

INFOTURBE TULEVIKUST

ÜLO JAAKSOO

Cybernetica AS juhatuse esimees

Arengufondi seminar

11.12.2008

Juttu tuleb...

- ▶▶ IKT trendid
- ▶▶ Tehnoloogia on muutunud, inimloomus mitte
- ▶▶ Turvaökonomikast
- ▶▶ Neli ohtu ja võimalust
- ▶▶ Kokkuvõte

IKT areng

- ▶▶ 1960 – suurarvutid, arvutuskeskused
- ▶▶ 1970 – miniarvutid
- ▶▶ 1980 – personaalarvutid, Ethernet, Internet
- ▶▶ 1990 – veebiteenused, tulemüürid, VPN-id
- ▶▶ 2000 – GRID, traadita andmeside,..

- ▶▶ **Moore'i seadus:** *arvutusvõimsus kahekordistud iga 18 kuu järel*

10 a jooksul, st aastaks 2018 suureneb arvutusvõimsus
 $2^{\text{astmel}(120/18)}=101,1$ so praktiliselt sada korda. Mis me selle
100X suurema võimsusega peale hakkame?

Ehitame mobiilseid vidinaid

- ▶▶ Telefoni ja PDA ristsugutisest arendatakse mobiilsed seadmed, mis ühendava inimesi, meediumi ja füüsilist keskkonda (GPS)
- ▶▶ Nokia N97 mälu on 32GB (300 m raamatuid riulil). 10 a pärast on seadme mälumaht 3,2TB (Kongressi raamatukogu trükiste maht on 10TB)
- ▶▶ Hulga sensoreid. Info semantiline analüüs
- ▶▶ Mobiilsest seadmest kujuneb inimese loomulik osa, mille ta ei oskagi elada. Näiteks lokaliseerimisteenuse puudumisel ei oska linnas liigelda
- ▶▶ Oluliseks probleemiks kujuneb info turvalisus ja isiku privaatsuse kaitse

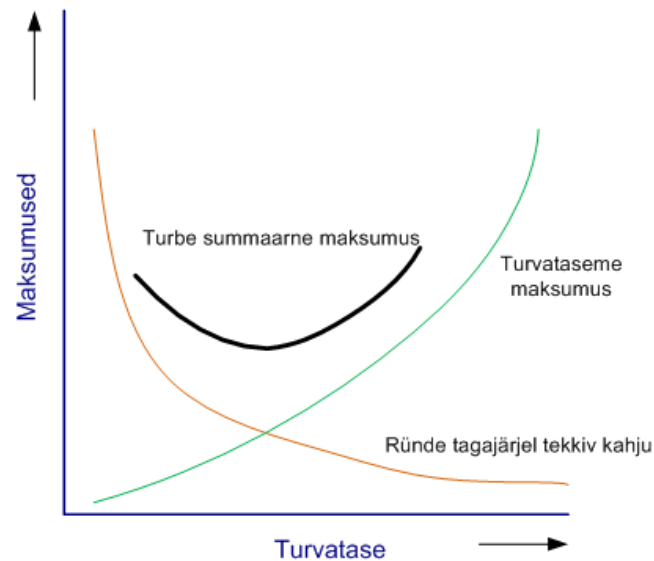
Inimloomus ei ole muutunud

- ▶ Ainuke, mis meie muutavas maailmas on konstantne on inimloomus. Inimesed valetavad, varastavad ja petavad samamoodi kui nad tegid tuhat aastat tagasi. Kuna suur osa elust on kolinud küberruumi, siis kõik need pahad teod toimuvad ka seal. Midagi uut ei ole ju tegelikult välja mõeldud, ainult aktsendid on teise kohta nihkunud
- ▶ Ettevõtte töötajad kujutavad suuremat ohtu, kui ründed väljast. Organisatsiooni perimeetrit oskame mingil määral kaitsta (tulemüürid jm), kuidas aga kaitsta omade eest?
- ▶ Traditsioonilised turvameetmed: süsteemi arhitektuurilised nipid, autentimine, sh biomeetriline, krüpteerimine, sissetungija tuvastamine jt arenevad järgmise 10 a jooksul edasi

Turvameetrika

- ▶▶ Turvalisus on alati kompromiss, mis on tasakaalustatud maksumusega. Vähesed meist kõnnivad ringi kuulivest seljas. Mitte sellepärast, et see oleks ebaefektiivne, vaid ta on ebamugav ja ei tasu ära
- ▶▶ Turvalisus on millegi üle kauplemine ja kauplemine on lihtsam kui see toimub numbrite keeles
- ▶▶ Turvalisust tuleb mõõta. Mõõta, see tähendab teada. Otsustamise aluseks on mõõtetulemused.
- ▶▶ Kas süsteem on turvalisem kui aasta tagasi? Kui suur on minu süsteemi turvalisus võrreldes partneriga? Kas ma kulutan paraja hulga raha turvalisuse saavutamiseks?
- ▶▶ Need on küsimused, mis vajavad vastust nüüd ja tulevikus. Praegu rakendatavast parimast praktikast jääb väheks.

Turvaökonomika



Turvaseme maksumus

- Turvapoliitika juurutamise maksumus
- Kasutaja autentimise konfigureerimise maksumus
- Backupfailide konfigureerimise maksumus
- Võrguliikluse jälgimise maksumus
- Kasutaja käitumise monitooringu maksumus
-

Ründe tagajärjel tekkiv kahju

- Sissetungimise vastumeetmete kulud
- Intellektuaalse omandi kaoga seotud kulud
- Käideldavuse piirangust tekkiv kahju
- Kliendiinfo lekkimisest tekkiv kahju
-

Neli ohtu ja võimalust

- ▶ **Internet kukub kokku.** 35 aastat tagasi usaldasid arendajad üksteist ja arvutid ei olnud eriti töökindlad. Nüüd kui me kasutame peaaegu samu protokolle, on olukord peapeale pööratud. Me usaldame arvuteid, kuid ei usalda inimesi. Protokollide täiustamine
- ▶ **Ülemaailmne infokriis**, analoogne praegusele finantskriisile. Kes valdab infot, selle käes on võim. 95% meililiiklusest on spämm, on olemas tõhusad isiku profiili koostamise vahendid jms. Arvutid tõmmatakse võrgust välja. Otsene negatiivne mõju reaalmajandusele. Ei tea, mida teha
- ▶ **Elektrondokumentide hävimine.** Puudub archiveerimise poliitika ja vahendid. Säilitamine tähenda kopeerimist, mis tagab andmete käideldavuse, tervikluse ja konfidentsiaalsuse. Ärimudeli loomise võimalus olemas
- ▶ **Puudub turvaökonomika.** Ei osta määrata turvameetmete rakendamise tulemusel ärahoitavat võimalikku kahju. Ärimudeli koostamise võimalus olemas

Kokkuvõte

- ▶▶ Tehnoloogia areng viib meie elu piirideta küberruumi. See on paratamatus
- ▶▶ Petmine, valetamine, varastamine toimub ka küberruumis
- ▶▶ Talutavate elutingimuste saavutamiseks tuleb kuritegevusega võidelda. Selleks on vaja ressursse
- ▶▶ Turvaökonomika, sh infovarade hindamine on järgmise 10 a tipp-prioriteetne valdkond, mis suunab meid ratsionaalsele ressursikasutusele
- ▶▶ Elektrondokumentide turvaline arhiveerimine on möödapääsmatu

Eile – turvaperimeeter olema



Egeskov Slot, Denmark (1554)

Täna – turvaperimeeter puudub

