

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

9. září 2017

Vedoucí práce: PhDr. Petra Fiřová

Autor práce: Bc. Daniel Dušek

Obsah

1	Úvod	1
2	Slovníček pojmů	4
3	Výuka informatiky dle Rámcového Vzdělávacího Programu a Školního Vzdělávacího Programu	5
4	Vstupní dovednosti	6
4.1	Vstupní dovednosti	6
4.2	Pomůcky pro výuku	6
4.3	Časový rozvrh napříč ročníky	6
4.4	Formy výuky	6
4.4.1	Forma výuky: Výklad s živou ukázkou	6
4.4.2	Forma výuky: Praktický domácí úkol, studenti kooperují	6
4.4.3	Forma výuky: Návštěva člověka z praxe	7
5	Tématický plán výuky	8
6	Osnova témat v jednotlivých ročnících	9
7	Ukázky příprav na hodiny	10
7.1	Příprava 1 – Krádeže identity	10
7.1.1	Specifikace tématu hodiny	10
7.1.2	Stanovené cíle	10
7.1.3	Náplň hodiny a časový plán	11
7.1.4	Nutné pomůcky pro hodinu	12
7.2	Příprava 2 – Nebezpečí skryté v dokumentech Microsoft Office	13
7.2.1	Specifikace tématu hodiny	13
7.2.2	Stanovené cíle	14
7.2.3	Diskuse o souvislostech se studenty	14

7.2.4	Náplň hodiny a časový plán	15
7.2.5	Nutné pomůcky pro hodinu	16
7.2.6	Text snímků prezentace	17
7.3	Příprava 3 – Obecná bezpečnost na Internetu	17
7.3.1	Specifikace tématu hodiny	17
7.3.2	Stanovené cíle	18
7.3.3	Náplň hodiny a časový plán	18
7.3.4	Nutné pomůcky pro hodinu	20
7.3.5	Text snímků prezentace	21
7.4	Příprava 4 – Časté a zajímavé pojmy ze světa Kybernetické Bezpečnosti .	21
7.4.1	Specifikace tématu hodiny	22
7.4.2	Stanovené cíle	22
7.4.3	Náplň hodiny a časový plán	23
7.4.4	Nutné pomůcky pro hodinu	24
7.4.5	Text snímků prezentace	24
8	Závěr	25

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 páčání 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, ne-li 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 velická 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.

Phishing – Typ útoku při kterém útočník předstírá, že je důvěryhodná, uživateli dobře známá entita, aby uživatele přiměl k vydání osobních či jinak citlivých informací a dat.

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 technologií 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 prvního 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 Stanovené cíle

Student rozumí pojmu *krádež identity* a chápe rizika spojená s touto hrozbou. Student zná kanály, kterými ke krádeži identity může dojít a chápe, že na Internetu jde o velmi běžnou záležitost. Dále zná právní následky, kterým může čelit v případě, že se krádeže identity dopustí a uvědomuje si co vše je možné považovat za krádež identity. Dojde-li v hodině k demonstraci podvržení emailu odcházejícího z jakékoliv emailové schránky, student je také

schopen toto podvržení reprodukovat. Student si je vědom, že u jakéhokoliv emailu, co se objeví v jeho emailové schránce, hrozí riziko, že nebyl odeslán osobou, která je uvedena jako jeho odesílatel. Student je schopen dle probraného algoritmu rozhodnout, zda je bezpečné email otevřít, či zda je lépe ho smazat. Existuje-li student s vyšším zájmem o informatiku, nebo problematiku efektivní obrany proti podvržení emailové identity, jsou mu poskytnuty doplňující zdroje informace řešící tento 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 odesílatel.

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 držaná 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 – Nebezpečí skryté v dokumentech Microsoft Office

Příprava na hodinu s tématem **Nebezpečí skryté v dokumentech Microsoft Office** je rozdělena do následujících částí:

- Specifikace tématu hodiny,
- stanovené cíle,
- diskuse o souvislostech se studenty,
- náplň hodiny a časový plán,
- nutné pomůcky pro hodinu
- text snímků prezentace.

7.2.1 Specifikace tématu hodiny

Hodina je zaměřená na – v době psaní práce – velmi aktuální a časté nebezpečí, a to škodlivý kód skrytý v souborech produkováných nástroji kancelářské sady Microsoft Office. V hodině je probráno z principiálního hlediska jak ke skrytí kódu do dokumentů dochází a z jakého důvodu nemusí ani velmi kvalitní antivirové programy detekovat tento typ škodlivého kódu dříve, než je pozdě. Je zahrnuto vysvětlení významu „makro“ v kontextu dokumentů Microsoft Office. Dále je v hodině vysvětleno jakým způsobem je možné se bránit proti napadení počítače tímto způsobem, a jaké další bezpečnostní opatření je vhodné přijmout před otevřením dokumentu získaného z internetu. Hodina také nabízí vhodný prostor k zopakování poznatků z hodiny na téma *Krádeže identity* – vyučující zde může, ve snaze navést žáky k vymyšlení již probraného bezpečnostního opatření připomenout algoritmus pro bezpečné otevírání a práci s emaily (probraný právě v hodině *Krádeže identity*). Studenti jsou v hodině také seznámeni se všemi známými koncovkami souborů produkováných nástroji sady Microsoft Office, které mohou ukrývat spustitelná makra.

7.2.2 Stanovené cíle

Student rozumí tomu, co je to makro – v kontextu dokumentů produkovaných nástroji kancelářské sady Microsoft Office. Student si uvědomuje rizika, která může přinášet bezhlavé otevírání těchto dokumentů. Student zná obecně známé koncovky dokumentů Microsoft Office. Student rozumí principům útoku na počítač skrze spuštění maker v dokumentu a je schopen mu zabránit příslušnými bezpečnostními opatřeními. Student rozumí možným nastavením úrovně bezpečnosti v programech sady Microsoft Office. Student umí vysvětlit pojem „obfuskace“ a k čemu slouží. Student zná název programovacího jazyka, ve kterém jsou makra pro programy Microsoft Office typicky psána, je schopen velmi jednoduché, ukázkové makro naprogramovat.

7.2.3 Diskuse o souvislostech se studenty

Hodina by měla být řazena tak, že je probírána až po tom, co studenti v informatice probrali práci s nástroji kancelářské sady Microsoft Office. Vyučující tedy může využít již existujících znalostních základů studentů a diskutovat s nimi na začátku hodiny o tématických souvislostech mezi tím, co se již naučili a znalostmi, které si studenti mají z hodiny odnést.

Vyučující může například vznést otázku: „Jaké koncovky mohou mít soubory vyprodukované nástroji sady MS Office?“. Studenti následně mohou přicházet se svými nápady, které koncovky dokumenty mohou mít. Vyučující na základě toho může vypožorovat, kteří ze studentů mají větší znalost sady MS Office a případně se jich pak dotazovat na další aspekty nově probírané látky.

Během této diskuse vyučující společně se studenty prodiskutuje, jaká je motivace útočníků skrývat nebezpečný kód do dokumentových souborů. Výsledkem diskuse na toto téma by mělo být uvědomění studentů, že hlavní motivací proč skrývat škodlivý kód do dokumentů je jejich vysoká rozšířenost a používání i velmi netechnickými typy uživatelů. Dokumenty navíc tuto možnost skrývání nebezpečné funkcionality přímo podporují, což je dělá pro útočníky perfektním nástrojem k zneužití.

7.2.4 Náplň hodiny a časový plán

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

4.–10. minuta - Představení tématu a diskuse popsaná v části **Diskuse o souvislostech se studenty**. Od studentů se očekává, že si nové termíny zapíší do sešitu, popřípadě dokumentu, který používají k psaní elektronických zápisů z hodiny, s vlastním vysvětlením. Toto očekávání je studentům sděleno v tomto čase.

11.–25. minuta - Frontální forma výkladu kombinovaná s monologickým výkladem využita k vysvětlení základních pojmů hodiny - vysvětlení pojmu „makro“ a jeho souvislosti s Microsoft Office, společně s osvětlením významu slova „makro“ pak vysvětlení principu jeho funkce a pokus o zjištění dotazováním třídy, proč jsou tedy makra tak nebezpečná. Není-li výsledkem dotazování taková odpověď jakou si vyučující představoval (např. to, že díky tomu, že makro je v podstatě kód v programovacím jazyce, ve kterém lze naprogramovat cokoliv (pokud je třída dostatečně pokročilá, volitelné představení dalšího pojmu „výpočetně úplný“, či „turingovsky kompletní“)), vysvětlí studentům vyučující jakou odpověď hledal a proč. V moment kdy je osvětlován princip funkce maker je zaveden nový pojem - *Visual Basic* - programovací jazyk užívaný k tvorbě maker.

26.–35. minuta - Demonstrace jednoduchého funkčního a nebezpečného makra, na konkrétním příkladu - kód stažený ze vzdáleného serveru vykonaný pod aktuálním uživatelem přihlášeném na počítači. Na tomto příkladě vyučující studentům vysvětlí, že právě tohle je důvod, proč i kvalitní antivirové řešení mohou mít s detekcí tohoto škodlivého programu problém. Dále je názorně ukázán rozdíl mezi makrem které je „obfuskované“ a které je neobfuskované a zmíněno, že „obfuskace“ se využívá k skrytí kódu maker před uživateli, ale i antiviry. Ukázka jednoduchého, ale bezpečného makra a popuzení studentů, aby ho replikovali a spustili na svých počítačích.

36.–45. minuta - Uzavření látky a vysvětlení, jak správně nastavit Microsoft Office, aby bylo předejito automatickému spouštění maker. Při této příležitosti jsou žákům také vysvětleny jednotlivé úrovně nastavení bezpečnosti v Microsoft Office, a které z nich jsou bezpečné. Zbyde-li z kterékoliv části hodiny čas, v závěrečné části je také vhodný prostor

k demonstraci existujících způsobů, kterými se útočníci pokouší lidi přimět k spouštění nebezpečných souborů.

7.2.5 Nutné pomůcky pro hodinu

Pro splnění cílů hodiny a pohodlnou demonstraci probíraného učiva je potřeba, aby v místnosti, kde probíhá výuka byl přítomen počítač s operačním systémem *Microsoft Windows*, s nainstalovanými programy kancelářské sady *Microsoft Office*. Tento počítač by měl být napojen na dataprojektor, který promítá obraz tak, aby ho třída viděla v reálném čase. Vyučující si dále připraví soubor typu *docx*, do kterého ukryje „obfuskované“ makro, které spustí příkazovou řádku a vypíše do ní text. Připojení k Internetu je pro tuto vyučovací hodinu volitelné, avšak příhodné, neb je-li počítač připojen k Internetu, je možné demonstrovat pokročilé techniky, kterými se virus skrývá před detekcí anti-virovými programy.

7.2.6 Text snímků prezentace

Sample frame title

This is a text in first frame. More text, something that is very readable and sensible, whatever that means.



7.3 Příprava 3 – Obecná bezpečnost na Internetu

Příprava na hodinu s tématem **Obecná bezpečnost na Internetu** je rozdělena do několika částí:

- Specifikace tématu hodiny,
- stanovené cíle,
- náplň hodiny a časový plán,
- nutné pomůcky pro hodinu
- text snímků prezentace.

7.3.1 Specifikace tématu hodiny

Tato hodina se zabývá aspekty obecné bezpečnosti z hlediska základního uživatelského používání internetového prohlížeče a interakce s webem jako takovým. Částečně téma

této hodiny navazuje na předchozí hodinu zaměřenou na **Krádeže identity** - tato hodina se blíže zaměří na speciální případ krádeže identity, a to případ, kdy podvrtná stránka napodobuje svým vzhledem vzhled stránky, kterou uživatel zná a věří ji. Tomuto specializované případu se taktéž říká *Phishing*.

7.3.2 Stanovené cíle

Student zná a rozumím pojmům *phishing*, *vývojářská konzole* či jen *konzole*, *zdrojový kód*, *http* a *https*. Student umí rozlišit mezi bezpečnou webovou stránkou a stránkou, která se za bezpečnou webovou stránku pouze vydává. Student dovede posoudit, zda je přípustné do konkrétní webové stránky vyplňovat jakékoliv osobní informace. Student zná a umí vysvětlit problémy z hlediska bezpečnosti, které nastávají při využívání stránek bez podpory HTTPS (tedy stránek, které pro přenos informací mezi uživatelem a serverem využívají HTTP). Student ví k čemu slouží v prohlížeči tzv. *vývojářská konzole* a uvědomuje si, rizika, které neuvážené kopírování a vkládání textu do ní může přinášet.

7.3.3 Náplň hodiny a časový plán

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

4.–10. minuta - Lehké představení tématu hodiny a odkázání se na hodinu týkající se **Krádeže identity**. Vyučující pokládáním otázek zjistí kolik si toho studenti ze zmíněné hodiny pamatují a nasměruje je na takové odpovědi, které povedou k tématu této hodiny. Například se může zeptat: „Jaké si pamatujete, [Jméno Studenta], možné krádeže identity, ke kterým dochází?“, cílem je dovést studenty ke specializovanému případu krádeže identity a to tomu případu, kdy se stránka vydává za jinou, uživateli známou stránku, což je přímo jedno z témat, které budou probírány.

11.–25. minuta - Vyučující využívající počítač připojený k Internetu a data projektoru spustí prohlížeč a ukáže studentům co je to vývojářská konzole a jakým způsobem je ji možné otevřít (tedy klávesou F12). Jsou-li studentům k dispozici počítače s nainstalovanými prohlížeči, vyučující jim pokyne, aby si to také ozkoušeli a vyřeší případné

problémy studentů, kterým se konzoli nepodaří najít. Na náhodném webu pak studentům ukáže jak se vepsání kódu do konzole na webu projeví - nejprve na jednoduchém příkladu (vyskakovací okénko), potom na složitějším (úprava obsahu stránky). Vysvětlí jim, že tyto změny se projevují pouze u něho v počítači, změny co provede se nezobrazí dalším návštěvníkům stránky. Pro zvědavé studenty pak může zmínit, že jazyk, kterým se konzole ovládá se jmenuje *Javascript* a používá se hojně pro tvorbu webu.

Studenti pravděpodobně touto dobou již vědí, že webové stránky jsou programovány a že existuje nějaký kód, na základě kterého jsou stránky zobrazovány. Vyučující toto pro jistotu připomene a ukáže studentům, jak je možné zdrojový kód stránek prohlížet (pro většinu prohlížečů klávesová zkratka CTRL + U). Při ukázce zdrojového kódu existující stránky studentům vysvětlí, že zkopírováním zdrojového kódu stránky a souvisejících souborů k sobě na webovou adresu, by došlo k vytvoření opticky shodné kopie webové stránky, která bude ovšem pod kontrolou někoho jiného. Vyučující se pak zeptá studentů, jestli si dovedou představit nějaký „nepříjemný“ scénář, ke kterému by mohlo takto dojít. Studenti by měli dojít k tomu, že by někdo mohl takto získávat informace od lidí, kteří si stránku spletou s originálem. Pokud na to studenti nedojdou, vyučující jim toto prozradí.

V tento moment také vyučující studentům popíše správný postup před zadáním jakýchkoliv soukromých či citlivých informací do webových stránek. Uživatel by měl **vždy** před vyplněním informací do stránky ověřit, že se opravdu nachází na stránce, na které předpokládá, že je. Toto ověření provede zkontrolováním adresního řádku v prohlížeči. Vyučující zmíní, že ne vždy musí být na první pohled zřejmé, že jde o závadnou stránku - velmi často jsou dnes používány názvy podobné názvu originálu. Jako konkrétní případ lze uvést stránku *PayPal.com*, pro kterou existuje spousta podobných webových stránek, které se snaží napodobit originální jméno, aby působily důvěryhodně, například tedy *PayiPal.com*, či *PayPall.com*. Vyučující se dotáže studentů jaký by použili postup, pokud by si nebyli jistí, že jsou opravdu na stránce, na které chtějí být. Tato otázka může vést na vtipnou odpověď ze stran studentů ve způsobu „Vygooglím si tu stránku?“, která bude v tomto případě na místě a pomůže uvolnit atmosféru v hodině.

Dalším vodítkem hodným zmínění je pak to, zda prohlížeč ve svém adresním řádku má

před adresou webové stránky text `https://` nebo `http://`. Většina stránek velkých, středních, ale i menších organizací bude mít před adresou právě `https://`. Většina podvodných stránek `https://` mít vůbec nebude, nebo jen velmi krátkodobě. Vyučující vysvětlí studentům, že většina stránek má zájem o to mít `https`, protože komunikace po tomto protokolu je šifrovaná a zaručuje, že po cestě nebude podvržena, napodobena, či zachycena. To znamená například, že při odesílání formuláře s přihlašovacími údaji na stránce bez aktivního `https` spojení, je možné zachytit přihlašovací údaje po cestě mezi uživatelem a webovou stránkou; to na stránkách s aktivním `https` spojením možné není, právě proto, že komunikace je šifrovaná.

26.–40. minuta - Vyučující se s využitím oporných snímků prezentace vrátí k vývojářské konzoli, se kterou studenty seznámil dříve v hodině. Na konkrétních případech skriptů, které byly v minulosti využívány k šíření spamu mezi uživateli sociální sítě Facebook, představí scénář, kterým je možné využít vývojářskou konzoli proti nic netušícímu uživateli. Vysvětlí scénář, který spočívá v přesvědčení uživatelů, že když nakopírují kód do své vývojářské konzole, odemknou si prémiovou verzi sociální sítě, která má lepší možnosti než ta stávající. Uživatelé, kteří kód nakopírují do konzole a pak spustí můžou například nevědomě pozvat všechny své přátele k oblíbení si stránky, která patří útočníkovi, nebo můžou kompromitovat část svých citlivých dat. Vyučující představí reálné případy, kdy k podobným situacím došlo a varuje studenty, aby nikdy takto kód do konzole nekopírovali, pokud nevědí co dělá. Bude-li čas a vhodná situace, vyučující může také jako zajímavost zmínit, že Facebook na tuto hrozbu reagoval a nyní při zobrazení vývojářské konzole v prohlížeči varuje uživatele, aby do ní nic nekopírovali.

41.–45. minuta - Shrnutí probrané látky a uzavření tématu. Vyučující dá prostor studentům pro otázky.

7.3.4 Nutné pomůcky pro hodinu

Pro efektivní realizaci výuky tak, aby bylo dosaženo stanových cílů je potřeba, aby vyučující měl k dispozici počítač připojený k Internetu s data projektorem zobrazujícím obrazovku počítače třídně. Počítač by měl být vybaven dostatečně moderním interneto-

vým prohlížečem, který obsahuje tzv. *vývojářskou konzoli*.

7.3.5 Text snímků prezentace

Sem přijdou snímky prezentace k hodině.

7.4 Příprava 4 – Časté a zajímavé pojmy ze světa Kybernetické Bezpečnosti

Příprava na hodinu s tématem **Časté a zajímavé pojmy ze světa Kybernetické Bezpečnosti** je rozdělena do několika částí:

- Specifikace tématu hodiny,
- stanovené cíle,
- náplň hodiny a časový plán,
- nutné pomůcky pro hodinu
- text snímků prezentace.

Hodina je strukturována ve smyslu prezentace různých nepřímo souvisejících pojmů, se kterými se i běžný člověk, který s kybernetickou bezpečností nepřijde do styku na dení bázi, často setká. Na začátku hodiny je studentům představen seznam pojmů, které budou v hodině představeny a diskutovány. Následně jsou pak pojmy jeden po druhém postupně představovány, přičemž při každém přejití na nový pojem se vyučující dotazuje třídy, zda se s pojmem již setkali, popř. zda ho někdo ve třídě dokáže zjednodušeně vysvětlit. Tuto hodinu je možné zařadit na začátek celé výuky kybernetické bezpečnosti, kdy poslouží jako motivace studentů ke studiu a věnování se kybernetické bezpečnosti. Zároveň, pokud bude hodina podána vyhovující formou, může sloužit jako velmi lehký úvod do zajímavých aspektů kybernetické bezpečnosti čímž může u studentů získat na popularitě. Další možností řazení hodiny je její umístění na konec vyučovacího roku, jako poslední zrelaxované a odléhcené téma pro třídu, které studentům dá podnět k vlastnímu studiu kybernetické bezpečnosti i dále - například během prázdnin před dalším během

předmětu. Řazení na konec roku je výhodné v tom, že studenti již prošli celým předmětem, spoustu podstatných termínů znají a rozumí jim. A tedy je možné probrat v rámci této hodiny i více komplexní a zajímavá témata, popřípadě provést důkladnou diskuzi na téma.

7.4.1 Specifikace tématu hodiny

Hodina se tématicky zabývá vzájemně nepřímo souvisejícími termíny z oblasti kybernetické bezpečnosti. Pojmy probírané v hodině jsou vybrány tak, aby většinu z nich studenti již za svůj život slyšeli a tato hodina jim pomohla tyto termíny správně uchopit. Probírané termíny jsou pak také vybírány na základě jakési „popularity“, neb mají ve studentech vzbudit zvědavost a určitý pocit senzace, mají na ně působit zajímavě a tajemně. Tato konkrétní příprava na hodinu se zabývá tématem útoků v síti internetu DoS a DDoS, některými častými útoky na webové aplikace, sociálním inženýrstvím, anonymním pohybem po Internetu, síti TOR a *Deep Webem*. Probrán je také termín botnet. V reálné situaci by však tato příprava na hodinu měla být připravena s ohledem na aktuální důležité termíny a události, které se dějí v oblasti kybernetické bezpečnosti dějí v době očekávaného výkladu, aby poskytnuté informace byly dostatečně aktuální a zajímavé.

7.4.2 Stanovené cíle

Student rozumí pojmům DoS a DDoS útok a dovede vysvětlit rozdíl mezi nimi. Student umí vyjmenovat a bez zabíhání do detailů přiblížit alespoň 2 časté útoky na webové aplikace. Student zná pojem „sociální inženýrství“ a uvědomuje si jeho rizika a právní závadnost případné aplikace jeho disciplín. Student ví co je to *TOR* a k čemu slouží. Student ví jakým způsobem je možné přistoupit na tzv. „*Deep Web*“, a co je na něm možné nalézt. Uvědomuje si, že samotný přístup na *Deep web* není trestný, avšak vyhledávání a prohlížení materiálů, které jsou v rozporu se zákony země, ve které žije, může způsobit právní problémy. Student rozumí pojmu botnet a zná nějaké historicky obrovské botnety a jejich roli ve světě.

7.4.3 Náplň hodiny a časový plán

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

4.–8. minuta - Vyučující promítne na data projektoru úvodní snímek prezentace, na kterém jsou pod sebou v seznamu vypsány termíny, o kterých plánuje v hodině mluvit. Pokyne studentům, aby si zběžně přečetli seznam a dá jim na to trochu času. Následně studentům prozradí, že o těchto pojmech budou tuto hodinu mluvit, a že nyní bude číst pojmy jeden po druhém a pokud někdo ve třídě tento pojem již slyšel, zvedne ruku. Vyučující pak na základě počtu rukou, které zůstávají dole detekuje nejméně obecně známý pojem a bude vědět, na který termín si má vyhradit nejvíce, a naopak nejméně času. Dle situace a času může vyučující pobídnout někoho ze třídy, aby pojem lehce osvětlil zbytku třídy, bude-li chtít.

9.–35. minuta - V tomto časovém úseku budou vysvětlovány a diskutovány jednotlivé témata a termíny, kterými se hodina zabývá. V rámci přípravy je to řazeno do jednoho, dlouhého časového úseku, neb se očekává, že vyučující bude pracovat s časem během hodiny dynamicky - dle znalostí třídy, řazení této hodiny a rozsáhlosti diskusí a studentských dotazů k jednotlivým probíraným tématům.

Vyučující začne přepnutím snímku prezentace na snímek o DoS a DDoS útocích. Vysvětlí studentům anglický význam a překlad těchto zkratk (*Denial of Service*, *Distributed Denial of Service*). Vyučující objasní studentům, že tento populární útok je založen na nárazovém mnohonásobném připojení více klientů / instancí klientů na server za účelem vytížení serveru a znemožnění přístupu legitimních klientů. Po vysvětlení základního principu a významu zkratk se vyučující pokusí společně se třídou dojít metodou pokládání vhodných otázek k zásadnímu rozdílu mezi útoky. Studenti by měli dojít k uvědomění, že *DDoS* útok je založený na větším množství klientů, rozmístěných například po celém světě, kteří naráz provádějí *DoS* útok. Nedojdou-li k tomu studenti sami od sebe, bude jim to vyučujícím prozrazeno.

Plynulým navázáním na tyto často vyskytující se typy útoků se vyučující přesune k další, pro studenty jistě velmi zajímavé oblasti - vyvětlení, jak principiálně může probí-

hat útok, při kterém se útočník na stejné síti (například. wifi) dostane na počítač oběti útoku. Společně s načnutím tohoto tématu se vyučující posune na odpovídající snímek své prezentace. Popíše jeden z možných scénářů, kterým by útok mohl proběhnout, aby studentům principiálně přiblížil jak to reálně celé probíhá, proto, aby konkretizoval představu o tom, co to znamená, když se řekne, že „útočníci se hacknuli do počítače [jméno napadeného člověka]“. Bodově půjde o vysvětlení, že útočník si nejprve provede „průzkum“ v rámci kterého nějakým způsobem „proskenuje“ síť. Skenováním sítě je myšleno zjištění jaká zařízení jsou v síti na jakých adresách. Jakmile zjistí útočník zařízení v síti, skenuje pak přímo jednotlivě ty. Útočník se pokusí zaslat zprávy na konkrétní zařízení a podle způsobů, kterým zařízení odpovídají někdy dokáže určit, jaký operační systém a v jaké verzi na strojích běží, popřípadě někdy i jaké programy. Dalším krokem je pak to, že útočník nalezne způsob, jak operační systém, nebo běžící program zneužít tak, aby mu byl udělen přístup k zařízení. Toto probíhá typicky tak, že vyhledá v databázi známých bezpečnostních problémů problém konkrétního programového vybavení, které běží na zařízeních v síti. Tohoto bezpečnostního problému dále využije k tomu aby zařízení napadl a převzal nad ním kontrolu.

7.4.4 Nutné pomůcky pro hodinu

Pro splnění cílů hodiny mimořádně není nutné žádné speciální elektronické vybavení. Celou hodinu je možné odvést a odvykládat ve standardní učebně, avšak vyučující může benefitovat z dostupnosti počítače napojeného na data projektor. Počítač s data projektorem může využít k živým ukázkám vykládané látky a promítání textů a obrázků na snímcích oporné prezentace. Není-li počítač s data projektorem k dispozici, obsah snímků prezentací lze vyměnit za tabuli a fix, popřípadě křídou.

7.4.5 Text snímků prezentace

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>>.