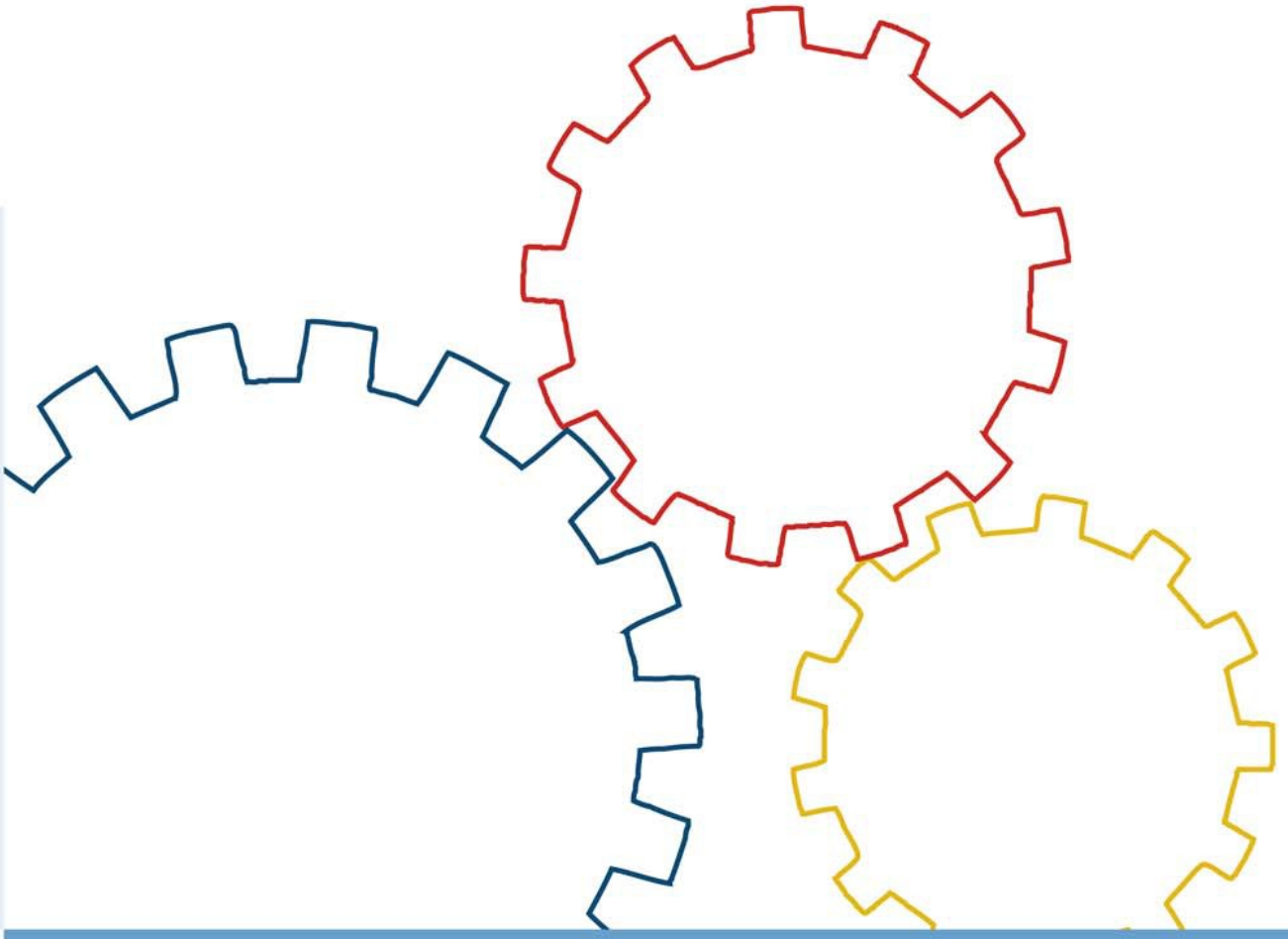
Bundesamt
für Sicherheit in der
Informationstechnik

Standard BSI 100-2

IT-etalonturbe metoodika



www.bsi.bund.de/gshb

Versioon 2.0

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185–189, 53175 Bonn

Sisukord

1 Sissejuhatus

1.1 Versioonide ajalugu

Seis	Versioon	Muudatused
Detsember 2005	1.0	
Mai 2008	2.0	Keskendub rohkem infoturbele võrreldes varasema IT-turbega, mistõttu on mõisteid kohandatud • Täiendatud andmekaitseaspektid • Kohandatud ISO standardite täiendustega • Parem liigendus • Struktuurianalüüsiks vajalike andmete kogumise järjekorra muutus Turbeprotsessi ülesannete selge lahutamine: peatükk 3 käsitleb ettevalmistavaid ja peatükid 4–6 rakenduslikke ülesandeid

1.2 Eesmärk

BSI on IT-etalonturbe näol välja töötanud tõhusa infoturbehalduse metoodika, mida saab kohandada ettevõtte või ametiasutuse konkreetsete oludega.

Järgnevates peatükkides kirjeldatud metoodika põhineb standardil BSI 100-1 „Infoturbehalduse süsteemid (ISMS)" (vt [BSI1]) ja selgitab seal esitletud IT-etalonturbe metoodikat. Infoturbehalduse süsteem (ISMS) sisaldab infoturbe planeerimise ja organiseerimise metoodikat, mille eesmärk on infoturbe piisava turbeastme saavutamine ja selle säilitamine. Sel eesmärgil kirjeldatakse põhjalikult iga standardis BSI 100-1 kirjeldatud faasi puhul soovitatud rakendusmeetodeid.

IT-etalonturve kujutab endast standardit, mis aitab organisatsiooni kogu infot piisavalt kaitsta ja kaitset säilitada. BSI poolt aastal 1994 kasutusele võetud ja sellest alates pidevalt täiustatud IT-etalonturbe metoodika pakub esiteks võimalusi infoturbehalduse süsteemi loomiseks ning teiseks põhjalikku alust riskianalüüsiks, olemasoleva turbeastme kontrollimiseks ja sobiva infoturbe juurutamiseks.

IT-etalonturbe üks tähtsam eesmärk on vähendada infoturbeprotsessi käigushoidmisele kuluvat tööd, pakkudes komplekssset ja jätkusuutlikku metoodikat, millega infoturvet pidevalt paremaks muuta. Seetõttu kajastavad IT-etalonturbe kataloogid levinud tööprotsesside ja IT-süsteemidega kaasnevaid standardseid ohte ja nende turbemeetmeid, mida tuleks vajadust mööda organisatsioonis rakendada. IT-etalonturbes soovitatud standardsete töökorraldust, personali ja taristuid puudutavate ning tehniliste turbemeetmetega saavutatakse tööprotsesside jaoks turve, mis vastab olulise info kaitsmiseks sobivale ja piisavale tavalisele turbeastmele. IT-etalonturbe kataloogides kajastuvad meetmed loovad muu hulgas hea aluse suure turbevajadusega IT-süsteemide ja rakenduste jaoks, kuid tavapärasest tõhusamat turvet pakuvad paljudel juhtudel isegi tavalahendused.

1.3 Sihtrühm

See dokument on suunatud peamiselt töötajatele, kes vastutavad infoturbe tagamise eest, samuti turbeekspertidele ja -nõustajatele ning kõikidele teistele huvilistele, kes puutuvad kokku infoturbehaldusega. Lisaks pakub see mõistlikku alginfot ka IT-turbe eest vastutavatele töötajatele,

juhttöötajatele ja projektihalduritele, kes peavad tagama, et nende hallatud organisatsioonis või projektides turvet unarusse ei jäetaks.

IT-etalonturvet saab rakendada ükskõik kui suurtes ning mis tahes eripäradega institutsioonides, mis vajavad soodsat ja sihipärast metoodikat nende jaoks vajaliku infoturbe ülesehitamiseks ja elluviimiseks. Institutsioon tähistab selles kontekstis nii ettevõtteid, ametiasutusi kui ka muid avalik-õiguslikke või eraalgatuslikke organisatsioone. IT-etalonturbe metoodikat saavad kasutada nii väga väiksed kui ka väga suured institutsioonid. Seejuures peab siiski arvestama, et kõiki soovitusi tuleb vaadelda konkreetse institutsiooni kontekstis ja sellest tuleb lähtuda ka nende elluviimisel.

1.4 Kasutussuunised

Standardis BSI 100-1 „Infoturbehalduse süsteemid" kirjeldatakse, milliste meetoditega on institutsioonis üldjuhul võimalik infoturvet juurutada ja suunata. Konkreetseid nõuandeid, mis aitavad infoturbehalduse süsteemi samm-sammult kasutusele võtta, pakub IT-etalonturbe metoodika. Seejuures kirjeldatakse protsessi erinevaid faase ja tutvustatakse ülesannetega toimetulekuks vajalikke lahendusi, mis on end juba praktikas tõestanud.

See metoodika loob ISMS-ile laialdase raamistiku, mille kohandamisega saavutatakse institutsiooni individuaalsetele vajadustele vastav infoturbehalduse süsteem. Pideva ja tõhusa infoturbeprotsessi edukas juurutamine eeldab mitmeid töösamme. IT-etalonturbe metoodika ja kataloogid annavad selleks juhiseid ja praktilisi nõuandeid.

Lisaks on IT-etalonturbe metoodika ka standard, mille alusel võib organisatsioon avalikustada sertifikaadi oma ISMS-i kvaliteedi kohta, ning kriteerium, mille abil saab hankida infot teiste organisatsioonide ISMS-i kvaliteedi kohta.

IT-etalonturbel põhinevat standardi ISO 27001 sertifikaati võib kasutada võimalikele koostööpartneritele esitatava turbenõudena, et täpsustada, milline peab olema partneri vajalik turbeaste. Ka neil juhtudel, kus ISMS-i aluseks võetakse mõni teine metoodika, võib IT-etalonturbest siiski kasu olla. Näiteks pakub IT-etalonturve võimalikke lahendusi mitmetele infoturbega seotud probleemsetele valdkondadele nagu kontseptsioonide loomine, revisjonide korraldamine või infoturbesertifikaadid. Olenevalt püstitatud ülesandest saab IT-etalonturvet rakendata mitmel moel, nt võib kasutada ainult selle üksikuid aspekte. Lähtuvalt kasutusalast võib teinekord ka juba üksikute komponentide, ohu- ja meetmekataloogide ning muude IT-etalonturbe abivahendite rakendamine luua tõhusa aluse turbehalduse töö tagamiseks.

Teisest peatükist leiate ülevaate ISMS-i kasutuselevõtu oluliste sammude ja turbekontseptsiooni koostamise metoodika kohta.

Kolmandas peatükis kirjeldatakse, milline võib olla infoturbeprotsessi evitamisfaas ja millised on seejuures kasulikud organisatsioonistruktuurid. Lisaks esitatakse viis, kuidas töötavat turbehaldust süstemaatiliselt juurutada ja seda töö käigus edasi arendada.

Neljandas peatükis kirjeldatakse IT-etalonturbe metoodikale vastavat turbekontseptsiooni koostamist. Seejuures näidatakse, kuidas koguda infokoosluse kohta algandmeid ja kuidas neid andmehulki rühmade moodustamisega vähendada. Seejärel tuleb olenevalt tööprotsessidest kindlaks määrata rakenduste, IT-süsteemide, sideühenduste ja ruumide turbevajadused. IT-etalonturbe kataloogide soovituste hulgast tuleb valida vaadeldava infokoosluse jaoks sobivad moodulid ja meetmed, luues IT-etalonturbe alusel oma organisatsioonile sobiva mudeli. Enne turbemeetmete võtmist tuleb IT-etalonturbe standardi BSI 100-3 (vt [BSI3]) põhjal teha turbeanalüüs ja seejärel riskianalüüs, et tuvastada ja defineerida olemasolevad ja lisanduvad turbemeetmed, et neid saaks integreerida IT-etalonturbe metoodikaga.

Kindlaks määratud ja konsolideeritud turbemeetmete rakendamist käsitleb viies peatükk.

ISMS-i oluline ülesanne on infoturbe tagamine. Infoturbe tagamist käsitleb kuues peatükk, mis selgitab kõige muu hulgas ka võimalusi, kuidas saavutatud turbeastet sertifitseerimise abil avalikustada.

IT-etalonturbe metoodikat ning ennekõike IT-etalonturbe katalooge täiendatakse regulaarselt ja kohandatakse uusimate suundumustega. Pidev kogemuste vahetamine IT-etalonturbe kasutajatega võimaldab arendust, mis arvestab kasutajate reaalsete vajadustega. Selle töö eesmärk on päevakohaste soovituste jagamine, et vältida ja kõrvaldada tüüpilisi turbeprobleeme.

1.5 Kasutatud kirjandus

[BSI1] „Managementsysteme für Informationssicherheit (ISMS)", standard BSI 100-1, versioon 1.5, mai 2008, www.bsi.bund.de

[BSI2] „IT-Grundschutz-Vorgehensweise", standard BSI 100-2, versioon 2.0, mai 2008, www.bsi.bund.de

[BSI3] „Risikoanalyse auf der Basis von IT-Grundschutz", standard BSI 100-3, versioon 2.5, mai 2008, www.bsi.bund.de

[GSK] „IT-Grundschutz-Kataloge – Standard-Sicherheitsmaßnahmen", BSI, ilmub kord aastas, http://www.bsi.bund.de/gshb

[SHB] „IT-Sicherheitshandbuch – Handbuch für die sichere Anwendung der Informationstechnik", BSI, versioon 1.0, märts 1992, Saksa riiklik trükikoda

[OECD] „Guidelines for the security of information systems and networks", Organisation for Economic Co-operation and Development (OECD), 2002, www.oecd.org/sti/security-privacy

[ZERT] „Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz – Prüfschema für ISO 27001-Audits", BSI, versioon 1.2, märts 2008, www.bsi.bund.de/gshb/zert

[ZERT2] „Zertifizierungsschema für Auditteamleiter für ISO 27001-Audits auf der Basis von IT-Grundschutz", BSI, märts 2008, www.bsi.bund.de/gshb/zert

[27000] ISO/IEC 27000 (3. CD, 2008) „ISMS – Overview and vocabulary", ISO/IEC JTC1/SC27

[27001] ISO/IEC 27001:2005 „Information technology – Security techniques – Information security management systems requirements specification", ISO/IEC JTC1/SC27

[27002] ISO/IEC 27002:2005 „Information technology – Code of practice for information security management", ISO/IEC JTC1/SC27

[27005] ISO/IEC 27005 (2. FCD, 2008) „Information security risk management", ISO/IEC JTC1/SC27

2 IT-etalonturbel põhinev infoturbehaldus

Ettevõtete ja ametiasutuste andmed on oluline väärtus, mida tuleb sobivalt kaitsta. Tänapäeval koostatakse, salvestatakse, transporditakse ja töödeldakse andmeid kui mitte täielikult, siis vähemasti osaliselt kindlasti IT-süsteemidega. Moodsad majandus- ja haldusprotsessid ei saa tänapäeval enam IT-ta toimida. Usaldusväärselt toimiv infotöötlus on iga ettevõtte jaoks asendamatu. Ebapiisavalt kaitstud info kujutab endast sageli alahinnatud riski, mis võib mõne institutsiooni puhul ohustada isegi selle olemasolu. Seejuures on info ja IT piisav turve saavutatav juba suhteliselt väikeste vahenditega.

Kõikide institutsiooni tööprotsesside, info ja IT-süsteemide jaoks vajaliku turbeastme saavutamiseks ei piisa üksnes viirusetõrjetarkvara, tulemüüride või andmevarundussüsteemide soetamisest. Oluline on tervikliku kontseptsiooni loomine. Esmajoones tähendab see töötavat ja organisatsiooniga integreeritud turbehaldust. Infoturbehaldus on üldise riskihalduse see osa, mis peab tagama info, rakenduste ja IT-süsteemide konfidentsiaalsuse, tervikluse ja käideldavuse. Seejuures on tegu pideva protsessiga, mille strateegiaid ja kontsepte tuleb pidevalt kontrollida ning vajaduse korral kohandada, et tagada nende kasutuskõlblikkus ja tõhusus.

Infoturbe puhul pole oluline mitte ainult tehnoloogia, vaid ka töökorralduslikud ja personaliga seotud raamtingimused. IT-etalonturbe metoodika ja BSI IT-etalonturbe kataloogid on andnud sellesse valdkonda oma pikaajalise panuse, avaldades tüüpilistele töövaldkondadele, rakendustele ja IT-süsteemidele nii tehnilisi kui ka mittetehnilisi standardseid turbesoovitusi. Esiplaanil on seejuures praktilised ja tööprotsessidest lähtuvad soovitused, mis võimaldavad turbemeetmete võtmise teha võimalikult lihtsaks ja vältida ülikeerukaid metoodikaid.

IT-etalonturbe metoodika näitab, kuidas luua tõhusat infoturbehalduse süsteemi ning kuidas IT-etalonturbe katalooge selle ülesande raames kasutada. IT-etalonturbe metoodika pakub koos IT-etalonturbe kataloogidega süsteemset võimalust turbekontseptsioonide väljatöötamiseks ning praktikas järele proovitud standardseid turbemeetmeid, mida juba arvukad ametiasutused ja ettevõtted edukalt kasutavad.

Alates 1994. aastast ilmuv, nüüdseks juba umbes 4000-leheküljeline IT-etalonturbe kataloogide kogu kirjeldab detailselt võimalikke ohte ja turbemeetmeid. IT-etalonturbe katalooge täiendatakse pidevalt, et ajaga kaasas käia. Kogu IT-etalonturbe info on tasuta kättesaadav BSI kodulehel. Toetamaks ametiasutuste ja ettevõtete rahvusvahelist koostööd, on kõik IT-etalonturbe dokumendid elektrooniliselt saadaval ka ingliskeelsena.

Üha suurem hulk tööprotsesse on omavahel ühendatud info- ja sidetehnoloogiaga. Selle tagajärjel muutuvad tehnilised süsteemid üha keerukamaks ja suureneb sõltuvus õigesti töötavast tehnoloogiast. Seega on eesmärgipärase turbeastme saavutamiseks ja tagamiseks vajalik, et kõik tööprotsessis osalejad tegutseksid plaanipäraselt ja organiseeritult. Selle protsessi juurutamist kõikides valdkondades saab tagada vaid juhul, kui juhtkonna kõrgeim tasand selle oma ülesandeks võtab. Juhtkonna kõrgeim tasand vastutab organisatsiooni sihipärase ja nõuetekohase toimimise eest ning tagab seeläbi infoturbe nii organisatsiooni sees kui ka sellest väljaspool. Seega peab juhtkond olema ühtaegu turbeprotsessi algataja, suunaja ja kontrollija. Infoturbe tagamiseks kõikides tööprotsessides tuleb välja töötada infoturbe strateegilised juhtnöörid, kontseptuaalsed nõuded ja töökorralduse raamtingimused.

Kuigi infoturbe eest vastutab alati juhtkonna kõrgeim tasand, delegeeritakse infoturbe tagamise ülesanne tavaliselt mõnele infoturbespetsialistile. IT-etalonturbe dokumentides on seda isikut sageli nimetatud infoturbespetsialistiks, kuid tema reaalsed tööülesanded on IT-turbest siiski palju laiemad.

Kui vastavad raamtingimused puuduvad, tuleks esmalt teha katset puuduvaid turbemeetmeid juurutada tööprotsesside tasandil. Kõikidel juhtudel tuleb kindlasti püüda juhtkonnale selgeks teha, milleks on infoturve vajalik, nii et juhtkond tulevikus selle eest ka täiel rinnal vastutust kannaks. Sageli on juhtunud, et infoturbega arvestatakse ainult tööprotsessides ning sellega on teema ammendunud, kuid tuleks arvestada, et nii parandatakse turvet ainult ajutiselt ega tagata turbe jätkusuutlikku arengut.

IT-etalonturbe meetod on võimalus, kuidas infoturbehaldust välja töötada ja seda organisatsiooniga

integreerida. Kui institutsioonil on tõhus ja tööprotsessidega integreeritud infoturbehaldus, võib olla kindel, et eesmärgiks seatud turbeastet suudetakse nii hoida kui ka tõhustada. See tagab, et institutsioon on võimeline silmitsi seisma ka uute proovilepanekutega.

Põhjalik ja hästi toimiv turbehaldus on institutsiooni turbemeetmete usaldusväärse ja järjepideva rakendamise asendamatu alus. Seetõttu on peale selle dokumendi põhjaliku kirjelduse IT-etalonturbe kataloogides ka moodul „Turbehaldus". Selle mooduli eesmärk on anda ühtne metoodika IT-etalonturbe rakendamiseks ning kaasata IT-etalonturbel tuginev turbehaldus standardile ISO 27001 vastavasse sertifitseerimisse.

IT-etalonturbe metoodika kõrval on IT-etalonturbe kataloogides ka palju nõuandeid selliste turbeprotsesside juurutamise kohta, mis põhinevad praktikas järele proovitud ja end juba tõestanud standardsetel turbemeetmetel. IT-etalonturbe eesmärk on saavutada võimalikult terviklik käsitlusviis. Standardsete töökorraldust, personali ja taristuid puudutavate ning tehniliste turbemeetmete võtmisega saavutatakse turve, mis vastab olulise info kaitsmiseks sobivale ja piisavale tavalisele turbeastmele. Meetmed loovad muu hulgas ka hea aluse suure turbevajadusega IT-süsteemide ja rakenduste jaoks, kuid tavapärasest tõhusamat turvet pakuvad paljudel juhtudel isegi tavalahendused.

IT-etalonturbe kataloogides kirjeldatakse, kuidas standardsete turbemeetmete põhjal turbekontseptsioone koostada ja nende täitmist kontrollida. Infotehnoloogia tüüpiliste protsesside, rakenduste ja komponentide jaoks on lisaks olemas sobivad standardsete turbemeetmetega moodulid. Need moodulid on oma eesmärgi alusel jagatud järgmiseks viieks osaks.

- Esimene osa sisaldab paljusid infoturbe üldisi aspekte. Siia kuuluvad nt moodulid „Personal", „Andmevarunduspoliitika" ja „Väljasttellimine".
- Teine osa käsitleb kõiki ehituse ja tehnikaga seotud asjaolusid. Siin osas on nt moodulid „Hooned", „Serveriruum" ja „Kodutöökoht".
- Kolmas osa keskendub konkreetsetele IT-süsteemidele. Siin osas on nt moodulid „Klient", „Server", „Kaugtöökoht", „Sülearvuti" ja „Mobiiltelefon".
- Neljandas osas vaadeldakse IT-süsteemide ühendamisega seotud aspekte, nt „Heterogeensed võrgud", „WLAN", „VoIP" ning „Võrgu- ja süsteemihaldus".
- Viies osa on rakendustest. Siia kuuluvad nt moodulid „E-post", „Veebiserver" ja „Andmebaasid".

Iga moodul sisaldab teema lühikirjeldust, nimekirja viidetega olulistele ohtudele ja vajalikele standardsetele turbemeetmetele. Ohud ja meetmed on üksteisest eraldatud vastavatesse ohu- ja meetmekataloogidesse. Ohukataloogid jaotuvad kategooriatesse „Vääramatu jõud", „Organisatsioonilised puudused", „Inimvead", „Tehnilised rikked" ja „Ründed". Meetmekataloogid sisaldavad selliseid kategooriaid nagu „Taristud", „Töökorraldus", „Personal", „Riist- ja tarkvara", „Kommunikatsioon" ning „Valmisolek hädaolukorraks".

2.1 Temaatika

Infoturbe eesmärk on info kaitsmine. Andmed võivad olla nii paberil, arvutis kui ka inimeste peas. IT-turve tegeleb esmajoones elektrooniliselt salvestatud andmete ja nende töötlemise kaitsmisega. Seega on „infoturve" tähenduse poolest parem ja laiem termin kui „IT-turve", mistõttu kasutataksegi aina enam terminit „infoturve". Seevastu IT-etalonturbe eesmärk on juba algusest peale olnud terviklik käsitlusviis, millega kaasatakse turbeprotsessi ka kõik sellised töö jaoks olulised andmed ja protsessid, mida IT otseselt ei puuduta või puudutab ainult osaliselt. Kuna aga erialakirjanduses kasutatakse endistviisi terminit „IT-turve", on see nii siin kui ka teistes IT-etalonturvet käsitlevates väljaannetes jätkuvalt kasutusel, kuigi tekstide koostamisel liigutakse järk-järgult siiski infoturbe suunas.

Infoturbe eesmärk on kaitsta info konfidentsiaalsust, terviklust ja käideldavust. Selle alla kuulub ka infotöötluse, seega eriti just IT-süsteemide kaitsmine. Infoturve käsitleb aga ka tervikluse erijuhu alla käivat info ja teadete autentsust ning nende vaieldamatut tõesust.

Infoturbeprotsessi juurutamiseks ja pidevaks tööshoidmiseks vajalikku planeerimist ja suunamist

nimetatakse infoturbehalduseks. Samadel põhjustel, mis kehtivad terminite „infoturve” ja „IT-turve” kohta, kasutatakse paljudes BSI dokumentides termini „infoturbehaldus” asemel sageli veel lühemat terminit „IT-turbehaldus”.

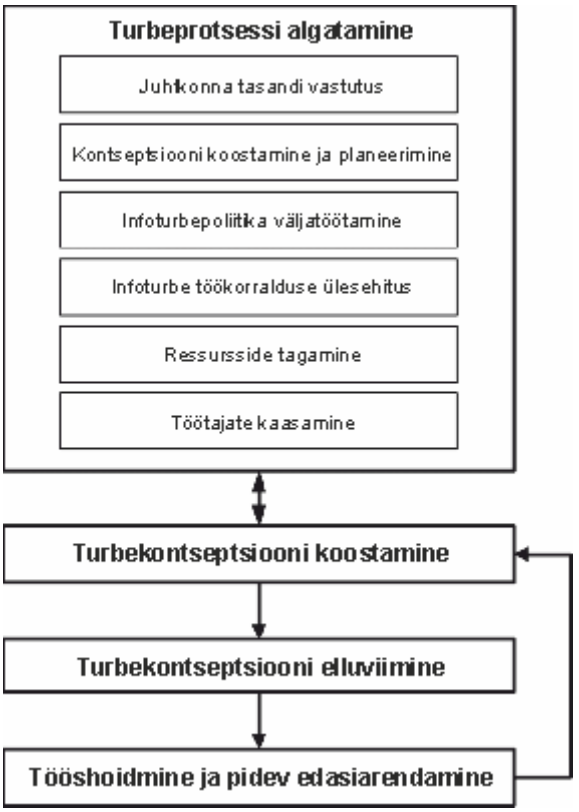
2.2 Infoturbeprotsessi ülevaade

IT-etalonturbe metoodika on institutsioonis abiks infoturbeprotsessi juurutamisel ja tööshoidmisel, näidates nii üldisi võimalusi ja meetodeid kui ka lahendusi konkreetsetele probleemidele.

Sobiva turbeastme saavutamine eeldab turbeprotsessi süstemaatilist kujundamist. IT-etalonturbe käsitluses koosneb turbeprotsess järgmistest faasidest:

- turbeprotsessi algatamine;
    - vastutuse teadvustamine juhtkonna tasandil;
    - turbeprotsessi kontseptsiooni koostamine ja planeerimine;
    - infoturbepoliitika väljatöötamine;
    - infoturbehalduse jaoks sobiva organisatsioonistruktuuri loomine;
    - finants-, personali- ja ajaressursside tagamine;
    - kõikide töötajate kaasamine turbeprotsessi;
- turbekontseptsiooni koostamine;
- turbekontseptsiooni elluviimine;
- infoturbe tööshoidmine ja selle pidev edasiarendamine.

Infoturbe eest vastutavad töötajad saavad IT-etalonturbe metoodikat ja katalooge kasutada erinevatel põhjustel ja eesmärkidel. Tingimused, kui intensiivselt ja millises järjekorras eri faase rakendada, annavad ette institutsiooni olemasolev turbekeskkond ja kasutaja vaatepunktid. Näiteks on turbekontseptsiooni regulaarsel ümbertöötamisel rõhuasetus sageli hoopis teine kui uute tööprotsesside integreerimisel.



Joonis 1. Turbeprotsessi faasid

Mõned faasid on teostatavad ka paralleelselt, nt võib turbeprotsessi kontseptsiooni loomine ja planeerimine toimuda infoturbeosakonna loomisega ühel ja samal ajal ning töötajaid saab koolitada ja teavitada kogu protsessi vältel. Sellisel juhul tuleb ettepoole toodud faase õigel ajal vastavalt uutele tulemustele ka muuta.

Järgnevalt antakse lühike ülevaade turbeprotsessi faasidest.

Turbeprotsessi algatamine

Turbeprotsessi algatamine, suunamine ja kontrollimine on juhtkonna ülesanne. Ühest küljest läheb selleks tarvis infoturbe strateegilisi juhtnööre ja teisest küljest organisatsioonilisi raamtingimusi. Toimiva turbeprotsessi ülesehitamist ja organisatsiooni vajalike struktuuride kindlaksmääramist kirjeldatakse kolmandas peatükis.

Turbekontseptsiooni koostamine

IT-etalonturbele vastava turbekontseptsiooni koostamine on mitmeosaline protsess, mida kirjeldatakse põhjalikult neljandas peatükis. Tähtsamad sammud on järgmised:

- struktuurianalüüs;
- turbevajaduse kindlaksmääramine;
- meetmete valik ja kohandamine;
- esmane turbekontroll;
- täiendav turbeanalüüs.

Turbekontseptsiooni elluviimine

Piisav turve saavutatakse ainult siis, kui esmalt selgitatakse välja puudused ja turbekontseptsiooni hetkeseis, seejärel tuvastatakse vajalikud meetmed ning lõpuks hakatakse neid meetmeid ka

järjekindlalt ellu viima. Viiendas peatükis kirjeldatakse, millega tuleb turbemeetmete planeerimisel arvestada.

Toimiva infoturbe tagamine ja pidev täiustamine

Turbehalduse eesmärk on vajaliku turbeastme saavutamine ning selle hoidmine ja pidev täiustamine. Sel põhjusel tuleb turbeprotsessi ja organisatsiooni infoturbestruktuure regulaarselt kontrollida, et veenduda, kas need on sobivad ja piisavalt tõhusad. Samuti tuleb kontrollida, kas turbekontseptsiooni meetmed on piisavalt praktilised ning kas neid rakendatakse õigesti. Kuues peatükk pakub ülevaadet sellest, millised tegevused on vajalikud infoturbe tööshoidmiseks ja tõhustamiseks.

2.3 IT-etalonturbe kataloogide kasutamine

Pärast seda, kui juhtkond on turbeprotsessi kindlaks määranud, st töötanud välja infoturbepoliitika ja loonud infoturbe toimimiseks vajalikud organisatsioonilised eeltingimused, jätkub turbeprotsessi elluviimine turbekontseptsiooni abil operatiivsel tasandil. Seetõttu on infoturbehalduse üks tähtsamaid ülesandeid kindlasti turbekontseptsiooni koostamine. Eelmise faasi tulemuste alusel tuvastatakse vajalikud turbemeetmed ja dokumenteeritakse need turbekontseptsioonina.

Kuna IT valdkonna ja selle kasutuskeskkonna tingimused on väga heterogeensed, kasutab IT-etalonturve nende paremaks struktureerimiseks ja töötlemiseks moodulprintsiipi. IT-etalonturbe kataloogide moodulites kirjeldatakse organisatsiooni infoturbe tüüpilisi valdkondi ja aspekte alates üldteemadest (nt infoturbehaldusest, hädaolukordadeks valmisolekust või andmevarunduse kontseptsioonist) kuni IT keskkonna erikomponentideni välja. IT-etalonturbe kataloogid sisaldavad mooduleid, kuhu on koondatud erinevate komponentide, metoodikate ja IT-süsteemide ohukirjeldused ning soovitatavad turbemeetmed. BSI muudab ja värskendab olemasolevaid mooduleid regulaarselt, et soovitused oleksid kooskõlas tehnika arenguga. Olemasolevatele lisaks koostatakse vajaduse korral ka uusi mooduleid.

Moodulitel on IT-etalonturbe metoodikas keskne roll. Kasutuse lihtsustamiseks on moodulid ühtse ülesehitusega. Iga moodul algab vaadeldavate komponentide, metoodika või IT-süsteemi lühikese kirjeldusega. Seejärel kirjeldatakse ohte. Ohud jagunevad seejuures valdkondadesse „Vääramatu jõud", „Organisatsioonilised puudused", „Inimvead", „Tehnilised rikked" ja „Ründed".

IT-etalonturbe kataloogides loetletud meetmed on standardsed turbemeetmed, mis tuleb moodulite kaupa vastavalt tehnika tasemele ellu viia, et tagada sobiv esmane turve. Seejuures on IT-etalonturbes nõutavad ja ISO 27001 sertifikaadi saamiseks vajalikud meetmed mõistliku turbeastme tagamise minimaalseks eelduseks ja neid tuleb seega kõikidel juhtudel kindlasti võtta. Need meetmed on IT-etalonturbe kataloogides tähistatud tähtedega L ja M. Meetmed, mille puhul kasutatakse märgistust „Täiendavad", on samuti praktikas järele proovitud, kuid nende võtmine on oluline tavapärasest suurema turbevajaduse korral. Seevastu meetmed märgistusega „W" annavad edasi teadmisi.

IT-etalonturbega loodavad turbekontseptsioonid on kompaktsed, sest kontseptsioonis tuleb viidata ainult IT-etalonturbe kataloogide asjakohastele meetmetele. See tagab hea arusaadavuse ja ülevaatlikkuse. Meetmetes toodud soovituste kergemaks elluviimiseks sisaldavad kataloogid ka turbemeetmete põhjalikke kirjeldusi. Erialase sõnavara kasutamisel on püütud arvestada sellega, et kirjeldused oleksid võimalikult loetavad ja arusaadavad.

Et meetmeid oleks lihtsam võtta, on IT-etalonturbe kataloogide tekstid kättesaadavad ka elektroonilisel kujul. Meetmete võtmist toetatakse muu hulgas ka abivahendite ja näitelahendustega, mis tuginevad osalt BSI töötajate ja osalt IT-etalonturbe kasutajate kogemustele.

Lisainfot leiate IT-etalonturbe kataloogide sissejuhatavatest peatükkidest, samuti selle standardi peatükist 4.4.

3 Turbeprotsessi algatamine

Institutsioonile sobiva ja piisava infoturbe saavutamine eeldab ühelt poolt planeeritud tegevust ja teiselt poolt adekvaatset organisatsioonistruktuuri. Lisaks tuleb kindlaks määrata turbe-eesmärgid ja nende eesmärkide saavutamise strateegia ning tagada turbeprotsessi järjepidevus. Kuna tegu on olulise valdkonnaga, mis kätkeb suurt vastutust ja mille otsused on kaugeleulatuvate tagajärgedega, peab algatajaks olema juhtkonna kõrgeim tasand.

3.1 Vastutuse võtmine juhtkonna tasandil

Iga ametkonna ja iga ettevõtte juhatuse kõrgeim tasand vastutab selle eest, et kõik valdkonnad toimiksid sihipäraselt ja nõuetekohaselt ning et kõik riskid saaksid võimalikult vara tuvastatud ja minimeeritud. Olenevalt organisatsiooni liigist ja selle tegevusvaldkonnast võivad selle tegevust reguleerida erinevad seadused. Kuna tööprotsessid olenevad infotehnoloogiast järjest rohkem, esitatakse ka sisemisele ja välisele infoturbele üha rangemaid nõudeid.

Turbeprotsessi algatamine, suunamine ja kontrollimine on juhtkonna ülesanne. Kuigi turbe elluviimise ja tööshoidmise kohustus delegeeritakse tavaliselt mõnele infoturbespetsialistile, jääb vastutus infoturbe eest alati juhtkonna kanda. Seejuures peab juhtkond infoturbehalduse protsessist ka ise intensiivselt osa võtma. Ainult nii saab infoturbehaldusega tagada, et institutsioon ei pea silmitsi seisma üle jõu käivate riskide ega ohuga teha väärinvesteeringuid. Juhtkonna kõrgeim tasand langetab seega otsuseid riskidega toimetulemise kohta ja eraldab vajalikud ressursid.

Tõsiasja, et turberiskide ennetamise ja nendele reageerimise eest vastutab juhtkond, ei mõista mitte kõik juhtkonnad kahjuks õigel ajal. Seetõttu jäetakse sageli infoturbega seotud kohustused ja vastutusalad kindlaks määramata. Kui IT- või turbespetsialistid ei edasta juhtkonnale õigel ajal ennetavat infot selle kohta, et info haldamise, tööprotsesside toimimise ja infotehnoloogia käsitsemisega võivad kaasneda riskid, võib juhtkond nad pärast turvaintsidenti selle eest vastutavaks teha. Seetõttu peaksid spetsialistid juhtkonda puuduliku infoturbega seotud riskidest ja võimalikest tagajärgedest ilmtingimata informeerima. Juhtkonna kohustus on aga tagada, et asjakohane info jõuaks nendeni õigel ajal ja vajalikus mahus. Turbe puhul on olulised nt järgmised teemad:

- institutsiooni ja selles hallatavat infot ohustavad turberiskid ning nende võimalikud tagajärjed ja kulud;
- turvaintsidentide mõju kriitilise tähtsusega tööprotsessidele;
- seadustest ja lepingutest tulenevad turbenõuded;
- spetsiaalselt institutsiooni tegevusvaldkonna jaoks välja töötatud standardsed infoturbemetoodikad;
- sertifitseerimine kui protsess, mis aitab klientidele, äripartneritele ja järelevalveorganisatsioonidele tõendada saavutatud infoturbeastet.

Kuna kõrvaliste kolmandate isikute ütlustel on sageli palju suurem mõju kui oma töötajate sõnadel, võib olla mõistlik kasutada juhtkonna teavitamiseks väliseid nõustajaid.

Juhtkond vastutab küll turbe-eesmärkide saavutamise eest, kuid turbeprotsessis peavad siiski osalema kõik organisatsiooni töötajad. Ideaaljuhul tuleks seejuures kinni pidada järgmistest põhimõtetest:

- infoturbe initsiatiiv peab tulema ametiasutuse või ettevõtte juhtkonnalt;
- infoturbe koguvastutus lasub juhatuse kõrgeimal tasandil;
- ametiasutuse ja ettevõtte juhtkond toetab aktiivselt infoturbe tagamist;
- ametiasutuse ja ettevõtte juhtkond nimetab ametisse infoturbe tagamise eest vastutavad töötajad ja
- tagab neile ressursid ning aitab neil omandada vajalikke oskusi;

- juhtkond on infoturbe tagamisel teistele eeskujuks.

Siia alla kuulub muu hulgas see, et juhtkond peab ka ise kõikidest ette antud turbereeglitest kinni pidama.

Juhtkond peab esmajoones seisma selle eest, et infoturve integreeritaks kõikide oluliste tööprotsesside, -ülesannete ja projektidega. Kogemused on näidanud, et infoturbespetsialist vajab ametiasutuse või ettevõtte juhtkonna täielikku tuge, et reaalselt vastutavad isikud kaasaksid teda igasse olulisse tegevusse ja ta oleks seeläbi võimeline tagama temalt nõutud tulemusi.

Juhtkond peab nii infoturbehaldusele kui ka kõikidele teistele valdkondadele kehtestama sellised eesmärgid, et turbeaste, mille poole püüeldakse, oleks igas valdkonnas saavutatav olemasolevate ressurssidega (personal, aeg, rahalised võimalused).

Peatüki 3.1 „Vastutuse võtmine juhtkonna tasandil" rõhuasetus

- Juhtkonnale selgitatakse puuduliku infoturbe võimalikke riske ja tagajärgi.
- Juhtkond võtab enda kanda infoturbe tagamise koguvastutuse.
- Juhtkond algatab organisatsioonisisese infoturbeprotsessi.

3.2 Turbeprotsessi kontseptsiooni koostamine ja planeerimine

Sobiva turbeastme saavutamiseks ja tagamiseks tuleb juurutada hästi toimiv infoturbeprotsess ning määrata kindlaks sobiv infoturbestrateegia. Infoturbestrateegia võimaldab planeerida edasisi samme, mis aitavad jõuda seatud turbe-eesmärkideni. Selle strateegia kehtestab juhtkond, arvestades seejuures ettevõtte ärieesmärkide või ametiasutuse tööülesannetega. Juhtkond annab ette põhilised turbe-eesmärgid ja määrab kindlaks, milline on tööülesannete täitmiseks vajalik infoturbeaste. Juhtkond peab tagama ka selleks vajalikud vahendid.

3.2.1 Raamtingimuste väljaselgitamine

Kõikide tööprotsesside ja tegevuste, kaasa arvatud infoturbe põhieesmärgid peavad lähtuma institutsiooni ülesannetest ja eesmärkidest. Sobiva infoturbestrateegia valimiseks peab seega iga institutsioon esmalt tuvastama oma olulisemad tööprotsessid ja -ülesanded ning määrama kindlaks nende infoturbevajaduse. Tänapäeval on vähe valdkondi, kus olulised tööprotsessid saaksid toimida infotehnoloogia abita. Kui otsustatakse selle üle, milline turbeaste on info ja infotehnoloogia turbe tagamiseks sobilik, tuleb aluseks võtta tööprotsesside ja nende käigus töödeldava info ning kasutatud infotehnoloogia vahelised seosed. Järgnevalt kirjeldatakse seda otsustamise protsessi lähemalt.

Iga tööprotsessi jaoks tuleb määrata kontaktisik, kes on n-ö info omanik ning vastutab kõikide selle tööprotsessiga seotud ja infotöötlust puudutavate küsimuste eest. Spetsialistid ja info omanikud vastutavad neile usaldatud tööprotsesside raames nt ülesannete delegeerimise eest. Iga tööprotsessi puhul tuleb kindlaks määrata, kui oluline on selles töödeldav info ja kui suur on selle info turbevajadus. Juhtkond peab iga tööprotsessi turbevajaduse kinnitama, sest turbevajadusest olenevad omakorda rakendatavad turbenõuded ja ressursid.

Tööprotsesside analüüsi põhjal saab teha järeldusi selle kohta, kuidas mõjutaksid organisatsiooni tööd turvaintsidendid. Sageli piisab ka sellest, kui piirduda tööprotsesside üldise kirjeldusega.

Vastused tuleks leida järgmistele küsimustele:

- millised on organisatsiooni tööprotsessid ja milline on nende seos organisatsioonis püstitatud eesmärkidega?
- millised tööprotsessid olenevad hästi toimivast, st stabiilselt ja nõuetekohaselt töötavast infotehnoloogiast?
- millist infot nende tööprotsesside raames töödeldakse?

- milline info on eriti oluline ning konfidentsiaalsuse, tervikluse ja käideldavuse seisukohast eriti suure turbevajadusega ja miks (nt isikuandmed, klientide andmed, ärisaladused, patendid, metoodikate kirjeldused)?

Paljud sisesed raamtingimused võivad mõjutada infoturvet ja seetõttu tuleb need tuvastada. Selles varases staadiumis ei ole peamine eesmärk infotehnoloogia detailne kirjeldus. Siiski läheb tarvis vähemalt umbkaudset ülevaadet, milles tuuakse välja, millist infot tööprotsessis töödeldakse ning milliseid rakendusi ja IT-süsteeme selleks kasutatakse.

Siseste raamtingimuste kõrval tuleb tuvastada ka kõik infoturvet mõjutavad välised raamtingimused, nt järgmised:

- seadustega ette antud raamtingimused (riiklikud ja rahvusvahelised seadused ning määrused);
- välismõjud, nt geograafilisest asendist või sotsiaalsetest ja kultuurilistest raamtingimustest lähtuvad mõjud;
- klientide, tarnijate ja äripartnerite nõudmised, turu hetkeseis, konkurentsiolukord ja muud olulised turupõhised sõltuvusseosed;
- tegevusalale omased turbestandardid.

Kõigi oluliste tööprotsesside raamtingimuste kiireks ja põhjalikuks kindlaksmääramiseks tuleks iga tööprotsessi jaoks maha pidada lühike turbekoosolek. Sellised turbekoosolekud peaksid toimuma infoturbespetsialisti juhtimisel, kaasata tuleks vastava info omanik või spetsialist, samuti vastav IT-spetsialist. Tulemused tuleks eelmääratud mudeli alusel dokumenteerida.

3.2.2 Infoturbe üldeesmärkide sõnastamine

Igat turbeprotsessi tuleks alustada sellest, et selgitatakse välja infoturbe täpsed eesmärgid. Muidu võidakse välja töötada turbestrateegiaid ja -kontsepte, mis ei vasta institutsiooni tegelikele vajadustele. Selle tulemuseks võib olla tahtmatute riskide võtmine, kuid ka investeeringud ebasobivatesse või liiga keerulistesse turbemeetmetesse.

Seetõttu tuleks institutsiooni põhieesmärkidest ja raamtingimustest esmalt tuletada üldised turbe-eesmärgid. Nendest tuleks omakorda turbekontseptsiooni koostamisel ja infoturbe töökorralduse kujundamisel välja töötada konkreetsed turbenõuded, mis reguleerivad info kasutamist ja IT-süsteemide käitamist. Institutsiooni üldised turbe-eesmärgid võivad olla nt järgmised:

- tööprotsesside ja infoga ümberkäimise suur usaldusväärsus (info käideldavus, terviklus ja konfidentsiaalsus);
- institutsiooni hea maine tagamine avalikkuse silmis;
- tehnoloogiasse, infosse, tööprotsessidesse ja teadmistesse investeeritud väärtuste säilitamine;
- suure või asendamatu väärtusega infotöötluse kaitsmine;
- info kvaliteedi tagamine, nt kui seda infot kasutatakse kaugeleulatuvate otsuste langetamiseks;
- seaduses ettenähtud nõuete tagamine;
- kulude minimeerimine võimalike kahjude korral (st nii kahjude vältimine kui ka toimetulek nende tagajärgedega);
- organisatsioonisiseste tööprotsesside järjepidevuse tagamine.

Turbe-eesmärkide kindlaksmääramiseks tuleks esmalt hinnata, millised tööprotsessid on institutsiooni ülesannete täitmiseks vajalikud ja milline on nende tähtsuse järjekord. Seejuures on oluline välja selgitada, mil määral oleneb organisatsiooni ülesannete täitmine info konfidentsiaalsusest, terviklusest ja käideldavusest ning kasutatud infotehnoloogiast ja selle töökindlusest. Turbe-eesmärkide defineerimiseks on mõistlik kaitstavaid väärtusi, nt käideldavust, terviklust ja konfidentsiaalsust, selgelt nimetada ja vajaduse korral need ka tähtsuse järjekorda seada. Sellised määratlused muutuvad

väga oluliseks turbeprotsessi jaoks vajalike turbemeetmete ja strateegiate valimisel.

Infoturbe ja turbeastme eesmärkide kindlaksmääramine on siiski vaid infoturbeprotsessi algus. Konkreetseid ressursse ja investeeringuid puudutavad otsused vajavad hiljem ka juhatuse kõrgeima tasandi kinnitust. See tähendab, et selles faasis pole infokoosluse ja turbemeetmete võimalike kulude detailne analüüs vajalik, tuleb vaid kindlaks teha, mis on organisatsiooni jaoks oluline ja miks.

3.2.3 Tööprotsesside sobiva turbeastme kindlaksmääramine

Infoturbe-eesmärkide paremaks mõistmiseks võib eesmärgiks seatud turbeastet kirjeldada üksikute, selgelt esiletõstetud organisatsiooni tööprotsesside või valdkondade näitel, arvestades infoturbe peamiste eesmärkidega (konfidentsiaalsus, terviklus ja käideldavus). Sellest on hiljem kasu detailsema turbekontseptsiooni koostamisel.

Järgnevalt on toodud mõned näited, kuidas selgitada välja sobiv turbeaste. Turbeastme (tavaline, keskmine või kõrge) väljaselgitamiseks tuleb hinnata, millised väited tunduvad teie olukorraga kõige sarnasemad. Selles turbeprotsessi faasis on oluline sõnastada esimesed suunavad väited, mida saab võtta aluseks järgmistes faasides, kuid üksikasjalik turbevajadus määratakse kindlaks alles hiljem.

Kõrge

- Ilmtingimata on tarvis tagada konfidentsiaalse info turve ning olulised turbevaldkonnad peavad vastama eriti rangetele konfidentsiaalsusnõuetele.
- Ülimalt oluline on info korrektsus.
- Institutsiooni tsentraalsed tööülesanded ei ole IT-ta täidetavad. Kriitilistele situatsioonidele tuleb reageerida väga kiiresti, mistõttu peab kogu aeg olema käepärast kõige värskem info. Töökatkestused pole vastuvõetavad.
- Kindlasti tuleb tagada isikuandmete kaitse. Muidu on ohus asjaosaliste elu ja tervis või isikuvabadus.

Kokkuvõte: IT-rike seiskaks institutsiooni töö täielikult või mõjutaks laialdaselt ühiskondlikke või majanduslikke huve.

Keskmine

- Ilmtingimata on tarvis tagada konfidentsiaalse info turve ning olulised turbevaldkonnad peavad vastama rangetele konfidentsiaalsusnõuetele.
- Töödeldav info peab säilima korrektsena ning võimalikud vead peavad olema äratuntavad ja välditavad.
- Institutsiooni tsentraalsetes valdkondades kasutatakse ajaliselt kriitilisi tööprotsesse või täidetakse hulgi kuhjuvaid ülesandeid, mida ei saa IT abita täita. Vastuvõetavad on ainult lühikesed töökatkestused.
- Isikuandmete kaitse peab vastama rangetele nõuetele. Muidu esineb oht, et asjaomase isiku ühiskondlik positsioon või tema majanduslik seis saab andmete avalikustamise tõttu raskelt kannatada.

Kokkuvõte: kahju korral muutub institutsiooni kesksete valdkondade toimimine võimatuks. Kahjude tagajärjed pärsivad tugevalt kas institutsiooni või sellega seotud kolmandate isikute tegevust.

Madal

- Sisekasutuse jaoks ette nähtud info peab olema kaitstud.
- Väiksemad vead on vastuvõetavad. Sellele vaatamata peab siiski olema võimalik õigel ajal märgata ja vältida vigu, mis võiksid tööülesannete täitmist oluliselt pärssida.
- Pikemad töökatkestused, mille tagajärjeks oleks tähtaegade ületamine, ei ole vastuvõetavad.

- Institutsioon peab tagama isikuandmete kaitse. Muidu esineb oht, et andmete avalikustamise tõttu saab kannatada asjaomase isiku ühiskondlik positsioon või majanduslik seis.

Kokkuvõte: kahjustused pärsiksid institutsiooni tööd.

Infoturbele seatavate eesmärkide sõnastamisel on juhtkonna kaasamine vältimatu. Sellesse turbeprotsessi jaoks olulisse etappi on võib-olla mõistlik kaasata ka väline infoturbespetsialist. Turbeastme väljaselgitamiseks tuleb vaadelda organisatsiooni eesmärke ja nendega seotud turbenõudeid, kuid seejuures tuleb võtta arvesse ka seda, et turbemeetmete juurutamiseks eraldatud ressursid on tavaliselt piiratud. Sel põhjusel on eriti oluline jõuda selgusele, milline on käideldavuse, tervikluse ja konfidentsiaalsuse tegelik vajadus, sest mida kõrgemat turbeastet soovitakse saavutada, seda rohkem kulub selleks aega ja muid ressursse. Kui võimalik, tuleks sõnastatud nõuded seada ka tähtsuse järjekorda. Sellest on abi turbeprotsessi hilisemates faasides ressursside planeerimisel.

Kirjelduse täpsusest

Infoturbeprotsessi varases faasis pole tarvis kõiki rakendusi ja IT-süsteeme detailselt kirjeldada ega ka põhjalikku riskianalüüsi teha. Oluline on saada ülevaade sellest, millised on tööprotsessidele või metoodikatele esitatavad turbenõuded. Näiteks peaks eesmärgiks seatud turbeastme alusel saama vastata järgmistele küsimustele:

- milline info on institutsiooni jaoks konfidentsiaalsuse, tervikluse ja käideldavuse seisukohast eriti oluline?
- millised institutsiooni jaoks olulised tööd muutuvad IT-ta võimatuks, osaliselt võimatuks või ainult suure lisavaevaga tehtavaks?
- millised institutsiooni olulised otsused sõltuvad info ja IT-süsteemide konfidentsiaalsusest, terviklusest ja käideldavusest?
- millised võivad olla tahtlike ja tahtmatute turvaintsidentide tagajärjed?
- kas IT-süsteemidega töödeldakse infot, mis on eriti suure turbevajadusega?
- kas olulised otsused sõltuvad infotehnoloogia abil töödeldava info korrektsusest, aktuaalsusest ja käideldavusest?
- millised seadusest tulenevad nõuded (nt andmekaitsenõuded) tekitavad vajaduse erimeetmete järele?

Eesmärgiks seatud turbeastme kirjeldused tuleb kohandada analüüsitava keskkonnaga. Lühikesed põhjendused on hiljem abiks meetmete planeerimisel. Näiteks haigla puhul võivad need kõlada järgmiselt: röntgeniosakonnas peab infoturbeaste olema väga kõrge, sest IT-süsteemide korrektsusest sõltub inimeste elu.

Peatüki 3.2 „Turbeprotsessi kontseptsiooni koostamine ja planeerimine” rõhuasetus

- Kõikide tööprotsesside jaoks kontaktisikute nimetamine
- Info ja tööprotsesside kaalukusele umbkaudse hinnangu andmine
- Raamtingimuste tuvastamine
- Tööprotsesside ja info olulisuse kindlaksmääramine
- Infoturbe üldeesmärkide kindlaksmääramine
- Juhtkonnalt nõusoleku saamine

3.3 Infoturbepoliitika väljatöötamine

Infoturbepoliitika raames kirjeldatakse kõikidele arusaadavalt, milliste eesmärkide jaoks ning milliste vahendite ja struktuuridega hakatakse institutsioonis tagama infoturvet. Infoturbepoliitika sisaldab institutsiooni infoturbe-eesmärke ja turbestrateegiat. Turbe-eesmärkide kaudu väljendab turbepoliitika

seega ametiasutuses või ettevõttes eesmärgiks seatud turbeastet. Seetõttu on ühtaegu tegu nii eesmärgi kui ka kinnitusega, et kirjeldatud turbeastet soovitakse saavutada kõikidel institutsiooni tasanditel.

Infoturbepoliitika väljatöötamine peaks hõlmama järgmisi samme.

3.3.1 Ametiasutuse või ettevõtte juhtkonna vastutus infoturbepoliitikas

Infoturbepoliitikaga dokumenteeritakse juhtkonna strateegiline seisukoht infoturbe eesmärkide saavutamisel kõikidel institutsiooni tasanditel.

Kuna infoturbepoliitika on institutsiooni infoturbe keskne dokument, peab see olema koostatud selliselt, et kõik institutsiooni üksused ja osakonnad tunneksid neile määratud sisu ära. Seega tuleb koostamisse kaasata võimalikult palju üksuseid. Sellele vaatamata peab iga institutsioon lõpuks siiski ise otsustama, millised osakonnad ja hierarhiatasandid on turbepoliitika väljatöötamisel olulised.

Siinkohal oleks mõistlik kasutada institutsiooni allüksuste töötajate erialaseid teadmisi. Näiteks võiks töösse kaasata oluliste rakenduste, IT-käituse, turbe (info, IT ja taristute) valdkonna vastutavad spetsialistid, samuti andmekaitsespetsialisti, personaliosakonna, töötajate esindaja, revidendi, finantsvaldkonna esindaja ja juristi.

3.3.2 Infoturbepoliitika kehtivusala ja sisu defineerimine

Infoturbepoliitika peab kirjeldama, milliste valdkondade kohta see kehtib. Kehtivusala võib hõlmata institutsiooni tervikuna või ka ainult selle üksikuid osasid. Siinkohal on oluline, et kehtivusalas oleksid täielikult kindlaks määratud vajalikud tööülesanded ja -protsessid. Kehtivusala täpne kindlaksmääramine võib osutuda üpris keeruliseks eriti just suuremate organisatsioonide puhul. Seejuures võib olla abiks, kui lähtuda vastutusaladest.

Turbepoliitika peaks olema sõnastatud lühidalt ja lihtsalt, sest praktika on näidanud, et enam kui kahekümneleheküljelised dokumendid ei ole otstarbekad. Dokumentatsioon peaks sisaldama vähemalt järgmist infot:

- infoturbe olulisus ning olulise info ja IT tähtsus tööülesannete täitmisel;
- infoturbe eesmärkide seos institutsiooni eesmärkide ja ülesannetega;
- turbestrateegia põhjal IT jaoks kehtestatud turbe-eesmärgid ja nende tuumelemendid;
- kinnitus, et organisatsiooni juhtkond rakendab turbepoliitikat, kirjeldused, kuidas infoturbeprotsessi jaoks hakatakse looma organisatsiooni struktuuri ja selle edukuse kontrollimise suuniseid.

Lisada võib ka nt järgmist infot:

- töötajate paremaks motiveerimiseks võib nimetada mõningaid tööprotsesside jaoks olulisi ohte ja seadusi ning muid olulisi raamtingimusi (nt lepingutest tulenevaid nõudeid);
- loetelu turbeprotsessi jaoks olulistest ülesannetest ja vastutusaladest (eriti need, mis puudutavad infoturbehalduse meeskonda, infoturbespetsialisti, IT kasutajaid ja administraatoreid). Lisaks võiks üles lugeda organisatsiooni allüksused või nende töötajate ametinimetused, kelle poole saab turvet puudutavate küsimuste korral pöörduda;
- võib kajastada infot edaspidiste infoturvet tõhustavate koolituste ja teavitusmeetmete kohta.

Joonis 2. Infoturbepoliitika sisu

3.3.3 Infoturbepoliitikat väljatöötava meeskonna loomine

Kui organisatsioonis on infoturbehalduse meeskond juba loodud, tuleks infoturbepoliitika väljatöötamine, kontrollimine ja muutmine usaldada selle meeskonna kätte. Seejärel tuleks poliitika kavand esitada kinnitamiseks ametiasutuse või ettevõtte juhtkonnale.

Kui infoturbehalduse valdkond on alles loomisel, tuleks moodustada meeskond, kelle ülesandeks saab turbepoliitika väljatöötamine. See meeskond võib turbeprotsessi arenedes võtta lõpuks enda kanda ka infoturbehalduse meeskonna ülesanded. Mõistlik oleks, kui sellesse meeskonda kuuluksid IT kasutajate esindaja, IT-süsteemide käitajate esindaja ja üks või mitu töötajat, kes on juba saanud piisavalt infoturbekoolitust. Ideaaljuhul peaks selles protsessis ajutiselt osalema ka mõni juhtkonna liige, kes oskab hinnata infotöötluse tähtsust institutsioonis.

3.3.4 Infoturbepoliitika avalikustamine

Ettevõtte või ametiasutuse juhtkond peab oma eesmärke ja ootusi turbepoliitika avalikustamisega rõhutama ning selgitama infoturbe olulisust kogu institutsioonis. Kõik töötajad peavad seega turbepoliitikat teadma ja sellest aru saama. Uutele töötajatele tuleb turbepoliitikat selgitada kindlasti enne seda, kui nad saavad juurdepääsu infotöötluse võimalustele.

Kuna ametiasutuse või ettevõtte juhtkond kannab turbepoliitika eest suurt vastutust, peab poliitika olema kirja pandud. Ametkonna või ettevõtte juhtkond peab turbepoliitika ametlikult heaks kiitma. Turbepoliitika sisu ei pea olema organisatsioonis mitte ainult teada, vaid ka võimalikult lihtsasti kättesaadav, nt organisatsiooni intranetis. Kui turbepoliitika sisaldab konfidentsiaalset infot, tuleb seda infot kajastada lisades, mis on konfidentsiaalsena selgelt tähistatud.

Lõpetuseks tuleb kõikidele töötajatele selgitada, et pühendumus, koostöö ja vastutustundlikkus on üldiste tööülesannete täitmise kõrval kindlasti väga olulised ka infoturbe tagamisel.

3.3.5 Infoturbepoliitika ajakohastamine

Infoturbepoliitika puhul tuleb regulaarselt kontrollida, kas see on piisavalt ajakohane, ja vajaduse korral seda kohandada. Selleks tuleks näiteks uurida, kas institutsiooni eesmärgid ja ülesanded ning seeläbi ka tööprotsessid, olulised IT-protseduurid ja institutsiooni struktuur on oluliselt muutunud ning kas kasutusele on võetud uusi IT-süsteeme. IT-valdkonna ja turbeolukorra kiire muutumise tõttu tuleks turbepoliitika sobivust kontrollida vähemalt iga kahe aasta möödudes.

Peatüki 3.3 „Turbepoliitika väljatöötamine" rõhuasetus

- Juhtkonna algatus turbepoliitika väljatöötamiseks
- Kehtivusala kindlaksmääramine
- Turbepoliitikat väljatöötava meeskonna loomine
- Turbepoliitika kinnitamine juhtkonnas
- Turbepoliitika avalikustamine
- Turbepoliitika regulaarne kontrollimine ja vajaduse korral uuendamine

3.4 Turbeprotsessi töökorraldus

Eesmärgiks seatud turbeastet on võimalik saavutada ainult siis, kui infoturbeprotsessi rakendatakse kogu institutsioonis. Kuna turbeprotsess mõjutab tervet institutsiooni, tuleb töötajate jaoks kindlaks määrata nende rollid ja rollide alusel ka ülesanded. Rollid tuleb anda kvalifitseeritud töötajatele. Ainult nii saab tagada, et kõikide oluliste aspektidega on arvestatud ja kõik tööülesanded täidetakse tõhusalt.

Infoturbeprotsessi edendamiseks ja kehtestamiseks vajalikku organiseerimist nimetatakse infoturbe

töökorralduseks.

See, kui palju inimesi infoturbega tegeleb, millistesse struktuuridesse nad jaotuvad ja kui palju on neil oma ülesannete täitmiseks ressursse, oleneb institutsiooni suurusest, eripärast ja struktuurist. Infoturbeprotsessi koordineerimiseks ja haldamiseks ning tõhusa suhtluse tagamiseks tuleb kindlasti kõikidel juhtudel ametisse nimetada infoturbespetsialist. Suuremates organisatsioonides on tavaliselt inimesi, kes täidavad erinevaid infoturbeülesandeid, kindlasti veel rohkem. Selliste töötajate tegevuse kooskõlastamiseks tuleks luua infoturbehalduse meeskond, kelle ülesanne on reguleerida kõiki infoturbe üldprobleeme ning töötada välja plaane, nõudeid ja suuniseid.

Et institutsiooni juhtkonnaga saaks kiiresti kontakti võtta, peaksid need rollid olema organiseeritud eksperdirühmana. Juhtkonnas peaks infoturbe eest vastutama üks kindel tegevjuht, kellele infoturbe eest vastutav töötaja esitab oma aruanded.

Olenemata sellest, millise lahenduse kasuks infoturbe töökorralduse puhul ka ei otsustata, tuleb kindlasti arvestada kolme põhireegliga.

Infoturbehalduse rollide defineerimise põhireeglid

- Vastutus tööülesannete nõuetekohase ja kindla täitmise eest (ja seega ka vastutus infoturbe eest) lasub juhtkonnal.
- Ametisse tuleb nimetada vähemalt üks isik (tavaliselt infoturbespetsialist), kes hakkab infoturbeprotsessi edendama ja juhtima.
- Iga töötaja vastutab võrdsel määral nii oma peamise tööülesande kui ka infoturbe tagamise eest oma töökohal ja selle ümbruses.

3.4.1 Infoturbe integreerimine üleorganisatsiooniliste tegevuste ja protsessidega

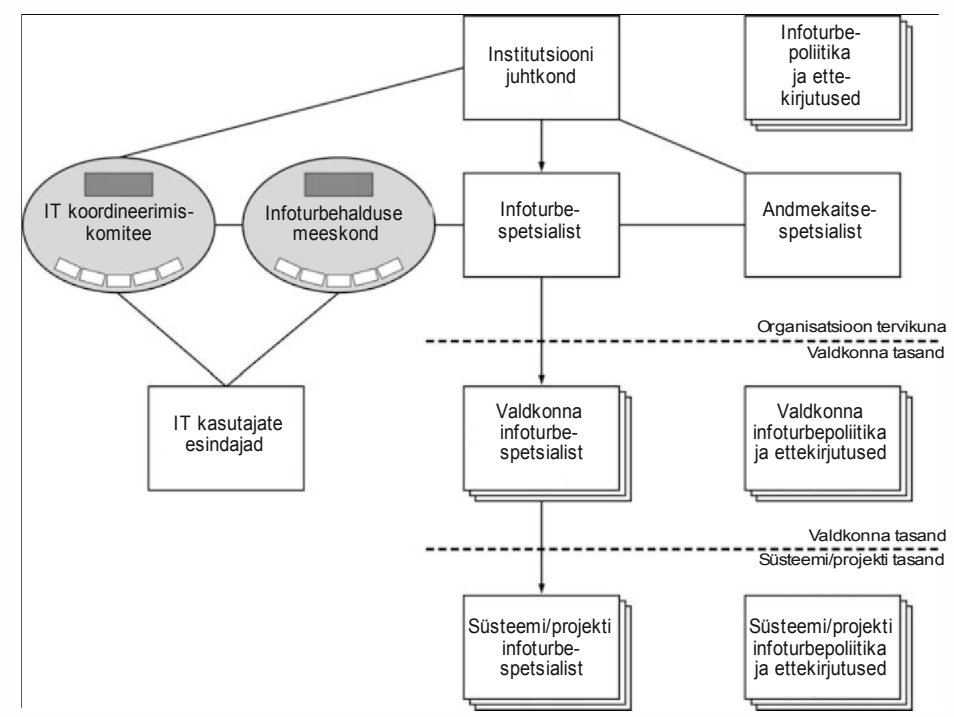
Infoturbehaldus on küll vaid üks paljudest olulistest haldusülesannetest, kuid mõjutab pea kõiki institutsiooni valdkondi. Seega tuleb infoturbehaldus olemasolevate organisatsioonistruktuuridega mõistlikult integreerida ja määrata kindlaks kontaktisikud. Ülesanded ja vastutusalad peavad olema üksteisest selgelt eraldatud. Seejuures peab olema tagatud, et vajalike turbeaspektidega ei arvestata mitte ainult üksikute meetmete, vaid kõikide strateegiliste otsuste puhul (nt väljasttellimisel või uute elektrooniliste turundusmeetodite kasutamisel). Selle tagamiseks on oluline kaasata infoturbe töökorraldus kõikidesse infoturvet mõjutavatesse projektidesse.

Eriti just suuremates institutsioonides on sageli juba kasutusel kõikehõlmav riskihaldussüsteem. Kuna IT-ga seotud riskid kuuluvad tööprotsesside kõige olulisemate riskide hulka, tuleks IT-ga seotud ohtude haldamine viia kooskõlla juba olemasolevate haldusmeetoditega.

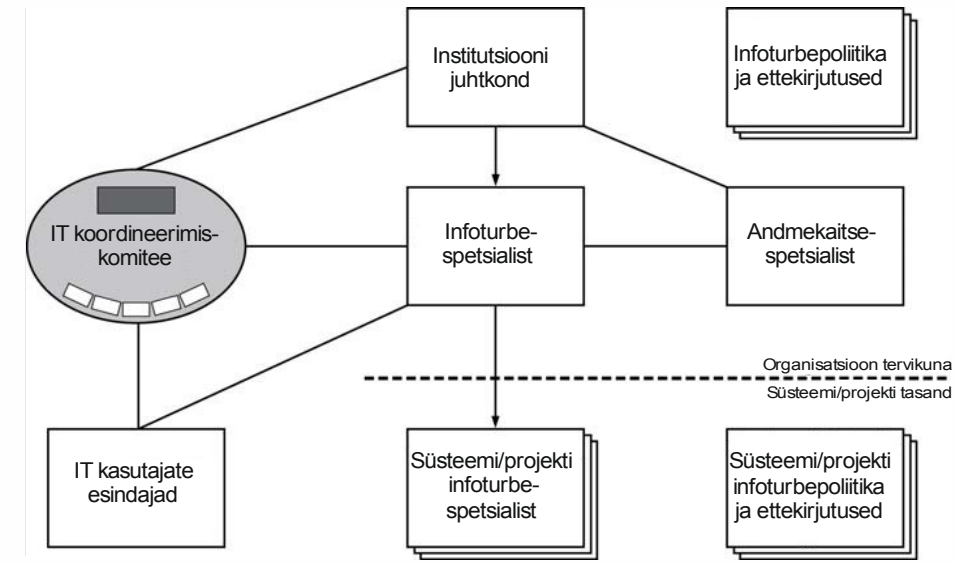
3.4.2 Infoturbe töökorralduse ülesehitus

Olenevalt organisatsiooni suurusest on infoturbehalduse korraldamiseks mitu võimalust.

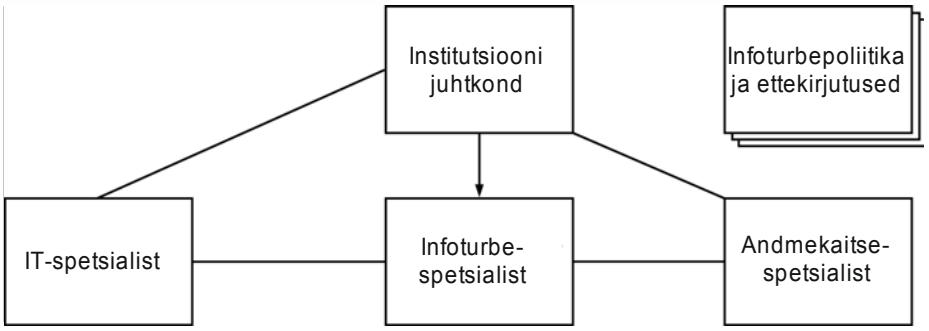
Alljärgnevad joonised kirjeldavad nendest kolme. Esimene joonis näitab suure organisatsiooni infoturbehalduse töökorraldust. Teine joonis kujutab keskmise suurusega organisatsiooni, kus on infoturbehalduse meeskonna ja infoturbespetsialisti ülesanded kokku liidetud. Kolmas joonis näitab väikese organisatsiooni infoturbehalduse töökorraldust, mis peab hõlmama kõiki infoturbespetsialistide ülesandeid.



Joonis 3.1. Suure organisatsiooni infoturbehalduse töökorraldus



Joonis 3.2. Keskmise suurusega organisatsiooni infoturbehalduse töökorraldus



Joonis 3.3. Väikse organisatsiooni infoturbehalduse töökorraldus

Siinkohal on sobilik märkida, et joonistel näidatud kesksed rollid ei pea ilmtingimata kuuluma eri inimestele. Rollide jaotamine oleneb institutsiooni suurusest, olemasolevatest ressurssidest ja eesmärgiks seatud turbeastmest. Infoturvet tagavate ressursside planeerimisel tuleb jälgida, et eesmärgiks seatud turbeastet oleks võimalik ka reaalselt saavutada.

3.4.3 Infoturbehalduse töökorralduse ülesanded, vastutusalad ja kompetentsid

Infoturbespetsialistidel ja infoturbehalduse meeskonnal peavad olema selgelt defineeritud ülesanded, vastutusalad ja kompetentsid, mille peab kindlaks määrama juhtkond. Selleks, et nad saaksid oma ülesandeid täita, tuleb nad kaasata kõikidesse olulistesse protsessidesse ja otsustesse. Rollid tuleb siduda organisatsiooni struktuuriga selliselt, et kõik asjaosalised saaksid üksteisega suhelda. Infoturbespetsialisti ja infoturbehalduse meeskonna liikme ülesanded tuleb usaldada kvalifitseeritud personalile. Vajaduse korral saab osa ülesandeid delegeerida ka osakondade infoturbespetsialistidele või projektijuhtidele ning IT-süsteemide turbespetsialistidele.

3.4.4 Infoturbespetsialist

Infoturve jääb sageli igapäevaste tööde kõrval tagaplaanile. Kui töötajate vastutusalad ei ole täpselt kindlaks määratud, tekib oht, et infoturve on alati „kindlasti kellegi teise probleem”. Seetõttu lükatakse vastutust infoturbe eest seni ühelt teisele, kuni lõpuks tekib igaühel arvamus, et tegu pole tema ülesandega. Sellise olukorra vältimiseks tuleb kõikide infoturvet puudutavate eesmärkide jaoks ametisse nimetada peamine kontaktisik – infoturbespetsialist, kes koordineerib infoturbeülesannete täitmist ja hoolitseb selle valdkonna edendamise eest. Küsimuste korral, kas selle isiku kõrvale on tarvis ka teisi turbespetsialiste ja kuidas infoturvet organiseerida, tuleb lähtuda institutsiooni liigist ja suurusest.

Infoturbe eest vastutava isiku rolli nimetatakse olenevalt institutsiooni liigist ja eesmärgist erinevalt. Sagedasemad ametinimetused on infoturbespetsialist, Chief Security Officer (CSO), Chief Information Security Officer (CISO) või Information Security Manager. Turbespetsialisti nimetus antakse sageli inimestele, kes vastutavad töökaitse, tööohutuse või tehase turvalisuse eest.

Turbeprotsessi edukaks planeerimiseks, rakendamiseks ja tööshoidmiseks peavad töötajate vastutusalad olema selgelt kindlaks määratud. Seega peavad olema täpselt sõnastatud ka ametinimetusega kaasnevad tööülesanded, et kõik teaks, mil määral nad vastutavad erinevate infoturbe-eesmärkide saavutamise eest. Lisaks tuleb ametisse nimetada töötajad, kellel on asjakohane kvalifikatsioon, ning anda nende käsutusse piisavalt ressursse, mis võimaldaksid neil tööülesandeid täita.

Vastutusalad ja ülesanded

Infoturbespetsialist vastutab kogu institutsioonisisese infoturbe eest. Infoturbespetsialisti peamine ülesanne on toetada ametiasutuse või ettevõtte juhtkonda nende infoturbeülesannete täitmisel, neid nõustada ja abistada. Tema ülesanded on muu hulgas järgmised:

- infoturbeprotsessi juhtimine ja osalemine kõikide selle protsessiga seotud ülesannete täitmisel;
- juhtkonna toetamine infoturbepoliitika väljatöötamisel;
- turbekontseptsiooni, hädaolukorraks valmisoleku kontseptsiooni, muude osakontseptsioonide ning süsteemi turbesuuniste koordineerimine, samuti infoturvet tagavate lisasuuniste ja -reeglite väljatöötamine;
- turbemeetmete kasutuselevõtu algatamine ja nende täitmise kontrollimine;
- aruannete esitamine juhtkonnale ja infoturbehalduse meeskonnale, et teavitada neid infoturbe hetkeseisust;
- turbega seotud projektide koordineerimine;
- turvaintsidentide uurimine;
- infoturbe teadvustamis- ja koolitusmeetmete võtmine ja koordineerimine.

Infoturbespetsialist tuleb kaasata kõikidesse suurematesse projektidesse, mis mõjutavad olulisel määral infotöötlust, samuti peab ta osalema uute rakenduste ja IT-süsteemide kasutuselevõtus. Nii on võimalik tagada, et projektide erinevates faasides arvestatakse piisavalt ka turbeaspektidega.

Nõuete profiil

Oma tööülesannete täitmiseks peaksid infoturbespetsialistil olema vajalikud teadmised ja kogemused infoturbe ja infotehnoloogia vallas. Kuna see amet nõuab erinevaid oskusi, tuleb sobiva isiku valimisel jälgida, et tal oleksid järgmised kutseomadused:

- infoturbe-eesmärkide mõistmine, institutsiooni ülesannetest ja eesmärkidest ülevaate omamine;
- koostöövõime, valmisolek meeskonnatööks ja oskus end kehtestada. See on amet, kus läheb võib-olla isegi rohkem kui kusagil mujal tarvis head suhtlusoskust: juhtkond peab alati olema turbeprotsessi puudutavate küsimuste lahendamisse kaasatud. Ta peab nõudma otsuste langetamist ja kaasama turbeprotsessi töötajaid (vajaduse korral osakonna infoturbespetsialisti abil);
- kogemused projektihalduses, ideaaljuhul süsteemianalüüsi vallas, lisaks riskianalüüsi meetodite tundmine.

Infoturbespetsialist peab olema valmis selleks, et tal tuleb tundma õppida uusi valdkondi ja hoida end kursis infotehnoloogia arengusuundadega. Tal peavad olema ülesannete täitmiseks piisavad erialased teadmised ning ta peab end vajaduse korral ka täiendama.

Koostöö ja kommunikatsioon

Koostöö oma organisatsiooni ja ka väliste töötajatega eeldab väga head suhtlusoskust, sest töötajaid tuleb sageli esmalt veenda, et turbemeetmed, mida peetakse tihti tüütuks lisakohustuseks, on kindlasti vajalikud. Väga tundlik teema on ka töötajate küsitlemine turbe seisukohast oluliste sündmuste ja puudujääkide korral. Et selline küsitlemine oleks tulemuslik, tuleb töötajaid veenda selles, et ausad vastused ei tekita neile lisaprobleeme.

Infoturbespetsialisti suhtlusoskus pole oluline mitte ainult töötajatega suhtlemisel. Sama oluline kui töötajatega suhtlemine on see, et turbespetsialist suudaks oma seisukohad selgeks teha ka ametiasutuse või ettevõtte juhtkonnale. Ta peab olema piisavalt enesekindel ja hea suhtleja, et vajaduse korral mitte nõustuda otsustega, mis ei ole kooskõlas infotehnoloogia turvalise käitamise põhimõtetega.

Sõltumatus

Infoturbespetsialisti kompetents peaks olema võrreldav juhtkonna omaga, mis tähendab, et infoturbespetsialist allub otseselt juhtkonnale ning ei pea täitma ühegi teise tasandi isikute otseseid käske ega korraldusi. Näiteks võib esineda probleeme, kui enda tavaliste tööülesannete kõrval hakkab infoturbespetsialisti rolli täitma mõni aktiivne administraator, sest siis võib suure tõenäosusega tekkida huvide konflikt. Ametite ühendamine võib põhjustada olukorra, kus üks ja sama inimene peaks

infoturbespetsialistina takistama otsust, mis kergendaks oluliselt tema tööd administraatorina või millel on koguni tema otsese ülemuse suur poolehoid. Infoturbespetsialistil peab olema alati otsene õigus võtta ühendust ametiasutuse või ettevõtte juhtkonnaga, et neid informeerida turbeintsidentidest, -riskidest ja -meetmetest. Samas tuleb ka teda ennast põhjalikult ja õigel ajal informeerida kõigest institutsioonis toimuvast, millel on otsene seos tema tööga.

Ameti ühendamine andmekaitsespetsialisti tööülesannetega

Sageli tekib küsimus, kas infoturbespetsialistina võiks töötada ka inimene, kes täidab andmekaitsespetsialisti rolli (andmekaitsespetsialisti ülesannetest tuleb juttu allpool). Need rollid ei välista üksteist, kuid mõned aspektid tuleb kõigepealt kindlasti selgeks teha:

- mõlema rolli kattuvus tuleb täpselt kindlaks määrata ja dokumenteerida; lisaks peaks mõlemal töökohal olema juhatuse ees aruandluskohustus; tuleks mõelda, kas konfliktsed teemad peaks suunama lisakontrolliks järelvalveosakonda;
- infoturbespetsialistil peab olema piisavalt ressursse mõlema rolli täitmiseks, vajaduse korral tuleb talle määrata abilised.

Ei tohi unustada, et infoturbespetsialist peab kindlasti olema piisavalt kvalifitseeritud.

3.4.5 Infoturbehalduse meeskond

Infoturbehalduse meeskond abistab infoturbespetsialisti, koordineerides organisatsiooni üldist turvet puudutavaid tööülesandeid, kogudes infot ja viies läbi kontrolle. Meeskonna täpne suurus oleneb organisatsiooni suurusest, eesmärgiks seatud turbeastmest ja olemasolevatest ressurssidest. Äärmuslikul juhul koosneb infoturbemeeskond ainult ühest isikust – infoturbespetsialistist, kes peab sellisel juhul kõikide nende ülesannete eest üksinda hoolt kandma.

Infoturbehalduse meeskonna peamised ülesanded on järgmised:

- infoturbe-eesmärkide ja -strateegiate kindlaksmääramine ning infoturbepoliitika väljatöötamine;
- infoturbepoliitika rakendamise kontrollimine;
- turbeprotsessi algatamine, juhtimine ja kontrollimine;
- abistamine turbekontseptsiooni koostamisel;
- turbekontseptsioonis kavandatud turbemeetmete plaanipärase toimivuse, sobivuse ja tõhususe kontrollimine;
- infoturbe koolitus- ja teadvustamisprogrammide koostamine;
- infoturbe koordineerimiskomitee ja juhtkonna nõustamine infoturbe küsimustes.

Meeskonna liikmed

Oma ülesannete täitmiseks peaks infoturbehalduse meeskond koosnema isikutest, kellel on piisavad teadmised infoturbest, tehnilised teadmised IT-süsteemidest ning tööde organiseerimise ja juhtimise kogemused. Lisaks peavad infoturbehalduse meeskonnas olema esindatud organisatsiooni erinevad valdkonnad. Infoturbehalduse meeskonnas peaksid olema vähemalt järgmiste rollidega isikud: IT kasutamise eest vastutav isik, infoturbespetsialist ja kasutajate esindaja. Kuna meeskonna töö puudutab sageli ka isikuandmeid, peaks infoturbehalduse meeskonda kuuluma ka andmekaitsespetsialist. Kui organisatsioonis on selline komitee juba olemas, võib nende ülesandeid vastavalt laiendada. Siiski on infoturbe olulisuse rõhutamiseks mõistlik kasutada eraldi infoturbehalduse meeskonda ja anda sellele vajalikud ressursid.

3.4.6 Osakonna infoturbespetsialist, projekti või IT-süsteemi turbespetsialist

Suurte organisatsioonide puhul võib olla vajalik kasutada eri osakondades eri infoturbespetsialiste. Osakonna infoturbespetsialist vastutab oma osakonna (nt harukontori) tööprotsesside, rakenduste ja

IT-süsteemide kõikide turbevajaduste eest. Olenevalt hallatavast osakonnast saab osakonna infoturbespetsialisti ülesande anda isikule, kes juba täidab sama tüüpi ülesandeid, nt osakonna IT-spetsialistile (kui on olemas). Osakonna infoturbespetsialisti valimisel tuleb alati jälgida, et ta tunneks põhjalikult oma osakonna ülesandeid, olusid ja tööprotsesse.

Organisatsiooni erinevatel tööprotsessidel, rakendustel ja IT-süsteemidel on sageli erinevad turbenõuded, mis võivad olla koondatud spetsiifilisse turbepoliitikasse ning mille täitmiseks tuleb võtta erinevaid turbemeetmeid. Sama kehtib ka projekti turbespetsialisti kohta, kuid erinevus seisneb selles, et ülesanded ei ole mitte IT-süsteemide-, vaid projektipõhised.

Projekti, IT-süsteemi või osakonna turbespetsialisti ülesanded on järgmised:

- infoturbespetsialistide ettekirjutuste täitmine;
- IT-süsteemi turbepoliitikale vastavate turbemeetmete võtmine või muude spetsiifiliste turbesuuniste elluviimine;
- info kogumine projekti või IT-süsteemi kohta ja selle edastamine infoturbespetsialistile;
- töötajate kohapealse kontaktisiku ülesannete täitmine;
- abistamine spetsiifilise turbepoliitika elluviimiseks vajalike turbemeetmete valimisel;
- töötajate koolitus- ja teadvustamisvajaduste väljaselgitamine;
- logifailide regulaarne kontrollimine ja analüüsimine;
- infoturbespetsialisti teavitamine turbevaldkonnas aset leidnud olulistest vahejuhtumitest.

Nõuete profiil

Töötajal peavad olema järgmised kutseoskused:

- detailsed teadmised infotehnoloogiast, sest nii on kergem töötajatega vestelda ja leida IT-süsteemidele sobivad turbemeetmed;
- teadmised projektihaldusest, millest oleks kasu küsitluste organiseerimisel ja plaanide koostamisel ning turbemeetmete elluviimisel ja kontrollimisel.

3.4.7 IT koordineerimiskomitee

IT koordineerimiskomitee pole tavaliselt institutsiooni püsiv üksus, vaid see kutsutakse kokku vajaduse korral (nt suuremate IT-projektide planeerimisel). Komitee ülesanne on infoturbehalduse meeskonna, IT kasutajate, infoturbespetsialisti ja ametiasutuse või ettevõtte juhtkonna koostöö koordineerimine.

3.4.8 Andmekaitsespetsialist

Andmekaitse jääb sageli teisejärguliseks, sest see takistavat infotöötluse tõhusat toimimist, kuid samas on andmekaitsenõuded seadustesse sisse kirjutatud ning nende rikkumisega võivad kaasneda suured trahvid ja pikaajaline vabadusekaotus.

Sageli antakse andmekaitsespetsialisti ülesanded täita mõnele isikule, kellel on juba mõni teine amet. Sellega luuakse olukord, kus võib tekkida kahe ameti huvide konflikt. Näiteks kui isik peab oma uues, andmekaitsespetsialisti rollis iseennast oma algsete tööülesannete kontekstis (nt IT-juhina) kontrollima.

Et sellist olukorda vältida, tuleb andmekaitseprobleemidega tegelemiseks ametisse määrata kompetentne ja kvalifitseeritud kontaktisik, kes hoolitseb kõikide institutsioonisiseste andmekaitseaspektide eest ning tagab nende elluviimise ja kontrolli. Sellisel juhul peab ta tegema tihedat koostööd infoturbespetsialistiga, kuuluma infoturbehalduse meeskonda ja teavitama oma tööst vahetult ametiasutuse või ettevõtte juhtkonda.

Õige rakenduse korral on andmekaitse töödes abiks ega mõju koormavana. Kui mõni ametiasutus või ettevõte kogub liiga palju isikuandmeid, kustutab need liiga hilja või edastab neid volitamatult, ei riku ta mitte üksnes andmekaitseõigust, vaid kulutab ka oma tööprotsesside täitmiseks vajalikust rohkem aega ja raha. Andmekaitse järgimine on esmajoones kodaniku- ja kliendisõbraliku käitumise tunnus, sest see muudab protseduurid läbipaistvaks.

Iga institutsioon peaks ametisse määrama andmekaitsespetsialisti. Paljudes valdkondades on andmekaitsespetsialisti ametikoht isegi seadusega ette nähtud. Ka need institutsioonid, kus pole andmekaitsespetsialisti ametisse nimetatud, peavad siiski andmekaitsenõuetest kinni pidama. Selleks võib kasutada ka infoturbehalduse meeskonda või revisjoniosakonda.

Nõuete profiil

Andmekaitsespetsialistina võib töötada ainult selline isik, kellel on vastavate ülesannete täitmiseks sobivad erialased teadmised ning kes on piisavalt usaldusväärne. Ülesannete täitmiseks peab ta tundma tehnoloogiat, töökorraldust ja seadusi. Andmekaitsespetsialist peab tundma seadusest tulenevaid ettekirjutusi, valdkonna andmekaitsenõudeid ja institutsioonile kehtivaid erieeskirju ning suutma neid ka rakendada. Eriti oluline õigusnorm on andmekaitseseadus. Andmekaitsespetsialist peab lisaks hästi tundma ka institutsiooni ja tal peavad olema väga põhjalikud teadmised infotehnoloogiast. Kui töötaja ei ole piisavalt kvalifitseeritud, tuleb talle anda võimalus end koolitada. Oma ametiasutuse või ettevõtte ülesandeid ja tööviise peaks andmekaitsespetsialist tundma oma kogemustele tuginedes, et olla suuteline täitma talle määratud kontrolli- ja nõustamisülesandeid.

Andmekaitsespetsialist ei pea tundma mitte ainult neid funktsioone. Olenevalt töödeldavate isikuandmete mahust ja hulgast ning sellega seotud andmekaitseprobleemidest võib olla vajalik täita ka muid tööülesandeid. Seda võib eriti sageli kohata just väiksemate institutsioonide puhul. Seejuures tuleb kindlasti jälgida, et ei tekiks huvide konflikte ega liigset sõltuvust, mis võiks kahjustada tööülesannete täitmist. Andmekaitse- ja infoturbespetsialisti ülesandeid on võimalik ka ühendada.

Kaasamiskohustus

Andmekaitsespetsialistil peab olema otsene ja alatine õigus võtta ühendust ametiasutuse või ettevõtte juhtkonnaga ning saada õigel ajal põhjalikku infot kõigest ametiasutuses või ettevõttes toimuvast, mis on otseselt seotud tema tööga. Teda tuleb kaasata andmekaitse valdkonna jaoks olulistesse protsessidesse, samuti tuleb teda teavitada plaanidest, mis puudutavad isikuandmeid. Vajaduse korral peavad teda aitama töötajad, kellel on suuremad tehnilised või õigusteadmised.

Vastutusalad ja ülesanded

Andmekaitsespetsialist peab hoolitsema selle eest, et institutsioon täidaks piisaval määral andmekaitsenõudeid. Ta peab jälgima, et kõikides valdkondades peetaks kinni andmekaitse-eeskirjadest. Ta täidab oma ülesandeid peamiselt nõustamise ja kontrollimisega. Esmaülesanne on nõustamine. Andmekaitsespetsialist on kõikide andmekaitset puudutavate küsimuste korral töötajate usaldusväärne kontaktisik. Vigade või tegematajätmiste avastamisel peaks ta esmalt koos asjaosalistega püüdma leida tulemuslikke lahendusi.

Andmekaitsespetsialist peab ametiasutuse või ettevõtte juhtkonnal aitama isikuandmeid kaitsta ja vältida vahejuhtumeid, mis võiksid kahjustada institutsiooni mainet. Ta peaks suhtlema ka töötajate esindusega. Hea koostöö pole vajalik mitte ainult isikuandmete töötlemise konfidentsiaalsuse tagamiseks.

Andmekaitsespetsialisti tööülesanded olenevad kõige muu kõrval ka ametiasutuse või ettevõtte suurusest, ülesehitusest ja liigendusest.

Peatüki 3.4 „Turbeprotsessi töökorraldus” rõhuasetus

- Infoturbeprotsessi kujundavate rollide kindlaksmääramine
- Rollidega kaasnevate ülesannete ja vastutusalade kindlaksmääramine
- Rollide jaoks sobiva personali leidmine

- Infoturbehalduse töökorralduse dokumenteerimine
- Infoturbehalduse integreerimine organisatsiooni töökorraldusega

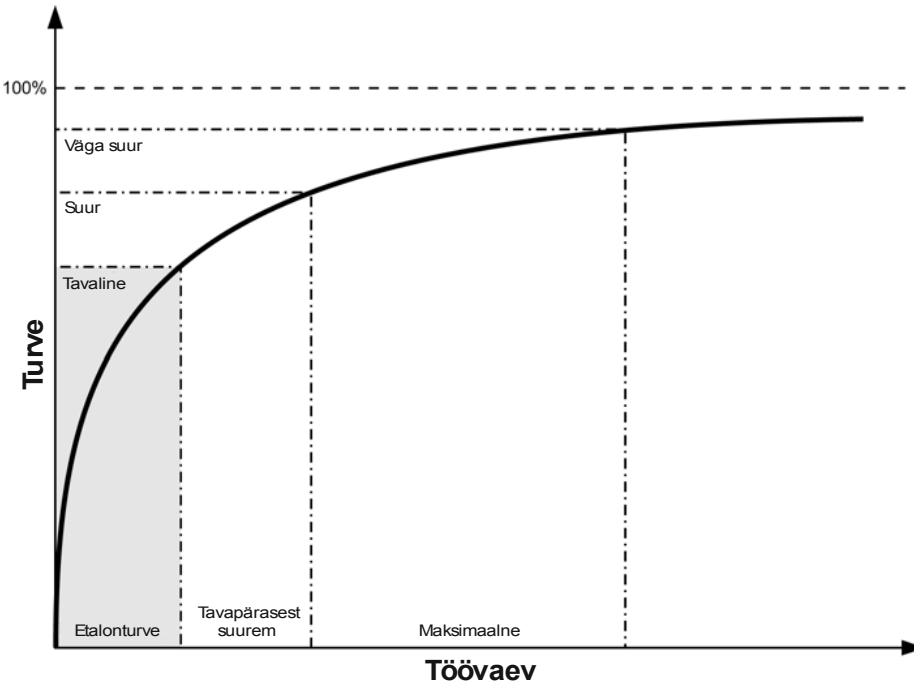
3.5 Infoturbe tagamiseks vajalike ressursside eraldamine

Tähelepanuta jäänud ohud võivad teadupärast põhjustada kahju, kuid teisalt kulub omajagu ressursse ka riskiennetusega tegelemisele. Efektiivse riskihaldusega saab neid kulusid kontrolli all hoida. Piisava infoturbe tagamine ja tööshoidmine nõuavad aga aega ja vaeva. Seepärast tuleb turbeastme kindlaksmääramisel ja institutsiooni konkreetsete turbenõuete sõnastamisel kindlasti jälgida, et eesmärgiks seatud turbeaste oleks ka majanduslikult mõistlik.

3.5.1 Kulutõhus turbestrateegia

Turbestrateegia kujundamisel tuleb algusest peale arvestada ka selle kuluaspektidega. Kui selgub, et vajalikke turbemeetmeid ei saa olemasolevate ressurssidega võtta, tuleb strateegiat muuta. Olukorras, kus soovide ja finantsvahendite vahel osutuvad käärid liiga suureks, tuleb kriitilise pilguga analüüsida tööprotsesse või IT-süsteemide käitamise meetodeid.

Kogemus näitab, et turbeastme tõstmiseks vajaliku aja ja vaeva ning seeläbi saavutatava reaalse turbeastme suhe on seda ebasoodsam, mida kõrgem turbeaste on eesmärgiks seatud. Täiuslikku infoturvet pole võimalik saavutada. Allolev diagramm näitab, kui palju tuleb eesmärgiks seatud turbeastme nimel vaeva näha. See aitab orienteerivalt hinnata, kui palju läheb turbeastme saavutamiseks tarvis personali-, aja- ja finantsressursse.



Joonis 4. Infoturbele kulutatava aja, töövaeva ja saadava kasu suhe

Turbeprotsessi töösammude valimisel tuleb iga meetme puhul täpselt analüüsida selle kulude ja kasu suhet. Turbe oluliseks tõhustamiseks saab sageli kasutada lihtsaid töökorralduslikke meetmeid, mille juurutamine ei nõua kuigi palju vaeva ega ka tehnilist lisavarustust. Alles pärast nende elementaarsete turbemeetmete võtmist on mõistlik investeerida tehnoloogiasse ja põhjalikesse turbetaristutesse.

Infoturve nõuab finants-, personali- ja ajaressursse ning juhtkond peab neid eraldama vastavalt eesmärgiks seatud nõuetele. IT-turvet seostatakse väga sageli eksikombel ainult tehniliste lahendustega. Sel põhjusel on parem kasutada terminit „infoturve". Ennekõike on oluline teada, et

investeeringud personali on tihti palju efektiivsemad kui investeeringud turbetehnoloogiasse. Tehnoloogia üksinda ei suuda probleeme lahendada. Tehnilised meetmed tuleb alati siduda sobiva töökorraldusliku raamistikuga.

3.5.2 Infoturbehalduse töökorralduse ressursid

Infoturbealased küsitlused on näidanud, et kõige efektiivsemaks turbemeetmeks on sageli osutunud infoturbespetsialisti ametissenimetamine. Pärast eraldiseisva infoturbespetsialisti ametikoha loomist on enamikus institutsioonides turvaintsidentide arv märgatavalt vähenenud. Selleks, et infoturbespetsialist saaks oma tööülesandeid täita, peab tal oma tööks olema piisavalt aega. Väiksemates organisatsioonides on võimalik, et infoturbespetsialisti ülesanded võtab enda kanda mõni teine töötaja, tehes seda oma põhitöö kõrvalt.

Töötajaid, kelle jaoks on infoturbehalduse meeskonnas töötamine põhitöö, saavad palgal pidada ainult väga vähesed institutsioonid, nt kas väga suured või sellised, kus on suur vajadus infoturbe järele. Enamasti täidavad neid ülesandeid aga töötajad oma tavaülesannete kõrvalt. Erandiks on siiski turbeprotsessi juurutamine. Kui vähegi võimalik, tuleks infoturbehalduse meeskonna liikmed selles faasis oma muudest tööülesannetest vabastada. See, kas infoturbehalduse meeskonna ja infoturbespetsialisti ametikoha lahutamine on ka hiljem mõistlik, oleneb sellest, kui palju ülesandeid soovitakse lahutada. Lõpliku otsuse peab langetama ametiasutuse või ettevõtte juhtkond. Infoturbehalduse meeskond peaks igal juhul regulaarselt koosolekuid pidama, et tagada turbeprotsessi pidev juhtimine.

Infoturbehalduse meeskonna sisseseadmine võimaldab turbeprotsessi kaasata organisatsiooni erinevaid üksusi ja ühendada kompetentse. Seeläbi saab infoturvet kõikides organisatsiooni üksustes kiiremini ellu viia ja asjatut ressursside kulutamist on vähem. Turbevaldkonna tegevuste koordineerimisse saab kaasata nt organisatsiooni järgmised allüksused: infoturve, revisjon, IT-administratsioon, IT-juhatus, andmekaitse, töötajate esindus, erialaosakonnad, hoonetehnoloogia, juristid ja finantsosakond.

Juurdepääs välistele ressurssidele

Praktika on näidanud, et organisatsioonisisestel turbeekspertidel on sageli liiga vähe aega, et analüüsida kõiki olulisi turbetegureid ja raamtingimusi (nt seadusi või tehnilisi küsimusi). Vahel puuduvad neil ka asjakohased baasteadmised, kuidas sellist analüüsi teha. Sellisel juhul on mõistlik kasutada organisatsioonivälíseid eksperte. Selleks peavad institutsiooni turbeeksperdid esmalt olukorra dokumenteerima, et juhtkond saaks seejärel eraldada piisavalt ressursse.

Infoturvet võib tõhustada ka IT-süsteemide või teatud teenuste (nt tulemüüri teenuse) väljasttellimine, kui seeläbi saab kasutada spetsialiste, keda organisatsioonis endas pole. IT-etalonturbe kataloogide moodul B 1.11 „Väljasttellimine" annab soovitusi, mida sellistel juhtudel turbe puhul silmas pidada.

3.5.3 Infoturbe kontrollimise ressursid

Turbemeetmete tõhususe ja sobivuse süstemaatiliseks kontrollimiseks peab olema piisavalt ressursse. Võimaluse korral tuleb kontrollida ka seda, kas kasutatud ressursid ja saavutatud turve on tasakaalus. Näiteks kui selgub, et teatud IT-süsteemide kaitsmine põhjustab majanduslikult tarbetult suuri kulutusi, tuleb leida alternatiivsed meetmed. Kui vajaliku turbeastme säilitamisega kaasnev aja- ja ressursikulu on liiga suur, võib olla mõistlik ühendada teatud IT-süsteemid ebaturvaliste võrkude küljest lahti.

3.5.4 IT-süsteemide käitamise ressursid

IT-süsteemide turvalise käitamise eelduseks on nende veatu toimimine, seega on nii korralik planeerimine kui ka töö korraldamine hädavajalikud. Seetõttu tuleb IT-süsteemide käitamiseks eraldada piisavalt ressursse. Turbemeetmed saavad hakata efektiivselt toimima enamasti alles pärast seda, kui institutsioon on suutnud lahendada IT-süsteemide käitamise tüüpprobleemid, milleks on nt väike eelarve, ülekoormatud administraatorid või halvasti struktureeritud ja hooldatud IT.

Peatüki 3.5 „Infoturbe tagamiseks vajalike ressursside eraldamine" rõhuasetus

- Sobivuse ja majandusliku tasuvuse arvestamine turbeprotsessis
- Tasakaalu loomine infoturbe töökorraldusliku ja tehnilise poole vahel
- IT-süsteemide käitamiseks, infoturbe halduseks ja kontrolliks vajalike ressursside nõudmine
- Vajaduse korral väliste ressursside kasutamine

3.6 Kõikide töötajate kaasamine turbeprotsessi

Infoturve puudutab eranditult kõiki töötajaid. Igaüks saab vastutustundliku ja turbereegleid järgiva käitumisega anda panuse kahjude vältimisse ja turbeprotsessi edu tagamisse. Infoturbeaspektide teadvustamine ja töötajate erialased koolitused on seega infoturbe tagamise põhieelduseks. Ka töökliima, ühised väärtused ja töötajate koostöövalmidus on infoturbe seisukohast olulised.

Kõikide, nii organisatsioonisiseste kui ka -väliste töötajate puhul tuleb alati arvestada infoturbeaspektidega ja seda alates personali valimisest kuni töötajate lahkumiseni.

3.6.1 Koolitamine ja teadlikkuse suurendamine

Turbemeetmeid puudutava teadlikkuse suurendamiseks tuleb kõiki töötajaid asjakohaselt koolitada. Seega on vaja luua sihtrühmade (nt administraatorite, juhatajate, kasutajate, valvurite) jaoks erinevad koolituskontseptsioonid. Infoturbekoolitused tuleb seejuures integreerida olemasolevate koolituskontseptsioonidega.

Kõiki töötajaid, kes alles võetakse tööle või kellele määratakse uued ülesanded, on vaja põhjalikult juhendada ja koolitada. Koolitusmeetmetesse tuleb kaasata kõik olulised turbeaspektid. Ka kogenud IT-kasutajad peavad oma teadmisi regulaarselt värskendama ja täiendama.

Töötajatele tuleb regulaarselt teadvustada infoturbe olulisust, et nad oskaks oma igapäevatöös infoga alati õigesti ümber käia ja tunneks ka võimalikke riske. Infoturbe olulisuse paremaks teadvustamiseks on mõistlik luua intraneti kaudu ligipääsetav turbefoorum, kus avaldatakse nt nõuandeid turbemeetmete kohta, antakse ülevaade aktuaalsetest kahjudest, pakutakse töötajatele infoturbealaseid õpikodasid või ettekandeid ning jagatakse erialaseid ajakirju.

3.6.2 Kommunikatsioon, integreerimine ja teavitamiskanalid

Selleks, et töötajad järgiksid ka pärast väljaõpet ja turbe vajalikkuse teadvustamist ettenähtud turbemeetmeid, tuleb määrata ametisse turbeküsimuste kontaktisikud ning töötajaid selgelt teavitada, et nende poole saab ja tuleb probleemide korral pöörduda. Ainult nii on võimalik töötajaid aktiivselt abistada ning turbepoliitikat ja -kontseptsioone praktikas järjepidevalt ellu viia. Selle alla kuuluvad ka turvaintsidentidest teavitamist ja nende võimalikku eskaleerumist puudutavad tegutsemis- ja käitumisjuhised. Iga töötaja peab teadma, kuidas turvaintsidendi kahtluse korral käituda ja kelle poole pöörduda. Lisaks peab olema võimalik vajalikku infot edastada kiirelt ja oludest sõltumatult, nt ka siis, kui IT-süsteemid enam ei tööta.

Töötajatele tuleb selgitada turbemeetmete vajalikkust. Eriti oluline on see neil juhtudel, kus turbemeetmete juurutamine tähendab töötajatele mõnest mugavusest või funktsioonist loobumist. Mõningate turbemeetmete võtmisse on kohustuslik kaasata ka töötajate esindus.

Kui töötajad kaasatakse turbemeetmete planeerimisse või töökorraldust puudutavate reeglite väljatöötamisse piisavalt vara, on sellel mitu eelist:

- institutsioonisiseseid teadmisi ja ideid suudetakse paremini ära kasutada;
- suureneb turbemeetmete ja töökorralduslike reeglite praktilisus ja tõhusus;
- suureneb töötajate valmidus nõudeid ja meetmeid igapäevatöös täpselt järgida;

- töökliimale mõjub positiivselt, kui töötajad saavad osaleda juhtkonna otsustes.

3.6.3 Tööülesannete vahetumine ja töötajate lahkumine

Kui töötajad institutsioonist lahkuvad, võtavad enda kanda mõne uue ülesande või jäävad mõningatest oma kohustustest ilma, tuleb võtta asjakohaseid turbemeetmeid ja asjaolud dokumenteerida. Kui töötaja institutsioonist lahkub või kui tema tööülesanded muutuvad, on tal tavaliselt kohustus sellest teavitada mitut osakonda ning seejärel on osakondadel õigus võtta mitmeid meetmeid, nt nõuda võtmete ja töötunnistuste tagastamist, kohandada pääsuõigusi rakendustele ja infole, teavitada uksehoidjaid ja muud personali jne. Turberiskide vältimiseks peab identiteedi ja volituste halduse protsess olema selgelt defineeritud, nt juhendite või kontrollnimekirjaga. Kui töötaja osales turbeprotsessis, tuleb uuendada ka asjakohaseid dokumente, nt hädaolukorraks valmisoleku plaani.

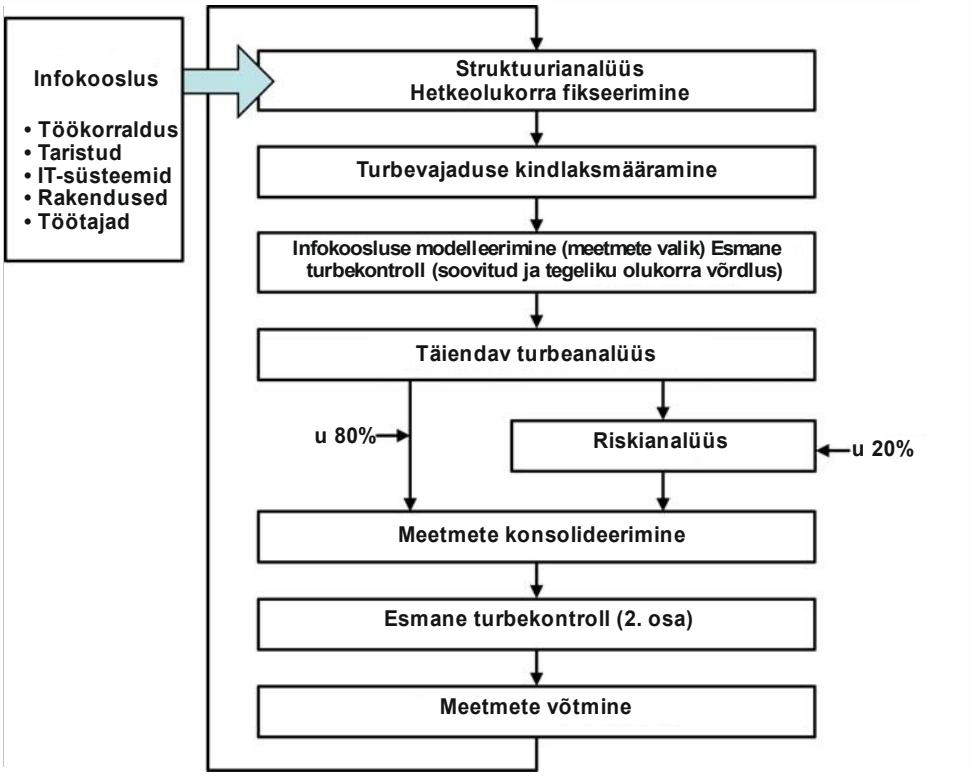
Lisaks on mõistlik teavitada töötajaid juba võimalikult varakult (nt töölepingus) nende kohustustest tööülesannete muutumisel või töösuhete lõppemisel. Muu hulgas tuleks rõhutada töötaja vaikimiskohustust.

Peatükis 3.6 „Kõikide töötajate kaasamine turbeprotsessi" rõhuasetus

- Töötajate ja nende esinduse piisavalt varajane kaasamine turbemeetmete ja reeglite planeerimisse ning väljatöötamisse
- Kõikide töötajate koolitamine ja nende regulaarne teavitamine, et selgitada infoturbe olulisust
- Turbemeetmete eesmärkide selgitamine kõikidele töötajatele
- Turbeküsimuste kontaktisikute ametissemääramine ja nende vastutusalade avalikustamine töötajatele
- Turvaintsidentidest teavitamist ja nende võimalikku eskaleerumist puudutavate tegutsemis- ja käitumisjuhiste kindlaksmääramine ning nende avalikustamine töötajatele
- Vajalike turbemeetmete võtmise tagamine töötajate lahkumisel või nende tööülesannete muutumisel

4 IT-etalonturbest lähtuva turbekontseptsiooni koostamine

IT-etalonturbe üks eesmärk on pakkuda pragmaatilist ja tõhusat metoodikat, mis tagab vajaliku turbeastme ning mis võib olla ka kõrgema turbeastme aluskivi. Kui infoturbeprotsess on juba käivitatud ning turbepoliitika ja infoturbe töökorraldus kindlaks määratud, hakatakse looma institutsiooni turbekontseptsiooni. Selleks soovitatakse IT-etalonturbe kataloogides tööprotsesside, rakenduste ja IT-süsteemide jaoks töökorraldust, personali, taristuid ja tehnikat puudutavaid standardseid turbemeetmeid. Need meetmed on jaotatud üksteisele toetuvatesse moodulitesse.



Joonis 5. Infoturbehalduse turbekontseptsiooni koostamine

IT-etalonturbe metoodika

Traditsioonilise riskianalüüsi raames tuvastatakse esmalt ohud ja seostatakse need nende esinemuse tõenäosusega, et valida sobivad turbemeetmed, seejärel saab hinnata ka jääkriske. Need sammud on IT-etalonturbes iga mooduli puhul juba varem tehtud ning moodulid kajastavad tüüpiliste kasutusstsenaariumide jaoks sobivaid turbemeetmeid. IT-etalonturbe rakendamisel taandub analüüs eesmärkide ja hetkeolukorra võrdlusele, st selgitatakse välja, millised IT-etalonturbe kataloogides soovitatud meetmed on juba võetud ning milliseid alles tuleb võtta. Analüüsi raames tuvastatud puuduvad või ebapiisavalt võetud meetmed näitavad turbepuudujääke, mis tuleb soovitatud meetmete abil kõrvaldada. Täiendav turbeanalüüs tuleb teha alles oluliselt suurema turbevajaduse korral, võttes arvesse kulusid ja nende loodetavat kasutegurit. Tavaliselt piisab sellisel juhul sellest, kui täiendada IT-etalonturbe kataloogide meetmeid vastavate individuaalsete ja rangemate meetmetega. Standard BSI 100-3 „IT-etalonturbel põhinev riskianalüüs" kirjeldab metoodikat, mis on traditsioonilisest riskianalüüsist lihtsam.

IT-etalonturbel põhineva turbekontseptsiooni koostamisel võib laias laastus eristada allnimetatud valdkondi.

Kehtivusala määramine

IT-etalonturbe elluviimine üheainsa suure sammuna on sageli liiga raske ettevõtmine. Paljud väikesed sammud ning pikaajaline ja pidev tõhustamisprotsess, mis ei vaja suuri alginvesteeringuid, on sageli edukamad. Nii võib olla alguses mõistlik seada eesmärgiks juurutada soovitud turbeaste esmalt ainult üksikutes väljavalitud valdkondades. Nendest algpunktidest lähtudes tuleks tõhustada turvet kogu organisatsioonis.

Kõigepealt tuleb seega välja valida valdkond, mille jaoks turbekontseptsioon luua ja milles see ellu viia. See võib olla nt organisatsiooni mõni konkreetne osakond. Valida võib ka valdkondi, mis puudutavad kindlaid tööprotsesse, kaasa arvatud selleks vajalikud taristud.

IT-etalonturbes nimetatakse turbekontseptsiooni kehtivusala ka infokoosluseks.

Struktuurianalüüs

Turbekontseptsiooni loomiseks ja eriti just IT-etalonturbe kataloogide kasutamiseks tuleb analüüsida ja dokumenteerida, kuidas tööprotsessid, rakendused ja olemasolev infotehnoloogia koos toimivad. Kuna tänapäeval on tavaline, et IT-süsteemid on omavahel tugevalt ühendatud, saab edasise tehnilise analüüsi jaoks kasutada võrgu topoloogilist skeemi. Arvestada tuleb järgmiste aspektidega:

- infokoosluses töötavad rakendused ja nendega toetatavad tööprotsessid;
- infokoosluse töökorraldust ja personali puudutavad raamtingimused;
- infokoosluses kasutatavad võrguühendusega ja -ühenduseta IT-süsteemid;
- IT-süsteemidevahelised ja -välised sideühendused;
- olemasolevad taristud.

Struktuurianalüüsi erinevad sammud on üksikasjalike tegutsemisjuhiste kujul esitatud selle dokumendi peatükis 4.2.

Turbevajaduse kindlaksmääramine

Turbevajaduse kindlaksmääramise eesmärk on tuvastada, milline on tööprotsesside, nendes töödeldava info ning selleks kasutatud infotehnoloogia piisav ja sobiv turve. Selleks vaadeldakse iga rakenduse ja sellega töödeldava info puhul võimalikke kahjusid, mis võivad tekkida seoses konfidentsiaalsus-, terviklus- või käideldavusprobleemidega. Muu hulgas on oluline anda võimalikele tagajärgedele realistlik hinnang. Praktika on näidanud, et mõistlik on kasutada kolme turbevajaduse kategooriat: „Madal", „Keskmine" ja „Kõrge".

Turbevajaduse kindlaksmääramise üksikuid samme kirjeldatakse põhjalikult selle dokumendi peatükis 4.3.

Meetmete valik ja kohandamine

Selleks, et IT-etalonturbe katalooge infokoosluse peal rakendada, läheb tarvis põhjalikku infot selle struktuuri ja sellesse kuuluvate sihtobjektide kohta. See info tuvastatakse eelkirjeldatud töösammudega. Olemasoleva infokoosluse jaoks sobivate turbemeetmete tuvastamiseks tuleb IT-etalonturbe kataloogide mooduleid kohandada olemasolevate objektide ja valdkondadega.

Seda protseduuri kirjeldatakse põhjalikult peatükis 4.4.

Esmane turbekontroll

Esmane turbekontroll on organiseeriv tööetapp, mis annab kiire ülevaate olemasolevast turbeastmest. Intervjuudega tuvastatakse olemasoleva (IT-etalonturbe järgi modelleeritud) infokoosluse seisund, võttes arvesse seda, mil määral on suudetud IT-etalonturvet seni juba rakendada. Selle tulemusel saab koostada kataloogi, kus iga meetme juures on selle rakendamise seisundina kirjas kas „pole oluline", „jah", „osaliselt" või „ei". Tuvastades meetmed, mida pole ellu viidud või mis on ellu viidud ainult osaliselt, leitakse ka võimalused, kuidas vaadeldud tööprotsesse ja infotehnoloogia turvet täiendada.

Esmase turbekontrolli tegevusplaani kirjeldab peatükk 4.5. Seejuures võetakse projekti läbiviimisel arvesse nii töökorralduslikke aspekte kui ka tööprotsesside erivajadusi.

Täiendavad turbemeetmed

IT-etalonturbe standardsed turbemeetmed pakuvad tavaolukorras sobivat ja piisavat turvet. Suure või väga suure turbevajaduse korral oleks siiski mõistlik kontrollida, kas institutsioonil võib tarvis minna teisigi või tavapärasest rangemaid turbemeetmeid. See kehtib ka siis, kui tegu on eriliste kasutustingimustega või kui kasutatakse komponente, mida IT-etalonturbe kataloogide olemasolevad moodulid ei kajasta. Siinkohal tuleb esmalt asjakohase *täiendava turbeanalüüsiga välja selgitada*, kas hõlmatud valdkondade jaoks on vaja koostada eraldi riskianalüüs.

Riskianalüüsi üks võimalik metoodika on toodud standardis BSI 100-3 „IT-etalonturbel põhinev riskianalüüs". Sellest metoodikast annab ülevaate peatükk 4.6. Riskianalüüsi edukas läbiviimine oleneb suuresti projektiga tegeleva meeskonna erialastest teadmistest. Seega on sageli mõistlik kaasata kogenud välist personali.

4.1 Turbekontseptsiooni kehtivusala määramine

Enne turbekontseptsiooni koostamist tuleb kindlaks määrata, millistes institutsiooni valdkondades see kehtima hakkab. See võib olla identne infoturbepoliitika kehtivusalaga, kuid vahel võib olla mõistlik luua väiksemate valdkondade jaoks eraldi turbekontseptsioonid. Kontseptsiooni tasuks jaotada osadeks nt juhtudel, kus tervikliku kontseptsiooni koostamine tundub esimese sammuna veel liiga töömahukas ja mõned kindlad tööprotsessid on turbepoliitika kohaselt teistest olulisemad.

Tehniliste aspektide kõrval tuleb kehtivusala piiritlemisel arvestada ka töökorralduse aspektidega, et töötajate kohustusi ja vastutust oleks võimalik täpselt kindlaks määrata. Kõikidel juhtudel peab olema selge, millist infot ja milliseid tööprotsesse peab turbekontseptsioon kindlasti käsitlema.

Turbekontseptsiooni kehtivusalade piiritlemisel tuleb arvestada järgmist:

- kehtivusala peab hõlmama võimalikult paljusid valdkondi, aspekte ja komponente, mida läheb tarvis tööprotsesside täitmiseks või institutsiooni allüksuste abistamiseks ning mida hallatakse institutsiooni sees;
- kui see pole võimalik põhjusel, et mõned vaadeldud tööprotsessid olenevad välistest partneritest (nt väljasttellimise tõttu), peavad olema selgelt defineeritud nende tööprotsesside ühenduspunktid, et nendega saaks turbekontseptsiooni koostamisel arvestada.

Infokooslus

Turbekontseptsiooni koostamise kehtivusala nimetatakse edaspidi infokoosluseks (kasutusel on ka termin „IT-kooslus"). IT-kooslus kirjeldab kehtivusala esmajoones selle tehnilisest vaatepunktist. Kuid IT-kooslus ei sisalda siiski mitte üksnes IT-komponente, vaid ka infot, töökorraldust tagavaid meetmeid, töövaldkondi, vastutusalasid ja füüsilisi taristuid. Seega on infokooslus terminina siinkohal parem ja tabavam.

Infokooslus hõlmab seega taristuid, töökorraldust, personali ja tehnilisi komponente, mis on mõeldud tööülesannete täitmiseks mõnes infotöötluse valdkonnas. Infokooslus võib hõlmata institutsiooni kogu infotöötlust või ka ainult selle üksikuid valdkondi, mis on liigendatud kas töökorralduslike või tehniliste meetmete põhjal (nt osakondade andmevõrgud) või ühiste tööprotsesside või rakenduste põhjal (nt personali infosüsteem).

Turbekontseptsiooni koostamiseks koondatakse vaadeldava infokoosluse osad kokku ja analüüsitakse infokoosluse struktuuri. Selle struktuurianalüüsi süstemaatilist metoodikat kirjeldatakse järgmises peatükis.

Peatüki 4.1 „Turbekontseptsiooni kehtivusala määramine" rõhuasetus

- Kehtivusalasse kuuluvate kriitiliste tööprotsesside või institutsiooni osakondade tuvastamine
- Kehtivusala selge piiritlemine
- Väliste partnerite ühenduskohtade kirjeldus

4.2 Struktuurianalüüs

Struktuurianalüüs aitab esile tõsta IT-etalonturbele vastava turbekontseptsiooni koostamisel vajaminevat infot. Seejuures tuleb vaadelda kõiki komponente (infot, rakendusi, IT-süsteeme, ruume, sidevõrke), mida läheb tarvis kehtivusalasse kuuluvate tööprotsesside täitmiseks.

Selleks tuleb tuvastada töö seisukohast kriitilise tähtsusega info ning vastavad IT-süsteemid, ruumid ja võrgud. Klassikalise käsitlusviisi järgi tuleks esmalt tuvastada rakendused ja seejärel nendest lähtuvad edasised objektid. Sellise meetodi puuduseks on asjaolu, et abstraktseid rakendusi on sageli väga raske mõista, kui puudub võimalus seostada neid konkreetsete tehniliste komponentidega. Seega võib olla mõnel juhul mõistlik, erinevalt siinkohal näidatud järjekorrast, vaadelda esmalt IT-süsteeme, sest rakendusi on IT-süsteemide alusel sageli palju kergem tuvastada.

Tuleb arvestada, et objektid ja andmed, mida struktuurianalüüsi raames vaadeldakse, ei ole olulised tavaliselt mitte ainult turbeprotsessi jaoks, vaid ka organisatsiooni tööprotsesside ja haldusülesannete seisukohast. Seega tuleks kontrollida, kas on juba olemas andmebaasid või mõned muud ülevaatevõimalused, mida saaks struktuurianalüüsi raames andmeallikatena kasutada. Näiteks on paljudes institutsioonides olemas inventari, konfiguratsioonihalduse või tööprotsesside andmebaasid. See annab võimaluse sünergia tekkeks.

Struktuurianalüüs jaotub järgmisteks osadeks:

- kehtivusalasse kuuluvate tööprotsesside, rakenduste ja info tuvastamine;
- võrgu planeeringu analüüs;
- IT-süsteemide ja nendesarnaste objektide analüüs;
- ruumide ülesmärkimine.

Kõikide ülesannete puhul tuleb arvestada sellega, et sageli pole otstarbekas vaadelda igat objekti ükshaaval. Selle asemel tuleks sarnased objektid koondada rühmadesse.

4.2.1 Keerukuse vähendamine rühmade moodustamisega

Struktuurianalüüs pakub olulisi põhiandmeid kogu turbeprotsessi jaoks. Infokooslus moodustub enamasti paljudest üksikobjektidest, millega tuleb kontseptsiooni loomisel arvestada. Kui aga vaadelda kõiki loogilisi ja tehnilisi objekte eraldi, on oht, et struktuurianalüüsi tulemused pole andmete suure hulga ja keerukuse tõttu enam hoomatavad. Seega tuleks sarnased objektid koondada rühmadesse.

Kui baaskonfiguratsioone pole palju, aitab tehniliste komponentide rühmitamine haldamist oluliselt lihtsustada. IT-keskkonna võimalikult suure sisese standardiseerimisega vähendatakse ka turbeaukude ohtu ning selle valdkonna turbemeetmeid saab võtta nii, et erinevaid kitsaskohti pole tarvis eristada. See pole kasulik mitte ainult infoturbe, vaid ka kulude seisukohast.

Objektid saab liigitada samasse rühma, kui nende kohta kehtib järgnev:

- nad on sama tüüpi;
- nad on sarnase konfiguratsiooniga;
- nad on ühtmoodi võrku ühendatud (IT-süsteemide puhul ühendatud nt sama kommutaatoriga);
- nende haldamisele ja taristutele kehtivad sarnased raamtingimused;
- nad on mõeldud sarnaste rakenduste jaoks;
- nad on sama turbevajadusega.

Rühmade moodustamise nõuetele tuginedes võib infoturbe puhul oletada, et rühma kuuluva komponendi pisteline kontroll kajastab kogu rühma turbeseisundit.

Rühmade moodustamise oluliseks näiteks on klientsüsteemid. Klientsüsteeme on institutsioonis tavaliselt üpris palju, kuid eeltoodud reeglite põhjal saab need koondada ülevaatlikesse rühmadesse.

Sama kehtib ka ruumide ja muude objektide kohta. Suurtes infokooslustes, kus liiasuse või parema andmetöötlusvõimsuse tagamiseks täidavad paljud serverid sama ülesannet, saab rühmadesse koondada ka servereid.

Järgnevalt kirjeldatakse ja selgitatakse struktuurianalüüsi erinevaid ülesandeid. Näite põhjalikuma versiooni leiate BSI veebilehelt IT-etalonturbe abivahendite alt. Kõikide ülesannete puhul tuleb objektid koondada rühmadesse, eeldusel et see on mõistlik ja lubatud.

Peatüki 4.2.1 „Keerukuse vähendamine rühmade moodustamisega" rõhuasetus

- Kõikide struktuurianalüüsi ülesannete puhul sarnaste objektide koondamine rühmadesse
- Rühmadesse koondatud objektide tüübi ja arvu ülesmärkimine

4.2.2 Rakenduste ja nendega seotud info ülesmärkimine

Selles faasis tuleb infokoosluse iga tööprotsessi kohta välja selgitada seotud rakendused ja info. Rakendused on kõikvõimalikud meetodid, mida läheb tarvis ametiasutuse ja ettevõtte tööprotsesside toetamiseks.

Vaadeldavate rakenduste kajastamise detailsus tuleb igas institutsioonis eraldi valida. Eesmärk on tagada, et struktuurianalüüsi tegemine ja turbevajaduse kindlaksmääramine oleks võimalikult läbinähtav ja tõhus. Siinkohal võivad abiks olla ka IT-etalonturbe kataloogide rakendusekihtide moodulid.

Töövaeva vähendamiseks saab infokoosluse struktuuri analüüsimisel piirduda ka vaadeldavate tööprotsesside jaoks hädavajalike rakenduste ja infoga. Seejuures on oluline, et analüüsis võetaks arvesse vähemalt selliseid rakendusi ja infot, millega seotud tööprotsessidele kehtivad vähemalt miinimumnõuded kas:

- konfidentsiaalsuse,
- tervikluse
- või käideldavuse vallas.

Selle tagamiseks tuleks rakenduste kohta andmete kogumisel küsida kasutajatelt või rakenduste eest vastutavatelt isikutelt, samuti tööprotsessi eest vastutavatelt isikutelt nende hinnangut.

Rakenduste üha suureneva keerukuse tõttu pole tööprotsessi ja konkreetse rakenduse seosed sageli piisavalt selged isegi vastutavatele spetsialistidele. Seega tuleks iga tööprotsessi puhul tuvastada, milliseid rakendusi see vajab ja milliseid andmeid seejuures kasutatakse. Need sõltuvusseosed tuleb tuvastada institutsiooni osakonna, rakenduste eest vastutavate spetsialistide ja abistava IT-osakonna ühise koosoleku raames.

Juhul kui erinevalt siin soovitatud järjekorrast vaadeldakse esmalt IT-süsteeme, on sageli kasulik, kui rakenduste kohta hakatakse infot koguma esmajoones IT-süsteemide alusel. Seejuures tuleks alustada serveritest, sest nende mõju on kõige laialdasem. Võimalikult tasakaalustatud pildi saamiseks on seejärel võimalik neid andmeid klient- ja töökohasüsteemide põhjal täiendada. Pärast seda tuleb veel tuvastada, millised võrguühenduselemendid toetavad milliseid rakendusi.

Liigituse arusaadavuse suurendamiseks tuleb rakendused nummerdada. Kuna paljud infoturbespetsialistid täidavad samal ajal ka andmekaitsespetsialisti töökohustusi ja vastutavad seega ka isikuandmete turbe eest, on sobilik juba siinkohal ära märkida, kas kirjeldatud rakendus salvestab ja/või töötleb isikuandmeid. Rakenduse turbevajadus tuleneb tavaliselt sellega töödeldava info turbevajadusest. Seega tuleks sellise info liik dokumenteerida ka tabelina.

Lisaks oleks rakenduste puhul mõistlik kajastada ka seda infot, millised tööprotsessid neid rakendusi vajavad. Kirja tuleks panna ka vastutav isik ja rakenduse kasutaja, et kontaktisikuid oleks kergem üles leida või et jõuda kiiremini asjasse puutuvate kasutajarühmadeni.

Rakendusi kajastava info kogumisel tuleks vaadelda ka andmekandjaid ja dokumente ning käsitleda

neid sama moodi nagu rakendusi. Andmekandjad ja dokumendid, mis ei ole mõne rakenduse või IT-süsteemiga selgelt seotud, tuleb struktuurianalüüsiga eraldi integreerida. Loomulikult pole seejuures otstarbekas kõiki andmekandjaid ükshaaval vaadelda. Esiteks tuleks vaadelda ainult selliseid andmekandjaid ja dokumente, mille suhtes kehtib vähemalt minimaalne turbevajadus, ning teiseks tuleks need koondada rühmadesse. Järgnevalt on toodud struktuurianalüüsis eraldi vaadeldavate andmekandjate ja dokumentide näited:

- arhiveerimise ja varundamise andmekandjad;
- väliste partneritega andmevahetuseks kasutatavad andmekandjad;
- andmete transpordiks ettenähtud USB-mälupulgad;
- väljaprindituna käepärast hoitavad käsiraamatud hädaolukordade tarbeks;
- mikrofilmid;
- partnerite ja klientidega sõlmitud olulised lepingud.

Rakenduste sõltuvussuhete tuvastamine

Parema ülevaate saamiseks võib soovi korral ära näidata rakenduste sõltuvussuhted. Näiteks ei saa tellimusi töödelda, kui puudub info laovarude kohta.

Sündmuste dokumenteerimiseks võib kasutada tabelit või asjakohast tarkvara.

Näide: töökorralduse ja haldamise amet (THA) – 1. osa

Järgnevalt näidatakse fiktiivse ametiasutuse THA näitel, kuidas võiks rakendusi dokumenteerida. Tuleb arvestada, et THA struktuur pole infoturbe tagamise seisukohast sugugi optimaalne. See on mõeldud vaid IT-etalonturbe metoodika evitamise näitlikustamiseks. Selles dokumendis antakse üksnes ülevaade. Tervikliku näite leiate IT-etalonturbe abivahendite hulgast.

THA on fiktiivne ametiasutus, kus töötab 150 inimest, kellest 130 kasutavad lauaarvuteid. Ametiasutuse peakorter asub Bonnis ja harukontor Berliinis, kus täidetakse muu hulgas selliseid tööülesandeid nagu reeglite loomine, normeerimine ja koordineerimine. 130-st infotehnoloogiat kasutavast töötajast töötab 90 Bonnis ja 40 Berliinis.

Tööülesannete täitmiseks on kõik töökohad omavahel võrku ühendatud. Berliini harukontor on ametiasutuse võrguga ühendatud renditud püsiühenduse kaudu. Iga töötaja saab mis tahes ajal vaadata kõiki tööprotsessidele kehtestatud direktiive ja eeskirju ning formulare ja tekstimooduleid. Kõik olulised töötulemused kantakse tsentraalsesse andmebaasi. Visandid koostatakse, edastatakse ja allkirjastatakse eranditult elektrooniliselt. Kõikide vajalike tööfunktsioonide tagamine ja haldamine on Bonnis asuva IT-osakonna ülesanne.

THA tööprotsesse hallatakse elektrooniliselt ja nende nimetused põhinevad kaheastmelisel skeemil. Lühendi GP (tööprotsess) taga on põhiprotsessi number, pärast sidekriipsu alamprotsessi number, nt GP0-2.

Järgnevalt esitatakse väljavõte rakendustest ja nendega seotud info kajastamisest THA näitel.

Nr	Rakendus	Info liik*	Vastutav isik	Kasutajad	Tööprotsessid
A1	Isikuandmete töötlemine	P	Z1	Z1	GP0-1, GP0-2
A2	Toetuste maksmine	P	Z2	Kõik	GP0-2
A3	Lähetuskulude tasaarveldamine	P/V/F	Z2	Kõik	GP0-1, GP0-3
A4	Kasutajate autentimine	P/S	IT1	Kõik	GP0, GP5, GP6
A5	Süsteemihaldus	S	IT3	IT3	Kõik
A6	Büroosisene suhtlus	P/V/F/S	IT3	Kõik	Kõik

A7	Tsentraalne dokumendihaldus	P/V/F/S	Z1	Kõik	GP0, GP5
A8	USB-mälupulgad	P/V/F	IT3	IT3	GP0-1, GP0-3

* Legend:

- P = isikuandmed
- V = THA haldusinfo, nt institutsiooni struktuur ja juhised
- F = THA töövaldkonna info, nt suhtlus klientidega
- S = süsteemiinfo / tehniline info, nt IT-süsteemide konfiguratsiooniandmed

Iga rakenduse juurde on lisatud info liik, et oleks võimalik kiirelt näha, milline on seda infot töötlevate rakenduste turbevajadus. Ülemises tabelis kasutatud kategooriad on näited, st need ei ole infokategooriate soovitused.

Peatüki 4.2.2 „Rakenduste ja nendega seotud info ülesmärkimine" rõhuasetus

- Koostöö vaadeldava osakonna, rakenduste eest vastutava isiku ja abistava IT-osakonna vahel eesmärgiga uurida välja analüüsitavate tööprotsesside jaoks olulised rakendused
- Rakenduste ülevaate koostamine ja täiendamine üheselt mõistetavate numbrite või lühenditega
- Iga rakendusega seotud asjakohaste tööprotsesside, töödeldava info, vastutavate isikute ja vajaduse korral ka kasutajate kirjapanek
- Märkimine iga rakenduse kohta, kui palju kasutatakse seda isikuandmete töötlemiseks

4.2.3 Võrgu planeeringu analüüs

Edasise tehnilise analüüsi puhul on sobilik lähtuda võrgu planeeringust (nt võrgu topoloogiaskeemist). Võrguplaan on vaadeldavate info- ja sidetehnoloogia komponentide ning nende ühenduste graafiline ülevaade. Võrguplaanid või muud sellised graafilised ülevaated on enamikus institutsioonides kindlasti juba olemas, sest neid läheb tarvis süsteemide käitamisel. Konkreetsel juhul peaks plaan kajastama infoturbe seisukohta arvesse võttes vähemalt järgmisi objekte:

- IT-süsteemid, st klientsüsteemide ja serveritena töötavad arvutid, aktiivsed võrgukomponendid (nt kommutaatorid, marsruuterid, WLAN-i pääsupunktid), võrguprinterid jne;
- nende süsteemide vahelised võrguühendused, st LAN-ühendused (nt Ethernet, TokenRing), WLAN-id, magistraaltehnoloogia (nt FDDI, ATM) jne;
- vaadeldavast valdkonnast välja suunatud ühendused, st ISDN-i või modemi sissevalimise juurdepääsud, analoogtehnoloogia või marsruuterite internetiühendused, raadioside või renditud kaabliühendused eemal asuvate hoonete või harukontorite ühendamiseks jne.

Iga näidatud objekti juurde kuulub minimaalne hulk infot, mille leiab vastavast kataloogist. Iga IT-süsteemi puhul tuleks kajastada vähemalt järgmist infot:

- selge tähis (nt täielik hostinimi või ID-number);
- tüüp ja funktsioon (nt rakenduse X andmebaasiserver);
- baasiks olev platvorm (st riistvaraplatvorm ja operatsioonisüsteem);
- asukoht (nt hoone ja töökabineti number);
- vastutav administraator;
- olemasolevad sideliidesed (nt internetiühendus, Bluetooth, WLAN-i adapter);
- võrguühenduse liik ja võrguaadress. Oluline pole mitte ainult süsteeme, vaid ka

süsteemidevahelisi võrguühendusi ja välisühendusi kajastav info:

- kaabli või sideühenduse liik (nt optiline kaabel või WLAN, mis põhineb standardil IEEE 802.11);
- maksimaalne andmeedastuskiirus (nt 100 Mbps);
- alumistes kihtides kasutatavad võrguprotokollid (nt Ethernet, TCP/IP);
- välisühenduste puhul välise võrgu info (nt internet, teenusepakkuja nimi).

Võrguplaanis peavad kajastuma ka virtuaalsed IT-süsteemid ja võrguühendused, nt virtuaalsed kohtvõrgud (VLAN-id) või privaatvõrgud (VPN-id), kui nendega loodavad loogilised (virtuaalsed) struktuurid erinevad olulisel määral füüsilistest struktuuridest. Ülevaate tagamiseks võib olla otstarbekas kujutada loogilisi (virtuaalseid) struktuure eraldi võrguplaanis.

Erineva turbevajadusega valdkonnad tuleks ka erinevalt tähistada.

Kui vähegi võimalik, peaks võrguplaan olema elektrooniline ja selliselt ka hooldatav. Kui institutsiooni infotehnoloogia puhul on teatud suurusjärk juba ületatud, tuleks võrguplaani koostamiseks ja hooldamiseks kasutada abiprogramme, sest dokumentatsioon on keeruline ja muutub pidevalt.

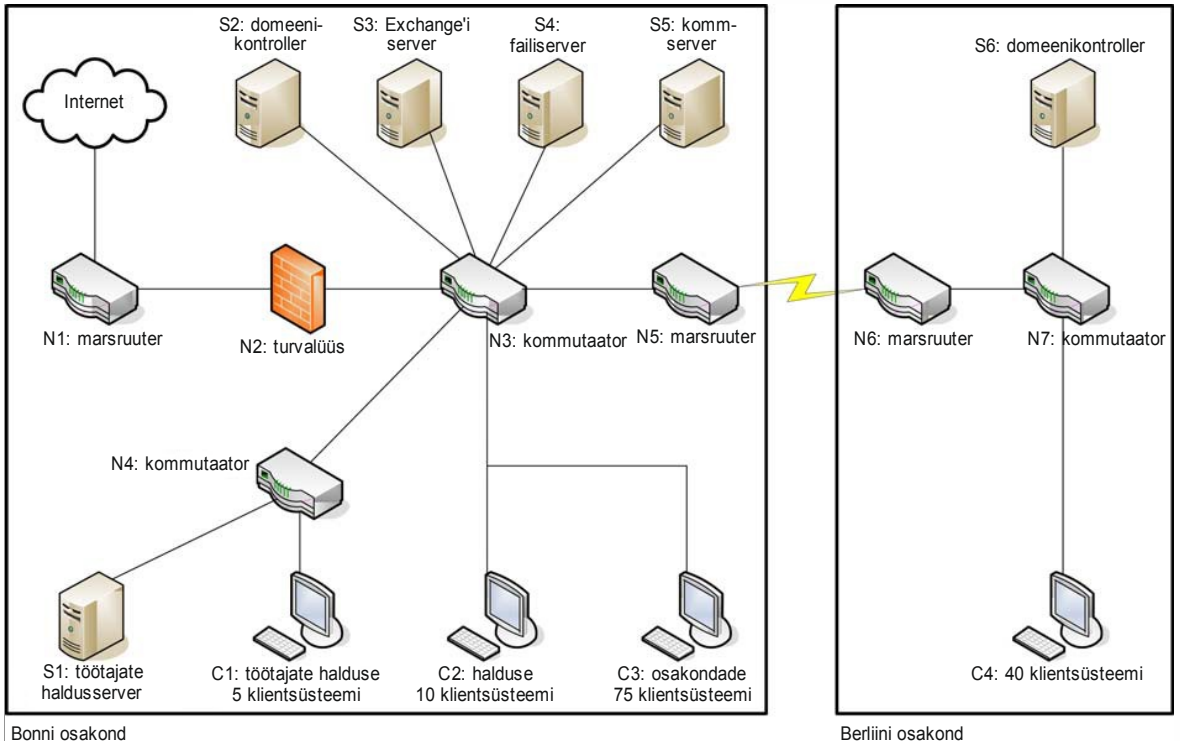
Võrguplaani värskendamine

Kuna IT-struktuuri kohandatakse pidevalt institutsiooni vajadustega ja võrguplaani hooldamine nõuab ressursse, ei ole võrguplaanid sageli piisavalt aktuaalsed. Pigem muudetakse plaani ainult IT-struktuuri suuremate muudatuste korral.

Struktuurianalüüsi järgmise sammuna tuleb olemasolevat võrguplaani (või osaplaane, kui tervikplaan on ülevaatlikkuse tagamiseks osadeks jaotatud) võrrelda IT tegeliku struktuuriga ja plaani vajaduse korral uuendada. Selleks tuleb pidada nõu IT eest vastutavate töötajate ning rakenduste ja võrkude administraatoritega. Kui võrkude ja süsteemide tsentraalseks halduseks kasutatakse programme, tuleks kindlasti alati kontrollida, kas nendest programmidest on võrguplaani koostamisel abi. Siinkohal tuleb arvestada, et komponentide automaatsed või poolautomaatsed tuvastamisfunktsioonid koormavad ajutiselt võrku. Seega peab olema tagatud, et lisanduv võrguliiklus ei pärsiks IT-süsteemide tööd. Automaatse või poolautomaatse tuvastamise tulemused tuleb kindlasti ka üle kontrollida, et näha, kas kõik olulised komponendid ikka leiti üles.

Näide: töökorralduse ja haldamise amet (THA) – 2. osa

Järgnevalt on esitatud näide selle kohta, kuidas võib välja näha fiktiivse THA võrguplaan.



Joonis 6. Struktuurianalüüsi võrguplaani näide

Näidatud võrguplaanis tähistatakse IT-süsteeme numbri (servereid, klientsüsteeme ja aktiivseid võrgukomponente kajastavad tähised S*n*, C*n* või N*n*) ja funktsiooniga.

Nii Berliinis kui ka Bonnis on klientsüsteemid liigitatud rühmadesse. Kuigi kõik 130 klientsüsteemi on peaaegu ühesuguse konfiguratsiooniga, erinevad nad üksteisest siiski töödeldavat infot, rakendusi, võrguühendusi ja taristuid puudutavate raamtingimuste poolest. Rühm C1 tähistab personaliosakonna 5 klientsüsteemi. Neil on juurdepääs Bonni personaliosakonna serverile S1. Rühmad C2 ja C3 koondavad haldusosakonna 10 ja Bonni osakonna 75 klientsüsteemi. Need erinevad vaid kasutatavate programmide poolest. Rühm C4 tähistab Berliini harukontori osakondade klientsüsteeme. Rühmadest C1–C3 erinevad nad ümbritseva taristu ja tervikvõrguga ühendamise poolest.

Peatüki 4.2.3 „Võrgu planeeringu analüüs” rõhuasetus
• Võrgu olemasoleva graafilise kujutise, nt võrgu topoloogiaskeemide uurimine • Vajaduse korral võrguplaanide värskendamine või uute plaanide koostamine • Olemasolevate IT-süsteemide lisainfo kontrollimine ning vajaduse korral selle värskendamine ja täiendamine • Olemasolevate sideühenduste lisainfo kontrollimine ning vajaduse korral selle värskendamine ja täiendamine

4.2.4 IT-süsteemide ülesmärkimine

Hilisema turbevajaduse tuvastamise ja infokoosluse modelleerimise jaoks tuleks olemasolevatest ja planeeritud IT-süsteemidest koostada tabel. Termin „IT-süsteem” tähistab peale arvutite ka aktiivseid võrgukomponente, võrguprintereid, kodukeskjaamu jms. Esikohal on IT-süsteemi tehniline teostus, nt töökohaarvuti, Windows Server 2003, Windows XP klientsüsteem, Unixi server, kodukeskjaam. Siinkohal tuleks vaadelda ainult süsteemi (nt Unixi serverit kui tervikut), mitte üksikuid komponente, millest IT-süsteem koosneb (seega mitte arvutit, klaviatuuri ega monitori vms).

Täieliku ja korrektse info kogumine olemasolevate ja planeeritud IT-süsteemide kohta on enamat kui ainult turbekontseptsiooni koostamise abivahend. Seda infot läheb tarvis ka IT-süsteemide kontrollimiseks, hooldamiseks, veaotsinguks ja remondiks.

Infot tuleb koguda nii võrku ühendatud kui ka võrku ühendamata IT-süsteemide kohta, eriti siis, kui senine võrguplaan neid süsteeme ei kajasta. IT-süsteeme, mis on võrguplaanis koondatud üheks rühmaks, võib käsitleda ühe tervikobjektina. Ka võrguplaanist puuduvate IT-süsteemide puhul tuleb kontrollida, kas neid oleks otstarbekas liigitada rühmadesse. See on võimalik nt suurema arvu võrku ühendamata töökohaarvutite puhul, mis vastavad peatükis 4.2.1 nimetatud rühmade moodustamise tingimustele.

Nende andmete kogumise käigus tuleb edasise töö tarbeks märkida üles järgmine info:

- IT-süsteemi konkreetne tähis;
- kirjeldus (tüüp ja funktsioon);
- platvorm (nt riistvara arhitektuur / operatsioonisüsteem);
- rühmade puhul: rühmadeks koondatud IT-süsteemide arv;
- IT-süsteemi paigalduskoht;
- IT-süsteemi olek (töös, katsetusrežiimis, planeerimisel);
- IT-süsteemi kasutajad / administraatorid.

Seejärel näidatakse ära rakenduste ja IT-süsteemide seosed. Seosena võidakse kasutada nii selliseid IT-süsteeme, milles rakendused töötavad, kui ka selliseid, mis nende rakenduste andmeid edastavad. Tulemuseks on ülevaade, mis näitab oluliste rakenduste ja süsteemide seoseid.

Näide: töökorralduse ja haldamise amet (THA) – 3. osa

Järgnevas tabelis on näitena toodud THA IT-süsteemide nimekirja väljavõte.

Nr	Kirjeldus	Platvorm	Arv	Paigaldus koht	Seisund	Kasutajad
S1	Personalihalduse server	Windows Server 2003	1	Bonn, R 1.01	Töös	Personal
S2	Domeenikontrollerid	Windows Server 2003	1	Bonn, R 3.10	Töös	Kõik IT-kasutajad
C1	Isikuandmeid töötlevate klientsüsteemide rühm	Windows Vista	5	Bonn, R 1.02 – R 1.06	Töös	Personal
C2	Haldusosakonna klientsüsteemide rühm	Windows Vista	10	Bonn, R 1.07 – R 1.16	Töös	Haldusosakond
C6	Berliini osakonna sülearvutite rühm	Windows Vistaga sülearvuti	2	Berliin, R 2.01	Töös	Kõik Berliini harukontori IT-kasutajad
N1	Internetimarsruuter	Marsruuter	1	Bonn, R 3.09	Töös	Kõik IT-kasutajad
N2	Tulemüür	Unixiga töötav lüüsirakendus	1	Bonn, R 3.09	Töös	Kõik IT-kasutajad
N3	Kommutaator	Kommutaator	1	Bonn, R 3.09	Töös	Kõik IT-kasutajad

T1	Bonni kodukeskjaam	ISDN-kodukeskjaam	1	Bonn, B.02	Töös	Kõik Bonni peakorteri töötajad

IT-süsteemid/rühmad S1, S2, C1, C2, N1, N2 ja N3 on võetud otse võrguplaanist. Nendele on juurde lisatud võrku ühendamata IT-süsteemid C6 (sülearvuti) ja T1 (kodukeskjaam). ???

Järgnevalt näidatakse THA näitel väljavõtet rakenduste ja IT-süsteemide seostest.

Rakenduse kirjeldus		**IT-süsteemid**						
Nr	**Rakendus / info**	S1	S2	S3	S4	S5	S6	S7
A1	Isikuandmete töötlemine	X						
A2	Toetuste maksmine	X						
A3	Lähetuskulude tasaarveldamine	X						
A4	Kasutajate autentimine		X				X	
A5	Süsteemihaldus		X					
A6	Büroosisene suhtlus			X				
A7	Tsentraalne dokumendihaldus				X			
A8	USB-mälupulgad							

Legend: Ai X Sj = rakenduse Ai töö sõltub IT-süsteemist Sj.

Peatüki 4.2.4 „IT-süsteemide ülesmärkimine" rõhuasetus

- Kontrollimine, kas olemasolevate või planeeritud IT-süsteemide kohta leiduvad andmebaasid sobivad edasise töö lähtepunktiks
- Ühendatud ja ühendamata IT-süsteemide nimekirja koostamine või värskendamine ja täiendamine
- IT-süsteemide või nende rühmade tähistamine selgete numbrite või lühenditega
- Rakenduste seostamine nende töö jaoks vajalike IT-süsteemidega (nt serverid, klientsüsteemid, võrguühenduselemendid)

4.2.5 Ruumide ülesmärkimine

Tööprotsesse ei tule vaadelda mitte üksnes IT-süsteemide, vaid ka institutsiooni taristu, nt ruumide põhjal. Olenevalt suurusest ja mitmest muust tegurist võib institutsioon asuda kas eraldi hoones või ka ainult hoone ühel korrusel. Paljud institutsioonid kasutavad harukontoreid, mis võivad asuda üksteisest väga kaugel või mida tuleb jagada teiste institutsioonidega. Sageli tuleb tööprotsesside täitmiseks kasutada võõraid ruume ja sõlmida selleks asjakohased kasutuslepingud.

Turbekontseptsioon peab arvestama kõikide harukontoritega, mida seob omavahel samade tööülesannete täitmine. Arvestada tuleb institutsiooni territooriumi, hoonete, korruste, ruumide ja ka nendevaheliste liikumisteedega. Kõik sideühendused, mis läbivad kõrvalistele osalistele/isikutele ligipääsetavaid alasid, on välisühendused. Sama kehtib ka traadita sidekanalite kohta, kui pole võimalik välistada, et kolmas osaline võib neile ligi pääseda.

IT-etalonturbe järgi toimuva modelleerimise ning vajaduste ja tegeliku olukorra võrdluse planeerimise jaoks on kasulik koostada ülevaade kõikidest asukohtadest, eriti aga ruumidest, kus asuvad IT-süsteemid või mida kasutatakse IT-süsteemide käitamiseks. Selle alla kuuluvad sellised ruumid, mida kasutatakse eranditult IT-süsteemide käitamiseks (nt serveriruumid, andmekandjaarhiivid), ruumid, milles kasutatakse IT-süsteeme lisaks teistele ülesannetele (nt bürooruumid), ja ka ruumid, millest kulgevad läbi sideühendused. Kui IT-süsteemid asuvad eraldi tehnikaruumi asemel kaitsekapis, tuleb kaitsekappi vaadelda eraldi ruumina.

Teadmiseks: IT-süsteeme kajastava info kogumisel märgitakse üles ka paigalduskohad. Lisaks tuleb uurida, kas muudes ruumides hoitakse kaitsmist vajavat infot. Ka need ruumid tuleb analüüsi kaasata. Muu hulgas tuleb arvestada veel ka ruumidega, kus hoitakse mitteelektroonilist infot, nt pabertoimikuid või mikrofilme. Dokumentatsioon peab näitama töödeldava info liiki.

Näide: töökorralduse ja haldamise amet (THA) – 4. osa

Järgnev lõik esitab THA näitel, milline võib olla ruumide ülevaatlik tabel. Siin on juba jäetud ka tühjad kohad ruumide turbevajaduse kindlaksmääramiseks, kuid need lahtrid täidetakse alles järgmise sammu ajal.

Ruum			IT / info	Turbevajadus		
Nimetus	**Liik**	**Asukoht**	**IT-süsteemid / andmekandjad**	**Konfidentsiaalsus**	**Terviklus**	**Käideldavus**
R U.02	Andmekandjaarhiiv	Bonni hoone	Varundusandmekandja (serverite S1–S5 iganädalane			
R B.02	Tehnikaruum	Bonni hoone	Kodukeskjaam			
R 1.01	Serveriruum	Bonni hoone	S1, N4			
R 1.02 – R 1.06	Bürooruumid	Bonni hoone	C1			
R 3.11	Kaitsekapp ruumis R 3.11	Bonni hoone	Varundusandmekandja (serverite S1–S5 igapäevane varukoopia)			
R E.03	Serveriruum	Berliini hoone	S6, N6, N7			
R 2.01 – R 2.40	Bürooruumid	Berliini hoone	C4, mõned faksiaparaatidega			

Peatüki 4.2.5 „Ruumide ülesmärkimine" rõhuasetus

- Nimekirja koostamine kõikidest asukohtadest, hoonetest ja ruumidest, mis märgiti üles IT-süsteeme kajastava info kogumisel
- Muude ruumide lisamine, kui nendes ruumides hoitakse või töödeldakse turbevajadusega infot

4.3 Turbevajaduse kindlaksmääramine

Turbevajaduse kindlaksmääramine aitab langetada infokoosluses leiduvate objektide puhul otsust, milline on nende objektide vajadus konfidentsiaalsuse, tervikluse ja käideldavuse järele. Turbevajadus oleneb asjakohaste rakenduste ja vastavate tööprotsesside võimalikest kahjudest.

Infokoosluse turbevajaduse kindlaksmääramine koosneb järgmistest etappidest:

- turbevajaduse kategooriate defineerimine;
- rakenduste turbevajaduse kindlaksmääramine;
- IT-süsteemide turbevajaduse kindlaksmääramine;
- ruumide turbevajaduse kindlaksmääramine;
- sideühenduste turbevajaduse kindlaksmääramine;
- kindlaksmääratud turbevajaduste põhjal tehtavad järeldused.

Turbevajaduse kategooriate definitsiooni kohaselt määratakse esmalt kindlaks tööprotsesside ja rakenduste turbevajadused, lähtudes seejuures tüüpilistest kahjustsenaariumidest. Seejärel tuletatakse

nende põhjal üksikute IT-süsteemide, ruumide ja sideühenduste turbevajadused.

Järgmistes jaotistes kirjeldatakse seda meetodit põhjalikumalt.

4.3.1 Turbevajaduse kategooriate defineerimine

Kuna turbevajadust pole tavaliselt võimalik täpselt mõõta, piirdub IT-etalonturve edaspidi kvalitatiivse hinnanguga, jaotades turbevajaduse järgmiseks kolmeks kategooriaks.

Turbevajaduse kategooriad	
Madal	Kahjude tagajärjed on piiratud ja ülevaatlikud.
Keskmine	Kahjudel võivad olla ulatuslikud tagajärjed.
Kõrge	Kahjude tõttu võib ohtu sattuda institutsiooni edasitoimimine, kahjudel on katastroofilised tagajärjed.

Järgmised sammud selgitavad, kuidas määrata kindlaks tööprotsesside ja nendega seotud rakenduste turbevajaduse kategooria.

Tööprotsessi, rakenduse või andmete konfidentsiaalsuse, tervikluse või käideldavuse kaost tingitud kahjude korral saab enamasti eristada järgmisi kahjustsenaariume:

- seaduste, ettekirjutuste või lepingute rikkumine;
- infot puudutava iseseisva otsustamise õiguse piiramine;
- isikupuutumatuse rikkumine;
- tööülesannete täitmise piiramine;
- negatiivsed sise- ja välismõjud;
- rahalised tagajärjed.

Kahju korral on sageli tegu mitme kahjustsenaariumiga. Näiteks võib rakenduse töö seiskumine mõjutada tööülesannete täitmist ning sellega võib omakorda kaasneda rahaline ja mainekahju.

Turbevajaduse kategooriate „L”, „M” ja „H” üksteisest paremaks eraldamiseks tuleks kindlaks määrata kahjustsenaariumide piirid. Allolevad tabelid aitavad otsustada, milline on potentsiaalsest kahjust ja selle tagajärgedest tulenev turbevajadus. Institutsioon peab neid tabeleid kindlasti kohandama, et need vastaksid tegelikele oludele.

Turbevajaduse kategooria „L”	
1. Seaduste, ettekirjutuste või lepingute rikkumine	• Eeskirjade ja seaduste rikkumise tagajärjed pole rasked. • Lepingut rikutakse vähe, leppetrahvid on minimaalsed.
2. Infot puudutava iseseisva otsustamise õiguse piiramine	• Tegu on isikuandmetega, mille töötlemisega võib saada kannatada asjaomase isiku ühiskondlik positsioon või majanduslik seis.
3. Isikupuutumatuse rikkumine	• Mõju on ebatõenäoline.
4. Tööülesannete täitmise piiramine	• Asjaomane isik peaks mõju talutavaks. • Töökatkestuse maksimaalne vastuvõetav kestus ületab 24 tundi.
5. Negatiivsed sise- ja välismõjud	• Vähene või ainult organisatsioonisisene mainekahju või usalduse vähenemine.
6. Rahalised tagajärjed	• Organisatsiooni jaoks talutav rahaline kahju.

Turbevajaduse kategooria „M”	
1. Seaduste, ettekirjutuste või lepingute rikkumine	• Eeskirjade ja seaduste rikkumisel on rasked tagajärjed. • Lepingu rikkumisega kaasneksid suured leppetrahvid.
2. Infot puudutava iseseisva otsustamise õiguse piiramine	• Tegu on isikuandmetega, mille töötlemisega võib saada kannatada asjaomase isiku ühiskondlik positsioon või majanduslik seis.
3. Isikupuutumatuse rikkumine	• Isikupuutumatuse rikkumist ei ole võimalik täielikult välistada.
4. Tööülesannete täitmise piiramine	• Osa asjaomaste isikute jaoks oleks mõju vastuvõetamatu. • Töökatkestuse maksimaalne vastuvõetav kestus on 1–24 tundi.
5. Negatiivsed sise- ja välismõjud	• Maine ja usaldusväärsus saaksid ulatuslikult kahjustada.
6. Rahalised tagajärjed	• Rahaline kahju on märkimisväärne, kuid ei ohusta organisatsiooni olemasolu.

Turbevajaduse kategooria „H”	
1. Seaduste, ettekirjutuste või lepingute rikkumine	• Eeskirjade ja seaduste jäme rikkumine. • Lepingu rikkumisest tuleneva vastutusega seotud tagajärjed oleksid laostavad.
2. Infot puudutava iseseisva otsustamise õiguse piiramine	• Tegu on isikuandmetega, mille töötlemine seaks ohtu asjaomase isiku elu ja tervise või vabaduse.
3. Isikupuutumatuse rikkumine	• Isikupuutumatus võib saada märkimisväärselt kahjustada. • Elu ja tervis satuvad ohtu.
4. Tööülesannete täitmise piiramine	• Asjaomane isik peaks mõju talumatuks. • Töökatkestuse maksimaalne vastuvõetav kestus on lühem kui üks tund.
5. Negatiivsed sise- ja välismõjud	• Üleriigiline mainekahju või usalduse kaotamine võib võtta koguni olemasolu ohustavad mõõtmed.
6. Rahalised tagajärjed	• Rahaline kahju ohustaks organisatsiooni olemasolu.

Kui olude täpsem analüüs näitab, et peale nende kuue kahjustsenaariumi saab rakendada ka teisi, tuleb need lisada. Ka kõikide selliste kahjude puhul, mis ei mahu nende stsenaariumide raamesse, tuleb samuti kindlaks määrata, mis eristab kategooriaid „L”, „M” või „H”.

Lisaks tuleb arvestada institutsiooni eripäradega: kui suurettevõtte jaoks on 200 000 euro suurune kahju selle käivet ja IT eelarvet arvesse võttes tühine, siis väikeettevõtte puhul võib 10 000 euro suurune kahju juba tema olemasolu ohustada. Seega võib olla mõistlik määrata piiriks mõni protsentuaalne suurus, mis lähtub kogukäibest, kasumist või mõnest muust sellisest näitajast.

Samast vaatepunktist võib läheneda ka käideldavusele. Näiteks võib 24-tunnine katkestus olla

turbevajaduse kategoorias „Tavaline" veel vastuvõetav. Kui aga sellised katkestused sagenevad ja leiavad aset nt rohkem kui kord nädalas, ei ole need summeeritult enam vastuvõetavad. Seega tuleb turbevajaduse kategooriate alusel tuvastatud käideldavusnõudeid täpsustada.

Punkti „Infot puudutava iseseisva otsustamise õiguse piiramine" turbevajaduse hindamiseks pakuvad mõned Saksa andmekaitsespetsialistid konkreetseid näiteid, mille selgitused on kirjas turbeastmete kontseptsioonides.

Tõmmates piiri tavalise ja suure turbevajaduse vahele, tuleks arvestada, et tavalise turbevajaduse puhul peab piisama IT-etalonturbe standardsetest turbemeetmetest. Tehtud järeldused tuleb turbekontseptsioonis dokumenteerida, sest nendest olenevad turbemeetmete valik ja kulud.

Peatüki 4.3.1 „Turbevajaduse kategooriate defineerimine" rõhuasetus

- Turbevajaduse kategooriate defineerimiseks vajalike tüüpiliste kahjustsenaariumidega arvestamine
- Turbevajaduse kategooriate „L", „M" või „H" kindlaksmääramine ja kohandamine institutsiooni oludega

4.3.2 Rakenduste turbevajaduse kindlaksmääramine

Rakenduste puhul tuleb vaadelda maksimaalseid lühi- ja pikaajalisi kahjusid, mis tekivad siis, kui peaks kaduma rakenduse või info konfidentsiaalsus, terviklus või käideldavus. Esitades küsimuse „Mis juhtuks, kui ... ?", luuakse *kasutaja vaatepunktist* realistlikud kahjustsenaariumid ja kirjeldatakse eeldatavaid materiaalseid või ideelisi kahjusid. Võimalike kahjude suurus määrab lõpuks kindlaks ka rakenduse turbevajaduse. Seejuures tuleb rakenduste eest vastutavatelt isikutelt ja rakenduste kasutajatelt kindlasti küsida nende isiklikku hinnangut. Tavaliselt on neil hea ettekujutus võimalikest kahjudest ja nad saavad anda olulisi juhtnööre andmete kogumiseks.

Turbevajaduse kindlaksmääramisse tuleb kaasata ka struktuurianalüüsi raames andmekandjate ja dokumendirühmade kohta kogutud andmed.

Selleks, et lihtsustada võimalike kahjude ja mõjude tuvastamist, on selle standardi lisas ära toodud asjakohased küsimused. See abimaterjal ei pretendeeri täiuslikkusele, tegu on orientiiriga. Institutsiooni individuaalsete ülesannete ja seisundiga arvestamiseks tuleb neid küsimusi kindlasti täiendada ja muuta.

Vaadeldavate rakenduste turbevajaduse kindlaksmääramine on riskihalduse raames tehtav otsus ja see mõjutab sageli olulisel määral vaadeldava infokoosluse turbekontseptsiooni. Rakenduste turbevajadust mõjutab oluliselt ka tehnika ja taristu (nt serverite ja ruumide) turbevajadus.

Turbevajaduse ja selle alusel tehtavate infoturbehaldust puudutavate otsuste paremaks mõistmiseks ja hilisemaks kontrollimiseks tuleb rakenduste kindlaksmääratud turbevajadused põhjalikult dokumenteerida. Seejuures tuleb jälgida, et peale turbevajaduse kohta tehtud otsuste dokumenteeritaks kindlasti ka otsuste põhjendused. Need põhjendused võimaldavad otsuseid hiljem kontrollida ja ka edaspidi kasutada.

Näide: töökorralduse ja haldamise amet (THA) – 5. osa

Järgnevas tabelis tuuakse THA näitel välja olulised rakendused, nende turbevajadused ja põhjendused.

Rakendus			Turbevajaduse kindlaksmääramine		
Nr	**Tähistus**	**Isikuandmed**	**Rõhuasetus**	**Turbevajadus**	**Põhjendus**
A1	Isikuandmete töötlemine	X	Konfidentsiaalsus	M	Isikuandmed on eriti suure turbevajadusega, sest nende avalikustamine võib asjaomaseid isikuid oluliselt mõjutada.
			Terviklus	L	Turbevajadus on tavaline, sest vigu märgatakse ruttu ja andmeid saab tagantjärele korrigeerida.
			Käideldavus	L	Manuaalsete töömeetodite kasutamine võimaldab toime tulla kuni ühenädalase katkestusega.
A2	Toetuste maksmine	X	Konfidentsiaalsus	M	Toetuste maksmise andmed on eriti suure turbevajadusega isikuandmed, mis võivad osalt sisaldada ka infot haiguste või diagnooside kohta. Avalikustamine võib asjaomaseid isikuid oluliselt mõjutada.
			Terviklus	L	Turbevajadus on tavaline, sest vigu märgatakse ruttu ja andmeid saab tagantjärele korrigeerida.
			Käideldavus	L	Manuaalsete töömeetodite kasutamine võimaldab toime tulla kuni ühenädalase katkestusega.

Siinkohal võib olla mõistlik vaadelda peale selle info ka tööprotsessi kui terviku turbevajadust. Selleks tuleks kirjeldada rakenduse eesmärki tööprotsessi raames ja teha sellest järeldused rakenduse olulisuse kohta. Olulisust saab liigitada järgmiselt:

rakenduse olulisuse aste tööprotsessi jaoks:

- **L:** vastuvõetava lisapingutuse abil saab tööprotsess toimuda ka teisi vahendeid kasutades (nt käsitsi töötades);
- **M:** tööprotsessi käigushoidmine nõuab suurt lisapingutust ja teiste vahendite kasutamist;
- **H:** tööprotsess ei saa rakenduseta toimida.

Selliste terviklike seoste loomise peamine eelis seisneb selles, et juhtkond saab rakenduste turbevajaduse kindlaksmääramist reguleerida. Näiteks on võimalik, et vastutav isik liigitas rakenduse turbevajaduse oma vaatepunkti järgi kategooriasse „L", kuid juhtkond leiab, et see on tööprotsesside toimimise seisukohast hoopis suurema turbevajadusega.

Ka need lisaandmed tuleks dokumenteerida tabelitena või vastava tarkvara abil.

Peatüki 4.3.2 „Rakenduste turbevajaduse kindlaksmääramine" rõhuasetus

- Rakenduste turbevajaduse kindlaksmääramine kahjustsenaariumide ja küsimuste kataloogide alusel
- Turbevajaduse ja vastavate põhjenduste dokumenteerimine tabelitena

4.3.3 IT-süsteemide turbevajaduse kindlaksmääramine

IT-süsteemi turbevajaduse kindlaksmääramiseks tuleb vaadelda esmalt IT-süsteemiga otseselt seotud rakendusi. Ülevaate sellest, millised rakendused on milliste IT-süsteemide jaoks olulised, andis struktuurianalüüs (vt ptk 4.2.4). IT-süsteemi turbevajaduse kindlaksmääramiseks kasutatakse rakenduste turbevajadusi (vt ptk 4.3.2).

IT-süsteemide turbevajaduse kindlaksmääramiseks tuleb vaadelda asjaomaste rakenduste kahjusid tervikuna. Esmajoones on määravaks kahju või kahjud, mille tagajärjed mõjutavad IT-süsteemi turbevajadust kõige rohkem **(maksimumiprintsiip)**.

Vaadeldes võimalikke kahjusid ja nende tagajärgi, tuleb arvestada sellega, et IT-rakendused võivad oma töös kasutada ka teiste rakenduste töötulemusi. Eraldi vaadelduna mitte väga oluline rakendus A võib olla tegelikult märksa olulisem, kui tema tulemused on vajalikud tähtsa rakenduse B tulemuste jaoks. Sel juhul kehtib rakenduse B jaoks kindlaksmääratud turbevajadus ka rakendusele A. Kui rakendused töötavad erinevates IT-süsteemides, tuleb ühe IT-süsteemi turbevajaduse nõuded üle kanda ka teisele IT-süsteemile **(sõltuvusseostega arvestamine)**.

Kui üks IT-süsteem on lähtekohaks mitmele rakendusele või erinevale infole, tuleb vaadelda, kas mitme (nt väikse) kahju kuhjumise tagajärjel võib tekkida suur kahju. Seeläbi suureneb ka IT-süsteemi turbevajadus **(kumulatsiooniefekt)**.

Näide. Võrguserver sisaldab kõiki institutsiooni kliendiandmete töötlemiseks vajalikke rakendusi. Ühe sellise rakenduse rikke võimalikud tagajärjed hinnatakse väikseks, sest selle asendamiseks on olemas piisavalt alternatiive. Kui aga serveris tekiks rike (ja seeläbi ei töötaks ka ükski seda serverit kasutav rakendus), oleks ka kahju oluliselt suurem. On võimalik, et tööülesandeid ei saa enam tähtajaks täita. Seega on sellise tsentraalse komponendi turbevajadus oluliselt suurem.

Võimalik on ka vastupidine mõju. Näiteks võib rakenduse turbevajadus olla suur, kuid see ei mõjuta vaadeldavat IT-süsteemi, sest sellest IT-süsteemist olenevad ainult rakenduse ebaolulised osad. Antud juhul on tegu suhtelise turbevajadusega **(jaotusefekt)**.

Näide. Jaotusefekt esineb peamiselt seoses käideldavusega. Näiteks võib IT-süsteemide liiasuse korral üksikute komponentide turbevajadus olla rakenduse terviklikust turbevajadusest väiksem. Ka konfidentsiaalsuse puhul on jaotusefekt mõeldav: kui on tuvastatud, et klientsüsteem kasutab ülimalt konfidentsiaalse andmebaasirakenduse väheolulisi andmeid, võib klientsüsteemi turbevajadus olla andmebaasiserveriga võrreldes suhteliselt väike.

Tulemuste esitamine

IT-süsteemide kindlaksmääratud turbevajadused tuleb koondada tabelisse. See tabel peab näitama, milline on iga IT-süsteemi põhiväärtuste, st konfidentsiaalsuse, tervikluse ja käideldavuse turbevajadus. IT-süsteemi terviklik turbevajadus oleneb jällegi konfidentsiaalsuse, tervikluse ja käideldavuse maksimumväärtustest. Seega on IT-süsteemi turbevajadus suur, kui vähemalt ühe põhiväärtuse turbevajadus on suur. Üldiselt on mõistlik IT-süsteemi iga põhiväärtuse turbevajadus eraldi dokumenteerida, sest nendest tulenevad turbemeetmed on tavaliselt erinevad.

IT-süsteemi suur turbevajadus võib tuleneda nt sellest, et konfidentsiaalsuse turbevajadus on suur, kuid tervikluse ja käideldavuse järgi tavaline. Seetõttu on turbevajadus tervikuna küll suur, kuid see ei tähenda, et tervikluse ja käideldavuse turbeks peaks võtma sama rangeid meetmeid nagu konfidentsiaalsuse puhul.

IT-süsteemide turbevajaduse kindlaksmääramisel tehtud järeldusi tuleb põhjendada, et otsused oleksid mõistetavad ka valdkonnas vähem pädevate töötajate jaoks. Selleks saab viidata rakenduste turbevajaduse kindlaksmääramisele.

Näide: töökorralduse ja haldamise amet (THA) – 6. osa

IT-süsteemide kindlaksmääratud turbevajadusi saab dokumenteerida järgmisel viisil (väljavõte).

IT-süsteem		Turbevajaduse kindlaksmääramine		
Nr	**Kirjeldus**	**Põhiväärtus**	**Turbevajadus**	**Põhjendus**
S1	Personalihalduse server	Konfidentsiaalsus	M	Maksimumiprintsiip
		Terviklus	L	Maksimumiprintsiip
		Käideldavus	L	Maksimumiprintsiip
S2	Domeenikontrollerid	Konfidentsiaalsus	L	Maksimumiprintsiip
		Terviklus	M	Maksimumiprintsiip
		Käideldavus	L	Rakenduse A4 kindlaksmääratud turbevajaduse järgi oleks selle põhiväärtuse turbevajadus suur. Siiski tuleb arvestada, et see rakendus on jaotatud kahe arvuti peale. Berliini töötajad saavad autentimiseks kasutada ka Bonni harukontori teist domeenikontrollerit S6. Domeenikontrolleri S2 puhul on talutav selle kuni 72-tunnine tõrge. Tänu jaotusefektile on turbevajadus seega tavaline.

Teadmiseks: kui suurem osa IT-süsteemis töötavatest rakendustest on üksnes tavalise turbevajadusega ja ainult üks või kaks rakendust suure turbevajadusega, tuleks kaaluda võimalust viia suure turbevajadusega rakendused üle eraldi IT-süsteemi, sest nii saab seda palju eesmärgipärasemalt kaitsta ja see on sageli ka soodsam. Juhtkonnale võiks esitada vastavasisulise ettepaneku.

Peatüki 4.3.3 „IT-süsteemide turbevajaduse kindlaksmääramine" rõhuasetus

- IT-süsteemide turbevajaduse tuvastamine rakenduste turbevajaduse põhjal
- Sõltuvusseoste, maksimumiprintsiibi ja vajaduse korral ka kumulatsiooni- või jaotusefektiga arvestamine
- Iga IT-süsteemi või süsteemide rühma konfidentsiaalsuse, tervikluse ja käideldavuse dokumenteerimine

4.3.4 Ruumide turbevajaduse kindlaksmääramine

Rakenduste ja IT-süsteemide turbevajaduse tulemustest saab tuletada ka vastavate asukohtade ja ruumide turbevajaduse. Turbevajadus oleneb ruumis asuvatest IT-süsteemidest, töödeldavast infost või seal hoitavatest ja kasutatavatest andmekandjatest ning lähtub maksimumiprintsiibist. Kui ühes ruumis on suur hulk IT-süsteeme, andmekandjaid vms, nagu seda kohtab sageli serveriruumides, arvutuskeskustes või andmekandjaarhiivides, tuleb arvestada ka võimalike sõltuvusseoste ja kumulatsiooniefektidega. Iga turbevajaduse hinnangu kohta tuleb lisada ka põhjendus.

Parema ülevaate saamiseks tuleks kogu vajalik info koondada tabelisse, lähtudes juba eelkoostatud ruumide ülevaatest.

Näide: töökorralduse ja haldamise amet (THA) – 7. osa

Alljärgnev tabel on väljavõte ruumide turbevajadusest THA näitel.

Ruum			IT / info	Turbevajadus		
Tähistus	**Liik**	**Asukoht**	**IT-süsteemid / andmekandjad**	**Konfidentsiaalsus**	**Terviklus**	**Käideldavus**
R U.02	Andmekandjaarhiiv	Bonni hoone	Varundusandmekandja (serverite S1–S5 iganädalane varukoopia)	M	M	L
R B.02	Tehnikaruum	Bonni hoone	Kodukeskjaam	L	L	M
R 1.01	Serveriruum	Bonni hoone	S1, N4	M	M	L
R 1.02 – R 1.06	Bürooruumid	Bonni hoone	C1	M	L	L
R 3.11	Kaitsekapp ruumis R 3.11	Bonni hoone	Varundusandmekandja (serverite S1–S5 igapäevane varukoopia)	M	M	L
R E.03	Serveriruum	Berliini hoone	S6, N6, N7	L	M	M
R 2.01 – R 2.40	Bürooruumid	Berliini hoone	C4, mõned faksiaparaatidega	L	L	L

Peatüki 4.3.4 „Ruumide turbevajaduse kindlaksmääramine" rõhuasetus

- Ruumide turbevajaduse tuletamine IT-süsteemide ja rakenduste turbevajadusest
- Sõltuvusseoste, maksimumiprintsiibi ja vajaduse korral ka kumulatsiooniefektiga arvestamine
- Tulemuste ja põhjenduste dokumenteerimine arusaadavuse tagamiseks

4.3.5 Sideühenduste turbevajaduse kindlaksmääramine

Kui rakenduste, IT-süsteemide ja ruumide turbevajadus on kindlaks määratud, tuleb vaadelda võrgustruktuuri turbevajadust. Aluseks võetakse vaadeldava infokoosluse võrguplaan, mille väljatöötamist käsitleb peatükk 4.2.3.

Sideühenduste analüüsimine võimaldab otsustada, millised sideliinid vajavad krüptograafilisi turbemeetmeid, millised liinid peavad olema liiasusega ja milliste ühenduste kaudu võidakse toime panna ründeid nii seest kui ka väljast. Kriitilised on seejuures järgmised sideühendused.

- Välisühendused, mis on seotud ühe või mitme alaga, mis pole organisatsiooni kontrolli all (nt interneti ühenduskaablid või organisatsioonile mittekuuluval territooriumil asuvad kaablid). Siia võivad kuuluda ka traadita sideühendused, sest nende pealtkuulamist organisatsiooniväliselt alalt on väga raske takistada. Välisühenduste puhul on oht, et väline ründaja võib püüda tungida kaitstavasse süsteemi või paigutada sinna arvutiviiruseid või Trooja hobuseid. Lisaks võivad organisatsiooni enda töötajad samade ühenduste kaudu konfidentsiaalset infot välja saata. Suures ohus on ka välisühenduste käideldavus.
- Suure turbevajadusega infot edastavad sideühendused, kusjuures info ranged turbenõuded võivad puudutada nii konfidentsiaalsust, terviklust kui ka käideldavust. Neid ühendusi võidakse ära kasutada tahtlikuks pealtkuulamiseks või manipuleerimiseks. Lisaks võib sellise ühenduse katkemisega kaasneda infokoosluse oluliste osade funktsionaalsuse kadu.
- Sideühendused, mida ei tohi kasutada teatud eriti suure turbevajadusega info edastamiseks. Siinkohal on tegu eelkõige konfidentsiaalse infoga. Näiteks kui võrgu ühenduselemendid on sobimatu või vale konfiguratsiooniga, võib juhtuda, et selliste ühenduste kaudu edastatakse infot, mida tegelikult ei soovitud nende kaudu edastada, ja seeläbi saab seda infot ära kasutada.

Kriitiliste sideühenduste tuvastamiseks võib kasutada järgmisi soovitusi. Esmalt liigitatakse kõik välisühendused kriitiliste ühenduste hulka. Seejärel vaadeldakse kõiki ühendusi, mis puutuvad kokku IT-süsteemidega, millel on kas suur või väga suur turbevajadus. Seejuures tuvastatakse need ühendused, mida kasutatakse suure turbevajadusega info edastamiseks. Seejärel vaadeldakse selliseid

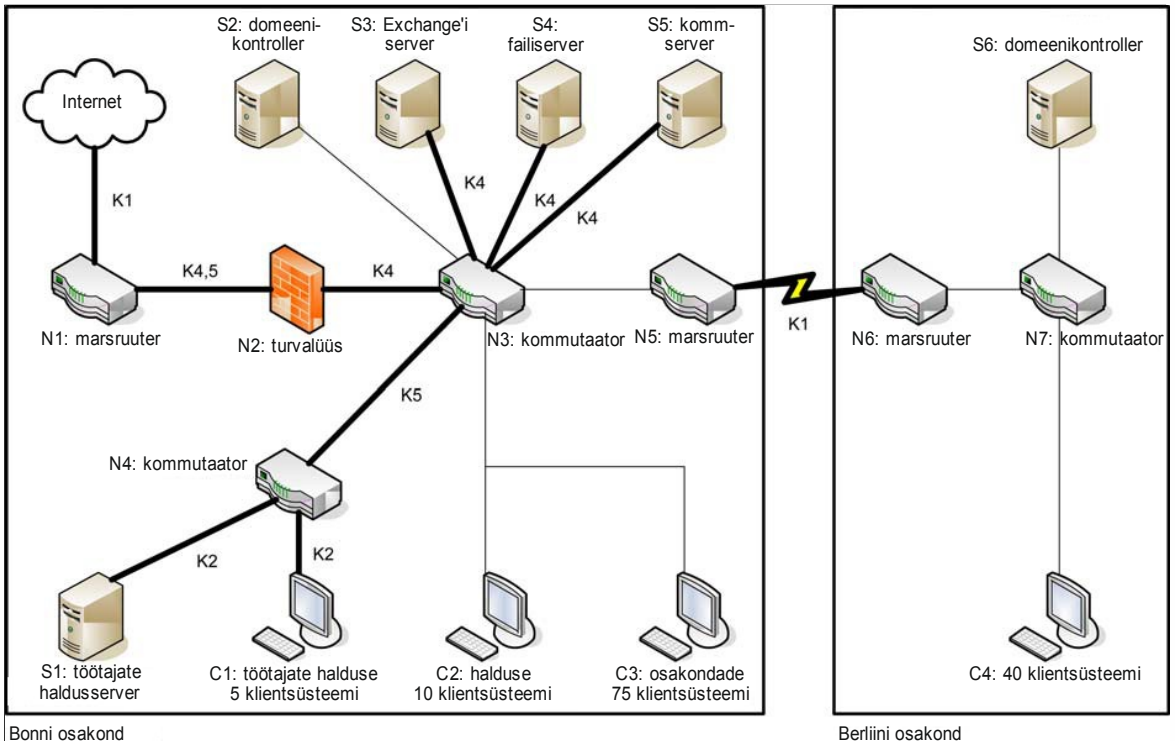
ühendusi, mille kaudu saadetakse neid suure turbevajadusega andmeid edasi. Lõpetuseks tuleb tuvastada need sideühendused, mida ei tohi kasutada sellise info edastamiseks. Selleks tuleb teada järgmist:

- kust kulgeb kaabel?
- kas tegu on välisühendusega?
- kas ühenduse kaudu edastatakse suure turbevajadusega infot ning kas ühenduse turbevajadus tuleneb konfidentsiaalsusest, terviklusest või käideldavusest?
- kas ühenduse kaudu tohib edastada suure turbevajadusega infot?

Otsused selle kohta, millised sideühendused on kriitilised, tuleb dokumenteerida kas tabelina või võrguplaanis graafiliselt esile tõsta.

Näide: töökorralduse ja haldamise amet (THA) – 8. osa

THA näites on kriitilised ühendused järgmised.



Joonis 7. Kriitilisi ühendusi kajastav võrguplaan

Kriitilisi ühendusi tähistavad joonisel paksud jooned. Joonte juures olevate K-tähtede järel paiknevad arvud tähistavad põhjust või põhjuseid, miks ühendus on kriitilise tähtsusega. Asjakohased põhjused on ära toodud järgmises tabelis.

	Kriitilisuse põhjus				
Ühendus	**K 1 välisühendus**	**K 2 M konfidentsiaalsus**	**K 3 Mterviklus**	**K 4 M käideldavus**	**K 5 andmete edastamine keelatud**
N1 – Internet	X				
N5 – N6	X				
S1 – N4		X			
S3 – N3				X	
S4 – N3				X	
S5 – N3				X	
C1 – N4		X			
N1 – N2				X	X
N2 – N3				X	
N4 – N3					X

Selliste andmete kogumisel on eriti oluline, et koostatud ülevaade saaks täielik. Turvet võib tervikuna kahjustada isegi see, kui tähelepanuta jääb kas või **üks** kriitiline ühendus. Välisühenduste hulka liigituvad nt püsiühendused, DSL-ühendused, faksiühendused, traadita ühendused ja ISDN-i liidesed. Paljudes moodsates sülearvutites on modemi- ja raadiosideühenduste liidesed. Multifunktsionaalsetes seadmetes, mida saab kasutada nii skannimiseks, kopeerimiseks kui ka printimiseks, on sageli olemas ka modem ning nendega on võimalik fakse saata. Kui selliseid või seda tüüpi sideühendusi kasutatakse, tuleb need turbeprotsessiga süstemaatiliselt integreerida.

Peatüki 4.3.5 „Sideühenduste turbevajaduse kindlaksmääramine" rõhuasetus

- Andmete kogumine välisühenduste kohta
- Kriitilise info saatmiseks kasutatavate ühenduste tuvastamine
- Selliste ühenduste tuvastamine, mida ei tohi kasutada teatud liiki info edastamiseks
- Kõikide kriitiliste sideühenduste koondamine tabeliks või jooniseks

4.3.6 Tuvastatud turbevajaduse põhjal tehtavad järeldused

Turbevajaduse tuvastamise tulemused on lähtepunktiks turbekontseptsiooni edasisel koostamisel. IT-etalonturbes soovitatud standardsete turbemeetmetega saavutatava turbe jaoks eeldatakse turbevajaduse kategooriate vaatepunktist järgmist.

IT-etalonturbest lähtuva standardsete turbemeetmete mõju	
Turbevajaduse kategooria „L"	Enamasti piisab IT-etalonturbe standardsetest turbemeetmetest.
Turbevajaduse kategooria „M"	IT-etalonturbest lähtuvad standardsed turbemeetmed sobivad lähtepunktiks, kuid ei pruugi olla piisavad. Lisameetmete vajadus tuleb välja selgitada täiendava turbeanalüüsiga.
Turbevajaduse kategooria „H"	IT-etalonturbest lähtuvad standardsed turbemeetmed sobivad lähtepunktiks, kuid enamasti nendest üksi ei piisa. Vajalikud lisameetmed tuleb tuvastada täiendava turbeanalüüsiga.

Suure või väga suure turbevajaduse korral tuleb täiendav turbeanalüüs teha ka siis, kui vaadeldava

infokoosluse objektide kohta kehtib järgnev:

- objektid ei ühildu IT-etalonturbe olemasolevate moodulitega piisavalt (objekte ei õnnestu nende põhjal modelleerida);
- objekte kasutatakse stsenaariumides (keskkondades, rakendustena), mida IT-etalonturve ei käsitle.

Täiendava turbeanalüüsi kohta pakub põhjalikku lisainfot peatükk 4.6.

Erineva turbevajadusega valdkonnad

Turbevajaduse kindlaksmääramisel on sageli näha, et vaadeldud infokoosluse piires on valdkondi, kus töödeldakse infot, mille turbevajadus on suur või koguni väga suur. Isegi kui väga suur turbevajadus kehtib ainult mõnede üksikute esiletõstetud andmete kohta, viivad tihe võrgustruktuur ning IT-süsteemide ja rakenduste vahelised rohked ühendused kiirelt olukorrani, kus tavapärasest suurem turbevajadus kandub maksimumiprintsiibi tõttu üle ka teistesse valdkondadesse.

Seega tuleks erineva turbevajadusega alad riskide ja kulude vähendamiseks lahutada turbetsoonideks. Sellised turbetsoonid võivad lähtuda ruumidest, tehnikast või personalist.

Näited

- Ruumipõhised turbetsoonid. Vältimaks olukorda, kus iga bürooruum peab olema pidevalt lukus või valve all, tuleb arvukate külastajatega aladest eraldada suure turbevajadusega alad. Seega peaksid koosoleku-, koolitusruumid, muud ürituseruumid ning söökla, kus einestavad ka külalised, asuma hoones võimalikult sissepääsu lähedal. Sel juhul saab uksehoidja paremini valvata büroodega hooneosa juurdepääsu. Eriti suure turbevajadusega alad (nt arendusosakonnad) peaksid olema kaitstud muu pääsukontrolli, nt kiipkaardiga.
- Tehnikapõhised turbetsoonid. Selleks, et konfidentsiaalsed andmed ei väljuks LAN-i teatud segmentidest ning et välistada olukord, kus teatud komponentide tõrked või nende vastu suunatud ründed mõjutavad töökindlust, tuleks kohtvõrk jaotada mitmeks alamvõrguks (vt ka IT-etalonturbe kataloogi meedet M 5.77 „Alamvõrkude rajamine").
- Personalipõhised turbetsoonid. Igale isikule tuleb anda ainult nii palju õigusi, kui ta oma ülesannete täitmiseks vajab. Lisaks on mitmeid rolle, mida ei tohiks anda korraga ühele isikule. Nii ei tohiks nt revident töötada samal ajal raamatupidaja ja IT-administraatorina, sest siis ta ei saa ega tohi end ise kontrollida. Pääsuõiguste andmise lihtsustamiseks peaksid isikud, kes täidavad erinevaid ülesandeid, töötama eraldi rühmades või osakondades.

Turbetsoonide loomise otstarbekust tuleks kaaluda alati juba võimalikult vara, nt uute tööprotsesside või rakenduste planeerimisel. Sageli võimaldab see kõikides järgnevates faasides kuni auditini välja töövaeva oluliselt vähendada.

Peatüki 4.3.6 „Tuvastatud turbevajaduse põhjal tehtavad järeldused" rõhuasetus

- Kontrollimine, kas suurema turbevajadusega objektid saab koondata turbetsoonidesse
- Suurema turbevajadusega objektide äramärkimine täiendavaks turbeanalüüsiks

4.4 Meetmete valik ja kohandamine

Pärast struktuurianalüüsi ja turbevajaduse tuvastamist on järgmine keskne ülesanne IT-etalonturbe kataloogide moodulite põhjal infokoosluse modelleerimine. Selle tulemusel koostatakse infokoosluse jaoks IT-etalonturbe mudel, mis koosneb erinevatest ja vajaduse korral ka korduvalt kasutatud moodulitest ning näitab moodulite ja infokoosluse turbe olulisi seoseid.

4.4.1 IT-etalonturbe kataloogid

IT-etalonturbe aktuaalseid katalooge saab alla laadida BSI veebiserverist.

Moodulid

IT-etalonturbe kataloogid sisaldavad mooduleid, kuhu on koondatud erinevate komponentide, metoodikate ja IT-süsteemide ohukirjeldused ning soovitatavad turbemeetmed.

Igas moodulis kirjeldatakse esmalt eeldatavaid ohte, arvestades seejuures nii tüüpiliste kui ka vähem tüüpiliste ehk väga harva esinevate ohtudega. Ohtude käsitlemine on tüüpiliste infotöötluskeskkondade lihtsustatud riskianalüüsi osa, mille põhjal töötas BSI välja valdkondade „Taristud", „Personal", „Töökorraldus", „Riist- ja tarkvara", „Kommunikatsioon" ja „Valmisolek hädaolukorraks" turbemeetmete paketid. Nende eeliseks on see, et tüüpilistel kasutusjuhtudel, kus soovitakse saavutada keskmist turbeastet, ei pea kasutajad tegema keerukaid analüüse. Piisab, kui kataloogidest leitakse vaadeldud rakenduste, IT-süsteemide või tööprotsessidega ühilduvad moodulid ning võetakse järjepidevalt ja täielikult seal soovitatud meetmeid. Ka siis, kui tegu on erikomponentide või eriliste kasutuskeskkondadega, mida IT-etalonturve ei käsitle piisavalt, on IT-etalonturbe kataloogidest siiski palju abi.

Sellisel juhul tuleb teha täiendav turbeanalüüs, mis võib keskenduda komponentide või raamtingimuste eriohtudele.

IT-valdkonnas toimuva uuendustegevuse ja versiooniuuendustega kaasaskäimiseks on IT-etalonturbe kataloogid üles ehitatud moodulite kaupa, mistõttu on neid ka kergem täiendada ja uuendada.

Moodulid on koondatud järgmistesse rühmadesse:

B 1 „Üldkomponendid"

B 2 „Infrastruktuur"

B 3 „IT-süsteemid"

B 4 „Võrgud"

B 5 „Rakendused"

Ohukataloogid

See valdkond sisaldab moodulites nimetatud ohtude põhjalikke kirjeldusi. Ohukataloogid on jagatud viieks osaks:

G 1 „Vääramatu jõud"

G 2 „Organisatsioonilised puudused"

G 3 „Inimvead"

G 4 „Tehnilised rikked"

G 5 „Ründed"

Meetmekataloogid

Selles osas kirjeldatakse põhjalikult IT-etalonturbe kataloogide moodulites nimetatud turbemeetmeid. Meetmekataloogid on jaotatud kuueks:

M 1 „Infrastruktuur"

M 2 „Organisatsioon"

M 3 „Personal"

M 4 „Riist- ja tarkvara"

M 5 „Kommunikatsioon"

M 6 „Valmisolek hädaolukorraks"

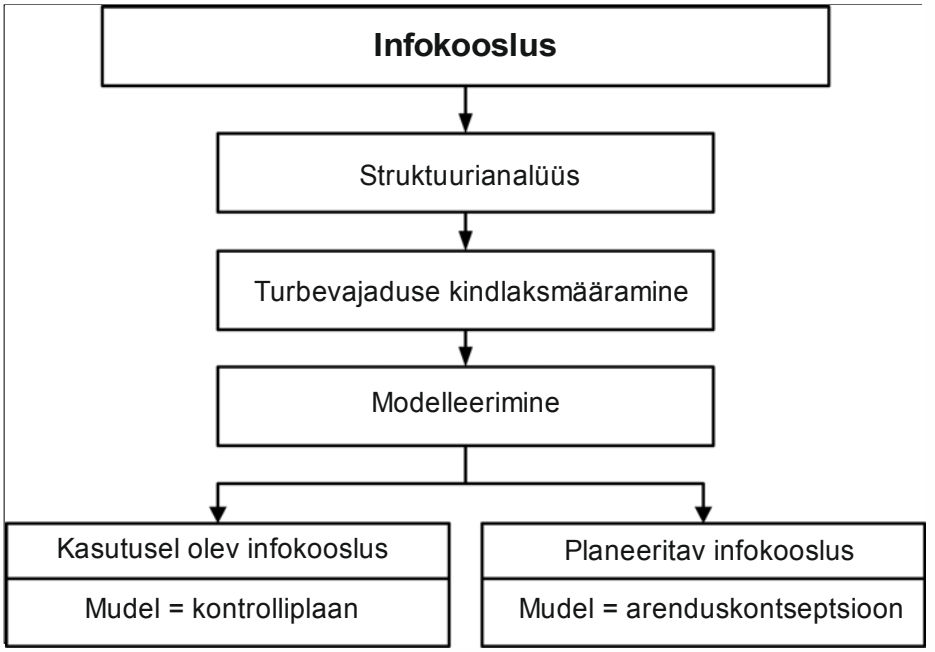
4.4.2 Infokoosluse modelleerimine

IT-etalonturbe mudeli loomisel ei ole vahet, kas vaadeldava infokoosluse IT-süsteemid on juba

kasutusel või on tegu alles planeeritava infokooslusega. Mudelit saab kasutada erinevalt.

- Olemasoleva infokoosluse IT-etalonturbe mudeli puhul on tegu olukorraga, kus mudel määrab kasutatud moodulite abil kindlaks olulised standardsed turbemeetmed. Seda saab kasutada **kontrolliplaanina**, et võrrelda soovitud olukorda tegeliku olukorraga.
- Seevastu alles planeeritava infokoosluse IT-etalonturbe mudelit kasutatakse pigem **arenduskontseptsioonina**. See kirjeldab valitud moodulite abil, milliseid standardseid turbemeetmeid tuleb infokoosluse loomisel võtta.

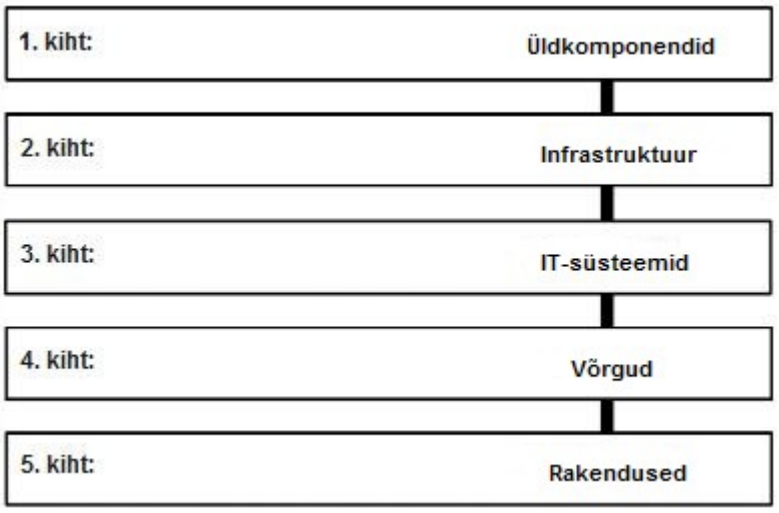
Järgnev joonis selgitab modelleerimise järjekorda turbeprotsessis ja selle võimalikke tulemusi.



Joonis 8. IT-etalonturbest lähtuva modelleerimise tulemus

Kasutusel oleva infokoosluse puhul leidub kindlasti ka komponente, mida alles planeeritakse. Sellisel juhul on tulemuseks IT-etalonturbe mudel, milles on olemas nii kontrolliplaan kui ka arenduskontseptsiooni osad. Kõik kontrolliplaanis ja arenduskontseptsioonis ette nähtud turbemeetmed moodustavad turbekontseptsiooni koostamise aluse. Juba võetud turbemeetmete kõrval tuleb siinkohal arvestada ka sellistega, mis liigitati soovitud ja tegeliku olukorra võrdlemisel ebapiisavaks või puuduvaks või mis on vajalikud infokoosluse planeeritavate komponentide jaoks.

Kuna infokooslus on enamasti keerulise ülesehitusega, võib IT-etalonturbe kataloogi moodulitel põhinevaks modelleerimiseks turbeaspektid teemade järgi rühmadeks jaotada.



Joonis 9. IT-etalonturbe mudeli kihid

Infokoosluse turbeaspektid kuuluvad eri kihtidesse järgmiste põhimõtete alusel.

- 1. kiht käsitleb üldisi turbeaspekte, mis kehtivad kogu infokooslusele või vähemalt suurele osale sellest. See puudutab eriti just üldiseid kontseptsioone ja nendest tuletatud reegleid. 1. kihi tüüpilised moodulid on muu hulgas „Turbehaldus", „Töökorraldus", „Andmevarunduspoliitika" ja „Viirusetõrjekontseptsioon".
- 2. kiht hõlmab ehitustehnilisi olusid ja koondab taristute turbeaspekte. See puudutab esmajoones mooduleid „Hooned", „Serveriruum", „Kaitsekapp" ja „Kodutöökoht".
- 3. kiht hõlmab infokoosluse erinevaid IT-süsteeme, mida võidakse vaadelda ka rühmadena. Käsitletakse nii klientsüsteemide, serverite kui ka autonoomsete süsteemide turbeaspekte. Sellesse kihti kuuluvad nt moodulid „Kodukeskjaam", „Sülearvuti" ja „Windows XP klientsüsteem".
- 4. kiht hõlmab võrkude aspekte, mis pole seotud kindlate IT-süsteemidega, vaid kõikide võrguühenduste ja kommunikatsiooniga. Selle alla kuuluvad nt moodulid „Heterogeensed võrgud", „WLAN" ja „Kaugpöördus".
- 5. kiht hõlmab infokoosluses kasutatavaid rakendusi. Selles kihis saab modelleerimiseks muu hulgas kasutada mooduleid „E-post", „Veebiserver", „Faksiserver" ja „Andmebaasid".

Kihtidesse jaotamisel on järgmised eelised.

- Aspektide sorteerimine ja koondamine rühmadesse vähendab infoturbe keerukust.
- Hierarhias kõrgemal asetsevate aspektide ja taristute üldiste probleemide vaatlemine IT-süsteemidest eraldi võimaldab vältida kordusi, sest asjakohased teemad töötatakse läbi vaid üks kord ja tervikuna, mitte iga IT-süsteemi puhul uuesti.
- Kihid on valitud selliselt, et rühmadesse saab koondada ka vaadeldud aspektide vastutusalad. Esmajoones puudutab 1. kiht info turvalise käsitsemise põhimõtteid, 2. kiht tehnikat, 3. kiht administraatoreid ja IT kasutajaid, 4. kiht võrgu- ja süsteemiadministraatoreid ning 4. kiht rakenduste eest vastutavaid isikuid ja käitajaid.
- Turbeaspektide jaotamine kihtidesse võimaldab nendest tulenevate turbekontseptsioonide üksikuid aspekte kergemini värskendada ja täiendada, ilma et see puudutaks olulisel määral teisi kihte.

IT-etalonturbest lähtuval modelleerimisel tuleb seega otsustada, kas ja kuidas iga kihi mooduleid kasutada. Olenevalt vaadeldud moodulitest võivad infokoosluse modelleerimise sihtobjektid olla erinevad: üksikud tööprotsessid või komponendid, komponentide rühmad, hooned, asukohad,

organisatsiooni allüksused jne.

IT-etalonturbe mudel ehk moodulite ja sihtobjektide seosed tuleb dokumenteerida tabelina. See tabel peab sisaldama järgmisi tulpasid:

- mooduli number ja pealkiri;
- sihtobjekt või -rühm: kasutada võib nt komponendi/rühma ID-numbrit või hoone/organisatsiooni allüksuse nime;
- kontaktisik(ud): see tulp jääb esialgu tühjaks. Kontaktisikut ei määrata modelleerimise käigus, vaid alles esmase turbekontrolli ajal tehtava soovitud ja tegeliku olukorra võrdluse raames;
- lisainfo: sellesse tulpa saab kirja panna ääremärkused ja modelleerimise põhjused.

Näide: töökorralduse ja haldamise amet (THA) – 9. osa

Järgnev tabel on väljavõte fiktiivse asutuse THA modelleerimise näitest.

Nr	Mooduli pealkiri	Sihtobjekt/-rühm	Kontakt-isik(ud)	Lisainfo
B 1.1	Organisatsioon	Bonni peakorter		Töökorraldust käsitlevat moodulit tuleb vaadelda Bonni ja Berliini puhul eraldi, sest Berliinis kehtib teistsugune töökorraldus.
B 1.1	Organisatsioon	Berliini harukontor		
B 1.2	Personal	THA tervikuna		THA personali hallatakse tsentraalselt Bonnis.
B 2.5	Andmekandja-arhiiv	R U.02 (Bonn)		Selles ruumis hoitakse varukoopiate andmekandjaid.
B 3.203	Sülearvuti	C5		Bonni/Berliini sülearvutid koondatakse ühte rühma.
B 3.203	Sülearvuti	C6		
B 5.4	Veebiserver	S5		S5 on intraneti server.
B 5.7	Andmebaasid	S5		Serveris S5 käitatakse andmebaasi.

Infokoosluse modelleerimise detailse kirjelduse leiate IT-etalonturbe kataloogide peatükist „Kihimudel ja modelleerimine”. Eriti rõhutatakse seal lisatingimusi, mis näitavad, millal ja milliste sihtobjektide puhul on mõistlik konkreetset moodulit kasutada.

4.4.3 Meetmete kohandamine

Modelleerimise käigus väljavalitud IT-etalonturbe kataloogide mooduleid tuleb rakendada vaadeldava infokoosluse objektide peal. Moodulites soovitatud turbemeetmed on tavaliselt nende komponentide jaoks sobivad ja piisavad.

Turbekontseptsiooni koostamiseks või auditiks tuleb need meetmed üle vaadata. IT-etalonturbe meetmed on sõnastatud selliselt, et nad sobivad võimalikult paljudele keskkondadele, ühtlasi on kirjeldused ka piisavalt põhjalikud, et neid praktikas kasutada.

Sellele vaatamata tuleb soovitatud meetmed kohandada sobivaks organisatsiooni reaalsete oludega. Näiteks võib osutuda vajalikuks:

- meetmeid täpsustada, nt lisada tehnilisi üksikasju;
- meetmeid kohandada organisatsiooni keelekasutusega, nt anda rollidele teised nimetused;
- eemaldada meetmetest vaadeldava valdkonna jaoks ebaolulised soovitused.

Meetmetekstide rakendamisel tuleb alati lähtuda teksti mõttest. Kõik muudatused, mis kalduvad kõrvale IT-etalonturbe kataloogide soovitustest, tuleb dokumenteerida, et need muudatused oleksid ka hiljem arusaadavad.

Selleks, et IT-etalonturbe tekste oleks lihtsam kohandada, on kõik tekstid, moodulid, ohukirjeldused, meetmed, tabelid ja abivahendid ka elektrooniliselt kättesaadavad. See võimaldab neid tekste turbekontseptsiooni koostamisel ja meetmete elluviimisel paremini ära kasutada.

Meetmete analüüsimisel võib ka selguda, et mõned IT-etalonturbes soovitatud meetmed pole konkreetsete raamtingimuste tõttu vajalikud. Meetmed võivad osutuda liigseks nt juhul, kui teatud ohtudele reageeritakse juba teiste meetmetega või kui meetmetes antud soovitused pole olulised (nt kui asjakohaseid teenuseid pole aktiveeritud). Täiendavad või tühistatud turbemeetmed tuleks turbekontseptsioonis dokumenteerida. See kergendab ka esmase turbekontrolli tegemist.

Meetmete valimisel ja kohandamisel tuleb jälgida, et need oleksid alati sobivad. Sobiv tähendab järgmist:

- toime (efektiivsus): meetmed peavad tõhusalt kaitsma võimalike ohtude eest ehk vastama turbevajadusele;
- sobivus: meetmed peavad olema võimalikult praktilised, st meetmete võtmine ei tohi takistada juba väljakujunenud tööprotsesse ning need ei tohi õõnestada teiste turbemeetmete kaitsvat toimet;
- praktilisus: meetmed peavad olema kergesti arusaadavad, lihtsasti kasutatavad ja minimaalselt veaohtlikud;
- vastuvõetavus: meetmed ei tohi töötajates tekitada vastuseisu, samuti kedagi diskrimineerida ega negatiivselt mõjutada;
- majanduslik tasuvus: kasutatud vahendid peavad andma võimalikult hea tulemuse. Seega peavad meetmed ühest küljest riske võimalikult hästi minimeerima ning teisest küljest peab meetmetega kaasnevate kulude ja kaitstavate väärtuste vahel valitsema hea tasakaal.

Peatüki 4.4 „Meetmete valik ja kohandamine" rõhuasetus

- IT-etalonturbe kataloogide peatüki „Kihimudel ja modelleerimine" süstemaatiline läbitöötamine
- Iga IT-etalonturbe kataloogide mooduli ja vaadeldud infokoosluse sihtobjekti ühilduvuse tuvastamine
- Moodulite seostamine sihtobjektidega (IT-etalonturbe mudel) ja kontaktisikute dokumenteerimine
- Modelleerimata jäänud objektide äramärkimine täiendavaks turbeanalüüsiks
- Sobivate moodulite meetmetekstide hoolikas läbilugemine ja vajaduse korral nende kohandamine

4.5 Esmane turbekontroll

Edaspidiste tööde puhul eeldatakse, et vaadeldava infokoosluse jaoks on järgmised IT-etalonturbel põhineva turbekontseptsiooni osad juba valmis.

Infokoosluse struktuurianalüüsiga on olemasolevast infotehnoloogiast koostatud ülevaade, mis näitab ära IT kasutuskohad ja IT-d vajavad rakendused. Lisaks on struktuurianalüüsiga tuvastatud rakenduste, IT-süsteemide, kasutatud ruumide ja sideühenduste turbevajadus. Nende andmete põhjal on tehtud IT-etalonturbel põhinev infokoosluse modelleerimine. Modelleerimise tulemusel on teada vaadeldava infokoosluse ja IT-etalonturbe moodulite seosed.

Selles peatükis kirjeldatakse esmast turbekontrolli. Esmane turbekontroll koosneb kolmest sammust. Esimene samm hõlmab töökorralduslikke ettevalmistusi, eriti aga kontaktisikute valimist soovitud ja

tegeliku olukorra võrdluse jaoks. Teise sammuna võrreldakse intervjuude ja pisteliste kontrollidega soovitud ja tegelikku olukorda. Viimase sammu moodustab soovitud ja tegeliku olukorra võrdlemisel põhinevate tulemuste ja põhjenduste dokumenteerimine.

Järgnevalt kirjeldatakse esmase turbekontrolli samme lähemalt.

4.5.1 Esmase turbekontrolli töökorralduslikud ettevalmistused

Soovitud ja tegeliku olukorra võrdluse õnnestumiseks tuleb teha mõningaid ettevalmistusi. Esmalt tuleb läbi vaadata kõik organisatsioonisisesed turbeprotsesse reguleerivad dokumendid, nt reeglid, töö- ja turbejuhised, käsiraamatud ning informeerivad käitumisjuhised. Nendest dokumentidest võib olla abi võetud meetmete tuvastamisel, eriti kui on tarvis välja selgitada, milline on praegune töökorraldus. Lisaks tuleb kindlaks teha, kes vastutab nende dokumentide sisu eest, et hiljem oleks võimalik õige kontaktisik määrata.

Järgmisena tuleb kindlaks määrata, kas ja millises mahus on meetmete võtmisel vaja kasutada välist abi. See võib olla vajalik nt väliste arvutuskeskuste, ülimuslike ametiasutuste, väljasttellitud tööprotsesside või IT-töö eest hoolt kandvate firmade, aga ka taristuid puudutavate meetmete eest vastutavate ehitusametite korral.

Soovitud ja tegeliku olukorra võrdluse oluline samm on sobivate intervjueeritavate leidmine. Selleks tuleks esmalt igale moodulile, mida on kasutatud vaadeldava infokoosluse modelleerimiseks, määrata peamine kontaktisik.

- 1. kihi „Üldkomponendid” moodulite puhul saab sobiva kontaktisiku leida üldjuhul otse moodulis käsitletava teema järgi. Näiteks tuleks mooduli B 1.2 „Personal” kontaktisikuks valida personaliosakonna töötaja. Kontseptsioonimoodulite, nt mooduli B 1.4 „Andmevarunduspoliitika” puhul saab tavaliselt kasutada mõnda töötajat, kes vastutab asjakohase dokumentatsiooni täiendamise eest. Küsitleda võib ka töötajat, kelle ülesannete hulka kuulub vaadeldava valdkonna reeglite täiendamine.
- 2. kihi „Infrastruktuur” puhul tuleks sobiva kontaktisiku valik kooskõlastada organisatsiooni sisekommunikatsiooni või tehnikaosakonnaga. Olenevalt vaadeldava institutsiooni suurusest on võimalik, et hoonete ja kaitsekappide eest vastutavad erinevad kontaktisikud. Väiksemates institutsioonides valdab seda infot sageli nt majajuhataja. Taristute puhul tuleb arvestada ka nende osadega, mis jäävad institutsiooni mõjupiirkonnast välja. See puudutab eriti just suuremaid institutsioone.
- 3. kihi „IT-süsteemid” ja 4. kihi „Võrgud” moodulid käsitlevad rohkem turbemeetmete tehnilisi aspekte. Seega sobib üldjuhul peamiseks kontaktisikuks modelleerimisega seotud moodulile vastavate komponentide või komponentide rühma administraator.
- 5. kihi „Rakendused” moodulite peamisteks kontaktisikuteks tuleks valida rakenduste nõustajad või rakenduste eest vastutavad isikud.

Peamine kontaktisik ei oska sageli vastata kõikidele moodulit puudutavatele küsimustele. Seega tuleks intervjueerida ka ühte või mitut lisaisikut. Seda, milliseid töötajaid veel küsitleda, saab otsustada iga meetme kirjelduse alguses olevate sissekannete „Algatamise eest vastutavad:” ja „Rakendamise eest vastutavad:” järgi.

Süsteemide eest vastutavate isikute, administraatorite ja muude kontaktisikute intervjueerimiseks tuleks koostada ajakava. Eriti oluline on tähtaegade kooskõlastamine siis, kui tuleb võtta ühendust isikutega organisatsiooni teistest allüksustest või teistest institutsioonidest. Lisaks oleks mõistlik juba võimalikult vara kindlaks määrata ka alternatiivsed kohtumisajad.

Olenevalt projektirühma suurusest tuleks intervjuudeks moodustada meeskonnad ja ülesanded nende vahel ära jaotada. Praktikas on end hästi tõestanud kaheliikmelised rühmad. Nii saab üks inimene küsimusi esitada ning teine vastuseid ja lisainfot üles märkida.

Peatüki 4.5.1 „Esmase turbekontrolli töökorralduslikud ettevalmistused” rõhuasetus

- Organisatsioonisiseseid reegleid puudutava dokumentatsiooni uurimine ja dokumentatsiooni eest vastutavate isikute väljaselgitamine
- Organisatsioonivälise üksuste küsitlemisvajaduse kindlakstegemine
- Kontaktisiku määramine igale modelleerimiseks kasutatud moodulile
- Intervjuude ajakava koostamine
- Intervjuude tarbeks meeskonna moodustamine

4.5.2 Soovitud ja tegeliku olukorra võrdlus

Kui kõik vajalikud eeltööd on tehtud, võib alata tegelik võrdlus, mille puhul tuleb võtta arvesse ka eelmääratud tähtaegu. Võrdluse käigus uuritakse järgemööda intervjueeritavate isikute vastutusalasse kuuluvate moodulite meetmeid.

Iga meetme võtmist kajastav vastus saab olla üks alljärgnevatest.

Ebaoluline	–	Soovitatud meetmeid ei ole tarvis sellisel kujul võtta, sest ohu vältimise eest kannavad juba hoolt muud tõhusamad meetmed (nt meetmed, mis ei kajastu IT-etalonturbes, kuid mis on sama tõhusad) või on soovitatud meetmed ebaolulised (nt põhjusel, et asjakohaseid teenuseid ei ole sisse lülitatud).
Jah	–	Kõik meetmed on juba täielikult, tõhusalt ja sobivalt võetud.
Osaliselt	–	Mõned soovitused on ellu viidud, teised veel mitte või ainult osaliselt.
Ei	–	Meetmes märgitud soovitused on suuremalt jaolt veel ellu viimata.

Intervjuude ajal ei tasuks meetmete teksti ette lugeda, sest see ei soodusta kahekõnet. Seepärast peab intervjueerija ilmtingimata tundma mooduli sisu ja ta võiks abimaterjalina kasutada märksõnadega kontrollinimekirju. Siiski tasuks hoida käepärast ka meetmete täistekstid, et kahtluse korral arusaamatusi vältida. Intervjueerimise ajal ei tasu vastuseid otse arvutisse trükkida, sest see juhib kõikide asjaosaliste tähelepanu kõrvale ja segab suhtlemist.

Intervjuu alustamisel tuleb luua pingevaba ja produktiivne õhkkond, nt võib sissejuhatuseks tutvustada esmase turbekontrolli eesmärki. Jätkata tasuks meetmepealkirjade loetlemise ja meetme lühikirjeldusega. Monoloogi pidamise asemel tasuks anda vastaspoolele võimalus kirjeldada meetme juba elluviidud osi ja seejärel täpsustada veel ebaselgeid punkte.

Küsitlemise teemavaldkond peab keskenduma ennekõike standardsele turbeastmele, st sellest suurema turbevajadusega rakenduste aspekte tuleks vaadelda alles pärast esmase turbekontrolli lõpetamist. Kui intervjuu käigus tekib vajadus ütlusi üle kontrollida, tasub seda teha kohe ja koostöös intervjueeritavaga. Näiteks võiks asjakohased reeglid ja kontseptsioonid üheskoos pisteliselt läbi vaadata, taristute kohta küsides tasuks kontaktisikuga minna kontrollkäigule ning IT-süsteemide seadistusi käsitledes tuleks minna mõne väljavalitud klientsüsteemi või serveri juurde ja seadistus üle kontrollida.

Peatüki 4.5.2 „Soovitud ja tegeliku olukorra võrdlus" rõhuasetus

- Valdkonnaga sobiva kontrollnimekirja koostamine
- Esmase turbekontrolli eesmärkide selgitamine intervjueeritavatele
- Meetmete võtmise seisundi väljaselgitamine
- Vastuste kinnitamine objektide pistelise kontrolliga

• Küsitletute teavitamine tulemustest

4.5.3 Tulemuste dokumenteerimine

Esmase turbekontrolli tulemused tuleb dokumenteerida selliselt, et need oleksid kõikidele asjaosalistele mõistetavad ja et neid saaks kasutada puudulikult võetud meetmete tõhustamiseks. Selleks, et lihtsustada esmase turbekontrolli tulemuste dokumenteerimist on kaks abivahendit.

Üks nendest on ISKE tööriist. See tarkvara toetab kogu IT-etalonturbe metoodika rakendamist, st alates algandmete kogumisest, turbevajaduse tuvastamisest, täiendavast turbe- ja riskianalüüsist ning soovitud ja tegeliku olukorra võrdlusest (esmane turbekontroll) kuni meetmete rakendamiseni välja. Selle tarkvaraga on mugav tulemusi analüüsida ja ümber töötada, nt saab otsida sissekandeid, luua raporteid, koostada kuluhinnanguid ja kasutada statistikafunktsioone.

Lisaks saab IT-etalonturbe abivahenditena kasutada blankette. IT-etalonturbe iga mooduli kohta on olemas Wordi vormingus fail, mille tabelisse saab kokku koguda mooduli iga meetme soovitud ja tegeliku olukorra võrdluse tulemused.

ISKE tööriista väljadele või blankettidele tuleks esmalt märkida järgmine info:

- modelleerimisel mooduliga seostatud komponentide või komponentide rühma numbrid ja nimetused;
- komponentide või komponentide rühma asukohad;
- andmete kogumise kuupäev ja koguja nimi;
- küsitletud kontaktisikud.

Soovitud ja tegeliku olukorra võrdluse lõpptulemused kogutakse blanketil olevasse tabelisse. Seejuures tuleb mooduli iga meetme puhul täita väljad järgmiselt.

- Rakendatavuse aste (ebaoluline / jah / osaliselt / ei)

  Siia pannakse kirja intervjuu käigus meetme kohta tuvastatud rakendatavuse aste.

- Rakendamise lõppkuupäev

  See väli jääb esmase turbekontrolli ajal tavaliselt täitmata. See täidetakse rakendamise planeerimisel, kui määratakse kindlaks meetme täieliku rakendamise lõppkuupäev.

- Vastutav isik

  Kui soovitud ja tegeliku olukorra võrdluse käigus selgub, kes töötajatest vastutab seni puudulikult võetud meetme täieliku rakendamise eest, võib tema nime siia juba kirja panna. Kui vastutav isik pole veel teada, tuleb see väli tühjaks jätta. Sellisel juhul määratakse vastutav isik ja pannakse ta kirja hilisema rakendamisplaani koostamise ajal.

- Märkused / meetmete võtmata jätmise põhjendused

  Meetmete puhul, mille võtmine ei tundu vajalik, tuleb siia kirjutada põhjendus või asendusmeede. Seevastu nende meetmete puhul, mida ei ole veel võetud või mis on võetud ainult osaliselt, tuleb kirja panna, milliseid meetmes kajastuvaid soovitusi pole seni veel arvesse võetud. Sellele andmeväljale tuleb kirjutada ka kogu lisainfo, millest on kasu puuduste kõrvaldamisel või millega tuleb meetme puhul arvestada.

- Kuluhinnang

  Meetmete puhul, mida ei ole veel võetud või mis on võetud ainult osaliselt, saab siia kirja panna, kui suur on puuduste kõrvaldamise raha- ja ajakulu.

Peatüki 4.5.3 „Tulemuste dokumenteerimine" rõhuasetus
• Iga sihtobjekti põhiinfo kirjapanemine utiliiti, andmebaasi või blanketile

- Esmase turbekontrolli ja meetmete rakendamise kontrolli tulemuste kirjapanemine
- Tühjade väljade jätmine, et oleks võimalik lisada sinna infot rakendamise planeerimise kohta

4.6 Täiendav turbeanalüüs

IT-etalonturbe standardsed turbemeetmed sobivad enamasti kõikidele tüüpilistele tööprotsessidele, rakendustele ja IT-süsteemidele, mille turbevajadus vastab kategooriale „L". Sellele vaatamata esineb ka juhte, kus IT-etalonturbe meetmeid tuleb riskianalüüsi põhjal täiendada.

4.6.1 IT-etalonturbe metoodika kaheastmeline käsitlus

Parema tõhususe saavutamiseks käsitletakse IT-etalonturvet kahes astmes. Esimeses astmes määratakse kindlaks infokooslusse kuuluvate objektide turbevajadus. Modelleerimise abil selgitatakse iga sihtobjekti puhul välja selle tüüpilised ohud ja asjakohased standardsed turbemeetmed. Seejuures tuleb alati üldistada ning lähtuda tavapärasest kasutusstsenaariumist ja turbevajadusest. Sel moel saab infokoosluse turbeastet IT-etalonturbe kataloogide moodulite abil kiirelt ja tõhusalt suurendada. Kokkuvõtvalt võib öelda, et esimene aste pakub turbemeetmeid, mis võimaldavad vältida praktikas väga sageli esinevaid elementaarseid ohte. IT-etalonturbe esimeses astmes analüüsitakse seega juba üpris põhjalikult kõikvõimalikke riske.

Seevastu teises astmes püütakse selgitada välja, kas infokoosluse puhul on oluline arvestada ka muude, st tavapärasest teistsuguste riskidega.

4.6.2 Täiendava turbeanalüüsi metoodika

Täiendav turbeanalüüs tuleb teha kõikide infokoosluse sihtobjektide puhul, mis vastavad järgmistele tingimustele:

- kolmest põhiväärtusest (konfidentsiaalsus, terviklus või käideldavus) on vähemalt ühe turbevajadus kas M või H;
- sihtobjekt ei ühildu IT-etalonturbe olemasolevate moodulitega piisavalt (seda ei õnnestu nende põhjal modelleerida);
- sihtobjekte kasutatakse stsenaariumides (nt keskkondades või koos rakendustega), mida IT-etalonturve ei käsitle.

Eesmärk on teha iga sihtobjekti kohta otsus, kas edasine riskianalüüs on vajalik. Täiendavat turbeanalüüsi vajavate rakenduste või IT-süsteemide näideteks on finantsteenusepakkuja internetipanganduse teenus ja eriliste reaalaja-operatsioonisüsteemidega IT-lahendused.

Töövaeva vähendamiseks tuleks sihtobjektid täiendava turbeanalüüsi raames koondada sobivatesse rühmadesse. See kehtib näiteks ka kriitiliste sideühenduste kohta. Sellised ühendused saab sageli koondada kriitilisteks võrgusektsioonideks, alamvõrkudeks, sideharudeks jms.

Haldusraportis tuleb iga sihtobjekti või sihtobjektide rühma puhul, kui neile kehtib vähemalt üks eelmainitud tingimus, pisteliselt põhjendada, kas edasine riskianalüüs on vajalik või mitte. Sihtobjektid, mille puhul täiendav riskianalüüs on vajalik, koondatakse riskivaldkondadesse. Eesmärk on näidata, millised valdkonnad vajavad täiendavat riskianalüüsi.

Täiendava turbeanalüüsi raames tehtavate otsuste aluseks on institutsiooni üldeesmärgid, riskihalduse põhimõtted ja võib-olla ka ressursside planeerimine. Haldusraport saadetakse kinnitamiseks institutsiooni juhtkonnale. Seega vastutab juhtkond.

Näide: töökorralduse ja haldamise amet (THA) – 10. osa

Turbevajaduse tuvastamise käigus selgunud andmete põhjal ja eriliste kasutustingimuste tõttu vajab THA mitmeid täiendavaid turbeanalüüse. Järgnev tabel näitab tulemuste väljavõtet.

Sihtobjekt	Täiendav turbeanalüüs, haldusraporti väljavõtted
Domeenikontroller S2	Kuna domeenikontroller S2 täidab olulisi tsentraalseid haldusülesandeid, kehtivad sellele ranged terviklusnõuded. Süsteemil on juba olemas ka mõned sisemised turbemehhanismid, mis kaitsevad seda tahtlike ja juhuslike manipulatsioonide eest. Kaaluti mõningate tehniliste lisameetmete võtmist, kuid nendest loobuti, sest need ei ühildunud teiste kasutatud toodetega piisavalt hästi. Seepärast soovitab IT-osakond hoolitseda süsteemi S2 suurema turbevajaduse eest organisatoorsete meetmetega, nt tuleks IT revisjoniosakonnas teha sagedasi ja regulaarseid auditeid. Süsteemi S2 edasine riskianalüüs pole praegusel juhul vajalik.
Kriitilised sideühendused N1-N2/internet	THA internetiühendusest tulenev oht on vaadeldud aja jooksul pidevalt kasvanud. Eriti saab esile tõsta rämpsposti ja pahavaraga seotud probleeme. IT-osakond soovitab seetõttu teha internetiühenduse riskianalüüs.
Kriitilised sideühendused N3-S3/S4/S5/N2	Mainitud sideühendustele kehtivad tavapärasest rangemad käideldavusnõuded. Järgmiseks kvartaliks planeeritud ja kinnitatud tehnilise ümberstruktureerimise raames eemaldatakse süsteemist tsentraalne kommutaator N3. Uus struktuur on liiasusega, et vältida üheainsa rikkepunkti (Single Point of Failure) ohtu. Kuna mainitud kriitiliste sideühenduste puhul on seega tegu ajutiste lahendustega, soovitab IT-osakond nende ühenduste riskianalüüsist esialgu loobuda.
Serveriruum R E.03 Berliinis	Berliinis ruumis R E.03 käitatavale tehnikale kehtivad eriti ranged käideldavusnõuded. Sellele serveriruumile on tehtud riskianalüüs, kuid see on vananenud. Seetõttu soovitab IT-osakond teha Berliini ruumile R E.03 uus riskianalüüs.

Täielik haldusraport esitatakse juhtkonnale kinnitamiseks.

Teadmiseks: tabelis loetletud IT-osakonna soovitused THA-le on fiktiivsed näited, mitte konkreetsed soovitused sellisteks kasutusjuhtudeks.

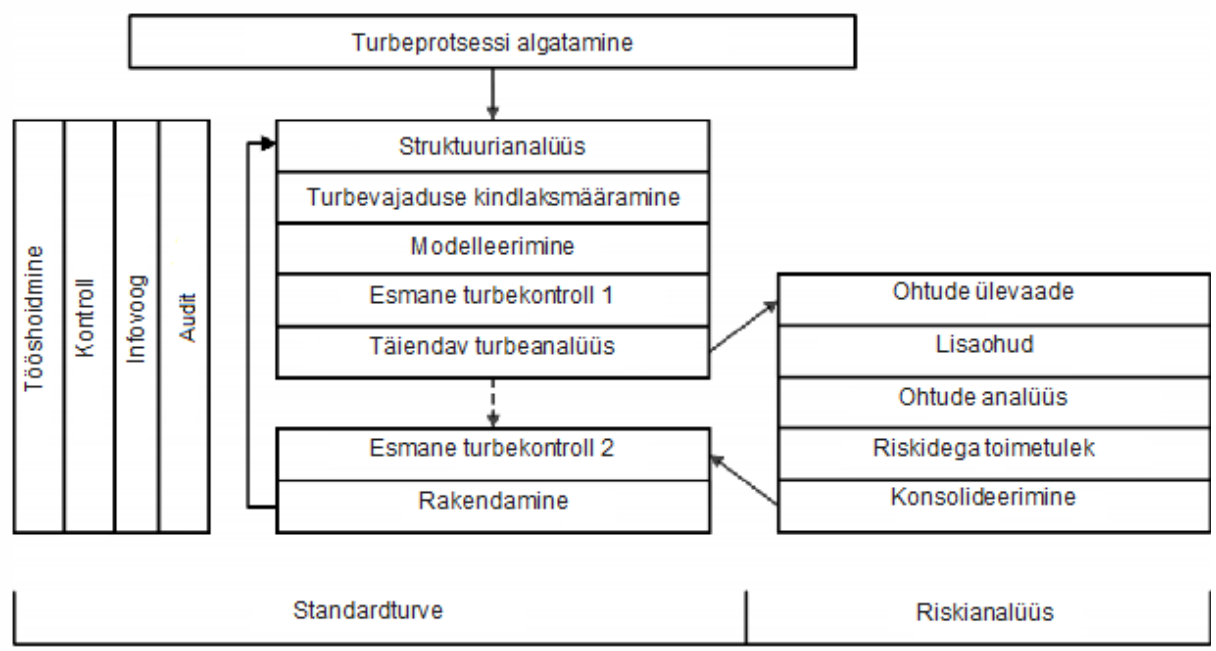
4.6.3 IT-etalonturbel põhinev riskianalüüs

Infoturbe raames tehtava riskianalüüsi ülesanne on tuvastada infokooslust ähvardavad ohud ja hinnata nendest tulenevaid riske. Eesmärk on riskide vähendamine sobivate vastumeetmetega, jääkriskide teadvustamine ja seeläbi koguriski süstemaatiline vähendamine.

IT-etalonturbe metoodikat rakendades peab juhtkond lähtuma täiendava turbeanalüüsi haldusraportitest ja otsustama, millistele objektidele tuleb teha riskianalüüs. Riskianalüüsiga seotud kulud piirduvad seega valdkondadega, mille puhul on selline tegevus otstarbekohane ja kasutoov.

Täiendava riskianalüüsi raames vastu võetavate otsuste jaoks soovitab rakendada standardit BSI 100-3 „IT-etalonturbel põhinev riskianalüüs”.

Seal kirjeldatud metoodikat saab IT-etalonturbe protsessiga integreerida järgmisel viisil.



Joonis 10. Riskianalüüsi integreerimine IT-etalonturbe protsessiga

Esikohal on küsimus: millistele infokooslust ähvardavatele ohtudele on IT-etalonturbe standardsete turbemeetmete võtmisega reageeritud ebapiisavalt või üldse reageerimata jäetud?

Sellele küsimusele vastamiseks soovitatakse standardis „IT-etalonturbel põhinev riskianalüüs" järgmisi töösamme.

- Ülevaate koostamine ohtudest

  Selles esimeses töösammus koostatakse iga analüüsitava sihtobjekti jaoks IT-etalonturvet ähvardavate oluliste ohtude loetelu.

- Lisaohtude tuvastamine

  IT-etalonturbe kataloogidest teada saadud ohtude loetelu täiendatakse lisaohtudega, mis tulenevad vastavatest kasutusstsenaariumidest. Seda tehakse ühise ajurünnakuga.

- Ohtude analüüs

  Iga sihtobjekti ja iga ohu puhul kontrollitakse, kas senised turbemeetmed pakuvad piisavat kaitset. Kontrollikriteeriumideks on seejuures täielikkus, mehhanismi tugevus ja usaldusväärsus.

- Riskikäsitluse meetmete valik

  Juhtkond peab kehtestama suunised, kuidas riskidega ümber käia. Asjakohased soovitused esitavad tavaliselt infoturbehalduse eest vastutavad töötajad. Riskidega toimetulekuks on järgmised võimalused:

  - riske saab turbemeetmete võtmisega vähendada;
  - riske saab vältida (nt tööprotsesside või infokoosluse struktuuri muutmisega);
  - riske saab mujale suunata (nt väljasttellimise või kindlustuslepingutega);
  - riskidega võib leppida.

  Turbekontseptsiooni tuleb kirja panna, kuidas erinevate turberiskidega ümber käia. Seejuures tuleb hinnata ka jääkriskide suurust ja see arusaadavalt dokumenteerida.

- Turbekontseptsiooni konsolideerimine

Enne esialgse IT-etalonturbe protsessiga jätkamist tuleb täiendatud turbekontseptsioon konsolideerida. Selle käigus kontrollitakse turbemeetmete sobivust, koosmõju ja kasutajasõbralikkust.

Standardis „IT-etalonturbel põhinev riskianalüüs" selgitatakse muu hulgas ka seda, kuidas kasutada seda metoodikat siis, kui infokoosluses on objekte, millele IT-etalonturbe kataloogides ei leidu sobivat vastet.

Metoodika põhjaliku ülevaate leiate standardist BSI 100-3.

Oluline! IT-etalonturbel põhineva riskianalüüsi metoodika võimaldab vajaduse korral leida ka selliseid turbemeetmeid, mida IT-etalonturbe kataloogides ei ole. Seda metoodikat on paljude teiste sarnaste metoodikatega küll tunduvalt lihtsustatud, kuid selle rakendamisega kaasneb sageli siiski märkimisväärne töökulu. Kõige olulisemate turbeprobleemide võimalikult kiireks kõrvaldamiseks on mõnikord otstarbekas võtta kasutusele *esmalt* IT-etalonturbe meetmed ja *alles seejärel* teha riskianalüüs (erinevalt eespool näidatud skeemist). Sellisel juhul tuleb küll mõningaid samme korrata, kuid IT-etalonturbe meetmeid saab juba varem võtta. Selline alternatiivne järjekord on eriti kasulik järgmistel juhtudel:

1. kui vaadeldav infokooslus on juba reaalselt olemas ja töötab;
2. kui olemasolevaid objekte ei saa IT-etalonturbe kataloogide moodulite abil piisavalt täpselt modelleerida.

Seevastu selliste infokoosluste puhul, mis on alles planeerimisjärgus, mis sisaldavad ebatavalist tehnoloogiat või mille kasutusstsenaarium on ebatavaline, soovitatakse kasutada eespool näidatud algset järjestust. Järgmine tabel näitab mõlema järjekorra eeliseid ja puudujääke.

Riskianalüüs vahetult pärast esmast turbekontrolli	**Riskianalüüs pärast IT-etalonturbe meetmete võtmist**
Võimalikud eelised Jääb ära võimalik lisatöö, sest ei võeta meetmeid, mida peaks hilisema riskianalüüsi põhjal võib-olla tõhusamatega asendama. Võimalikud tavapärasest rangemad turbemeetmed tuvastatakse ja ka rakendatakse varem.	Võimalikud eelised IT-etalonturbe meetmeid võetakse varem, sest riskianalüüs on sageli töömahukas. Esmalt kõrvaldatakse elementaarsed turvaaugud ja alles seejärel asutakse analüüsima tõsisemaid ohte.
Võimalikud puudused IT-etalonturbe meetmeid võetakse hiljem, sest riskianalüüs on sageli töömahukas. Elementaarsed turvaaugud võivad jääda tähelepanuta, sest eelisjärjekorras analüüsitakse tõsisemaid ohte.	Võimalikud puudused Lisatöö tekkimise oht, sest võib juhtuda, et võetakse IT-etalonturbe meetmeid, mis tuleb hilisema riskianalüüsi põhjal asendada tõhusamatega. Võimalikud tavapärasest rangemad turbemeetmed tuvastatakse ja ka rakendatakse hiljem.

Lisaks on IT-etalonturbel põhinevat riskianalüüsi sageli kergem teha, sest seda rakendatakse järk-järgult infokoosluse väiksemate osade peal. Näiteks võib esimese sammuna piirduda ruumide ja taristutega, st keskenduda sellistele valdkondadele nagu tuleohutus, veekahjustuste vältimine, volitamata isikute juurdepääsu piiramine ning nõuetekohane elektrivarustus ja klimatiseerimine.

Paljudes ametiasutustes ja ettevõtetes on riskianalüüsi või -halduse meetmed juba välja töötatud. Ühtse metoodika kasutamiseks võib sellisel juhul olla kasulik, kui olemasolevad meetodid võetakse kasutusele ka infoturbe valdkonnas ning standardist BSI 100-3 võetakse üle ainult mõned vajalikud aspektid. Rahvusvahelisel tasandil on infoturbe riskianalüüside tegemiseks kasutusel mitu metoodikat. Need metoodikad erinevad oma detailsuse, vormi ja temaatilise rõhuasetuse poolest. Olenevalt institutsiooni raamtingimustest ja infokoosluse liigist tuleb infoturbe riskide analüüsimiseks kasutada standardi BSI 100-3 asemel võib-olla mõnda teist end hästi tõestanud metoodikat või seda metoodikat kohandada.

Institutsiooni riskianalüüsi tegemiseks valitud metoodika tuleb dokumenteerida ja juhtkond peab selle vastu võtma. **Riskianalüüsi tegemise reeglistik** peab vastama muu hulgas järgmistele küsimustele:

- millistel eeldustel võib täiendava turbeanalüüsi raames teha otsuse loobuda riskianalüüsist?
- millistel tingimustel on riskianalüüsi tegemine vältimatu?
- millist metoodikat/standardit kasutatakse riskianalüüsiks?
- kuidas kohandataks valitud metoodikat institutsiooni vajadustega?
- millised organisatsiooni allüksused vastutavad riskianalüüsi erinevate osaülesannete eest?
- kuidas integreeritakse riskianalüüsid turbeprotsessiga, nt enne või pärast IT-etalonturbe meetmete võtmist?
- millised on riskianalüüsi aruandekohustused?

Peatüki 4.6 „Täiendav turbeanalüüs" rõhuasetus

- Institutsiooni riskianalüüsi tegemise metoodika dokumenteerimine ja esitamine juhatusele kinnitamiseks
- Riskianalüüsi vajavate objektide või objektirühmade tuvastamine
- Täiendava turbeanalüüsi haldusraporti koostamine
- Haldusraporti esitamine juhatusele kinnitamiseks
- Vajaduse korral standardi BSI 100-3 „IT-etalonturbel põhinev riskianalüüs" süstemaatiline läbitöötamine
- Riskianalüüsi tulemuste integreerimine turbekontseptsiooniga

5 Turbekontseptsiooni elluviimine

Selles peatükis kirjeldatakse turbemeetmete planeerimise ja elluviimise aspekte. Täpsemalt käsitletakse turbemeetmete planeerimist, võtmist, toetamist ja kontrolli.

Infokoosluse jaoks väljatöötatava turbekontseptsiooni etappidest peavad olema nüüdseks läbitud struktuurianalüüs, turbevajaduse kindlaksmääramine ja modelleerimine. Samuti peavad selleks etapiks olema tehtud esmane turbekontroll ning sellele järgnev soovitud ja tegeliku olukorra võrdlus. Juhul kui mõningate valdkondade jaoks on tehtud riskianalüüs, peaksid nüüdseks olema välja töötatud ka soovitused, milliseid meetmeid võtta, et nendega oleks võimalik edaspidi juba arvestada.

Meetmete võtmiseks vajalikud ressursid, kaasa arvatud rahaline ressurss, on sageli üpris piiratud. Seetõttu on järgnevalt kirjeldatud töösammude eesmärk selgitada ettenähtud turbemeetmete võtmist ennekõike efektiivsuse vaatepunktist. Peatüki lõpust leiate selle käsitluse kohta ka selgitava näite.

5.1 Analüüsitulemuste hindamine

Üldpildi saamiseks tuleks esmalt analüüsida ainult selliseid IT-etalonturbe meetmeid, mida ei ole veel kas üldse võetud või mis on võetud ainult osaliselt. Selleks võiks kasutada esmase turbekontrolli tulemusi ning kõik poolikult võetud ja veel võtmata turbemeetmed tuleks koondada tabelisse.

Samuti tuleb arvestada võimalike lisameetmetega, mille vajadus on riskianalüüsidega kindlaks tehtud. Ka need meetmed koondatakse tabelisse. Lisameetmete liigitamisel tuleb lähtuda eelkäsitletud modelleerimisest ja selle sihtobjektidest ning IT-etalonturbe moodulitest.

5.2 Meetmete konsolideerimine

Enne turbemeetmete võtmist tuleb need konsolideerida. Juhul kui tehti riskianalüüse, tuleb nende tulemused integreerida edasise protsessiga, sest nende põhjal võis lisanduda uusi turbemeetmeid, samuti võis selguda, et mõned IT-etalonturbe kataloogide meetmed vajavad kas asendamist või täiendamist. Siinkohal tuleks kontrollida, kas leidub selliseid IT-etalonturbe meetmeid, mille võtmisest saab loobuda põhjusel, et see asendatakse hoopis mõne rangema meetmega.

Kuna IT-etalonturbe raames esitatakse väga palju erinevaid soovitusi nii töökorralduse kui ka tehnilise teostuse kohta, tuleb valitud meetmeid võib-olla veel täpsustada, st kohandada institutsiooni töökorralduse ja tehniliste oludega. Lisaks tuleks turbemeetmeid veel kord kontrollida selle suhtes, kas need on tõepoolest kõige sobivamad: meetmed peavad institutsiooni võimalike ohtude eest efektiivselt kaitsma, kuid olema samal ajal ka võimalikult praktilised, st meetmete võtmine ei tohi takistada juba väljakujunenud tööprotsesse ning need ei tohi õõnestada teiste turbemeetmete kaitsvat toimet. Selliste vastuolude leidmisel tuleb esialgu väljavalitud IT-etalonturbe meetmed asendada tõhusamatega.

Ülevaatlikkuse säilimiseks, täpsemalt selleks, et ka tulevikus oleks aru saada, milliste põhimõtete alusel on võetavate meetmete nimekirju koostatud ja muudetud, tuleks sellekohased otsused dokumenteerida.

Lisanõuandeid turbemeetmete konsolideerimise kohta leiate ka standardist 100-3.

Näited

- Riskianalüüsiga tehti kindlaks, et IT-etalonturbe meetmete kõrval tuleb institutsioonis juurutada ka kiipkaardil põhinev autentimissüsteem ning isikuandmete töötlemist kaitsev klientsüsteemide kõvaketaste lokaalne krüpteerimine. Selline lisameede asendaks nt isikuandmete turvet puudutavat ja klientsüsteemidele esialgu ette nähtud meedet M 4.48 „Paroolikaitse Windows NT all ”.
- Esmase turbekontrolliga tehti kindlaks, et meede M 1.24 „Veetorude vältimine IT-ruumis” on seni võtmata ja et olemasolevate ehituskonstruktsioonide tõttu ei ole selle meetme võtmine majanduslikult vastuvõetav. Selle asemel tuleks võtta asendusmeede, mis näeb ette, et veetorudele

tuleb paigaldada vett eemale juhtivad plekid koos anduritega. Anduri töölelülitumisel peab asjakohane teade laekuma kas uksehoidjale või mõnele teisele hoone eest vastutavale isikule, kes saab olukorrale kiiresti reageerida ja tekkiva veekahjustuse ära hoida.

5.3 Kulude ja töömahu hindamine

Kuna turbemeetmete võtmise eelarve on alati piiratud, tuleb iga meetme kohta üles märkida, kui suur on selle investeeringu kulu ja kui palju vajab see meede personaliressurssi. Siinkohal tuleb vahet teha ühekordsetel investeeringutel ja personalikulul ning korduvatel kuludel. Selles etapis võib tihti selguda, et tehnoloogia pealt kokkuhoitud summad toovad endaga tulevikus kaasa pideva personalikulu.

Seetõttu on vajalik kindlaks teha, kas kõik ettenähtud turbemeetmed on ka majanduslikult mõttekad. Juhul kui meetmete hulgast leitakse selliseid, mille võtmiseks ei ole piisavalt raha, tuleks kaaluda sobivaid asendusmeetmeid või analüüsida, kas meetme võtmata jätmisel tekkiv jääkrisk on institutsiooni jaoks talutav või mitte. Ka see otsus tuleb kindlasti dokumenteerida.

Olukorras, kus meetmete hinnangulised ressursid, st raha ja piisav hulk personali, on olemas, võib asuda järgmise etapi juurde. Paljudel juhtudel tuleb esmalt siiski vastu võtta otsus, kui palju ressursse tohib institutsioon turbemeetmete võtmisele kulutada. Selleks on soovitatav otsustajatele (juhtkond, IT-juht, infoturbespetsialist jne) ette valmistada ettekanne, mis toob välja turbeanalüüsi tulemused. Ettekandes tuleks tähtsuse järjekorras, st turbevajaduse põhjal, loetleda kõikvõimalikud puudused (seni võtmata või ebapiisavalt võetud turbemeetmed). Meetmete loetlemise kõrval tuleks välja tuua ka nende võtmise oletatavad kulud ja tööde hinnanguline maht. Ettekande lõpus tuleks anda hinnang, kui suur võiks olla kogu ettevõtmise eelarve.

Väikse eelarve korral, mis ei luba kindlasti kõiki puuduvaid turbemeetmeid võtta, tuleks ära näidata jääkohud, mis tekivad siis, kui osa meetmeid jäetakse kas võtmata või võetakse kunagi hiljem. Selleks tööks saab kasutada IT-etalonturbe abivahendite alt leitavaid ristreferentside tabeleid. Ristreferentside tabelid annavad iga mooduli kohta ülevaate meetmetest ja nende mõjust ohtude kõrvaldamisele. Nende tabelite põhjal saab kontrollida ka seda, milliseid IT-etalonturbe kataloogides loetletud ohte pole seni piisavalt käsitletud. Jääkrisk, st juhuslike ja tahtlikult esilekutsutavate intsidentide ohud, tuleb lahti seletada võimalikult läbipaistvalt ning ette valmistada selliselt, et juhtkond saaks selle kohta võtta vastu otsuse. Edasisi samme saab astuda alles pärast juhtkonna otsust jääkriskide kohta, sest juhtkond vastutab tagajärgede eest.

5.4 Meetmete võtmise järjekorra kindlaksmääramine

Olukorras, kus institutsioonil ei ole kas piisavalt raha või personali, et kõiki turbemeetmeid kohe võtta, tuleb kindlaks määrata meetmete võtmise järjekord. Järjekorra väljatöötamisel tuleb arvestada järgmiste aspektidega.

- Meetmete võtmise järjekord peaks lähtuma meetmete kasutustsükli liigitusest. Ülevaade meetmete kasutustsükli liigituse ehk meetmete võtmise ajalise järjekorra kohta on toodud igas moodulis. Loomulikult tuleb alati alustada nendest meetmetest, mis kuuluvad planeerimise ja kontseptsiooni väljatöötamise, mitte võtmise või käitamise valdkonda.
- Lisaks võetakse iga meetme puhul arvesse, kui oluline on see meede IT-etalonturbe saavutamiseks, ja esitatakse selle põhjal meetmete liigitus. Liigitustähised (L - Madal , M – Keskmine, H - Kõrge, Z – soovituslik, W – teadmised) näitavad ära meetme olulisuse turbekontseptsioonis. A-kategooria meetmed on väga sageli üliolulised ja seetõttu tuleb neid võtta eelisjärjekorras.
- Mõnede meetmete puhul tekib võtmise kindel järjekord nende loogiliste seoste põhjal. Näiteks on nii meede M 2.25 „Süsteemi konfiguratsiooni dokumenteerimine" kui ka meede M 2.26 „Administraatori ja tema asetäitja määramine" väga olulised, aga kui administraatorit ei ole, on meedet M 2.25 väga raske võtta.

- Osa meetmete mõju võib olla väga laiaulatuslik ning teised jällegi võivad mõjuda ainult lokaalselt. Seetõttu on sageli üpris mõttekas arvestada esmalt meetmetega, millel on laiaulatuslik mõju.
- Mõned moodulid mõjutavad eesmärgiks seatud turbeastme saavutamist enam kui teised. Eelisjärjekorras tuleks vaadelda suurema mõjuga mooduleid ja seda eriti siis, kui püütakse kõrvaldada väga suure turbevajadusega valdkonna vigu. Näiteks tuleks esmalt tegeleda serveri turbega (muu hulgas rakendada moodulit B 3.101 „Server") ja alles seejärel asuda serveriga ühendatud klientsüsteemide turbe kallale.
- Moodulid, mille puhul selgub, et nendes on väga palju meetmeid, mida ei ole seni võetud, tähistavad valdkondi, milles on kõige enam puudujääke. Ka neid valdkondi tuleks käsitleda eelisjärjekorras.

Otsused, milliseid turbemeetmeid võtta ja milliste meetmete võtmine edasi lükata, tuleb juriidilistel kaalutlustel hoolikalt dokumenteerida. Kahtluse korral tuleks konsulteerida spetsialistidega ja nende nõuanded samuti dokumenteerida, et hilisemate vaidluste korral oleks võimalik tõestada tööde hoolikat teostust.

5.5 Ülesannete ja vastutuse kindlaksmääramine

Pärast meetmete võtmise järjekorra kehtestamist tuleb kindlaks määrata, kes millised meetmed mis ajaks võtab. Kogemused on näidanud, et ilma sellise tööplaanita hakkab meetmete võtmine kas oluliselt venima või katkeb sootuks. Siinkohal tuleks arvestada, et vastutajaks määratud isik oleks talle usaldatud meetme võtmiseks piisavalt pädev ja et talle antaks kõik tööks vajalikud ressursid.

Samuti tuleb kindlaks määrata, kes vastutab meetmete võtmise kontrollimise eest, st tuleb määrata isik, kellele antakse meetmete võtmisest aru. Vastutavaks isikuks nimetatakse enamasti infoturbespetsialist. Tööde arengujärku tuleb pidevalt kontrollida, et tähtajad venima ei hakkaks.

Koostatav tööplaan peaks sisaldama vähemalt järgmist infot:

- sihtobjekti kirjeldus (kasutuskeskkond);
- vaadeldava mooduli number;
- meetme pealkiri või kirjeldus;
- meetmete võtmise planeeritud tähtajad;
- eelarve, mida ei tohi ületada;
- meetmete võtmise eest vastutavad isikud;
- meetmete võtmise kontrollimise eest vastutavad isikud.

5.6 Meetmete võtmise abimeetmed

Meetmete võtmisel on oluline, et juba algusest peale planeeritaks piisavalt ka seda, kuidas neid täpselt võtta. Võtmist abistavate meetmete hulka kuulub nt töötajate teadlikkuse suurendamine eesmärgiga selgitada, miks töötajad peavad turbemeetmeid järgima ja millised võivad olla turbemeetmete eiramise tagajärjed.

Lisaks tuleb asjaomaseid töötajaid ka piisavalt koolitada, et nad oskaksid võetavaid turbemeetmeid õigesti kasutada. Kui koolitustest loobutakse, jäävad meetmed tihti kas võtmata või ei avalda need loodetud toimet, sest kui töötajaid ei ole piisavalt informeeritud, tekib neil infoturbe suhtes sageli tõrjuv hoiak.

Näide: töökorralduse ja haldamise amet (THA) – 11. osa

Järgnevalt kirjeldatakse äsja mainitud aspekte fiktiivse THA näitel. Tabel kajastab mõningaid võetavaid meetmeid ja nende kuluhinnangut.

Sihtobjekt	Moodul	Meede	Seisund	Kulu	Märkus
Riist- ja tarkvara haldus	B 1.9	M 2.11 „Paroolide kasutamise reeglid”	T	a) 0 eurot b) 2 PT c) 0 eurot/aasta d) 0,5 PT/aasta	
Serveriruum R 3.10	B 2.4	M 1.24. „Vett ärajuhtivate plekkide ja veeanduri paigaldus koos uksehoidjat teavitava seiresüsteemiga”	N	a) 4000 eurot b) 3 PT c) 0 eurot/aasta d) 1 PT/aasta	
Server S4	B 3.101	M 1.28 „Lokaalne puhvertoiteallikas (UPS)”	N	a) 1000 eurot b) 1 PT c) 0 eurot/aasta d) 0,5 PT/aasta	
Klient Windows 2000 all	B 3.207	M 4.1 „PC ja serveri paroolkaitse“ ja M 4.41 „Sobivate IT-süsteemide turvatoodete valimine“	N	a) 1400 eurot b) 2 PT c) 0 eurot/aasta d) 2 PT/aasta	
...					

Legend

- Seisund (= meetme võtmise seisund)

  T = osaliselt võetud, N = täiesti võtmata
- Kulud

  a) = ühekordne investeerimiskulu

  b) = ühekordne personalikulu (PT = ühe isiku tööpäev)

  c) = korduv investeerimiskulu

  d) = korduv personalikulu (PT = ühe isiku tööpäev)

Järgneb tööplaani tabeli näide, mis koostatakse eelmise tabeli ja juhtkonna otsuste põhjal.

Tööplaan (seis 01.09.20xy)						
Sihtobjekt	**Moodul**	**Meede**	**Võtmise lõppkuupäev**	**Vastutav isik**	**Eelarve, mida ei tohi ületada**	**Märkus**
Riist- ja tarkvara haldus	B 1.9	M 2.11 „Paroolide kasutamise reeglid”	31.12.20xy	a) Peeter b) Liisa	a) 0 eurot b) 2 PT c) 0 eurot/aasta d) 0,5 PT/aasta	
Serveriruum R 3.10	B 2.4	M 1.24 „Vett ärajuhtivate plekkide ja veeanduri paigaldus koos uksehoidjat teavitava seiresüsteemiga”	30.04.20xy	a) Jüri b) Toomas	a) 1000 eurot b) 2 PT c) 0 eurot/aasta d) 1 PT/aasta	Plekid paigaldada üksnes joogivee- ja kanalisatsiooni-torude alla.
Server S4	B 3.101	M 1.28 „Lokaalne puhvertoiteallikas (UPS)”	31.10.20xy	a) Rein b) Liisa	a) 500 eurot b) 1 PT c) 0 eurot/aasta d) 0,5 PT/aasta	

Klient Windows 2000 all	B 3.207	M 4.1 „PC ja serveri paroolkaitse“ ja M 4.41 „Sobivate IT-süsteemide turvatoodete valimine“	31.12.20xy	a) Rein b) Liisa	a) 1400 eurot b) 2 PT c) 0 eurot/aasta d) 2 PT/aasta	
...						

Legend

- Vastutav isik

  a) = meetme võtmise eest vastutav isik

  a) = meetme võtmise kontrollimise eest vastutav isik

- Eelarve, mida ei tohi ületada: meetmete võtmiseks olemasolevad ressursid

  a) = ühekordne investeerimiskulu

  b) = ühekordne personalikulu (PT = ühe isiku tööpäev)

  c) = korduv investeerimiskulu

  d) = korduv personalikulu (PT = ühe isiku tööpäev)

Selle info põhjal saab meetmete võtmist kontrollida ja juhtida.

Peatüki 5 „Turbekontseptsiooni elluviimine” rõhuasetus

- Seni võtmata või ainult osaliselt võetud IT-etalonturbe meetmete ja vajalike lisameetmete koondamine tabelisse
- Turbemeetmete konsolideerimine, st liigsete meetmete kõrvaleheitmine, üldiste meetmete kohandamine kohapealsete oludega ja meetmete sobivuse kontrollimine
- Meetmete võtmisega seotud ühekordsete ja korduvate kulude väljaselgitamine
- Liigsete kulude või teiste põhjuste tõttu võtmata jäetavate turbemeetmete asendusmeetmete väljaselgitamine
- Otsuste langetamine selle kohta, kui palju tohib milliseid ressursse meetmete võtmiseks kulutada
- Võimaliku jääkriski väljaselgitamine ja sellekohaste otsuste langetamine juhtkonna tasandil
- Turbemeetmete võtmise järjekorra kindlaksmääramine, selle põhjendamine ja dokumenteerimine
- Meetmete võtmise tähtaegade kindlaksmääramine ja vastutavate isikute nimetamine
- Meetmete võtmise ja selle tähtaegade järgimise kontrollimine
- Asjaomaste töötajate koolitamine ja nende teadlikkuse suurendamine

6 Toimiva infoturbe tagamine ja pidev täiustamine

Infoturbeprotsessi tagamine ja pidev täiustamine ei eelda mitte ainult asjakohaste turbemeetmete võtmist ja dokumentatsiooni pidevat värskendamist, vaid ka protsessi enda analüüsimist ja kontrollimist, et veenduda selle tõhususes. Turbeprotsessi tõhusust peaks regulaarselt hindama juhtkond (juhtkonna hinnang). Vajaduse korral (nt kui esineb tavapärasest rohkem turvaintsidente või kui raamtingimustes peaks tehtama suuri muudatusi) tuleks asjakohaseid koosolekuid pidada ka kokkulepitust sagedamini. Kõik tulemused ja otsused tuleb arusaadavalt dokumenteerida.

6.1 Turbeprotsessi kontroll kõikidel tasanditel

Infoturbeprotsessi kontroll on vältimatu, sest ühelt poolt aitab selline tegevus tuvastada ja kõrvaldada võimalikke vigu ja puudusi ning teisalt võimaldab see infoturbeprotsessi optimeerida. Ühtlasi saab kontrolliga parendada ka strateegiat, meetmeid ja töökorraldust.

Järgnevalt kirjeldatakse selle valdkonna olulisimaid aspekte.

6.1.1 Infoturbeprotsessi kontrollimeetodid

Turbeprotsessi parendamiseks ja selle tõhususe kontrollimiseks tuleks juurutada sellised protseduurid ja mehhanismid, mis aitaksid kontrollida nii seda, kas meetmed, mida on plaanis võtta, on ka reaalselt võetud, ja kas need meetmed toimivad efektiivselt. Seetõttu peaks infoturbestrateegia sisaldama ka põhimõtteid, kuidas eesmärkide saavutamist mõõta. Selliste mõõtmiste lähtepunktid võivad olla nt järgmised:

- turvaintsidentide tuvastamine, dokumenteerimine ja analüüs;
- turvaintsidente jäljendavate harjutuste ja katsetuste tegemine ning tulemuste dokumenteerimine;
- sise- ja välisauditid ning andmekaitsekontrollid;
- konkreetsetel turbekriteeriumidel põhinev sertifitseerimine.

Võetud meetmete tõhusust tuleks kontrollida siseaudititega. Siinkohal on oluline, et asjakohaseid kontrolle ei viiks läbi need inimesed, kes turbekontseptsiooni välja töötasid. Kontrollimiseks oleks mõistlik kasutada väliseid eksperte.

Kuna audititega seotud tööde hulk oleneb väga palju institutsiooni suurusest ja selle infokoosluse keerukusest, saab neid nõudeid väga edukalt rakendada ka väiksemates institutsioonides. Nende puhul piisab võib-olla isegi sellest, kui korraldada kord aastas IT-süsteemide tehniline kontroll, vaadata läbi asjakohane dokumentatsioon ning korraldada õpikoda, kus töötajad saavad vahetada oma kogemusi ja rääkida turbekontseptsiooniga seonduvatest probleemidest.

6.1.2 Turbemeetmete võtmise kontroll

Meetmete võtmise plaan, kuhu on märgitud, millised ülesanded peavad mis ajaks tehtud olema, võimaldab kontrollida, kas planeeritud töökavast on kinni peetud. Heakskiidetud turbemeetmete õigeaegse võtmise üks olulisi eeldusi on ressursside õige planeerimine. Seepärast tuleks kontrollimisel pöörata tähelepanu ka sellele, kas meetmete võtmiseks eraldati õigel ajal piisavalt ressursse, st kas tööde tegemiseks oli piisavalt raha ja personali. Infoturbeprotsessi kontrolli ainus eesmärk pole aga välja selgitada, kas turbekontseptsioonis ettenähtud ülesanded on täidetud. Oluline on ka võimalike planeerimisvigade kiire tuvastamine ning kui kontseptsiooni rakendamine selle algsel kujul tundub ebarealistlik, siis ka turbekontseptsiooni muutmine.

Pärast uute meetmete võtmist peaks infoturbespetsialist kontrollima ennekõike seda, kas töötajad aktsepteerivad ja järgivad neid meetmeid või suhtuvad nendesse pigem umbusklikult. Kui töötajad turbemeetmeid ei aktsepteeri, on ebaõnnestumine juba ette teada. Põhjused tuleb üles leida ja kõrvaldada. Enamasti piisab täiendavast teavitustööst.

Turberevisjon

IT-etalonturbe kataloogides toodud meetmeid saab kasutada ka infoturbe revisjoni tarbeks. Selleks soovitatakse samu protseduure nagu esmase turbekontrolli puhul. Aega ja vaeva saab suuresti kokku hoida, kui iga IT-etalonturbe kataloogi mooduli kohta töötatakse meetmete põhjal välja institutsiooni eripäradega arvestav eraldi küsimustik. See lihtsustab revisjonide tegemist ja suurendab tulemuste kasutusvõimalusi.

6.1.3 Infoturbestrateegia sobilikkus

Infoturbeprotsessi edukaks suunamiseks ja juhtimiseks peab juhtkonnal olema hea ülevaade sellest, mil määral on valitud turbestrateegia aidanud turbe-eesmärke ellu viia.

Turbe-eesmärkide, raamtingimuste ja turbekontseptsiooni aktuaalsus

Pikemas perspektiivis on turbe-eesmärke ja raamtingimusi muu hulgas tarvis ka kontrollida. Infoturbepoliitika ja turbestrateegia kohandamine on elementaarne tegevus ennekõike kiiresti arenevate valdkondade puhul.

Turbekontseptsiooni loomisel tuleb arvestada ka potentsiaalsete muutustega tööprotsessides (uute IT-süsteemide kasutuselevõtt, kolimine), töökorralduses (nt väljasttellimine) ja võimalikes raamtingimustes (seaduste ja nõuete muutumine). Turbekontseptsiooni ja selle dokumentatsiooni tuleb iga olulise muutuse korral värskendada. Institutsiooni muudatuste tegemise protsessi puhul peab sellega arvestama. Seetõttu tuleb infoturbeprotsess integreerida institutsiooni muudatuste tegemise protsessiga.

Majanduslikkuse hindamine

Pidevalt tuleks jälgida ka turbestrateegia ja selle spetsiifiliste turbemeetmete majanduslikkust. Infoturbele tehtavaid kulutusi on küll üpris raske kokku arvutada, kuid edasise planeerimise jaoks on kindlasti abiks, kui kontrollitakse, kas seni võetud meetmete puhul vastavad nende tegelikud kulud planeeritud kuludele või on mõistlikum kasutada hoopis teisi turbemeetmeid, mis nõuavad vähem ressursse. Samuti on oluline, et võetud turbemeetmete puhul analüüsitaks pidevalt, kui suur on nende kasutegur.

Enda töötajate ja võõraste tagasiside

Protsessides tekkinud vigade ja puuduste kohta ei anna infot mitte ainult infoturbe tööprotsessid ja revisjon, vaid ka institutsiooni enda töötajad, samuti koostööpartnerid ja kliendid. Seetõttu peab institutsioonis olema välja töötatud tõhus protseduur, kuidas väljastpoolt saabuvate kaebuste ja tagasisidega asjakohaselt ümber käia.

Klientide ja töötajate kaebused võivad olla ka märk rahulolematusest. Rahulolematuse põhjused tuleks võimalikult hästi kõrvaldada, sest rahulolevate töötajate puhul on hooletusest ja pahatahtlikust tegevusest tingitud ning tööprotsessi segavate vigade tekkimise oht palju väiksem.

Seega tuleb välja töötada ühtne protseduur, kuidas kaebustega ümber käia ja kuidas asjakohane info institutsiooni sees peaks edasi liikuma, ning määrata kindlad vastutusalad. Näiteks tuleks kaebustele vastata võimalikult kiiresti, sest muidu võib inimesele tunduda, et temasse ei suhtuta piisavalt tõsiselt. Probleemide kohta laekunud infot tuleb analüüsida, et selgitada välja edasised tegevused. Vigade taastekkimise vältimiseks peab institutsioon võtma asjakohaseid parandusmeetmeid, mis kõrvaldavad vigade tekkepõhjuse.

6.1.4 Infoturbeprotsessi tulemuste kasutamine

Tõhususe kontrolli tulemused võimaldavad infoturbeprotsessi parendada. Kontrolli tulemusena võib nt selguda, et turbe-eesmärke, -strateegiat või -kontseptsiooni tuleb muuta ning infoturbe töökorraldust vajadust mööda ümber kujundada. Mõningatel juhtudel võib IT-s ja tööprotsessides teha suuri

muudatusi ka siis, kui seniste raamtingimuste põhjal on selge, et turbe-eesmärkide saavutamine osutub kas võimatuks või väga raskeks (tekib väga suur finants- või personalikulu). Kui otsustatakse suuremate muudatuste ja paranduste kasuks, tuleb turbehalduse eest vastutavatel töötajatel alustada taas turbe planeerimisest.

Kõiki valdkondi peavad analüüsima selles valdkonnas pädevad inimesed, st nad peavad olema piisavalt kompetentsed ja sõltumatud. Kontseptsioonide täielikkust ja õigsust ei tohiks kontrollida kontseptsioonide väljatöötajad.

Infoturbeprotsessi kontrollimise ja parendamise metoodika tuleb dokumenteerida suunisena ning juhtkond peab selle vastu võtma. **Infoturbeprotsessi kontrolli ja parendamise suunis** peaks ennekõike kehtestama reeglid, kuidas infoturbe siseauditeid teha ja kuidas tulemused muutmisprotsessiga integreerida. Kontrollide tulemused ja aruanded on enamasti ülimalt konfidentsiaalsed ning seetõttu tuleb neid ka hästi kaitsta.

Peatüki „Turbeprotsessi kontroll kõikidel tasanditel" rõhuasetus

- Institutsiooni infoturbeprotsessi kontrollimise ja parendamise metoodika dokumenteerimine eraldi suunisena ning selle esitamine juhatusele kinnitamiseks
- Turbe-eesmärkide saavutamise mõõtmise funktsiooni integreerimine turbestrateegiaga
- Meetmete võtmise plaani järgimise kontroll
- Kinnitatud meetmete võtmise kontroll
- Kinnitatud meetmete tõhususe kontroll
- Turbemeetmete aktsepteerimise kontroll ja vajaduse korral parendamine
- Koostaja ja kontrollija rollikonflikti vältimine
- Kontrollitulemuste konfidentsiaalsuse tagamine
- Turbe-eesmärkide, -strateegiate ja -kontseptsioonide sobivuse ja aktuaalsuse kontroll
- Turbestrateegia ja selle meetmete majanduslikkuse ning nende elluviimiseks eraldatud ressursside sobivuse kontroll
- Paranduste tegemine infoturbeprotsessis kontrolli tulemuste põhjal

6.2 Infoturbeprotsessi infovoog

Infoturbeprotsessi kontrollimise ja parendamise tulemusena koostatakse institutsioonis sageli kõikvõimalikke dokumente, nt aruandeid, auditite raporteid, turbekatsetuste hinnanguid, turvaintsidente käsitlevaid teateid. Kõik need dokumendid peavad olema asjalikud ja nende sihtrühmale arusaadavad. Kuna mitte kõik dokumendid ei sobi oma sisult ja vormilt juhtkonnale esitamiseks, on infoturbespetsialisti ja infoturbehalduse meeskonna ülesanne see info kokku koguda ning juhtkonna jaoks lühidalt ja ülevaatlikult kokku võtta.

6.2.1 Juhtkonnale esitatavad aruanded

Ametiasutuse või ettevõtte juhtkond saab infoturbeprotsessi õigesti juhtida ja suunata vaid siis, kui neile on infoturbe kohta esitatud õiged ja olulised andmed. Olulisi andmeid peavad sisaldama haldusaruanded ja nendes tuleks käsitleda vähemalt järgmisi aspekte:

- auditite ja andmekaitsekontrollide tulemused;
- turvaintsidentide aruanded;
- infoturbeprotsessi senise edu ja seniste probleemide aruanded.

Infoturbehalduse eest vastutavad isikud peavad juhtkonda regulaarselt ja sobivas vormis informeerima nii kontrollide tulemustest kui ka infoturbe seisundist. Juhtkonda tuleb teavitada probleemidest,

õnnestumistest ja võimalustest, kuidas midagi paremaks muuta. Juhtkond võtab haldusaruanded teadmiseks ja algatab vajaduse korral asjakohaste meetmete võtmise.

6.2.2 Infoturbeprotsessi dokumenteerimine

Infoturbeprotsessi edukuse määrab mitmel põhjusel selle dokumentatsioon. Piisava dokumentatsiooni eelised:

- vastuvõetud otsuste parem mõistetavus;
- võimalus protsesse korrata ja standardiseerida;
- puuduste ja vigade tuvastamine ja nende vältimine tulevikus.

Dokumentatsiooni puhul saab kasutusotstarbele toetudes eristada järgmisi dokumendiliike.

- Tehniline dokumentatsioon ja tööprotsesside dokumentatsioon (sihtrühm: eksperdid)

  Selles dokumentatsioonis kirjeldatakse tööprotsesside ning nendega seotud IT-süsteemide ja rakenduste värskeimat seisundit. Tehnilise dokumentatsiooni puhul vaieldakse väga sageli selle vajaliku detailsuse üle. Pragmaatilise käsituse kohaselt võetakse aluseks süsteemide ja rakenduste taastamine, st dokumentatsioon peab olema selline, et võrdsete teadmistega eksperdid oleksid võimelised seda kasutama ning et administraator ei pea lähtuma mitte oma mälust, vaid oma teadmistest. Olemasolevat dokumentatsiooni tuleks hinnata turbeõppuste raames ja turvaintsidentide käsitlemisel ning seda asjakohaselt parendada. Seda liiki dokumentatsiooni hulka kuuluvad muu hulgas järgmised dokumendid:

  - installimis- ja konfigureerimisjuhised;
  - pärast turvaintsidenti kasutatavad taastamisjuhised;
  - katsetamisprotseduuride ja kasutusse lubamise protseduuride dokumentatsioon;
  - rikete ja turvaintsidentide puhul kehtivad käitumisjuhised.

- Töötajatele suunatud juhised (sihtrühm: töötajad)

  Turbemeetmed tuleb töötajate jaoks sõnastada ja dokumenteerida arusaadavate juhistena. Lisaks tuleb töötajaid piisavalt informeerida ja koolitada, et nad oleksid juhistest teadlikud ning oskaksid neid järgida. Seda liiki dokumentatsiooni hulka kuuluvad nt järgmised dokumendid:

  - tööprotsesside kirjeldus ja töökorralduslikud nõuded;
  - interneti kasutamise reeglid;
  - käitumine turvaintsidentide korral;

- Juhtimisotsuste dokumentatsioon (sihtrühm: juhtkond)

  Infoturbeprotsessi ja -strateegia kohta vastu võetud olulised otsused tuleb dokumenteerida.

- Seadused ja ettekirjutused (sihtrühm: juhtkond)

  Infotöötlust võivad reguleerida paljud seadused, ettekirjutused ja nõuded. Iga institutsioon peaks enda jaoks dokumenteerima kõige olulisemad tööprotsesse, IT-süsteemide käitamist ja infoturvet mõjutavad seadused, ettekirjutused ja nõuded ning üles märkima, millised on nende nõuete eiramise tagajärjed.

Tuleb tagada, et kogu dokumentatsioon oleks alati värske. Selleks tuleb dokumentatsiooni koostamine integreerida muutmisprotsessiga.

6.2.3 Info liikumine ja teavitamiskanalid

Infoturbeprotsessi tagamiseks on elementaarne, et info liikumine ja teavitamiskanalid oleks kõikidele teada ning võimalikud muutused kehtestataks kõikjal läbivalt ühte moodi. Infovoogude liikumise

analüüsimiseks ja parendamiseks saab kasutada koolituste, testide ja auditite tulemusi.

Infoturbeprotsessi info liikumise ja teavitamiskanalite kasutamise metoodika tuleb dokumenteerida suunisena ning juhtkond peab selle vastu võtma. **Info liikumise ja teavitamiskanalite kasutamise suunis** peaks reguleerima ennekõike infoturbeprotsessi kriitiliste infovoogude liikumist. Siinkohal tuleks eristada info hankimise ja edastamise kohustust.

Sünergiaefektide ärakasutamine infovoo heaks

Paljudes institutsioonides on sageli kindlaks määratud, kuidas teenuse osutamine või IT-kasutuse tugiteenus peab töötama. Seetõttu on sageli võimalik ära kasutada sünergiaefekte, mis tekivad infoturbeprotsessi liitmisest olemasolevate tööprotsessidega. Näiteks saab turvaintsidentidest teavitamise kanaleid integreerida IT-tugiteenusega ja võimsuse planeerimise valdkonna liita hädaolukordadeks ettevalmistamisega.

Paljusid turbevaldkonna jaoks hangitud andmeid saab kasutada ka muul otstarbel. Turbemeetmete võtmine võib omakorda positiivselt mõjuda protsesside optimeerimisele. Näiteks on info omanike kindlaksmääramine või info analüüsimine ühtsete hindamiskriteeriumide alusel kindlasti oluline institutsiooni enamatele valdkondadele kui ainult infoturve. Samuti võib olla kindel, et teadmisi tööprotsesside ning IT-süsteemide ja rakenduste sõltuvusseostest saavad kasutada ka paljud teised peale infoturbehalduse. Nende põhjal saab nt analüüsida tööprotsesside või ka toodete konkreetseid IT-kulusid, mida kajastatakse tavaliselt tervikuna üldkulude all.

Peatüki 6.2 „Info liikumine ja teavitamiskanalid" rõhuasetus

- Infoturbeprotsessi info liikumise ja teavitamiskanalite kasutamise metoodika dokumenteerimine suunisena ning esitamine juhtkonnale vastuvõtmiseks
- Juhtkonna informeerimine infoturbeprotsessi sündmustest, kontrollidest ja seisundist
- Vajaduse korral vajalike parandusmeetmete kohta otsuste hankimine
- Kogu infoturbeprotsessi arusaadav dokumenteerimine ja dokumentatsiooni ajakohastamine
- Vajaduse korral dokumentatsiooni kvaliteedi hindamine ning dokumentatsiooni täiendamine või värskendamine
- Infoturbeprotsessi teavituskanalite toimimise pidev tagamine
- Infoturbeprotsessi ja teiste juhtimisprotsesside sünergiaefektide leidmine