



Kui on tahe, on ka võimalus!

Andmeturbe praktika ja teooria tasakaal

Erkki Leego
juhtivpartner
Hansson, Leego & Partner



Erkki Leego – juhtivpartner

- Üle 12 aasta tundliku info kaitsel
 - Vabariigi Presidendi Kantselei, infonõunik
 - Riigikogu Kantselei, infosüsteemide ja tehnikaosakonna juhataja
 - Tartu Ülikooli Kliinikum, IT direktor
 - Hansson Leego & Partner, juhtivpartner
- Hansson, Leego & Partner
 - Ida-Tallinna Keskhaigla, Põhja- Eesti Regionaalhaigla, Fontes PMP, Riigikogu Kantselei, Õiguskantsleri Kantselei
 - Riskianalüüs, tegevuskava
 - Tervise Arengu Instituut, Tartu ja Pärnu linnavalitsus, Kadrina vallavalitsus, Riigikantselei
 - ISKE rakendamine
 - TÜ Eesti Geenivaramu; Quattromed HTI Laborid; Lemeks; Rait; Omandi; Tallmac
 - Strateegiline IT juhtimine

100% turvalisust ei ole olemas



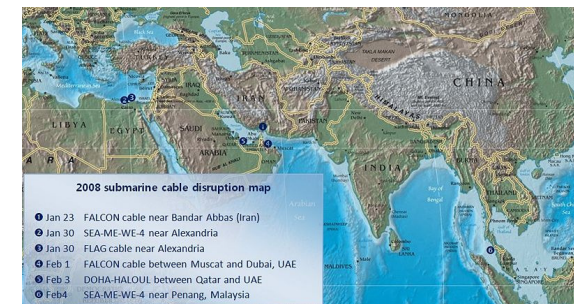
HANSSON, LEEGO
& PARTNER

Kui on tahe, on ka võimalus!

- 9/11 terrorirünnak (11.09.01)
 - Kaks 110-korruselist WTC hoonet ja hulk muid hooneid hävinenud, 18 000 väikest äri hävinenud või ümber paigutatud
 - Börsid (NYSE, ASE, NASDAQ) suletud 6 päeva
 - Investeerimispank Cantor Fitzgerald L.P. kaotas 658 töötajat
- Societe Generale hiigelpettus (01/08)
 - Jérôme Kerviel kauplemistehingud põhjustasid pangale 76 miljardit krooni kahju
 - Süüdistus volitamata ligipääsus ja usalduse kuritarvitamises
- Lähis-Ida riikide interneti katkestus (01/08)
 - Mitme veealuse kaabli katkemine põhjustas paljude Lähis-Ida riikide Interneti side kadumise 10 päevaks
 - 80 milj. kasutajat häiritud (70% Egiptusest, 60% Indiast)
- UK MTA andmete kadumise intsident (10/07)
 - Kaks Suurbritannia maksu- ja tolliameti arvutiketast kõikide lastetoetust saanud perede andmetega läks teekonnal ühest kontorist teise kaduma
 - Intsident puudutab 25 milj. UK elanikku
- Küberrünnakud Eestis kevad 2007
 - DOS rünnakud Eesti riigiasutustele ja pankadele



 **SOCIETE GENERALE**
Corporate & Investment Banking



Erkki Leego – juhtivpartner

- ISO27000 standardite perekond. Infotehnoloogia,
...
- EVS-ISO/IEC 13335 1-5 Infoturbe halduse suunised
- ISO 13569 Pangandus ja sellega seotud rahandusteenused
- ITIL (IT Infrastructure Library), IT teenuste haldamise parima praktika kogum
- IT Grundschutzhandbuch – Saksamaa infoturbeameti IT etalonturbe käsiraamat
- COBIT (ISACA juures tegutsev IT Governance Institute)– IT juhtimise raamistik ärieesmärkide tagamisel
- ISKE – Eestis riigiasutustele kehtestatud infoturbe raamistik

- ISKE - Infosüsteemide turvameetmete süsteem (etalonturve)
 - Riigi ja kohalike omavalitsuste andmekogude jaoks
 - Valitsuse määrus 252 (20.12.07), rakendusjuhend ver. 5.0 (34+2164 lk) (haldab RIA)
 - Andmete turvaklass – 3 komponenti, 4 taset (K2T3S1)
 - Turbeastmed – madal (L), keskmine (M) ja kõrge (H)
 - Andmekogu kasutusele võtmise ajaks peavad turvameetmed olema rakendatud
- Infosüsteemid tuleb regulaarselt auditeerida
 - Turbeastme H audit iga 2 aasta järel (01.03.09)
 - Turbeastme M audit iga 3 aasta järel (01.12.10)
 - Turbeastme L audit iga 4 aasta järel (01.03.11)



- Turvaeesmärgid ja – põhimõtted
- Turbe organisatsioon ja infrastruktuur
- Infoturbe ja riskianalüüsi ning riskihalduse strateegia
- Informatsiooni tundlikkus ja riskid
- Riistvara ja tarkvara turve
- Side turve
- Füüsiline turve
- Personali turve
- Dokumentide ja andmekandjate turve
- Tegevuskatkematus, sh ootamatuste plaanimise ja avariijärgse taaste, strateegia ja plaan(id)
- Kaugtöö
- Alltöövõtu poliitika
- Muudatuste reguleerimine

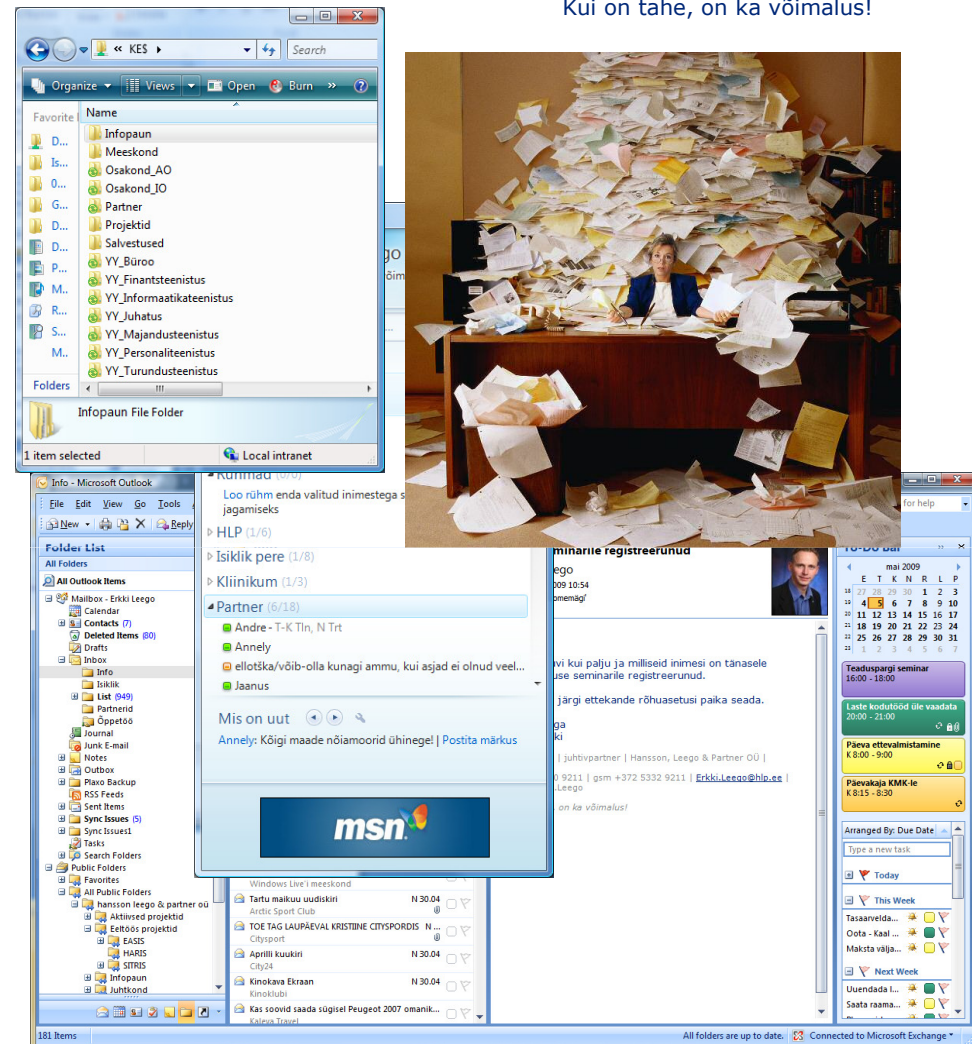


Andmete väärtus

Erinevad infoallikad

- Andmebaaside kanded
- Dokumendid
 - Elektroonilised
 - Paberdokumendid
- E-kirjad
- Koosolekute märkmed - salvestused
- Telefonivestlused
- Skype vestlused
- Tööde register

Kui on tahe, on ka võimalus!



Erkki Leego – juhtivpartner



- Mida on vaja kaitsta?
 - Miks on seda vaja kaitsta? Mis juhtub siis kui ei kaitse?
- Milliseid potentsiaalseid ebasoovitavaid tagajärgi me soovime vältida?
 - Millise hinnaga? Kui suurt katkestust võime me enne tegutsemist taluda?
- Kuidas me määratleme ja efektiivselt haldame jääkriski?

The Art of Information Security Governance, Julia H. Allen, 2008, Qatar Information Security Forum

Erkki Leego – juhtivpartner



Põhimõisted



1. Konfidentsiaalsus

- Andmete kättesaadavus ainult selleks volitatud isikule või tehnilisele vahendile

2. Terviklus

- Andmete õigsuse, täielikkuse ja ajakohasuse tagatus ning päritolu autentsus ja volitamata muutuste puudumine

3. Käideldavus

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

Andmete turvaklass (nt. K2T3S1)



HANSSON, LEEGO
& PARTNER

Kui on tahe, on ka võimalus!

Andmete käideldavus (K):

K0 – töökindlus – pole oluline; jõudlus – pole oluline;

K1 – töökindlus – 90% (lubatud summaarne seisak nädalas ~ ööpäev); lubatav nõutava reaktsioonija kasv tippkoormusel – tunnid (1÷10);

K2 – töökindlus – 99% (lubatud summaarne seisak nädalas ~ 2 tundi); lubatav nõutava reaktsioonija kasv tippkoormusel – minutid (1÷10);

K3 – töökindlus – 99,9% (lubatud summaarne seisak nädalas ~ 10 minutit); lubatav nõutava reaktsioonija kasv tippkoormusel – sekundid (1÷10).

Andmete terviklus (T):

T0 – info allikas, muutmise ega hävitamise tuvastatavus ei ole olulised; info õigsuse, täielikkuse ja ajakohasuse kontroll pole vajalik;

T1 – info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad; info õigsuse, täielikkuse ja ajakohasuse kontroll erijuhtudel ja vastavalt vajadusele;

T2 – info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad; vajalik on info õigsuse, täielikkuse ja ajakohasuse perioodiline kontroll;

T3 – info allikas, selle muutmise ja hävitamise faktil peab olema tõestusväärne; vajalik on info õigsuse, täielikkuse ja ajakohasuse kontroll reaalajas.

Andmete konfidentsiaalsus (S):

S0 – avalik info: juurdepääsu teabele ei piirata (st lugemisõigus on kõigil huvitatutel, muutmise õigus on määratud tervikluse nõuetega);

S1 – info asutusesiseseks kasutamiseks: juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral;

S2 – salajane info: info kasutamine on lubatud ainult teatud kindlatele kasutajate gruppidele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral;

S3 – ülisalajane info: info kasutamine on lubatud ainult teatud kindlatele kasutajatele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral.

Allikas: VV määrus 20.12.07 nr. 252 „Infosüsteemide turvameetmete süsteem“

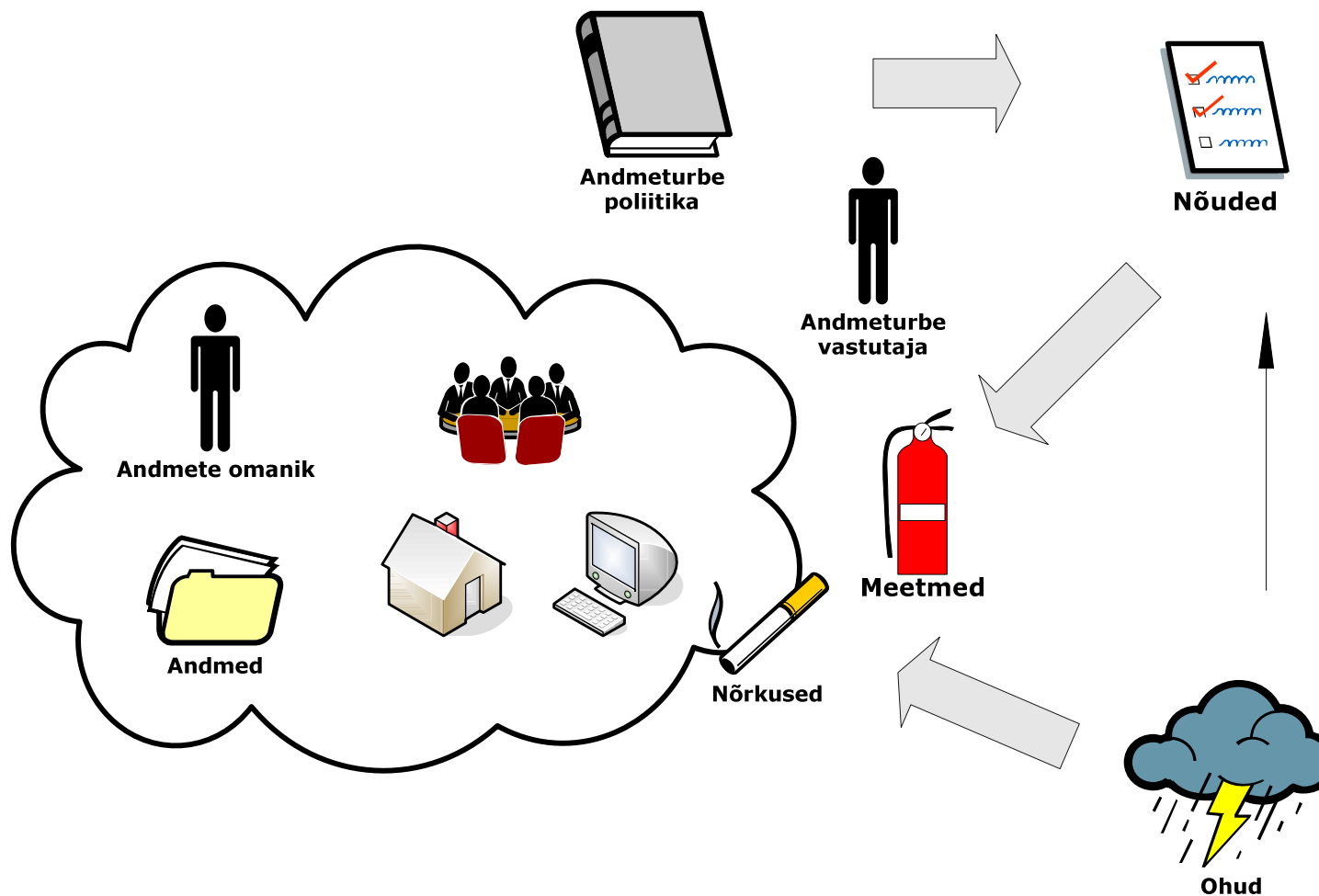
Erkki Leego – juhtivpartner

Andmeturbe praktika ja teooria tasakaal / 10.06.10 / KHK arvutierialade seminar Haapsalus (12/40)

- 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

Ründed ja muud ohud (ISKE)



HANSSON, LEEGO
& PARTNER

Kui on tahe, on ka võimalus!

- G1 – vääramatute jõud
- G2 – organisatsioonilised puudused
- G3 – inimvead
- G4 – tehnilised rikked ja defektid
- G5 – ründed
- G6 – andmekaitseohud

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

- Turvameetmed otstarbe järgi:
 - ennetavad meetmed
 - avastusmeetmed
 - taastusmeetmed

- Turvameetmed teostusviisi järgi:
 - organisatsioonilised meetmed
 - füüsilised meetmed
 - infotehnoloogilised meetmed

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

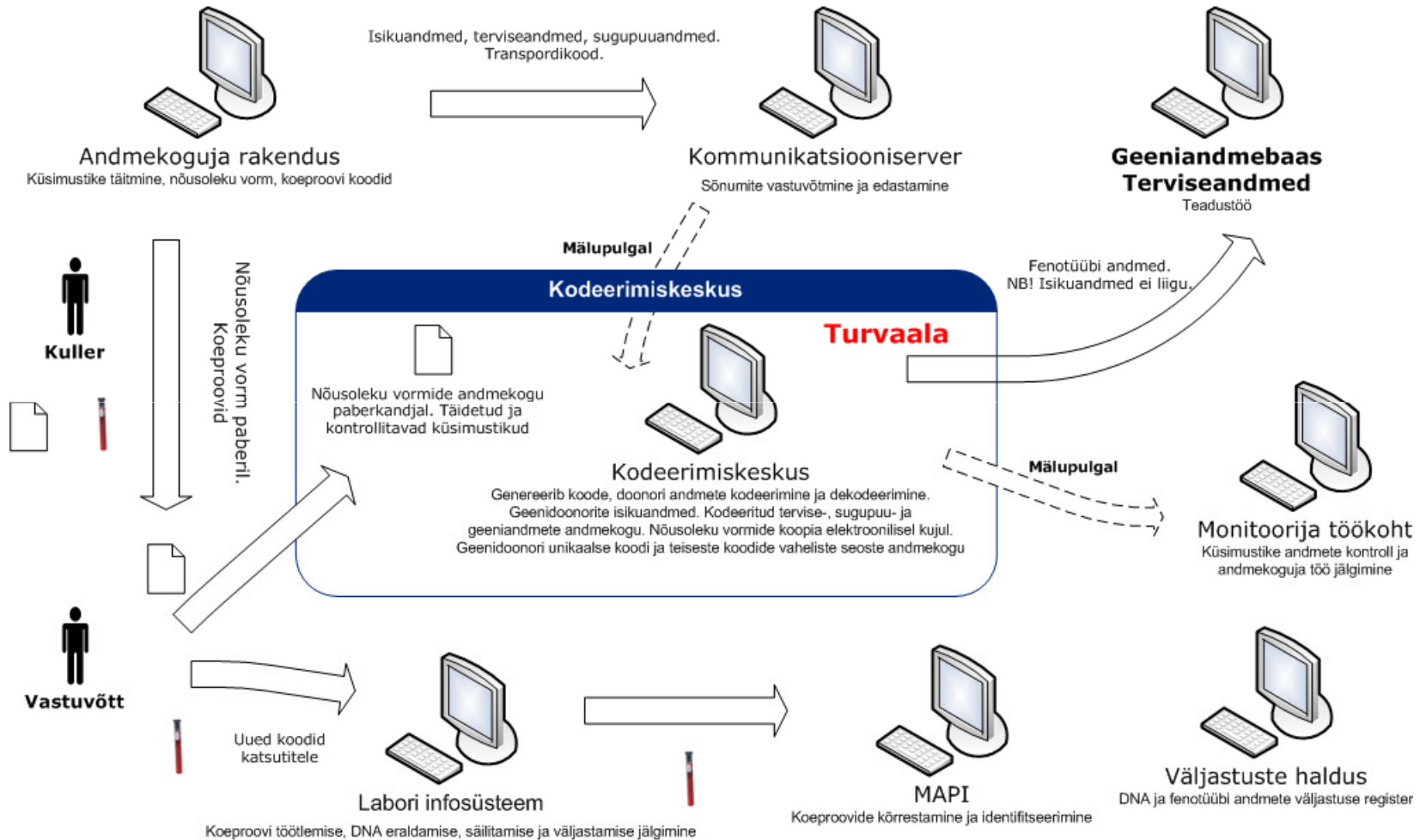


Näited infosüsteemidest

- Riigikogu Kantselei
 - Hääletussüsteemi töökindlus
 - 15.11.07 Postimees: "Keskerakonna tuntuim poolt- ja vastunuppudega mängija on Tõnu Kauba. 2000. aasta augustis visati ta aastaks fraktsioonist välja, kuna tema poolthääl aitas ametist maha võtta tollase kaitseväge juhataja Johannes Kerdi. Kaks aastat hiljem karistas fraktsioon Kaubat Ja Anti Liivi, sest nende süül õnnestus opositsioonil riigieelarve eelnõu parlamendi menetlusest välja lükata."
- Tartu Ülikooli Kliinikum
 - 22 suurt infosüsteemi 24/7
- Tartu Ülikooli Eesti Geenivaramu
 - Isikuandmete turvaline haldus

Näide infosüsteemist - EGV

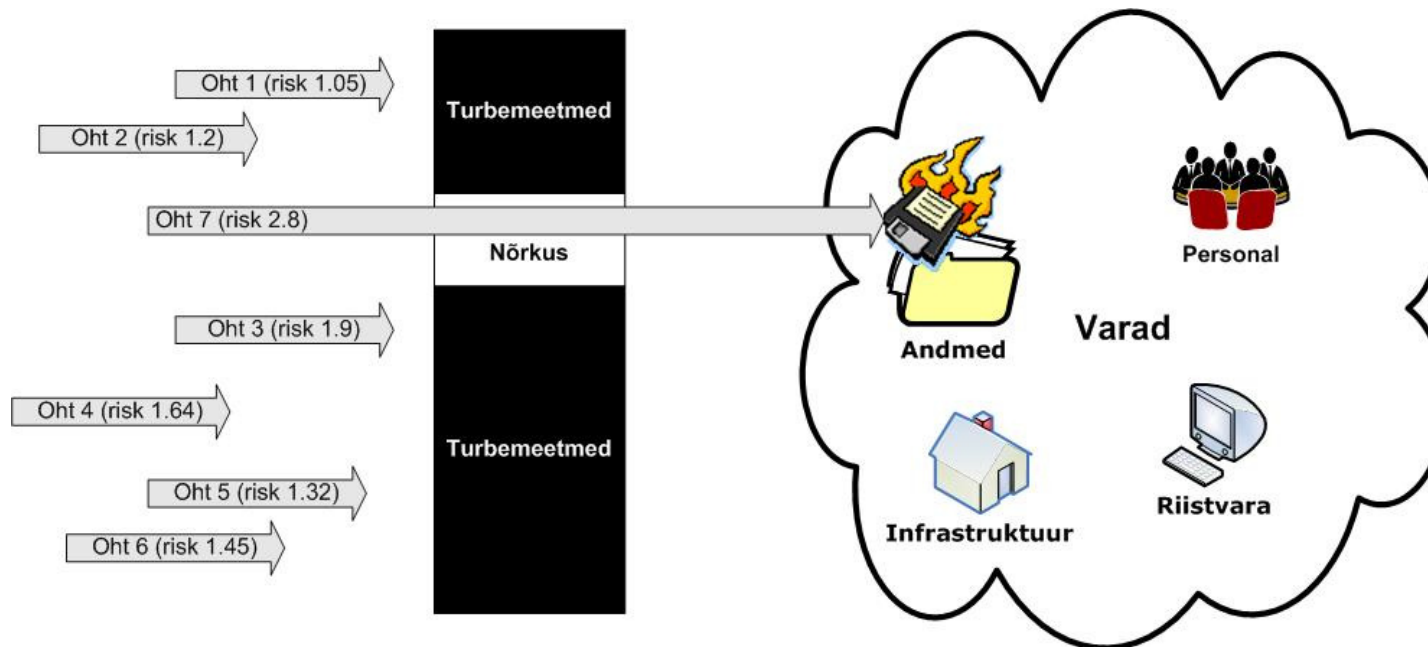
Kui on tahe, on ka võimalus!



Erkki Leego – juhtivpartner



Riski hindamine

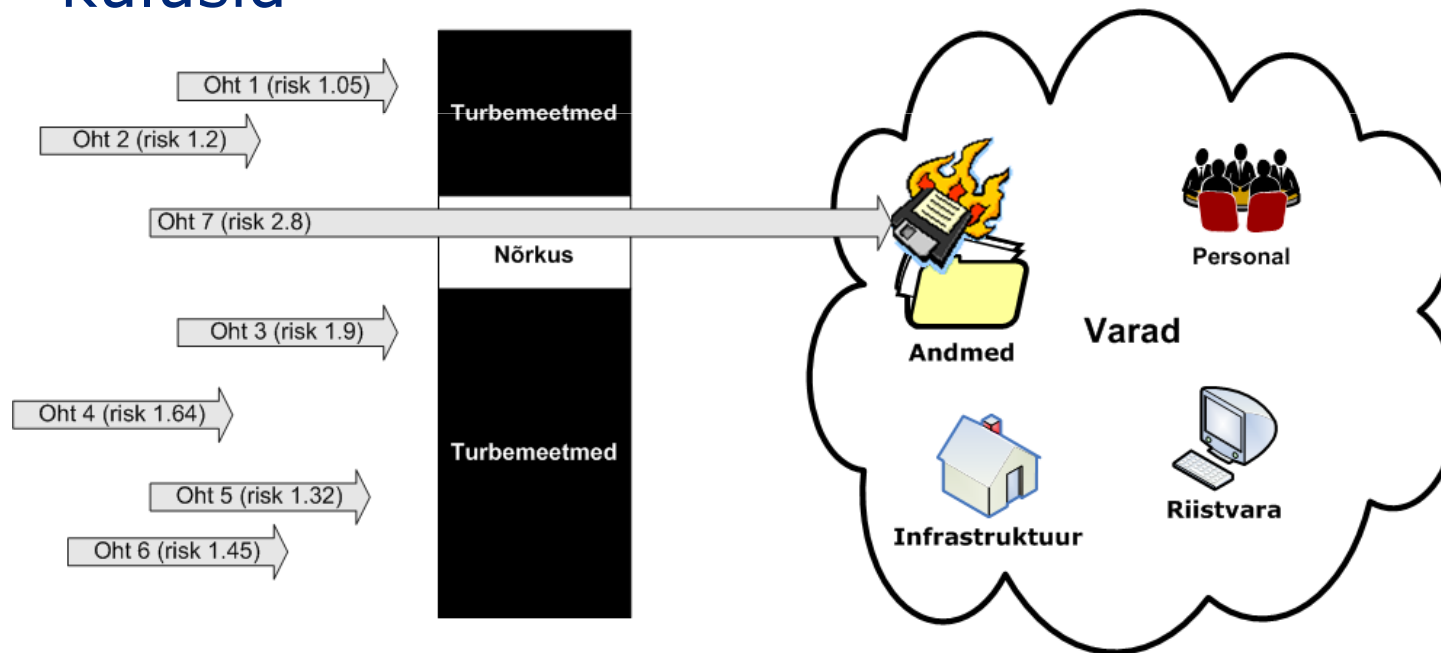


Riski suuruse hindamise valem

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

{ väike = 1, keskmine = 2, suur = 3 }

- Riskianalüüs annab ülevaate ettevõtte infovaradest ja nende kaitse olukorrast
- Juhtkonna poolt määratletud jääkrisk annab võimaluse piiritleda meetmeid ja kaasnevaid kulusid



10 tavalisemat probleemi

1. Ebatäielik ülevaade firma infovaradest ja turbe seisust
2. Töötajate hägus vastutus ja ebalojaalsus
3. Hoonete, uste, akende füüsilise turbe puudulikkus
4. Puudulikult hallatud pääsuõigused
5. Ettevõtte töötajate vähene turvateadlikkus
6. Puuduvad või vääralt hoiustatud tagavarakoopiad
7. Puudulik viirustõrje arvutites
8. Dokumentide ebapiisav arhiveerimine ja hävitamine
9. Ebakindel toitevõrk ja puuduvad tagavaravooluseadmed
10. Logide või nende analüüsi puudumine



Inimesed ja vastutus

- Andmeturve on seotud paljude valdkondadega
- Osapooled
 - Tippjuhtkond
 - Andmeturbe eest vastutaja
 - Valdonna eest vastutaja
 - IT meeskond
 - Tavatöötaja
 - Koostööpartner

- Personali valik
- Vastutus
- Teadlikkus
- Koolitus ja teavitamine
- Järelevalve



Dokumentatsioon



Mida pole kirjas, pole olemas

- Infoturbe poliitika
- Infoturbe kontseptsioon
- Infosüsteemi kasutamise kord
- Arvutikasutaja juhend
- Kurivaratõrje kontseptsioon
- Turvaintsidentide käsitlemise kord
- Turvaaspektid ja teavituskanalid
- IKT teenuste väljasttellimise kord
- Pääsulubade haldamise kord
- Pääsulubade register
- Krüptokontseptsioon
- Infosüsteemide spetsifikatsioon
- Infosüsteemide visuaalne skeem
- IS teenuste kirjeldused
- Serverite kirjeldused
- Tulemüüri kirjeldus
- Võrguseadmete kirjeldused
- Riistvara standard tööjaamadele
- Tarkvara standard tööjaamadele
- Tööjaamade ja lisaseadmete loend
- Serveri taasteplaan
- Töökoha taasteplaan
- Arvutivõrgu taasteplaan
- Varundusplaanid



Hea praktika

Efektive turbehalduse 11 tunnust



HANSSON, LEEGO
& PARTNER

Kui on tahe, on ka võimalus!



Governing for Enterprise Security (GES) Implementation Guide by Julia H. Allen and Jody R. Westby, 2007, <http://www.cert.org/governance/ges.html>

Erkki Leego – juhtivpartner

Mida parimad teevad?



HANSSON, LEEGO
& PARTNER

Parim = turbeintsidentide arv, nendega toimetulemise keskmine aeg, mittevastavuste arv ja nendega toimetulemise aeg

Kui on tahe, on ka võimalus!

- 70%: on loodud terviklikud turvalisuse ja vastavuse poliitikad
 - 70%: tegevjuht on turbe- ja riskihalduse esmane "omanik"
 - 52%: nähtav on turvalisuse ja vastavuste võtmeinfo
 - 78%: juhte informeeritakse regulaarselt IT-riskidest
 - 67%: on rakendatud kontrollid poliitika nõuete täitmise monitoorimiseks
 - 67%: on määratlenud kogu auditeerimiseks ja aruandmiseks vajamineva info
- Ühe aasta möödumisel:
 - 63%: vähendasid tegelike turbeintsidentide arvu
 - 70%: vähendasid keskmist intsidentidega toimetulemise aega
 - 48%: vähendasid keskmist intsidentidega toimetulemise kulu
 - 74%: vähendasid mittevastavuste arvu (auditi negatiivseid tulemusi)

Security Governance and Risk Management: The Rewards of Doing the Right Things and Doing Things Right, nov. 2007, Aberdeen Group. 140 organisatsiooni küsitlus

Erkki Leego – juhtivpartner

- Kulud olukorra hindamisele ja meetmete sh. dokumentatsioonile väljatöötamisele
 - väline konsultatsioon, enda töötajate tegevused
- Kulud infrastruktuuri planeerimisele ja seadistamisele
 - väline konsultatsioon, enda töötajate tegevused
- Investeeringud infrastruktuuri
 - tööjaamad, serverid, võrguseadmed, tagavara-koopiaseadmed või nende renditeenuse sisseostmine
- Investeeringud tarkvarale ja litsentsidele
- Investeeringud füüsilise turbe tagamiseks
- Kulud koolitusele ja teavitamistele

Kuidas mitte üle pingutada?

- Kulude õigsust on keeruline hinnata – turve on edukas siis kui midagi ei juhtu ...
- Tunne oma ettevõtte infoturbe olukorda
 - Riskianalüüs toob välja pingerea probleemidest ja nõrkustest
 - Tee selgeks mida ette võtta saab ja määratle kuna seda tehakse
- Lähtu äri-põhistest kriteeriumitest
 - Turvalisus on ärifunktsioon ja peab saama selliselt käsitletud
 - Valdkonnal peab olema selge vastutaja
 - Tee investeringuotsuseid samal viisil kui teisi ettevõtte ärilisi investeringuotsuseid
- Turve on protsess
 - Loo turvalisusele orienteeritud kultuur
 - Liigu paremuse suunas teadlike ja jõukohaste sammudega

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

Lähtuda tuleb standarditest, aga ...

... jalad peavad maas olema!

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

Andmeturbe praktika ja teooria tasakaal / 10.06.10 / KHK arvutierialade seminar Haapsalus (40/40)