

## Bezpečnost na Internetu

- viry, největší nebezpečí - změnilý svůj charakter
  - dříve mazaly soubory, šířily se hlavně na disketách
  - dnes se snaží co nejvíce rozšířit, využívají poštu a bezpečnostní chyby v softwaru (např. vir Sobig.F, není destruktivní, nemění data, ale může zahltnit servery svými kopiemi, velká rychlost šíření)
- 1983 - Fred. Cohen na Pensylvánské univ. použil kód, který se dokázal sám zničit - označil jej termínem virus
- Brain (1986) byl první virus pro PC (Pakistánci bratři Basit a Amjads Farooq Alvi)
- viry se dokážou klonovat, vložit do dalších programů, jejich destruktivní činnost může být vázána na urč. datum, na určitý úkon, např. po určitém počtu spuštění nakaženého programu dochází k mazání disku
- Dělení virů:
  - **podle umístění v paměti (rezidentní** - je obtížnější je vytvořit (operační paměť); **ne rezidentní** - hist. nejstarší (souborové viry např. na HDD)
  - **podle cíle napadení (bootovací** - napadají zaváděcí sektor; **souborové** - spustitelné programy .COM, .EXE, .BAT, .OVL, .SYS, .BIN)
- další škodlivé kódy:
  - **červi (worms)**- nekládají se do jiných pgmů, nepotřebují hostitele ke své replikaci, ale jsou ve formě samostatných souborů, které se spustí hned při startu poč., pro šíření využívají služeb sítě
  - **bomby** - (logické, časované, SMS bombery)
  - **dialer** - přeměruje připojení uživatele na jiné číslo s vysokým tarifem
  - **backdoors** -(zadní vrátka) umožňují vzdálenou správu počítače bez vědomí majitele = trojský kůň
  - **hoax** - není virus, ale e-mailová poplašná zpráva, varuje před virem a vyzývá k šíření
  - **makroviry** - rozšířily se spolu s kancelářskými balíky, napadají datové soubory, dokumenty (Wordu, Excelu, PowerP....) - **Concept** jsou nezávislé na platformě a op. systému
  - **trojské koně** - program, který vykonává obvykle očekávanou činnost, ale navíc činnost, o které uživ. nemá ponětí (např. odesílá soubory, zašifruje data a za vydání dešifrovacího klíče vyžaduje výpalné, PWS - Password stealing trojan)
  - viry využívají bezpečnostní díry v programech, např. chyba v kontrole hesla při přístupu ke sdíleným prostředkům v síti (využívá červ I-Worm/Opas)
  - tyto díry se vyskytují v každém softwaru
  - je třeba instalovat tzv. záplaty
- antiviry - pomoc až po nákaze
- firewally - je-li správně nastaven, může zabránit infekci předem, odhalí pokusy o průnik
  - jednodušší FW bývá i součástí antivirového programu různé programy této kategorie se těžko snášejí
- Bezpečné chování na Internetu
  - **antivirové programy** nezbytností, 1x týdně aktualizace virové databáze
  - uživatel by neměl spouštět neznámé soubory .COM, EXE, BAT, SCR, JS, VBS, PIF ani posílat tyto soubory partnerům
  - neotvírat soubory v příloze se dvěma příponami - např. NAME.BMP.EXE nebo NAME.TXT.VBS

- instalace nových programů - měly by pocházet od důvěryhodného zdroje, příp. od autora
  - červi v příloze pošty často používají názvy se sex. podtextem např. PAMELA\_NUDE.VBS - neotevírat
  - červ jako spustitelný soubor může být maskován **jinou ikonou**, např. jako obrázek, text
  - nepřijímat přílohy od cizích v online chat systémech jako: ICQ, IRC, AOL Instant Messenger
  - **hesla** - používat různá (např. pro přístup k poč., k mailové schránce) a měnit tak 1x za měsíc
- Heslo - nejdůlež. prvek ověřovacího mechanismu
    - autentizační údaje uživatele (jméno a heslo)
    - dříve se heslo přenášelo jako otevřený text, nebo jednoduše kódované
    - dnes se používají metody jednosměrného kódování v souborech, kde jsou uložena hesla, těžko lze zpětně získat heslo
    - je třeba speciální nástroj (jako John the Ripper, nejlepší na luštění Unix. hesel, používá hrubou sílu i slovníkový útok)
    - programy, které dokáží heslo u souboru zjistit: StarSlayer, Password Recovery Suite, ARJ Password Solver, fast Zip Cracker  
problém nejsou ani PDF soubory
    - svými programy pro luštění hesel je známá ruská firma **Elcomsoft**
    - luštění hesel **hrubou silou**  
za 1 hodinu lze louskačem vyzkoušet min. 20000 variant, je těžší, **když neznáme délku hesla**  
počet možných kombinací závisí na délce hesla  
mělo by mít **více než 8 znaků** a používat i **číslíce a speciální znaky** (%, #)
    - **slovníkově orientované útoky**  
program zkouší všechna slova ve slovníku (tak 250000 slov), zkouší i různé velikosti písmen  
číslíce a speciální znaky v heslech neodhalitelné  
na Internetu více než 120 slovníků
- Spam - nevyžádaná komerční nabídka
    - tvoří třetinu z asi 30 miliard ročně rozesílaných zpráv
    - problém zejména **kapacitní**, zatěžuje přenosové a úschovné kapacity
    - obtížný boj - technologie těžko rozeznává spam od regulérního mailu
    - filtry = blokování nevyžádaného, černá listina (80% účinnost)
    - opak je bílá listina, propuštění předem domluveného, do seznamu se dají ti, jejichž mail systém propustí
    - tuto funkci by měl nabízet e-mailový klient
- spyware
    - zpomaluje chod počítače, doluje informace o uživateli, které stránky navštěvuje, atd., může se skrývat v softwaru, který je distribuován zdarma