

Ettevõtte infoturbe alused

Erkki Leego
juhtivpartner
Hansson, Leego & Partner





1. Konfidentsiaalsus

- Andmete kättesaadavus ainult selleks volitatud tarbijaile (isikutele või tehnilistele süsteemidele) ning kättesaamatus kõigile ülejäänutele

2. Terviklus

- Andmete päritolu autentsus ning volitamatu muutuste puudumine

3. Käideldavus

- Kasutamiskõlblike andmete õigeaegne ja hõlbus kättesaadavus selleks volitatud tarbijaile (isikutele või tehnilistele vahenditele)

Andmete turvaklass (nt. R1K2T3S1)



HANSSON, LEEGO
& PARTNER

Kui on tahe, on ka võimalus!

<p>Teabe hilinemise tagajärgede lubatav kaalukus (R):</p> <p>R0 - teabe saamatajäamisega ei kaasne tagajärgi; R1 - teabe saamatajäamisega võib tuua kaasa takistusi funktsiooni täitmisele; R2 - teabe saamatajäamisega toob kaasa olulise takistuse funktsiooni täitmisele; R3 - teabe saamatajäamisega toob kaasa funktsiooni täitmatajäämise.</p>	<p>Aegkriitilise teabe käideldavus (K):</p> <p>K0 - teabe saamisele ei ole seatud tähtaegu; K1 - teabe saamisele on seatud tähtaeg päevades; K2 - oluline on teabe saamine tundide jooksul; K3 - oluline on teabe saamine sekundite jooksul.</p>
<p>Teabe terviklus (T):</p> <p>T0 - teabe allikas ega muutmise tuvastatavus ei ole olulised; T1 - teabe muutmise fakt peab olema tuvastatav; T2 - teabe allikas peab olema tuvastatav; T3 - tabel on tõestusväärne.</p>	<p>Teabe konfidentsiaalsus (S):</p> <p>S0 - juurdepääsu teabele ei piirata; S1 - teabele juurdepääsu tingimuseks on juurdepääsu taotleva isiku identifitseerimine; S2 - juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral; S3 - teave on seaduse alusel tunnustatud juurdepääsupiiranguga teabeks.</p>

Allikas: VV määrus nr. 273 „Infosüsteemide turvameetmete süsteemi kehtestamine”

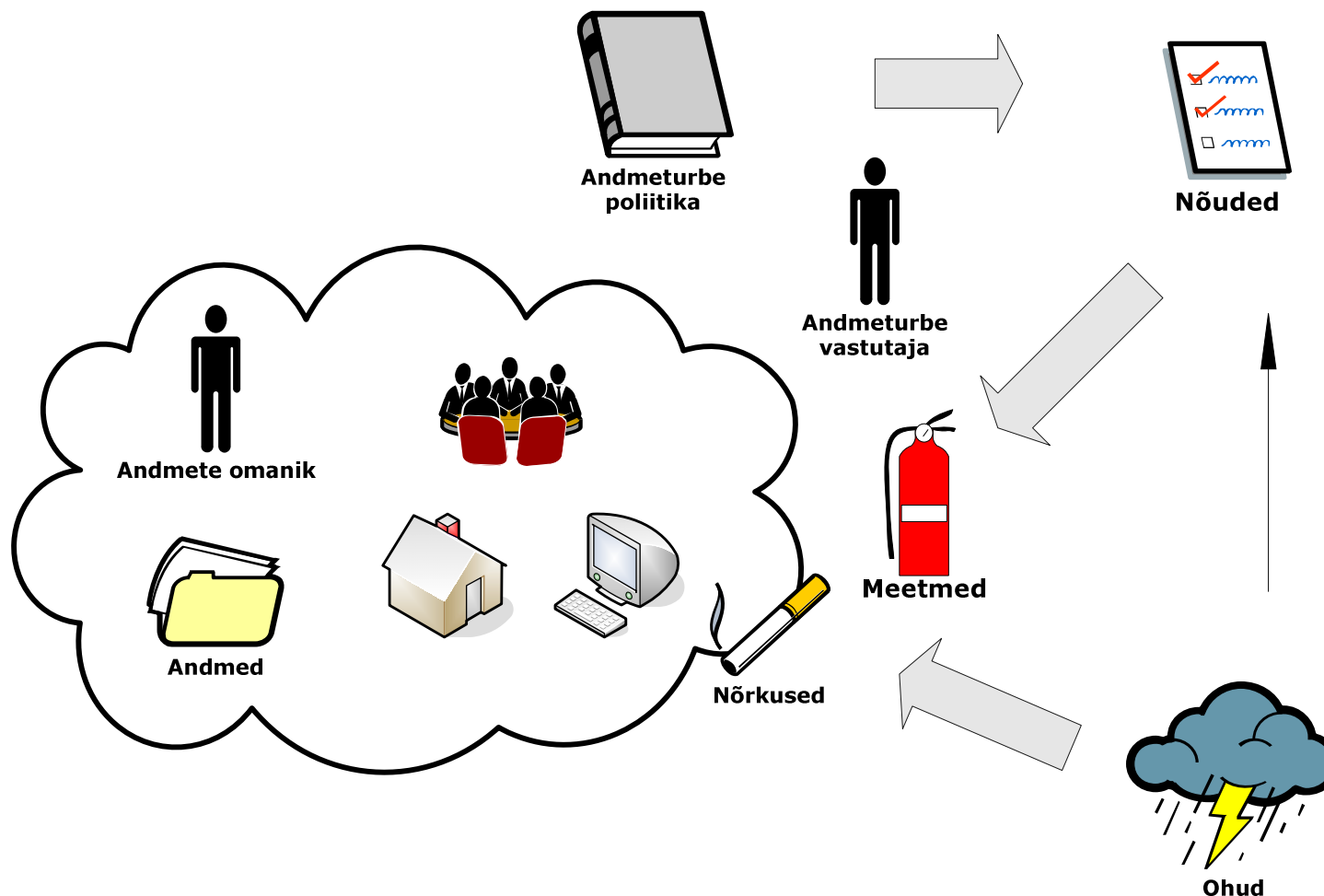
Erkki Leego – juhtivpartner



- Oht
 - Süsteemi või organisatsiooni kahjustada võiva soovimatu intsidendi potentsiaalne põhjus
- Nõrkused
 - Vara või vararühma nõrk koht, mida saab ära kasutada oht
- Risk
 - Võimalus, et vaadeldav oht kasutab ära mingi vara või vararühma nõrkused, põhjustades varade kaotuse või kahjustuse
- Turvameede
 - Riski kahandav teoviis, protseduur või mehhanism

Andmeturbe põhimõisted

Kui on tahe, on ka võimalus!

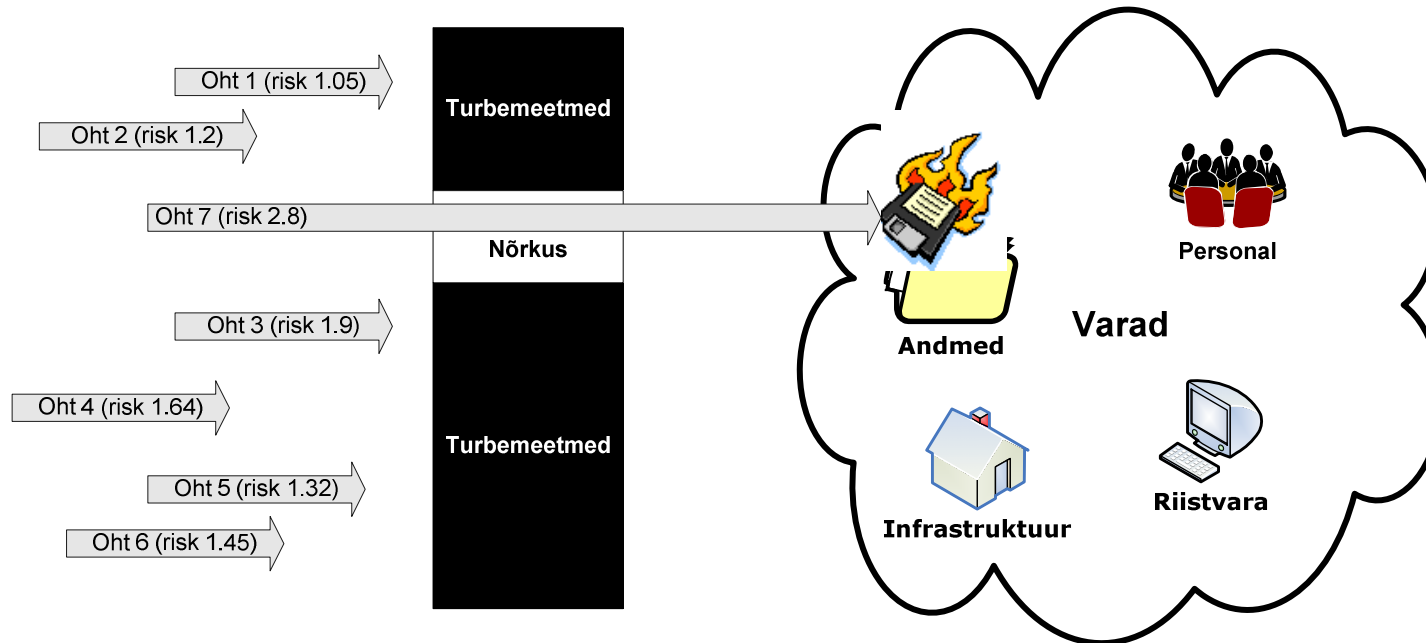


Erkki Leego – juhtivpartner

- Maavärin
- Üleujutus
- Orkaan
- Äike
- Tööstustegevus
- Pommirünne
- Relvade kasutamine
- Kahjutuli
- Sihilik kahjustamine
- Elektritoite katkemine
- Veevarustuse katkemine
- Õhu konditsioneerimise rike
- Riistvara rikked
- Toite kõikumine
- Äärmuslik temperatuur ja niiskus
- Tolm
- Elektromagnetiline kiirgus
- Elektrostaatilised laengud
- Vargus
- Salvestuskandjate volitamatu kasutamine
- Salvestuskandjate rikkumine
- Ekspluatatsioonipersonali eksitus
- Hoolduseksitus
- Tarkvara tõrge
- Tarkvara kasutamine volitamata poolt
- Tarkvara kasutamine volitamata viisil
- Kasutaja identsuse teesklus
- Tarkvara ebaseaduslik kasutamine
- Ründetarkvara
- Tarkvara ebaseaduslik import või eksport
- Ekspluatatsioonipersonali eksitus
- Hoolduseksitus
- Volitamata kasutajate võrgupöördus
- Võrguaparatuuri kasutamine volitamata viisil
- Võrgukomponentide tehniline rike
- Edastusvead
- Liinide kahjustused
- Liikluse ülekoormus
- Pealtkuulamine
- Sidesse sisseimbumine
- Liikluse analüüs
- Sõnumite väär marsuutimine
- Sõnumite ümbermarsuutimine
- Salgamine
- Sideteenuste (st võrguteenuste) tõrge
- Personalinappus
- Kasutajate eksitused
- Ressursside väärkasutus

- Keskkond ja infrastruktuur
 - nt. hoonete, uste ja akende füüsilise turbe puudumine
- Riistvara
 - nt. tundlikkus pinge kõikumiste suhtes
- Tarkvara
 - nt. pääsuõiguste väär jaotamine
- Side
 - nt. kaitsmata sideliinid
- Dokumendid
 - nt. hooletus kõrvaldamisel
- Personal
 - nt. puudulikud töölevõtmise protseduurid

- Riskianalüüs annab pingerea ohtudest, mis ettevõtte tegevust kõige rohkem kahjustada võivad
- Etalonturbe meetoodika
 - turvameetmete valimine kõigi süsteemide jaoks mingil etalontasemel. See tähendab, et sõltumata asutuse eripärast rakendatakse teatud etalonvalikut meetmeid ja loota, et sellest piisab. Puuduseks on, et kui etalontase on määratud liiga kõrgele, tehakse liigseid kulutusi.
- Mitteformaalne meetoodika
 - ei põhine struktureeritud meetoditel, vaid kasutab ära inimeste teadmust ja kogemust. Puuduseks võib olla, et struktureeritud meetodikata kasvab mõnede riskide ja vaatlusalade tähelepanuta jätmise tõenäosus.
- Detailne riskianalüüs
 - kõigi süsteemide detailne analüüs. See hõlmab varade piiritlemist ja väärtustamist, neid varasid ähvardavate ohtude tugevuse hindamist ja varade nõrkuste hindamist.
- Segametoodika
 - jämeda riskianalüüsiga selgitatakse välja süsteemid, mille risk on suur või mis on eluliselt tähtsad organisatsiooni talitlusele. Saadud tulemuse põhjal liigitatakse süsteemid sellisteks, mis asjakohase kaitse saavutamiseks nõuavad detailset riskianalüüsi, ja sellisteks millele piisab etalonkaitsest.



Riski suuruse hindamise valem

$$\left(\begin{array}{l} \text{Ohu} \\ \text{realiseerumise} \\ \text{tõenäosus} \\ \text{(väike, keskmine, suur) * K1} \end{array} + \begin{array}{l} \text{Ohu} \\ \text{realiseerumise} \\ \text{hõlpsus} \\ \text{(väike, keskmine, suur) * K2} \end{array} + \begin{array}{l} \text{Mainekahju} \\ \text{(väike, keskmine, suur) * K3} \end{array} + \begin{array}{l} \text{Rahaline} \\ \text{kahju} \\ \text{(väike, keskmine, suur) * K4} \end{array} \right) / 4 = \text{Risk}$$

{ väike = 1, keskmine = 2, suur = 3 }

- Turvameetmed otstarbe järgi:
 - ennetavad, avastus- ja taastusmeetmed
- Turvameetmed teostusviisi järgi:
 - organisatsioonilised, füüsilised ja infotehnoloogilised meetmed
- Esmased andmeturbemeetmed (näide)
 - Usaldusväärse elektroonilise identiteedi tagamine
 - Infosüsteemi kasutajate korra kehtestamine
 - Kasutajatunnuste väljastamise korra kehtestamine
 - Võtmete ja koodide väljastamine kontrolli alla
 - Konfidentsiaalsusnõuded töölepinguisse
 - Ruumide ja seadmete kaitse

- Talitluspidevusplaani peab määratlema, millal on tegemist kriisiga, kes kriisi eest vastutab, kuidas toimub teavitamine ja millised tegevused kriisi korral käivitatakse.
- Põhikomponendid
 - põhiprotsessi ja tugiprotsesside kirjeldus koos oluliste ressurssidega,
 - kriiside määratlus, vastutava kriisijuhi määramine ja kriisiteavituse korraldus
 - alternatiivtegevuste kavad ja oluliste ressursside taasteplaanid
 - plaani kaasajastamise, koolituse ja testimise korraldus

10 olulisemat meedet



1. Uksed lukku ka tööpäeva ajal
2. Pidage arvet kasutajatunnuste üle
3. Tagage turvainfo jõudmine töötajateni
4. Tehke regulaarselt tagavarakoopiaid
5. Viirustõrje igasse arvutisse
6. Dokumentide hoidmiseks kindel kord
7. Tagavaratoide olulistele seadmetele
8. Kontrolljäljed kõikidest tegevustest
9. Reeglid andmete kasutamiseks
10. Koostage ülevaade oma infovaradest

Mida ette võtta?

- Määrake andmeturbe eest vastutaja
- Tehke ettevõttes infovarade inventuur
- Määrake andmetele omanikud
- Töötage välja ja rakendage ettevõtte turvameetmed
- Kontrollige regulaarselt protseduuride täitmist

- Andmekaitse algab suhtumisest
- Andmeturve ei ole IT spetsialistide pärusmaa
- Andmeturbega ei tasu üle pingutada

Täna!



Kui on tahe, on ka võimalus!

Kui on tahe, on ka võimalus!

Erkki Leego, erkki.leego@hlp.ee, www.hlp.ee

Erkki Leego – juhtivpartner