Fakulta informačních technologií,
Vysoké učení technické v Brně

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

28. 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 o neuvěřitelných 300%.

* Na jednu stranu možná i uklidňujícím faktem je, (cilem jsou firmy...pokračuj)

Reakcí českého školství na prudký rozvoj a expanzi výpočetní techniky byla samozřejmě snaha naučit žáky a studenty s těmito novými technologiemi pracovat a interagovat. Tato snaha byla realizována mezi lety 2007-2009 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.

—Technika se neustále se zrychlujícím rozvojem oblasti informatiky a zvyšující se dostupností elektroniky schopné připojovat se do Internetu,

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