22. Bezpečnost

1. Ukládání dat

- archivační úložná média:
  - HDD - životnost asi 4 roky a další mechanická média (Bernoulliho disk, děrný štítek, magnetooptický disk)
  - magnetické pásky, dlouhodobé uložení dat, stejné jako floppy disk (jenom technologie) životnost klidně i 30 let
  - CD a DVD, či Blu-ray - životnost kolem 20 let
- jelikož jeden HDD má malou kapacitu, využívají se vícenásobná disková pole, RAID popisuje topologii diskového pole, vztahy, co a jaký disk dělá, jedná se pouze o normu
  - redundant array of independent disks
  - při softwarové realizaci se o zápis do jednotlivých disků stará OS
  - hardwarová realizace spočívá ve využití řadiče, obsluha RAIDu, independence od procesoru
  - *degradované pole*, stav pole disků, kdy jeden či více disků selže, potom je třeba, v závislosti na implementovám RAIDu, data rekonstruovat
  - *hot add* - přidání nového disku do již existujícího pole
  - *spare disk* - rezervní, označujeme $+N$ za daným typem RAIDu, $\$N$ je počet rezervních disků
  - *RAID0*: není skutečný RAID neobsahuje redundanci dat, rw rychlost je n-násobná
  - *RAID1*: mirroring
  - *RAID5*: alespoň tři členy, přičemž na každém je paritní součet vedlejšího disku, které se používají při rekonstrukci dat, odstraněna nevýhoda RAID4, kde byly paritní sektory na jednom disku
  - *RAID6*: totéž co RAID5, akorát se používají dva paritní bloky
  - *RAID10*: uložiště stripováno na dva diskové clustery, ty jsou potom ještě mirrorovány
- *mdadm* je linuxí utilita k správě a sledování softwarově definovaného RAID pole, open-source
- další metodou zálohování dat je *cloudové uložiště* - data jsou na vzdáleném serveru, u nás je pouze abstrakce, virtuální uložiště
- *CryFS*: slouží pro realtime kryptografii dat, funguje s cloudovými uložišti Dropboox, OneDrive či iCloud, je to open-source

2. Zálohování dat

- zálohovací program *borg* umožňuje:
  - inkrementální zálohy
  - deduplikaci dat
  - účinný ve využívání prostoru, komprese dat
  - SHA-256 data enkrypce
  - komprese *lz4*
  - open-source
- *rsync*:
  - program, který slouží pro přenos dat (synchronizace)
  - deduplikace, pouze delta dat na jednotlivých zařízeních

3. Firewall

- jedná se síťový prvek, který reguluje provoz na počítačové síti
- podle kofigurace zabezpečuje do dané úrovně
- paketové filtry
  - dropování paketů, které přišly z uržitého portu, nebo ip adresy
  - kotrola na třetí či čtvrté vrstvě OSI
- aplikační brány
  - sedmá vrstva OSI
  - proxy
  - vysoké zabezpečení proti známým protokolům

4. Hackerské metody

- **phishing**: metoda, se určitá aplikace jeví jako skutečná, ale jedná se o podvrh, nejčastěji slouží k získání hesel
- **SQL injection**: technika k napadení databázové vrstvy pomocí vsunutí programu, který pozmění chování databáze
- **XSS**: cross-site scripting, vložením kódu do dynamické části webu se pozmění její chování, lze takhle obejít omezení přístupu, útočník vloží svůj kód do stránky ověřeného uživatele
- **broken acces control**: dnes nejpoužívanější technika dle *QWASP*, útočník obejde přístupové restrikce a může modifikovat jinak zabezpečený obsah