

## 8 Bezpečnost OS

### Obsah hodiny



Obsahem této hodiny je bezpečnost OS, možnosti ohrožení počítače a ochrany.

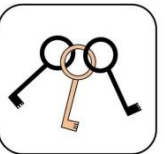
### Cíl hodiny



Po prostudování budete schopni:

- vyjmenovat možnosti ohrožení
- objasnit význam ochrany počítače
- orientovat se v možnostech ochrany

### Klíčová slova



Malware, Exploitování, Záplata, Firewall, Antimalware, Rezidentní štít, Kontrola integrity, Heuristická analýza, Antivirový monitor

### 8.1 Bezpečnost PC a nejčastější chyby

S tím, jak jde dopředu vývoj počítačů a jejich programového vybavení, zrychluje se (zejména v poslední době) i nárůst množství hrozeb.

Často se zaměřují na krádež a zneužití osobních dat a vzdálené ovládnutí infikovaných počítačů s cílem zisku. Většina útoků pochází z webových stránek a velice časté je použití technik sociálního inženýrství - tedy zneužití důvěry a nezkušenosti uživatelů.

Nebezpečím pro počítač a tedy pro data může být:

- Software (používání neověřeného SW)
  - Malware (malicious software – škodlivý SW)
  - Aplikace obsahující chybný kód (bezpečnostní díry) umožňující exploitování
- Lidský faktor
  - Nezodpovědný, nepoučený uživatel
  - Sociální inženýrství

- Chyby hardware
- Přírodní katastrofy

První dva faktory do jisté míry ovlivnit můžeme, ty další dva bohužel ne, ale ani ty by nás neměly zaskočit. Nemůžeme sice zabránit ani chybě HW ani přírodní katastrofě, ale můžeme minimalizovat následky a to tím, že budeme pečlivě a pravidelně data zálohovat.

## 8.2 Používání neověřeného SW

Každý neověřený program, který stáhneme z Internetu (nebo získáme jiným způsobem) a nainstalujeme do svého počítače může ohrozit jeho bezpečnost.

Jedním z největších nebezpečí pro uživatele je malware (malicious software – škodlivý software), což je jakýkoliv software, který byl vyvinut za účelem poškozování počítačových systémů.

Nejčastějším a nejstarším malware jsou počítačové viry, které mohou v okamžiku zlikvidovat výsledek práce vytvořené za dlouhou dobu. Nehrozí sice riziko přenosu počítačového viru na člověka, ale zjištění, že jste právě přišli o důležitá data vaše zdraví (a nejen to) ohrozit může.

Rada malware se zaměřuje na získání soukromých informací uživatele. Je třeba si uvědomit, že data jsou dnes nesmírně důležitá, lze je zpeněžit či jinak zneužít. Příkladem velmi citlivých dat je např. spojení k bankovnímu účtu či platební kartě, důvěrné úřední informace.

Bezpečnostním rizikem jsou dále aplikace, které obsahují chybný kód. Chybný kód vytváří bezpečnostní díry. Představuje vstupní bránu pro řadu útoků, ať už lokálních nebo vzdálených, způsobuje časté havárie, ztráty dat a zbytečné úniky výpočetního výkonu. Jedná se o vady nebo přehlédnutí v návrhu programu nebo v prostředí, ve kterém program pracuje. Každá takováto chyba v programu může být zneužitelná útočníkem – exploitování<sup>1</sup>.

Naštěstí ve většině případů chybného kódu dříve, či později existuje i „záplata“, která ho odstraňuje.

---

<sup>1</sup> Exploitování programu znamená přinutit programy vykonávat to, co chce útočník, dokonce i když je program navržen tak, aby tomu zabránil. Exploitování je základem hackingu.

### 8.3 Lidský faktor

Obecně nejslabším článkem počítačové bezpečnosti je vždy člověk - uživatel. Každý uživatel, ať už si to uvědomuje či nikoliv, ovlivňuje úroveň počítačové bezpečnosti.

Bohužel jen velmi málo uživatelů ví, jak se správně chovat z hlediska počítačové bezpečnosti. Proto většina z nich opakuje stále stejné chyby, které mohou vést k narušení bezpečnosti, a to jak jejich dat, tak celého systému. Jedná se např. o

- stahování, instalaci, používání neověřeného SW
- používání jednoduchého hesla
- nedostatečná ochrana citlivých dat (včetně hesla)
- nesprávně používaný nebo dokonce chybějící bezpečnostní SW

Dalším velkým nebezpečím je „sociální inženýrství“, které se zabývá tím, jak podvodně od uživatele získat data umožňující přístup k počítači. Využívá řady technik postavených na lidské důvěřivosti.

Mnoho firem bylo okradeno „spícím“ malwarem, který uživatelé zcela nevědomky pronesli přes dokonalé firewally na svém flash disku.

K dokonalosti tuto techniku dovedl jeden penetrační team, který koupil pěknou laserovou myš, přidělal do ní mikrokontroler AVR teensy, USB hub a flash disk. Myš pak hezky zabalenou poslal několika zaměstnancům jako reklamní dárek a skutečně se jim to povedlo - jedna žena si jí s sebou vzala do jinak dokonale zabezpečené firmy. Po připojení do USB se probudil teensy, nastavil se do režimu USB klávesnice a pomocí klávesových zkratk spustil malware umístěný v myši na flash disku.

### 8.4 Bezpečnostní technologie

Bezpečnost je řada procesů, jejichž součástí jsou nejen různé bezpečnostní produkty, ale rovněž lidé!!

Zabezpečení počítače proti uvedeným možnostem napadení spočívá především v prevenci:

- Používání bezpečných programů
- Používání bezpečnostního sw (antimalware, firewall)
- Správná konfigurace služeb, sw, firewallu
- Aktualizace – OS (záplaty), aplikací, antivirových programů
- Opatrnost uživatele, proškolení uživatele
- Zálohování
- Bezpečná likvidace datových nosičů

Pro ochranu počítačů a celých počítačových sítí se používá řada bezpečnostních technologií a produktů. Patří mezi ně především:

- Antivirový a další bezpečnostní sw
- Provádění pravidelných aktualizací
- Síťové bezpečnostní technologie
  - Používání VPN (Virtuální privátní síť)
  - Firewall, stínící směrovač, proxy server
- Biometrické snímače
- ...

## 8.5 Bezpečnostní software

Základní ochranu jednotlivých počítačů zajišťuje bezpečnostní software. Jsou to programy a aplikace umožňující ochranu počítače. Na každém počítači by neměly chybět dva základní typy:

- firewall
- antimalware

Úkolem firewallu je zabránit jakémukoli neoprávněnému pokusu o vniknutí do počítače, a to přísným hlídáním nejen příchozích, ale i odchozích dat.

Antimalware má zase na starosti rozpoznat jakýkoli program, který byl vytvořen právě za účelem poškození počítače (tzv. malware = malicious software = zákeřný software, zahrnující i viry), a zamezit jeho instalaci. Některé antimalwary jsou schopné reagovat zpětně, neboli umí vyčistit již infikované oblasti.

Důležité je pravidelně provádět aktualizace bezpečnostních programů - tzv. update. Nejsou jen zbytečnou (a zdržující) zábavou bezpečnostních programů. Ani denní aktualizace není jen reklamním trikem výrobců. Čím čerstvější update, tím větší pravděpodobnost ochrany před nově vzniklými vetřelci.

### Firewall

Firewall (FW) představuje bariéru (zeď) mezi počítačem a sítí, ke které se chcete připojit. Poskytuje ochranu před útokem „zvenčí“, zabraňuje průchodu nechtěných přenosů. Primárním úkolem FW je detekovat a blokovat.

FW jsou součástí bezpečnostního SW operačního systému nebo si můžete opatřit FW od jiných výrobců.

Firemní FW je spíše záležitostí ochrany sítě a síťového provozu, pro jednotlivé počítače se používá osobní firewall.

Správně nakonfigurovaný osobní FW znemožňuje síťovou práci malware a mnohdy vede k jeho snadné detekci.

Hlavním účelem FW je filtrování paketů. Filtrování paketů znamená, že se blokuje nebo povoluje přenos dat (paketů) na základě kontroly některých vlastností (atributů) a to jak odchozích tak příchozích paketů. Tato kontrola se provádí na základě pravidel. Kontroluje se

- zdrojová, cílová IP adresa,
- síťový protokol,
- přenosový protokol (TCP, UDP),
- zdrojový, cílový port.

Nejjednodušší pravidlo vypadá asi takto:

*„Aplikaci X povol TCP i UDP obousměrnou komunikaci na portech 25, 110 a 143, jinak se zeptej uživatele.“*

Tím, že se firewall zeptá uživatele, jak má se kterým spojením naložit, dochází k budování sady pravidel bezpečného připojení. Správná pravidla jsou základem nastavení osobního FW. Pozor! Přílišná restrikce může zamezit přístupu k některým službám.

Osobních FW jsou k dispozici jako součást OS, další lze nalézt na Internetu. Většinou je výrobci nabízejí zdarma jako „odlehčenou“ variantu svých dalších produktů, a je možno je použít pro osobní potřebu:

- Sygate Personal Firewall
- SoftPerfect Personal Firewall

Pokud je počítač k Internetu připojen přímo, lze jeho zabezpečení včetně firewallu do jisté míry zkontrolovat použitím některých online testů, například:

- AuditMyPC.com – Firewall test
- Sygate.com – Security scan
- TestMyFirewall.com – Firewall test
- PCFlank.com – PC Flank's tests

## **8.6 Antivirové systémy**

Komplexním SW, který primárně chrání váš počítač před malware, je antivirový program. Disponuje řadou nástrojů pro detekci a identifikaci malware (nejen virů). Uživatel by je měl znát a měl by být schopen je správně nakonfigurovat.

AV rozeznává malware od regulérního software na základě určitých rysů (databáze vzorků a zkoumání chování atd.), které jsou přidávány AV společnostmi formou updatů. Pozor! AV většinou není schopen rozpoznat malware, pokud ho nemá ve své databázi. Dále potřebuje informace jak nalezený malware vyléčit (to se týká vlastně jen virů; nejčastější dnešní forma malware je samostatný soubor, tj. léčení odpovídá smazání). Z uvedených důvodů je proto velmi důležité AV pravidelně aktualizovat. Pokud je počítač připojen k Internetu, lze provádět aktualizace automaticky.

Pokud antivirový program úspěšně detekuje a identifikuje virus, může:

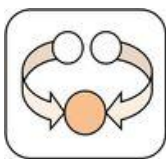
- se pokusit opravit/vyléčit soubor odstraněním viru ze souboru (pokud je to technicky možné),
- umístit soubor do karantény/truhly (virus se dále nemůže šířit, protože ho nelze dále používat),
- smazat infikovaný soubor (i s virem).

### **Známé antivirové systémy**

- Microsoft Security Essentials – bezplatný antivirus i pro menší podniky
- AVG – antivirový systém od české firmy AVG Technologies (dříve Grisoft).
- Norton AntiVirus – produkt firmy Symantec pro domácí uživatele
- ESET NOD32 Antivirus – slovenský komerční antivirový program
- Kaspersky Antivirus – výrobek ruské společnosti Kaspersky Labs
- avast! – český antivirový program od firmy ALWIL Software. Pro domácí nekomerční použití freeware.

Nevýhodou je možnost omylu a "nalezení" viru v souboru, který není virem napaden.

## Shrnutí kapitoly



Nebezpečím pro počítač a tedy pro data může být:

- Software (používání neověřeného SW)
  - Malware (malicious software – škodlivý software)
  - Aplikace obsahující chybný kód (bezpečnostní díry) umožňující exploitování
- Lidský faktor
  - Nezodpovědný, nepoučený uživatel
  - Sociální inženýrství
- Chyby hardware
- Přírodní katastrofy

Bezpečnost je řada procesů, jejichž součástí jsou nejen různé bezpečnostní produkty, ale rovněž lidé!!

Zabezpečení počítače proti uvedeným možnostem napadení spočívá především v prevenci:

- Používání bezpečných programů
- Používání bezpečnostního sw (antimalware, firewall)
- Správná konfigurace služeb, sw, firewallu
- Aktualizace – OS (záplaty), aplikací, antivirových programů
- Opatrnost uživatele, proškolení uživatele
- Zálohování
- Bezpečná likvidace datových nosičů

## Kontrolní otázky a úkoly



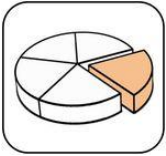
- 1) Jaké jsou možnosti ohrožení PC z pohledu SW?
- 2) Jaký vliv má na bezpečnost PC lidský faktor?
- 3) Jak chráníme počítač?
- 4) Co je to antimalware?
- 5) Co je to firewall a na jakém principu funguje?
- 6) Jmenujte tři antivirové programy

## Otázky k zamyšlení



1) Kdo je hacker a cracker?

## Použitá literatura a jiné zdroje:



- [1] BITTO, Ondřej . Vybíráme osobní firewall [online]. 10. 8. 2005 [cit. 2011-11-16]. Lupa.cz. Dostupné z WWW:  
<<http://www.lupa.cz/clanky/vybirame-osobni-firewall-1/>>.
- [2] HÁK, Igor. *Moderní počítačové viry*. třetí vydání. Hradec Králové: Fakulta informatiky a managementu – Katedra informatiky a kvantitativních metod, 2005. Dostupné z:  
<http://www.viry.cz/download/kniha.pdf>