

Počítačová bezpečnost

Lukáš Jakubík

Softwarové hrozby

- **Všeobecně malware** (z angl. malicious)
 - Počítačový program určený ke vniknutí nebo poškození počítačového systému
- **Spyware**
 - Bez vědomí uživatele shromažďuje a odesílá data
 - Keylogger
- **Bootsektorové viry**
 - Nacházejí se v bootovacích oblastech disket, CD
 - Namísto zavedení OS se sami kopírují do paměti

Softwarové hrozby II.

- **Viry**

- Malý program, který se umí vložit do jiného programu a s ním se šířit

- 1982 „Elk Cloner” vir na Apple
 - 1986 „Brain” pákistánský vir šířen na disketách světem

- **Červy**

- Program, který je schopen se šířit sám, bez hosta

- 2000 „I Love You” – VBS skript přiložen do emailové správy a spuštěn automaticky emailovým klientem

Softwarové hrozby III.

- **Trojský kůň**
 - Malware umístěn do systému pod zástěrkou jiné funkcionality
 - Password-stealing (PWS)
 - Dropper
 - Proxy Trojan
- **Makrovir**
 - Napadají dokumenty Microsoft Word a Excel
 - Využití Visual Basic for Application
 - W97M/Melissa

Softwarové hrozby IV.

- **Rootkit** („sada nástrojů pro správce“)
 - 2005 Sony vydává audio CD se skrytým softwarem
 - Extended copy protection (XCP)
 - Šlo o rootkit bránící kopírování CD
 - Po vložení CD se nainstaloval přehrávač CD v PC, společně s aplikací, která skrývala některé systémové soubory a znemožnila zkopírování CD
 - Toto skrývaní souborů s předponou \$sys\$ mohl využít i jiný útočník

Společenské hrozby

- **Sociální inženýrství**
 - způsob získávání důležitých informací od uživatelů bez jejich vědomí
- **Druhy útoků**
 - I. Přímý přístup
 - II. Důležitý uživatel
 - III. Bezmocný uživatel
 - IV. Pracovník technické podpory
 - V. Obrácená sociotechnika

Společenské hrozby II.



- **Kevin Mitnick (*1963)**
 - Označen jako nejlepší hacker v dějinách
 - Ukradl několik tisíc souborů s daty a nejméně 20 000 čísel kreditních karet, tisícovky megabajtů chráněného SW
 - Naboural se do počítače Velitelství vzdušné obrany Severní Ameriky a další
 - Používal důmyslné techniky k ovlivňování lidí
 - Jedna z nejhledanějších osob v historii FBI
 - Soudním výrokem mu byl zakázán jakýkoliv přístup k PC
 - Kniha *Umění klamu*

Bezpečnostní software

- **Antivirové programy**

- Kontrolují data na základě virové databáze
- Neznámé hrozby pomocí inteligentní heursitiky
 - Alwil Avast!
 - AVG Internet Security 2012
 - Norton AntiVirus 2012
 - ESET Smart Security 5



Bezpečnostní software II.

- **Firewall**

- Odděluje provoz mezi dvěma sítěmi – propouští data jedním nebo druhým směrem podle předem definovaných pravidel
- Jako součást OS – jen vstupní filtry (nutný základ)
- Jako samostatná aplikace (hodně dotazů)
- Podniková proxy brána (omezení obsahu)
- UTM (profesionální řešení)
 - SonicWALL UTM Firewall

Hrozby z Internetu

- **Adware**
 - Znepříjemňuje práci na PC neustálou reklamou
 - Příznaky: vnucování stránek, pop-up okna atd.
- **Falešné produkty**
 - Falešné antispywarové a jiné bezpečnostní produkty
 - Instalujeme např. na základě odkazů ze spamu
- **Dialer**
 - Mění způsob přístupu na Internet, používán u vytáčeného připojení, změna na zahraničního ISP

Hrozby z Internetu II.

- **Phishing**

- První kontakt je většinou přes důvěryhodný e-mail
- Obsahuje překrytý URL odkaz na podvržené stránky
- Snaha o získání citlivých informací

- **Pharming**

- Přesměrování na podvodné stránky formou změny DNS záznamu – těžko detekovatelné uživatelem
- Pokročilá snaha o získání citlivých informací
- Často vyžaduje pomoc trojského koně

Hrozby z Internetu III.

- **Tracking cookie („sledovací cookie“)**
 - Identifikuje uživatele a připraví pro něj upravenou webovou stránku, podle jeho předešlé historie
- **Exploit („bezpečnostní díra“)**
 - Využívají známých bezpečnostních děr v operačních systémech
 - Využívá se poté k dalšímu spouštění škodlivého software
 - Ochrana je v neustálé aktualizaci všeho softwaru

Hrozby z Internetu IV.

- **Hijacker („únosce“)**
 - Přímo napadá Internet Explorer, e-mailový klienty, případně i operační systém
 - Mění nastavení – získává plnou kontrolu nad systémem
- **Backdoor („zadní dvířka“)**
 - Po spuštění postiženého souboru se ukryje v systému a vyčkává na kontakt zvenčí
 - Tvůrce viru má poté přístup na postižený PC

Cracking

- Cracking je zásah do spustitelného programu
- Často za účelem prolomení ochrany proti neoprávněnému použití
 - Crackování her
 - Odemčení nepřístupných funkcí
- **Nástroje pro crackery**
 - Disassembler (zpětně analyzuje spustitelný soubor)
 - HEX editor (umožňuje editaci binárních dat)
 - Debugger (odhaluje chyby, zefektivňuje crack)

Cracking II.

- **Anticracking ochrany**
 - Snaha omezit šíření a crackingové úpravy spustitelných souborů
 - Registrační číslo
 - Klíčový soubor
 - Kontrola originálního CD a ochrany na něm
 - Hardwarový klíč
 - Zmatečný kód
 - Závislosti mezi soubory aplikace
 - ...

Odkazy

- <https://sites.google.com/site/intomatika/antivirove-programy>
- <http://www.antivirovecentrum.cz/firewally.aspx>
- <http://programujte.com/clanek/2006080803-cracking-2-cast/>
- <http://programujte.com/clanek/2006080401-cracking-1-cast/>
- <http://www.spyware.kvalitne.cz/>
- <http://www.bezpecnyinternet.cz/pokrocily/internetove-bankovnictvi/phishing-a-pharming.aspx>
- <http://www.fi.muni.cz/usr/jkucera/pv109/2003p/xsimek3sociotechnika.htm>
- <http://www.avg.com/cz-cs/caste-dotazy.num-2334>
- <http://owebu.blogger.cz/Bezpecnost/Nebezpeci-na-internetu-Exploit-Hijacker-a-BHO>
- <http://zivotopis.osobnosti.cz/kevin--mitnick.php>