

Kuidas turvalisusega mitte üle pingutada?

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
 - Põhja-Eesti Regionaalhaigla
 - riskianalüüs, poliitika, talitluspidevusplaan
 - Ida-Tallinna Keskhaigla
 - riskianalüüs, tegevuskava
 - Fontes PMP
 - riskianalüüs, tegevuskava
 - Õiguskantsleri kantselei
 - turvalisuse ja infoturbe poliitika piisavuse audit
 - Riigikogu kantselei
 - riskianalüüs ja tegevuskava
 - Majandus- ja kommunikatsiooniministeerium
 - ISKE rakendamise pilootprojekt Lääne-Viru maavalitsuses
 - Gennet Laboratories
 - turvalisuse ja poliitika sobivuse hindamine delikaatsete isikuandmetega töötlemiseks mõeldud infosüsteemide arendamisel ja hooldamisel
 - Eesti Geenivaramu; Quattromed; Lemeks; Rait; Omandi; Tallmac
 - Strateegiline IT juhtimine

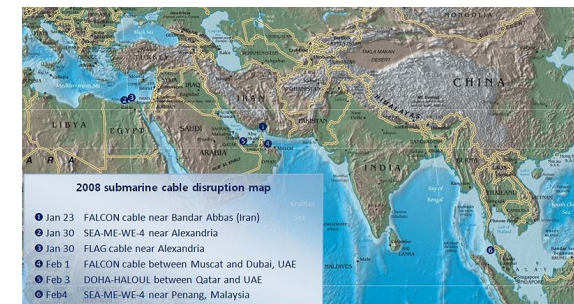
100% turvalisust ei ole olemas



HANSSON, LEEGO
& PARTNER

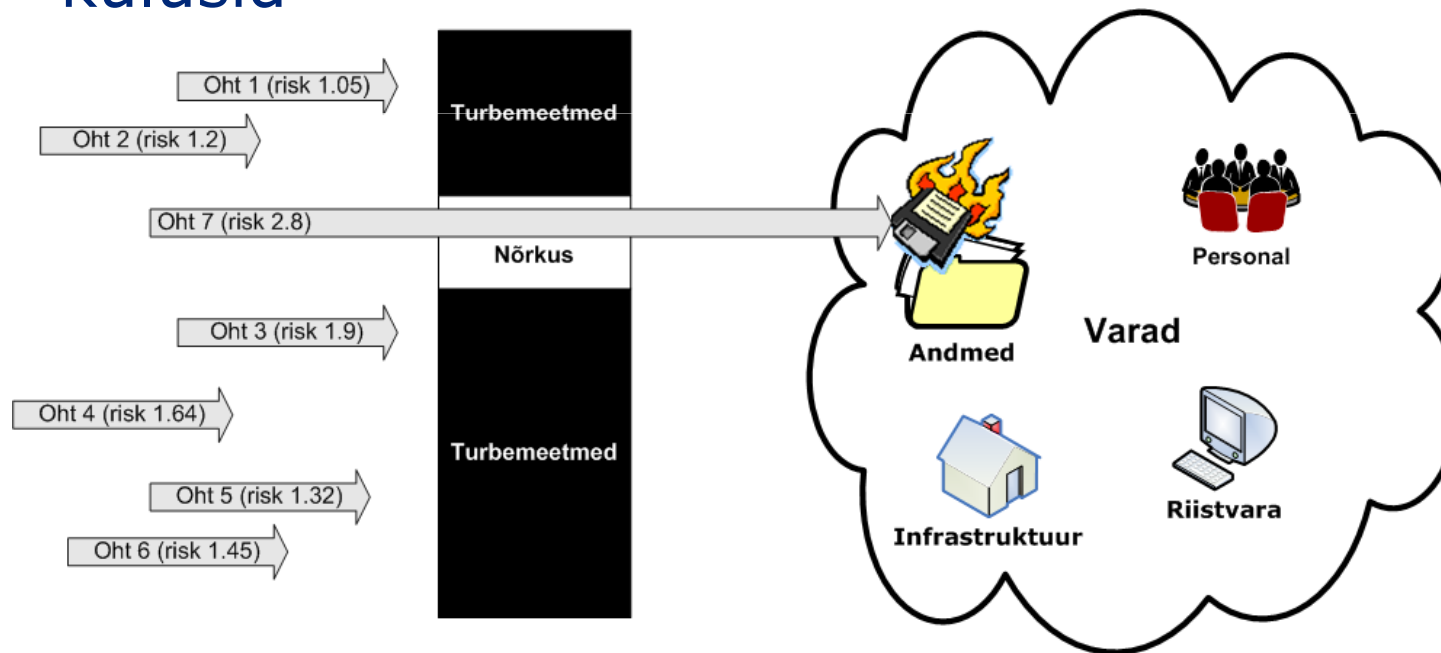
Kui on tahe, on ka võimalus!

- 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



Erkki Leego – juhtivpartner

- 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

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



- 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?

- 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

- 100% turvalisus pole võimalik – määratle oma jääkrisk
- Ole teadlik oma infovarade kaitse olukorrast
- Liigu paremuse suunas teadlike ja jõukohaste sammudega

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