskusia. V takom prípade môže učiteľ zvážiť zaradenie phishingového testu na domácu úlohu.