Obsah

17 Viry, WWW, FTP

17.1 Viry

- počítačové programy s cílem napadnout systém a dále se rozšířit
- motivace – profit, šíření zprávy, zábava, ukázání chyby, sabotáž systémů (DDoS)…
- využití hostovacího programu
  - computer worm nepotřebuje externí program
- většina virů směřována na MS Windows
- přenos přes soubory, po síti, USB flash disky…
- antiviry – programy chránící před viry

17.1.1 Historie

- 1949 – John von Neumann – Teorie sebereplikujícího se automatu
- 1982 – *Elk Cloner* – první vir ve veřejnosti
- 1984 – Fred Cohen – definoval pojem virus

17.1.2 Druhy virů

- spyware – vir vytvořen za účelem shromažďovat data o uživateli bez jeho vědomí
- adware – zahlcení počítače reklamami
- malware – software s účelem jakkoliv uškodit počítači
  - viry, červy, Trojské viry, Spyware, Adware, Ransomware…
- rozdělení podle hostitelů
  - spustitelné soubory – com, exe, elf…
  - boot sektory disket a disků, MBR (master boot record)
  - dávkové soubory a scripty – bat, sh…
  - makra v MS Office
  - speciální scripty aplikací
- rozdělení podle způsobu činnosti
  - rezidentní viry – program nepokračuje, zůstává v RAM, infikuje soubory, se kterými uživatel pracuje
  - nerezidentní viry – vir začne infikovat hned po spuštění vše, co najde
  - stealth viry
    - snaha maskovat
    - při kontrole antivirem vrátí aplikaci původní data
    - dnes lehce odhalitelné
    - hlavně pro MS-DOS, dnes využití rootkitů
  - makro viry
    - makra kopírovaná z dokumentu do dokumentu
    - šíření v office souborech
    - dnes již ne moc rozšířené

Ransomware

- šifrování dat na pevném disku
- uzamčení systému s výhružnou zprávou
- požadavky výkupného (většinou krypto – BTC…)
- zrod v Rusku, dnes již mezinárodní
- distribuce pomocí trojského koně
- typy
  - file coders (CryptoLocker, CTB-Locker…)
  - scareware – falešné antiviry
  - screen lockers
  - doxing – vyhrožování osobními údaji
  - phising

Spacefiller virus

- hledá volné místo v kódu namísto připojení na konce programu
- nezvětší se velikost souboru – těžší idetifikovatelnost

Trojský kůň

- přetvářka za užitečný software
- práce v utajení
- editace uživatelských souborů, blokace souborů, DDoS tool, zpomalení počítače
- řešení – reinstalace systému

DDoS attack

- distributed denial of service
- vyřazení služby/serveru zahlcením daty a požadavky
- znepřístupnění/zpomalení služby ostatním
- DoS – posílání z jednoho počítače, DDoS – posílání požadavků ze sítě počítačů

17.1.3 Prevence

- ověřené antiviry
- ověřování pochybných mailů a dalších zpráv
- kontrola aktualizací programů
- vyhýbání se pochybným stránkám
- vyhýbání se pirátství
- zálohy počítače
- použití bezpečnějšího systému

Antiviry

- programy bojující proti virů
- kontrola souborů a programů
- Kaspersky, Bitdefender, Norton, McAfee, ESET, Windows Defender, AVG…

17.2 FTP

- File Transfer Protocol
- protokol pro přenos souborů, komunikace se serverem
- využití TCP/IP
- přenos velkých souborů, základ infrastruktury firem…
- zabezpečení přes SSL/TLS
- přenos také přes SSH
- multiplatform
- možný přístup přes webový prohlížeč nebo prohlížeč souborů

- nevýhody – přístupové údaje přenášeny jako plain text

17.3 WWW

- World Wide Web
- informační systém pro sdílení dat a webových stránek
- www. – subdoména
  - používána hlavně při začátcích internetu, dnes přesměrovává na samotné stránky
- přenos dat přes HTTP(s)
- hostování souborů na web serverech
- přístup přes webové prohlížeče
- odkaz – adresa webové stránky
- cesta adres získávána přes DNS