Fakulta informačních technologií,
Vysoké učení technické v Brně

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

30. července 2017 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 školidvý 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 informační 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, kterými 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 informační bezpečnosti do osnov je zcela opačný pól informační bezpečnosti. Doposud bylo psáno hlavně o způsobech ochrany a osvěty běžných uživatelů výpočetní techniky pro útokům ze strany hackerů. Stejně, ne-li více důležitou částí výuky informační 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 (source needed), 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 16ti letý chlapec [INSERT NAME HERE], který naprogramoval aplikaci, kterou nahrál na CD s rodinnými fotkami, která způsobila, že po strčení CD do počítače došlo k vymazání všech rodinných fotek jak z CD, tak z počítače, do kterého bylo CD zastrčeno. [INSERT NAME HERE] 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, [INSERT NAME HERE] 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 [INSERT NUMBER OF YEARS HERE] let vězení. Příběh [NAME HERE] 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 [NAME HERE] měl. I z tohoto důvodu je třeba šířit povědomí o informační 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. Autor této práce považuje tuto reakci za dobře načasovanou a vhodnou.

Tato sekce bude obsahovat argumenty pro zavedení výuky (základů) informační bezpečnosti na gymnázia, možná i (pro více textu) zmínku o tom, co tahle sekce obsahuje - klasické natahováky. Bodově z konzultace: argumenty pro. Možné citace and témata: vzrůstající počet kybernetických útoků, důležitost vštípení žákům do hlavy jak nebezpečné je páchat trestnou činnost přes počítač, za co je můžou odsoudit, na jak dlouho a jak snadno pro blbosti.

2 Kapitola 1 - RVP, ŠVP konkrétní školy, ...

Bez dalších poznámek, pravděpodobně půjde o rozbor toho co mi bude k dispozici (pokud nezískám ŠVP, asi se pustím do počtu hodin z RVP a zkusím vygooglit ŠVP nějaké školy, co to má veřejně). Patří sem informace o ŠVP/RVP, počet hodin na týden.

3 Kapitola 2 - Vstupní dovednosti, ... to be clarified

Bodově z konzultace: předpokládané vstupní dovednosti, ve kterých ročnících by se to mělo vyučovat (předběžně domluveno na všechny), probrat možné formy výuky (výklad, exkurze, protip: přivedení člověka odsouzeného za trestnou činnost (část s vysvětlováním právní závadnosti)), formy výuky (co to vůbec je? :D), potřebné pomůcky pro realizaci: jak výkonné musí být počítače, jaké by měly být jejich parametry (asi internet je třeba), jde využít telefony (jak?), interaktivní tabule

4 Kapitola 3 - OBSAHOVÁ ČÁST - tématický plán výuky

Bez dalších poznámek, hádám, že tady si budu muset nastudovat jak vypadá tématický plán výuky a pokusit se přijít s vlastním (asi různý témata: spoofing mailů, nedůvěryhodnost spojení se stránkami (možnost napodobení jejich vzhledu), rozeznávání potenciálních útočníků (možná cool hra pro třídu - každému dát papírek s informací, kterou má z někoho zjistit, aniž by si toho ten někdo byl vědom; ne na hodinu ale jako domácí úkol na týden?), nevyžádaná pošta, právní stránka věci)

5 Kapitola 4 - Osnova témat v jednotlivých ročnících

Bodově z konzultace: doplnit o didaktické hry (viz. výše), postupy a návody jak to učit. Jestli demonstrace, nebo jen teorie (vždycky demonstrace imho).

6 Kapitola 5 - 4 ukázky příprav na hodinu

Asi potenciálně nejdelší část, hodně si s tím vyhraju, naplánuji časově co se v kolika hodinách bude dělat... ideální bude asi zakomponovat falšování mailu a ukázka jak snadné je udělat aby stránka vypadala stejně jako originální stránka, aniž by byla.

7 Závěr

Zhodnocení celé práce, zhruba na 1 A4