4. Andmeturve

2005

Kava

3.1. Andmeturbest rakenduste vaatevinklist
3.2. Andmeturbe põhimõisted
3.3. Infoturvaja käsulaud *(mitte väga tõsiselt)*
3.4. Infoturvapoliitika
3.5. ISO 17799
3.6. Example:
Personnel Security Management Audit

2

4.1. Andmeturbest rakenduste vaatevinklist

Probleemist

- Eri kodanikud näevad andmeturbes eri asju:
  - tavakodanik - viirused, mõttetud reeglid, veateated
  - admin - lõputu tüütu paikamine
  - võrguehitajad - kulud tulemüüridele
- Andmeturve RAKENDUSTE vaatevinklist:
  - probleemid ja nende põhjused
  - miks tehnika meid ei aita.
  - mis aitab?

4

MORAAL

- Rakenduste turvamine on alateadvustatud teema.
  Sellega tuleb tegeleda, kui teil vähegi midagi kaitsta on.
- Tehnilised *off-the-shelf* vahendid ei aita:
  vaja ka ise **mõelda.**

- *"Security is common sense applied all the time and in all places".*

5

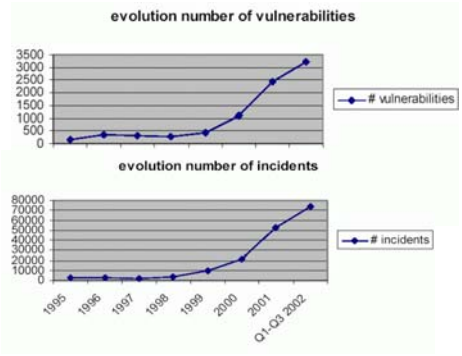
Keskkond muutub

- Väline keskkond läheb järjest hullemaks!
  - viiruselained on igapäevane elu
  - rünnete hulk kasvab
  - tuntud turvavigade hulk kasvab
  - ründevahendid automatiseeruvad ja muutuvad targemaks
  - ründaja *required-knowledge* muutub madalamaks;
    häkkimine on koolilaste hobi (*Script kiddie*)

  - Selle tõestuseks tsiteeritakse numbreid,
    vehitakse (eksponentsiaalsete) graafikutega, ...

6

Hirmutavad graafikud (2003)...



7

Tegelikult on kaks palju hullemat trendi!

– RÜNDAJAD muutuvad

– Rünnatavad RAKENDUSED muutuvad

8

Ründajad muutuvad

- Häkkerid vs kurikaelad
  - Siiani oli enamik ründeid *proof-of-concept* tasemel; organiseerimata, kasusaamise eesmärgita, häkkerlikud.
  - See trend on muutunud! Häkkerid on asunud oma oskusi korralikult müüma.
- Näited
  - Ründed pankade klientide vastu
  - "Tagurpidised" kaardimaksed USA netipankades
  - Hiljutine *Distributed Denial of Service* rünne Hansapanga vastu

9

Ründajad muutuvad

>> Tehnilised ründed on läinud pahatahtlikuks !! <<
>> Häkkerid koopereeruvad tõelise kuritegevusega. <<

- Mida see ***teile*** tähendab?
  - *Script kiddie*'e asemel on turul kodanik, kes teeb teie vastu tellimustööd.
  - Ta eesmärk on varastada ära teie andmed või saada endale teie raha.
  - Tal on aega ***analüüsiks***.
  - Ta ei kasuta standardvahendeid, vaid ***mõtleb***.
  - Ja ta ei ründa su serverit, vaid ***rakendust***.

10

Rakendused muutuvad

- Rakenduste keerukus kasvab.
  - Keerukuse kasv 10x --> vigade kasv 100x .. 1000x:
    rohkem koodi, vähem testimisaega iga haru jaoks,
    rohkem komponentide-vahelisi interaktsioone.
  - Kunagine "*feature*-ism" on asendunud teadliku *"add a feature, change packaging, SELL SELL SELL"* paradigmaga
  - *Know-how per feature* väheneb;
    tundmatud teenused on "igaks juhuks" lahti.

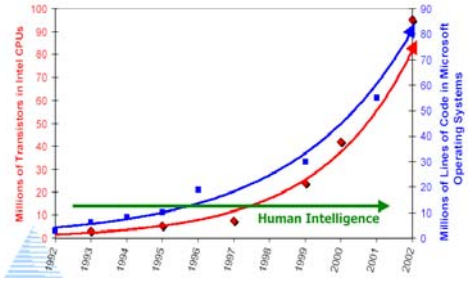
11

Rakenduste piirid kaovad

- Rakenduste avatus suureneb.
  Põhjus - kapitalism.
  - *"Sell first, patch online later"* on turul eluks vajalik.
  - Lisaks on kõik protokollid/teenused ennast osavalt HTTP-ks ümber maskeerinud.
- Läbi lastakse kogu liiklus ning alles rakendus on see, mis peab sikud lammastest eraldama.

12

Rakenduste keerukus



13

Mille vastu me ennast kaitseme?

- Eri sorti ründed tekitavad eri sorti riske.
  - Viirused - töökorralduslik kaos
  - *DoS* - PR-mured
  - Aga rakenduste kaudu toimivad ründed ohustavad otseselt teie andmeid ja raha.
- Mis saab, kui kõik meie teenused lähevad täis-*online*-sse?

14

Tehnika küündimatusest

- Tehnika on nagu uksel olev lukk.
  - Joodiku hoiab see eemal.
  - Aga taga varga vastu ei aita.
    Varas varastab võtme.
    Või läheb aknast.
    Või maskeerub koristajatädiks...
- Sama seis on tehniliste turvavahenditega.
- Olukorras, kus kõik on HTTP (või VOIP), on tulemüür nagu lukk, mille võti on ukse kõrval.

>> Kuidagi tuleb kaitsta ka rakendusi!! <<

15

Tulemused?

- Kas on olemas suurem veebiserver, kus
  - ei ole siseinfot jagavaid veateateid
  - tehakse KÕIKJAL parameetrite lauskontrolli
  - on mõeldud kõigi teiste lihtsate veebi-tasemel rünnete peale
- Asja teeb hullemaks brauseri-vigade segapudru.
- Pea kõik suuremad Eesti veebiteenusepakkujad on (olnud) IMELIHTSATELE rünnetele lahti.
- Rünnetest ei teata, kuna neid ei avastata.

16

4.2. Andmeturbe põhimõisted

Andmeturve ja audiitor

- Üks peamisi valdkondi, mida IS audiitor käsitleb!

18

Organisatsiooni varad

- **füüsilised varad** (nt arvutite riistvara, sideseadmed, hooned)
- **informatsioon ja andmed** (dokumendid, andmebaasid)
- **tarkvara**
- mingi **toote valmistuse** või **teenuse andmise võime**
- **inimesed**
- **ainetud varad** (maineväärtus, imago)

19

Infovarad

- **Infovarade mõiste**
  - andmed, riistvara ja sideliinid, tarkvara ja teenused
  - ja veel: andmekandjad, dokumendid, rajatised, hooned, personal
- **Infovarade väärtus**
  - soetusmaksumus + võimalikud kahjud:
    - varade taastamise kulud
    - tegevuse katkemisega seotud kahjud
    - kahjud konfidentsiaalse teabe lekkimisest
- **Spetsiifilised omadused**
  - portatiivsus
  - võimalus vältida füüsilist kontakti

20

Turvatahud

- **käideldavus**
  - info või teenus peab olema kasutatav
- **terviklus**
  - info peab säilima oma algkujul
- **konfidentsiaalsus**
  - info ei tohi volitamatult levida
- **seaduslikkus ja eetilisus**

21

Turvatahud

- **Käideldavus** (*availability*) tähendab varade takistusteta kättesaadavust volitatud kasutajaile (isikutele või alamsüsteemidele) ja nende teovõimet. Muuhulgas tähendab see, et ka turvasüsteemid ise ei tohi volitatud kasutajaile teha takistusi varade kasutamisel ning nende süsteemide tekitatud ajutised kitsendused peavad olema võimalikult väikesed. Seda aspekti tuleb turvameetmete rakendamisel silmas pidada, leides alati optimaalse kompromissi turvalisuse ja kasutusmugavuse vahel. Näiteks hakkavad kasutajad ülemääraselt rangeid turvaeeskirju lihtsalt ignoreerima, otsima võimalusi liiga aeganõudvatest pääsuprotseduuridest möödahiilimiseks jne.
- **Terviklus** (*integrity*) tähendab, et varasid tohivad modifitseerida ainult volitatud asjaosalised. Selles kontekstis hõlmab modifitseerimine muuhulgas kirjutust, muutmist, oleku muutmist, kustutust ja loomist.
- **Konfidentsiaalsus** (*confidentiality*) tähendab, et arvutisüsteemi varad on kättesaadavad ainult volitatud asjaosalistele. Pääsu tüüp on "lugemislik": lugemine, kuvamine, print või lihtsalt mingi objekti olemasolu teadmine.
- Informatsioon võib oma loomult olla avalik ja üldkättesaadav, kuid on kellegi seaduslik omand. Seda silmas pidades lisavad mõned autorid neljanda põhiatribuudina **seaduslikkuse** ja **eetilisuse**.

22

Turvameetmed

Varad

↓

Ohud

↓

Teenused

↓

Mehhanismid

↓

Turvameetmed

23

Turvapoliitika määratlus

- Infovaradel on rahas mõõdetav väärtus.
- Ohud ähvardavad meie varadest tükki välja võtta.
- **Turvateenused** takistavad ohtude realiseerumist ja/või aitavad vähendada ohtude realiseerumisel saadavat kahju.
- **Turvamehhanismid** realiseerivad turvateenuseid.
- **Turvameetmed** paigutavad mehhanismid organisatsiooni või süsteemi konteksti.
- **Turvapoliitika** on organisatsiooni infoturbetegevuse alusdokument.

24

Ohtude põhitüübid

- hävitamine
- korruptsioon või muutmine
- vargus, kõrvaldamine või kaotsiminek
- informatsiooni paljastamine
- teenuse tõkestamine

25

Ohtude liigitus

- juhuslikud / tahtlikud
- passiivsed / aktiivsed
- sisemised / välised

- rünne: realiseerunud tahtlik oht

26

Ohtude tuvastamine

Ohtude tuvastamine on primaarse tähtsusega infoturbesüsteemi rajamise ja täiustamise juures:

- kui meil puudub info meie konkreetset süsteemi ähvardavatest ohtudest ning selle vastu suunatud rünnetest, siis ei ole meil õrna aimugi sellest, mida kaitsta, kuidas kaitsta ja kui palju ressursse enesekaitsele kulutada.

27

Ohtude tuvastamine

Ohtude tuvastamiseks kasutatakse:

- *jälgimis-*,
- *logimis-* ja
- *hoiatamismehhanisme*.

28

Infosüsteemi jälgimine

Jälgimisel vaadeldakse süsteemi mingite komponentide olekuid, analüüsitakse neid ning tehakse mingeid järeldusi

- nt: oht tuvastatud: kas hoiatada või logida?
- Eriti ohtlikest sündmustest võidakse süsteemiadministraatorit või turvamehi viivitamatult hoiatada;
- Põhjalikuma analüüsi tarbeks salvestatakse (logitakse) vähemohtlike (või ka ohutute) sündmuste toimumise aegrida.

29

Ohtude tõkestamine

Ohtude tõkestamise peamised mehhanismid on:

- **pääsu reguleerimine** ja
- **krüptotehnika**
  - mida kasutatakse ennekõike infovarade peamiste turvatahkude kaitsmiseks.

30

Pääsukontrolli mehhanism

• Pääsupoliitika realiseerub pääsukontrolli mehhanismi abil. ISO1989 (*ISO Access Control Framework*) eristab:

–pääsukontrolli jõustamise mehhanismi (AEF, *Access Control Enforcement Facility*) ja

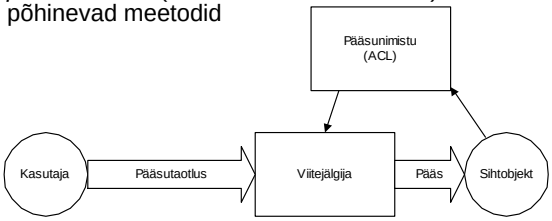
–pääsuoloa andmise mehhanismi (ADF, *Access Control Decision Facility*).

•Kui ADF otsustab, et pääs on lubatud, siis AEF suunab päringu objektini, vastasel korral kehtestatakse eriolukord

31

Pääsunimistud (ACL)

•Pääsukontrolli realiseerimisel on ühtedeks levinumateks meetoditeks *pääsunimistul* (*Access Control List,* ACL) põhinevad meetodid



32

Rollipõhised pääsupoliitikad

• Roll vastab ametile või ametis sisalduvale tööfunktsioonile

–Näiteks võib professoril olla järgmised rollid: lektor, teadur, nõustaja, õpetatud nõukogu liige, väitekirjade kaitsmiskomisjoni esimees jne.

• Õigused antakse rollile, mitte isikule

• Rollile antakse vaid need õigused, mis on tarvilikud rolli ülesannete täitmiseks

• Rollid võivad moodustada hierarhilise süsteemi, milles on määratav pärilikkuse suhe – detailsemalt määratletud roll pärib ülemrolli õigused

–Näiteks matemaatika lektor saab pärimise teel kõik lektori õigused.

33

Pääsuõiguste haldamine - praktika

• Praktikas annab pääsuõigused infovarade valdaja vastavalt *taotleja ülemuse (nt osakonna juhataja) pöördumisele*.

• Oluline on pääsuõiguste regulaarne ülevaatamine – töötaja funktsioonid võivad muutuda, ta võib firmast üldse lahkuda.

– Pole haruldane, et pääsuõigused oluliste infovaradele on firmast ammu lahkunud kodanikel

34

Näide: tarkvaraarendajate pääsuõigused operatiivsüsteemis

• On oluline sätestada tarkvaraarendajatele ajutiste pääsuõiguste omistamine/nende äravõtmine firma operatiivsüsteemis (*live system*)

–Ühelt poolt nõuab *kohustuste lahususe printsiip*, et arendajatel poleks üldse pääsuõigusi operatiivsüsteemis

–Teisalt on vaid arendajatel kompetents operatiivsüsteemi avariide likvideerimiseks – seega avariiolukorras tuleb arendajatele need õigused anda

• On aga vajalik, et sel juhul oleksid arendajate tegevused rangelt kontrollitavad ja oleks tagatud nende õiguste automaatne äravõtt avariiolukorra likvideerimise lõppedes.

35

Krüpteerimine

- **Krüpteerimine** on andmete teisendamine volitamata kasutaja jaoks loetamatusse vormi, mille lugemine on võimalik vaid salajase võtme abil.
- Krüpteerimine kui vahend on esile kerkinud seoses vajadusega anda informatsiooni digitaalsetele esitusvormidele samasugused omadused, nagu seda on allkirjastatud ja salastatud paberdokumentidel.
  - Viimaseid on raske kopeerida ja võltsida, mida aga ei saa öelda näiteks andmefailide kohta.
  - Tänapäevaseid vahendeid õigesti kasutades on võimalik digitaalseid dokumente muuta palju kindlamateks kui seda on paberdokumendid.

36

Krüptosüsteemid

- **Sümmeetriliste krüptosüsteemide** puhul kasutatakse šifreerimiseks ja dešifreerimiseks ühtainsat võtit, mida tuleb turvalisuse tagamiseks hoida salajas, aeg-ajalt vahetada ning mille edastamiseks võib kasutada ainult turvalisi kanaleid. Sümmeetriliste krüptoalgoritmide peamine eelis on nende kiirus; neid kasutatakse edastatavate andmete šifreerimiseks.
- **Asümmeetriliste krüptosüsteemide** (avaliku võtmega süsteemide puhul) kasutatakse šifreerimiseks ühte võtit ja dešifreerimiseks teist. Igal süsteemis osaleval subjektil on kaks võtit - salajane, mida ta kasutab teistele saadetavate sõnumite signeerimiseks, ning avalik, mida teised kasutavad talle saadetavate sõnumite krüpteerimiseks. Avaliku võtmega krüptograafiat kasutatakse ka poolte autentimiseks.
- **Räsifunktsioone** kasutatakse sõnumilühendite loomiseks. Nende sisend on suvalise pikkusega sõnum, millest luuakse kindla pikkusega krüptograafiline lühend. Tugeva räsifunktsiooni puhul on kahe erineva sõnumi jaoks sama lühendi saamise tõenäosus väga väike; samuti ei ole lühendit teades võimalik tuletada esialgset sõnumit. Neid funktsioone kasutatakse andmete tervikluse tagamiseks: kui vastuvõetud sõnumist õnnestub arvutada vastuvõetud lühend, siis on alust arvata, et sõnum ei ole sidekanalis riknenud.
- **Taastemehhanisme** kasutatakse realiseerunud ohtude tagajärgede kõrvaldamiseks. Taastemehhanismide hulka kuuluvad nt varundamine, infotöötlussüsteemi kriitiliste sõlmede dubleerimine ja operatsioonide päeviku pidamine.

37

Sisemised ja välised ründed

- **Sisemiste** rünnete korral käituvad süsteemi seaduslikud kasutajad ettenähtust erineval või volitamatul viisil. Enamik tuntud raaliroimadest on põhinenud sisemistel rünnetel, mida ei tõkestanud turvamehhanismid. Sisemiste rünnete osakaaluks hinnatakse koguni 70%; üle poole turvaprobleemidest põhjustab inimfaktor - süsteemi legaalsed kasutajad ja nende eksimused.
- **Väliste** rünnete korral võib ründaja kasutada näiteks (aktiivset või passiivset) salaharundit, kiirguste jälgimist, süsteemi volitatud kasutaja või komponendi teesklemist ning möödahiilimist autentimise või pääsu reguleerimise mehhanismidest.

38

Ründed

- **Identifikaatorite hõivamine** (*identity interception*). Suhtlusprotsessi ühe või mitme osapoole identifikaatorite vaatlemine nende väärkasutuse eesmärgil.
- **Teesklus** (*masquerade*). Ühe kasutaja teesklemine teise poolt, juurdepääsuks informatsioonile või lisaprivileegide saamiseks. Tavaliselt kaasneb sellega mõni muu aktiivse ründe vorm, eriti taasesitus ja sõnumi muutmine.
- **Taasesitus** (*replay*). Sõnumi või selle osa salvestamine ja hilisem kordamine volitamata toime saavutamiseks, nt. autentimisjada kasutamine teeskluseks.
- **Andmete hõivamine** (*data interception*). Volitamata subjekti sooritatav andmete vaatlus.
- **Andmete manipuleerimine** (*data manipulation*). Volitamata subjekti sooritatav andmete asendamine, lisamine, kõrvaldamine või andmete järjestuse muutmine volitamata toime saavutamiseks.

39

Rünnete tüübid

- identifikaatorite hõivamine (*identity interception*)
- teesklus (*masquerade*)
- taasesitus (*replay*)
- andmete hõivamine (*data interception*)
- teenuse tõkestamine (*denial of service*)
- väärmarsruutimine (*misrouting*)
- liikluse analüüs (*traffic analysis*)
- salauks (*trapdoor*)
- Trooja hobune (*Trojan Horse*)

40

Ründed – selgitused (osaliselt)

- **Teenuse tõkestamine** (*denial of service*). Leiab aset siis, kui mingi subjekt ei saa täita oma ülesandeid või käitub nii, et ta takistab teistel subjektidel oma ülesannete täitmist. Rünne võib olla üldine (nt. kõigi sõnumite kõrvaldamisega) või spetsiifiline (nt. teatud sihtkohta suunatud sõnumite kõrvaldamisega). Rünne võib kujutada endast ka sõnumite genereerimist, nt. võrgu ülekoormamise eesmärgil.
- **Väärmarsruutimine** (*misrouting*). Sidetrakti volitamata ümbermarsruutimine. Võib leida aset OSI kihtides 1-3.
- **Liikluse analüüs** (*traffic analysis*). Suhtlusinformatsiooni (nt. andmeliikluse olemasolu või puudumise, sageduse, suuna, järjestuse, tüübi, mahu jne.) volitamata vaatlemine.
- **Salauks** (*trapdoor*). Süsteemi mingi elemendi selline muudatus, mis võimaldab ründajal vastava käsuga või teatava sündmuse (sündmustiku) korral sooritada volitamata toimingu; näiteks parooli kontrolli niisuguse modifitseerimise, mille tulemusena süsteem loeb õigeks ka ründaja parooli.
- **Trooja hobune** (*Trojan Horse*). Süsteemi element, millel on lisaks seaduspärasele funktsioonile ka mingi volitamata funktsioon; näiteks retranslaator, mis ühtlasi kopeerib sõnumeid ka mingisse volitamata kanalisse.

41

Turvateenused

- autentimine
  - partneri autentimine
  - andmeallika autentimine
- pääsu reguleerimine
- konfidentsiaalsuse, tervikluse ja käideldavuse tagamine
- salgamise vääramine
  - vääramine allika tõestusega
  - vääramine saabumise tõestusega

42

Turvateenused – mida me tahame saavutada?

- **Autentimine** tähendab väidetava identiteedi tõendamist.
  - ISO 7498-2 defineerib **andmeallika autentimise** (*data origin authentication*) kui saadud andmete väidetava allika tõendamise ja
  - **partneri autentimise** (*peer-entity authentication*) kui partnersubjekti väidetava identiteedi tõendamise mingis andmevahetusühenduses.
- ISO 7498-2 järgi on **pääsu reguleerimine** (*access control*) ressurssidele volitamatu juurdepääsu vältimine, kaasa arvatud ressursside volitamatul viisil kasutamise vältimine.
- **Salgamise vääramine**.
  - **Allika tõestusega**: andmete saajale antakse tõestus andmete lähtekoha kohta. See kaitseb saatja katsete eest tõele vastukäivalt eitada andmete või nende sisu saatmist.
  - **Saabumise tõestusega**: andmete saatjale antakse tõestus andmete kättesaamise kohta. See kaitseb saaja katsete eest tõele vastukäivalt eitada andmete või nende sisu kättesaamist.

43

Turvamehhanismid

- ohtude **tuvastamine**
  - jälgimine, logimine, hoiatamine
- ohtude **tõkestamine**
  - pääsu reguleerimine
  - krüptotehnika
    - sümmeetrilised (salajase võtmega)
      - › šifreerimine
    - asümmeetrilised (avaliku võtmega)
      - › autentimine (ja šifreerimine)
    - räsifunktsioonid
      - › sõnumilühendid
- **taaste** (tagajärgede kõrvaldamine)
  - varundamine

44

Turvameetmed

- organisatsioonilised
- füüsilised
- infotehnoloogilised

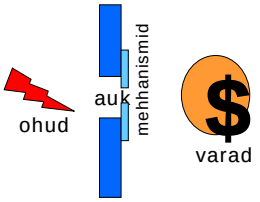
45

Turvameetmed

- **Organisatsioonilised**: Personalile suunatud meetmed. Andmete klassifitseerimine konfidentsiaalsuse (avalik, ametialaseks kasutamiseks / *restricted*, konfidentsiaalne / *confidential*, salajane / *secret*, täiesti salajane / *top secret*), tervikluse (madal, keskmine, kõrge) ja käideldavuse järgi (tähtsusetu, soovitav, kriitiline). Infovarade registrid. Turvameetmete plaanimine ja haldus. Eeskirjad dokumentatsiooni ja andmekandjate kohta.
- **Füüsilised**: Üldnõuded. Infotöötlusüksuse asukoht. Arvutuskeskuse ehituslik osa
- **Infotehnoloogilised**: käideldavuse ja tervikluse tõstmine stiihiliste ohtude tõrjumise teel (UPSid, varundamine, kontrollkoodid, dubleerimine). Konfidentsiaalsuse tagamiseks kiirguslekete vältimine. Lisaks ründetõrjemehhanismid - pääsu reguleerimine, krüptotehnilised meetodid ja autentimine.

46

Turvaauk



Turvamehhanismide lisamine võimaldab auke väiksemaks teha, kuid päris kinni ei õnnestu neid kunagi toppida.

47

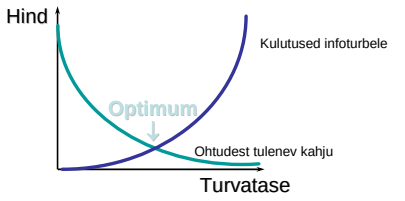
Turvaaugud

- Turvamehhanismide lisamine võimaldab auke väiksemaks teha, kuid päris kinni ei õnnestu neid kunagi toppida.
- Ohud leiavad alati uusi auke.

48

Turvarisk

- varade väärtus × ohtude realiseerumise tõenäosus
- kui palju maksab turbele kulutada?



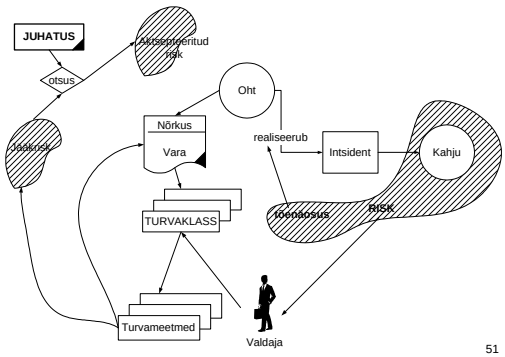
49

Turvarisk

- **Turvarisk** on rahas väljendatav suurus, mis võrdub ohtude realiseerumisel tekkiva kahju ning nende ohtude realiseerumise tõenäosuse korrutisega.
- Riski hindamiseks tuleb kõigepealt hinnata varade väärtus ja määrata kindlaks varasid ähvardavad ohud ning nende realiseerumise tõenäosused.
- Seejärel tuleb määratleda turvaeesmärgid - mida me tahame kaitsta ja kui tugevalt.
- Lõpuks on vaja välja selgitada püstitatud eesmärkide saavutamiseks vajalikud turvameetmed, hinnata nende rakendamisega seotud kulutusi ning vajadusel (kui kulutused infoturbele ületavad ohtude realiseerumisest tuleneva tõenäolise kahju) turvaeesmärke korrigeerida.

50

Turvaprotsess



51

Infoturbe plaanist (1)

• Teha inventuur/täiendada loetelu kõikidest infotehnoloogilistest seadmetest, süsteemidest ja andmebaasidest = infovaradest.
• Tagada, et kõigile turvatavatele infovaradele on määratud omanik/valdaja (formaalselt on firma ise oma infovarade omanik ja delegeerib selle õiguse äripoole sisuliselt seda vara valdavale isikule). Infovara valdaja vastutab vara turvalise käitamise (nt pääsuõiguste haldamine) ja säilitamise (nt varukoopiate tegemine ja säilitamine) eest. Vajalike toimingute teostamise delegeerib valdaja omakorda IT spetsialistidele – kuid mitte vastutust!
• Infovarade haldamise kontroll

52

Infoturbe plaanist (2)

• Uute/modifitseeritud infrastruktuuri komponentide infoturbe analüüs, riskide määratlemine ja vajaduse korral testimine
  –vastavate turvameetmete ja käitusprotseduuride loomine/täiendamine/ modifitseerimine
  –meetmete ja protseduuride täitmise kontroll
• Uute/modifitseeritud rakenduste infoturbe analüüs, riskide määratlemine ja vajaduse korral testimine
  – vastavate turvameetmete ja käitusprotseduuride loomine/täiendamine modifitseerimine
  –meetmete ja protseduuride täitmise kontrol

53

Infoturbe plaanist (3)

• Talitluspidevuse plaanid (kaasaarvatud kriisiolukorra plaanid)
• Infotehnoloogiliste intsidentide registreerimise korraldamine ja kontroll
• Infrastruktuuri ja rakenduste seiresüsteemide arendamine ja seire kontroll
• Infosüsteemide pääsukontrolli täiendamine ja uuendamine
• Infotehnoloogiliste turvapoliitikate loomine/täiendamine/kaasajastamine

54

4.3. Infoturvaja käsulaud

(mitte väga tõsiselt)

Infoturvaja käsulaud (1)

- Ära püüa aru saada süsteemidest, mida sa turvama pead – piisab, kui kasutad oma kogemusi ja intuitsiooni
- Ära krüpteeri andmebaase, eriti neid, mis sisaldavad tundlikke andmeid
- Ära installeeri opsüsteemi (andmebaasihaldesüsteemi jne) korrektsioone („paikasid“) – see on liiga aeganõudev, süsteemi uues versioonis on korrektsioonid niigi sees
- Kui töötaja firmast lahkub, jäta kehtima tema pääsuõigused – ei või iial teada, millal tal miskit vaja võib minna

56

Infoturvaja käsulaud (2)

- Ära koosta turvapoliitikaid, -meetmeid ja -reegleid. Sa tead niigi, mida teha on vaja
- Kui firmal siiski mingi turvapoliitika on, ära selle tähtsust ülehinda. Kuna turvapoliitikat keegi ajakohastanud pole, on see ilmselt vananenud. Printsiipi “tee seda mis kirjas ja pane kirja mis teed” (*“do what you say and say what you do”)* ära võta tõsiselt, ammugi pole mõtet seda toimisjuhiseks pidada
- Püüa infoturve täies ulatuses sisse osta – miks peaks firmas keegi infoturbele aega kulutama ja infoturbe probleemidega pead vaevama. Pealegi ehk saab nii ka vastutuse enda kaelast ära sokutada

57

Infoturvaja käsulaud (3)

- Mitte mingil juhul ära raiska aega infosüsteemide inventuurile ega firma arvutivõrgu dokumenteerimisele
- Anna kõigile töötajatele võimalikult suured õigused kõigis infosüsteemides. Kõik peavad kõigele ligi pääsema – see on demokraatlik ja õiglane, pealegi langeb nii ära ka tülikas pääsuõiguste haldamise probleem
- Tugine ainult tehnoloogiale – tulemüürid, krüpteerimine ja viirusetõrje tarkvara on kõik, mis sa vajad
- Ära raiska aega talitluspidevuse plaanide koostamisele – sa ju ei kaota pead ja oled piisavalt nutikas ka keerulises hädaolukorras
- Pole mõtet kulutada raha seiresüsteemidele – kui midagi juhtub, saab sellest niigi teada

58

Infoturvaja käsulaud (4)

- Häkkerite rünnetega võitlemisel lähtu printsiibist *„probleemidega tegeldakse siis, kui nad esile kerkivad“*
- Parooliks on sobivaimad sinu enda, sinu koera, naise või ämma nimi – on kindel, et nii sa paroole ei unusta. Siiski tuleks parool kindluse mõttes kleepida ka klaviatuuri alla (kollase kleepsuga kuvari külge ei pane paroole enam keegi). Parooliasjanduse lihtsustamiseks võib sama ülesandeid täitvatel töötajatel sama parool olla. Paroole (regulaarselt) uuendada pole vaja, see tekitab ainult segadust. Kõige vähem segadusi tekib, kui valida parooliks “parool”
- Töötajate infoturbe alasel koolitusel ja treeningutel mõtet pole – las igaüks tegeleb parem oma põhitööga

59

4.4. Infoturvapoliitika

(Info)turvapoliitika

- (Info)turvapoliitika on eeskirjade, juhiste ja menetluste kogum, mis suunavad varade, (peamiselt infovarade) haldust, kaitset ja jaotamist organisatsioonis ning ta IT süsteemides
  - Kui jätta eest ära eesliide info- (st turvapoliitika), siis peab infovarade asemel vaatama kõiki varasid

61

Infoturvapoliitika sisaldab

- infoturbe motivatsioon
- nõutav turvatase
- vastutus
- infoturbe alane töökorraldus

62

Miks on vaja infoturvapoliitikat?

- Peapõhjus – enamike (info)varade (eriti andmete) kaitse eeldab süstemaatilist tegevust kogu sellega seotud organisatsioonis, mis arvestab erinevate elualade spetsiifikaid ja nõudeid
- Infoturvepoliitika ei ole mitte IT spetsialistide pärusmaa, vaid reeglina suure hulga erinevate elualade spetsialistide turbefoorumi koostöö tulem

63

Tippjuhtkonna roll

- Vaid tippjuhtkond teab, kuivõrd tähtis osakaal on organisatsiooni tegevuses erinevate varade erinevate omadustel ning kui olulist kahju võib nende kadumine kogu organisatsioonile tekitada
- Seepärast peab just juhtkond olema see, kes paneb paika, millisel tasemel on erinevate (info)varade erinevaid omadusi on vaja kaitsta. Konkreetsed suunised pannakse aga kokku erinevate alade spetsialistide poolt

64

Infoturvapoliitika tuleks ...

koostada järgmiste talitluste esindajate osavõtul:

- tippjuhtkond
- audit
- rahandus
- infosüsteemid (spetsialistid ja kasutajad)
- tehnovõrgud ja infrastruktuur (st hoone ehitusliku osa eest vastutajad)
- personalitalitlus
- üleüldine turve

65

Turvapoliitika elemendid

- Peab sätestama kõikide varade (omaduste) jaoks üldeesmärgid, kusjuures vajalik on kooskõla
- Selgelt peavad olema määratletud seos IT poliitikaga ja turunduspoliitikaga
- Peavad olema määratud teed (viisid), kuidas turvaülesanne erinevates valdkondades lahendatakse (riskianalüüs, etalonturbe metoodika)
- Selgelt peab paika olema pandud vastutus ja kohustused

66

Turvapoliitika tüüpsisu (1)

1. Sissejuhatus
   - ülevaade
   - turvapoliitika rakendusala ja eesmärk
2. Turvaeesmärgid ja -põhimõtted
   - eesmärgid
   - põhimõtted
3. Turbe organisatsioon ja infrastruktuur
   - kohustused
   - (konkreetsete alamsüsteemide) turvapoliitikad
   - turvaintsidentidest teatamine

67

Turvapoliitika tüüpsisu (2)

4. Infoturbe ja riskianalüüsi strateegia
   - sissejuhatus
   - riskianalüüs ja riskihaldus
   - turbe vastavuse kontroll
5. Informatsiooni tundlikkus ja riskid
   - sissejuhatus
   - informatsiooni märgistuse süsteem
   - ülevaade organisatsiooni informatsioonist
   - informatsiooni väärtus ja tundlikkustasemed
   - ülevaade ohtudest, nõrkustest ja riskidest

68

Turvapoliitika tüüpsisu (3)

6. Riistvara ja tarkvara turve
   - identimine ja autentimine
   - pääsu reguleerimine
   - arvestus ja revisjonipäevik
   - täielik kustutus, ründetarkvara
   - personaal- ja sülearvutite turve
7. Side turve
   - võrkude infrastruktuur
   - Internet
   - side krüpteerimine ja autentimine

69

Turvapoliitika tüüpsisu (4)

8.Füüsiline turve
- hoone turvalisus ja kaitse, sh teenuste kaitse
- volitamata hõive
- juurdepääs arvutitele
- juurdepääs andmekandjatele
- personali kaitse
- piksekaitse, kahjutule ja vee kaitse
- ohtude avastamine ja teatamine
- seadmete kaitse varguse eest
- teeninduse ja hoolduse reguleerimine

70

Turvapoliitika tüüpsisu (5)

9. Personali turve
- palkamistingimused
- turvateadlikkus ja -koolitus
- personal ja lepingulised töötajad
- kolmandad osapooled

10. Dokumentide ja andmekandjate turve
- säilitamine
- edastamine
- kõrvaldamine (hävitamine)

71

Turvapoliitika tüüpsisu (6)

11.Tegevus eriolukordades
- varundamine, sh varukoopiad
- eriolukordade strateegia
- olulisemate eriolukordade plaanid

12. Kaugtöö

13. Alltöövõtu poliitika

14. Muudatuste reguleerimine
- turvapoliitika muutmispõhimõtted
- turvapoliitika staatus organisatsioonis

72

Turvapoliitika tüüpsisu (7)

Lisad:

A. Turvajuhendite loend

B. Seadused ja eeskirjad

C. Organisatsiooni infoturbe eest vastutava isiku pädevus

D. Infoturbe foorumi pädevus

E. Oluliste alamsüsteemide (komponentide) turvapoliitika sisukord

73

Alusmaterjal

- Eesti rahvuslik turbehalduse standard
- EVS ISO/IEC 13335 osad 1 kuni 4 (üle võetud tõlkemeetodil ISO standardist):
  - Osa 1: mõisted ja mudelid
  - Osa 2: turbehaldus ja plaanimine
  - Osa 3: turbehalduse meetodid
  - Osa 4: turvameetmete valimine

74

4.5. ISO 17799

BS 7799

- Provides guidelines and recommendations for security management.
- Part 1 - S tandard
- Part 2 - Certification

76

ISO 17799

- ... accepted as International Standard (2002)

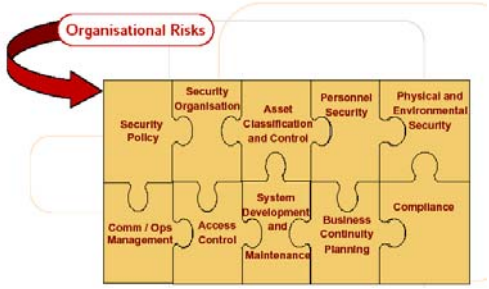
77

The Standard: What Is It?

- “A comprehensive set of controls comprising best practices in information security”
- Comprises TWO parts - a code of practice (ISO17799) and a specification for an information security management system (BS7799-2)
- Basically… an internationally recognised generic information security standard

78

ISO 17799 Modules



79

ISO 17799

1. Business Continuity Planning
2. Access Control
3. System Development and Maintenance
4. Physical and Environmental Security
5. Compliance
6. Personnel Security
7. Security Organisation
8. Comm / Ops Management
9. Asset Classification and Control
10. Security Policy

80

ISO 17799 Objectives

1. Business Continuity Planning

The objectives of this section are:

- To counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.

82

2. Access Control

The objectives of this section are:

1) To control access to information
2) To prevent unauthorised access to information systems
3) To ensure the protection of networked services
4) To prevent unauthorized computer access
5) To detect unauthorised activities.
6) To ensure information security when using mobile computing and tele-networking facilities

83

3. System Development and Maintenance

The objectives of this section are:

1) To ensure security is built into operational systems;
2) To prevent loss, modification or misuse of user data in application systems;
3) To protect the confidentiality, authenticity and integrity of information;
4) To ensure IT projects and support activities are conducted in a secure manner;
5) To maintain the security of application system software and data.

84

4. Physical and Environmental Security

The objectives of this section are:

1) To prevent unauthorised access, damage and interference to business premises and information;
2) To prevent loss, damage or compromise of assets and interruption to business activities;
3) To prevent compromise or theft of information and information processing facilities.

85

5. Compliance

The objectives of this section are:

1) To avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements
2) To ensure compliance of systems with organizational security policies and standards
3) To maximize the effectiveness of and to minimize interference to/from the system audit process.

86

6. Personnel Security

The objectives of this section are:

1) To reduce risks of human error, theft, fraud or misuse of facilities;
2) To ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work;
3) To minimise the damage from security incidents and malfunctions and learn from such incidents.

87

7. Security Organisation

The objectives of this section are:

1) To manage information security within the Company;
2) To maintain the security of organizational information processing facilities and information assets accessed by third parties.
3) To maintain the security of information when the responsibility for information processing has been outsourced to another organization.

88

8. Comm / Ops Management

The objectives of this section are:

1) To ensure the correct and secure operation of information processing facilities;
2) To minimise the risk of systems failures;
3) To protect the integrity of software and information;
4) To maintain the integrity and availability of information processing and communication;
5) To ensure the safeguarding of information in networks and the protection of the supporting infrastructure;
6) To prevent damage to assets and interruptions to business activities;
7) To prevent loss, modification or misuse of information exchanged between organizations.

89

9. Asset Classification and Control

The objectives of this section are:

- To maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.

90

10. Security Policy

The objectives of this section are:

- To provide management direction and support for information security.

91

10. Security Policy

- Documented & communicate IS policy
- Regularly reviewed

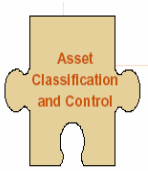
92

7. Security Organisation

- Allocation of roles & responsibilities
- 3rd-party access risks/controls
- Outsourcing

93

9. Asset Classification and Control



- Inventory of Assets
- Clas s ification based on sensitivity/business impact

94

6. Personnel Security

- Recruitment s creening
- Awarenes s & training
- Reporting of incidents

95

4. Physical and Environmental Security

- Phys ical s ecurity perimeters
- Equipment siting
- Clear desk & clear screen

96

8. Comm / Ops Management

- Incident procedures
- Segregation of duties
- System planning & acceptance
- Malicious software protection
- E -mail controls

97

2. Access Control

- Managing Access
  - Application Level
  - Operating Level
  - Network Level

98

3. System Development and Maintenance

- Change control procedures
- Segregation of environments
- Security requirements

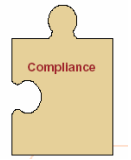
99

1. Business Continuity Planning

- Business continuity plans
- BCP framework and team roles & responsibilities
- Testing continuity plans
- Maintaining and updating continuity plans

100

5. Compliance



- Copyright controls
- Retention of records and information
- Compliance with legislation - Data protection
- Compliance with company policy

101