

Minu andmed, kallis vara

Erkki Leego
juhtivpartner
Hansson, Leego & Partner



Erkki Leego – juhtivpartner

1. Ettekandja ja HLP tutvustus
2. Ettevõtte IT vajadus ja teabehaldus
3. IT teenuse sisseost
4. Andmekaitse
5. Kokkuvõte

- Haridus - MSc informaatikas
- Tööalane
 - Hansson Leego & Partner, juhtivpartner
 - Tartu Ülikooli Kliinikum, IT direktor
 - Riigikogu Kantselei, infosüsteemide ja tehnikaosakonna juhataja
 - Vabariigi Presidendi Kantselei, infonõunik
 - Tartu Ülikooli teabetalitus, vanemtoimetaja
- Õppejõud
 - Tartu Ülikool
 - 2007 - ... Kursus „Kasutajaliideste kavandamine“
 - International University Concordia Audentes
 - 1999-2004 Hüperteksti kursus meediatudengitele

- Konsultatsiooni- ja IT juhtimise ettevõtte



HANSSON, LEEGO
& PARTNER

- Firma põhitegevus on ettevõtete esindajana nende infosüsteemide toimimise ja arengu tagamine läbi kõrget erialast kompetentsi ja laialdast kogemust nõudvate teenuste
- HLP eksperdid on teostanud üle 100 IT arendusprojekti ning taganud infosüsteemi toimimist rohkem kui 70 ettevõttes (20-3000 töötajat).

1. ITK - IT juhtimine ja konsultatsioon

- Ettevõtte strateegiline IT juhtimine
- Infosüsteemi toimimise tagamine ja hooldus
- Infosüsteemi audit ja konsultatsioon

2. PRK - Arenduse koordineerimine ja järelvalve

- Ettevõtte esindamine IT arendusprojektides
- Hangete läbiviimine
- Tellijapoolne projektijuhtimine ja järelvalve

3. ATK - Andmeturbe konsultatsioon

- Riskianalüüsi läbiviimine
- Andmeturbe audit
- Talituspidevuse plaani koostamine
- ISKE juurutamine

- AS Rait, AS Lemeks, AS Tallmac, Quattromed
 - Infosüsteemi (>60 arvutit) toimimise koordineerimine (IT juht ja IT koordinaator)
- TÜ Eesti Geenivaramu
 - IT strateegia koostamine ja elluviimine, koostöövõrgustiku ning asutuse esindatuse tagamine olulistel valdkonna konverentsidel
- Lemeks AS, Salvest AS
 - Microsoft Dynamics AX tootmise komponendi juurutamise koordineerimine tellija esindajana
- Põllumajandusministeerium
 - Põllumajandusministeeriumi haldusala infosüsteemide kaardistamine ja IT strateegia koostamiseks lähteandmete koondamine
- Riigikogu Kantselei, Tartu Linnavalitsus, Fontes, ...
 - ISKE juurutamine, infovarade turvalisuse ja infoturbe poliitika piisavuse ning tervikluse auditeerimine
- Gruusia tervishoiu- ja sotsiaalprojektide rakendamise keskus
 - IT partner konsultatsiooniprojektis „Improvement of Hospital Governance/Management and Strategic planning“

* Terviknimekiri töödest - <http://www.hlp.ee/Projektid.htm>



Ettevõtte IT korraldus ja teabehaldus

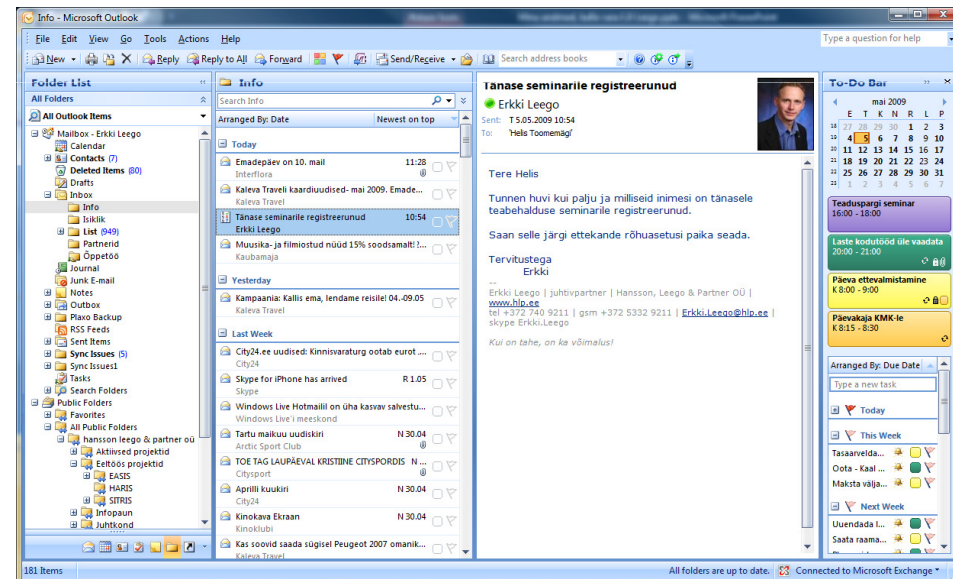
- Igapäevane elu toimib
 - Arvutid, serverid, võrk ja printerid töötavad
 - Standard- ja spetsiaaltarkvara toimib
 - Kui on probleem, saab kelleltki abi
 - Andmeturve tagatud
- Toimub areng
 - Ettevõtte kasvule ja ärifookusele vastavalt IT süsteemi arendamine
 - Tarkvaratoodete kasutuselevõtt (majandustarkvara, kliendihaldus jmt.)
 - Spetsiaaltarkvara loomine ja arendamine

- Õige informatsioon õigel ajal õiges kohas
 - Kes
 - Isiklik, ettevõtte, partnerid, kogukond, avalikkus
 - Kus
 - Minu arvuti, sisevõrk, erinevad asukohad
 - Kuna
 - Kohe, tööajal või ööajal, aastaid hiljem
 - Mis
 - Milline informatsioon? Kas volitatud?
 - Millega
 - Tööjaam, sülearvuti, nutitelefon

	Samal ajal	Erineval ajal
Samas kohas	“näost näkku” (klassid, koosolekuruumid)	asünkroonne suhtlus (projekti ajakava, koordineerimine)
Erinevates kohtades	sünkroonne jagatud (jagatud redaktorid, videoülekanne, <i>chat</i>)	asünkroonne jagatud (e-post, listserverid, blogid, wikid)

1. Suhtlusvahendid
 - E-post
 - Vestlus - Skype, MSN
2. Failisüsteem/dokumendihoidla
3. Siseinfo ja teadmusvaramu haldus
4. Raamatupidamine/majandusarvestus
5. Põhitegevusega seotud rakendused

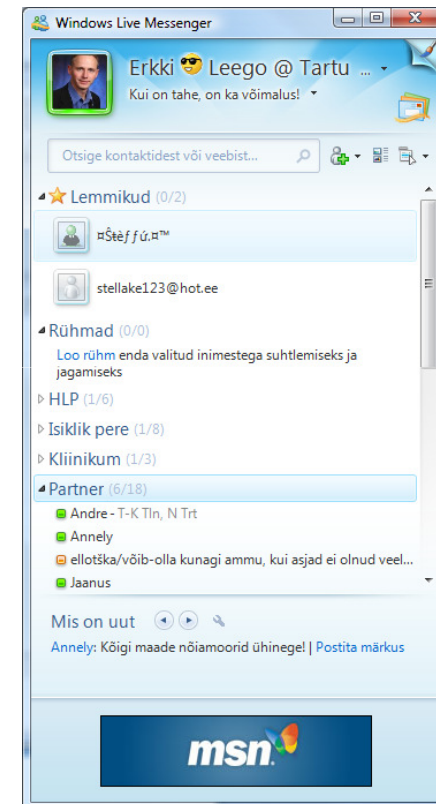
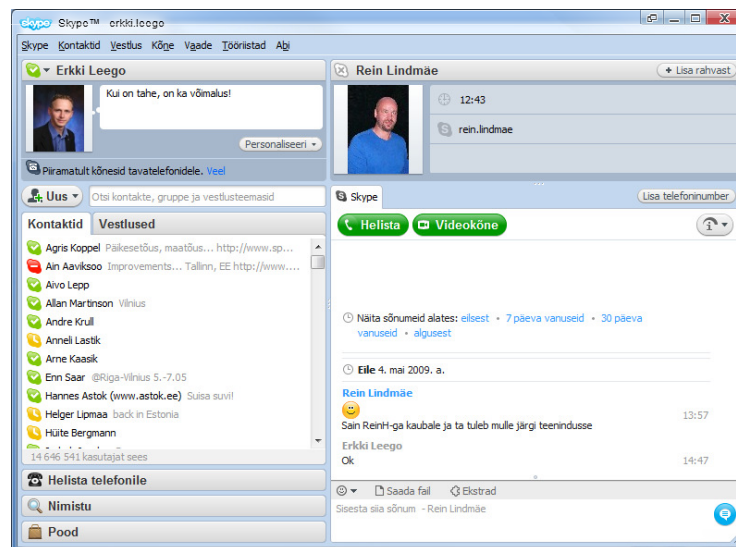
- Teemad millega arvestada
 - Kus e-post füüsiliselt asub – kättesaadavus ja töökindlus
 - Kuidas arhiveerida ja struktureerida
 - Erakirjade ja töökirjade eraldamine
 - Kas saata e-kirjas dokument manusena või viide dokumendi asukohale
 - Identiteet – disain ja struktuur
 - Avalike kataloogide olemasolu ja ülesehitus



Vestlus – Skype, MSN

Kui on tahe, on ka võimalus!

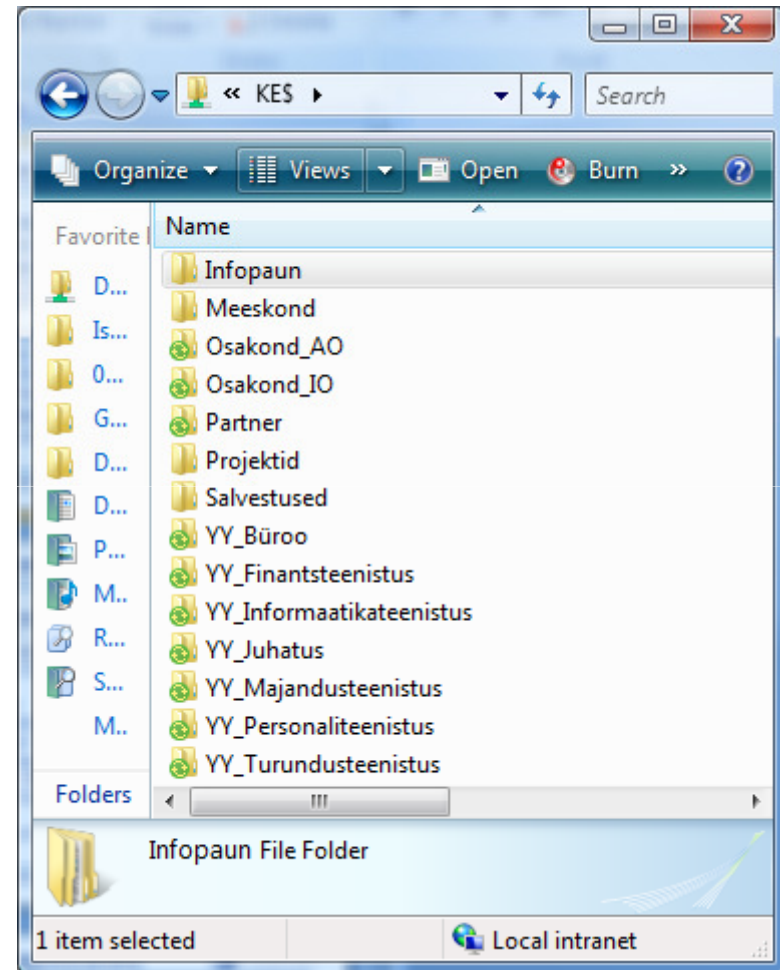
- Teemad millega arvestada
 - Kas on ettevõttes lubatud ja soovitud?
 - Kontode nimed ettevõtte väärilised
 - Kas ja kuidas teisi teavitatakse
 - Kas ja kuidas vestlusi archiveeritakse



Erkki Leego – juhtivpartner

Teemad millega arvestada

- Asukoht
 - E-postkast
 - Arvuti kõvaketas
 - Ettevõtte jagatud ketas
 - Ettevõtte e-kirjade ühiskataloogid
 - Dokumendihaldussüsteem
 - Veeb (koduleht, intranet, ekstranet)
- Struktuur
 - Kuidas määratleda kõigi jaoks loogiline õige koht, kust on võimalik ja osatakse otsida ka aastaid hiljem teiste inimeste poolt?
- Failide edastamine
 - E-kirja manused
 - Välised kandjad (CD, USB pulk, ...)
 - Viide asukohale
- Juurdepääs
 - Kas juurdepääs on võimalik igal ajal igast kohast?



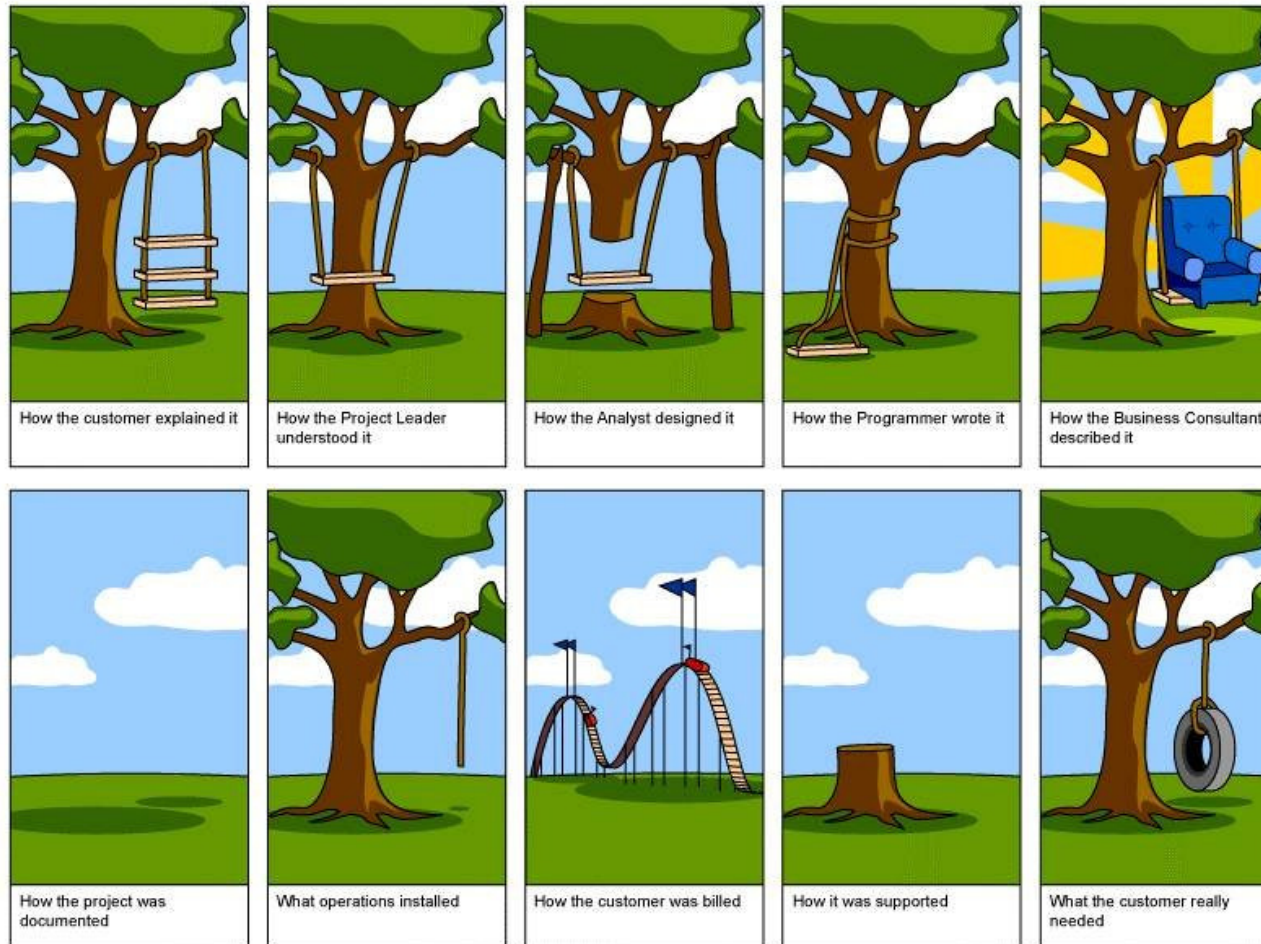
- Oluline metainfo
 - Pealkiri, autor, versioon, aeg, asukoht
- Kirjeldav ja jätkusuutlik failinimi
 - "HLP IT infrastruktuuri kirjeldus 1.0 Leego.docx"
 - "GEEN-K-81 Geenivaramu arhitektuuri visioon (Jaak Vilo) 0.08 Leego.doc"
- Üks "õige" asukoht
 - Peab kehtima eeldus – kui faili selles asukohas ei ole, siis teda ei ole olemas
 - \\domina\Projektid\GEEN\Rakendused\Operatiivbaas
- Juurdepääsuõigused
 - 3 lihttaset– juurdepääs puudub, lugemine, kirjutamine

- Teemad millega arvestada
 - Täiendamine ja kättesaadavus
 - Kas täiendamine jagatud või ühe inimese käes
 - Kas juurde pääseb sisevõrgus või ka kaugelt
 - Asukoht ja vahend
 - Failisüsteem
 - E-post või e-posti avalik kataloog
 - Intranet
 - Wiki, blogid, ...
 - Tavapärased siseinfo ühikud
 - Sündmuste info (nt. sünnipäevad)
 - Ettevõtte pildi- ja videovaramu
 - Ettevõtte esitlusmaterjalide ja taustinfo varamu
 - Infomaterjalid enesetäiendamiseks
 - Turuinformatsioon ja valdkondade taust

- Eripärased rakendused põhitegevuse efektiivseks teostamiseks
 - Tootmise planeerimine, dokumendimenetlus, kliendihaldus, tellimuste haldus, jne.
- HLP näide
 - Mindjet Mindmanager – teabehalduse ja visualiseerimise tarkvara
 - Gyronix – tööde halduse tarkvara Mindmanagerile
 - SysAid – arvutiabi tööde haldustarkvara
- Teemad millega arvestada
 - Kas osta valmistarkvara või arendada ise?
 - Soovitus - üldjuhul otstarbekas soetada valmistarkvara

Arendus keeruline

Kui on tahe, on ka võimalus!



Erkki Leego – juhtivpartner



1. Kerge õppida
2. Efektiivne kasutada
3. Kerge meelde tuletada
4. Vähe vigu
5. Meeldiv kasutada



IT teenuse sisseost



- Tarkvara hooldus ja tugi
 - Standardtarkvara
 - Spetsiaaltarkvara
- Riistvara hooldus ja tugi
 - Tööjaamad, serverid, võrk, printerid jmt.
- Arendus- ja juurutusteenused
 - Erilahenduse väljatöötamine
 - Valmistootte integreerimine ja juurutamine
- Konsultatsiooniteenused
 - IT juht – strateegia, tegevuskava, eelarve
 - Projektijuhtimine ja järelevalve
 - Andmeturbe tagamine
 - Mitmesugused eriprojektid – “mobiilne kontor” jmt.

Oma IT meeskond

- Igapäevane elu
 - Tööjaamade administreerimine
 - Serverite administreerimine
 - Kasutajatoe osutamine
 - Dokumenteerimine
 - Andmeturbe tagamine
 - Juhtkonnapoolne IT meeskonna järelevalve
 - ...
- Areng
 - Strateegiline ja taktikaline planeerimine
 - Süsteemianalüüs
 - Programmeerimine
 - Testimine
 - Projektijuhtimine
 - Hankimine ja järelevalve
 - ...

Sisseostmisel

- Hankimine
- Järelevalve

- Suured IT ettevõtted paljude erinevate teenustega
- Spetsialiseerunud ettevõtted
 - Riist- ja tarkvara müüjad
 - Valmistoodete müüjad ja juurutajad
 - Infosüsteemi töö tagajad
 - Tarkvaraarendajad
 - ...
- Tellija esindajad ja konsultandid
- "Patsiga poiss"



Oma töötaja

- Kuupalk
 - 15 000.- + 4950.- (sotsiaalmaks)
- Kontorikulud
 - Töövahendid (arvuti, tarkvara, pliiatsid jne.)
 - Kontori rent
- Koolitus
 - 25 000.-/tk
- Motiveerimine
 - Preemiad
 - Firmaüritused

Teenuseosutaja

- Nt. 50 arvutiga süsteemi toimimise tagamine
 - 12 000.-/kuus
- Eiprojektid
 - 400 – 2000 kr/tund

- Teenuse sisu, kvaliteet ja tulemus ei vasta ootustele
 - Kokkulepped ja teenuse kvaliteedi määratlused lepingus pealiskaudsed või mõistetakse erinevalt
 - “Fassaadi taga” nõrk spetsialist või vilets töökorraldus
- Liiga tugev sõltuvus teenusepakkujast
 - Teadmused lastakse koguneda ainult teenuseosutaja kätte
 - Sõltuvus võib kaasa tuua hoolimatuse või hinnatõusu
- Teenuseosutaja ei saa aru või ei hooli ettevõtte ärist
 - IT lahendused ja valikud ei toeta piisavalt äristrateegiat
 - Teenuseosutaja ei saa osa ettevõtte igapäevaelust ja aktiivsus piiritletud rangelt oma teenusega



- Saab keskenduda põhitegevusele
 - Ei ole vaja tegeleda keerulise tugiteenuse arendamisega
- Parim kompetents ja kogemus tunnikaupa
 - IT tööjõuturul tihe konkurents
 - Vaja on palju erinevaid kompetentse, mida ühes inimeses (meeskonnas) ei ole
 - Spetsialiseerunud ettevõtte kvaliteet kasvab läbi paljude klientide ja projektide
- Vastutus selgepiiriline
 - Tasu siis kui töö kvaliteetselt tehtud
- Kulude kokkuhoid
 - Sisseostetava teenuse kulud on tavaliselt väiksemad

- Ettevõtte peab suutma olla oma infosüsteemi **omanik**
- Tööjaamade ja lisaseadmete loend;
- Kasutajate loend;
- Tarkvara loend;
- Serverite loend;
- Võrguseadmete loend;
- Teenuste loend;
- Hooldus- ning arenduspartnerid ja nende vastutusalad;
- Infosüsteemi hoolduseks teostatud tööde fikseerimine.



Andmekaitse

100% turvalisust ei ole olemas



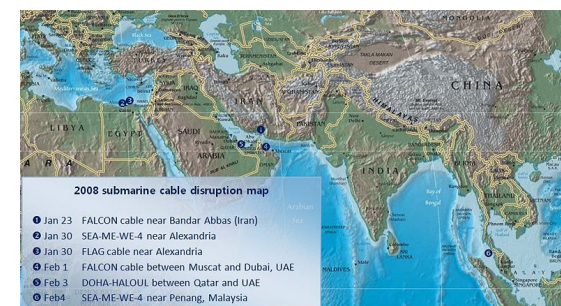
HANSSON, LEEGO
& PARTNER

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



1. Konfidentsiaalsus

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

2. Terviklus

- Andmete päritolu autentsus ning volitamata 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 - teabel on tõestusväärtsus.</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>

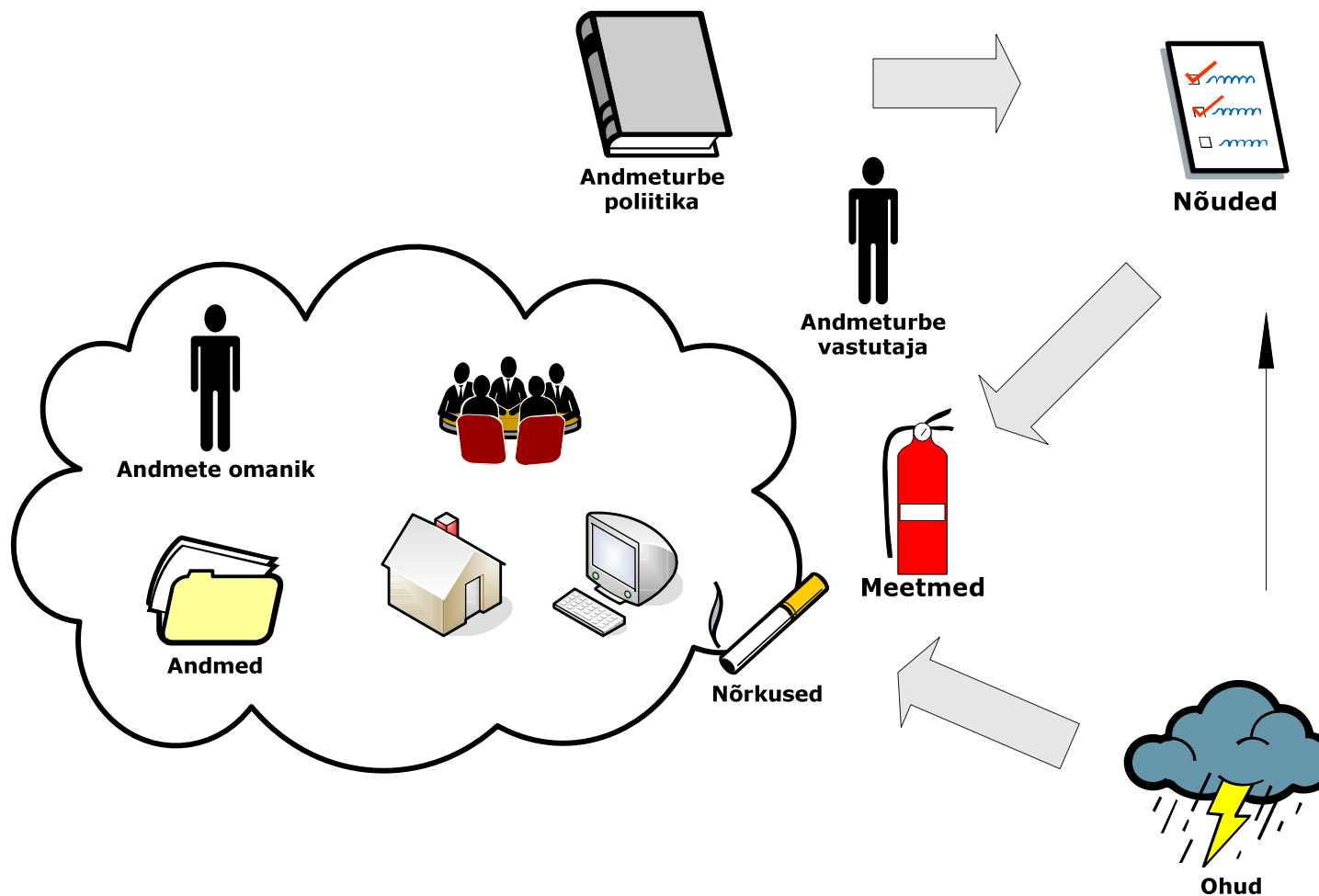
Allikas: VV määrus nr. 273 „Infosüsteemide turvameetmete süsteemi kehtestamine”

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 rikenemine
- Ekspluatatsioonipersonali eksitus
- Hoolduseksitus
- Tarkvara tõrge
- Tarkvara kasutamine volitamatute 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

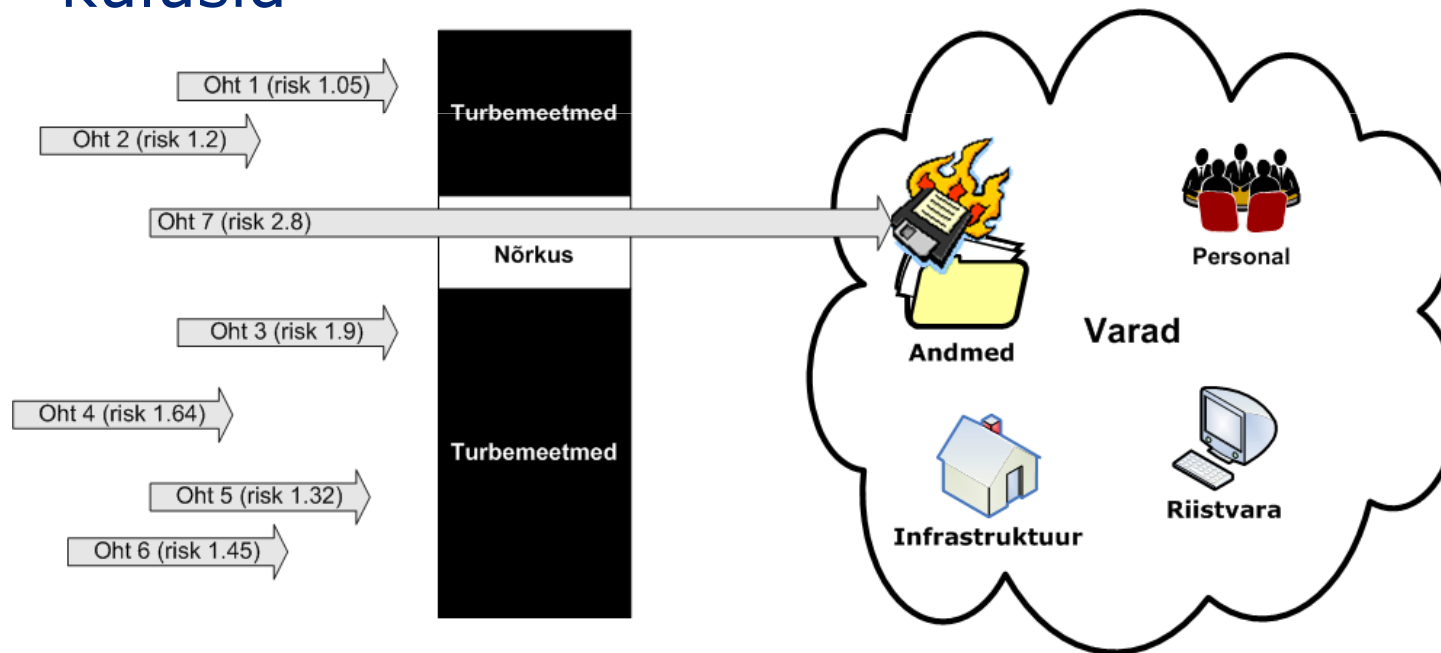
- Keskkond ja infrastruktuur
 - nt. hoonete, uste ja akende füüsilise turbe puudumine
- Riistvara
 - nt. tundlikkus pinge kõikumiste suhtes
- Tarkvara
 - nt. pääsuõiguste väär jaotamine
- Side
 - nt. kaitsmata sideliinid
- Dokumendid
 - nt. hooletus kõrvaldamisel
- Personal
 - nt. puudulikud töölevõtmise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

- Turvameetmed otstarbe järgi:
 - ennetavad, 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



- 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?

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



- Talitluspidevusplaan 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



- 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

- Andmed on tänapäeva ettevõttes suur väärtus
- Teabehalduse võtmeküsimus on jätkusuutlikus andmete säilimise ja ülesleidmise tähenduses
- Kaasa IT juhtimises, hoolduses ja arenduses kompetentseid partnereid
- Andmekaitse algab omanikutundest ja vastutusest
- Lihtsate vahenditega on võimalik teabehalduse kvaliteeti oluliselt tõsta

Aitäh!



Kui on tahe, on ka võimalus!

Kui on tahe, on ka võimalus!

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

Erkki Leego – juhtivpartner