Výukový materiál zpracován v rámci projektu EU peníze školám

Registrační číslo projektu: CZ. 1.07/1.5.00/34.0233

Šablona	III/2
Název	VY_32_INOVACE_184_Poc.hrozby_teorie

Název školy	Hotelová škola Bohemia s.r.o. Víta Nejedlého 482 Chrudim
Jméno autora	Mgr. Markéta Valentová
Tematický okruh	Informační technologie pro 2. ročník SŠ
Ročník	2. ročník – 22 žáků
Téma	Počítačové hrozby - teoretická část

Anotace	Materiál je určen na vysvětlení základních znalostí z počítačových sítí. Jedná se o výukový materiál. Vyučující využívají k jeho prezentaci informační technologie.
Metodický pokyn	Žáci při výkladu pracují písemnou formou.
Datum vytvoření	10. 10. 2012

POČÍTAČOVÉ HROZBY

Nejznámější počítačové hrozby:

- Počítačový vir
- Počítačový červ
- Trojský kůň
- Spam
- Spyware
- Adware
- Riskware
- Physhing
- Pharming
- Hoax
- Cracker
- Hacker

Počítačový vir

- Virus je typ programu, který se dokáže šířit tím, že vytváří (někdy upravené) kopie sebe sama.
- Virus se neumí šířit sám, ale využívá k šíření jiné spustitelné soubory či dokumenty = hostitele. Virus se mezi dvěma počítači může přenést jedině tím, že někdo přenese celého hostitele, např. nějaký uživatel (obvykle neúmyslně) přenese nebo přepošle celý soubor.
- Některé viry mohou být cíleně ničivé (např. mazat soubory na disku), mnoho jiných virů je relativně neškodných popřípadě pouze obtěžujících.
- U některých virů se ničivý kód spouští až se zpožděním (např. v určité datum či po nakažení určitého počtu jiných hostitelů), což se někdy označuje jako (logická) bomba.
- Dnes jsou klasické počítačové viry na jistém ústupu oproti červům, které se šíří prostřednictvím počítačových sítí, hlavně Internetu.

Počítačový červ

- Počítačový program, který je schopen automatického rozesílání kopií sebe sama na jiné počítače. Poté, co infikuje systém, převezme kontrolu nad prostředky zodpovědnými za síťovou komunikaci a využívá je ke svému vlastnímu šíření.
- Červ obvykle vykonává v počítači nějakou sekundární činnost:
  - zneprovoznění počítače, nebo jeho součástí
  - odstraňování souborů uložených v počítači
  - prohledávání počítače za účelem získání osobních dat, která mohou pro autora programu znamenat nějaký profit
  - vytváření „zadních vrátek" do systému (tzv. backdoor), která poté mohou být využita jako přímá cesta k infikování počítače dalšími nákazami
- Důsledky většího rozšíření červa:
  - snížení rychlosti sítě (včetně internetu)
  - způsobují majitelům postižených počítačů finanční škody

Trojský kůň

- Trojský kůň jako samostatný program
  - Tváří se užitečně – například hra, spořič obrazovky nebo nějaký jednoduchý nástroj. Někdy se trojský kůň vydává za program k odstraňování jiných počítačových hrozeb.
  - V MS Windows může trojský kůň využít skrývání přípon souborů. Vypadá pak jako soubor s obrázkem, zvukem, archivem nebo čímkoliv jiným, přestože se ve skutečnosti jedná o spustitelný kód. Chce-li uživatel obrázek kliknutím zobrazit, je ve skutečnosti spuštěn program (trojský kůň).
- Trojský kůň jako součást jiné aplikace
  - Uživatel stažením kopie aplikace (nejčastěji bez platné licence nebo jako volně šířený program) může získat pozměněnou kopii aplikace obsahující aplikaci + trojského koně.
- Trojský kůň nedokáže sám infikovat další počítače nebo programy svojí kopií. Existují však počítačoví červi, které na napadeném počítači instalují různé trojské koně.

Spam

- Nevyžádané elektronické sdělení (zpráva, e-mail), které je obvykle rozesíláno masově.
- Nejčastěji se jedná o e-mailové zprávy, ale spam se rozšířil i do rychlých textových zpráv, diskuzních fór nebo komentářů článků uveřejněných na internetu.

Spyware

- Počítačový program, který za pomocí internetu odesílá informace z počítače uživatele bez jeho vědomí.
- Odesílány jsou statistické informace, jako přehled navštívených WWW stránek, nainstalovaných programů atd. Často jsou tyto informace využity pro cílenou reklamu na zájmy a činnosti uživatele, nikdo však nedokáže zaručit že nebudou zneužita, nebo že spyware nebude odesílat i vaše citlivá data.
- Spyware se šíří spolu s mnoha sharewarovými a freewarovými programy.
- Existují anti-spyware programy, které se zabývají nalezením a odstraněním (i prevencí) spyware z počítače.

Adware

- Počítačové programy, které jsou nabízeny za sníženou cenu nebo častěji zcela zdarma, ale obsahují v sobě jistou formu reklamy.
- Způsobují zobrazování reklamních poutačů (bannerů), vyskakovacích oken, přehrávání zvukové reklamy a to při používání programu nebo po dobu, kdy je program v počítači nainstalován.
- Míra nepříjemnosti přitom může být u různých programů (adware) různá. Funkčně adware může být i dobrým programem.
- Některé adware jsou ale zároveň i spyware.

Riskware

- Počítačový program, který nebyl vytvořen s úmyslem poškodit počítač, ale obsahuje chyby, které mohou spouštět nebo zastavovat pročítačové procesy a služby, či jiné programy.
- Chyby v riskware mohou umožňovat průchod dalších počítačových hrozeb (virů, červů, spyware, ...)

Physhing

- Podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) v elektronické komunikaci .
- Rozesílání e-mailových zpráv, které často vyzývají adresáta k zadání osobních údajů na falešnou stránku, jejíž podoba je takřka identická s oficiální stránkou. Stránka může například napodobovat přihlašovací okno internetového bankovnictví.

Pharming

- Podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.).
- Principem je napadení a přepsání IP adresy, což způsobí např. přesměrování klienta na falešné stránky internetového bankovnictví po napsání internetové adresy banky do prohlížeče. Tyto stránky jsou obvykle k nerozeznání od skutečných stránek banky.
- Ani zkušení uživatelé nemusejí poznat rozdíl (na rozdíl od příbuzné techniky phishingu, která využívá elektronickou komunikaci).

Hoax

- Podvodné, poplašné, žertovné, neaktuální, řetězové zprávy
- Nevyžádané e-mailové zprávy (případně zprávy ICQ, Skype, ...), které se snaží čtenáře přesvědčit, aby je šířil dál.
- Nejčastěji se jedná o varování před počítačovým virem, prosbu o pomoc, informace o nebezpečí atd.
- Zpráva je vždy smyšlená.
- Aktuální seznam naleznete na www.hoax.cz

Cracker

- Cracker (black hat) je označení pro člověka, který zneužívá své vědomosti o počítačové bezpečnosti ke svému prospěchu při průnicích do cizích počítačů.
- Cracker musí mít dobré znalosti o principech fungování počítačů (informační technologie), programování, počítačové bezpečnosti, kryptografii a podobně.
- V médiích je často pro crackery nesprávně používán termín hacker.

Hacker

- Hackeři jsou počítačoví specialisté či programátoři s detailními znalostmi fungování systému, dokážou ho výborně používat, ale především si ho i upravit podle svých potřeb.
- Hacker (white hat) využívá své znalosti ve prospěch uživatelů počítačových systémů (tj. odstraňuje programátorské chyby, diagnostikuje vadný hardware, programuje obtížné algoritmy).

Zdroje:

- http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_virus
- http://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_%C4%8Derv
- http://cs.wikipedia.org/wiki/Trojsk%C3%BD_k%C5%AF%C5%88_(program)
- http://cs.wikipedia.org/wiki/Phishing
- http://cs.wikipedia.org/wiki/Pharming
- http://cs.wikipedia.org/wiki/Hacker
- http://cs.wikipedia.org/wiki/Cracker
- http://www.slovnik-cizich-slov.net/?slovo=spam
- http://www.slovnik-cizich-slov.net/?slovo=adware
- http://www.slovnik-cizich-slov.net/?slovo=spyware
- http://www.slovnik-cizich-slov.net/riskware/
- http://www.slovnik-cizich-slov.net/?slovo=hoax