Vello Hanson, Märt Laur, Monika Oit, Kristjan Alliksoo

INFOSÜSTEEMIDE TURVE
I
TURVARISK

TEINE, UUENDATUD JA TÄIENDATUD TRÜKK

CYBERNETICA AS
TALLINN 2009

Infosüsteemide turve:

I Turvarisk

(1997 Vello Hanson; 2009 Vello Hanson, Märt Laur, Kristjan Alliksoo, Monika Oit)

II Turbe tehnoloogia

(1998 Vello Hanson, Ahto Buldas, Helger Lipmaa)

Korrektuur: Imbi Nõgisto

Kaas: Andres Abe

Täname: Mari Seeba ja Meelis Roos, kelle sisukad kommentaarid aitasid raamatu valmimisele kaasa.

Teise trüki saateks

Alustades 1990ndate keskpaigas infosüsteemide turvet käsitleva raamatu kokkupanekut, arvasime, et käsikäes infotehnoloogia kiire arenguga läheb kasutajatel vaja ka süstemaatilisi teadmisi infoturbest. Tegelikult kulus veel aastaid, enne kui selleks tekkis reaalne vajadus, kuid ajendas seda siis ühiskondlik initsiatiiv või midagi muud, oli see tungiv. Raamatu esimene trükk kadus lettidelt, aga nõudlus selle järele kasvas.

Esmatrüki koostamise ajal oli infoturbevaldkond veel uudne, mistõttu nappis ka infoallikaid; lähtematerjalina tuli kasutada alles arenemisjärgus standardeid ja metoodikaid. Viimasel aastakümnel on valdkond aga hoogsalt arenenud ning võimalused saada ajakohast informatsiooni oluliselt avardunud. Täna võib Eestist leida mitmeid infoturbealase teadmuse allikaid nagu eestikeelsed infoturbehalduse standardid (Standardikeskus), isikuandmete kaitse meetmed (Andmekaitse Inspektsioon) ning ülevaade riigi- ja kohalike omavalitsuse asutustele mõeldud kolmeastmelisest etalonturbe süsteemist koos praktiliste rakendusnäidetega (Riigi Infosüsteemide Arenduskeskus). Koduarvuti turvalisuse osas annavad teavet suuremad pangad ja projekti "Vaata Maailma" andmekaitseprogramm; teavituskampaaniatega on liitunud ka CERT Eesti. Infoturve on ka küberkaitse põhiline komponent.

Tänu sellele on teadlikkus hakanud küll kasvama, aga nii mõnigi kord saavutatakse see raaliroima ohvriks langemise hinnaga. Kui 1996. aastal võis end tunda suhteliselt kaitstuna (peamiseks nakkusallikaks oli diskett), siis tänapäeval, kus asutused ja ettevõtted on ühendatud nii Internetiga kui ka omavahel, saab kahjurvara levida ennenägematu kiirusega ja ulatuses (nt uss Slammer nakatas esimese 10 minutiga 75 000 serverit). Äri kolimine Internetti on avanud tee uutele ründeviisidele ning eriliigilisi ründeid rakendatakse mitmesugustes kombinatsioonides raaliroimarite majanduslikesse huvidesse. Seda arvestades pöörasimegi kõige rohkem tähelepanu peatükile „Ohud" – täiesti uued on jaotised, mis käsitlevad rämpsposti, robotivõrke ning mobiilside- ja ummistusründeid; põhjalikult uuenenud on andmed viiruste jm kahjurvara kohta. Kõikjal raamatus uuendasime ja täiendasime ka statistikat, kuigi pärast kaksiktornide langemist USAs on organisatsioonid muutunud ründeid puudutava teabe avaldamisega väga ettevaatlikuks.

Üks suuremaid teise trüki väärtusi on uuenenud tõlkesõnastik, mida täiendasime veerandtuhande terminiga riskide, auditeerimise, turvatehnika, ohtude ja rünnete

osas. Enamik termineid on varustatud värskete standardiviidetega, mille järgi on võimalik leida määratlus või saada rohkem teavet teema kohta.

Loodame, et värskendatud ülevaade turvariskist ja süsteemne pilt infoturbe korraldusest annab täiendava panuse lugejate turvateadmuse kasvu ning et nagu esmatrükk, nii on ka teine trükk loetav kas või kümme aastat pärast väljaandmist.

Sissejuhatus

Koos iseseisvuse taassünniga jõudis Eestisse ka infotehnoloogiline ärkamisaeg. Ligi kahekümne aastaga oleme jõudnud selleni, et Interneti-teenuseid kasutavad sajad tuhanded inimesed ning arvutisüsteemid on meie tööelus saanud kriitilise kaalu. Niisugune sõltuvus on muutnud aktuaalseks arvutisüsteemide töökindluse ja turvalisuse probleemid, mis on eriti pakilised, kuna võrdselt tehnilise progressiga on arenenud ka selle varjupool: kahjurvara, andmekaod, sissetungid võrgust, tarkvarapiraatlus ja muud informatsioonist sõltuva ühiskonna normaalset talitlust häirivad ilmingud.

Kõikjale tunginud Internet on aken maailma mitte ainult teadmishimulisele Lõuna-Eesti koolipoisile või Hiiumaa külaelanikule, vaid ka pahatahtlike kavatsustega arvutihuvilistele. Võrgust leitavad vahendid lubavad isegi kasinate tehniliste teadmistega tekitada infosüsteemides tõsiseid kahjustusi. Kui 1990ndate alguses seisnesid raaliroimad siinmail peamiselt arvutivargustes, siis juba mõni aasta hiljem hakati rakendama võrgust saadud muukraudu ja häkkerite oskusteavet, millele järgnes tõsisemate infokahjustuste sari ning raha kaugvarguse katsed. Praegusajal tuleb tõdeda, et sportlikust häkkimishuvist või labasest arvutivandalismist innustatud indiviidide koha on võtnud majanduslikest huvidest motiveeritud arvutikurjategijad, kelle töömeetodid katavad kogu infotehnoloogiliste vahendite spektri.

Turvaintsidentide mõjul on ettevõtted ja riigiasutused 20. sajandi lõpuaastaist alates hakanud turvaprobleeme teadvustama, vähe ollakse aga informeeritud turvaliste andmetöötlussüsteemide sihipärase rajamise ja käigushoiu meetoditest. Turvaküsimustega tegelevad peamiselt süsteemiülemad (administraatorid), kes suudavad enamasti kursis olla aktuaalsete ohtude ja nende kõrvaldamise hetkevahenditega, kuid ei ole sageli suutelised süstemaatiliselt korraldama oma objektide kompleksset turvet.

1993. aastal koostas praegune Cybernetica AS riigiasutuste tellimusel uuringuaruande "Andmeturbe infotehnoloogilised meetodid", mis oli Eestis esmakordne ülevaade andmete ja infotöötlussüsteemide turvalisuse kõigist infotehnoloogilistest aspektidest: andmeturbe eesmärkidest, ohtudest ja nende analüüsist, turvapoliitikast, süsteemide turbe spetsiifikast, turvamehhanismidest jne. Käesolev raamat on selle ülevaate edasiarendus, mis võtab arvesse vahepealsetel aastatel toimunud arengut ning asetab veelgi tugevama rõhu arvutivõrkude turvalisusele.

Raamatu teine trükk võtab arvesse Cybernetica turvaspetsialistide laialdast kogemust nii infoturbe õigusruumi korrastamisel kui ka turvamehhanismide alases teadustöös, aga ka kogemust, mis on saadud oma arendusprojektide ning auditi- ja konsultatsioonitegevuse kaudu. Ehkki tänased teadmised võimaldaks infosüsteemide turbest kirjutada palju mahukama ülevaate, on raamatu kokkupanemisel olnud eesmärk jääda konspektiivseks ja pigem anda lugejale viiteid detailsema teabe allikatele.

„Infosüsteemide turve“ ei ole turvanippide kogu, vaid süstemaatiline ülevaade infoturbest kui eridistsipliinist. Raamat selgitab nii teooriat kui ka praktikat ning on mõeldud eelkõige infotehnoloogiat kasutavate asutuste juhtidele ja infosüsteemide turvalisusega tegelevatele spetsialistidele. Kasulik on ta ka infotehniliste erialade õppejõududele ja üliõpilastele ning kõigile, keda huvitab infosüsteemide muutmine turvaliseks. Raamatu esimene osa käsitleb turbeala põhimõisteid. Kesksel kohal on ohud ja turvaaugud ning neist tulenev turvarisk: eelkõige tuleb tunda vaenlast. Teine osa (ilmunud 1998) vaatleb infoturbetehnoloogia üldist arsenali, milles tuleb osata orienteeruda sobivate tõrjerelvade valimiseks.

Loodetavasti aitab raamat kaasa sellele, et infoühiskonnas omandaks eestlane lisaks infotehnilistele oskustele ka vajaliku turvakultuuri ja võiks senisest muretumalt kasutada oma arvutit enda ja ühiskonna hüvanguks.

Koostajad

I TURVARISK

Sisukord

1 TURVALISUS

Turvalisusel on infotehnoloogias oma spetsiifiline sisu. Ta ei tähenda lihtsalt kaitstust või puutumatust. Turvalisus on mitmemõõtmeline mõiste, ta tähendab mitme infotehnoloogiliselt olulise omaduse püsimist ohtude kiuste. Infosüsteemide edukaks turbeks tuleb kõigepealt selgesti mõista turvaülesande olemust, selleks aga eelkõige turvalisuse olemust. Esmavajalikke põhimõisteid seletab esimene peatükk.

1.1 Infosüsteemi varad

Turvaprobleemid tekivad kõikjal, kus kellegi omanduses või käsutuses on varasid — materiaalseid või intellektuaalseid ressursse, millel on mingi, enamasti rahas väljendatav väärtus.

Infosüsteem on standardi ISO 2382 määratluses

> *informatsiooni andev ja jaotav infotöötlussüsteem koos juurdekuuluvate organisatsiooniliste ressurssidega, sealhulgas inim-, tehniliste ja rahaliste ressurssidega.*

Infosüsteemide peamised varad on

- andmed,
- infotehniline aparatuur (arvutisüsteemide riistvara, bürootehnika, sideseadmed),
- andmesidekanalid,
- baas- ja rakendustarkvara.

Süsteemiga seotud ressursside hulka kuuluvad veel

- organisatsioon (selle struktuur ja talitlus),
- personal,
- andmekandjad,
- dokumendid,
- infrastruktuur (territoorium, rajatised ja kommunikatsioonid).

Nende turvalisusega seotud küsimused ei ole ainult infotöötlusspetsiifilised.

Muude kaitstavate varade, näiteks pangaseifi või relvalaoga võrreldes on arvutisüsteemide varadel oma spetsiifika, mida tuleb turvameetmete kavandamisel arvestada.

- **Varade väärtus**. Arvutis salvestatud andmebaasi väärtus võib sageli ületada pangaseifi sisu väärtuse. Infotehnilisele süsteemile tekitatud kaudne kahju on enamasti suurem kahjustatud komponendi otsesest rahalisest väärtusest (vt ka 1.4).
- **Portatiivsus**. Riistvara võib portfelli mahutada sadade tuhandete kroonide väärtuses, andmeid veelgi suuremas väärtuses.

- **Võimalus vältida füüsilist kontakti**. Adekvaatse kaitseta elektronarveldus ning muud võrguteenused võimaldavad vargusi ja muid kahjustusi ilma füüsilise sissetungita kahju-kannataja juurde.
- **Kahjustuste varjatus**. Informatsioon ei hävi kopeerimisel, vargust saab tuvastada ainult kaudselt. Informatsiooni modifitseerimine (näiteks ründetarkvaraga) toime võidakse avastada liiga hilja.

1.2 Turvalisuse mõiste

Traditsiooniliselt on varade turvalisuseks nimetatud varade kolme esmavajaliku omaduse tagamist teatavas konkreetsetest tingimustest sõltuvas ulatuses.

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.

Konfidentsiaalsusele sisult lähedane, kuid turvaprobleemidelt erinev on aspekt, mis hõlmab näiteks autoriõiguste kaitset: informatsioon võib oma loomult olla avalik ja üldkättesaadav, kuid on kellegi seaduslik omand. Seda silmas pidades lisavad paljud mudelid, metoodikad ja turvapoliitikad neljanda põhiatribuudina legaalsuse ja eetilisuse. Tõsi küll, nende kaitset on praktikas võimalik korraldada mitte omaniku, vaid kasutaja poolel, st arvutisüsteemide omanikud võivad kohaldada meetmeid näiteks varastatud tarkvara kasutamise tõkestamiseks.

Kuna käideldavus sisaldab endas teovõime nõuet, meenutab ta teataval määral süsteemi töökindluse nõuet, kuid ei kattu sellega (vt allpool). Seni on töökindlus turvamudelitest välja jäetud ja teda on vaadeldud turvaprobleemidest lahus. Komplekssemad käsitlusviisid püüavad opereerida omaniku ja legaalse kasutaja seisukohalt otstarbekamate infotöötlussüsteemi kvaliteedi agregeeritud näitajatega (T. Beth, J.C. Laprie, T. Olovsson jt).

Näiteks T. Olovsson esitab järgmise kvaliteedinäitajate taksonoomia:

- **sõltumisväärsus e teenuse kvaliteet** (*dependability*),

- **käideldavus** (*availability*),
- **töökindlus** (*reliability*),
- **ohutus** (*safety*),
- **turvalisus** (*security*),
- **terviklus** (*integrity*),
- **konfidentsiaalsus** (*confidentiality*).

Kvaliteedi komponendid on selles skeemis määratletud nii.

Käideldavus *A(t)* on tõenäosus, millega süsteem on kasutuskõlblik hetkel *t* ning iseloomustab teenuse olemasolu.

Töökindlus *R(t)* on tõenäosus, millega süsteem täidab oma funktsioone ajavahemikul $[t_0,t]$ eeldusel, et ta töötas hetkel t_0, ning iseloomustab teenuse pidevust.

Ohutus *S(t)* on tõenäosus, millega süsteem täidab temalt nõutavaid funktsioone tõrgeteta või ilmutab tõrkeid, millel ei ole oluliselt kahjulikke tagajärgi, nt materiaaset kahju ega traumasid (tõrkekindel töö).

Turvalisus on süsteemi võime kaitsta oma objektide (ressursside ja informatsiooni) terviklust ja konfidentsiaalsust. Turvateoreetikud peavad otstarbekaks defineerida ka turvalisust analoogiliselt ülaltooduile tõenäosusena *Sec(t)*, millega süsteem suudab oma objektide terviklust ja konfidentsiaalsust kaitsta etteantud ajavahemikul $[t_0, t]$. See võimaldaks kasutada turvamõõte, mis oleksid analoogilised näiteks keskmisele tõrke-eelsele töövältusele (MTTF), ja kvaliteediaspekte mugavamalt komplekssselt käsitleda. Turvalisuse kvantitatiivne kirjeldamine nõuab aga veel mahukaid uuringuid.

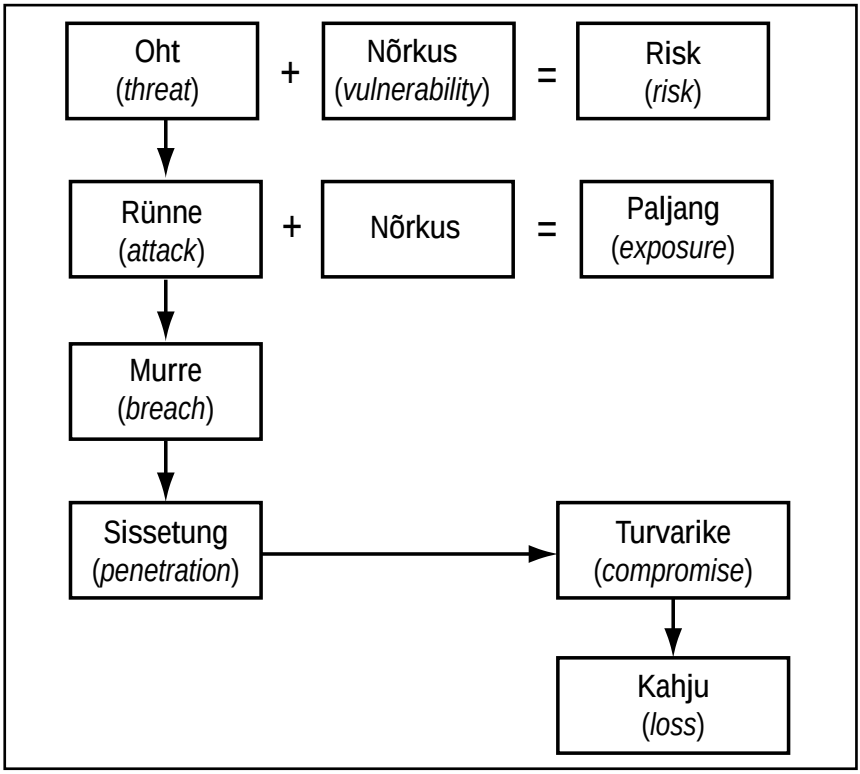
Olovssoni mudeli realiseerimine võimaldaks optimeerida süsteemi teenusekvaliteeti, sest üldjuhul võivad kvaliteedi eri aspektid olla vastuolus. Ehkki näiteks mitmed töökindluse tõstmise meetodid võivad ühtlasi lisada ka turvalisust, on lihtne leida ka vastupidiseid olukordi. Ainuüksi turvamehhanismide lisamine süsteemile suurendab keerukust, kahandades seega töökindlust.

Kuna enamik kasutuselolevaid turvametoodikaid, -standardeid ja -hindesüsteeme põhinevad traditsioonilisel kolmekomponendilisel käsitlusel, on seda üldiselt järgitud ka käesolevas raamatus. Viiteid puutepunktidele töökindluse ja ohutuse probleemidele on esitatud riskianalüüsi osas, eriti seoses Rahvusvahelise Elektrotehnikakomisjoni eelstandardiga IEC 1508, mis muuhulgas spetsifitseerib nõuded käideldavusele ja terviklusele töökindluse ja ohutuse eesmärgil.

1.3 Turvalisuse rikkumine

Kaitstavate varade soovimatu olekumuutus ei tarvitse toimuda silmapilkselt. Enamasti on see mitmeastmeline protsess, mille eri järke on rikkumiste tuvastamiseks ja kaitsevahendite kavandamiseks kasulik piiritleda ja eristada.

ISO 2382-8 esitab selleks joonisel 1 oleva skeemi, mis võtab kokku rikkumisprotsessi eri järgud ja nende realiseerumise tagajärjed.



Joonis 1. Turvalisuse rikkumise tasemed

See skeem kirjeldab eeskätt sihilikku kahjustustegevust. Stiihiliste ohtude puhul ei saa kõnelda ründest või sissetungist, vaid ohu realiseerumisest. Skeemi olulisemaid komponente käsitletakse allpool detailsemalt. Praktikas kasutatavad riskianalüüsi ja turbearenduse metoodikad ei järgi enamasti täpselt ISO skeemi.

1.4 Turvariketest põhjustatud kahjud

Iga konkreetse objekti turvatarbe otsustamisel tuleb arvestada olemasolevatest varadest ja ettevõtte või organisatsiooni tegevuse spetsiifikast lähtudes võimalikult täielikult ohtude realiseerimisel tekkivaid kahjusid:

- ***otsesed kahjud*** on väljendatavad hävinud või kaotsiläinud komponendi hinna või kahjustatud komponendi taaste- või remondikuludena;
- ***kaudsed kahjud*** ilmnevad tööseisakute ja muude asutuse talitluse häirete, toodangu või teenuste mahu või kvaliteedi languse, välissanktsioonide rakendumise ja asutuse maine languse kaudu.

Enamasti on kahjud kaudsed ja seetõttu rahalises väärtuses raskesti hinnatavad. Tüüpilised on tabelis 1 olevad kahjude liigid.

Tabel 1. Kahjude liigid

Kahjude liik	Näiteid	Kriteerium
1. Seaduste, eeskirjade, lepingute vms rikkumine	• Põhiseadus, kriminaalkoodeks, tsiviilkoodeks, andmekaitse seadused, autoriõiguse konventsioonid, patendikaitse • Halduseeskirjad, statuudid, teenistusmäärustikud • Isikuandmete kasutamist ja privaatsust puudutavad seadused või tavad • Andmetöötluse hooldelepingud, konfidentsiaalsuslepingud	Kvalitatiivne: kaalukus Kvantitatiivne: nt lepingutrahvide suurus
2. Isikliku heaolu või tervise kahjustamine	• Meditsiiniseire arvutid • Meditsiinidiagnostika süsteemid· • Lennujuhtimisarvutid· • Liikluse reguleerimise süsteemid	Trauma tõenäosus
3. Ülesannete täitmise kahjustus	• Tähtaegade ületamine haldusandmete töötlusviivituse tõttu • Tarnete hilinemine tellimuste töötluse viivituse tõttu • Defektne toodang väärade juhtimisandmete tõttu • Ebapiisav kvaliteedi tagamine testimissüsteemi tõrke tõttu	Kvalitatiivne: talutavus asjassepuutuvaile Kvantitatiivne: suurim lubatav seisakuaeg

Kahjude liik	Näiteid	Kriteerium
4. Negatiivne mõju välis-suhetele	• Asutuse maine kahjustamine • Asutuse usaldatavuse langus • Koostöösuhete kahjustamine • Asutuse töö kvaliteedi usaldatavuse langus • Konkurentsipositsiooni kaotus	Kvalitatiivne hinnang
5. Rahaline kahju	• Uurimis- ja arendustulemuste volitamata avalikustamine • Andmete manipuleerimine raamatupidamis-süsteemis • Läbimüügi vähenemine IT-juhitava tootmise tõrke tõttu • Tellimuste kaotus turustusstrateegia või käibeandmete volitamata avalikustamise tõttu • Tõrge reisibüroo registreerimissüsteemis • Tõrge panga arveldussüsteemis • Riistvara vargus või häving • Vead arvandmete (nt koguste, kuupäevade, koefitsentide) sisestamisel süsteemi	Rahaline väärtus

Ühest Briti organisatsioone hõlmanud 2008. aasta uuringust (PwC) ilmneb, et 25% riketest liigitati „vähemalt tõsist mõju“ avaldavaks. Kõige suuremaid kulusid põhjustas esiteks äritegevuse katkemine, teiseks intsidendile reageerimine. Kõige ohtlikumaks peeti süsteemi riket või andmete muutmist, mis 47% juhtudest põhjustas seisakuid kuni 10 tööpäeva.

2 OHUD

Ohud on potentsiaalsed turvakahjude algallikad, mis adekvaatsete kaitsemeetmete puudumisel võivad põhjustada turvarikkeid. Edukaks kaitseks tuleb kõigepealt hästi tunda vaenlast. See peatükk annab ohtudest süstemaatilise ülevaate.

2.1 Ohtude liigid

Toime järgi võib ohud liigitada nelja põhitüüpi.

1. **Halvang** (*interruption*) ilmneb selles, et mingi vara hävib, muutub kättesaamatuks või kasutuskõlbmatuks, st rikutud on vara käideldavus. Halvangu näiteid: mingi riistvarakomponendi häving, programmi või andmefaili kustutus, kettal asuva faili muutumine kättesaamatuks operatsioonisüsteemi või failiohjuri rikke tõttu.

2. **Infopüük** (*interception*) tähendab mingi volitamata subjekti (isiku, programmi, arvutisüsteemi) rünnet konfidentsiaalsusele (ebaseaduslikku kopeerimist, pealtkuulamist jne). Süsteemi poolt vaadatuna on see **andmeleke**.

3. **Modifitseering** (*modification*) on volitamatu muudatuste tegemine.

4. **Võltsing** (*fabrication*) laias tähenduses hõlmab võltsitud objektide lisamist infosüsteemi, sõnumite reprodutseerimist vääras kontekstis, sõnumi saatmise või saamise salgamist jms.

Need ohud võivad toimida kõigile süsteemi komponentidele.

Tabel 2. Ohtude liigid

	Riistvara	**Tarkvara**	**Side**	**Andmed**
Halvang	Teenuse tõkestus	Kustutus	Ummistus	Kaotsiminek
Infopüük	Vargus	Kopeerimine	Liini kuulamine	Kopeerimine
Modifitseering	Konfiguratsiooni muutmine	Loogikapomm	Marsruudi muutmine	Järjestuse muutmine
Võltsing	Kasutamise eitamine	Paroolipüüde-programm	Teesklus	Fiktiivsete lisamine

On ka muid analoogilisi toime liigitusi, mis lähtuvad vastava organisatsiooni varade ja kahjude spetsiifikast. Näiteks USA mereväe infoturbe juhendites on toime neli klassi sellised: häving, modifitseering, salastusrike ja teenuse tõkestus.

Ohuallikate olemuse järgi on turvalisuse seisukohalt otstarbekas eristada sihilikke sekkumiskatseid stiihilistest teguritest. Sageli püütakse turvameetmete valimisel kaitsta süsteeme ainult teadlike sissetungide eest (eriti pärast mõnd teatavaks saanud õnnestunud sissemurdu), tegelike kahjude statistika aga näitab juhuslike mõjurite märksa kaalukamat rolli.

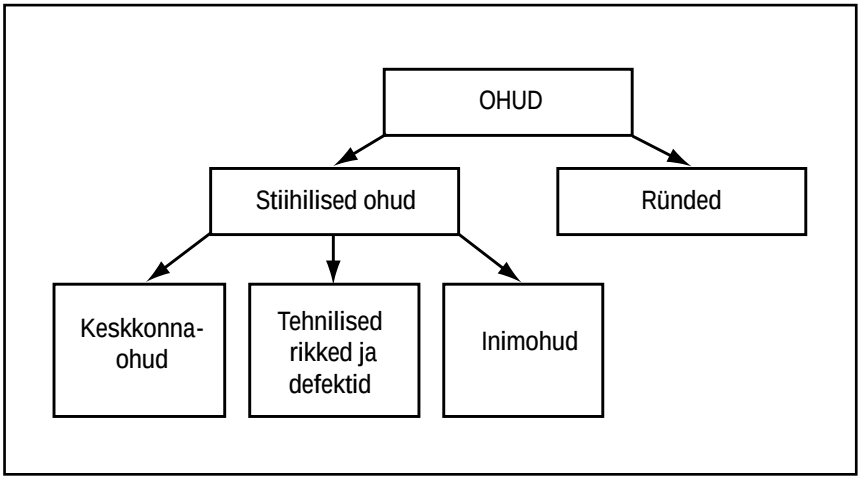
1. **Stiihilised** ohud tulenevad vääramatust looduslikust jõust, mis võib olla loomult juhuslik (äike, ujutus) või regulaarne (kulumine, materjalide väsimine, saastumine), aga ka inimvigadest, mida võivad põhjustada ebapiisavad oskused, hooletus, juhtimisvead, keskkonnategurid. Eriti kaalukad on juhtimis- ja otsustusvead infosüsteemi elutsükli kõigis järkudes. Turvaülesande püstituse ja lahendamise tarbeks on kasulik rühmitada niisugused stiihilised ja poolstiihilised ohud nende kandja järgi:

a) keskkonnaohud,

b) infosüsteemi või infrastruktuuri tehnilised rikked ja defektid,

c) inimohud.

2. **Ründeohud** lähtuvad inimestest, kes on mitmesugustel motiividel ja ajenditel (isiklikud huvid, huligaansus, riiklik või eraluure jne) valmis sihilikult kahju tekitama. Neid ohte on otstarbekas eritleda ründeobjektide ja meetodite järgi.



Joonis 2. Ohtude liigitus ohuallikate järgi

Detailsemalt käsitletakse tüüpilise kasutussituatsiooni levinumaid stiihilisi ja ründeohte järgmistes alajaotistes. Loetletud ohtude arvestamisest piisab objekti keskmise või kõrge kaitsetaseme kavandamiseks. Maksimaalse kaitsetaseme taotlemisel tuleb ohtude spetsifikatsiooni täiendada haruldasematega, eriti tehniliselt keerukate ja kulukate professionaalsete ründemeetoditega.

2.2 Keskkonnaohud

Infosüsteeme ohustavad mitmesugused ilmastikunähtused, loodusõnnetused, stiihilised tehislikud mõjurid ja väliskeskkonna avariid. Turvaülesande lahendamisel tuleb arvestada vähemalt järgmistega.

2.2.1 Äike

võib indutseerida purustavaid impulsse või häiringuid sideliinides ja aparatuuris, põhjustada lühiajalisi toitekatkestusi või -häiringuid alajaamade kaitseseadmete rakendumise kaudu ning kahjustada kaitsmata infrastruktuure. Keskmine välk (200 kA × 50...100 µs) tekitab elektroonikaaparatuuri ohustavaid toitepinge tõukeid 2 km raadiuses.

2.2.2 Tormid

võivad kahjustada infrastruktuuri ning seeläbi kahjustada või hävitada seadmeid. Näiteks kui konditsioneeri jahutustorud on viidud katusele, võib katuse purunemine tormis põhjustada külmutusaine lekke arvutikeskusesse.

2.2.3 Kahjutuli

saab enamasti alguse stiihilistest teguritest (elektriline ülekoormus, keevitustööd, jõuluküünlad, unustatud kohvikeetja, äike) ning nende toimet soodustavatest tehnilistest (tulekindlate vaheuste puudumine, kaablikanalite ehitusviis) ja organisatsioonilistest (süttivate materjalide väär ladustus, kustutite vähesus või halb paigutus) puuetest. Lisaks otsesele termilisele toimele tuleb arvestada põlemissaaduste agressiivset keemilist toimet, eriti tehismaterjalide puhul (näiteks kaablite põlemisel). Kaudselt ohustavad elektroonikaseadmeid ka vale tüüpi kustutussüsteemid: vaht-, vesi- või pulberkustutite kasutamine võib ka väikese põlengu korral põhjustada suuri kahjusid.

2.2.4 Vesi

loodusliku protsessi (vihm, üleujutus), infrastruktuuri avarii või väärkäsitsuse (lekkiv veetorustik, kanalisatsioon, keskkütteradiaator või konditsioneer, rakendunud sprinkler) tõttu või inimtegevuse (koristamine, tulekustutus) tulemusena.

2.2.5 Lubamatu temperatuur ja niiskus

tekitavad aparatuuri tõrkeid ning kahjustavad andmekandjaid ja infotöötlusmaterjale. Ruumide mikrokliima hindamisel tuleb arvestada, et otsene päikesekiirgus võib üsna tavalistes tingimustes tekitada mingis ruumiosas üle 50° C ulatuva temperatuuri. Korraliku ventilatsioonisüsteemi asendav avatud aken võib põhjustada lubatavast suuremat õhuniiskust ning niiskuse kondenseerumist aparatuuris.

2.2.6 Tolm ja saastumine

kahjustavad eeskätt andmekandjaid ja elektromehaanilisi seadmeid (CD-draiv, printer, skanner, faks). Seadmete saastumisel tolmuga võib temperatuur seadme sees ületada lubatu. Üldreeglina on seade saastumisele seda tundlikum, mida kõrgemasse klassi kuuluvad ta jõudlus- ja kvaliteediparameetrid (täpsus, tundlikkus, eraldusvõime jne).

2.2.7 Elektromagnetilised kiirgushäiringud

võivad lähtuda looduslikust (äike, magnettorm) või tehisallikast (mootor, trafo, magnetkaardiriider, lähedal asuv raadio- või televisioonisaatja, kõrgepingeliin) ning tekitada tõrkeid aparatuuris. Tugev magnetväli kahjustab ka magnetandmekandjaid (kassettlint). Mobiilvõrgu käideldavuses (mis on väiksem kui püsivõrgul) võib elektromagnetiliste kiirgushäiringute mõjul esineda olulisi häireid või katkestusi.

2.2.8 Väliste infrastruktuuride rikked või häiringud

Kõige sagedamini esinevad elektritoite häiringud, eriti toite katkemine (katkestused kestusega alla 1 s on sagedad, kusjuures infotehnika tööd võivad häirida katkestused kestusega üle 10 ms). Vastavad rahvusvahelised standardid eristavad tagajärgede ja kaitsemeetmete seisukohalt toitehäiringute nelja põhiliiki:

- pinge täielik või tugev kadu (*outage*),
- pingetõuge (ajutine ülepinge, *surge*),
- impulsshäiring (*spike*),
- müra (*noise*).

Arvestada tuleb ka telefonivõrgu valeühendustega. On näiteks teada juhtumeid, kus valeühenduse tõttu vääral aadressil faksi saatnud firma jäi ilma suurest tellimusest. Faksi saatmisel võivad tekkida vead edastushäirete tõttu.

2.3 Tehnilised rikked ja defektid

Turvameetmete valimise seisukohalt on kasulik vaadelda sedalaadi ohte eraldi, ehkki nad on olemuselt sekundaarsed, st tulenevad valmistus- või kasutusprotsessis toiminud keskkonna- või inimteguritest.

2.3.1 Infotöötluse infrastruktuuri avarii,

eriti sisevõrkude katkestus (elekter, telefon, küte, ventilatsioon, vesi, signalisatsioon, gaas vm). Oluline toime on ka konditsioneeride riketel, torustike leketel jms. Toimet tugevdab tehnovõrkude vastastikune sõltuvus, näiteks konditsioneerimise sõltuvus veevarustusest. Võrreldes analoogilise objektivälise avariiga on infrastruktuuri lokaalne osa asutuse enda kontrolli all ja ta käigushoiuks tuleb rakendada teistsuguseid meetmeid.

2.3.2 Riistvara defektid ja rikked,

alates IT-süsteemi avariist (tehnilise rikke, inimvea, vääramatu jõu vm tõttu) ja lõpetades üksikseadmete riketega, millest tulenev teabe puudulikkus või vigasus pole alati märgatav. Olulised ohud on võrgu- või süsteemihaldussüsteemi komponentide tõrked – näiteks saab ründaja ära kasutada võrguhalduskomponendi tõrget, et tuua oma arvuti märkamatult võrku.

2.3.3 Sideliinide rikked ja häiringud

Levinuimad on liinihäired keskkonna toimel (magnetväli, kaablite vastastikune induktsioon, lubamatu temperatuur, kaabli mehaaniline koormus vms). Kaabli varje mõlema otsa maandamisel võivad varjes tekkida häirivad tasandusvoolud. Induktsioonist või lekkevoolust tingitud läbikoste võimaldab liini hõlpsat pealtkuulamist. Tüüpsed andmesidevahendid sisaldavad tavaliselt piisavaid mehhanisme liinihäiretest põhjustatud vigade tuvastuseks, kuid näiteks faksisõnumite kasutamisel tähtsate otsuste alusena tuleb arvestada võimalikke edastushäiretest tulenevaid vigu. Häiringud võivad ka rikkuda IP-kõnesid VPN-i kaudu. Turvameetmete valimisel tuleb lisaks inimtegevusele ja tehnokeskkonnale arvestada ka muid kahjustavaid tegureid (rotid, taimede juured).

2.3.4 Infokandjate defektid

võivad tekkida juba valmistusprotsessis, aga ka vananemise, keskkonnamõjurite jms tõttu. Muuhulgas võib infokandjaid kahjustada näiteks ehitustolm. Salvestised võivad hävida ka vananemise, magnetväljade, kõrge temperatuuri, viiruste või kogemata kustutuse tõttu. Näiteks termopaber võib rikneda vananemise, temperatuuri, valguse, markertindi või liimide toimel.

2.3.5 Turvavahendite tõrked

vananemise, toite kao, väärkasutuse, saastumise vms tõttu. Peamiselt puudutab see füüsilisi vahendeid (lukud, magnet- või kiipkaardid, tuletõrje- ja valvesignalisatsiooni andurid, videomonitorid).

2.4 Inimohud

Stiihilise loomuga inimohud võivad lähtuda töötajate endi oskamatusest, hooletusest, tähelepanematusest jm individuaalsetest omadustest, kuid neid võivad esile kutsuda või soodustada ka väsimus või tervisehäired ning neid põhjustavad ebasoodsad füüsilised või sotsiaalpsühholoogilised keskkonnatingimused ja organisatsioonilised puudused.

2.4.1 Personali väljalangemine,

ajutiseks või alaliselt, näiteks haiguse, õnnetusjuhtumi, surma, streigi, töölt lahkumise vms tõttu. Stiihilistest põhjustest tingitud ajutise äraolekuga võrdset toimet avaldavad ka korralised äraolekud (puhkused, ametisõidud jms), kui nendega õigeaegselt ei arvestata.

2.4.2 Juhuslikud äpardused,

näiteks järgmised tüüpilised.

- Seadme või andmete hävitamine kogemata (kohvi pillamine seadmesse, arvuti väljalülitus rakendusprogramme sulgemata, kinnitusnõudest loobumine failihalduriga töötamisel).
- Väärad kaabliühendused (sealhulgas halva dokumentatsiooni ja märgistuse tõttu).
- Liinide kahjustamine kogemata, näiteks kaevetöödel, seinte puurimisel, naelutamisel, seadmete tassimisel, puhastusvee kasutamisel jne.
- Väära või lisa-andmekogumi saatmine andmekandjaga (jäi andmekandjal kustutamata, salvestati terve kataloog, aeti failid segi).
- Keskjaama rike käsitsemisvea tõttu (ümberkonfigureerimisel või -programmeerimisel, hooldetöödel).
- Automaatvastaja väär käsitsemine (eksitused mitmefunktsiooniliste klahvidega, kogemata kustutus).
- Kõnepartneri puudulik identifitseerimine.
- Õiguste kogemata andmine.
- Printimine valesse võrguprinterisse (nt väljaspoole turvatsooni).

2.5 Ründed

2.5.1 Ründeallikad

Riskiteguritena tuleb arvestada järgmisi inimrühmi.

1. **Infosüsteemide volitatud kasutajad**. Uuringud näitavad, et sisemise ründe oht ületab senise statistika kohaselt tunduvalt välistest allikatest lähtuva ohu. Ohte tekitavad järgmised asjaolud:

- eetiliste tõkete puudumine ebaseadusliku kasu taotlemisel,
- vallandatute või ahistatute kättemaksumotiivid,
- poliitilised või ideoloogilised motiivid.

2. **Majandus- ja sõjalise luure agendid**. Statistika ei peegelda neid arusaadavatel põhjustel täielikult, kuid nende osatähtsus on suhteliselt väike – sagedasemad on konkureerivate firmade majandusliku ning tehnilise spionaaži ja piraatluse juhud. 2007. aastast on teada juhtum, kus Hiina sõjaväevõime süüdistati küberrünnakus Pentagoni vastu. Sama aasta lõpus hoiatas Briti vastuluureteenistus MI5 ligi 300 Ühendkuningriigi ettevõtet elektronluure ohu eest. 2008. aastal ilmnes, et Saksa föderaalne luureteenistus BND oli kasutanud nuhkvara Afganistani kaubandus- ja tööstusministeeriumi vastu. Samal aastal süüdistasid Hiinat küberspionaažis ka Belgia ja India.

Eesti oludes on mainimist väärt 2007. aasta aprillikuu küberrünnakud valitsusasutuste veebisaitide vastu. Teadvustada tuleb ka poliit- ja tööstusspionaažist tulenevaid ohte, millele loovad eriti soodsa pinnase ideelised, sügavalt isiklikud ja majanduslikud motiivid. Selle näiteks on nn H. Simmi juhtum [23], kes kõrge riigiametnikuna edastas välisluurele täiesti salajase tasemega Eesti riigisaladusi ja salastatud välisteavet. Siinjuures on oluline, et töölevõtmisel tehtud taustakontroll ega hilisemad riigisaladusele juurdepääseja loa taustakontrollid ei tuvastanud midagi – see tähendab, et taustakontroll võimaldab riske maandada, kuid ei välista neid täielikult.

3. **Häkkerid**. Nende arvele lähevad küll mitmed kõmulised raaliroimad (S. Jaschani ussid *NetSky* ja *Sasser*, mis saastasid Internetis 2004. a üle 500 000

arvuti), kuid statistika näitab, et nende osatähtsus nii juhtumite arvult kui ka kahjude kogusummalt jääb alla firmade oma töötajatest lähtuvatele ohtudele.

4. **Muud**. Siinsetes oludes tuleb kindlasti arvestada kriminaalse elemendi rünnetega. Kahjude suuruselt on peamine hetkeoht praegu arvutivargused.

Ründekanalid on põhiliselt järgmised:

1) arvutite ja sidesüsteemide kaugvõrgud;

2) vahetu kontakt rünnatava objekti infosüsteemide, infrastruktuuride või personaliga;

3) ründetarkvara sisaldavad andmekandjad, näiteks viirustega nakatatud mälupulgad.

Selline järjestus vastab ka senisele sageduse ja ohtlikkuse pingereale. Siinjuures on oluline, et võrkude arengu dünaamika on järsult suurendanud võrkude kaudu sooritatavate rünnete kaalu, eriti kui arvestada lisamõjurina elektronarvelduse jms materiaalselt motiveerivate võrguteenuste levikut.

2.5.2 Füüsilised ründed

Ohustavad eelkõige infosüsteemide käideldavust ja terviklust.

- Infrastruktuuri füüsiline rünne, näiteks kivi viskamine aknasse, pommi peitmine hoonesse, hoone süütamine. Kahjustav toime ei ole üheselt määratud ründe ulatuse ega realiseerumisastmega (ka pommiähvardus halvab normaalse talitluse). Rünne ei tule tingimata väljastpoolt (psühhopaat, terrorist, anarhist, konkurent jne), arvestada tuleb ka personali hulgast lähtuvat ohtu (vt 2.5.1).
- Vandalism sarnaneb oma toimelt füüsilisele ründele, kuid pole sihikindel; toimepanijaks võib olla joobnu, pettunud murdvaras vms.
- Volitamatu sisenemine hoonesse, muuhulgas sissemurdmise või turvavahendi halvamise teel on mitmete sellest tulenevate muude ohtude allikas.
- Vargus on füüsiline rünne aparatuuri, andmekandjate või paberdokumentatsiooni puhul, tarkvara ja informatsiooni saab aga varastada ka kopeerimise teel. Sisult on vargus ka asutuse infotehniliste ressursside volitamatu kasutamine isiklikeks vajadusteks (vt 2.5.3); kuna seda teeb peamiselt oma personal, on ressursivargust turvameetmete spetsiifika seisukohalt kasulik vaadelda eraldi ohuna. Füüsilise varguse võimalusega tuleb arvestada eriti mobiilsüsteemide (pihuarvuti, sülearvuti, mobiiltelefon) puhul.

- Infotehniliste seadmete või tarvikute manipuleerimine või hävitamine näiteks kättemaksu, luure või huligaansuse ajenditel.

2.5.3 Ressursside väärkasutus

Ohustab kõiki turvalisuse komponente, eelkõige käideldavust ja konfidentsiaalsust. Sageli tuleneb mitte kuritahtlikest motiividest, vaid uudishimust, tehnilisest huvist jne kõige "häkkerlikum" pahe.

- Arvutisüsteemide volitamata kasutamine. Enamasti põhineb paroolide puudumisel või nende väljaselgitamisel (vt ka 2.5.8).
- Kasutajaõiguste kuritarvitus, alates mittesihipärasest kasutamisest ning lõpetades võõraste paroolide lugemise, lubamatute kustutuste ja muude turvariketega.
- Süsteemiülema ("administraatori") õiguste kuritarvitus; selleks on praeguste levinumate platvormide (Unix ja/või Windows) puhul suured võimalused, sisuliselt on võimatu hoida tehniliste vahenditega ülema haldusvolitusi lahus juurdepääsust kõigile süsteemi ressurssidele.
- Unix-süsteemi saab kuritarvitada teesklusega (vt ka 2.5.6).
- Siseoht on suur hoolde- või haldustööde ajal; võib ilmneda katseid oma privileege suurendada, nendes olukordades sagenevad ka süsteemide krahhid.
- Telefoniteenuste vargus, nt personali era-kaugekõned.
- Faksiaparaadi volitamata kasutamine, näiteks fakside volitamata saatmine asutuse plangil, erasõnumite saatmine (vt ka 2.5.5, 2.5.6).

2.5.4 Ressursside blokeerimine

Ohustab eelkõige käideldavust, võib olla sihilik või tekkida volitamatu kasutamise kõrvalnähuna (vt ka 3.2.1). Avaldusvormid on ressursispetsiifilised.

- Teenuse halvamine, näiteks programmide massiline käivitus, kataloogi täitmine kogu ulatuses, võrgu ülekoormamine.
- Faksi vastuvõtu sihilik blokeerimine rohkete ja mahukate sõnumitega, mis viivad kiiresti paberi lõppemiseni või vastuvõtupuhvri täitumiseni. Juga- või kseroprindiga faksiaparaatidel ammendab musta lehe saatmine (eriti mugav on seda saata arvutist) kiiresti värvaine.
- Automaatvastaja sihilik ülekoormamine, nii et lindi kiire täitumise tõttu jäävad oodatavad vajalikud sõnumid saamata.

Vt ka jaotist 2.8 „Hajus ummistusrünne“.

2.5.5 Infopüük

Ohustab konfidentsiaalsust. Tüüpilisi ilmnemisvorme.

- Pealtkuulamine ruumides, näiteks salamikrofoniga, mobiiltelefoniga, salvestama jäetud diktofoniga või kuulates valjuhääldirežiimi lülitatud lauatelefoni kaudu ruumis toimuvat taustkõnelust. Ruume võidakse kuulata ka arvutite mikrofonide kaudu, nt hankides juurdepääsu failile /dev/audio Unixi all.
- Telefonikõnede ja andmesaadetiste pealtkuulamine näiteks ümbersuunamise käigus. Lihtsamal juhul võib seda teha uudishimulik töötaja, kes võtab vastu teistele adresseeritud kõnesid, kuulab kõnesid kõrvalt, vaatleb väljahelistamisel numbreid jne.
- Süsteemis salvestatud andmete volitamata lugemine või kopeerimine. Näiteks on väljastpoolt tellitud hooldetööde teostajal enamasti juurdepääs andmetele.
- Printerisse või skännerisse unustatud konfidentsiaalse dokumendi volitamata lugemine.
- Sisekeskjaama mälus salvestatud andmete leke. Sellised andmed võivad sisaldada turvatehnilist teavet (privileegid, paroolid) või muud konfidentsiaalset informatsiooni (elektroonilised telefonikataloogid).
- Liini kuulamine, alates operatsioonisüsteemi komplekti kuuluvate võrgudiagnostika vahendite kasutamisest ja lõpetades spetsialiseeritud võrguanalüsaatoritega. “Liini” tuleb mõista üsna laias tähenduses. Näiteks võib elektronpostisõnumeid kopeerida nende marsruudi suvalises (sõlm)punktis. Liini kuulamise eesmärk ei ole tingimata sõnumite sisu teadasaamine – sõnumid võivad olla krüpteeritud või nende sisu võib olla kergesti aimatav; sellistel juhtudel annab isegi rohkem konfidentsiaalset teavet liiklusvoo analüüs, eesmärgiga selgitada välja saatmisajad, edastusmahud, adressaat, meiliaadressid vms.
- Sissetung arvutitesse modemi kaudu (modemiühendusega arvuti liinile jätmisel pärast töö lõppu).
- Andmekandjate volitamata kopeerimine, näiteks nende edasitoimetamise käigus.
- Mobiiltelefoniga pildistamine.
- Suhtlusosavus (*social engineering*): näiteks maskeerumine IT-toeks ning telefoni või meili teel paroolide väljameelitamine.

2.5.6 Võltsimine

- Sõnumite salvestus ja taasesitus, näiteks paroolide hankimiseks (vt ka 2.5.9, trooja hobused) või suurte võltstellimustega kahju tekitamiseks.
- Teesklus, st sõnumite saatmine võltsrekvisiitidega (võõras parool, võltsitud saatja aadress) ja/või sobivat haruühendust kasutades; vrd 2.5.3). Suhteliselt lihtne on näiteks IP-tüssamine (IP-aadressi võltsimine, IP spoofing), kasutades sobivalt konfigureeritud võrguteenuseid (rlogin, rsh, rexec, X-Windows, RPC-põhised teenused); tõhusad ründed on võimalikud protokolli ARP kasutavates kohtvõrkudes, näiteks Ethernetil põhinevais.
- Teesklus faksimisel, nt allkirjade ja muude elementide monteerimine saadetisele.
- Näitlemine, st "oma inimeste" etendamine võib aset leida vahetult objektil (ründaja võib esineda näiteks telefonitehnikuna vms) või telefonitsi ("sekretär", kelle ülemus unustas parooli jne).
- Sõnumi saamise või saatmise salgamine on mugav võimalus näiteks sisseantud tellimusest loobumiseks, lubatud kiire tarne ärajätmiseks, desinformeerimiseks jne.

2.5.7 Süsteemide manipuleerimine

- Andmete või tarkvara manipuleerimine, näiteks valeandmete sisestus, pääsuõiguste muutmine, operatsioonisüsteemi tarkvara muutmine jne.
- Liinide manipuleerimine – mitte tingimata väljaspool objekti, on ka siserisk, sealhulgas liinide kasutamine isiklikuks otstarbeks.
- Andmeedastuse manipuleerimine protokollide turvaaukude kaudu, näiteks lähtemarsruutimise (*source routing*) rünne (marsruudi kirjeldust saab teel manipuleerida), ICMP-protokolli väärkasutus (marsruuditabeli muutmine *Redirect*-pakettidega, ühenduse katkestamine võltsitud tõrketeatepakettidega *Destination Unreachable*) või marsruutimisprotokollide väärkasutus (RIP-pakettidega saab muuta marsruuti).
- Aparatuuri kaughoolde portide rünne. Ka sisekeskjaama kaughalduspordid on olnud häkkerite sagedane ründeobjekt.
- Automaatvastaja kaugmanipuleerimine võimaldab sooritada mitmeid kahjulikke operatsioone, näiteks pealt kuulata ruumis toimuvaid kõnelusi või kuulata, muuta või kustutada salvestatud sõnumeid.

2.5.8 Turvamehhanismide ründed

Ründe olemus sõltub turvamehhanismi tüübist ning mehhanismi ja ta töökeskkonna tegelikest või oletatavatest turvaaukudest. Infotehnilistest mehhanismidest on põhilisteks ründeobjektideks pääsu reguleerimise mehhanismid ja krüptosüsteemid. Niisuguste rünnete tüüpilised näited on järgmised (vt ka 2.5.9).

- Süstemaatiline paroolide mõistatamine. D. Kleini 1990. a sooritatud uuring, mis hõlmas 15000 kasutajakontot, näitas, et 24,2% paroolidest õnnestus nende triviaalsuse tõttu väga kiiresti ära arvata. Süsteemi turvaaukude kaudu saab aga leida ka näiliselt hästi kaitstud paroole; klassikaline näide on nn Morrise uss, mis kasutas Unixi turvaauku, et mõistatada krüpteeritud paroole sõnastiku kõigi märksõnade krüpteeritult läbiproovimisega. Tänapäevane näide on uss *Conficker* (2009), mis kasutas ühe ründevektorina nõrkade paroolide äraarvamist.
- Automaatvastaja kaugjuhtimise turvakoode saab PC ja modemi abil murda väga kiiresti.
- Sõrmejäljelugejaid saab petta lateksile vms materjalile pressitud sõrmejälje koopiaga.
- Näotuvastamise seadmeid saab petta inimese näost tehtud video ettemängimisega [30].
- Silma vikerkesta tuvastamise seadmeid saab petta, kasutades näole asetatud peeneralduslikku fotot vikerkestast, millesse on tehtud auk pupilli jaoks [30].
- Kõiki biomeetrilisi seadmeid ohustavad vahemeherünne, taasesitusrünne, võltsandmete süstimine, talletatud mallide manipuleerimine, ründed süsteemitarkvara vastu (näiteks lubatava hälbe suurendamine) ja füüsiline teenusetõkestus (stroboskoobi kasutamine optiliste andurite vastu, rünne staatilise elektrilaenguga jm) [30].

2.5.9 Ründetarkvara

Ohtlikke tarkvaratooteid võib nende otstarbe ja toime järgi jagada järgmistesse rühmadesse.

Legaalsed tüüptooted. Nende hulka kuuluvad eeskätt operatsioonisüsteemide faili- ja kettafunktsioonid ning paljud faili-, ketta-, diagnostika-, häälestus- jm utiliidid, mis volitamatul kasutamisel on äärmiselt ohtlikud, kuna võimaldavad läbi murda mitmetest lihtsamatest turvamehhanismidest.

Kahjurvara. Mitmesuguste nüansside eristamisel võib saada üsna mitmeid alaliike, mille arv üha kasvab, kuid peamised esindajad on järgmised.

- **Loogikapomm**. Mingi programmi sisse peidetud koodilõik, mille kahjustav toime käivitub etteantud ajahetkel või mingi tingimuse täitumisel. Algselt kasutati peamiselt hävitustööks, kuid on kasutatud ka andmepüügiks. Ei kopeeri end.
- **Trooja hobune**. Loogikapommi analoog iseseisva programmina. Näiteks on modifitseeritud sisselogimisprogrammi (võltsitud sisselogimisaknaga) kasutatud paroolipüüdeks. Põhimõtteliselt võib esineda suvalist tüüpi programmis. Põhieesmärk on anda ründajale kaugkontroll ohvri arvuti üle.
- **Uss** (*worm*). Iseseisev programm, levib tavaliselt võrgu kaudu, kasutades ära mitmesuguseid turvanõrkusi. Kopeerib end, hõivates sellega ressursse ja tekitades ülekoormust. Tavaliselt tekitab arvutisse ka tagaukse, mille kaudu saab arvuti haarata robotivõrku. Ei tarvitse endast nähtaval kujul märku anda või üritab ennast aktiivselt varjata.
- **Viirus**. Koodilõik, mis kopeerib end mingi programmi külge või programmilõigu asemele või ketta buutsektorisse. Lisaks ressursside raiskamisele kahjustab kõikvõimalikel muudel viisidel. Puhtakujulisi viirusi tänapäeval enam ei esine.
- **Makroviirus** ehk dokumendiviirus on tavalise viiruse analoog, mis on realiseeritud mingi rakendusprogrammi makrokeeles. Makroviiruste kõrgaeg jäi 1990ndate keskpaika ja lõppu, kui levisid kahjurid nagu *Concept* ja *Nuclear*.
- **Pseudoviirused** on võrgufolkloori saadus. Aeg-ajalt levivad meili teel või veebisaitide kaudu hoiatused mingite fantastiliste omadustega viiruste kohta, nt viirus *Tuxissa* paigaldavat teda sisaldava meili lugemisel Windowsi asemele operatsioonisüsteemi Linux. Pseudoviirused ei kujuta endast ohtu tavalises mõttes, kuid võivad tekitada paanikat vilumatu personali hulgas ja põhjustada tööseisakuid või vääraid toiminguid.
- **Pipett** (*dropper*) on programm, mis installeerib ussi või trooja hobuse.
- **Reklaamvara** on programm, mis pakub oma põhifunktsionaalsust vastutasuks reklaamide kuvamise eest. Reklaamvara võib olla eraldiseisev (*Zango Toolbar*), eraldiseisev ja pakendatud mõne teise tootega (*Messenger Plus! Live*) või sisalduda põhitootes (*RealPlayer*). Reklaamvara võib koguda teavet kasutaja brauseri- või arvutikasutuse kohta.
- **Nuhkvara** on pahaloomuline programm, mis on arvutisse paigaldatud kasutaja teadmata või loata ning mis lisaks kasutaja tegevuste seirele võib muuta ra-

kenduste ja operatsioonisüsteemi sätteid ning häirida brausimist, kuvades reklaame automaatselt või suunates kasutaja soovitud lehe asemel reklaamlehele. Nuhkvara võib harvadel juhtudel varastada ka isikuandmeid.

Turvamehhanismide ründe programmid. Sellesse rühma kuuluvad programmid, mis on spetsiaalselt määratud paroolide püüdeks, šifreeritud andmete dekrüpteerimiseks jne. Selline häkkeritoode on nt *YTFakeCreator*, mis võimaldab kahjurvara levitamiseks tekitada veebilehe YouTube võltskoopia, kus palutakse kasutajal videote mängimiseks alla laadida dekooder (tegelikult kahjur). Tööriist *Goolag Scanner* kasutab Google'i otsimootorit, et leida turvanõrkustega veebilehti, kuhu süstida ründekoodi. Tuntumad arvutikurjategijatele müüdavad häkkeritooted on *MPack*, *IcePack* ja *Neosploit*, mille hinnad võivad küündida tuhandete dollariteni.

Paanikatarkvara (*scareware*). Siia kuuluvad võlts-viirusetõrjeprogrammid, mille eesmärk on mängida kasutajate arvutiturbehirmudel, pannes kasutajaid ekslikult uskuma, et nende arvuti on nakatunud. Taktika edukust näitab Lee Shin-Ja juhtum, kes aastail 2005–2008 teenis 9,8 miljonit dollarit, levitades nuhkvara otsimise programmi, mis kuvas võltse turvahoiatusi ning veenas seeläbi kasutajaid ostma Doctor Virus viirusetõrjeprogrammi. 2008. aasta veebruaris levis mürgitatud Flash-reklaamide kaudu paanikatarkvara *Troj/Gida-B*, mis hirmutas kasutajaid ostma võlts-turvatarkvara.

Kuna kahjurvara osakaal ja mõju on maailmas alates 2000ndatest aastatest märgatavalt kasvanud, vaadeldakse seda järgmises alajaotises ohuklassina lähemalt.

2.6 Kahjurvara

Viimane aastakümme on toonud kahjurvara *(malware)* osas palju muutusi. Klassikalised faili- ja buutsektori viirused, millele raamatu esmatrükis võis pühendada terve peatüki, on tänapäeval unustusehõlma vajunud ning põhiosa ründetarkvarast moodustavad ussid ja trooja hobused. Uut ründetarkvara luuakse kiiremini ja samuti kaob see kiiremini kui varem. Kui 1998. aastal sisaldas McAfee viiruste andmebaas ligikaudu 50 000 viirusesignatuuri, siis 2009. aastaks kasvas see arv üle miljoni. Tänapäevased ründed on organiseeritumad kui varem ning tihti kavandatud teabe ja ressursside varguseks firmadelt ja eraisikutelt. Ehkki on ründeid, mida ajendab poliitika või religioon, jääb peamiseks motiiviks ikkagi raha ning seeläbi on küberkuritegevus võtnud mõõtmed, kus näiteks andmeturbefirma Sophos avastab uue nakatunud veebilehe iga 4,5 sekundi järel ning ohuanalüüsi keskus SophosLabs saab päevas 20 000 kahjurvara kahtlusega koodinäidist.

Statistikaga tutvumisel on oluline silmas pidada, et viirusetõrjetooteid pakkuvad suurfirmad nagu Kaspersky Labs, F-Secure ja Sophos liigitavad ja nimetavad kahjurvara erinevalt ning registreerivad ka nakkusjuhtumeid eri arvul, mistõttu sellekohastes näitajates võib esineda märgatavaid kõikumisi. Kuna kahjurvara eluiga on varasemast lühem, on ka statistika perioodiliti väga erinev. Ehkki andmetest nähtub, et domineerib endiselt Windows-platvormi ründetarkvara, satuvad vahel ründe alla ka "eksootilised" platvormid, nt Palm Pilot (trooja hobune *Phage*), Pocket PC (trooja hobune *Duts*), Symbian-mobiiltelefonid (uss *Cabir*) ja kaabel-TV võrku ühendatud arvutid (viirus *Tremor*).

Võrdlemisi puutumata jäänud on Macintosh. 2007. aasta lõpus teatati trooja hobusest *OSX.RSPlug.A* ja 2008. aasta lõpus trooja hobusest *OSX.Lamzev.A*, kuid mõlemad vajasid nakatamiseks installprogrammi käivitamist ja kahjuri paigaldamise lubamist. 2008. aasta juunis ilmus trooja hobune *OSX/Hovdy-A*, mis üritas varastada nakatunud arvutist paroole, avada tulemüüri ja muuta turvasätteid. Sama aasta novembris hakkas levima pipett *OSX/Jahlav-A*, mis maskeeris ennast legitiimseks rakenduseks, aga pärast paigaldamist laadis arvutisse täiendavat ründekoodi. Ehkki kõik Macintoshi ründeprogrammid on üritanud ära kasutada MacOS-i või mõne selle rakenduse turvanõrkusi, on nende levik sõltunud ohvrite kergeusklikkusest, mistõttu on nakatumiste arv jäänud marginaalseks. Tuleb siiski arvesse võtta, et mida enam kasvab Macintoshi turuosa, seda rohkem ründeid on tulevikus oodata.

Tabel 3 esitab peamised meilimanustega levivad kahjurprogrammid. Protsent näitab vastava kahjuri osakaalu kõigist meili teel levinud kahjuritest.

Tabel 3. Meilimanustega levivad kahjurprogrammid

	2008	2007
Troj/Agent	31,0%	–
Troj/Invo	18,1%	–
Mal/EncPk	13,8%	–
Mal/HckPk	–	23,7%
W32/Netsky	4,4%	19,9%
W32/Mytob	–	13,2%
Troj/Dorf (Storm)	–	10,1%
Troj/Pushdo	4,3%	2,0%
Troj/Doc	2,9%	–
Troj/FakeVir	2,2%	–
Mal/Iframe	1,8%	–
Troj/VidRar	1,6%	–
Troj/DwnLdr	1,5%	–
Muud	18,4%	12,3%

Tabelist nähtub, et üks aasta on enam kui küllaldane, et ründetarkvara levikus toimuksid suured muutused. Nii näiteks pole 2008ndal aastal registreeritud aasta varem laialt levinud kahjurprogramme *W32/Mytob*, *Storm* jt.

2.6.1 Põhiliigid

Võrreldes 1990ndate algusajaga on piir ründeprogrammide liikide vahel hägustunud. Nt *Melissa* on nii uss kui ka viirus; *Nimda* on nii uss, viirus kui ka trooja hobune (harilikult klassifitseeritakse ussiks). Kuna puhtaid oma liigi esindajaid jääb järjest vähemaks, saab rääkida vaid sellest, et kahjuril esinevad erineval määral ühe või teise liigi tunnused. Samuti tuleb seetõttu ühe või teise liigi kohta tehtud statistikat alati hoolikalt tõlgendada. Kahjurite põhiliigituse andis jaotis 2.5.9, alljärgnev täpsustab seda.

Uss

on iseseisev programm, mis levib võrgu kaudu, kasutades ära turvaauke levinud teenustes. Ussid ei vaja levimiseks kasutaja tegevust ning üritavad enda olemas-

olu varjata. Ussid on harilikult laia mõjuga, näiteks 2003. a augustis nakatas uss *W32/Sobig* üle 100 miljoni arvuti (*F-Secure*, 2008). Ussid liigituvad järgmiselt.

- **Meiliussid** käivitatakse kohalikus arvutis, misjärel nad levitavad ennast meili teel. Varased ussid kasutasid ära meiliprogramme või programmiliideseid rikutud masinas, et levitada enda koopiaid teistele aadressidele. Hilisemad ussid sisaldasid juba oma SMTP-mootorit, mis muutis nad vähem sõltuvaks ohvri meilisaatmisvõimalustest.
- **Windowsi failijagamise ussid** kasutavad levimiseks protokolle SMB ja CIFS ning harilikult kasutatakse neid koos teiste ründevahenditega.
- **Harilikud ussid** ei nõua kasutaja sekkumist ja kasutavad protokollil TCP/IP põhinevaid otseühendusi, et rünnata nõrkusi operatsioonisüsteemides ja rakendustes.

Ussi **toimelaengul** võib olla mõni järgmistest eesmärkidest.

- Puuduv/mittetoimiv. Ussi autor pole toimelaengut lisanud või esineb selles tõrge. Ka ilma toimelaenguta ussil (nt *Slammer*) võib olla võrgu ülekoormamise tõttu laastav mõju.
- Kaugjuurdepääsu andmine. Nt uss *Code Red II* tekitas ohvri arvutisse tagaukse, mis võimaldas ükskõik kellel käivitada arvutis suvalist koodi.
- Ummistusrünne. Nt ussid *Code Red* ja *Conficker* sisaldasid vahendeid ummistusründe sooritamiseks kas ettemääratud või hiljem ründaja määratava serveri vastu.
- Spämmivahendus. Nt uss *SoBig* tekitas ohvri arvutisse avatud meiliserveri. Selliste serverite kasutamine võimaldab spämmeritel vältida musti nimekirju, kus on teadaolevad spämmi levitavad arvutid.
- Väljapressimine. Uss šifreerib kettal olevad andmed, mille dešifreerimise eest tuleb kurjategijale maksta lunaraha.
- Andmepüük. Nt meili teel levinud uss *SirCam* lisas manusena mõne juhusliku faili nakatunud arvutist. Tänapäevased ussid võivad otsida dokumente, isikuja krediitkaardiandmeid jm ka teatud märksõnade järgi ning edastada sellised andmed ründajale.
- Andmehävitus, vandalism. Nt ussid *Chernobyl (CIH)* ja *Klez* sisaldasid aegreleega mehhanismi andmete kustutamiseks.
- HTML-proksi loomine. Veebipäringute vahendamine läbi ussi (nt *SoBig*) tekitatud juhuslike prokside muudab andmepüügi vm kuritegeliku eesmärgiga veebilehtede sulgemise keeruliseks.

- Uuenduste allalaadimine. Tänapäevased ussid (nt *Conficker*) laadivad Internetist uuendusi, mis võivad sisaldada uusi ründesihtmärke, täiendatud kaitset tõrjevahendite vastu jms.

Tänapäevased ussid kasutavad enda eemaldamise takistamiseks mitmesuguseid tehnikaid. Näiteks kasutas Windowsi uss *Conficker.C* järgmisi võtteid [28]:

- lukustas kettal oma teegifaili, et seda ei saaks avada ega kustutada;
- muutis pääsuõigusi, et ükski kasutaja (sh süsteemiülem) ei saaks Confickeri registrivõtit avada ega kustutada;
- blokeeris Windowsi teenused, mis laadisid uuendusi ja turvapaiku;
- haaras vahelt DNS-päringuid, et blokeerida ligipääs veebisaitidele, kust saaks alla laadida Windowsi ja viirusetõrjetarkvara uuendusi või vahendeid Confickeri eemaldamiseks;
- seiras käimasolevaid protsesse, et avastada ja lõpetada musta nimekirja kuuluvad rakendused (viirusetõrjeprogrammid, Confickeri eemaldusvahendid jms);
- kasutas koodi sogastamist ja krüpteerimist, virtuaalmasina tuvastamist jm, et takistada enda analüüsimist siluriga.

Eesti oludes väärib mainimist ussi *W32.Allaple* ehk *Win32.RAhack* ehk nn Starmani ussi juhtum. See on polümorfne uss, mis loodi 2006. a spetsiaalselt veebisaitide starman.ee ja if.ee vastu ummistusründe sooritamiseks, kasutades selleks SYN-tulvet (vt 2.8). Aastatel 2006–2007 oli ainuüksi Starmanile suunatud pidev andmevoog ca 200 Mbit/s, mis kahanes 2009. a keskpaigaks ligi 6000 nakatatud arvutist lähtuva 50 Mbit/s-ni. Uss kasutab levimiseks Windowsi nõrkuste vallutamist, sõnastikupõhist paroolide äraarvamist ning ohvri arvutis HTML-failide nakatamist. Kurioosseks teeb juhtumi asjaolu, et ussi autorile mõisteti küll reaalne vangistus, aga kuna ussil puudub keskne juhtimiskanal, siis pole selle levimist võimalik peatada (v.a turvapaiga MS04-012 laadimisega kõigisse ohustatud arvutitesse).

Trooja hobused

vajavad arvuti nakatamiseks enda käivitamist ning seetõttu maskeerivad end huviäratavaks failiks, millega ära petta kergeusklik või teadmatu kasutaja. Trooja hobused levivad meilimanuste, kiirpostiprogrammide, veebilehtede jm kaudu, aga ka usside koosseisus. Üldjoontes on ka nende eesmärgid samad, mis ussidel; lisaks ülalnimetatule näiteks:

- ohvri arvutist meiliaadresside korjamine, mis lisatakse spämmerite andmebaasi;

- volitamata juurdepääsu loomine netipankadele ja krediitkaardikontodele;
- kasutajaandmete varastamine populaarsetest võrgumängudest;
- arvutisse tagaukse tekitamine, mis võimaldab ründajal võtta arvuti enda kontrolli alla või haarata see robotivõrku;
- andmepüük mitmel eri viisil: juhuslikel hetkedel kuvatõmmiste tegemine (lootuses, et pildile talletuvad isiku- või finantsandmed), klahvivajutuste salvestamine, dokumendifailide varastamine jms.

Spämm

Ka spämmi saab kasutada ründevahendina. Näiteks võltsitud lähteaadressiga spämmikirjade saatmise tulemusel võib ohver sattuda musta nimekirja (meiliserverid hakkavad tema kirju blokeerima või filtreerima) või kannatada mainekahjusid (kui ohvri nimel saadetakse vaenu õhutavaid, kuritegelikke vm kirju).

2.6.2 Levik

Kahjurvara levimisviiside statistikat esitab PC-de kohta tabel 4. [35]

Tabel 4. Ründetarkvara peamised levimisviisid

Käivitatavad failid	40%
Meili manused	32%
Protokoll CIFS	28%
P2P-võrgud (Kazaa, Gnutella, BitTorrent jt)	19%
Kaugelt vallutatavad nõrkused	17%
Tagauks (Kuang2, Subseven)	6%
SQL-süstimine	3%
Failiedastus/ pesastatud HTTP URI/ Yahoo! Messenger	2%
Veeb	1%
Märkus: kuna mõned ründeprogrammid levivad mitmel viisil, on summaarne protsent üle 100.	

Sealjuures on loobutud kahjurite levitamisest käivitatavate manustena (kuna kasutajad on õppinud nende avamisest hoiduma) ning selle asemel viidatakse meilis veebiaadressile, kust ühel või teisel petumeetodil meelitatakse kasutaja kahjurvara alla laadima ja käivitama.

Käivitatavate failide kaudu (peamiselt end irdmeediale kopeerides) levivad viirused ja mõned ussid. Ehkki seoses diskettide kasutuselt kadumisega näitas see levikuviis langustrendi ning asendus jagatud võrguressursside ja meili kaudu levimisega, muutus see taas populaarseks koos mälupulkade levimisega.

Irdmeedia (nt mälupulgad) kaudu levivad ründeprogrammid nagu *VBS.Runauto*, *W32.Sality.AE*, *W32.Gammima.AG*, *W32.SillyDC*. Kui arvuti on nakatunud, siis teatud liik kahjurvara kopeerib ennast kõikidele salvestusseadmetele, mis arvutiga ühendatakse. Veelgi levinum on rünne *Autorun/Autoplay* funktsionaalsuse kaudu. Vaikesätetes Windows saab faili "autorun.inf" põhjal sooritada arvutiga ühendatud irdmeediaga automaatseid tegevusi, nt käivitada teatud faile. Seda ära kasutades kopeerib kahjur ennast mälupulgale, misjärel piisab nakatumiseks mälupulga ühendamisest järgmise arvutiga.

P2P- ehk võrdõigusvõrkudes (Gnutella, Bittorrent jt) levivad ründeprogrammid nagu *Worm.P2P.Bare.a*, mis kopeerivad ennast huviäratava nime all (xxx.exe, msn.exe) jagatud kaustadesse, et ahvatleda teisi kasutajaid ennast alla laadima. Ka võib kahjur maskeerida end kräkiks, mis tuleb käivitada allalaaditud piraatprogrammi kasutamiseks.

Kohtvõrkudes kasutavad kahjurid nagu *W32.mumu.b* levimiseks protokolle CIFS või SMB. Nakatunud arvuti võib omakorda nakatada failiserveri, kust kahjur levib kiirelt teistesse arvutitesse.

Veebilehtede kaudu levimine on meetod, kus küberkurjategijad kasutavad ära tasuta veebimajutuse pakkujaid, laadides üles kahjurvara sisaldavaid veebilehti ning levitades hüperlinke sellistele veebilehtedele foorumites ja blogides. Ajutise veebiserverina kasutatakse tihti ka nakatatud arvuteid, samuti on võimalik hoida veebilehti mõne küberkuritegevust soosiva teenusetarnija serveris.

SQL-süstimisel (*SQL injection*) ehk **SQL-manipuleerimisel** kasutatakse ära veebilehe turvanõrkusi andmebaasipäringute sooritamisel ning süstitakse sinna ründekoodi. SQL-süstimine võimaldab ka andmevargust (isikuandmed, meiliaadressid, krediitkaardinumbrid jms). Ründe hõlbustamiseks müüakse spetsiaalseid tööriistu, keskmise hinnaga 63 dollarit, mis otsivad ja nakatavad turvaaukudega veebilehti [35].

Kiirpostiprogrammides (MSN Messenger, Yahoo! Messenger jt) levivad ussid neljal peamisel viisil: kasutades ära tootja paljastunud API-t, kasutades ära Windowsi API-t, saates õige faili asemel hüperlingi nakatunud failile või modifitseerides rakenduse teeke, et levitada ennast koos kasutaja algse sõnumiga. Näiteks *W32.Aplore.A@mm* käivitab veebiserveri pordis 8180, seejärel saadab kõigile adressaatidele AIM-kliendi aadressiraamatus sõnumi, mis sisaldab linki

nakatatud süsteemile. Uss *W32.AimVen.Worm* asendab kõik kasutaja saadetud käivitatavad failid enda koopiaga.

Suhtlusvõrkudes (Facebook, MySpace jt) levivad peamiselt JavaScripti-põhised ründeprogrammid, mis meelitavad kasutajaid kahjurit enda arvutisse paigaldama. 2007. a septembris levis keskkonnas Orkut uss *JS/Adrecl-A*, mis nakatas üle 670 000 kasutajakonto. 2008. a jaanuaris levis keskkonnas Facebook rakendus „Secret Crush", mis meelitas kasutajaid alla laadima reklaamvara. Suhtlusvõrgud on ohtudele eriti avatud, kuna nende kasutajad kalduvad üksteist vaikimisi usaldama.

Mitmeastmelise ründe puhul kasutab kahjurvara ära esimest turvanõrkust, et hõlbustada järgmiseid ründeid. Näiteks trooja hobune (sisuliselt pipett) *Farfli* rikub nakatunud süsteemi turvalisuse, seejärel laadib alla ja paigaldab muud kahjurvara.

2.6.3 Kahjud

ITU uuring tsiteerib Computer Economics korraldatud küsitluse tulemusi, kus kahjurvara tekitatud otsest ülemaailmset kahju hinnatakse 13,2 miljardile dollarile (2006), millega jätkus senine langustrend (vrd 2005 – 14,2 miljardit, 2004 – 17,5 miljardit). Otseste kulude kahanemist seletab ühelt poolt tõrjetarkvara laiaulatuslikum rakendamine, teiselt poolt kaudsete kulude kasv (vt allpool). Võrdluseks pakub FBI uuring [3], et 2005. aastal läksid raaliroimad ja tulenevad kahjud ainuüksi Ühendriikidele maksma 67,2 miljardit dollarit. Veel raskem on hinnata eraisikutele tekitatud kahjusid. 2007. aastal viis ajakiri Consumer Reports läbi 2000 osalejaga küsitluse, mille põhjal ennustati, et kahjurvara ja spämm põhjustavad Ühendriikide lõpptarbijale kahjusid 7,1 miljardi dollari väärtuses.

Lisaks otsestele kahjudele nagu tööviljakuse langus, andmetele juurdepääsu kadumine ja andmete hävimine tuleb arvestada veel mitmete kaudsete kahjudega:

- ressursikulu tõrjetegevuse tugevdamiseks (riist- ja tarkvara soetamine);
- personalikulud (IT-turvapersonali laiendamine või koolitamine);
- organisatsiooni maine kahjustumine;
- turuosa kaotus;
- töötaja materiaalsed ja moraalsed kahjud;
- psühholoogilised kahjud (võimalik umbusaldus, nõiajaht jne);
- võimalik serveri seisak;

- ressursikulu kahjustuse lokaliseerimiseks, süsteemi korrastamiseks, kontrolliks, taastamiseks või reinstalleerimiseks ja taastamatute andmete asendamiseks.

Tabelis 5 on toodud CSI andmed (kahjurvaraga seotud) turvaintsidentide arvu kohta ühes organisatsioonis aasta jooksul (vastas 250 organisatsiooni).

Tabel 5. Aastane turvaintsidentide arv 2008. a

1-5	47%
6-10	14%
> 10	13%
Ei tea	26%

Järgnev 522 organisatsiooni hõlmanud uuring [4] kajastab kahjude detailset tüüpi. Protsendid väljendavad osakaalu vastajatest, kes märkisid, et vastav rünne on neid puudutanud.

CSI andmetel arvutati 2008. aastal ühe intsidendi keskmiseks hinnaks 288 618 dollarit (vrd 2007 – 345 005 dollarit, 2006 – 167 713 dollarit). Võrdluseks võib tuua 1994. aasta, kus NCC hindas viirusekahjuks keskmiselt 6000 dollarit ehk 48 korda vähem.

Uue nähtusena on tekkinud sihipärased (ehk konkreetse organisatsiooni või spetsiifilise tööstusharu vastu suunatud) ründed. 355 vastanust 23% tabas 1–5 sihipärast rünnet, 3% tabas 6–10 rünnet ning 1% tabas rohkem kui 10 rünnet aasta jooksul [4]. Sihipärastest rünnetest räägib ka jaotis 2.8 „Hajus ummistusrünne“.

Tabel 6. Rünnete osakaal aastate lõikes

Ründe liik	2008	2007	2006	2005	2004
Teenustetõkestus	21%	25%	25%	32%	39%
Sülearvuti vargus	42%	50%	47%	48%	49%
Telefonipettus	5%	5%	8%	10%	10%
Volitamata pöördus	29%	25%	32%	32%	37%
Viirus (ussid, trooja hobused jm)	50%	52%	65%	74%	78%
Finantspettus	12%	12%	9%	7%	8%
Sisekasutaja kuritarvitus	44%	59%	42%	48%	59%
Süsteemi läbistus	13%	13%	15%	14%	17%
Sabotaaž	2%	4%	3%	2%	5%
Firmaomase teabe kaotus/vargus	9%	8%	9%	9%	10%
Juhtmevaba võrgu kuritarvitus	14%	17%	9%	16%	15%
Veebilehe näotustamine	6%	10%	6%	5%	7%
Veebirakenduse väärkasutus	11%	9%	6%	5%	10%
Robotid	20%	21%			
DNSi ründed	8%	6%			
Kiirsuhtluse kuritarvitus	21%	25%			
Paroolide väljanuhkimine	9%	10%			
Kliendi andmete kaotus/ vargus	17%	17%			

Tabelis 7 on toodud turvaintside järeltoimingud [4]. Põhjustena, miks vaid napilt veerand vastanutest raporteeris intsidentidest korrakaitsele, toodi peamiselt välja kolm: intsidendi vähene kaalukus, usu puudumine korrakaitse abisse ning hirm mainekahjude ees. Eesti oludes ei teata, kelle poole intsidendi korral pöörduda ning samuti kardetakse mainekahjude tõttu intsidentidest raporteerida.

Tabel 7. Järeltoimingud

Üritas kurjategijat tuvastada	60%
Sulges turvaauke	54%
Installeeris turvapaiku	46%
Installeeris täiendavat turvatarkvara	37%
Muutis organisatsiooni turvapoliitikat	33%
Raporteeris intsidendist korrakaitsele	27%
Jättis intsidendist väljaspoole raporteerimata	24%
Paigaldas täiendavat riistvara	23%
Küsis juriidilist nõu	18%
Muu tegevus	15%

Tabelis 8 kajastub perioodil 2007–2008 ilmunud ründetarkvara päritolumaade jaotus.

Tabel 8. Ründetarkvara päritolumaad

Riik	**2008**	**2007**
USA	37,0%	23,4%
Hiina, sh HK	27,7%	51,4%
Venemaa	9,1%	9,6%
Saksamaa	2,3%	2,3%
Lõuna-Korea	2,1%	–
Ukraina	1,8%	3,0%
UK	1,7%	0,7%
Türgi	1,5%	–
Tšehhi	1,3%	–
Tai	1,2%	–
Muud	14,3%	6,6%

2.7 Mobiilside ründed

2.7.1 Ohud

Mobiilsidega on seotud järgmised ohud.

- Telefonikõnede pealtkuulamine
- Vestluste pealtkuulamine siseruumides
  - tavalise telefoniga
  - manipuleeritud telefoniga
- Väär andmeedastus
  - sisekasutaja seadmetega
  - välise osapoole vahendusel
- Lisateenuste (SMS-teenused, m-kaubandus, m-maksed) kasutamisega seotud viiruse- ja muud ohud
- Sõnumid valehäiretega

Tabelis 9 on mobiiltelefonide kasutamist mõjutavad tüüpilised ohud.

Tabel 9. Mobiiltelefonide tüüpilised ohud

Organisatsioonilised ohud
Puudulik reeglite ja protseduuride teadmine
Puudulik IT-turvameetmete seire
Õiguste volitamata kasutamine
Inimlikud eksitused
IT-turvameetmete järgimata jätmine
Paroolide kohatu käsitsemine
Teabe hoolimatu käsitsemine
Suhtluspartnerite identiteedi puudulik kontrollimine
Tehnilised vead
Mobiilse sidevõrgu kättesaamatus
Mobiiltelefoni rike
Tahtlikud teod
Andmete või tarkvara manipuleerimine
Vargus

Pseudoviirused
(SIM-)kaartide väärkasutus
Vestluste pealtkuulamine siseruumides mobiiltelefoni abil
Mobiiltelefonide manipuleerimine
Volitamata andmeside mobiiltelefoni abil
Telefonikõnede pealtkuulamine
Mobiiltelefoni kasutusega seotud kõneandmete analüüs

2.7.2 Kahjurvara mobiiltelefonidele

2005nda aasta alguseks oli välja arenenud kolm põhilist mobiiltelefonide kahjurvara liiki:

- ussid, mis levivad nutitelefonide protokollide ja teenuste kaudu;
- vandalismieesmärgiga trooja hobused, mis kasutavad ära operatsioonisüsteemi Symbian projekteerimisvigu;
- trooja hobused, mis on projekteeritud finantskasu eesmärgil.

Kõige esimeseks mobiiltelefonidele kirjutatud kahjuriks peetakse protokolli Bluetooth kaudu levivat ussi *Cabir*, mille häkkerigrupp 29A kirjutas idee tõestusena 2004. a juulis. 2006. a augustis oli teada 170 mobiilikahjurit ja 31 kahjurite perekonda [14]; kahjuritest tuntumad on *Duts*, *Skulls* ja MMS-sõnumitega levinud *CommWarrior*. Võrreldes PC-ga on mobiilikahjurite arv veel väike, kuid arvestades nutitelefonide kasvavat populaarsust, on oodata selle kasvu. Samuti muutub kahjurvara multiplatvormseks: nt *Trojan-SMS.J2ME* ohustab kõiki telefone (mitte üksnes nutitelefone), mis käitavad Java virtuaalmasinat.

Kahjurvaral võivad olla järgmised eesmärgid:

- levida Bluetoothi ja MMS-sõnumite kaudu,
- saata SMS-sõnumeid,
- nakatada telefonis olevaid faile,
- võimaldada telefoni üle kaugkontrolli,
- asendada ikoone või süsteemseid rakendusi,
- paigaldada võlts- või mittetöötavaid fonte ja rakendusi,
- takistada viirusetõrjeprogramme,
- paigaldada pahatahtlikke programme,

- tõkestada ligipääsu mälukaartidele,
- varastada andmeid.

Kahjurvara töömeetodeid:

- kõnede tegemine tasulistele numbritele (uss *WinCE.Pmcryptic.A*);
- SMSide saatmine tasulistele numbritele (trooja hobuste perekond *SMS.Python.Flocker*, trooja hobune *SMS.J2ME.Swapi.g*). Pettur, kellele number kuulub, võib teenida isegi poole iga sõnumi hinnast;
- SMSide saatmine vandalismieesmärgil (viirus *Mosquit.a*, mis oli maskeeritud kahjutuks telefonimänguks, aga hakkas ühel hetkel saatma SMSe kõigile adressaatidele telefoniraamatus);
- telefoni tarkvara rikkumine (trooja hobune *Skuller.a* kasutas ära platvormi Symbian nõrkust ja kustutas teatud rakenduste faile, mistõttu telefon lakkas töötamast pärast väljalülitamist; *Curse of Silence* kasutas ära Nokia S60-seeria nõrkust, mis võimaldab sobivalt konstrueeritud sõnumiga muuta ohvri telefoni võimetuks edasisi SMS-e saama).

Mobiiltelefonide kahjurvara (eelkõige trooja hobuste) **levikuviiside** seas on esikohal WAP-portaalid, mis pakuvad kasutajale helinate ja mängude jt rakenduste allalaadimist. Enamik trooja hobuseid on maskeeritud kas rakendusteks, mis lubavad tasuta SMSide saatmist või tasuta Interneti kasutamist, või pornograafilist laadi rakendusteks. Kahjurvara levitavaid saite massreklaamitakse foorumites ning Venemaal ja teistes SRÜ riikides ka populaarse kiirpostiprogrammi ICQ kaudu.

2.8 Hajus ummistusrünne

Hajus ummistusrünne (*Distributed Denial-of-Service attack*, **DDoS**) on korraga mitut ründeallikat kasutav arvutisüsteemi või välisvõrguühenduse tahtlik ülekoormamine eesmärgiga kutsuda esile süsteemi krahh, seiskumine või käideldavuse langus.

Ründe käigus suunatakse ohvrile rämpsandmete voog, mille töötlemine kas ummistab tema võrguühenduse või koormab ta ressursid üle, nii et ohver ei saa kas üldse või mõistliku aja jooksul vastata legitiimsete kasutajate päringutele. Ründe sooritamiseks kasutatakse harilikult robotivõrku (vt 2.9) ning spetsiaalseid ründevahendeid nagu *Stacheldraht*. Kuna rünnak lähtub väga erinevatest võrgupunktidest ning kasutatakse IP-tüssamist (*IP spoofing*), on ohvril võimatu ründeallikat kindlaks teha ning väga keeruline rünnet tõrjuda.

Ründel võivad olla järgmised eesmärgid.

- **Väljapressimine**. Ettevõtetele, kelle käive on otseses seoses arvutisüsteemide talitlusega (nt e-kaubandus ja võrgukasiinod), tähendaks ummistusrünne otsest rahalist kahju; seda teades võib kurjategija kasutada ummistusründega ähvardamist väljapressimiseks. Näiteks vangistati 2006. a grupp Vene küberkurjategijaid, kes ummistusründe ähvardusel olid mitmetelt Briti võrgukasiinodelt välja pressinud ligi 2,8 miljonit naelsterlingit.
- **Poliitilised või ideoloogilised motiivid**. Rünnatakse organisatsioone, kelle tegevused või vaated pole vastuvõetavad, näiteks valitsusasutuste veebisaidid või uudisteportaalid.
- **Oma oskuste tõendamine**
- **Kättemaks**. Rünnatakse kurjategijate tegevust häirivaid organisatsioone, nt spämmi vastu võitlejaid (Blue Security juhtum 2006).

Põhilised ründemeetodid on järgmised.

SYN-tulve (*SYN flood*) kasutab ära protokolli TCP nõrkust. Ründe käigus algatab klient (ründaja) serveriga (ohver) TCP-ühenduse, saates talle võltsitud lähteaadressiga paketi SYN. Server talletab uue ühenduse andmed ja üritab kliendile vastata paketiga SYN-ACK, kuid ei saa vastust, mistõttu ühendus jääb "poolavatuks". Kuna poolavatud ühendusi tekitab samaaegselt väga palju kliente, ei suuda server uutele (sh legitiimsetele) ühenduskatsetele enam vastata ning muutub kättesaamatuks, kuni avatud ühendused aeguvad.

ICMP-tulve (*ICMP flood, „Smurf" attack*) kasutab ründe võimendamiseks halvastikonfigureeritud marsruuterit. Ründaja saadab mõne marsruuteri leviaadressile võltsitud (st ohvri) lähteaadressiga ICMP-kajapäringu. Kui marsruuter on halvasti konfigureeritud, edastab ta kajapäringu kõigile (alam)võrgu arvutitele, mis omakorda saadavad ohvrile vastustetulva. Näiteks kui ründaja saadab 100 arvutiga võrku kajapakette kiirusel 100 Kbit/s, siis ohvrit tabab paketitulv mahus 10 Mbit/s. Rünnet, mis kasutab ICMP asemel UDP-kajapakette, nimetatakse ka *fraggle*-ründeks.

ICMP-tulve üks edasiarendusi on nn **DNSi võimendusrünne** (*DNS amplification attack*). See ründeviis kasutab ära valestikonfigureeritud nimeservereid, võltsitud UDP-pakette ja olukorda, kus nimeserver saadab väikesele päringule (nt 60 bit) palju suurema vastuse (nt 4300 bit). Ründamiseks saadab kurjategija nimeserverile tuhandeid võltsitud (st ohvri) lähteaadressiga rekursiivseid päringuid. Nimeserver saadab päringute töötlemise tulemusel ohvrile vastusetulva, mis ummistab tema võrguühenduse. Ründe muudavad tõhusamaks suurte päringuvastuste saatmisel fragmenteeruvad IP-paketid.

Hajusa ummistusründe eriliik on nn **degradeerimisrünne** (*pulsing flood, degradation-of-service attack*), mille eesmärk on ohvri veebisaidi kättesaadavuse häirimine. Sellise ründe puhul tulvatakse ohvri veebisaiti lühikeste vahelduvate impulssidega pikema aja jooksul, mis võib põhjustada rohkemgi kahju kui ühekordne suur ummistus.

HTTP-tulve (*HTTP flood*) on kõrgema taseme rünne, kus ohvri veebiserver või -rakendus ummistatakse harilike HTTP-päringutega. Sama päringumahu juures võimaldab see veebiservereid tõhusamalt üle koormata kui teised nimetatud ründed; ka on peaaegu võimatu eristada ründaja päringuid legitiimsetest päringutest.

Alljärgnev tabel kajastab hajusate ummistusrünnete mahu kasvu maailmas [39].

Tabel 10. Ummistusrünnete maht

Aasta	Suurim liiklusvoog, Gbit/s
2001	0,4
2002	1,2
2003	2,5
2004	10
2005	17
2006	24
2007	40

Üks tuntumaid ründejuhtumeid toimus 2004. aastal, kui ussiga *MyDoom* nakatunud arvutid aktiveerusid ettemääratud kuupäeval ja sooritasid hajusa ummistusründe SCO Groupi veebisaidi vastu.

Hajus ummistusrünne võib toimuda ka kuritahtliku kavatsuseta, näiteks kui ootamatult populaarseks muutunud veebisaiti tabab liiga suur liiklusvoog (nn Slashdoti efekt).

2.9 Robotivõrgud

Robotivõrk *(botnet)* on kahjurvaraga nakatatud arvutitest koosnev võrk, mis on küberkurjategija (*bot-herder*, robotikarjus) kontrolli all.

Robotivõrkude eesmärk on

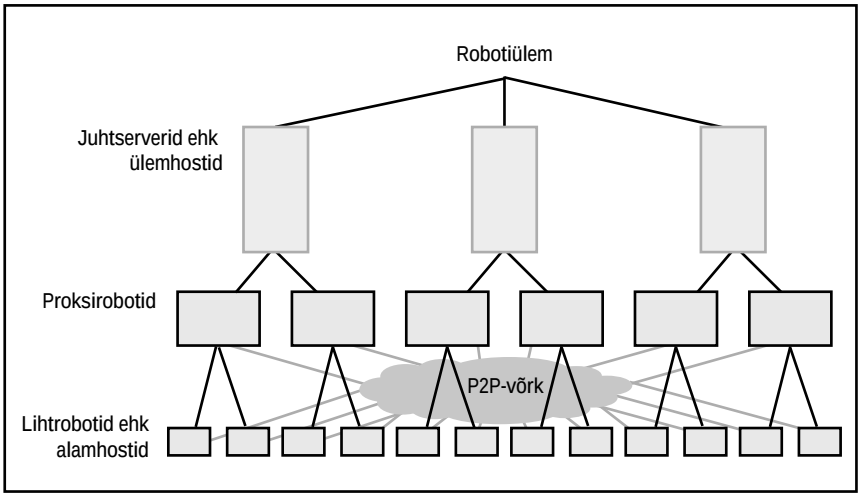
- levimine (uute hostide nakatamine),
- hajusad ummistusründed,
- identiteedivargus,
- kahjurvara levitamine,
- spämmimine (ravimite müük, finantspettused, andmepüük, rahapesijate värbamine).

Robotivõrkude arengus võib eristada kolme põlvkonda. Nn esimese põlvkonna robotivõrgud olid väikesed ning keskse käsijuhtimisega. Ründaja pidi saama juurdepääsu igasse arvutisse, et paigaldada sinna kontrolliprogramm. Teise põlvkonna robotivõrgud olid poolautonoomsed – roboteid juhiti eraldi punktidest, iga võrgusegmendi eest vastutas üks juhtserver ning võrgu omanik andis käsklusi juhtserveritele, mitte enam igale arvutile eraldi. Kolmanda põlvkonnaga, millele pani aluse uss *Storm*, ilmusid täisautonoomsed robotivõrgud, mida iseloomustavad järgmised omadused ([6] põhjal):

- nakatunud hostid sondeerivad ja vallutavad järgmisi turvanõrkustega hoste;
- nakatunud hostid kontrollivad regulaarselt enda „tervist“ (portide avatust ja internetiühenduse toimivust) ning raporteerivad sellest nn ülemhostidele (*supernode*);
- ülemhostid jagavad alamhostidele (harilikele nakkuskandjatele) töökäske ja pakuvad nimelahenduse teenust;
- nakatunud hostid teevad enda maskeerimiseks spämmi levitamisse pause;
- terve võrgusegment „uinub“ teatud ajaks, samuti maskeerimiseks;
- automaatne statistika kogumine rünnete efektiivsuse kohta nende peenhäälestamiseks;
- automaatne ummistusründe sooritamine teatud hostide vastu, mis külastavad nakatunud saite kahtlaselt tihti (pms kahjurvara uurivad organisatsioonid);
- automaatne uute robotite leidmine, kui senised hostid puhastatakse kahjurist või lahkuvad võrgust;

- avaliku võtme krüptograafia kasutamine, mis võimaldab muuhulgas võrgusegmente välja rentida;
- aadressi kiirvahetuse meetodi kasutamine (vt allpool).

Ühe võimaliku vaate tüüpilise robotivõrgu arhitektuurile esitab joonis 3.



Joonis 3. Robotivõrgu arhitektuur

Kui varasemalt kasutati robotivõrgu liikmete juhtimiseks protokolli IRC (üks esimesi selliseid oli 1999. a ilmunud kahjurvara *PrettyPark*, mis sisaldas IRC-põhist tagaust), siis praegusajal on levinud HTTP- või P2P-tüüpi protokollid. P2P-robotivõrgud kasutavad harilikult nn aadressi kiirvahetuse *(fast-flux)* meetodit, millega registreeritakse DNS-nimele vastav aadress ümber iga paari minuti järel. See tähendab, et teatud kahjurvara levitav veebisait, kuhu ohvrid suunatakse, jääb nime poolest samaks, kuid vahetab nii tihti aadressi, et teda sulgeda on praktiliselt võimatu. Aadressiloendis, milles võib olla sadu tuhandeid kirjeid, on harilikult teised robotivõrku hõivatud arvutid.

Üks tuntumatest robotivõrkudest on *Storm*, mis tekkis 2007. a jaanuaris, kui kahjur *Storm Worm* kasutas ära operatsioonisüsteemi Windows turvaauke ning tekitas ligi miljonist nakatunud arvutist koosneva P2P-robotivõrgu. 2009. aastal kerkis esile uus robotivõrk *Conficker* (ehk *Downadup*), mille tekitas samanimeline uss, nakatades ligi 10 miljonit arvutit. Teised tuntud robotivõrgud on *Srizbi* (ehk Zlob), *Rustock*, *Mega-D* ja *Dedler*. Muuhulgas läheb neist esimese kahe arvele üle 60% kogu robotivõrkude kaudu saadetud spämmist ([22] viitega *Leyden*, 2008).

Sealjuures on spämmimise kaudu ravimite müük näiteks Stormi põhiline tuluallikas [6]. Nn „Canadian Pharmacy“ veebisaidi reklaamimiseks rakendatakse rohkem kui 100 000 robotit, mis saadavad päevas 1,5 miljardit spämmisõnumit. Üldjuhul jõuavad tellitud ravimid ka tellijani (ehkki need on Hiina ja India võltsravimid), mistõttu „Canadian Pharmacy“ käibeks pakutakse 150 miljonit dollarit aastas. Saadud raha kasutatakse robotivõrgu ja uute rünnete arendamiseks. Suurt lisatulu pakub ka robotivõrgu väljarentimine. Kasutades avaliku võtmega krüptograafiat, on võimalik jaotada miljonitest arvutitest koosnev robotivõrk väiksemateks segmentideks, mida välja rentida spämmikampaaniaks, ummistusrünneteks jne. ITU andmetel maksab robotivõrgu rentimine 50–60 dollarit 1000–2000 roboti eest; renditasuna võetakse vastu ka varastatud krediitkaardinumbreid.

Kuna nüüdsed robotivõrgud pole keskselt juhitud ning nad kasutavad mitmesuguseid krüpteerimis- ja maskeerimistehnikaid, on neid sulgeda äärmiselt raske kui mitte võimatu. Näiteks *Srizbi* kliendid genereerivad teatud algoritmi alusel unikaalseid domeeninimesid (ypouaypu.com jms) ja üritavad nendega ühenduda, kasutades autentimiseks avaliku võtmega krüptograafiat. See tagab, et kurjategijad saavad varem või hiljem kontrolli robotivõrgu üle tagasi, registreerides õigel hetkel vastava domeeninime ja seades sinna üles juhtserveri.

2.10 Rämpspost

Rämpspost (*unsolicited bulk e-mail*, „soovimatu massiline postireklaam“) ehk spämm on reklaamsisuga meil, mis on masspostitatud selleks mitte luba andnud adressaatidele. Lisaks meilile ja Usenetile levib spämm tänapäeval ka kiirpostiprogrammides (*instant messaging spam* ehk „spim“), mobiiltelefonides (m-spämm), blogides ja protokolli VoIP kaudu (*spam over Internet Telephony* ehk „spit“).

Eesmärgilt liigitub rämpspost kolmeks:

- mingi toote (nt ravimid ja võlts-luksuskaubad) või teenuse (nt finantsteenused) reklaamimine või müümine. Kasumit teenitakse, kuna kaubad on tihti disaineritoodete odavad võltsingud;
- kasutaja arvuti nakatamine (nt *Storm Worm*). Nakatatud ja robotivõrku kaasatud arvutit saavad kurjategijad kasutada näiteks meilivahendajana;
- krediitkaardi- ja isikuandmete väljapetmine identiteedivarguse eesmärgil.

Rämpsposti levikule aitavad kaasa

- tema odavus,
- tema tasuvus,
- turvaaukudega koduarvutid, mis haaratakse robotivõrku ja pannakse rämpsposti saatma,
- avatud meiliserverid (*open relays*), mis võimaldavad kolmandatel osapooltel enda kaudu meili saata,
- avalikud WiFi-punktid.

Inimeste lõksumeelitamiseks kasutavad spämmijad päevakajalisi teemasid (nt USA presidendivalimiste ajal ahvatleti “skandaalsete” lugudega ning majanduslanguse ajal pakutakse võimalusi lisateenistuseks). Sophos Labs 2007. a küsitluse põhjal on spämmis reklaamitavaid kaupu ostnud 11% spämmi saajatest.

ITU (viitega *Ferris Research*, 2007) hindab spämmi globaalseks maksumuseks ärikasutajatele 100 miljardit dollarit (st kulud spämmitõrje riistvarale ja tarkvarale, tööseisakud ja tööviljakuse langus, kulud töötajate koolitamisele jpm), millest 35 miljardit moodustavad USA kahjud [22]. Sama uuring (viitega *Nucleus Research*, 2007) hindab spämmi haldamise kuludeks 712 dollarit ühe töötaja kohta ning 71 miljardit dollarit USA ettevõttete peale kokku.

Spämmi osakaaluks kõikidest meilidest pakutakse sõltuvalt infoallikast ja analüüsimeetodist 85–95 protsenti. Näiteks ühenduse MAAWG andmeil, mis saab andmeid ligi 240 miljonit meilikontot teenindavatelt Interneti teenusetarnijatelt, moodustas spämm 2007. aasta II kvartalis 86,7% kõigist meilidest ning arvestades kasutatud metoodikat, võib seda pidada statistiliseks alampiiriks [22]. Andmeid kinnitab MessageLabs uuring, mille järgi moodustas spämm 2007. aastal 84,6% kõigist meilidest.

Enam kui 80% kogu spämmist levitavad robotivõrgud, mis tekivad selleks spetsiaalselt loodud viirusetüvedest. Selle esimeseks näiteks on 2003. a levinud viirus *Sobig*, millest alates on kõik suuremad viirusepuhangud ajendatud robotivõrkude loomise ja nende kaudu spämmi saatmise eesmärgist.

Kasvab ka m-spämmi osakaal. ITU järgi saadeti 2006. aastal USA abonentidele 0,8 miljonit spämmisõnumit, 2007. aastal 1,1 miljonit ning 2008. aastal 1,5 miljonit [22].

Tabel 11 esitab rämpsposti osakaalu liigiti [36].

Tabel 11. Rämpsposti osakaal

Kategooria	**2009 I kv**	**2008**
Internet: veebihosting, veebikujundus, spämmivahendid	24%	23%
Tooted: koduelektroonika, riided	18%	28%
Vaba aeg: võrgukasiinod, mängud, puhkusepakkumised	18%	6%
Tervis: farmaatsiatooted, looduslikud ravimid	11%	8%
Rahandus: investeerimine, laenud, kinnisvara	10%	12%
Pettus: krediitkaardi verifitseerimine, teadaanded pangakonto kohta	7%	6%
Tüssamine: Nigeeria investeeringud, püramiidskeemid	6%	10%
Täiskasvanutele: pornograafia, tutvumiskuulutused, suhtenõuanded	6%	7%

Kaua aega spämmerite seas populaarne olnud *pump-and-dump* strateegia (rämpsaktsiate hinna manipuleerimine) sai 2007. a tagasilöögi, kui USA väärtpaberituru järelevalveorgan SEC peatas kauplemise hangeldamise aluseks olevate firmade aktsiatega.

Rämpsposti levikut uurides tuleb arvestada, et spämmerid üritavad varjata või võltsida oma tegelikku asukohta. Musta nimekirja sattumise vältimiseks kasutavad spämmerid meilivahenduseks trooja hobusega nakatatud arvuteid, mis on valitud piirkondadest, kus Interneti ühenduskiirus võimaldab saata meile kõige

suuremas mahus. Seetõttu pole allolevas jt sarnastes tabelites kindlat seost spämmi päritolumaa ning spämmerite asukoha vahel.

Tabelis 12 on toodud peamised spämmi vahendavad riigid.

Tabel 12. Spämmi päritolumaad

Riik	2008	2007
USA	17,5%	22,5%
Venemaa	7,8%	4,7%
Türgi	6,9%	3,1%
Hiina, sh HK	6,0%	6,0%
Brasiilia	4,4%	3,8%
Lõuna-Korea	3,7%	6,5%
Itaalia	3,3%	2,7%
UK	3,1%	–
Poola	3,0%	4,9%
India	2,9%	2,6%
Hispaania	2,8%	2,7%
Saksamaa	2,7%	3,5%
Muud	35,9%	33,5%

Ka päritolumaade osas läheb statistika lahku: nii näiteks on Symantec Corporationi 2008. a andmetel esikolmik USA (42%), UK (5%) ja Venemaa (4%) [35].

3 TURVAAUGUD

Nõrkus ehk turvaauk (*vulnerability*) on kaitstava objekti suvaline nõrk koht, mille kaudu saab realiseeruda objekti varasid ähvardav oht. Mõned standardmääratlused eristavad (infovara) turvaauku ja (turvameetmete) nõrkust, mõned defineerivad nõrkust turvameetmete kaudu, mõned ei tee vahet ohul ja nõrkusel. Sageli analüüsitakse nõrkusi puuduvate turvamehhanismide terminites. Nõrkused suurendavad riski, sest nad "lubavad" ohul kahjustada objekti. See peatükk annab turvaaukudest süstemaatilise ülevaate.

3.1 Infrastruktuuri nõrkused

Infrastruktuuri hulka liigitatakse eelkõige hooned ja ruumid, aga ka side- ja elektrikaablid ning nendega seotud kaitsekapid.

3.1.1 Kaitstava objekti ebasoodne asukoht

võib suurendada kõigi eespool loetletud stiihiliste ohtude või mõnede ründeohtude (murdvargus või vandalism äärelinnas) realiseerumise tõenäosust, aga ka lisada spetsiifilisi keskkonnaohte (keemiline saaste vastava ettevõtte naabruses, rasked liiklusõnnetused magistraalristmiku vahetus läheduses ning mitmesugused kaevetöödest tulenevad ohud: sideliinide rikkumine, ehitisele struktuursete kahjude tekitamine, töökeskkonna saastamine jm).

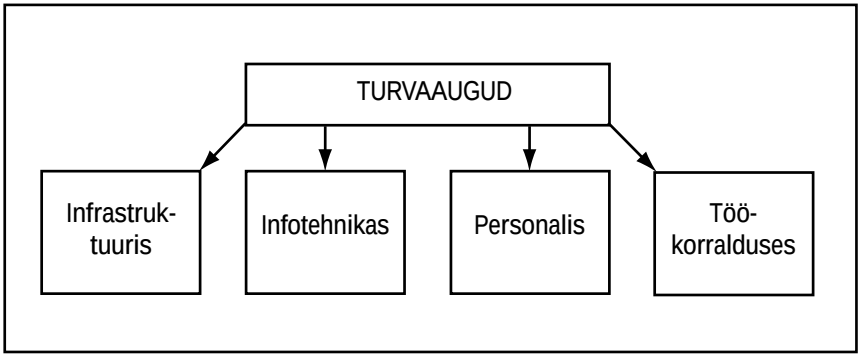
3.1.2 Primitiivne või amortiseerunud infrastruktuur

ei paku adekvaatset kaitset stiihiliste ohtude ega füüsiliste rünnete eest ning ei võimalda realiseerida mitmeid organisatsioonilisi ja infotehnilisi turvameetmeid, näiteks sissepääsu reguleerimisega seotuid.

3.1.3 Sidesüsteemi või infrastruktuuri puudused

Eravõrk tagab andmete turvalisuse kindlamalt kui avalik võrk. Kaabelvõrke peetakse kindlamaks kui traadita võrke. Traadita võrgud sõltuvad rohkem keskkonnast ja on avatumad pealtkuulamisele.

Võrreldes statsionaarsete võrkudega, on traadita kohtvõrgu komponente hõlpsam rünnata (nt võlts ühenduspunkt, vahendusrünne, teenusetõkestus).



Joonis 4. Turvaaukude paiknemisalad

3.2 Infotehnilised nõrkused

3.2.1 Piiratud ressursid

(toiteallika laeng, riistvara jõudlus, edastussüsteemi läbilaskevõime, andmekandja salvestusmaht jne) ohustavad ammendumisel eeskätt käideldavust, aga ka andmeterviklust. Ketta täitumise tõttu võivad kaotsi minna näiteks sisenev meil või revisjoniandmed. Infokadu tekib ka automaatvastaja salvestuskandja täitumisel. Sisemise toiteallika tühjenemisega tuleb arvestada peamiselt sülearvutite jm mobiilseadmete, aga ka näiteks automaatvastaja (avariipatarei) puhul.

3.2.2 Aparatuuri või sideliinide väär paigaldus

võimaldab realiseeruda mitmetel keskkonnaohtudel (veekahjustused, termiline toime, tolm, indutseeritud häired jne), füüsilistel rünnetel ning andmeluurel (ekraani jälgimine kõrvalt, sideliinide pealtkuulamine).

3.2.3 Parasiitkiirgus

Kõik seadmed ja neid ühendavad kaablid kiirgavad elektromagnetlaineid, mis võimaldab infopüüki. Parasiitkiirgusega analoogkiirgus on raadiovõrgu kiirgus väljapoole. Kasutades WLAN-kaardiga sülearvutit ja tasuta tarkvara, on võimalik leida puudulikult turvatud traadita võrke, mida saab ära kasutada näiteks anonüümseks spämmi saatmiseks.

3.2.4 Vead, defektid või dokumenteerimata omadused programmides

võivad tekitada mitte ainult stiihilisi tõrkeid (teatav sõna võib spelleri rippuma jätta jne), vaid ka turvaauke rünnete suhtes. Läbi aastate on avastatud turvadefekte brauseris Internet Explorer ja tõsiseid turvaauke operatsioonisüsteemis Windows. Nagu ikka, on juhuslikest programmivigadest märksa kaalukamad ja raskemini kõrvaldatavad programmide projekteerimise vead.

3.2.5 Algoritmide, protokollide ja sideprotseduuride puudused

Turvaauke võivad pakkuda näiteks keerukad kaugpääsu võimalused võrgustatud Unix-süsteemis. Autentimisvõimaluse puudumine X-serveri ja -kliendi vahel an-

nab kõigile X-Windowsi kasutajaile juurdepääsu kõigile ressurssidele, võimaldades näiteks saada koopiaid teise arvuti kuvadest. Autentimisvõimaluse puudumine NIS-serveri ja -kliendi vahel võimaldab kliendil saada piiramatu juurdepääsu serveril olevale informatsioonile.

Puuduste seas on muuhulgas järgmised:

- autentimise puudumine või puudulikkus (halvad paroolid, protseduuride turvaaugud);
- sidepartnerite puudulik autentimine (nt telefoni ja meili kasutamisel);
- nõrk autentimismeetod traadita kohtvõrgus (nt protokoll WEP);
- ebaturvalised protokollid avalikes võrkudes;
- krüptomooduli tõrge (tehniline rike, toitekatkestus, inimviga, rünne);
- vananenud krüptomeetodid;
- vead kodeeritud andmetes (edastusviga, salvestuskandja defekt).

3.2.6 Andmehalduse puudused

alates ebasobivatest andmevormingutest ja andmete ebaratsionaalsest struktureerimisest (mille tõttu on võib-olla raske isoleerida salajasi andmeid avalikest) ning lõpetades varukoopiate puudumisega, tähendavad riskimist asutuse peamise infovaraga. Andmehaldust raskendavad ka arhiivide indekseerimisvõtmete puudused, arhiivisüsteemi migreerimise puudused ja ebasobiva andmekandja kasutamine arhiveerimiseks.

3.2.7 Vahendite ja meetmete tülikus

võib ilmneda nii infotehnoloogilistes tööprotsessides kui ka turvasüsteemides. Sobimatud juht- või indikatsiooniseadised (nt sobimatu märgistikuga või märkide halva paigutusega klaviatuur, tuhm vedelkristallnäidik jne) ja vääralt projekteeritud või keelelt sobimatud kasutajaliidesed suurendavad inimvigade tõenäosust. Ebamugavaid või ülepingutatud turvameetmeid hakatakse tõenäoliselt sageli ignoreerima.

Puuduste seas on muuhulgas järgmised:

- andmebaasikasutajate vahetumise halb korraldus (seansi sulgemata jätmisel võidakse baasis teostada muudatusi eelneva kasutaja nimel);
- andmebaasihalduri keerukus (ebasobivus, väär install);

- andmebaasipöörduse keerukus;
- tulemusteta otsingud (ajakaod veebist otsimisel).

3.2.8 Seadmete ja vahendite mobiilsusest tulenevad ohud,

eeskätt tundlikkus keskkonnategurite suhtes. Võimalikud on ka füüsilised ründed ning oht, et pideva võrguühenduse puudumise tõttu hilineb andmete või olulise tarkvara automaatne uuendamine. Arvestada tuleb toiteallika vajadusega ja seadme või vahendi napimate ressurssidega võrreldes paikse seadme või vahendiga.

3.3 Personali nõrkused

Personalinõrkusi võib käsitleda ükskõik millise muu nõrkuse raames, kuna infoturbe ülesehitus ja toimimine on otseses sõltuvuses inimfaktorist. Seetõttu on järgnevad nõrkuste grupid kohati kattuvad. Personalinõrkuste avaldumine sõltub ka õigusaktide-alasest teavitamisest ja koolitusest ning organisatsiooni sisedistsipliinist.

3.3.1 Väärad menetlused

on teadmatusest või mugavusest tulenevad süstemaatilised toimimisvead, näiteks:

- failisüsteemide väär eksport Unixi all jätab failid kaitsetuks (täielikult on kaitstud ainult juurkasutajale *(root)* kuuluvad failid);
- andmekandja riskantne saatmine (võib minna kaotsi pakendi rebenemisel, dokumente sisaldavast suurest ümbrikust ei leita CD-ketast jne);
- faksi juriidilise siduvuse ülehindamine (kohtuvaidlustes ei tarvitseta faksisõnumit arvestada dokumendina);
- ühenduse lahutamata jäämine (ISDN-adapter);
- krüptomoodulite väär kasutamine (vead parameetrite sisestusel ja tööviisi valimisel);
- indeksiandmete halb sünkroniseerimine arhiveerimisel;
- andmebaaside sünkroniseerimisviga;
- vead mobiilseadmete sünkroniseerimisel;

- andmekappide sihilik väärkasutus mugavuspõhjustel (koodluku lahtijätmine).

3.3.2 Teadmatus ja motivatsioonitus

on turvaauk mitte ainult infotehnika kasutajate, vaid ka näiteks koristajate ja väljastpoolt kutsutavate või saadetud töötajate puhul. Juhendamatuse ja järelevalvetuse korral võivad nende tegutsemisega kaasneda ühenduste lahutamine, koristusveega tekitatud kahjustused, dokumentide või andmekandjate äraviskamine, katsed arvutitel mängida jne.

Puuduste seas on muuhulgas järgmised:

- andmekandjate ja dokumentide puudulik hävitamine kodutöökohas;
- sündmuste väär tõlgendamine (nt sissetungi tuvastamise süsteemis *(IDS)* väärignoreeringud või väärtuvastused);
- konfidentsiaalsuse kadu peidetud andmeosade kaudu (andmete üleandmisel);
- andmete kogemata manipuleerimine (oskamatus, teadmatus, liigsed õigused, hooletus);
- väljasttellimisprojekti negatiivne mõju organisatsiooni personalile.

3.3.3 Turvanõuete eiramine

Levinumad juhtumid on järgmised.

- Hooletus üldiste turvameetmete suhtes (võtmete hoidmine “mati all”, parooli jätmine lauale, varunduse vahelejätt, sissepääsuvõimalus tagaukse kaudu)
- Andmete konfidentsiaalsuse kadu infotehnoloogia kasutaja hooletuse tõttu (prinditud dokumendi unustamine printerisse, konfidentsiaalsete andmete avakujul transportimine mälupulgal)
- Infotehnoloogilise süsteemi turvatehniliselt väär kasutamine (liiga lihtsad paroolid, süsteemi lahtijätt lahkumisel, vaba juurdepääs varukoopiatele)
- Väär PC kasutajate vahetumine (välja- ja sisselogimiseta, nii et vastavad revisjoniandmed jäävad puudu)
- Infotehnoloogilise süsteemi väär haldus (väär installeerimine, pääsuõiguste liiga lõtv jagamine, logi puudumine)
- Väär pääsuõiguste haldus (võimalus kustutada logiandmeid, töö tegemiseks piisamatud pääsuõigused)
- Arhiivi andmekandja volitamata ülekirjutus või kustutus

- Infoturbe puudulik aktsepteerimine (paroolide üleskirjutamine jms)
- Meiliteenuste väärkasutus (saatja või saaja tööjaamas, sisevõrgus, meiliserveris)
- Töötava haldusserveri blokeerimine (tehingumehhanismi puudumisel tervikluserike)
- Puudulik infoturve väljasttellimise teostusjärgus
- Arhiivide andmekandjate puudulik hävitamine
- Andmete konfidentsiaalsuse või tervikluse kadu kasutaja vea tõttu (print jäi printerisse, andmeid ei kustutatud mälupulgalt)
- Õigusaktide ja lepingute sätete rikkumine (nt puuduliku turbe tõttu)
- Mehaaniliste koodlukkude võtmete väär kasutamine, eriti koodi muutmisel
- Registreerimata komponentide kasutamine (algparoolid võivad jääda muutmata)
- Vead kaugpöörduse autentimisteenuse kasutamisel (autentimisandmete lokaalne salvestus)
- Puudulik paroolihaldus (harv vahetamine, lohakas hoidmine jne)
- Andmebaasisüsteemi hooletu haldus (liigsed õigused, seire puudumine, harv varukopeerimine)
- Teabe hooletu kasutamine (väljalobisemine, hävitamata jätmine, sülearvuti laokilejätt jms)

Turvanõuete eiramine (sh turvaintsidendile reageerimata jätmine või selle varjamine) võib tuleneda vähesest teadlikkusest või puudulikust töökultuurist; ka on võimalik, et töötajad tajuvad turvanõudeid ebamugavate või ülepingutatuna.

3.4 Organisatsioonilised nõrkused

Ohtude realiseerumist soodustavad asutuse üldise töökorralduse ning infotehniliste ja turvalahenduste valimise ja kasutamise puudused.

3.4.1 Turbekorralduse puudused

- Infoturbe puudulik teadvustamine
- Sõnastamata või ebapiisav võrgu- ja süsteemihalduse strateegia
- Ressursside ebaökonoomne kasutamine puuduliku infoturbehalduse tõttu
- Sõltuvus välisest teenusetarnijast
- Välise teenusetarnija nõrkused
- Puudused välise tarnijaga sõlmitud lepingu tingimustes
- Halb väljasttellimise strateegia
- Halvad väljasttellimisprojekti lõpetamise sätted
- Puudulik turvaintsidentide käsitlus (aeglane reageerimine, vead pressisuhtluses jms)
- Puudulikud varunduse ja taaste protseduurid
- Tarkvara projekteerimisviga (protokollide ebaturvalisus; tüssamise ja spämmi võimalused)
- Mobiil- ja kaugtöö korraldamatus
- Tööprotsesside häiringud infoturbeintsidentide tõttu (nt teenus katkeb)

3.4.2 Töökorralduse puudused

- Iga kaitstava objekti suurim ohuallikas on reeglite (ametijuhendite, sisekorra- ja ohutuseeskirjade, ressursihalduse reeglite, turvapoliitika, info- ja turvasüsteemide haldusjuhendite jms) puudumine või puudulikkus.
- Reeglite puudulik tundmine, st töötajate piisamatu informeerimine ja koolitus
- Halb kohanemine infotehnoloogia või infrastruktuuri muutustega (uued vahendid, kolimine). Organisatsioonilist kohanemist nõuab ka turvameetmete kasutussevõtt – alates võtmeisikute või nende asendajate kättesaadavusest, paroole edasi andmata puhkuselemineku vältimisest jne.

- Infotehnoloogia halb tõhusus ja sagedad vead halbade töötingimuste tõttu (ergonoomia, mikrokliima, valgustus, klientide sagimine tööruumides)
- Volitamatud toimingud. Näiteks võib töötajate vaba pääs andme- või dokumendiarhiivi tekitada arhivaari eemalviibimise ajal segaduse ning põhjustada käideldavuse langust või konfidentsiaalsuse kadu.
- Andmekandjate saatmise korraldamatuse tagajärgedeks võivad olla väär aadress, ebaturvaline pakend või saadetise hilinemine.
- Struktureerimata andmekorraldus (kataloogisüsteem, versioonid, nimetused jne)
- Puudulik andmebaasi versiooniuuenduste organiseerimine
- Vead kaugpöörduse halduses (regulaarse varundamise puudumine, ribalaiuse raiskamine jms)
- Kaugtöötajate asendamise puudulikud eeskirjad
- Elektronposti aja autentimise puudumine (võimaldab võltsingut, pettust, salgamist)
- Elektronposti reguleerimata kasutamine (vastutus, aadressi ja vormingu õigsus)
- Sideliinide kontrollimatu kasutamine (väär faksi- või modemiplaatide häälestus)
- Puudulik auditeerimine
- Arhiivisäilikute digitaalsignatuuride regenereerimise puudused
- Paberdokumentide elektroonilise arhiveerimise puudused
- Aegunud või väär teave veebisaidis
- Õiguslike nõuete rikkumine arhiivisüsteemide kasutamisel

3.4.3 Ressursihalduse puudused

- Puuduvad, puudulikud või ühildamatud ressursid: programmi jaoks liiga nõrk arvuti, kaabel sobimatut tüüpi pistikutega, tähtajaks maksmata jäänud liiniüür, IT-materjalide pideva varu puudumine jne.
- Hoolduse puudumine või puudulikkus. Puudutab näiteks puhvertoiteallika (UPS) akude regulaarset laadimist, elektromehaaniliste seadmete (printer, paljundi, skanner, faks jt) puhastust, tulekustutite pidevat töökõlblikkust jms.

- Ressursside kontrollimatu kasutamine: isiklikud mälupulgad tööarvutites on potentsiaalne viiruseoht, väär puhastusaine või printeritint võib rikkuda seadmeid ja tekitada seisaku jne.
- Ebaturvaliselt paigutatud, lukustamata ja signalisatsioonita elektrikilbid võimaldavad igal soovijal igal ajal toite katkestada.
- Liinide väike läbilaskevõime ähvardab side ummistustega, kui võrk laieneb, edastusmaht kasvab või lisanduvad uued teenused. Kui kaablitrasside projekteerimisel ei ole laienemisvõimalusi arvestatud, ei ole võib-olla piisavalt ruumi lisakaablitele.
- Andmekandjate puudulik või väär märgistus ning halb arhiiviruum tähendavad viivitusi andmekandjate kasutamisel, seega käideldavuse langust.
- Sülearvuti edasiandmine ühelt kasutajalt teisele ilma asjakohaste protseduuride ja registreerimiseta ohustab tundlikke andmeid, suurendab viiruseriski ega võimalda turvarevisjoni.
- Faksimaterjalide ebapiisava varu korral lähevad sissetulevad sõnumid kaotsi.
- Tarkvara testimis- ja evitusprotseduuride puudumise või puudulikkuse tõttu võivad jääda leidmata tarkvara vead ja turvaaugud ning kasvab inimvigade risk. Sellised protseduurid nõuavad plaanilisi lisaressursse ja koolituse korraldust.
- Tarkvara testimine tegelike andmetega tähendab konfidentsiaalsuse kao ohtu, võimalikud programmivead aga võivad kahjustada andmeid.
- Autori- või omandiõiguse rikkumine, peamiselt ilmneb piraattarkvara kasutamise aktsepteerimisena. Rikkumise ilmnemisel võib asutus lisaks maine langusele kanda suurt materiaalset kahju kohtu- ja trahvikuludena.
- Vale salvestivõrgu ressursijaotus
- Interneti domeeninimede taotlemise või haldamise vead
- Kaugkliendi ühildumatus töökeskkonnaga (toitepinge, modemi omadused, sidevõrk)
- Ühildumatud võrgu aktiiv- ja passiivkomponendid (protokollide/teenuste teostuse lahknevus jms)
- Kaugtöötajate halb integratsioon infovoogu (hilistused töökohaga suhtlemisel)
- Hilistused kaugtöötajate ajutise piiratud kättesaadavuse tõttu
- Reaktsiooniaegade pikenemine kaugtöö-IT-süsteemi väljalangemisel

- Liini ebapiisav ribalaius (võrgu plaanimine tulevikuvaruta)
- Andmete kadu andmebaasis salvestusruumi puudumise tõttu

3.4.4 Dokumenteerimise puudused

- Dokumentatsiooni puudumine või puudulikkus tähendab pikemaid seisakuid konfiguratsiooni muutuste või tõrkeotsingu puhul.
- Andmekandjate puudulik märgistus ja saatedokumentide puudumine võib muuhulgas tekitada segadust versioonidega: uusim versioon võib jõuda kohale enne eelmist, saaja aga võtab kasutusele eelmise, pidades seda värskeimaks.
- Kaablite puudulik dokumenteerimine tekitab rikkeotsingu või muudatuste tegemise olukordades eriti suurt kahju siis, kui kaabelduse paigaldas teine firma.
- Töövahendite puudulik dokumenteerimine

3.4.5 Turvameetmete valimise puudused

Sellised puudused on sageli tingitud riskihalduse puudustest.

- Volitamatu sissepääs ruumidesse või volituste andmine vastava juhendamiseta (näiteks asenduskoristajale)
- Korraldamata kasutajavahetus mitme kasutajaga arvutil: ilma välja- ja sisselogimiseta ning isoleerimisele kuuluvate andmete ja programmide kustutuseta
- Vead Windows-PC integreerimisel Unix-võrku võimaldavad tungida PC-dest Unix-kataloogidesse, lugeda sealt paroole jne.
- Konfidentsiaalsusaugud Unix-süsteemis: näiteks võimaldavad *who*, *finger*, *ruser* peilida süsteemiülema äraolekut.
- Kaitsetus välisvõrgu eest, alates sellest, et kasutajanimed jms “legaalne” teave soodustab ründeid.
- Halb krüpteerimise korraldus: krüpteerimine sooritatakse kaitsmata keskkonnas, võti kirjutatakse samale andmekandjale, kus on krüpteeritud andmed jne.
- Vead konfigureerimisel ja opereerimisel (kahtlane priivara, aktiivsisu, käitusfailid meilis jms)
- Võrguhaldussüsteemi ebasobiv konfigureerimine (serveripääs, õigused)
- Võrguseadmete (marsruuterite ja kommutaatorite) väär konfigureerimine

- Vale traadita kohtvõrgu infrastruktuuri konfiguratsioon
- IP-kõne komponentide väär konfiguratsioon
- IP-kõne vahendustarkvara väär konfiguratsioon
- Võrgu aktiivkomponentide puudulik konfigureerimine
- Kaugklientide ebaturvaline konfigureerimine (ühildumatu autentimine, lubamatu tarkvara jms)
- Salvestisüsteemide ebaturvalised vaikesätted
- Võrguseadmete ebaturvalised vaikesätted
- Ebaturvalised krüptoalgoritmid (lühikesed võtmed jms)
- Turvalisuse kaotus krüpteeritud failisüsteemi kasutamisel
- Mitteusaldusväärsed või puuduvad traadita kohtvõrgu turvamehhanismid
- IP-kõne terminalide nõrkused
- Ebapiisavad traadita kohtvõrgu regulatsioonid
- Pihuarvutite puudulikud turvamehhanismid
- Andmebaasi turvamehhanismide (nt paroolid) puudumine või puudulikkus
- Automaatne CD-plaadi tuvastus
- Kaugpöördusteenuste väär kasutamine (volitamata teenused, ühendused muude võrkudega)
- Võrguvahendite (marsruuterid, kommutaatorid) kasutamise väär kavandamine
- Krüptoprotseduuride kasutamist puudutavate seaduste rikkumine
- Kasutajakeskkonna piisamatu piiramine (lubatavad funktsioonid Windowsi all jms)

3.4.6 Turvasüsteemide halduse puudused

- Turvameetmete ebapiisav järelevalve (revisjonitarkvara puudub, sündmuste logimine ei ole korraldatud efektiivselt).
- Revisjoniandmete analüüsi puudumine või ebaregulaarsus. Regulaarsusel on turvarikkumisi ja sisemisi ründeid peletav toime.
- Arhiivisüsteemide puudulikud kontrolljäljed

4 RISK

Eespool loetletud ohud on **potentsiaalsed** kahjude allikad. Ka vastava turvaaugu leidumine ei tähenda veel ohu tingimatut materialiseerumist kahjudeks. Ohtude realiseerumise tegelik sagedus sõltub ohu tüübist, turvaaugu "suurusest" ning objekti ja ta varade iseärasustest, näiteks andmete tundlikkusest. Ka ohu turvarikkeks muundumisel tekkiva kahju kaalukus sõltub konkreetsest objektist ning varieerub sealgi stohhastiliselt. Niisiis tuleb turvameetmete valimiseks osata hinnata **ohtude tegeliku toimimise tõenäosusi** ja prognoosida **oodatavaid kahjusid**. Riskianalüüs on selle peatüki ja kogu I osa põhisisu.

4.1 Ohtude statistika

Mõningase ettekujutuse ohtude realiseerumise suhtelisest tõenäosusest annab USAs realiseeruvate ohtude keskmine arv aastas (andmed USA mereväe riski-analüüsi metoodilisest juhendist).

Tabel 13. Ohtude keskmine arv USA-s

Turvarikke allikas/olemus	Keskmiselt aastas	
	Min	Max
Looduslik		
Välk	0,07	50
Torm	0,01	10
Lumetorm	0	10
Tornaado	0,00001	2
Orkaan	0,05	0,5
Liivatorm	0,01	0,5
Ujutus	0,01	0,5
Maavärin	0,005	0,2
Tsunaami	0	0,125
Maalihe	0	0,1
Vulkaanipurse	0	0,01
Muu stiihiline		
Inimviga	10	200
Riistvara tõrge	10	200
Tarkvaraviga	1	200
Side avarii	0,5	126
Elektrikatkestus	0,1	30
Keskkonnatõrge	0,1	10
Kiirgus	0,1	10
Infopaljang	0,2	5
Vedeliku leke	0,02	3
Kahjutuli	0,001	9
Rünne		
Pommiähvardus	0,01	100
Volitamatu kasutamine	0,009	5

Turvarikke allikas/olemus	Keskmiselt aastas	
	Min	Max
Infopaljang	0,2	5
Töötaja sabotaaž	0,1	5
Vandalism	0,008	1
Vargus	0,015	1
Võltsing	0,09	0,5
Andmete muutmine	0,083	0,462
Tänavarahutused	0	0,29
Terroriakt	0,009	0,1
Tarkvara muutmine	0,00225	0,0125

Tabelis 13 esitatud keskmiste arvude väga laiad vahemikud on seletatavad regionaalsete looduslike ja sotsiaalsete iseärasuste, organisatsioonide tüübi ja suuruse ning muude selliste tegurite tugeva varieerumisega suurriigi tingimustes. Euroopa kohta võib võrdlusandmeid leida Suurbritannias korraldatud uuringust [16]; ohtude liigitus erineb siin ülaltoodust ja kvantitatiivseks näitajaks on vastavat turvariket nentinute protsent vastajaist.

Tabelid 14 ja 15 kajastavad *Infowatchi* esimese üleeuroopalise turvauuringu tulemusi [19]. Protsendid näitavad ohu realiseerumist nentinud organisatsioonide osakaalu.

Paljud ohud on omavahel seotud – näiteks pettus nõuab tundliku informatsiooni moonutamist, majanduslikud aruanded ja sabotaaž on alati seotud konfidentsiaalse informatsiooni lekkimise või andmete kaoga jne.

Tabel 14. Ohtude esinemissagedus 2008. a

Ohu liik	Oht	%
Stiihilised	Töötaja hooletus	65
	Riist- või tarkvara tõrge	13
Ründed	Andmete vargus	78
	Viirused	49
	Häkkerid	41
	Rämpspost	32
	Sabotaaž	15
	Rahaline pettus	7

Tabel 15. Välised ja sisemised ohud

Ohu liik	Oht	%
Välised	Viirused	49
	Häkkerid	41
	Rämpspost	32
Sisemised	Konfidentsiaalse teabe lekkimine	93
	Tundliku teabe moonutamine	85
	Riistvara vargus	34
	Pettus	29
	Andmete kadu	23
	Infosüsteemi tõrge	20
	Sabotaaž	9
	Muu	7

Tabel 16. Füüsiliste ohtude keskmine arv Euroopas

Turvarikke allikas/olemus	%
Arvuti rike	49
Voolukatkestus	48
Vargus	46
Kohtvõrgu rike	36
Laivõrgu rike	24
Välk	13
Ujutus	5
Kahjutuli	2
Sabotaaž	2

Olukorra kohta Eestis ei ole veel statistilisi andmeid kogutud. Ülaltoodud statistikanäidetest juhindumisel tuleb silmas pidada suuri erinevusi mitte ainult infosüsteemide suhtelises arvus ja tasemes, vaid ka turvameetmete ja üldise turvateadlikkuse tasemes. Näiteks PwC 2008. a andmetel [5] oli 55% küsitletud Suurbritannia organisatsioonidest kehtestatud formaalne dokumenteeritud turvapoliitika (vrd 2002 – 27%).

4.2 Turvarikete hind

Turvariketest tingitud kahjude kohta on raske saada rahuldavaid kvantitatiivseid näitajaid, sest mitmed kahjude liigid (näiteks asutuse reputatsiooni langus, vt ka 1.4) ilmnevad alles pikema aja jooksul ja on raskesti hinnatavad, pealegi on vastavate andmete avaldamine organisatsioonidele tunduvalt vastumeelsem kui turvarikete liikide teatamine. Seetõttu põhineb avaldatud statistika enamasti järjestuslikel või jämedatel 3–4-pallistel hinnangutel.

Tabel 17 põhineb 2006. a USA-s läbi viidud Computer Security Institute'i ja FBI uuringul „Computer Crime and Security Survey" [3]. Turvarikete põhjustatud kahjusid oli nõus avaldama 313 ettevõtet (neist 77% rohkem kui 100 töötajaga); kahjud on kõigi organisatsioonide peale kokku liidetud.

Tabel 17. Turvarikete hind

Ründeliik	**Kahju, $**
Viirused	15 691 460
Volitamata juurdepääs teabele	10 617 000
Sülearvuti või mobiilseadme vargus	6 642 660
Firmaomase teabe vargus	6 034 000
Teenusetõkestus	2 922 010
Finantspettus	2 556 900
Võrgu või meili sisemine kuritarvitus	1 849 810
Sidepettus	1 262 410
Robotivõrku haaratud arvutid	923 700
Süsteemi läbistamine väljastpoolt	758 000
Andmepüük, kus firma võltsitakse saatjaks	647 510
Raadiosidevõrgu kuritarvitus	469 010
Kiirposti kuritarvitus	291 510
Avaliku veebirakenduse väärkasutus	269 500
Andmete või võrkude sabotaaž	260 000
Veebisaidi näostustamine	162 500
Paroolide väljanuhkimine	161 210
Organisatsiooni DNS-serveri vallutus	90 100
Muud	885 000
Kokku	**52 494 290**

PwC küsitlus "*2008 Information Security Breaches*" palus Suurbritannia ettevõtetel muuhulgas hinnata asetleidnud turvaintsidente skaalal „tühisest" kuni „äärmiselt tõsiseni". Võrdlevad andmed esitab tabel 18 [5].

Tabel 18. Turvaintsidentide kaalukus

Tõsidus	**% 2008**	**% 2006**
Äärmiselt tõsine	3	4
Väga tõsine	8	7
Tõsine	14	17
Mitte tõsine	13	21
Tühine	7	13
Intsidente polnud/ ei avaldanud andmeid	55	38

Järgmisest tabelist nähtub, et Suurbritannias on avaldatud rahalised kahjud väiksemad kui USA-s – kõigest 14% vastanutest teatas arvestatavast kahjust [5].

Tabel 19. Turvaintsidentide tektitatud rahaline kahju

Kahju, £	**%**
Tühine	61
< 1000	25
1001 - 9999	12
> 10000	2

Järgmine samast uuringust pärit tabel näitab, et pikimaid tööseisakuid tekitas süsteemi rike või andmete muutumine [5]. Protsent näitab arvu vastanutest.

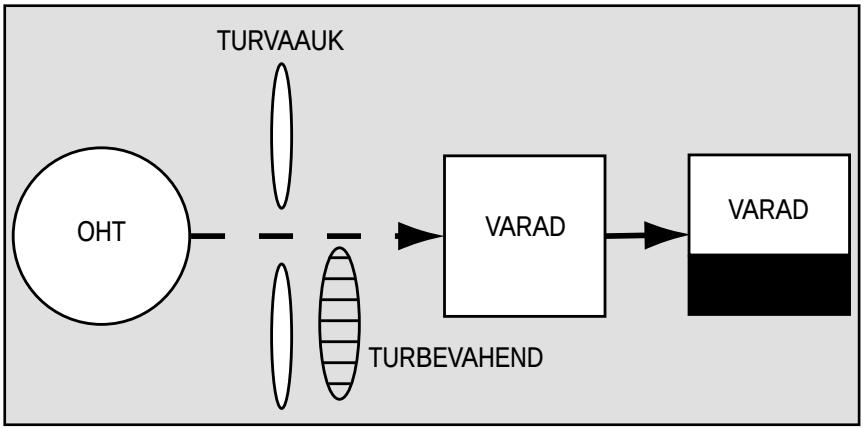
Tabel 20. Turvaintsidentidest põhjustatud tööseisakud

Kahju allikas/olemus	Kadu inimtöö-päevades	%
Viirus või segadust tekitav tarkvara	< 1	71
	2-10	21
	11-50	7
	> 51	1
Süsteemi rike või andmete muutumine	< 1	44
	2-10	47
	11-50	7
	> 51	2
Personali vead süsteemi kasutamisel	< 1	72
	2-10	24
	11-50	4
	> 51	-
Lubamatu juurdepääs väljastpoolt	< 1	61
	2-10	35
	11-50	4
	> 51	-
Seadmete vargus	< 1	70
	2-10	30
	11-50	-
	> 51	-
Arvutikelmus või konfidentsiaalsuse rikkumine	< 1	56
	2-10	40
	11-50	4
	> 51	-

Sealjuures hinnati halvima intsidendi põhjustatud keskmise kahju hinnaks 15000 naelsterlingit (vrd 2006 – 12500 naelsterlingit), millest põhiosa moodustas äritegevuse katkemine ning otsesed kulud intsidendile reageerimiseks [5].

4.3 Riskianalüüs

Risk on ohtudest tulenevate kahjude statistiline mõõt, mida on kasulik teada objekti turvatarbe otsustamiseks ja turvameetmete valimiseks. Riskianalüüsi eesmärk on prognoosida objektile tekitatavat kahju mingiks perioodiks, näiteks aastaks. Kui see prognoos on teada, taandub turvaküsimus tasuvuse määramise ülesandeks, milles võrreldakse prognoositud kahju võimalikele turvameetmetele tehtavate kulutustega sama perioodi kohta. Riskianalüüs on laiema turbeprotsessi, **riskihalduse** (*risk management*) osa.



Joonis 5. Turvaprobleem

Eri metoodikates on kasutusel erinevaid riski määratlusi; alljärgneva annab ISO.

Infoturvarisk on vaatlusaluse ohu potentsiaal ära kasutada mingi vara või vararühma nõrkusi ja tekitada seeläbi organisatsioonile kahju. Infoturvariski mõõdetakse sündmuse tõenäosuse *(p)* ja ta tagajärgede kombinatsiooniga.

On ka teisi määratlusi (NIST, NSA), aga need ei tingi olulisi erinevusi analüüsi metoodikas; mõlemal juhul on riskianalüüsi eesmärk sama ning mõlemal juhul algab analüüs varade, ohtude ja objekti nõrkuste spetsifitseerimisest. Teatavaid lahknevusi on nõrkuste tõlgendamisel: mõnede meetodite puhul võrreldakse olemasolevaid turvameetmeid ohtude neutraliseerimiseks vajalikega, lugedes nõrkuseks iga puuduva turvameetme. Selline lähenemine õigustab end lihtsamate turvaülesannete lahendamisel tüüpvahenditega, jätab aga kõrvale võimalikud muud vahendid. Nõrkus ei ole siiski lihtsalt ühe kindla turvameetme puudumine

(hoone halba asukohta ei saa ju neutraliseerida hoone viimisega turvalisemasse kohta).

Riskianalüüs sooritatakse üldjuhul järgmiste sammudena:

1) objekti piiritlemine ja varade liigitamine,

2) varade spetsifitseerimine,

3) varade hindamine,

4) ohtude, nõrkuste ja olemasolevate turbevahendite spetsifitseerimine,

5) turvarikete tõenäosuste hindamine,

6) oodatava aastase kahju hindamine.

Nendele sammudele järgneb riskihalduse järgmine etapp (sageli loetakse ka see riskianalüüsi osaks) - turvatarbe otsustamine, sobivate turvameetmete valimine, nende tasuvuse hindamine ja aktsepteeritava jääkriski suuruse otsustamine. Üldjoontes sarnaneb kogu protsess näiteks ettevõtte äristrateegia väljatöötamisega või muu sellise majandusülesandega. Turvaülesanne ongi olemuselt rentaablusülesanne: turvameetmed nõuavad kulutusi, need kulutused aga peavad end tasuma.

Analüüsi meetodid jagatakse tinglikult kvantitatiivseteks ja kvalitatiivseteks. Kvantitatiivsete meetodite puhul püütakse kasutada võimalikult täpseid statistikal ja kahjude rahalistel väärtustel põhinevaid arvandmeid, kvalitatiivsed meetodid opereerivad (tavaliselt kahe- kuni kuuepallise) subjektiivsete hinnangute skaalaga, mille aluseks võib olla mingitest normdokumentidest tulenev astmestik.

Lisaks neile kahele rühmale on kasutusel veel mitmesugused “varjatult” riskianalüüsi sisaldavad kaudsed turvatarbe või -taseme hindamise meetodid.

4.4 Kvantitatiivne riskianalüüs

4.4.1 Objekti piiritlemine ja liigendamine

See etapp on vajalik objekti edasiseks süstemaatiliseks lünkadeta käsitluseks.

Infosüsteemi peamised varad on loetletud eespool, jaotises 1.1. Turvaülesande seisukohalt on otstarbekas seda loetelu detailiseerida ja liigendada. Varade struktuur ja parameetrid sõltuvad organisatsiooni spetsiifikast, kuid liigendada tasub ikkagi mingi turvaloogilise ja praktikas kasulikuna tõendatud süsteemi alusel. Alljärgnevas on paar näidet.

1. Tüüpiline USA sõjaväeasutustes kasutatav infotehniliste varade liigendus (madalaim detailsustase on tabelis lühiduse mõttes ära jäetud), mille esimene tase ja analoogiline üldstruktuur on laialt kasutusel ka tsiviilasutuste ja firmade turvaanalüüsides.

2. Standard ISO 27002 (jaotis 7.1.1) loetleb näidetena järgmisi infosüsteemidega seotud varasid:

> a) **teave***:* andmebaasid ja andmefailid, lepingud ja lepped, süsteemidokumentatsioon, uurimisteave, kasutajajuhendid, koolitusmaterjal, töö- või tugiprotseduurid, jätkusuutlikkuse plaanid, laskumise korraldus, revisjonipäevikud ja arhiveeritud teave;
>
> b) **tarkvaralised varad**: rakendustarkvara, süsteemitarkvara, arendusinstrumendid ja utiliidid;
>
> c) **füüsilised varad**: arvutiseadmed, sideseadmed, ird-andmekandjad ja muu varustus;
>
> d) **teenused**: arvuti- ja sideteenused, kommunaalteenused, nt küte, valgustus, energiavarustus ja õhu konditsioneerimine;
>
> e) **inimesed ning nende kvalifikatsioon, oskused ja kogemused**;
>
> f) **immateriaalsed varad, näiteks organisatsiooni maine ja imago**.

3. BSI (Infotehnika Turbe Liiduamet) väljatöötatud moodulmetoodika Saksamaa riigiasutuste turvaülesannete lahendamiseks kasutab alljärgnevat objekti liigendust tüüpkomponenentideks (tabelis 22 toodud lühendatud kujul). Selles süsteemis ei käsitleta eraldi komponendina üht peamist vara – andmeid. Praktilistest kaalutlustest lähtudes spetsifitseeritakse need arvutisüsteemidega seostatud alamkomponentidena. Muus osas põhineb liigendus tüüpilise kasutatava info-

tehnoloogia konkreetsel hetkeseisul ja nõuab seetõttu regulaarset iga-aastast korrigeerimist. See liigendus ei ole eriti sobiv objekti üldise turvatarbe hindamiseks, kuid on äärmiselt otstarbekas komponentide turvameetmete valimiseks.

Tabel 21. Varade liigendus

Andmevarad	Salastusklassiga	Statistilised
	Operatiivsed	Isikuandmed
	Taktikalised	Logistilised
	Plaanimine	Muud
	Rahanduslikud	
Riistvara	Keskarvuti	Välisseadmed
	Andmekandjad	Personaalarvutid
	Eriarvutid	
Sidesüsteemide varad	Sideliinid	Kommutaatorid
	Sideprotseduurid	Telefonid
	Multiplekserid	Modemid
Tarkvara	Operatsioonisüsteemid	Testprogrammid
	Rakendusprogrammid	Sideprogrammid
	Tüüprakendused	Muud
Inimvarad	Arvutipersonal	
	Hoone personal	
	Seadmestiku personal	
Haldusvarad	Tehniline dokumentatsioon (tarkvara, riistvara jne)	Inventariloendid
	Talitlus (plaanid, juhendid, revisjonidokumendid)	Ekspluatatsiooniprotseduurid
	Protseduurid (avariiplaanid jne)	
Füüsilised varad	Keskkonnasüsteemid (vesi, elekter jne)	Varundusvahendid (avariitoide jne)
	Hoone	Materjalid (magnetkandjad, paber, värvilindid jne)
	Arvutiruumid	Bürooruumid

BSI järgi toimub objekti liigendamine kahes etapis. Esmalt liigendatakse süsteemi varad järgmiselt:

a) rakendused,

b) serverid,

c) tööjaamad,

d) võrgukomponendid,

e) ruumid.

Seejärel seostatakse iga vara (nt server) ühe või mitme tüüpmooduliga alljärgnevast tabelist (nt serveri võib seostada moodulitega „Andmetalletus“, „Server“ ja „Windows 2000 Server“).

4. Infovarade liigitus etalonturbe süsteemis ISKE:

a) andmekogud,

b) andmekogusid käitavad infovarad (serverid),

c) käitavaid infovarasid toetavad infovarad (võrguseadmed),

d) autonoomsed varad (hooned, ruumid, paberkandjad, andmekandjad).

Tabel 22. Objekti liigendus tüüpkomponentideks (lühendatult)

Üldkomponendid	1. IT-turvahaldus
	2. Organisatsioon
	3. Personal
	4. Talitluse pidevus
	5. Andmetalletus
	6. Andmekaitse
	7. Viirusetõrje
Infrastruktuur	1. Hooned
	2. Kaabeldus
	3. Ruumid:
	a) bürooruum,
	b) serveriruum,
	c) andmearhiivid,
	d) tehniliste infrastruktuuride ruum
	4. Andmeruumid ja -kambrid
	5. Kodukontor (kaugtöö)
Autonoomsed arvutisüsteemid	1. Sülearvuti
	2. Unix-süsteem
	3. Windows 2000 süsteem
	4. Internet-PC
	5. Windows XP süsteem
Kohtvõrgud	1. Unix-server
	2. Windows NT võrk
	3. Windows 2000 Server
Andmevahetussüsteemid	1. Tulemüür
	2. Marsruuterid ja kommutaatorid
	3. Salvestisüsteemid ja -võrgud
Sidesüsteemid	1. Sisekeskjaam
	2. Faksiaparaat
	3. Automaatvastaja
	4. Mobiiltelefon
	5. PDA
Muud komponendid	1. Tüüptarkvara
	2. Andmebaasid

4.4.2 Varade spetsifitseerimine

Varade spetsifitseerimist alustatakse olemasolevate ja kavandatud infosüsteemide (personaalarvuti, kohtvõrk, sisekeskjaam jne) loetlemisest, võttes arvesse ka paigaldamisel või kasutamata (töökõlblikud) süsteemid. Töö on otstarbekas sooritada kahes järgus.

Esimeses järgus koostatakse süsteemide loetelu, jättes täpsustamata nende komponendid (üksikseadmed), kuid märkides üles asukoha, kasutaja, rakendusoleku jms, näiteks, nagu näidatud tabelis 23.

Tabel 23. Varade spetsifitseerimise esimene järk

Nr	Nimetus	Asukoht	Võrk	Olek	Kasutaja
1.	UNIX-süsteem	A210	2	Testimisel	Osakond B
2.	Kohtvõrk	A-tiib		Paigaldamisel	Osakond B
3.	Core 2 Duo	A115	2	Töös	Raamatupidamine
4.	Core 2 Quad	A107		Kavas	Osakond C
5.	Keskjaam	B-tiib		Töös	Kogu asutus
...					

Teises järgus spetsifitseeritakse süsteemide peamised rakendused (funktsioonid) tähtsusjärjestuses. Rakendus hõlmab vastavat tarkvara ja andmekogumeid. Vajaduse korral võib käideldavuse, tervikluse või konfidentsiaalsuse mõttes olulisemad andmekogumid (failid, andmebaasid) märkida eraldi veergu. Näiteks nii, nagu näidatud tabelis 24.

Tabel 24. Varade spetsifitseerimise teine järk

Nr	Nimetus	Väärtus	Rakendused	Väärtus	Andmekogumid	Väärtus
3	Core 2 Duo		Palgaarvestus		Personalibaas	
			Arvete töötlus		Tarnijate baas	

Väärtuste lahtrid on lisatud järgmise sammu – varade hindamise – sooritamiseks.

4.4.3 Varade hindamine

Eelmiste sammudega koostatud spetsifikatsiooni põhjal hinnatakse varade väärtus, arvestades organisatsiooni ja IT-rakenduste spetsiifikat. Arvestada tuleks näiteks tabelis 25 näidatud parameetreid.

Tabel 25. Varade hindamise parameetrid

Riistvara	Asendusmaksumus
	Seisaku kestus
	Kulud riistvara ajutiseks üürimiseks
	Töötajate ja/või ületundide arv töö sooritamiseks käsitsi
	Seisaku kestel saamata jäänud tulu (tellimused jms)
Tarkvara	Tõrke identifitseerimiseks kuluv aeg
	Taaslaadimisele ja testimisele kuluv aeg
	Unikaaltarkvara uuesti loomisele kuluv aeg
	Unikaaltarkvara lähtekoodi avalikustamisest tulenev kahju
Andmed	Asendamise võimalikkus
	Taastemaksumus (nt paberdokumentide järgi taastamisel)
	Võimalikud seaduserikked (riigisaladus, isikuandmed jms)
	Sisekonfidentsiaalsus
	Ohud inimestele (nt meditsiinisüsteemides)
Personal	Ületundide arv
	Uue töötaja koolituskulud

Varasid hinnatakse kõigi kolme turvaaspekti – käideldavuse (A), tervikluse (I) ja konfidentsiaalsuse (C) – järgi, nende tähtsusjärjestuses. Kvantitatiivse analüüsi puhul väljendatakse iga vara väärtus rahaliselt, kolme aspektväärtuse summana:

$$V = V_A + V_I + V_C$$

Näide. Kui personaliandmeid sisaldava faili taastamiseks ($V_A + V_I$) kulub üks nädal 16000-kroonise töötasuga ametniku tööaega, faili avalikustamise eest (V_C) võib aga oodata 20000-kroonine trahv, siis

$$V = 4000 + 20000 = 24000 \text{ kr}$$

Praktikas ei saa aga varade väärtust tihti nii hõlpsalt määrata, eriti kaudsete ja tulenevate kahjude osas (vt ka jaotis 1.4). Tavaliselt tuleb selleks (eriti konfidentsiaalsuse puhul) kasutada tinglikku suhtelist suurusjärkude skaalat (0, kuni

100, kuni 1000, kuni 10000 jne kr), sest täpseid arvutuslikke väärtusi saada on paljude konfidentsiaalsuse rikete korral praktiliselt võimatu. Niisugustel juhtudel on otstarbekas lähtuda mingist välistel eeskirjadel, standarditel või muudel alustel põhinevast kahjude kaalukuse kvalitatiivsest liigitusest (vt jaotis 4.5 allpool), kinnistades igale kaalukusklassile jämeda rahalise kaalu.

4.4.4 Turvarikete tõenäosuse hindamine

Analüüsitakse ohtusid (vt 2. ptk) ja nõrkusi (vt 3. ptk), arvestades võimalikke olemasolevaid turvameetmeid, mis kõrvaldavad osa ohtudest. Turvarikete tõenäosuste hindamisel annab mõningaid pidepunkte tabel jaotises 4.1.

Korraliku statistika puudumisel määratakse võimalike rikete suhteline sagedus ohtude paarikaupa võrdluse teel. Sellise hinnangumeetodiga saadud tulemuse näide on tabelis 26 olev Stangi ja Mooni koostatud sageduste tabel. Tabeli teine pool sisaldab muid ohte meelevaldses järjestuses. Konfidentsiaalsuse, tervikluse, käideldavuse ja seaduslikkuse/eetika veerud näitavad, millistele atribuutidele toimib vastav oht, viimases veerus on vastava ohu suhteline tõenäosus autorite hinnangul.

Tabel 26. Rikete suhtelised sagedused

Oht	Konfidentsiaalsus	Terviklus	Käideldavus	Seaduslikkus/ eetika	Ohu suhteline sagedus
Inimeksitus	x	x	x		0,19
Piraatlus				x	0,17
Väär või vananenud informatsioon		x		x	0,16
Andmeleke	x				0,16
Sissetung volitatud kasutaja varjus	x				0,15
Kiirguslekete seire	x		x		0,13
Sihilik andmete või programmide hävitamine		x			0,13
Teesklus (volitatu kehastamine)	x	x	x		0,13
Ülekoormus			x		0,12
Väärmarsruutimine	x				0,11
Riistvara rike	x	x	x		0,09

Oht	Konfidentsiaalsus	Terviklus	Käideldavus	Seadusliikkus/ eetika	Ohu suhteline sagedus
Näiline (teeseldud) raaltöötlus	x			x	0,08
Andmepüük võrguanalüsaatoriga	x				0,07
Pettus		x			0,06
Tulekahjud ja loodusõnnetused		x	x		0,04
Võltsimine		x			0,03
Loogikapomm	x	x	x		0,03
Sisevargus, sh. andmete manip.-ne sisestusel		x			0,03
Kasutamise tõkestus ressursside sidumisega			x		0,02
Salauksed	x	x	x		0,01
Programmeerimisvead	x	x	x		
Sabotaaž		x	x		
Heitmaterjali (kopeer, kustutatud fail) uurimine	x				
Volitamatu utiliitidega manipuleerimine	x	x	x		
Vargus	x	x	x		
Trooja hobused	x	x	x		
Segadused tarkvara versioonidega		x			
Viirused		x	x		
Andmeliikluse salasalvestamine	x				

Teine subjektiivse hindamise võimalus on eeldada mitmesuguse kasutada oleva teabe põhjal ohtude realiseerumise intervalle, seejärel aga normaliseerida arvud, taandades nad aastasele perioodile, näiteks skaalaga tabelis 27.

Tabel 27. Ohtude eeldatavad sagedused

Eeldatava sagedus	Kordi aastas
Mitte iialgi	0
Kord 300 a jooksul	0,0033
Kord 200 a jooksul	0,005
Kord 100 a jooksul	0,01
Kord 50 a jooksul	0,02
Kord 25 a jooksul	0,04
Kord 5 a jooksul	0,2
Kord 2 a jooksul	0,5
Kord aastas	1,0
Kaks korda aastas	2,0
Kord kuus	12,0
Kord nädalas	52,0
Kord päevas	365

4.4.5 Oodatava aastase kahju arvutus

1. Arvutatakse oodatav aastane osakahju iga ohu T_j kohta:

$$L_j = f_j \times (V_1 + V_2 + ... + V_n),$$

kus

V_i on varad (nt arvuti 1, arvuti 2 jne), millele toimib sama oht T_j

f_j on ohu T_j sagedus aastas

Näide. Oht T_j = liigpingeimpulss toitevõrgus, f_j = 3 (korda aastas); varad on server taastemaksumusega 100000 kr ja kaheksa tööjaama keskmise taastemaksumusega 15000 kr. Pingetõuke tekitatav osakahju on L_j = 3(100000+8×15000) = 660000 kr.

2. Arvutatakse oodatav aastane osakahju iga vara V_i kohta:

$$L_j = V_j \times (f_1 + f_2 + ... + f_m),$$

kus

V_i on vara, millele toimivad ohud

f_j on ohu T_j sagedus aastas

3. Arvutatakse aastane oodatav kogukahju

a) ohuspetsiifiliste osakahjude alusel:

$$L = \sum L_j$$

b) varaspetsiifiliste osakahjude alusel:

$$L = \sum L_i$$

Tulemused peavad kokku langema. Arvutus mõlemat liiki osakahju alusel on kasulik selleks, et hinnata vastavalt üksikute varade osakaalu ja konkreetsete kahjude toimet kogukahjus. Täielik kahjukomponentide maatriks võimaldab saada kiire ülevaate kriitilistest varadest ja kriitilistest ohtudest.

Saadud tulemuse põhjal otsustatakse täiendavate turvameetmete vajadus.

4.5 Varade turvaliigitus

Riskianalüüsi tüübi (kvantitatiivne/kvalitatiivne) valimisel tuleb muuhulgas arvestada lähteandmete kvantiteerimisvõimalusi. Enamasti ei ole varade kõigi turvaaspektide väärtust võimalik hinnata täpses rahalises väljenduses. Seetõttu on varade spetsifitseerimisel kasulik esimeses lähenduses rakendada aspektiväärtuste jämedat liigitamist mõneastmelisel kvalitatiivsel skaalal. Kvantitatiivse analüüsi sooritamiseks tuleb skaala astmetele seejärel kinnistada orienteerivad rahalised väärtused, kvalitatiivseks analüüsiks piisab astmetele suhteliste arvuliste kaalude kinnistusest või kvalitatiivsete verbaalsete hinnangute juurde jäämisest.

4.5.1 Käideldavuse järgi

Tavalistes büroosüsteemides piisab harilikult kolmest-neljast üsna jämedalt määratletud käideldavusastmest, näiteks:

1. TÄHTSUSETU KÄIDELDAVUS. Teenuse halvang on ebamugav, kuid ei mõjuta talitlust oluliselt.

2. SOOVITAV KÄIDELDAVUS. Teenuse halvang tuleb võimaluse korral ära hoida.

3. ELUTÄHTIS KÄIDELDAVUS. Teenuse halvang ei ole lubatav.

Tunduvalt kõrgemad on käideldavuse ja tervikluse nõuded niisugustes reaalajasüsteemides, mille talitlusest sõltub inimeste ohutus (lennundus, tuumareaktorite

jt plahvatusohtlike objektide juhtimissüsteemid, meditsiinisüsteemid, relva- jm sõjalised süsteemid).

Selliste süsteemide puhul on väga täpsed ja ranged nõuded kasutusel infoturbe naabervaldkondades, **töökindluse** ja **ohutuse** tagamisel, st stiihilistest ohtudest tuleneva riski kahandamisega tegelevatel aladel. Siin on nende valdkondade oluline puutepunkt, millest lähtudes ongi viimastel aastatel hakatud tegelema vastavate mudelite ja meetodite integratsiooniga (vt Olovssoni mudel jaotises 1.2).

Ehkki enamikus firmadest või riigiasutustest ohutuskriitilised süsteemid puuduvad, on ka "tavalise" riskianalüüsi ja riskihalduse puhul mõndagi õppida niisuguste süsteemide käsitluse metoodikast. Ohutuskriitiliste süsteemide jaoks pakub ühtseid käideldavuse, tervikluse ja riski kriteeriume 1995. a. koostatud rahvusvahelise standardi IEC 1508 projekt.

See projekt defineerib käideldavuse kvantitatiivselt kui **tõenäosuse, millega süsteem toimib õigesti suvalisel ajahetkel** (nt 0,999). Käideldavusel ja terviklusel on töökindluse valdkonnas ka muid kvantitatiivseid mõõte, näiteks keskmine tõrketu töövältus (MTBF) jt.

4.5.2 Tervikluse järgi

Kui andmeterviklus on ettevõttele kriitiliselt tähtis, võib rakendada näiteks järgmist skaalat:

1. MADAL TERVIKLUS. Terviklus pole oluline, vead on lubatavad.

2. KESKMINE TERVIKLUS. Mõõdukad nõuded. Ei tohi olla vigu, mis tugevalt mõjutaksid talitlust.

3. KÕRGE TERVIKLUS. Vigu ei tohi olla.

Ohutuskriitiliste süsteemide jaoks defineerib IEC 1508 neli kvantitatiivselt määratud terviklustaset:

Tabel 28. Terviklustasemed

Terviklustase	Ohtliku tõrke tõenäosus
4	alla 10^{-4}
3	alla 10^{-3}
2	alla 10^{-2}
1	alla 10^{-1}

Tabel 28 illustreerib seost jämeda kvalitatiivse skaala ja täpsete kvantitatiivsete kriteeriumide vahel.

4.5.3 Konfidentsiaalsuse järgi

Riigiasutustes kasutatakse tavaliselt ametlikku dokumentide jaoks kehtestatud konfidentsiaalsusliigitust, vajaduse korral seda täpsustades. Selline liigitus tuleneb peamiselt vastavatest seadustest (riigisaladuse seadus, isikuandmeid ja nende kaitset puudutavad seadused, avaliku teabe seadus jm) ning nende rakendusmäärustest. Enamikus maades on kasutusel neli tundliku teabe klassi.

Äriettevõtted kasutavad mitmesuguseid sisemisi liigitusi, mis peavad kinnistama suhtelise kaalu ka mitmesugusele tundlikule majandusteabele – hindu või konkurentsi mõjutavale ning tehnilisele, autoriõiguslikule või patenditeabele.

Tabel 29 esitab tüüpilise tundlikkusliigituse koos mõnede sõjaliste ja äriliste vastetega.

Tabel 29. Tundlikkusliigitus

Klass	**USA riigikaitse**	**NATO**	**Tsiviilvasted: teave, mille paljastamine...**
Avalik			
Ametialaseks kasutamiseks	For Official Use Only (FOUO)	NATO Restricted	... mõjutab äritegevust negatiivselt Nt: sisemine telefoniteatmik, personaliandmed, kliente puudutavad üldandmed jne
Konfidentsiaalne	Confidential	NATO Confidential	... seab kahtluse alla äritegevuse edukuse Nt: andmed klientide, tellimuste ja kontaktide kohta, turundusuuringud, personali haldusega seotud andmed, pakkumised, raamatupidamisandmed, eelarve, seadustega määratud teave

Klass	USA riigikaitse	NATO	Tsiviilvasted: teave, mille paljastamine...
Salajane	Secret	NATO Secret	...kahjustab äritegevust Nt: äristrateegiad, perspektiivplaanid, tootearenduse andmed, ettevõtete ostu või liitumisega seotud andmed, mitmesugune seadustega määratud teave (muuhulgas riigikaitseline)
Täiesti salajane	Top Secret	Cosmic Top Secret	... lõpetab äritegevuse

4.5.4 Süsteemi ISKE aluseks olev turvaliigitus

Infovarade vajaliku turvataseme määramiseks kasutab ISKE (vt jaotist 4.9) neljapallilist skaalat ja kolme turvaeesmärki.

Iga turvaeesmärgi taseme määramisel tuleb arvestada nõuetega:

- seadustest ja lepingutest tulenevad nõuded,
- põhitegevuse (või äritegevuse) protsessidest tulenevad nõuded,
- tagajärgede kaalukus.

Tabel 30. ISKE turvaosaklasside skaala

Käideldavus	
Turvaosaklass K0	Töökindlus – pole oluline. Jõudlus – pole oluline.
K1	Töökindlus – 90% (lubatud summaarne seisak nädalas u ööpäev). Lubatav nõutava reaktsiooniaja kasv tippkoormusel – tunnid (1:10).
K2	Töökindlus – 99% (lubatud summaarne seisak nädalas u 2 tundi). Lubatav nõutava reaktsiooniaja kasv tippkoormusel – minutid (1:10).
K3	Töökindlus – 99,9% (lubatud summaarne seisak nädalas u 10 minutit). Lubatav nõutava reaktsiooniaja kasv tippkoormusel – sekundid (1:10).
Terviklus	
T0	Info allikas, muutmise ega hävitamise tuvastatavus ei ole olulised. Info õigsuse, täielikkuse ja ajakohasuse kontrollimine pole vajalik.
T1	Info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad. Info õigsuse, täielikkuse ja ajakohasuse kontrollimine toimub erijuhtudel ja vastavalt vajadusele.
T2	Info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad. Vajalik on info õigsuse, täielikkuse ja ajakohasuse perioodiline kontrollimine.
T3	Info allikal, selle muutmise ja hävitamise faktil peab olema tõestusväärtus. Vajalik on info õigsuse, täielikkuse ja ajakohasuse kontroll reaalajas.
Konfidentsiaalsus	
S0	Avalik teave: juurdepääsu teabele ei piirata (st lugemisõigus kõigil huvitatutel, muutmise õigus määratletud tervikluse nõuetega).
S1	Teave asutusesiseseks kasutamiseks: juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral.
S2	Salajane teave: teabe kasutamine on lubatud ainult teatud kindlatele kasutajagruppidele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral.
S3	Ülisalajane teave: teabe kasutamine on lubatud ainult teatud kindlatele kasutajatele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral.

Arvestades nõudeid, moodustatakse turvaosaklass (K0, T0 jne). Kui nimetatud nõuded määravad erinevad tasemed, siis tuleb turvaosaklassi määramisel lähtuda kõrgeimast tasemest. Kolme turvaosaklassi kombinatsioon moodustab turvaklassi (nt K1T2S2), mis on aluseks turbeastmete määramisel. Kasutusel on kolm tüüpturbe astet:

- madal turbeaste (L),
- keskmine turbeaste (M),
- kõrge turbeaste (H).

Tabel 31. Turbeastme määramine turvaklassi järgi

		K0	**K1**	**K2**	**K3**
T0	S0	L	L	M	H
	S1	L	L	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T1	S0	L	L	M	H
	S1	L	L	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T2	S0	M	M	M	H
	S1	M	M	M	H
	S2	M	M	M	H
	S3	H	H	H	H
T3	S0	H	H	H	H
	S1	H	H	H	H
	S2	H	H	H	H
	S3	H	H	H	H

Spetsifitseerimata varade (töökorraldusprotsessid, muud organisatsioonilised ressursid jne) turbeastme määramisel tuleb aluseks võtta kõrgeim infovaradele määratud turbeaste.

4.6 Riskiklassid

Häid pidepunkte turvariski analüüsi täpsustamiseks pakub taas ohutusriske käsitlev IEC 1508, mis defineerib kvalitatiivselt neli riskiklassi ning seob need (ohutus)rikete sageduse ja tagajärgede kaalukusega:

Tabel 32. Riskiklassid

Riskiklassid	Tõlgendus
I	Vastuvõtmatu risk
II	Soovimatu risk; vastuvõetav ainult siis, kui kahandamine on ebapraktiline või saavutatava tulemusega võrreldes ebaproportsionaalselt kulukas.
III	Talutav risk kui kahandamine on saavutatavast tulemusest kulukam.
IV	Tühine risk

Riskiklasside seos sageduse ja kaalukusega IEC 1508 kohaselt on näidatud tabelis 33.

Tabel 33. Riskiklasside seos sageduse ja kaalukusega

Sagedus	**Kaalukus**			
	Katastroofiline	**Kriitiline**	**Marginaalne**	**Tühine**
Sage	I	I	I	II
Võimalik	I	I	II	III
Harv	I	II	III	III
Haruldane	II	III	III	IV
Võimatu	III	III	IV	IV
Uskumatu	IV	IV	IV	IV

Kaalukuse tõlgendamise näitena üks sõjalistes süsteemides kasutatav kaalukusskaala on ära toodud tabelis 34.

Tabel 34. Kaalukusskaala

Kaalukusklass	Määratlus
Katastroofiline	Mitmed hukkunud
Kriitilinev	Üks hukkunu ja/või mitu rasket vigastust/kutsetraumat
Marginaalne	Üks raske vigastus/kutsetrauma ja/või mitu kerget vigastust/ kutsetraumat
Tühine	Mitte üle ühe kerge vigastuse/kutsetrauma

4.7 Kvalitatiivne riskianalüüs

Ülaltoodust on näha, et kvantitatiivne riskianalüüs on üsna töömahukas (tüüpiliselt tuleb arvestada 50–100 ohtu, sama arvu turvaaukude ning 20–50 liiki varadega) ning võib takerduda puudulike ja ebatäpsete lähteandmete tõttu. Õigustatud on ta seal, kus varade koguväärtus on suur ja ka kavandatavad turvameetmed võivad osutuda üsna kulukaiks.

Väikese ja keskmise koguväärtusega objektidel ning väga puudulike kvantitatiivsete lähteandmete korral on otstarbekam määrata turvarisk kvalitatiivselt.

Kvalitatiivne analüüs järgib üldjoontes ülaltoodud üldskeemi, kuid ohtude realiseerumissageduste ja varade aspektväärtuste võimalikult täpsete arvväärtuste asemel kasutatakse jämedat mõneastmelist skaalat ning samasugusel skaalal saadakse ka oodatava kahju hinnang.

Kui rakendada varade aspektväärtuste (maksimaalsete võimalike aspektkahjude) ja oodatavate kahjude (riski) hindamiseks viieastmelist skaalat, ohtude realiseerumissageduse hindamiseks aga neljaastmelist, annab seose lähteandmete ja riski vahel tabel 35.

Tabel 35. Riskiklassid

		OHU REALISEERUMISE SAGEDUS			
		Väike	**Keskmine**	**Suur**	**Väga suur**
VARA ASPEKT-VÄÄRTUS	Ebaoluline	Tühine	Tühine	Tühine	Tühine
	Märgatav	Tühine	Tühine	Väike	Keskmine
	Tunduv	Väike	Keskmine	Suur	Suur
	Suur	Keskmine	Keskmine	Suur	Väga suur
	Kriitiline	Suur	Suur	Väga suur	Väga suur

Varade kvalitatiivne hindamine on objektispetsiifiline ega tohiks objekti tundmisel tekitada raskusi. Realiseerumissageduste kohta on kasutuskõlblikke andmeid mõnevõrra raskem saada, eriti rünnete hindamisel. Rünnete puhul lähtuvad mitmed tüüpmetoodikad mõistlikust eeldusest, et ründe realiseerimist stimuleerib ründaja oodatav kasu (mitte tingimata materiaalne, taotleda võidakse ka superkräkkeri oreooli vms), pärsib aga oodatav ressursikulu (aeg, kulutused tehniliste vahendite täiustamisele või kellegi äraostmiseks jne).

Tüüpiline niisuguse eelduse põhjal koostatud riskitabel on näidatud tabelis 36.

Tabel 36. Riskitabel

KASU ründajale	RESSURSIKULU ründeks	TOIME objektile	RISK (oodatav kahju)
Suur	Väike	Väga tugev	Suur
	Keskmine		Keskmine/suur
	Suur		Väike/keskmine
Keskmine	Väike	Tõsine	Keskmine/suur
	Keskmine		Keskmine
	Suur		Keskmine/väike
Väike	Väike	Mitte eriti tõsine	Väike
	Keskmine		Väike
	Suur		Väike

4.8 Kaudne riskianalüüs. Tüüpturbe meetod

Objekti turvaanalüüsi algfaasis tuleb asutuse juhtkonnal sageli otsustada üldine turvavajadus ja edasine tegevuskava üsna nappide lähteandmete ja puuduliku teadmusega, sest turvaspetsialiste asutuses tavaliselt veel ei ole ning töömahuka lähteuuringu sooritamiseks peab kõigepealt olema põhjendatud selle vajadus ja ulatus.

Niisugune vajaliku turvataseme otsustamine ja tegeliku turvataseme hindamine vajalikuga võrreldes sisaldab tegelikult jämedat kvalitatiivset riskianalüüsi, ehkki otsustajad ei tarvitse ilmutatult kasutada riskianalüüsi mõisteid ega neid isegi detaiselt teada. See ei olegi algjärgus vajalik. Oluline on süstemaatiline otsustusprotseduur, mis lähtuks infosüsteemide rollist asutuse tegevuses ja annaks võimalikult objektiivse tulemuse.

Vajaliku turvataseme hindamine tähendab sisuliselt asutuse infovarade koguväärtuse jämedat kvalitatiivset hindamist. Vajaliku taseme otsustamisel lähtutakse järgmistest teguritest (vt ka jaotis 1.4):

1) oluliste talitluslike otsuste sõltuvus töödeldava informatsiooni käepärasusest, täpsusest ja relevantsusest (käideldavusest ja terviklusest);

2) tähtsate või väga tähtsate ülesannete täidetavuse sõltuvus töödeldavast informatsioonist (selle käideldavusest ja terviklusest);

3) mahukate ülesannete täidetavuse sõltuvus töödeldavast informatsioonist (selle käideldavusest ja terviklusest);

4) töödeldava informatsiooni konfidentsiaalsus.

Neljaastmelise turvaskaala määratleb asutuse talitlusnõuetest lähtudes tabel 37.

Tabel 37. Vajaliku turvataseme määramine

Käideldavus-nõuded	**Terviklus-nõuded**	**Konfident-siaalsus-nõuded**	**IT kahjustuse üldtoime**	**Vajalik turvatase**
Asutuse keskseid ülesandeid ei saa täita IT-ta. Kiired reaktsiooniajad kriitiliste otsuste puhul nõuavad pidevalt värske teabe olemasolu. Seisakud ei ole lubatavad.	Informatsioon peab olema maksimaalsel võimalikul määral õige.	Kriitilistel aladel peab konfidentsi-aalse teabe kaitse olema tagatud ja vastama range salastuse nõuetele.	IT väljalangemine halvab asutuse töö või tekitab tõsiseid tagajärgi ühiskonna või valdkonna suurtes osades	Maksimaalne
Asutuses on kesksel kohal aegkriitilised protsessid või on ulatuslikke ülesanded, mida saab täita ainult IT abil.· Lubatavad on ainult lühikesed seisakud.	Töödeldav informatsioon peab olema õige. Vigu peab saama avastada ja vältida.	Kriitilistel aladel peab konfidentsi-aalse teabe kaitse olema selgelt määratletud ja vastama kõrgetele nõuetele.	Kahjustus halvab asutuse kesksed funktsioonid, õõnestab tugevalt asutust või kolmandaid osapooli.	Kõrge
Lubatavad ei ole pikad seisakud, mis põhjustavad tähtaegade ületamist.	Väiksemad vead on lubatavad. Ülesannete täitmist tõsiselt kahjustavaid vigu peab saama avastada ja vältida.	Tagada tuleb ainult sisemiseks kasutamiseks määratud informatsiooni kaitse.	Kahjustus õõnestab asutust.	Mõõdukas
Pikki seisakuid tuleks vältida, mõõdukad seisakud on lubatavad	Vead on lubatavad, kui nad ei tee ülesannete täitmist võimatuks.	Informatsiooni konfidentsi-aalsust ei nõuta.	Kahjustus õõnestab asutust vähe.	Madal

Kui niisugune eelanalüüs näitab maksimaalse või kõrge turvataseme vajadust, on majanduslikult otstarbekas ülesannet täpsustada, sooritades kvantitatiivse või piisavalt detailse kvalitatiivse riskianalüüsi.

Kui eelanalüüs osutab mõõdukat või madalat turvatarvet, võib uurimist jätkata selliste turvatasemete jaoks väljatöötatud tüüpvahenditega. Tavaliselt kujutavad need endast küsimustikke, mis võimaldavad lokaliseerida objekti suurimaid turvaauke ja/või võrrelda objekti turvameetmeid teatava meetmete etalonkompleksiga, mis on välja töötatud vastava turvataseme saavutamiseks ning võimaldavad valida mingi läbiproovitud tüüplahenduse.

Niisuguseid üsna detailselt spetsifitseeritud tüüplahendusi sisaldavad näiteks NASA kuue turvatasemega metoodika ja Saksamaa riigiasutustes rakendatav keskmise turvataseme saavutamiseks määratud BSI metoodika. BSI meetod lähtub objekti tükeldamisest kihtideks tüüpmooduliteks (alamobjektideks); 2008. a versioonis oli selliseid mooduleid 74 (vt ka 4.4.1). Iga mooduli turvaspetsifikatsioon esitab mooduli ohud ja neid ohte kõrvaldavad turvameetmed.

Tüüplahenduste meetod võimaldab projekteerimisfaasis säästa aega ja kulutusi, kuid tekitab probleeme siis, kui tüüplahendus ei ole mingil põhjusel täielikult realiseeritav: jääkriski ja selle vastuvõetavust tuleb niisugusel juhul paratamatult hinnata muude, kulukamate meetoditega.

4.9 Tüüpturbe süsteem ISKE

ISKE on mõeldud andmekogude pidamisel kasutatavate infosüsteemide ja nendega seotud infovarade turvalisuse saavutamiseks ja säilitamiseks. ISKE rakendamine ei ole ühekordne projekt, vaid pidev protsess, sest muutuvad nii IT-keskkond, turvaohud, meetmed kui ka ISKE rakendusjuhend ise.

Turvameetmete määramiseks tuleb leida infovarale vastavad tüüpmoodulid (vt tabel 13). Tüüpmoodulite spetsifikatsioonis on loetelu meetmetest; meetmed tuleb rakendada arvestades turbeastet (vt 4.5.4 „Süsteemi ISKE aluseks olev turvaliigitus“). Aluseks tuleb võtta kõrgem turbeaste, st kõrgema turbeastme rakendamisel tuleb rakendada ka madalama turbeastme meetmed.

Kõrgema turbeastme meetmed jagunevad kohustuslikeks (HG) ja tingimuslikeks (HK, HT, HS). Tingimuslike meetmete rakendamine sõltub moodulirühma kõrgeima tasemega turvaosaklassi(de)st.

- Kõrgeima käideldavuse turvaosaklassi (K3) korral tuleb rakendada kõik alumises tabelis loetletud HK-meetmed.
- Kõrgeima terviklikkuse turvaosaklassi (T3) korral tuleb rakendada kõik alumises tabelis loetletud HT-meetmed.
- Kõrgeima konfidentsiaalsuse turvaosaklassi (S3) korral tuleb rakendada kõik alumises tabelis loetletud HS-meetmed.

Selleks, et saavutada soovitud tase, tuleb tüüpturbe puhul rakendada kõik turvameetmed. Tavapraktikas tehakse rakendamata meetmete osas eraldi detailne läbivaatus.

4.10 Riskianalüüsi automatiseerimine

Riskianalüüsi hõlbustavad selleks otstarbeks väljatöötatud analüüsiprogrammid. Võrreldes analüüsiküsimustike "käsitsi" töötlemisega (nt tabeliprogrammi abil), annab niisugune tarkvara enamasti 50 kuni 70% ajasäästu. Tooteid võib võimsuse ja funktsionaalsuse järgi laias laastus jagada kahte klassi – detailse kompleksanalüüsi pakettideks ja piiratud võimalustega nn ankeedidraiveriteks.

4.10.1 Detailse riskianalüüsi tarkvara

Niisugused paketid esitavad lähteandmete saamiseks sadu küsimusi, võimaldavad tavaliselt sooritada nii kvantitatiivset kui ka kvalitataiivset analüüsi ning on modulaarse struktuuriga, nii et kasutaja võib eraldi osta mingi funktsionaalse alamhulga (nt objekti füüsilise turbe hindamiseks). Hind varieerub sõltuvalt konfiguratsioonist, kuuludes keskmise funktsionaalsuse korral tavaliselt 10–20 tuhande dollari suurusjärku. Need on turbeala professionaalidele määratud instrumendid, mida kasutavad valitsused ja suurfirmad.

Selles klassis on üks juhtivaid tooteid sari RiskWatch samanimeliselt USA firmalt. RiskWatchi kasutab rida USA valisuse ametkondi, sh NASA ja mitmed kaitsestruktuurid, samuti paljud suurfirmad, nt *IBM*, *Vodafone*, *Mitsubishi* jt.

Suurte võimalustega ja paindlik on ühtsele teadmusbaasile toetuv ekspertsüsteem *Cobra* Briti firmalt *Ewen Associates*. Lisaks tavalise riskianalüüsi moodulile (Risk Consultant) sisaldab ta eraldi vahendeid näiteks kehtestatud turvapoliitika järgimise või standardile BS 7799 ja ISO 17799 vastavuse kontrolliks. Teistest tarkvaratoodetest mainivad nimetamist *Infogov Proteus Enterprise*, *SIGEA GxSGSI, Aexis RA2* ja *Acuity STREAM*.

Järgnev tabel esitab lühendatud kujul organisatsioonide Léger Research Foundation ja ENISA sooritatud tootevõrdlused [24].

Tabel 38. Riskianalüüsi pakettide võrdluse näide

	Callio Secura	**CERT OCTAVE**	**CRAMM**	**ÉBIOS**
Riskianalüüs:				
Tehniliste nõrkuste analüüs	Ei	Ei	Ei	Jah
Revisjonid	Jah	Jah	Jah	Jah
Riskihaldus:				
Protsess ohuallikate tuvastamiseks	Ei	Ei	Ei	Ei
Protsess nõrkuste tuvastamiseks	Ei	Ei	Ei	Jah
Protsess riskide hierarhiseerimiseks	Jah	Jah	Jah	Jah
Riskitaluvuse võrdlusbaas	Jah	Jah	Jah	Ei
Riski käsitlemine:				
Tasuvusanalüüs	Jah	Ei	Jah	Ei
Turvameetmete lisamine	Jah	Jah	Jah	Jah
Võimalike kahjude näitamine	Jah	Ei	Jah	Jah
Muu:				
Metoodika	Riskihaldus	Riskianalüüs	Riskihaldus	Riskihaldus
Mudel põhineb mänguteoorial/ otsustuspuudel	Ei	Jah	Ei	Ei
Mõõteskaala	Intervall-	Suhteline	Intervall-	Intervall-
Intervjuude kasutamine	Jah	Jah	Jah	Jah
Auditite kasutamine	Jah	Jah	Jah	Jah
Ühilduvus standarditega	ISO 27001, ISO 27002	OCTAVE meetod	ISO 27001	ISO 13335, ISO 15408, ISO 27002
Kohandatavad ankeedid	Jah	–	–	Jah
Rakendus(t)e tüüp	Veebipõhine	–	Autonoomne	Autonoomne

4.10.2 Kiiranalüüsi programmid

Sellesse klassi kuuluvad märksa piiratumate võimalustega vahendid. Nende andmehõive piirdub tavaliselt mõnekümne kuni sajakonna küsimusega ning analüüs hõlmab sageli ainult üht või paari alamobjekti või kaitseala (nt asutuse talitluse katkematust). Kommertstooted kuuluvad 1000 dollari hinnaklassi, kuid saadaval on ka priivara ja jaosvara. Odavatesse või tasuta toodetesse tasub siiski suhtuda ettevaatusega. Kuna selle klassi programmid on oma ehituselt üsna lihtsad, on selge, et müügihinda võetakse mitte koodijupi, vaid temas sisalduva turvaalase oskusteabe eest.

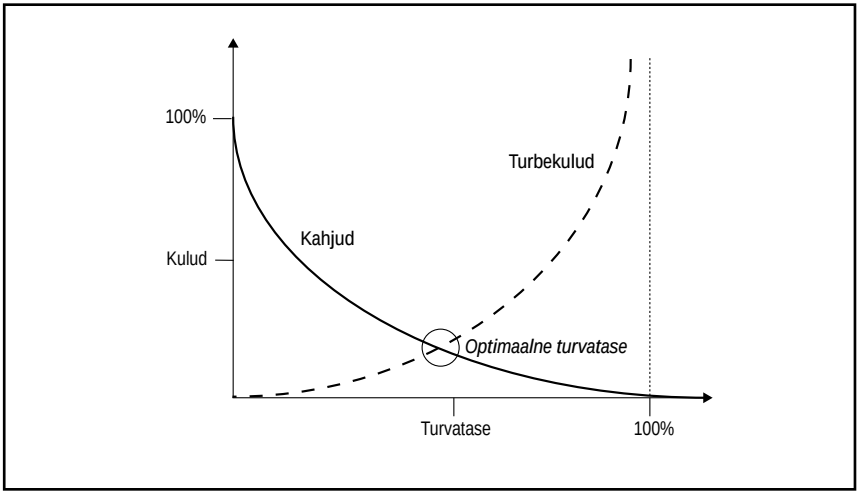
Küsitava väärtusega on sellised prii- ja jaosvaratooted, mis pretendeerivad küll täielikule kvalitatiivsele riskianalüüsile, kuid ei sisalda kuigi palju sisseehitatud teavet, pakkudes ainult elementaarse töötluse ja väljastuse funktsioone (nt *RISKIT* firmalt *Brian Rismam Associates*) ning jäädes seetõttu sisuliselt (ankeedita) ankeedidraiverite tasemele.

5 RISKI VÄHENDAMINE

Riski vähendamine on kogu infoturbe lõppeesmärk. Riski täielik kõrvaldamine on põhimõtteliselt võimatu, riski peaaegu täielikult kõrvaldamine aga ülemäära kulukas. See peatükk näitab kätte riski vähendamise üldise tee, laskumata tehnilistesse üksikasjadesse. Riskitõrjevahendite arsenali tutvustab raamatu II osa.

5.1 Turbe tasuvus

Riskianalüüsi tulemus ei anna üheselt lahendit järgmiste sammude sooritamiseks. Infovarade turve on tasuvusanalüüsi sisaldav tehnilis-majanduslik ülesanne, mille eesmärk on mitte varade maksimaalne, vaid optimaalne turvalisus. Tüüpiliselt kasvavad turbekulud turvamäära tõstmisel mitte lineaarselt, vaid eksponentsiaalselt (vt joonis 6). Optimaalne on minimaalsetele kogukuludele (kahjud + turbekulud) vastav turvatase.



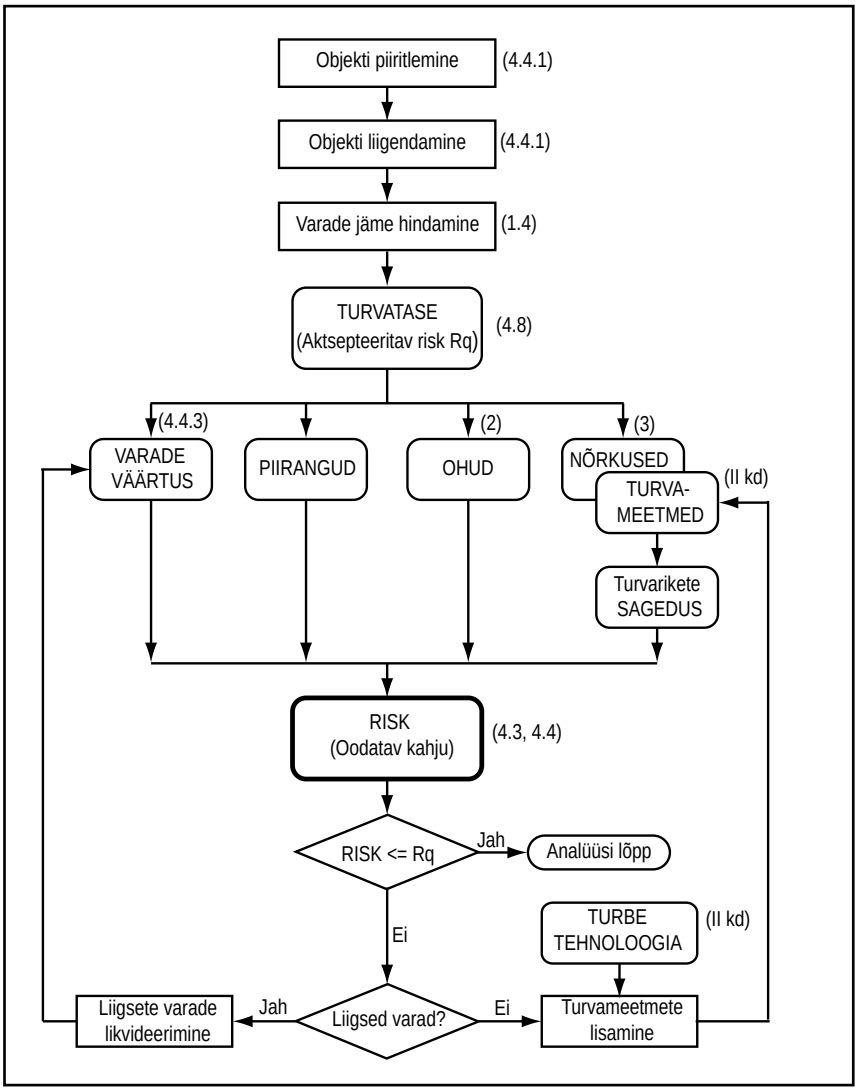
Joonis 6. Kahjude ja turbekulude tüüpiline sõltuvus turvatasemest

Arvutatud riski hindamise kriteeriumiks on **aktsepteeritav risk**, st selline oodatav kahju, mida on otstarbekas taluda, püüdmata teda kahandada üha kulukamate turvameetmetega. Kui arvutuslik risk ei ületa aktsepteeritavat, puudub turvameetmete lisamisel majanduslik põhjendus.

Kui arvutatud risk ületab aktsepteeritava, tuleb reastada suurusjärjestusse varade järgi arvutatud osakahjud ja ohtude järgi arvutatud osakahjud. Valitavad turvameetmed (vt II köide) tuleb suunata suurimatele varadele ja suurimatele ohtudele, arvestades meetmete võimalikku maksumust. Lisaks turvameetmetele tasub kaaluda ka turvakriitilistest, kuid vähetootlikest varadest loobumist.

Edasi on protsess iteratiivne. Valitud turvameetmete alusel korrigeeritakse ohtude ja nõrkuste loetelu ning ohtude realiseerumise tõenäosusi. Jääkriski leidmiseks korratakse riskianalüüsi. Protsessi korratakse, kuni jääkrisk on aktsepteeritav ja turbekulud on vastuvõetavad (vt joonis 7).

Turbekulude vastuvõetavus sõltub konkreetsest olukorrast; jämeda üldise orientiirina tasub teada, et 46% Suurbritannia erasektori ettevõtetest kulutas 2008. aastal infoturbele 6% või rohkem oma IT-eelarvest, sh 22% ettevõtetest rohkem kui 11% [5].



Joonis 7. Riski iteratiivne vähendamine

5.2 Infoturbe protsess

Kui organisatsioonis ei ole infoturvet kompleksselt ja süstemaatiliselt rakendatud, vajadus selleks on aga intuitiivsete hinnangute põhjal olemas, tuleb läbi teha turbeprotsess, mille tegevused ja tööd jagunevad neljaks järguks:

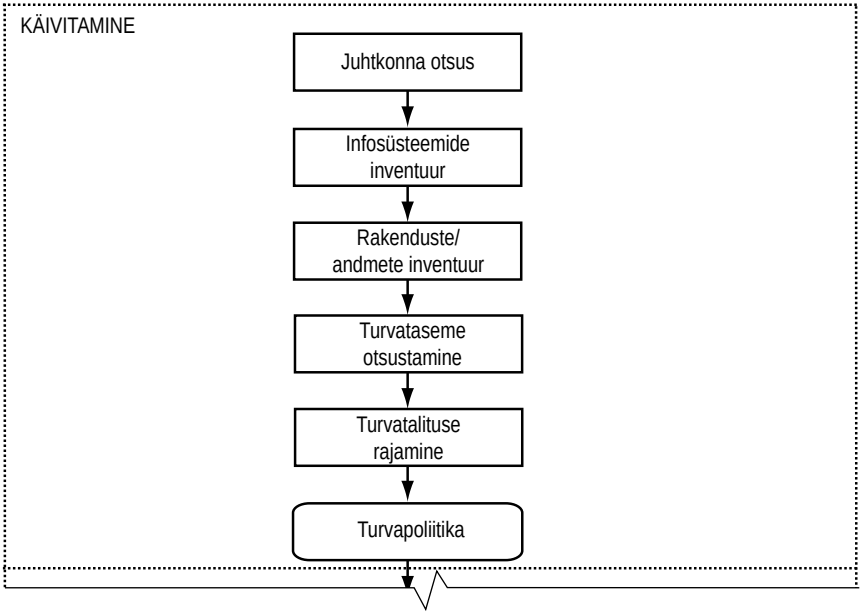
1) turbeprotsessi käivitamine,

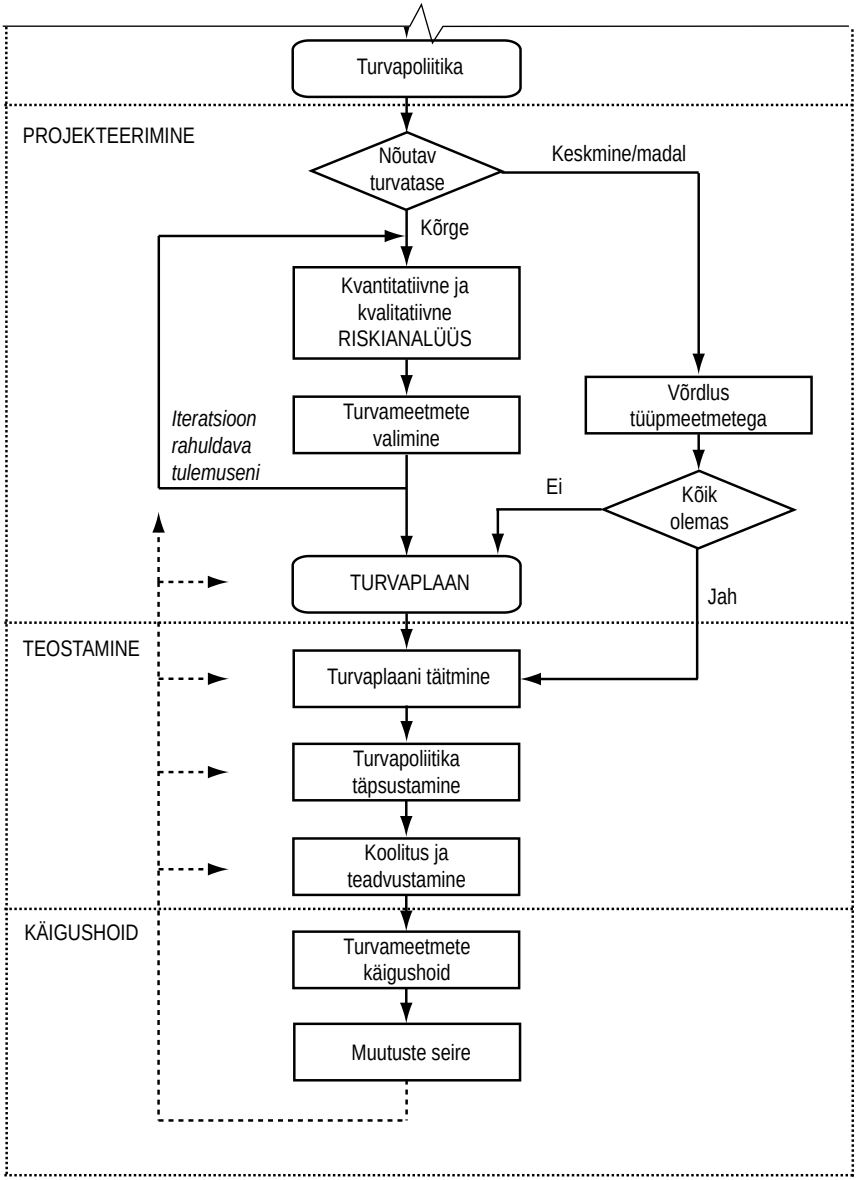
2) turbesüsteemi projekteerimine,

3) turbesüsteemi teostamine,

4) turbesüsteemi käigushoid.

Järkudeks ja põhitegevusteks liigendatud turvaprotsess on esitatud joonisel 8.





Joonis 8. Turbeprotsess

5.3 Turbeprotsessi käivitamine

Turbeprotsessi algatab asutuse või organisatsiooni juhtkond. Protsessi kõigis järkudes on oluline juhtkonna aktiivne toetus ja oma huvitatuse ilmutamine.

Kõigepealt tuleb välja selgitada turbe eesmärk, st selgitada välja otstarbekas **taotletav turvatase**. Selleks piiritletakse turbeobjekt (vt 4.4.1) ning sooritatakse infovarade inventuur (vt 4.4.2), alustades süsteemide spetsifitseerimisest ning jätkates iga süsteemi rakenduste ja andmete spetsifitseerimisega. Inventuur peab hõlmama ka plaanitud tulevasi süsteeme ning võimalikku konfiguratsioonide laienemist ja funktsioonide lisandumist.

Varad hinnatakse süsteemhaaval kvalitatiivselt käideldavuse, konfidentsiaalsuse ja tervikluse aspektist (vt 1.4 ja 4.5), fikseerides kõige kriitilisemad tundlikkusalad (iga süsteemi kõige tundlikumad rakendused ja turvaaspektid). Saadud koondandmete põhjal otsustatakse vajalik turvatase kaudse riskianalüüsi meetodil (vt 4.8). Otsus on kvalitatiivne, kuid peab piisava usaldatavusega eristama kõrget turvataset keskmisest või madalast.

Otsusega seatud eesmärgi saavutamiseks ja vajaliku turvataseme edaspidiseks tagamiseks luuakse asutuses **infoturbetalitus**, mille suurus sõltub asutuse suurusest ja informatiseerimisastmest. Väiksema asutuse puhul piisab ühestainsast infoturbele spetsialiseerunud infotehnoloogist; selleks võib äärmisel juhul olla ka vastava koolituse saanud senine süsteemiülem (administraator), ehkki üldiselt soovitatakse hoida süsteemi- ja turvaülema rollid lahus. Suuremas asutuses võiks talitus koosneda infoturbe peaspetsialistist ja suuremate allüksuste (nt osakondade) turvaülematest.

Selles järgus alustatakse ka **turvapoliitika** dokumenteerimist. Turvapoliitika dokument fikseerib kirjalikult asutuse sihid infosüsteemide turvalisuse alal, nende seose asutuse põhitalitluse sihtidega ning üldreeglid nende sihtide saavutamiseks. Dokument peab kirjeldama taotletavat turvataset selle määramisel aluseks olnud tegurite kaudu, sõnastades eesmärgid nende tegurite terminites. Protsessi käivitusjärgus puuduvad poliitika lõplikuks detailiseerimiseks vajalikud andmed, seetõttu täiendatakse dokumenti järgmistes järkudes.

Käivitusjärgus peab dokument sisaldama eelkõige järgmist teavet:

- infovarade (andmed, IT, infrastruktuur, personal, immateriaalsed varad) piiritlemine;

- turbevajaduste määratlemine (nõutava turvataseme väljaselgitamine ja kehtestamine vastavalt asutuse eesmärkidele ja õigusaktides kehtestatud nõuetele; turvaeesmärkide väljaselgitamine kõikide infovarade jaoks);
- infoturbeorganisatsiooni loomine (teadaanne infoturbetalituse rajamisest, turbeülema(te) nimetamine, personali vastutus infoturbe alal ja selle delegeerimine).

Järgmistes järkudes lisatakse teavet ja reegleid valitud turvameetmete teostuskavade, plaanitud koolitusürituste, talitluse käigus sooritatava infoturbe juhtimise ja läbivaatuse, turvaintsidentidele reageerimise jms kohta (vt ka ISO 27002).

Turvapoliitikat esmase organisatsioonilise turvameetmena käsitletakse põhjalikumalt raamatu II osas.

5.4 Turbesüsteemi projekteerimine

Selle järgu tegevused sõltuvad käivitusjärgus määratud nõutavast turvatasemest.

Kõrge turvatase nõuab ulatuslikke turvameetmeid, seega mahukamaid rahalisi ja muid ressursse. Intuitiivsed või liiga jämedalt põhjendatud otsused võivad siin kergesti viia vaeg- või liigturbest tingitud majanduslike kahjudeni, seetõttu on otstarbekas lähtuda kvantitatiivsest (vt 4.4) või võimalikult detailsest kvalitatiivsest (vt 4.7) riskianalüüsist.

Pärast turvameetmete valimist hinnatakse jämedalt nendega seotud kulutused, korratakse analüüsi ja leitakse jääkrisk. Vajaduse korral korrigeeritakse turvameetmete (ja varade) valikut. Iteratsioon lõpetatakse, kui juhtkond otsustab, et jääkrisk ja turvakulud on vastuvõetavad. Kui rahuldavat lahendit ei leita, tuleb korrigeerida turvaeesmärke, jaotades objekti erineva turvatasemega alamobjektideks ja nõudes kõrget turvataset ainult kõige kriitilisematele alamobjektidele.

Keskmine või madal turvatase on saavutatav tagasihoidlikumate meetmetega, seetõttu võib detailanalüüsist loobuda, võttes lahenduse aluseks mingi standardse või muu tunnustatud etalonlahenduse. Vormilt võib etalonlahenduse kirjeldus olla näiteks

- küsimustik,
- meetmete kataloog,
- meetmete kahe- või kolmemõõtmeline maatriks (nt põhiohtude ja/või turvataseme alusel),
- interaktiivne programm.

Sellise lahenduse kasutamine taandub senise süsteemi võrdlusele etalonsüsteemiga ning senises süsteemis puuduvate meetmete spetsifitseerimisele.

Projekteerimise tulemuseks peab olema funktsionaalprojekt – **turvaplaan**, mille peamised koostisosad on järgmised:

- teostamisele kuuluvate turbemeetmete ja -vahendite funktsionaalne spetsifikatsioon infotehnoloogiliste süsteemide haaval ning kahe või kolme alljärguna (nt lühikese, keskmise või pika teostustähtajaga),
- kulude kalkulatsioon (investeeringud, töötasud, koolituskulud jm),
- detailne ajakava prioriteetide, eelarvete ja tähtaegadega,
- teostuseks vajalike ürituste, väljatööteprojektide, detailprojektide jms loetelu,

- teostuse halduse plaan (kohustuste ja ressursside jaotus, teostuse juhtimismehhanismid jne).

Olukorra muutustele operatiivse reageerimise tagamiseks täpsustatakse andmed tööprojekti tasemeni (nt turvavahendite konkreetsete tüüpide valik jne) vahetult teostusjärgus.

5.5 Turbesüsteemi teostamine

Selles järgus täpsustatakse kõik lühitähtajalised plaanid ja spetsifikatsioonid, valitakse ja dokumenteeritakse organisatsioonilised turvameetmed ning hangitakse või töötatakse välja füüsilised ja infotehnoloogilised turvameetmed. (Turbetehnoloogia aluseid ja konkreetseid turvameetmeid käsitleb raamatu II osa.)

Lühitähtajalised plaanid täidetakse. Koostatakse koolitus- ja teadvustusseminaride kava ning vastavad õppematerjalid, võttes arvesse ka võimalikke turvameetmetest tingitud muutusi infotehnoloogia kasutamisel.

Täiendatakse turvapoliitika dokumenti. Koostatakse asutuse **turvajuhend**, mis sisaldab alalisi kohustusi infoturbe alal ning reegleid ja protseduure turvarikete puhuks, kaasa arvatud taasteplaan.

Koolitus- ja teadvustusüritused peavad hõlmama kogu personali, kaasa arvatud juhtkond, ning hõlmama eeskätt järgmisi teemasid:

- asutuse turvaeesmärgid ja -poliitika, kommenteeritult ja näidetega;
- infoturbe tähtsuse põhjused konkreetses asutuses;
- infoturbega seotud kohustused, ametijuhendid ja protseduurid;
- turvanõuete analüüsi tulemused, seletused ja neist tulenevad riski vähendamise kavad;
- turvavahendite teostuse ja kontrolli kavad;
- turvaintsidentide toime kasutajaile ja asutusele;
- turvarikete teadistuse vajadus ja teadistuse kord;
- turvaeeskirjade individuaalse rikkumise tagajärjed.

Kursusi tuleb korraldada regulaarselt, eriti tehnoloogilise või turvasituatsiooni oodatavate või asetleidnud muutuste korral ning eeskätt kaasates uusi töötajaid.

5.6 Turbesüsteemi käigushoid

Protsessi selles järgus on turvatalituse ja juhtkonna põhitegevused järgmised.

Infoturbe taseme säilitamine nõuab järgmisi eeldusi ja sooritatavaid töid.

- Turbevahendite hoolduseks talitluse ajal peavad olema organisatsioonilised eeskirjad. Neid tuleb järgida kõigi hooldetööde sooritamisel.
- Personali kohustused ja vastutus peavad olema ametijuhendite ja turvajuhendiga selgelt jaotatud ja piiritletud.
- Turbevahendite õiget talitlust tuleb regulaarselt kontrollida.
- Pidevalt tuleb jälgida jooksvat turvasituatsiooni. Turvavahendeid tuleb uute ohtude või turvaaukude ilmnemisel tugevdada või lisada, vajaduse korral korrates riskianalüüsi.
- Turvavahendid tuleb operatiivselt kohandada personali, organisatsiooni, riistvara, tarkvara, rakenduste, süsteemide asukoha jms muutustega.

Turbevahendite kontroll algab juba teostusjärgu lõpetamisel. Peamised toimingud ja tegevused on järgmised:

- turbevahendite õige teostuse kontroll enne nende käikuandmist;
- turbevahendite õige kasutamise perioodiline kontroll;
- turbevahendite kasutajatepoolse aktsepteerimise kontroll;
- turvapäevikute kontroll ja analüüs.

Eesmärgipärasuse kontroll on perioodiline. Kesksel kohal on

- saavutatu võrdlus turvapoliitikas fikseeritud eesmärkidega ja
- turvategevuse edukuse kontroll asutuse turvanõuete seisukohalt.

Muudatustele reageerimine peab olema seda operatiivsem, mida kõrgem on nõutav turvatase. Turvapoliitika, turvaplaan ja käigusolevad turvameetmed tuleb uuesti läbi vaadata kõigi oluliste muutuste puhul. Niisuguste muutuste hulka kuuluvad

- tööülesannete endi või nende tähtsuse muutused;
- füüsilised muutused, näiteks kolimine;
- muutused infotehnoloogias ja selle hindamises;
- muutused vajaliku käideldavuse, tervikluse ja konfidentsiaalsuse hindamises;

• ohtude või turvaaukude muutused.

Turvaintsidentidele reageerimine peab olema määratletud asutuse turvajuhendis. Eeskirjade täitmist tuleb regulaarselt kontrollida ning vajaduse korral turvajuhendit korrigeerida.

5.7 Infoturbe korralduse standardimine

Eelnevad jaotised andsid ülevaate turvariski haldamiseks vajalikest tegevustest. Kui raamatu esmatrüki ajal oli infoturbe korraldus veel nii uus valdkond, et puudusid standardid ja üldtunnustatud head tavad, siis tänaseks on pilt oluliselt muutunud.

Turvariski tulemuslikuks haldamiseks tuleb käsitleda võimalikke turvaohte ja -nõrkusi süsteemselt ja kõiki infoturbe aspekte arvestades. Protsesside süsteemsuse tagab standardsete metoodikate ja heade tavade järgimine. Standardid on olulised, sest lisaks protektsionistlikele ja turgu reguleerivatele eesmärkidele kehtestavad nad ühtse globaalse mõisteruumi ja panevad paika valdkonna üldpõhimõtted.

Infoturvet käsitlevaid standardiorganisatsioone on mitmeid. Neist suurim ja kõige laiema kandepinnaga on riikide rahvuslikke standardimisinstitutsioone ühendav Rahvusvaheline Standardiorganisatsioon (ISO), kes korraldab IT-standardimist koos Rahvusvahelise Elektrotehnikakomisjoniga (IEC) läbi vastava tehnilise ühendkomitee (JTC1). Infoturbe halduse osas kooskõlastab ISO oma standardimistegevust Rahvusvahelise Telekommunikatsiooniliiduga (ITU), mille käigus on ISO ja ITU teineteise standardeid üle võtnud. Teised koostööorganisatsioonid nagu OASIS, Liberty jt standardivad peamiselt turvalahendusi.

Infoturbe standardimine algaski turvalahendustest nagu TCSEC (*Trusted Computer Systems Evaluation Criteria*), koodnimetusega „Orange Book“, mis kehtestas USA juurtega sertifitseerimiskriteeriumid, ning selle Euroopa analoogist ITSEC (*Information Technology Security Evaluation Criteria*). Nende põhjal loodi hiljem *Common Criteria* (üldised nõuded turvatoodetele ja muudele turvalahendustele), millest on tänaseks saanud kolmeosaline standard „ISO/IEC 15408 Evaluation criteria for IT security“. Standard sätestab, et turvalahendus peab vastama teatud turvaeesmärkide komplektile (*Protection Profile*) ning määratleb eesmärkide täitmiseks vajalikud turvanõuded, millele vastavust kontrollitakse sertifitseerimisega.

Soovitud turvataseme saavutamiseks tuleb hallata mitte üksnes turvalahendusi, vaid kogu infoturbe korraldust. Esimese süsteemse käsitluse infoturbehaldusest pakkus Briti standardiorganisatsiooni (Briti BSI) loodud „BS 7799 Infoturbehalduse tegevusjuhis”, mis lõi mõiste „infoturbehalduse süsteem“ (*Information Security Management System*, ISMS). Standardi mitteametlik tõlge oli ühtlasi ka esimene eestikeelne infoturbe korraldamise juhend. Praegusajal

reguleerib finantsasutuste infoturbehaldust Eesti standard „EVS-ISO/IEC 13569 Pangandus ja sellega seotud teenused. Infoturbe korraldus."

Saksamaal töötas Infotehnika Turbe Liiduamet (Saksa BSI) riigiametite tarbeks välja tüüpturbe metoodika (vt 4.8), mis annab nii vahendid riskianalüüsiks ja turvanõuete määratlemiseks kui ka detailse kogumi vajalikke turvameetmeid. Saksa BSI infoturbe käsiraamatuid värskendatakse iga-aastaselt. Ka Eesti ISKE metoodika (vt 4.9) tugineb Saksa BSI metoodikale, kasutades kokkuleppel BSI-ga ära Saksa riigi pakutud võimalusi.

Infoturbehalduse aspekte käsitleb oma standardites ka USA riiklik standardimisorgan NIST, kes alates 1996. aastast annab välja föderaalseid infotöötluse standardeid (*Federal Information Processing Standards*, FIPS) ning ka mitmeid teisi turbehalduse ja turbetehnoloogiatega seotud standardeid. Ülevaade NISTi infotöötluse standarditest on kättesaadav aadressilt http://csrc.nist.gov/publications/. Standardimisega tegeleb USA-s ka vabatahtlik standardimisinstitutsioon ANSI, kes turvalisuse vallas ise aktiivne ei ole, aga aitab välja töötada ja levitada ISO vastavaid standardeid.

Kuna ISO/IEC infoturbe standardimise allkomitee SC27 pidas BS 7799 liiga raamatupidamisele suunitletuks, alustas ta uue turbehalduse standardi loomist. Rahvusvaheliselt jõuti turbehalduse standardimise osas üksmeelele viieosalise standardiga „ISO/IEC 13335 Infoturbe halduse suunised". See käsitleb infoturbe haldust pideva protsessina, mis hõlmab rolle nagu turvanõukogu, infoturbe eest vastutavad isikud jt. Tõlgituna on see üle võetud ka Eesti standarditeks.

- Osa 1: Infoturbe mõisted ja mudelid
- Osa 2: Infoturbe haldus ja plaanimine
- Osa 3: Infoturbe halduse meetodid
- Osa 4: Turvameetmete valimine
- Osa 5: Võrguturbe halduse suunised

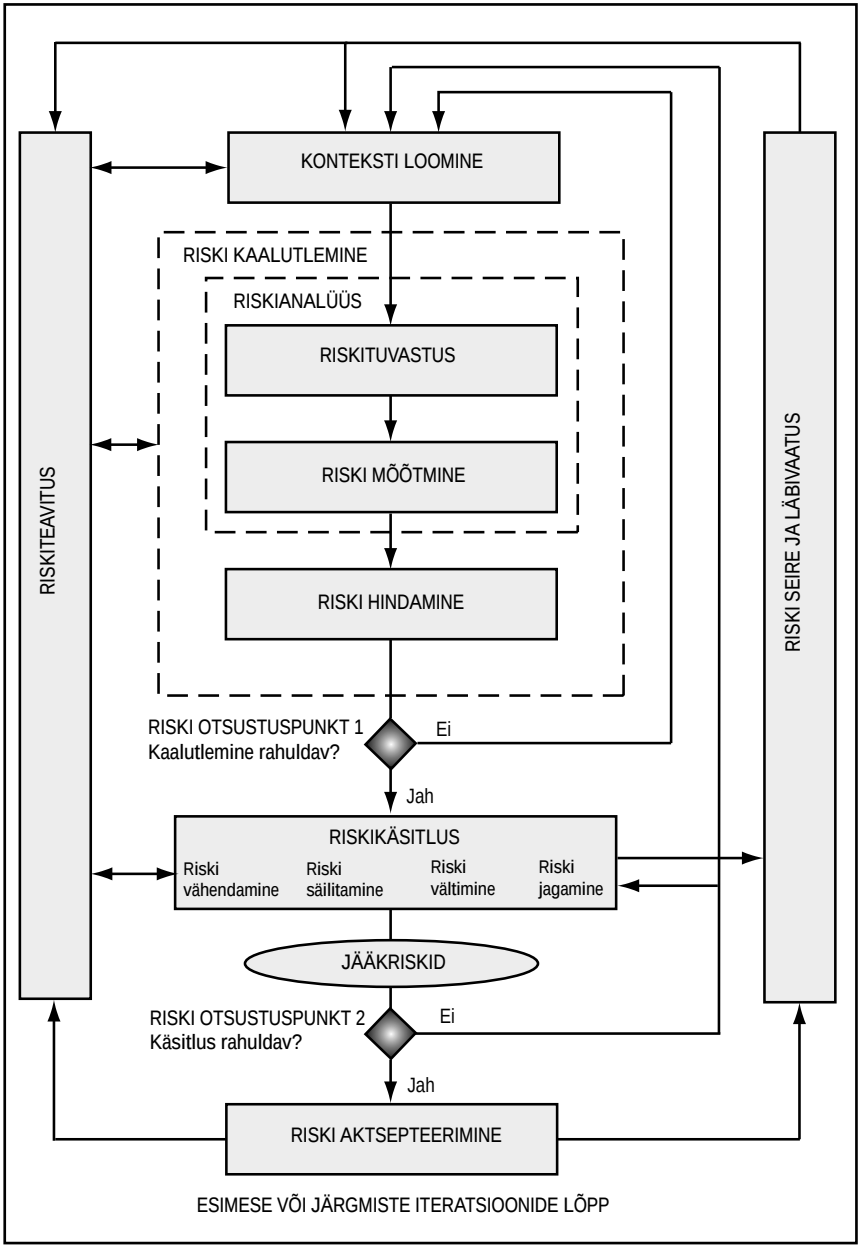
Väga laia valdkonnakäsitluse tõttu kujunes ISO 13335 üldsõnaliseks infoturbe halduse probleemide ülevaateks, mille praktiline külg ei vastanud ootustele. Seetõttu tõusis esile oma standardites turbehalduse sertifitseerimisnõudeid esitav Briti BSI, kelle standard BS 7799 võeti ISO standardiks (ja tõlkena Eesti standardiks) nime all "ISO/IEC 17799 Infoturbe halduse koodeks". Hoolimata ISO algsest vastuseisust võeti standardina vastu ka BS 7799 pakutud sertifitseerimisskeem.

Praeguseks on loodud infoturbe halduse standardite perekond ISO/IEC 27000. See põhineb standarditel 17799-1 ja 17799-2, mis olid aluseks vastavalt ISO/IEC

27002 ja ISO/IEC 27000 esmaversioonidele. 27000-seeria on kavandatud sertifitseerimisskeemiga standardite sarjana, nii nagu on ISO 9000 kvaliteedihaldussüsteemide osas, ISO 14000 keskkonnahaldussüsteemide osas ja ISO 20000 IT-teenuste halduse osas. Turbehalduse standardite arengukava näeb ette üha suuremat integratsiooni üldiste tööprotsesside ja keskkonnahalduse standarditega ning ühtse, kõiki haldusprotsesse käsitleva standardi loomist. See tähendab, et turbehalduse kavandamisel tuleks see algusest peale siduda teiste olemasolevate haldussüsteemidega.

Praegu on 27000-seeriast plaanitud ja osaliselt juba ka valmis järgmised standardid. Suund on kehtestada oma standard iga valdkonna jaoks, kus infoturbe haldus vajab mõnevõrra erilist käsitlust. Tärniga märgistatud standardite avaldamistähtaeg on raamatu kirjutamishetkel veel lahtine.

- ISO/IEC 27000: 2007, *Information security management systems - Overview and vocabulary*
- ISO/IEC 27001: 2005, *Information security management systems – Requirements*
- ISO/IEC 27002: 2005, *Code of practice for information security management*
- ISO/IEC 27003: 2008, *Information security management system implementation guidance*
- ISO/IEC 27004: 2007, *Information security management measurements*
- ISO/IEC 27005: 2007, *Information security risk management*
- ISO/IEC 27006: 2007, *Requirements for bodies providing audit and certification of certification of information security management systems*
- *ISO/IEC 27007, *Guidelines for information security management systems auditing*
- *ISO/IEC 27008, *Guide for auditors on ISMS controls*
- *ISO/IEC 27010, *Information Security Management for inter-sector communications*
- ITU-T X.1051 / ISO/IEC FDIS 27011: 2008*, Information security management guidelines for telecommunications organizations*
- *ISO/IEC 27012, *ISMS for e-government*
- *ISO/IEC 27013, *Guidance on integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001*



Joonis 9. Riski käsitlemise tegevus

- *ISO/IEC 27014, *Information Security Governence framework*
- *ISO/IEC 27015, *ISMS for Financial and Insurance Services Sector*

Eelolevast nähtub, et infoturbe riskihalduse osa on tänaseks jõudnud eraldi standardini ISO 27005, mis katab varem ISO 13335-3 ja ISO 13335-4 osades käsitletu. Uudsena on selles riskihalduse põhimõtteline skeem, mis annab selge ülevaate protsessi etappidest ja otsustuskohtadest.

Sellist riskihalduse protsessi eeldab ka infoturbe korraldust kirjeldav turbehalduse baasstandard ISO/IEC 27001. Turbehalduse korralduse aluseks on kohaldusmäärang (*Statement of Applicability*, SoA), mis sätestab nõuete rakendamise vastavalt riskikäsitlusplaanile. Kohaldusmäärang põhineb standardi ISO/IEC 27001 normatiivsel lisal A, mis loetleb kõigile organisatsioonidele üldjuhul rakendatavad turvameetmed, millest iga organisatsioon valib riskianalüüsi põhjal oma tegevuse jaoks vajalikud. Kohaldusmäärang on aluseks ka infoturbe halduse kontrollimisel – tema põhjal saab otsustada, kas organisatsioonis on selge arusaam riskidest ja tehtud konkreetsed otsused nende käsitlemiseks (st rakendada meetmeid või aktsepteerida risk). Kui see on tehtud, võib eeldada, et rakendatud meetmed on optimaalsed ning investeeringud infoturbesse asjakohased.

5.8 Infoturbe auditeerimine

Infoturbe auditeerimine on üks turvameetmetest. Rakendatud meetmete läbivaatus annab kinnituse nende asjakohase kasutamise kohta. Auditi tulemuseks on hinnang, kas rakendatud meetmed on vastavuses süsteemi(de)le esitatud nõuetele.

Infoturbe auditeerimine tähendas kunagi turvamehhanismide ülesehituse ja rakendamise analüüsi. Tänapäeval mõistetakse auditeerimise all kontrolli etteantud nõuetele vastavuse, headest tavadest kinnipidamise või teoreetiliste põhimõtete järgimise üle, mis juhindub objektiivsetest ja sõltumatust tagavatest protseduurireeglitest. Protseduurireeglid võivad olla riiklikult reguleeritud või kehtestatud mõne rahvusvahelise või erialaliidu standardiga. Eestis koondab IS audiitoreid Eesti Infosüsteemide Audiitorite Ühing (EISAÜ, *http://www.eisay.ee*), mis on ühtlasi ka Rahvusvahelise Infosüsteemide Auditi ja Juhtimise Assotsiatsiooni (ISACA, *http://www.isaca.org*) haruorganisatsioon.

Infoturbe auditeerimist sooritatakse järgmistel põhjustel.

1) Organisatsiooni juhtkond soovib sõltumatut hinnangut rakendatud turvameetmete asjakohasusele, et mõista kulutusi infoturbele või teha kindlaks (vastavalt turvariski käsitlusviisile), kas rakendatud meetmed maandavad konkreetse riski.

2) Koostööpartnerid nõuavad organisatsioonilt vastavust teatud turvatasemele, mille kohta peab hinnangu andma sõltumatu osapool. Eesti oludes nõuavad seda näiteks emaettevõtted siinsetelt tütarfirmadelt.

3) Organisatsioon soovib mainekujunduse vm eesmärgil veenduda, et turbehaldus vastab standarditele või muudele nõuetele (näiteks on Euroopa Liit kehtestanud mitmesuguseid turbehalduse nõuded makseagentuuridele).

4) Organisatsioonil on riiklikult kehtestatud kohustus lasta auditeerida oma turvalahendusi või turbehaldust nõutava turbetaseme tagamiseks (näiteks X-teega liituvatele andmekogude haldajatel).

Auditil on järgmised põhitüübid.

- **Vastavusaudit** on levinuim audititüüp, mis kontrollib vastavust mingitele nõuetele, mis võivad olla kehtestatud standardite, riiklike määruste, rahvusvaheliste kokkulepete vms-ga. Vastavusauditi tulemuseks on audiitori järeldusotsus auditeeritud süsteemi nõuetele vastavuse kohta; sealjuures peavad mittevastavused olema eraldi välja toodud ning tõendatud.

- **Sertifitseerimisaudit** on vastavusaudit, mille puhul lisandub järeldusotsusele sellekohane sertifikaat. Järeldusotsus peab olema positiivne ning auditeerija peab olema selleks tegevuseks akrediteeritud.
- **Konsultatsiooniauditi** käigus annab audiitor nõu turbehalduse korralduse või konkreetsete turvalahenduste osas vastavalt varasemale olukorra ja lahenduse analüüsile. Analüüsitakse turvalahenduse asjakohasust, et teha kindlaks, kas valitud lahendus on kvaliteetne ja asjakohane ning kas lahendust kasutatakse ettenähtud viisil. Auditi aruanne sisaldab olukorra analüüsi, mis toob välja võimalikud nõrkused ning pakub nendele lahendusi. Konsultatsiooniaudit nõuab audiitorilt põhjalikke teooriateadmisi ning hea tava järgi tohib konsultatsiooniauditi läbi viinud audiitor sooritada vastavusauditi sama infosüsteemi kohta alles 24 kuud hiljem.
- **Turvatestide** käigus sooritatakse valitud lahenduse läbistustestimine, kasutades tehnilisi abivahendeid. Audiitor peab tagama, et testimine ei kahjustaks süsteemide toimimist, analüüsima testitulemusi ning andma nende põhjal soovitusi olukorra parandamiseks.

Enimkasutatud turbehalduse vastavusauditid Eestis on ISO/IEC 27001 audit ja ISKE-põhine audit. ISKE järgi korraldatud turbehaldus vastab meetmete osas ka ISO/IEC 27001 nõuetele (st ISKE rakendamisel saab näidata vastavust standardile ISO/IEC 27001) – erinevus on vaid kohaldusmäärangu vormis, mis ISKE puhul on turvameetmete rakendatuse tabeli kujul. Kohaldusmäärang ongi kõige olulisem ISO/IEC 27001 vastavusauditi dokument, kuna see sisaldab põhiosa hindamiseks vajaminevast teabest. Eestis tegeleb ISKE-põhise auditimetoodika ja rakendustööriista väljatöötamisega Riigi Infosüsteemide Arenduskeskus (*http://www.ria.ee/iske)*.

Võrdluseks on mujal maailmas (eelkõige USA-s) levinud SOX-vastavusaudit (*Sarbanes-Oxley Act*), millega kontrollitakse finantssüsteemidele esitatud turvanõuete täitmist. 2002. aastal väljatöötatud SOXi eesmärk on muuta raamatupidamisreeglite karmistamise kaudu börsiettevõtete finantstegevus läbipaistvamaks (ajendatud peamiselt nn Enroni skandaalist). Kuna Eesti seadused nõudsid äriettevõtetelt varemgi raamatupidamise läbipaistvust ja auditeerimist, siis üldjuhul on kohalikud süsteemid juba vastavuses Sarbanes-Oxley nõuetega. Seetõttu huvitab selline audit pigem välisfirmade Eesti tütarettevõtteid ning on asjakohane vaid juhul, kui tegutsetakse emafirma reeglite järgi ning emafirma süsteeme kasutades.

Turbehalduse auditeerimisel on võimalik lähtuda standardist „EVS-EN ISO 19011:2005 Kvaliteedi- ja/või keskkonnajuhtimissüsteemide auditeerimise juhi-

sed“. Alljärgnevad põhiprintsiibid, mis pärinevad nimetatud standardist, rakenduvad kõikide valdkondade audiitoritele.

1) Tegevuse terviklus: audiitor teeb oma tööd ausalt ja vastutustundega, järgib seadusi ja audiitorite eetikakoodeksit, ei osale teadlikult seadusvastastes toimingutes, ent respekteerib auditeeritava organisatsiooni õiguspäraseid ja eetilise eesmärke.

2) Tõene ja korrektne aruandlus: auditi aruanne peegeldab kõiki auditi leide, ka neid, mille osas audiitor ja auditeeritav jäid eriarvamusele.

3) Professionaalne hoolikus: audiitor rakendab maksimaalselt oma teadmisi ja oskusi, et tagada kliendile vajalikul tasemel hinnangud tema olukorra kohta.

4) Konfidentsiaalsus: audiitor hoiab saladuses kõiki temale auditi käigus teatavaks saanud kliendi andmeid ja muud kliendi ärilist või muul eesmärgil konfidentsiaalseks peetavat teavet.

5) Sõltumatus: audiitor peab olema sõltumatu nii süsteemist kui ka organisatsioonist, keda ta auditeerib. Samuti peaks audiitoril olema auditi läbiviimiseks piisavalt aega – konkreetse tähtajaga piiratud audiitor ei ole täiesti sõltumatu.

6) Väidete tõendatus: audiitor peab koguma objektiivseid tõendeid mistahes oma väidete kinnitamiseks.

Standardi ISO 19011 laiendus on infoturbehalduse süsteemide auditeerimise suuniste standard ISO/IEC 27007, mis lisab täiendavad sätted ja juhised turbehaldussüsteemide auditeerimiseks.

Lähtuda võib ka rahvusvahelisi häid tavasid sisaldavast ISACA metoodikast, mida saab kasutada nii auditeerimise alusmaterjalina kui ka infosüsteemide ja nende aspektide arendamiseks ja haldamiseks. Kõik ISACA infosüsteemide auditeerimise standardid ja juhendid on 2009. aastast saadaval EISAÜ kaudu ka eesti keeles. Osaliselt on eesti keelde tõlgitud ka ISACA keskne infosüsteemide juhtimise ja auditeerimise metoodika CobiT v2.0 (*Control Objectives for Information and related Technology*). ISACA arendab metoodikaid ja raamistikke kooskõlas rahvusvaheliste standarditega, näiteks järgib CobiTi käsitlus kvaliteedihalduse standardit ISO 9000, tarkvara elutsükli standardit ISO/IEC 12207, turbehalduse standardit ISO/IEC 27001 jt.

Turbehalduse auditeerimisel tuleb audiitoril sooritada enamjaolt samad tegevused, mis turbehalduse juurutamisel:

1) tutvuda õigusruumi ja regulatsioonidega,

2) teha kindlaks süsteemi(de)le esitatud turvanõuded,

3) teha kindlaks organisatsiooni turvariskid,

4) teha kindlaks vajalikud turvataseme mõõdikud,

5) teha kindlaks turbehaldussüsteemi seire ja läbivaatuse tegevused,

6) vaadata läbi eelmiste auditite tulemused.

Auditi läbiviimist hõlbustab hästidokumenteeritud turbehalduse protsess, mis arvestab vajadusega turvameetmete rakendamise tõendusdokumentide järele. Selliste dokumentidena arvestatakse ka arvutisüsteemi logisid, meiliarhiive või muid andmeid, mille alusel saab otsustada, et protsessid toimivad kirjeldatud viisil. Sama kehtib ka turbehalduse mõõdikute kohta.

Turbehalduse auditi käigus puutub audiitor vältimatult kokku konfidentsiaalse teabega. Teatud juhtudel saab mingeid infosüsteemi aspekte auditeerida üksnes erivolitusega, näiteks kui süsteemis töödeldakse riigisaladust sisaldavaid andmeid. Sellised asjaolud on vaja tuvastada auditi ulatuse määratlemisel juba enne auditit.

Töö iseloomu tõttu esitatakse audiitoritele kõrgeid nõudeid. Näiteks ISO/IEC 27007 nõuab turbehaldussüsteemide audiitorilt ühest küljest laialdasi IT-alaseid teadmisi ja kogemust, teisest küljest süsteemianalüütiku oskusi, mis võimaldavad mõista ettevõtte või organisatsiooni protsesse ja ärinõudeid. Rahvusvaheliselt sertifitseerib audiitoreid ISACA, kelle sertifikaat CISA (*Certified Information Systems Auditor*) kinnitab, et audiitori teadmised vastavad rahvusvaheliselt tunnustatud tasemele. Sertifikaadi saamise eeldus on vastava eksami läbimine ning tõendatud praktiline kogemus; taseme hoidmine eeldab pidevat täiendkoolitust. Koolitatakse ka ISO/IEC 27001 vastavusauditi juhtaudiitoreid; koolituse läbinud ja reaalse kogemusega juhtaudiitorid registreeritakse rahvusvahelises audiitorite registris IRCA.

5.9 Kokkuvõtteks

Infosüsteemide turve on tulemuslik siis, kui ta viiakse läbi süsteemiarenduse lahutamatu osana, läbimõeldud ja metoodilise protsessina. Edu saavutamiseks ei piisa juhuslike tehniliste vahendite ja nippide kogust ega ka turbetehnoloogia põhjalikust tundmisest, otsustavaks saab organisatsiooniliste meetmete oskuslik ja järjekindel rakendamine töö kõigis järkudes, alates käivitusotsuste langetamisest ja lõpetades turbesüsteemide igapäevase käigushoiu korraldusega. Turvakultuur peegeldab asutuse üldist töökultuuri.

KASUTATUD ALLIKAID

STANDARDID

EVS juhend 7:2004 Riskihaldus. Sõnavara. Standardites kasutamise suunised (ISO/IEC juhend 73:2002).

EVS-ISO/IEC 18028-1:2006 Infotehnoloogia. Turbemeetodid. Infotehnoloogiavõrkude turve. Osa 1. Võrguturbe haldus

EVS-ISO/IEC 18028-2:2006 Turbemeetodid. Infotehnoloogiavõrkude turve. Osa 2. Võrguturbe arhitektuur

ISO/IEC aruanne TR 13335-1 Infotehnoloogia. Infoturbe halduse suunised. Osa 1. Infoturbe mõisted ja mudelid

ISO/IEC TR 13335-4 Infotehnoloogia. Infoturbe halduse suunised. Osa 4. Turvameetmete valimine

prEVS-ISO/IEC TR 13569:2006 Rahandusteenused. Infoturbe suunised (Kavand arvamusküsitluseks)

EVS-ISO/IEC 2382 Infotehnoloogia. Sõnastik

ISO/IEC 9126-1:2001 Tarkvaratehnika. Toote kvaliteet. Osa 1. Kvaliteedimudel

ISO 7498-2:1989 Information processing systems. Open Systems Interconnection. Basic Reference Model. Part 2. Security Architecture

ISO/IEC 11770 Infotehnoloogia. Turbemeetodid. Võtmehaldus

ISO/IEC WD 18014 Information technology. Security techniques. Time stamping services

ISO/IEC 10118-3: 1997 Information technology. Security techniques. Hash-functions. Part 3. Dedicated Hash-functions

ISO/IEC 15945:2002 Information technology. Security techniques. Specification of TTP services to support the application of digital signatures

prEVS-ISO/IEC 27001:2006 Infotehnoloogia. Turbemeetodid. Infoturbe halduse süsteemid. Nõuded

MUUD ALLIKAD

Raamatu kirjutamisel kasutatud allikate rohkuse tõttu on alljärgnevasse loetellu võetud ainult valik sisult ja mahult kaalukamaid.

[1] **1996** Computer Viruses Prevalence Survey. *NCSA*, 1996. 43 pp.

[2] **2006** Australian Computer Crime and Security Survey.

[3] **2006** CSI/FBI Computer Crime and Security Survey. Computer Security Institute, 2006.

[4] **2008** CSI Computer Crime & Security Survey. *Computer Security Institute*, 2008.

[5] **2008** Information Security Breaches Survey: Technical report. *Department for Business Enterprise & Regulatory Reform (BERR)*, 2008. www.berr.gov.uk/sectors/infosec

[6] **2008** Internet Malware Trends: Storm and the Future of Social Engineering. Ironport Systems (Cisco), 2008.

[7] **Bocan, V., Creţu, V.** Threats and Countermeasures in GSM Networks. Journal of Networks, vol. 1, no. 6, November/December 2006.

[8] **BS 7799:1995** Code of Practice for Information Security Management. *BSI*, 1995. 54 pp.

[9] **Castano, S. , Fugini, M., Martella, G., Samarati, P.** Database security. *Addison-Wesley Publishing Co*, 1995. 456 pp.

[10] **Computer** Assurance Guidelines for the Commercial Sector. *Department of Trade and Industry, Information Security Policy Group*, 1996

[11] **Computer** Security. CS4601. Monterey, CA: *Naval Postgraduate School*,1995.

[12] **Computer** Viruses. An Executive Brief. *Symantec*, 1996. 11 pp.

[13] **ENISA**, 2005 *(http://www.enisa.europa.eu/rmra/)*

[14] **Gostev, A.** Mobile Malware Evolution: An Overview, Part 1. Sep 29, 2006. *(http://www.viruslist.com/en/analysis?pubid=200119916)*

[15] **Harley, D.** alt.comp.virus Frequently Asked Questions. Version 1.02f. 1996. 57 pp.

[16] **Information** Security Breaches Survey 1996. *NCC*, 1996.

[17] **Information** Systems Security Policy. *Automated Information Security Policy Review Team*, 1995.

[18] **Information** Technology Security (ITS) Minimum Baseline Protective Requirements. Draft. *NASA*, 1996.

[19] **Infowatch:** Internal IT Threats in Europe 2006. (http://www.infowatch.com/threats?chapter=162971949&id=207784668)

[20] **IT Baseline Protection Manual** 2004**.** *Bundesamt für Sicherheit in der Informationstechnik*, 2004.

[21] **IT-Grundschutzhandbuch** 2008. *Bundesamt für Sicherheit in der Informationstechnik*, 2008.

[22] **ITU** Study on the Financial Aspects of Network Security: Malware and Spam. Final Report July 2008. International Telecommunication Union, 2008. (www.itu.int/ITU-D/cyb/cybersecurity/).

[23] **Kaitsepolitseiamet.** *Aastaraamat 2008*.

[24] **Léger Research Foundation** 2006 (*http://www.leger.ca/pages/articles/RAM.html*)

[25] **McAfee** Virtual Criminology Report 2008: Cybercrime Versus Cyberlaw. McAfee, Inc., 2008. (http://resources.mcafee.com/content/NAMcAfeeCriminologyReport)

[26] **MessageLabs** Intelligence: 2007 Annual Security Report. (http://www.messagelabs.com/resources/mlireports)

[27] **National** Industrial Security Program Operating Manual. Automated Information Security Policy Review Team, 1995.

[28] **Niall Fitzgibbon, Mike Wood.** Conficker.C. A Technical Analysis. *SophosLabs, Sophos Inc*, April 1, 2009.

[29] **NRL** IS Security Course and Handbook.

[30] **Roberts, C.M.** Biometric Attack Vectors And Defences. September 2006.

[31] **Schleier, J., Zimmermann, D.** Viren. SecuNet, 1996. 23 S.

[32] **Security** Risk Management Plan for Release B for the ECS Project. EOSDIS Core System Project. 627-CD-002-001. *Hughes Information Technology Systems*, 1996.

[33] **Stang, D. J.** Virus Prevention Policies that Work. *Seven Locks Software*, 1996. 24 pp.

[34] **Storey, N**. Safety-Critical Computer Systems. *Addison-Wesley Publishing*, 1996. 453 pp.

[35] **Symantec** Report on the Underground Economy. July 07–June 08. Symantec Corporation, November 2008.

[36] **Symantec** Spam Report. Symantec Corporation, 2009.

[37] **The Computer** Security Handbook of DCRT. National Institutes of Health, 1996.

[38] **US-CERT** Quarterly Trends And Analysis Report. August 25, 2008. Volume 3, Issue 3.

[39] **Worldwide** Infrastructure Security Report, Volume IV. Arbor Networks, 2008.