Bezpečnost v ICT

Úvod do ICT, 28. listopadu 2022

Prvky bezpečnosti

- Hesla
- Šifrování
- Certifikáty
- Zálohování

Hesla

- Nikomu neprozrazovat
- Volit neuhodnutelné
  - Platí, že „čím delší, tím lepší“ (bezpečnější)
  - **Nejsou třeba**: speciální znaky, velká písmena, čísla
- Poznačit tak maximálně do správce hesel
- Jaké heslo je dostatečně bezpečné?
- Před připojováním na veřejné Wi-Fi sítě už nevaruju

Šifry – kryptografie

- Převod „čitelných“ dat na „tajná“ data
  - Pomocí šifrovacího klíče
- Symetrické šifry
  - Jeden klíč, rychlé zpracování – (de)šifrování
- Asymetrické šifry
  - Dva klíče – soukromý a veřejný

Asymetrická kryptografie

- Šifrované e-maily
  - Odesílatel šifruje pomocí veřejného klíče příjemce
  - Příjemce dešifruje pomocí svého soukromého klíče
- Elektronické podepisování
  - Podepisující „podepíše“ svým soukromým klíčem
  - Kontrola pravosti pomocí veřejného klíče
- Výměna šifry pro symetrickou kryptografii

Hashovací funkce

- Z libovolně objemných dat (zpráv) vytvoří krátký otisk konstantní délky – hash
  - Sebemenší změna na vstupu znamená velkou změnu na výstupu
  - Z hashe je prakticky nemožné získat původní obsah
  - Existence dvou zpráv se stejným hashem je krajně nepravděpodobná
- Používá se pro uložení hesel či el. podpisy

Certifikát

- Elektronicky podepsaný veřejný šifrovací klíč
  - Kromě samotného klíče jsou zde také informace o subjektu, které klíč patří, např. jméno osoby či do kdy certifikát platí
- Princip přenosu důvěry
  - Pokud důvěřujeme certifikační autoritě, která certifikát vydala, důvěřujeme i držiteli certifikátu

Elektronické časové razítko

- Evidence toho, že dokument existoval v daném čase (může mu prodloužit platnost)
- Razítko dodává externí služba
  - TSA – Time-Stamp Authority
  - Kombinuje hash dokumentu s certifikátem autority a časem, za který ručí autorita
- Více: Wikipedie * služba Cesnetu

Elektronická pečeť

- Zaručuje původ a integritu dat
  - Jako podpis, ale pečetí organizace
  - Vhodné pro hromadné zpracování dat
- Autentizují téměř cokoli digitálního
  - Např. potvrzení o studiu v IS MU má pečeť
  - Rovněž „covidové certifikáty“ jsou pečetěny
- Více: Wikipedie * služba ProID

E-Government

- Datová schránka
- Elektronický občanský průkaz
- Národní bod pro identifikaci a autentizaci (www.identitaobcana.cz)
- Portál občana (obcan.portal.gov.cz)
- Nařízení eIDAS

Přístup na web skrze HTTPS

- Mezi TCP a HTTP se vklíní TLS
  - Protokol Transport Layer Security, nástupce SSL
- Server nabídne klientovi certifikát:
  - S veřejným klíčem (z něj se odvodí šifrovací klíč)
  - S datem platnosti a doménovým jménem
  - S informací o autoritě, která jej „vydala“
- Pokud vše „sedí“, další komunikace je šifrovaná

Zálohování

- Včera uložený soubor dnes již na svém místě nemusí být dostupný
- Příčiny
  - Uživatel – neopatrnost, nedbalost
  - Špatné médium
  - Živelná pohroma (zkrat, požár, povodeň …)
  - Krádež, virus, ransomware

Způsoby zálohování

- Vždy na jiné médium:
  - CD, DVD, flash-disk, externí disk …
  - Kopie (snapshoty, přírůstkové …)
  - RAID (diskové pole – zrcadlo)
  - Internetová úložiště (cloud a jeho funkce)
    https://it.muni.cz/prehledy/srovnani-ulozist

Způsoby ochrany dat

- Steganografie
  - Utajení komunikace / obsahu (např. v JPG)
- Digitální vodoznak
  - Dodatečná informace v dokumentu
  - Používá se k ochraně autorských práv
- DRM – Digital Rights Management
  - Šifrování autorsky chráněného obsahu

Domácí úkol

- Vygenerujte si své osobní uznávané certifikáty https://tcs.cesnet.cz/
- Použijte je pro podepsání dokumentů a zaslání šifrovaných e-mailů