Nädal 14 - Infoturve

Infoturve on andmete ja tehnoloogiliste süsteemide kaitse juhuslike ja pahatahtlike ohtude eest. Tänapäeva maailmas, kus arvutid ja tehnoloogia on igapäevase elu lahutamatuks osaks, muutub infoturve aina olulisemaks. Olulised teemad hõlmavad käideldavust, konfidentsiaalsust ja terviklust. Infoturve puudutab nii tehnilisi süsteeme kui ka inimkäitumist.

Infoturbe põhiprintsiibid (CIA-mudel)

1. **Käideldavus (*Availability*):** Andmed ja süsteemid peavad olema saadaval siis, kui neid vajatakse. Näiteks peab haigla infosüsteem olema ööpäevaringselt kättesaadav.
2. **Konfidentsiaalsus (*Confidentiality*):** Ainult volitatud isikud pääsevad andmetele ligi. Näiteks pangakonto andmeid tohib vaadata ainult konto omanik.
3. **Terviklus (*Integrity*):** Andmed peavad olema tõesed ja täielikud. Näiteks finantsaruanded ei tohi olla tahtlikult ega juhuslikult muudetud.

Infoturbe kihid

Infoturbe tagamiseks on vaja kaitsta mitmeid kihte:

1. **Krüptograafia:** Matemaatilised meetodid andmete turvamiseks, näiteks krüpteerimine ja digiallkirjad.
2. **Rakendused:** Tarkvarasüsteemid, mis kasutavad turvameetmeid.
3. **Lõppkasutaja:** Inimene, kes süsteeme kasutab, on sageli nõrgim lüli turvalisuses.

Krüptograafia

- **Põhimõisted:**
    - **Krüpteerimine:** Protsess, kus avatekst muudetakse salakirjaks.
    - **Dekrüpteerimine:** Protsess, kus salakiri muudetakse tagasi avatekstiks.
    - **Räsi:** Unikaalne „sõrmejälg“ failist või andmest, mida ei saa tagasiarvutada algandmeteks.
- **Tüübid:**
    - **Sümmeetriline krüptograafia:** Sama võtit kasutatakse nii krüpteerimiseks kui ka dekrüpteerimiseks. Näide: AES (*Advanced Encryption Standard*).
    - **Asümmeetriline krüptograafia:** Kasutatakse kahte võtit – avalikku ja privaatset. Näide: RSA ja elliptilised kõverad.
- **Soolamine:**
    - Soolamise käigus lisatakse igale paroolile juhuslik lisand (sool), enne kui see räsitakse. See aitab kaitsta paroolide andmebaasi nn "*rainbow table*" rünnakute eest.
    - Näide: Kui kaks kasutajat valivad sama parooli, muudab soolamise protsess need erinevateks räsideks.

    - Soolamine suurendab oluliselt paroolikaitse tõhusust, sest iga räsi on unikaalne ka sama sisendi korral.
- **Rakendused:**
    - Paroolide kaitse räside abil.
    - Digiallkirjad dokumentide autentsuse tagamiseks.
    - ID-kaart ja Mobiil-ID Eesti e-teenustes.

Infoturberiskid ja lahendused

1. **Pahavara:**
    - Probleem: Klahvinuhid, lunavara, viirused.
    - Lahendus: Viirusetõrje tarkvara ja regulaarsed tarkvarauuendused.
2. **Nõrgad paroolid:**
    - Probleem: Paroolid võivad lekkida või olla kergesti äraarvatavad.
    - Lahendus: Paroolihaldurid ja kahefaktoriline autentimine (2FA).
3. **Õngitsemine:**
    - Probleem: Pahatahtlikud lingid või e-kirjad, mis varastavad kasutajaandmeid.
    - Lahendus: Skeptiline suhtumine tundmatutesse linkidesse ja manustesse.

Plokiahel ja infoturve

Plokiahel on detsentraliseeritud andmebaas, mis salvestab tehingute ajalugu räsifunktsioonide abil.

- **Kasutus:**
    - Bitcoin ja teised krüptovaluutad.
    - Dokumendi allkirjastamine ja autentsuse tõestamine.
- **Kaitsemeetodid:**
    - Hajutatus vähendab ühekordse ründe riski.
    - Räsiahel tagab andmete terviklikkuse.

Infoturbe rakendused ja standardid

- **Eesti infoturbestandard (E-ITS):**
    - Eesti infoturbestandard on kooskõlas rahvusvaheliselt tunnustatud ISO/IEC 27001 standardiga.
    - Standard aitab organisatsioonidel saavutada sobiva infoturbe taseme.
- **Turvakihtide rakendused:**
    - **SSO (*Single Sign-On*):** Üks autentimine võimaldab juurdepääsu mitmele rakendusele.
    - **Turvaline digiallkirjastamine:** ID-kaart, Mobiil-ID, Smart-ID.
- **Küberturbe rakendused:**
    - **X-tee:** Andmevahetuskiht, mis tagab turvalisuse ja andmete hajutuse.
    - **Plokiahel:** Kasutatakse krüptovaluutades ja turvalises andmevahetuses.

Inimfaktor infoturbes

- **Probleemid:**
    - Lõppkasutajad on sageli lihtsasti manipuleeritavad.
    - Mugavus seab turvanõuetele piiranguid.
- **Lahendused:**
    - Koolitus ja teadlikkuse tõstmine.
    - Küberhügieeni parimate praktikate järgimine (nt tugevad paroolid, tarkvarauuendused).

Plokiahel ja kvantarvutid

- **Plokiahela kasutus:**
    - Turvaline andmevahetus ja kokkulepped (nt krüptovaluutad, NFT-d).
    - Tagab detsentraliseerituse ja andmete terviklikkuse.
- **Kvantarvutite mõju:**
    - Tänapäevased asümmeetrilised krüptograafia algoritmid võivad olla kvantarvutitega haavatavad.
    - Uued kvantkindlad algoritmid arendamisel.

Infoturve ei ole kunagi staatiline – see nõuab pidevat tähelepanu ja kohandumist muutuva keskkonnaga!