VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta elektrotechniky a komunikačních technologií

Závěrečná práce doplňujícího pedagogického studia

Implementace kybernetické bezpečnosti do ŠVP pro Informatiku a výpočetní techniku na gymnáziích

22. srpna 2017

Vedoucí práce: PhDr. Petra Fiľová

Autor práce: Bc. Daniel Dušek

Obsah

1 Úvod

Stejně jako bylo devatenácté století nazývané stoletím páry a dvacáté století stoletím techniky, bude jednou pravděpodobně dvacáté první století nazývané stoletím počítačů a sítí. Oblast techniky a informačních technologií se rozvíjí neustále vyšší a vyšší rychlostí, dostupnost „chytré“ elektroniky se zvyšuje tempem podobným. Společně s technikou a její vyšší dostupností se však objevuje další, bohužel nepříjemný fenomén – a sice zneužívání technologií a jejich vysoké dostupnosti k páchání trestné činnosti.

Trend zneužívání technologií a nedostatečné vzdělanosti v oblasti počítačové bezpečnosti lidí s nimi pracujících roste s každým rokem více a více. Útoky související s distribucí, v době psaní práce velmi populárního škodlivého software, zvaného ransomware vzrostly v počtu od roku 2015 neuvěřitelných 300%.

Na jednu stranu možná i uklidňujícím faktem je, že v případě ransomware jsou cílem typicky organizace, nikoliv jednotlivci. Bohužel i v tomto případě se často obětí stane právě i jednotlivec, a to zejména díky způsobu, kterým se ransomware a jemu podobné škodlivé programy šíří. Jedním z častých scénářů je případ, kdy je počítač infikován prostřednictvím nakaženého souboru typu .xls(x), .doc(x), .ppt(x) apod., tedy soubory běžně produkované nástroji sady Microsoft Office. Druhým, opět velmi častým scénářem je pak případ, kdy se škodlivý soubor pouze tváří být souborem dříve jmenovaných typů, avšak ve skutečnosti je souborem úplně jiného typu, obsahujícího škodlivý kód. V obou dvou scénářích je klíčové, aby ovšem pochybil lidský článek pracující s takovýmto souborem. Tomuto pochybení by bylo poměrně snadné předcházet, a to vyšším obecným povědomím o tom jak správně a bezpečně pracovat s počítačem a internetem.

Tohoto obecně vyššího povědomí by bylo možné dosáhnout například kladením vyššího důrazu na výuku kybernetické bezpečnosti ve školách v rámci výuky informačních technologií, výpočetní techniky a informatiky. V konkrétních termínech například místo kladení obrovského důrazu pouze na výuku práce s nástroji kancelářského balíku Microsoft Office slevit lehce z časové dotace vyhrazené na vysvětlování funkcionality a následné zkoušení žáků z ní, a tuto časovou úsporu věnovat k osvětlování způsobů a principů, kte-

rými jsou soubory balíku Microsoft Office zneužívány hackery pro napadení počítačů a způsobů obrany a bezpečné práce s těmito soubory. Snížení časové dotace na vysvětlování a zkoušení funkcionality by, dle autora této práce, nemuselo mít vyloženě negativní dopad, neboť většina dnešní generace přichází do styku s počítači a těmito programy na denní bázi. Navíc jsou tyto programy v posledních letech průběžně neustále vylepšovány z hlediska uživatelské přívětivosti, aby práce s nimi byla více intuitivní a snadná.

Dalším důvodem pro zavedení výuky kybernetické bezpečnosti do osnov je zcela opačný pól kybernetické bezpečnosti. Doposud bylo psáno hlavně o způsobech ochrany a osvěty běžných uživatelů výpočetní techniky proti útokům ze strany hackerů. Stejně, neli více důležitou částí výuky kybernetické bezpečnosti by měla být osvěta žáků o možných následcích zneužívání výpočetní techniky k páchání trestných činů. Mezi studenty se vyskytuje dnes již poměrně veliká část žáků, která je seznámena s prací s počítačem natolik, že je potenciálně schopná počítač i nějakým způsobem programovat. Někteří z těchto žáků mohou potřebovat vyjasnit fakt, že existuje hranice, za níž nesmí při programování svých aplikací zajít. Ačkoliv se to může zdát z prvního pohledu jako celkem jednoduchá otázka k diskusi, nemusí to vždy být pravda. Konkrétním případem může být 16 letý chlapec Ashkan Hosseini, jenž naprogramoval aplikaci, kterou nahrál na CD s rodinnými fotkami [1]. Aplikace následně způsobila, že po strčení CD do počítače došlo k vymazání všech rodinných fotek jak z CD, tak z počítače, do kterého bylo CD zastrčeno. Ashkan naprogramoval tuto aplikaci za účelem odstranění fotek na kterých se nacházel – jeho úmysly tedy nebyly vyloženě špatné a díky tomu, že CD putovalo pouze mezi rodinou, Ashkan nebyl nikým žalován. Pokud by se ale stalo, že by jeho aplikace unikla do světa a napadla cizí počítač, dopustil by se již vážného trestného činu, aniž by si tyto následky svých akcí uvědomil. V Americe by to pro něho pak mohlo znamenat až 5 let vězení. Příběh Ashkana Hosseiniho dopadl tedy naštěstí pro něho dobře, kde navíc jeho rodiče měli dostatek reflexe a nabídli mu možnost studovat oblast boje proti kybernetické kriminalitě, které se chopil. Ne všichni žáci však musí vždy přesně odlišit hranici toho, kdy končí „legrace“ a začíná páchání trestného činu, alespoň ne v oblasti počítačů a sítí, a ne všichni musí mít to štěstí, jaké Ashkan měl. I z tohoto důvodu je třeba šířit povědomí

o kybernetické bezpečnosti a implikacích, které může mít na život jedince nedodržování jejích zásad.

V letech 2007–2009 byla reakcí českého školství na prudký rozvoj a expanzi výpočetní techniky snaha naučit žáky a studenty s těmito novými technologiemi pracovat a interagovat. Tato snaha byla realizována v rámci vlnově vydávaných rámcově vzdělávacích programů – dále jen RVP – v nichž byl již povinně vyhrazen prostor pro výuku informačních a komunikačních technologií a informatiky [2]. Autor této práce považuje tuto reakci za dobře načasovanou a vhodnou.

Nyní však nastává nová éra, kdy zařízení schopná připojení k Internetu jsou doslova i obrazně na každém našem kroku. Každé zařízení připojené k Internetu se může stát cílem útoku, stejně jako se obětí počítačové kriminality může stát každá osoba s těmito zařízeními pracující. Vzniká tedy takto nová potřeba většího důrazu na výuku těchto aspektů práce s informačními technologiemi. Tato práce má za cíl demonstrovat konkrétní možnou implementaci takové výuky do výuky ICT na gymnáziích.

2 Slovníček pojmů

V textu této práce je možné se setkat s pojmy, které mají speciální význam v oblasti počítačové či kybernetické bezpečnosti, jenž se často liší od pocitového významu, který by si oblasti neznalý čtenář mohl vytvořit. Tato sekce si klade za cíl rozptýlit možné nejasnosti a mnohoznačnosti.

Malware – Souhrné označení pro programy které vykonávají škodlivou činnost (trojské koně, viry, programy špehující uživatele, programy zobrazující uživateli nevyžádanou reklamu, a další).

Škodlivý kód – Chce-li programátor přikázat počítači, aby vykonal nějakou činnost, popíše tuto činnost pomocí tzv. *kódu*. Škodlivý kód je pak takový kód, který je-li vykonán počítačem, provede něco, co uživatel/majitel tohoto počítače nechce. Útočníci se při útoku snaží typicky právě vykonat škodlivý kód na zařízení, které napadají. Tento škodlivý kód bývá velmi často nastražen a ukryt tak, aby si uživatel pracující s počítačem vůbec neuvědomil, že kód spouští a vykonává.

Nakažený soubor – Soubor v němž je kromě původního obsahu souboru navíc obsažen škodlivý kód. Škodlivý kód do souboru umístil buď přímo, nebo zprostředkovaně (například prostřednictvím škodlivého programu) útočník.

Ransomware – Škodlivý program založený na principu držení rukojmí. Program po průniku do počítače zašifruje některé soubory, popřípadě uživateli úplně znemožní práci s počítačem. Za zpřístupnění souborů či zařízení je po uživateli požadováno zaplacení výkupného. Zaplacení výkupného nemusí vždy vést k získání objektu, který je držen jako rukojmí.

3 Výuka informatiky dle Rámcového Vzdělávacího Programu a Školního Vzdělávacího Programu

Tato část práce se zabývá prostorem vyhrazeným pro výuku informatiky v rámci Rámcového Vzdělávacího Programu (dále jen RVP) a jeho možnou utilizací pro výuku kybernetické bezpečnosti. Dále je zde rozebrán konkrétní Školní Vzdělávací Program (dále jen ŠVP) v rámci něhož je vyhrazen prostor pro výuku informatiky. Jsou zde také zmíněny očekávané výstupní dovednosti, kterými by student po absolvování vyučování informatiky měl disponovat.

4 Vstupní dovednosti

V této části práce jsou vymezeny vstupní dovednosti, kterými by studenti pro úspěšnou výuku kybernetické bezpečnosti měli disponovat. Dále je zde navrženo a argumentováno časové zasazení výuky napříč ročníky, pokryty jsou také možné formy výuky vhodné pro předmět kybernetické bezpečnosti a nezbytné pomůcky pro kvalitní výuku.

4.1 Vstupní dovednosti

Text vstupních dovedností.

4.2 Pomůcky pro výuku

Test pomůcek ve výuce.

4.3 Časový rozvrh napříč ročníky

Text časového rozvrhu napříč ročníky

4.4 Formy výuky

Způsobů a forem, kterými lze vyučovat a demonstrovat kybernetickou bezpečnost by se jistě dalo vymyslet mnoho. Zde jsou shrnuty formy výuky, které autor práce považuje za efektivní a vhodné v oblasti kybernetické bezpečnosti, společně s argumentací využití právě těchto forem.

4.4.1 Forma výuky: Výklad s živou ukázkou

Text formy výuky.

4.4.2 Forma výuky: Praktický domácí úkol, studenti kooperují

Text formy výuky.

4.4.3 Forma výuky: Návštěva člověka z praxe

Text formy výuky.

5 Tématický plán výuky

Na následujících stránkách jsou popsány dva možné tématické plány výuky kybernetické bezpečnosti na gymnáziích. První tématický plán uvažuje možnost výuky kybernetické bezpečnosti v rámci výuky hodin informačních technologí po její celou dobu stanovenou školou. Druhý tématický plán je realizován s předpokladem, že například v rámci 3. a 4. ročníku, je pro výuku kybernetické bezpečnosti dedikován samostatný předmět.

V rámci prnvího tématického plánu má výuka kybernetické bezpečnosti sloužit jako *rozšíření* nebo *doplnění*, které je možné vložit do standardní výuky informatiky realizované na gymnáziích.

V případě druhého plánu, narozdíl od výuky kybernetické bezpečnosti v rámci výuky informatiky umožňuje studentům se přímou soustředit a profilovat v oblasti kybernetické bezpečnosti. Další výhodou takovéto výuky je možnost podání látky v nahuštěnější formě, s vyšším důrazem na konkrétní problémy a jejich správné uchopení. V případě dedikovaného předmětu se není nutné vázat na probírané oblasti ve výuce standardní informatiky, ale je možné se věnovat konkrétním problémům kybernetické bezpečnosti a jejich řešení. Profilování se studentů v oblasti kybernetické bezpečnosti pro ně v dnešní době může být obzvláště zajímavé, neb se očekává, že rokem 2023 bude nedostatek kvalifikovaných specialistů v oblasti kybernetické (a informační) bezpečnosti.

6 Osnova témat v jednotlivých ročnících

Tato část práce popisuje rozložení témat napříč jednotlivými ročníky a jejich náročnost. Jsou zde opět uvedeny dvě varianty – pro výuku kybernetické bezpečnosti v rámci výuky informatiky a pro výuku kybernetické bezpečnosti jako samostatného předmětu.

7 Ukázky příprav na hodiny

V této kapitole práce jsou prezentovány celkem čtyři ukázky možných příprav na hodiny výuky kybernetické bezpečnosti.

7.1 Příprava 1 – Krádeže identity

Příprava na hodinu s tématem **Krádeže identity** je rozdělena do následujících částí:

- Specifikace tématu hodiny,
- stanovené cíle,
- náplň hodiny a časový plán,
- nutné pomůcky pro hodinu,

Struktura rozložení přípravy na hodinu vychází z doporučené obecné struktury v dokumentu *Příprava učitele na výuku. Vzdělávání učitelů.* [3], kde tato obecná struktura je upravena tak, aby odpovídala přípravě na hodinu kybernetické bezpečnosti.

7.1.1 Specifikace tématu hodiny

Hodina se zabývá tématem krádeže identity na Internetu, riziky situací, kdy se člověk stane obětí krádeže identity (aktivní či pasivní oběť) a nejčastějšími typy identit, které jsou odcizovány, nebo jsou podvrhnutelné. V hodině by také měl být popsán a demonstrován způsob, kterým ke zcizení identity může dojít, včetně uvedení možných právních následků takové činnosti.

7.1.2 Stanové cíle

Studenti by po hodině měli rozumět pojmu *krádež identity* a měli by chápat rizika spojená s touto hrozbou. Budou znát kanály, kterými ke krádeži identity může dojít a budou chápat, že jde o na Internetu o velmi běžnou záležitost. Dále by měli být znát právní následky, kterým mohou čelit v případě že se dopustí krádeže identity, a co vše je možné považovat za krádež identity. V hodině dojde k demonstraci jak snadné je podvrhnout

email z téměř jakékoliv emailové schránky, žáci by měli být schopni podvržení emailu zopakovat. Zároveň budou žáci schopní u jakéhokoliv emailu, který dorazí do jejich emailové schránky rozhodnout na základě probraného algoritmu, zda je bezpečné email otevřít, či zda je lepší ho smazat. Existují-li ve třídě žáci, kteří se věnují informatice, nebo mají větší zájem o problematiku efektivní obrany proti podvržení emailové identity, budou jim poskytnuty doplňující zdroje informací, řešící problém.

7.1.3 Náplň hodiny a časový plán

0.–3. minuta - Zápis do třídní knihy, v případě, že výuka probíhá v počítačové učebně, zapnutí počítačů a přihlášení žáků do systému.

4.–10. minuta - Představení tématu krádeže identity, představení očekávané náplně hodiny, podáno formou slovní monologické metody.

11.–30. minuta - Frontální formou výuky kombinovanou s monologickým výkladem, vysvětlení žákům co to je krádež identity, jak se člověk může aktivně i pasivně stát obětí této techniky. Vyučující může pokládat otázky přímo žákům ohledně kanálů, po kterých může dojít k zneužití této techniky a pomáhat jim přijít s reálnými případy. Dále vyučující zdůrazní riziko podvržení cizí identity při emailové komunikaci, názorně demonstruje jak snadné to je – pokud se hodina odehrává v počítačové učebně, vybere z řad studentů dobrovolníka, který se přihlásí na učitelském počítači do emailu a vyučující z telefonu odešle podvržený email do schránky žáka, kde se, se svolením žáka, bude vydávat právě za žáka sedícího za počítačem. Následně třídě vysvětlí, jak velmi důležité v celém demonstračním scénáři bylo, aby dostal k odeslání emailu pod identitou žáka u počítače svolení. Plynule tak může přejít k vysvětlení právní závadnosti podvrhávání emailů a vysvětlí žákům, jakým následkům by mohli čelit, pokud by se pokusili podvržení emailové identity využít k nečestným účelům. Odehrává-li se výuka ve třídě, kde je převaha dívek, je možné uvést příklad ze seriálu *Prolhané krásky (anglicky Pretty Little Liars)*, kde jedna z hlavních postav, Caleb, právě podvržení emailové identity zneužije, aby mu byla zkrácena doba, co musí strávit po škole. V rámci tohoto časového okna také vyučující žákům vysvětlí jednoduchý algoritmus, podle kterého se mohou rozhodovat, zda přílohu, popřípadě celý

email, je možné bezpečně otevřít a nebo je lepší ho smazat. Algoritmus je založen na myšlence odpovědi na otázku: „Očekávám v tento čas, od tohoto odesilatele tuto zprávu?“, je-li odpověď ne, pak je lepší přílohu emailu nikdy neotevírat a spojit se s odesilatelem alternativním způsobem, například zavolat a ověřit, že email skutečně posílali odesilatel.

31.–40. minuta - Pokud žáci mezi 11.-30. minutou nedošli po navádějících otázkách učitele na to, že vytvoření stránky, která vypadá úplně stejně jako jiná stránka za účelem získávání dat uživatelů stránky, jejíž vzhled napodobují, vyučující tuto možnost krádeže identity zmíní. Pokud na ni žáci došli v předchozím bloku sami, zopakuje to ještě jednou, mimochodem se žákům zmíní, že této technice se velmi často říká *phishing* a vysvětlí jim, jak se bránit tomu, aby se nestali obětí – s využitím jednoduché principu zkontrolování adresy webové stránky, na které se nachází pokaždé, než na ní vyplní nějaké důvěrné údaje (heslo, uživatelské jméno, email).

41.–45. minuta - Existují-li žáci s větším zájmem o informatiku a specificky možnou obranu proti krádeži emailové identity, může je vyučující nasměrovat k samostudiu technologií pod zkratkami *DMARC*, *SPF*, *DKIM*. Dále vyučující, bude-li ve třídě zájem, zadá volitelný domácí úkol, kde jeho předmětem bude doručit do schránky vyučujícího umístěné ve službě *gmail.com* podvržený email s přesně zadanými náležitostmi (emailová identita držená taktéž vyučujícím), který nebude doručen do složky SPAM. První ze studentů, který uspěje může získat známku za aktivitu/bonusové body do předmětu.

7.1.4 Nutné pomůcky pro hodinu

Pro splnění stanových cílů hodiny je nutné, aby v místnosti, ve které má být hodina vyučována, byl přítomen počítač s připojením k internetu, s data projektorem. Vyučující by si s sebou měl přinést telefon, nebo notebook, taktéž s přístupem k Internetu. Alespoň 2 zařízení s přístupem k Internetu, kdy jedno ze zařízení je schopné posílat obraz na data projektor jsou nutné k výše popsaným demonstracím.

7.2 Příprava 2 –

Text přípravy na hodinu.

7.3 Příprava 3 –

Text přípravy na hodinu.

7.4 Příprava 4 –

Text přípravy na hodinu.

8 Závěr

Reference

[1] Selena Larsen: Malware researcher helps teen hackers turn skills into careers, *http://money.cnn.com/2017/07/12/technology/malware-researcher-helps-teen-hackers.*

[2] Národní Ústav pro Vzdělávání: Přehled vydávání RVP SOV po vlnách, *http://www.nuv.cz/t/prehled-vydavani-rvp-sov-po-vlnach.*

[3] ZIELENIECOVÁ, Pavla. *Příprava učitele na výuku. Vzdělávání učitelů.* [online prezentace]. Praha: Katedra didaktiky fyziky, Matematicko-fyzikální fakulta, UK, 2015, [cit. 2017-19-08]. Dostupný z WWW: <https://kdf.mff.cuni.cz/vyuka/pedagogika/materialy/2015%20ZS/8%20Priprava%20ucitele%20na%20vyuku.%20Legislativni%20zakotveni%20ucitele.pdf>.