POČÍTAČOVÉ VIRY
ANTIVIROVÉ PROGRAMY

Počítačový virus (zápis do sešitů)

- Program, který se dokáže šířit bez vědomí uživatele pomocí jiných spustitelných programů či dokumentů
- Chová se obdobně jako biologický vir
- Viry jsou jen jedním z druhů malwaru, zákeřného softwaru
- Některé viry mohou být tzv. polymorfní
- Viry se samostatně nešíří a šíří se tím, že od sebe sama vytváří kopie či nové druhy virů

Druhy virů

- **1.) Podle hostitele**
- *A) spustitelné programy*
- - COM a EXE
- - EXE v Microsoft Windows
- - ELF v UNIXu
- *B) boot sektory diskových oddílů*
- *C) soubory obsahující makra*
- - Microsof office
- *D) specializované skripty některých konkrétních aplikací*

2.) Podle způsobu činnosti

- *A) rezidentní/nerezidentní viry*
- - šíření ve chvíli spuštění hostitele a rozšíření virů do nenakažených souborů
- - uložení do operační paměti kde zůstane do vypnutí počítače a zatím infikuje soubory
- *B) stealth viry*
- - zachytí se na přerušení, kudy protékají veškerá data
- - pro modernější typy OS je nutno použít složitějších rootkitů (maskovacích zařízení)
- *C) makro viry*

Počítačový červ

- Program který se samovolného automatického rozesílání kopií sama sebe na jiné počítače
- Krom vlastního šíření má v počítači i sekundární funkci, která je červem nesena
- Jedná se o:
- 1) zneprovoznění počítače nebo jeho součástí
- 2) odstraňování souborů z počítače
- 3) šifrování souborů uživatele kriptovirálním útokem (ransomware)
- 4) prohledávání počítače za účelem získání osobních dat
- 5) zadní vrátka (průnik do počítače zvenčí)

Typy červů + ochrana

- **Typy**
- 1) e-mailový
- 2) internetový
- 3) IM (odkazy)
- 4) IRC (spustitelné soubory)
- **Ochrana**
- - neotvírat přílohy emailů
- - nespouštět odkazy na neznámé či nebezpečné stránce
- - nestahovat sdílený nelegální obsah

Antivirový program

- Slouží k identifikaci a eliminaci počítačových virů a jiných škodlivých softwarů
- Dvě techniky zajištění:
- 1) prohlížení souborů na lokálním disku
- 2) detekce podezřelé aktivity nějakého programu

Metody zjištění

- *1) virové databáze/slovníky*
- - při kontrole počítače zjišťuje zda se nějaký známý vir, který má zapsán v databázi neshoduje a pokud ano, nastanou 3 možnosti:
- A) pokusit se opravit/vyléčit soubor
- B) umístit soubor do karantény
- C) smazat infikovaný soubor

- *2) Nebezpečné chování*
- Kontroluje se pomocí tzv. Heuristické analýzy

Testování kvality antivirových programů

- **Měří se:**
- 1) počet neodhalených hrozeb
- 2) počet falešných poplachů
- Dále se potom zohledňuje
- - náročnost na systém
- - uživatelskou přívětivost
- - aktualizace

Nejznámější antivirové programy (zápis do sešitů)

- Trend Micro
- Microsof security essentials
- Avira antivirus
- AVG
- Norton AntiVirus
- ESET
- McAfee
- Kaspersky antivirus
- Avast