Bezpečnost dat v PC

Údržba a bezpečnost systému
ochrana dat

Hlavní důvody zabezpečení dat v PC

- technická závada hardware PC
- destruktivní působení uživatele
- činnost nepovolané osoby
- destruktivní působení škodlivého obsahu - viry, spyware

Prevence pro zabezpečení dat

- Bezpečnostní politika – účty na PC
- Oddělení systému a aplikací od datových souborů
  - vytvoření několika diskových oddílů - **programy**, **data**, **záloha**
  - vytvoření obrazu oddílu **programy** a jeho zálohování v oddílu **záloha**
- zabezpečení operačního systému a jeho aktualizace
- použití a aktualizace antivirového systému
- pravidelné zálohování dat mimo pevný disk - CD, DVD
- zálohování elektronické pošty - maily a účty

Zásady pro zabezpečení dat

- používání bezpečnostních nástrojů (antiviry, firewaly, zálohovací SW, …)
- pravidelná aktualizace zabezpečení (legálnost OS, …)
- **Ochrana dat před škodlivým obsahem** (malware, viry, …)

- Největší nebezpečí - **průnik a působení škodlivého obsahu z internetu**
- Pro zabezpečení je nutno použít kombinaci bezpečnostních systémů
- Firewall, Antivir,Antispyware,Antispam

Obrana - uživatelská

- Antivir - Norton Antivirus, NOD32, Avast
- Firewall - Norton Internet Security, Kerio Personal Firewall
- Systém pro detekci vniknutí - Norton Internet Security
- Systém pro detekci spywaru – AdAware
- Pravidelné aktualizace

Volba hesla

- **Ochrana před zneužitím účtu**

  na samotném počítači
  před anonymními útočníky z internetu
- **Správná volba**
  - 10 a více znaků, používat čísla a symboly
  - sestavit si heslo algoritmem z nějaké věty (např. 1. písmeno z prvního slova, 2.písmeno z druhého slova atd.)

pozn. český slovník má jen cca 300 000 slov

- **nikdy nikam neposílat svá hesla, pravidelně záplatovat systém** (update)

Odposlech, sledování a kradení údajů

- **Odposlech**
  - tvrdí se, že 95 % veškeré komunikace je odposlouchávánо
  - závislost na připojení v síti
  - aktivní vs. pasivní prvky
- **Bezpečné vymazání**
  - prohlížeče si automaticky pamatují historii (tzn. nastavit si správně internetové prohlížeče, vypnout automatické vyplňování formulářů)
  - vymazání a ani formátování disků nic v podstatě neřeší (studie 200 starých disků, kde z 90 % obnovili data včetně choulostivých; při prodávání či vyřazování je dobré použít speciální nástroje)
- **Přístupová práva**
  - definování toho, co kdo s čím kde a jak může na počítači dělat
  - lze obejít např. bootováním jiného systému z CD

Psychologické útoky, vylákání údajů

- **Phishing**
  - Vydáváním se za společnosti za účelem získání osobních informací či šíření virů
- **Nigerijské dopisy**
  - Může dojít k vylákání peněz z důvodu zaplacení posledních detailů
  - Po uživateli se chce, aby odletěl do Nigerie, cestu si zaplatí a tam je možné
  - Zneužití účtu k praní čistých peněz
- **Hoaxy - Plané poplachy**
  - poslat co nejvíc mailů pro získání peněz na operaci smrtelně nemocného člověka
  - smazat nějaký soubor, který je infikovaný (ve skutečnosti jde o nějaký systémový)
  - petice např. za kácení stromů, atd.
- **Proč škodí?**
  - útok na psychiku uživatelů
  - zahlcují sítě
  - způsobují ekonomicky měřitelné ztráty způsobené zdržováním od práce

Užitečné odkazy: www.hoax.cz