Riskianalüüs, turvastandardid

- Riskianalüüs
- Turvapoliitika
- TCSEC turvaklassid
- EAL turvaklassid
- ISO 27000 pere
- ISKE turvaklassid

Riskianalüüs

- Potentsiaalsete ohtude tõenäosused on erinevad
- Erinevate ohtude poolt tekitatav kahju on erinev
- Riskianalüüs — hindame reaalseid ohte ning kulutusi ning püüame leida aktsepteeritava riski, kus turbekulud on ligikaudu võrdsed tõenäoliste kahjudega

Riskianalüüsi sammud

- Objekti piiritlemine, varade liigitamine
- Varade spetsifitseerimine
- Varade hindamine
- Ohtude, nõrkuste ja olemasolevate turbevahendite spetsifitseerimine
- Turvarikete tõenäosuste hindamine
- Oodatava kahju hindamine

Turvapoliitika

- Ootused infosüsteemi korrektseks kasutamiseks
- Protseduurid turvaintsidentide ärahoidmiseks
- Protseduurid turvaintsidentidele reageerimiseks
- Igale objektile on määratud turbe eest vastutaja
- Aluseks igasugusele infoturbealasele tegevusele asutuses
- Turvalisus on protsess, mitte valmis saav asi. Seetõttu on ka turvapoliitika iteratiivselt uuenev.

TCSEC turvaklassid

- TCSEC — USA kaitseministeeriumi vanem turvanormistik ("vikerkaarevärvilised raamatud")
- D — minimaalne kaitse (sisuliselt turbeta süsteem)
- C1 — kaitstud OS, diskretsionaarne pääsu reguleerimine
- C2 — C1 + peenem granulaarsus + pidev auditeerimine
- B1 — C2 + mandatoorne pääsu reguleerimine
- B2 — B1 + formaalne mudel + hierarhilised turvatasemed
- B3 — B2 + topeltauditeerimine + vigade puudumine disainis
- A1 — B3 + formaalne tõestus, et süsteem on korrektne
- A2 — tuleviku jaoks reserveeritud

EAL turvaklassid — *Common Criteria*

- EAL1 — funktsionaalselt testitud
- EAL2 — struktuurselt testitud
- EAL3 — metoodiliselt arendatud; testitud
- EAL4 — metoodiliselt disainitud; testitud ja üle vaadatud
- EAL5 — poolformaalselt disainitud; testitud
- EAL6 — poolformaalselt verifitseeritud disain; testitud
- EAL7 — formaalselt verifitseeritud disain; testitud

ISO 27000 standardipere

- Standardipere turbe korraldamise kohta
- ISO/IEC 27000 — ülevaade ja terminoloogia
- **ISO/IEC 27001 — turbehaldus**
- ISO/IEC 27002 — infotehnoloogia, turbemeetodid, infoturbemeetodite tavakoodeks
- ...
- Rahvusvaheline standard auditeerimaks organisatsioone, süsteeme

Eesti etalonturbe süsteem — ISKE

- Infosüsteemide kolmeastmeline etalonturve
- `https://iske.ria.ee/`
- Kohustuslik riiklike andmekogude, riigi ja kohalike omavalitsuste sisemiste infosüsteemide jaoks
- Etalonturve — valmis turvameetmete komplekt vastavalt turvaklassile
- Põhineb esialgselt Saksa BSI etalonturbel, hiljem omasoodu edasi arenenud
- Riskianalüüs on suures osas varem valmis tehtud (ohtude ja meetmete kataloogid)
- Tulemuseks kolm taset — madal, keskmine, kõrge

Eesti turvaklassid (ISKE)

- 3 sõltumatut mõõdet
  - Konfidentsiaalsus (S)
  - Käideldavus (K)
  - Terviklus (T)
- Kokku on andmekogu turvaklassiks näiteks S0K2T2
- Igal mõõtmel 4 taset, seega kokku $4 \times 4 \times 4 = 64$ turvaklassi

Eesti turvaklassid — konfidentsiaalsus

- S3 — Andmete avalikustamine on ohtlik riigi, asutuse või inimese julgeolekule (võib põhjustada kontrollimatuid muutusi riigile või asutusele tähtsates süsteemides. Riigi korral on kahjud võrreldavad eelarvega, ettevõtte korral aastakäibega). Juurdepääsupiirangutega teave.
- S2 — Salajane. Andmete avalikustamine häirib riigi või asutuse funktsioneerimist või rikub inimese privaatsust (riigi korral ulatuvad kahjud miljonitesse, ettevõtte korral 10% aastakäibest). Juurdepääs lubatav piiratud ringile õigustatud huvi korral.
- S1 — Andmete avalikustamine võib põhjustada materiaalset või moraalset kahju. Asutusesiseseks kasutamiseks õigustatud huvi korral.
- S0 — Avalikud andmed

Eesti turvaklassid — käideldavus

- K3 — töökindlus 99,9% (seisak kuni 10 min nädalas), lubatav reaktsiooniaja kasv tippkoormusel sekundites (1-10)
- K2 — töökindlus 99% (seisak kuni 2h nädalas), lubatav reaktsiooniaja kasv tippkoormusel minutites (1-10)
- K1 — töökindlus 90% (seisak kuni ligi ööpäev nädalas), lubatav reaktsiooniaja kasv tippkoormusel tundides (1-10)
- K0 — töökindlus pole oluline, jõudlus pole oluline

Eesti turvaklassid — terviklus

- T3 — info allikal, selle muutmise ja hävitamise faktil peab olema tõestusväärtus; vajalik on info õigsuse, täielikkuse ja ajakohasuse kontroll reaalajas
- T2 — info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad; vajalikud on perioodilised info õigsuse, täielikkuse ja ajakohasuse kontrollid
- T1 — info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad; info õigsuse, täielikkuse, ajakohasuse kontrollid erijuhtudel ja vastavalt vajadusele
- T0 — info allikas, muutmise ega hävitamise tuvastatavus ei ole olulised; info õigsuse, täielikkuse ja ajakohasuse kontrollid pole vajalikud