Bundesamt
für Sicherheit in der
Informationstechnik

Riigi Infosüsteemide Arenduskeskus

Infoturbe juhend

Lühiülevaade olulisematest infoturbe alastest turvameetmetest

Copyright

Käesolevas infoturbe soovituste juhendis on esitatud kompaktne ülevaade tähtsamatest organisatoorsetest, infrastruktuuri alastest ja tehnilistest IT turvameetmetest. Juhend on mõeldud IT juhtidele ja infoturbe valdkonna eest vastutavatele inimestele riigiasutustes, väikestes ja keskmistes ettevõtetes. Juhendit saavad kasutada ka asutuste juhtkonnad ülevaate saamiseks olulisematest infoturbe alastest turvameetmetest ja olukorra hindamiseks oma asutuses.

Juhendi näol on tegemist Saksamaa Infoturbeameti *(BSI, Bundesamt für Sicherheit in der Informationstechnik)* dokumendi *„Leitfaden IT-Sicherheit“* osalise tõlkega. Nimetatud dokumendi koostamisel on kasutatud BSI IT etalonturbe juhendit, millest on välja toodud olulisemad infoturbe alased turvameetmed ja mis peaks olema rakendatud igas head infoturbe taset soovivas ettevõttes. BSI IT etalonturbe juhend on olnud aluseks ka ISKE (Infosüsteemide kolmeastmelise etalonturbe süsteem, www.ria.ee/iske) koostamise aluseks. ISKEt juurutavad asutused saavad käesolevat juhendit kasutada infoturbe teadlikkuse tõstmiseks organisatsioonis ja vajadusel ISKEst tulenevatele turvameetmetele rakendusprioriteetide määramisel.

Toomas Viira
Infoturbe juht
Riigi Infosüsteemide Arenduskeskus

„Leitfaden IT-Sicherheit“
saksa keelne tekst www.bsi.de/gshb/Leitfaden/GS-Leitfaden.pdf
„IT Security Guidelines”
inglise keelne. tekst www.bsi.de/english/gshb/guidelines/guidelines.pdf

Dr. Udo Helmbrecht
BSI *(saksa k. Bundesamt für Sicherheit in der Informationstechnik, Saksamaa Infoturbeameti)* president

Käesoleval ajal põhinevad töö- ja äriprotsessid aina rohkem ja rohkem IT lahendustel. Seoses sellega muutub aina tähtsamaks infotehnoloogia ja sidetehnoloogia turvalisus ja usaldusväärsus. Õige infoturbe alane kontseptsioon kujutab endast kindlat alust usaldusväärsele infoturbele. Käesolev juhend aitab Teil sellise aluse luua: siin on kompaktses vormis esitatud ülevaade kõige tähtsamatest turvameetmetest. Samuti on siin ära toodud näited praktikast, mis samuti juhivad tähelepanu vajalikele organisatoorsetele, infrastruktuuri alastele ja tehnilistele meetmetele. Olukorra analüüsimiseks saate kasutada dokumendis esitatud kontrollnimekirju. Üks on kindel - suurema turvalisuse saavutamine on võimalik ka ilma suure IT eelarveta.

Käesolevas infoturbe soovituste juhendis on esitatud kompaktne ülevaade tähtsamatest organisatoorsetest, infrastruktuuri alastest ja tehnilistest IT turvameetmetest. Juhend on mõeldud IT juhtidele ja administraatoritele väikestes ja keskmistes ettevõtetes ning riigiasutustes.

BSI
Referaat I 1.4 Süsteemi turvalisus, etalonturve
Postkast 20 03 63
53133 Bonn
Tel.: +49 (0) 1888-9582-369
E-post: gshb@bsi.bund.de
Internet: http://www.bsi.bund.de

Sisukord

1 Sissejuhatus

21. sajandil on elu ilma infotehnoloogiata ja sidesüsteemideta pea mõeldamatu. Seetõttu muutub aina tähtsamaks IT süsteemide turvalisus. Ka muutuvad seadused tõstavad infoturbe tähtsust: juhatused ja firmajuhid on tegemata jätmiste ja puudulike turvameetmete korral isiklikult vastutavad.

Praktikas aga on enamasti keeruline saavutada ja tagada piisavat infoturbe taset. Sellel on mitmeid põhjuseid: puuduvad ressursid, ebapiisavad eelarved ja tegelikult ka IT süsteemide aina kasvav keerukus. Paljud infoturbe tooted ja infoturbe konsultandid pakuvad välja üsna erinevaid lahendusi, mille hulgas on ka ekspertidel raske orienteeruda.

BSI pakub juba aastaid omalt poolt informatsiooni ja abi infoturbe alastel teemadel: BSI IT etalonturbe juhend on muutunud kõige põhjalikumaks infoturbe alaseks standardväljaandeks. Paljud ettevõtted ja riigiasutused kasutavad seda juhendit tähtsa alusena oma organisatsioonis turvameetmete koostamisel. Analoogselt infotehnoloogia arenguga on ka IT etalonturbe juhend keerukamaks ja mahukamaks muutunud. Seetõttu vajavad eelkõige väikese eelarve ja vähese tööjõuga väikese ja keskmise suurusega ettevõtted sissejuhatust teemasse, mida on võimalik lihtsalt ja kiirelt rakendada.

Käesolev dokument täidab selle soovi, andes kompaktse ja lihtsasti mõistetava ülevaate tähtsamatest IT turvameetmetest. Juhendi tähelepanukeskmes on organisatoorsed meetmed ja ohtude väljatoomine praktiliste näidete varal. Tehnilised detailid on juhendist teadlikult välja jäetud.

Seega need, kes käesolevas juhendis toodud meetmeid rakendavad või IT teenuste pakkujatega lepingute sõlmimisel selle juhendi sisust lähtuvad, loovad endale ise kindla aluse usaldusväärsele infoturbele.

2 Üldist infoturbe kohta

Turvalisus on üks inimeste põhivajadusi ja seega ka üks ühiskonna põhivajadusi. Eriti just meie globaliseerumise, suureneva mobiilsuse ning tööstusriikide aina suurema infotehnoloogiast ja sidesüsteemidest sõltumise ajastul kerkib turvalisuse vajadus aina enam päevakorda.
Kasvav haavatavus ja IT riskide tulemusena suurte majanduslike kahjude tekkimise oht aina tugevdavad survet võtmaks ette ennetavaid tegevusi, et aktiivse infoturbe juhtimise kaudu vältida ja vähendada jääkriske. Vastutus ei ole kindlasti piiratud ainult osakondadega, õigem oleks öelda, et turvalisus on firmajuhi asi. Ka seadused tegelevad firmajuhtidega. Mitmed seadused ja määrused teevad firmajuhid ja juhatuse liikmed vajalike tegevuste mittetegemisel personaalselt vastutavaks. Üheks väga levinud eksiarvamuseks on, et IT turvameetmed toovad endaga kindlasti kaasa suured investeeringud turvatehnikasse ja kõrge kvalifikatsiooniga personali palkamisse. Tegelikult ei ole see nii. Kõige tähtsamad edu tagavad tegurid on üldine mõistmine, läbimõeldud organisatsioonireeglid ning usaldusväärsed ja hästi informeeritud töötajad, kes täidavad turvalisuse alaseid nõudeid iseseisvalt ja motiveeritult. Seega ei pea toimiva ja efektiivse infoturbe alase kontseptsiooni loomine alati hindamatult kallis olema. Kõige mõjuvamad meetmed on üllatavalt lihtsad ja sageli ka ei maksa midagi!
Teine laialt levinud eksiarvamus puudutab turvavajaduste taset. Sageli kohtab selliseid väiteid:

"*Meie juures ei ole kunagi midagi juhtunud.*" See on väga julge väide. Võib-olla lihtsalt ei märgatud varasemaid turvaintsidente!

"*Mida meilt siis ikka võtta on, nii salajased meie andmed nüüd ka ei ole.*" Selline hinnang on enamikul juhtudel liiga pealiskaudne. Võimalike negatiivsete stsenaariumide hoolikal läbivaatamisel saab kiiresti selgeks, et väga hästi võidakse saada andmeid, mida saab mitmel moel kuritarvitada.

"*Meie arvutivõrk on turvaline.*" Sageli alahinnatakse ründajate võimeid. Samuti tuleb arvestada, et ka kogenud IT spetsialist või võrguspetsialist ei tea kõigest kõike ja võib vahel ka vigu teha. Seetõttu on kõige parem korraldada väliseid teste, mis annavad kohe informatsiooni selle kohta, kui turvaline arvutivõrk siis tegelikult on.

“*Meie töötajad on usaldusväärsed.*.” Mitmesugused statistilised ülevaated annavad teistsuguse pildi: enamik turvarikkumisi pannase toime seestpoolt. Samas ei pruugi sellistel puhkudel alati pahatahtlikkusega tegemist olla. Ka lihtsad eksimused, üliinnukas või uudishimulik tegutsemine koos vähese probleemiteadlikkusega tekitavad vahel suuri kahjusid.

Igaüks peab endale teadvustama, et turvalisus ei ole muutumatu seisund, vaid pidevalt muutuv protsess. Esitage endale pidevalt neid küsimusi:

► Millistel viisidel saaks Teie firma või riigiasutuse käsutuses olevat tundlikku informatsiooni kurjasti kasutada?

► Mida tooks kaasa see, kui tähtsate andmete serveris hoidmise ajal või ühest kohast teise ülekandmisel neid muudetakse? Siin võib peale pahatahtlikkuse põhjuseks olla ka lihtsalt tehniline rike.

► Mis juhtuks, kui Teie organisatsioonis tähtsad arvutid või muud IT alased seadmed äkki rikki lähevad ja pikemat aega, näiteks mitu päeva või nädalat, kasutuskõlbmatud on? Kas Te saaksite tööd edasi teha? Kui suured oleksid võimalikud kahjud?

Hästi läbimõeldud turvakontseptsioonide rakendamisel saavutate teatud aja jooksul lisaks turvalisusele ka muid eeliseid. Sageli näevad IT osakonnad järgnevaid “kõrvalefekte”:

Töötajad on usaldusväärsemad, töökvaliteet tõuseb.

Korralik infoturve eeldab ka korralikku ettevõttekultuuri, millega on seotud vastutustundlik tegutsemine, klientidele orienteeritus ja ettevõtte eesmärkidele pühendumine.

Konkurentsieelised

Tugev infoturve avaldab positiivset muljet klientidele ja äripartneritele ning sageli on see ka nende poolt nõutav.

IT süsteemide hooldusele kulub varasemast märksa vähem aega.

Administraatorid töötavad efektiivsemalt.

Administraatorid ja kasutajad tunnevad kogu süsteemi paremini. IT süsteemid on hästi dokumenteeritud, see aga hõlbustab administreerimist, planeerimist, tarkvara paigaldamist ja vigade kõrvaldamist. Lisaks hoiab hea IT alane turvakontseptsioon ära mõned probleemid, mille all administraatorid tavaliselt eriti kannatavad: kasutajad kasutavad samadeks eesmärkideks erinevaid programme, kasutatakse erinevaid

operatsioonisüsteeme, sama tarkvara erinevaid versioone, igal kasutajal on oma individuaalsed arvutiõigused, kasutajad kasutavad oma isiklikku tarkvara ja konfigureerivad oma tööarvuti ise, ilma selleks piisavaid teadmisi omamata. Keskne arvutihaldus on sellises olukorras pea võimatu ning iga arvutit tuleb aeganõudvalt eraldi analüüsida ja kontrollida.

3 Tähtsamad infoturbe alased mõisted

Infoturbe kolm põhiväärtust on järgnevad: konfidentsiaalsus, käideldavus ja terviklus.
Konfidentsiaalsus: Tundlikud andmed peavad olema volitamata kasutamise eest kaitstud.
Käideldavus: Kasutaja saab talle tööks vajalikke teenuseid, IT süsteemi funktsioone ja informatsiooni tööks vajalikul ajal kasutada.
Terviklus: Andmed püsivad terviklikuna ja ilma volitamata muudatusteta.
Infotehnoloogias nimetatakse informatsiooniks andmeid, millele saab lisada vajalikku lisainformatsiooni, nagu näiteks autor või loomise aeg. Seega tähendab informatsiooni tervikluse kadu seda , et andmeid on ilma volituseta muudetud, autor on valesti määratud või andmete loomise aeg on teiseks muudetud.

Lisaks veel sageli kasutatavaid termineid:
Autentimine: Kui kasutaja hakkab IT süsteemi kasutama, peab süsteem tuvastama, kas tegemist on volitatud kasutajaga. Selleks kasutatakse enamasti kasutajatunnust ja parooli. Samuti kasutatakse seda terminit IT komponentide ja programmide kontrollimise kohta.
Autoriseerimine: Süsteem peab kontrollima, kas vastav kasutaja, IT komponent või programm tohib mingit kindlat toimingut teostada.
Andmekaitse: Andmekaitse all mõeldakse isiklike andmete kaitset nende kuritarvitamise eest (seda terminit ei tohi andmeturbega segamini ajada).
Andmeturve: Andmeturbe all mõeldakse andmetele nõutava konfidentsiaalsuse, käideldavuse ja tervikluse tagamist. Seda nimetatakse ka infoturbeks.
Varukoopia: Andmeturbe raames tehakse andmetest varukoopiaid, mida säilitatakse, et andmete kaotsimineku või hävimise korral saaks neid taastada.
Ründetest: Ründetest on reeglina simulatsioonina toimiv proovirünnak kontrollimaks, kui kergesti või raskesti ligipääsetav on IT süsteem väljastpoolt tulevatele kolmandatele isikutele. Seda testi kasutatakse infoturbe alaste meetmete efektiivsuse kontrollimiseks.
Riskianalüüs: Riskianalüüsi abil uuritakse, kui tõenäoline on mingite probleemide tekkimine ja millised oleksid nende probleemide tagajärjed.
Turvapoliitika: Turvapoliitika on firma või riigiasutuse ametlik dokument, millesse pannakse kirja kõik kaitse eesmärgid ja üldised turvameetmed. Üksikasjalikud turvameetmed kirjeldatakse mahukamas turvakontseptsioonis.

4 Eksimused: negatiivsed näited hoiatustena

1. näide: “Varukoopiaid ei ole”

Advokaadibüroo kasutab väikest arvutivõrku ühe kekserveriga, millesse salvestatakse kõik andmed. Serveril on lintseade, millega tehakse andmetest regulaarselt varukoopiad. Administraator hoiab varukoopiaid oma kabinetis lukustatud kapis. Kui ühel päeval serveri kõvakettaga rike toimub, siis tuleb andmed varukoopialt taastada. Siis aga selgub, et serveri lindiseade oli juba tükk aega rikkis ega salvestanud lintidele mitte midagi. Ainus kasutatav varukoopia on rohkem kui viis aastat vana. Seega on kõik viimaste aastate andmed kaduma läinud.

Administraator oli andmeturbe planeerimisel mööda vaadanud veel ühest ohust – isegi kui lindiseade oleks korralikult töötanud, oleksid näiteks tulekahju või muu sellise katastroofi korral lisaks originaalandmetele ka kapis seisnud varukoopiad hävinud!

Turvameetmed

- ► Varukoopiaid tegevate seadmete regulaarne kontrollimine
- ► Andmete varukoopiatelt taastamise testimine ja harjutamine
- ► Varukoopiate hoidmine väljaspool bürood, näiteks panga turvakapis

2. näide: “Arvutiviirusega nakatumine”

Ettevõttes kasutatakse kogu IT süsteemis viirustõrje tarkvara. Samas toimub selle tarkvara uuendamine juhuslikult, näiteks koos operatsioonisüsteemi uuendamisega. Ühel päeval saab IT osakond hoiatusteate uuest e-posti viirusest, mis levib laialdaselt Internetis aina rohkemate kasutajate kaudu. Ettevõttel aga ei ole konfigureeritud viirustõrje tarkvara automaatset uuendamist, mis võimaldaks hädaolukorras kõigisse arvutitesse kiiresti viimase viiruste signatuuride uuenduse paigaldamist. Hädaolukorra raames ühendatakse ettevõtte e-postiserver internetist lahti. Tegelikult aga on see viirus juba varem ettevõtte sisevõrku sattunud ja selle edasist levikut ei saa niimoodi tõkestada. Kuna see viirus kustutab kontoritarkvaraga loodud dokumente, siis tuleb kõik arvutid kohtvõrgust lahti ühendada ja välja lülitada, kuni IT osakond nad ükshaaval viiruste signatuuride uuendusega varustab ja juba viiruse ohvriks langenud arvutid suure vaevaga puhastab. Ettevõtte kogu IT tehnoloogia on mitmeks päevaks praktiliselt kasutuskõlbmatu. Andmete hävimise, tellimuste täitmisega hilinemise ja kadumaläinud tööaja tõttu tekivad märkimisväärsed majanduslikud kahjud. Varsti pärast nende taastamistööde lõppu ilmuvad Internetti esimesed viirusevariandid, mis ei ole suure

vaevaga uuendatud viirusetõrje programmile veel tuntud. Kogu taastamistöö tuleb uuesti teha.

Turvameetmed

► viirustõrje programmide automaatseks uuendamiseks peab olema välja töötatud vastav kontseptsioon

► ei tohi ära unustada ka eraldiseisvaid IT saarekesi, s.t. sülearvuteid ja test-arvuteid

3. näide: "Administraatoriga juhtub õnnetus"

Keskmise suurusega ettevõttes töötab üksainus administraator, kes on juba aastaid üksi ettevõtte tarkvara, riistvaraga ja arvutivõrguga tegelenud. Ühel päeval juhtub temaga aga õnnetus ja ta ei ole enam töövõimeline.

Juba mõne päeva pärast kuhjuvad arvutivõrgus serveriprobleemid: ilmuvad veateated ja hoiatused, millele töötajad ei oska õigesti reageerida. Lühikese aja pärast jäävad mitmed arvutid seisma ega hakka ka pärast taaskäivitust enam tööle. Kui seejärel hakatakse uurima administraatori dokumente, siis tuleb välja, et aastate jooksul ei ole ettevõtte IT süsteemi peaaegu üldse dokumenteeritud. Isegi administraatori paroolid ei ole üles kirjutatud. Ka kiiruga appikutsutud IT firma ei suuda paroolide ja dokumentatsiooni puudumise tõttu midagi teha. Nüüd tuleb aega- ja vaevanõudvalt välja uurida, millised programmid on serveritesse paigaldatud ja kuhu on salvestatud ettevõtte jaoks olulised andmed. Kasutada tuleb veelgi ettevõtteväliste ekspertide abi, sest lisaks levinud standardlahendustele kasutatakse serverites ka individuaalseid erilahendusi, mida appikutsutud IT firma ei ole kunagi varem kohanud.

Kui kõik on lõpuks taastatud ja igapäevaseks tööks vajalikud süsteemid on taas töökorras, siis on möödunud juba mitu nädalat. Sellel ajal ei olnud ettevõttes võimalik tähtsaid tellimusi täita, kuna selleks vajalikud andmed ja süsteemid ei olnud kasutatavad. Tekkinud kahjud koos väliste IT teenuste arvetega moodustavad kokku kuuekohalise summa. Selline kulutus ohustab juba ettevõtte olemasolu. Samuti tuleb eelmise administraatori asemele leida sobiv uus inimene.

Turvameetmed

► Süsteemi seadistused ja parameetrid tuleb põhjalikult dokumenteerida

► Paroolid tuleb üles kirjutada ja turvaliselt hoiule panna

► Suuremate probleemide jaoks tuleb välja töötada hädaolukorras toimimise protseduur

► Tuleb kehtestada ka asendustöötajate poliitika

4. näide: “Häkkerirünnak Internetist”

Psühholoogil on väikelinnas oma praksis. Patsientide isikuandmeid hoiab ta oma arvutis, millel on ka internetiühendus. Ta tunneb oma arvutit hästi ja paigaldab sellesse tarkvara enamast ise. Andmed hoiab ta enda teada turvaliselt, sest arvutisse pääsemiseks on vaja parooli. Ühel päeval aga levib väikelinnas kulutulena jutt, et keegi anonüümne isik on patsientide isiklikke andmeid avaldanud internetis kohalikus foorumis. Politsei jõuab oma uuringutega psühholoogini ja leiab, et tema arvuti oli Interneti kaudu toimuvate volitamata sissetungide eest täiesti ebapiisavalt kaitstud ning langes tõenäoliselt häkkerirünnaku ohvriks. Kohus esitab süüdistuse patsientide isiklike andmetega hooletus ümberkäimises. Patsientidele tekitatud kahjud aga on tohutud ja arvudesse teisendamatud.

Turvameetmed

► Interneti ligipääs peab olema turvatud

► Krüpteeri konfidentsiaalsed andmed

5. näide: “Firmasisene pahatahtlikkus”

Väike, traditsioonidel põhinev ettevõte valmistab juba aastaid erivärve ja –lakke, kasutades selleks saladuses hoitavaid valemeid. Ühel päeval aga vahetab üks turundusosakonna töötaja töökohta ja hakkab tööle konkurendi juures. Pool aastat hiljem tuleb konkurent turule peaaegu identsete lakkidega. Alguses on ebaselge, kuidas salajased valemid ettevõttest välja said, kuna tootearenduse osakond ei ole ühendatud ettevõttesisese arvutivõrguga ega ka Internetiga. Seetõttu hakatakse endist töötajat tööstusspionaažis kahtlustama ja esitatakse selle kohta ka politseisse avaldus.

Kriminaalpolitsei suudab oma vahendite ja meetoditega välja selgitada, et kahtlusaluse arvutisse oli just neid salajasi andmeid salvestatud ja need hiljem sealt kustutatud. Nende asitõendite ees seistes tunnistab kahtlusalune oma süü üles. Tootearenduse osakonna ruumid ei olnud öösiti lukus ja seetõttu sai iga töötaja, kellel oli maja võti, märkamatult ka sinna sisse. Süüdlane oli pärast tööpäeva lõppu tootearenduse ruumidesse sisenenud, boot-flopiketta abil parooli küsimisest mööda hiilinud ja andmetele ligipääsu saanud. Põhjuseks oli asjaolu, et tema uus tööandja oli

töölevõtuvestlusel esitanud küsimuse, kas tal on “väärtuslikke teadmisi selle tööstusharu kohta”, mis võiksid uuele tööandjale konkurentsieelise anda.
Nii vargale kui ka kahele uue töökoha juhatuse liikmele esitati kriminaalsüüdistus ning neile mõisteti tingimisi karistus. Ettevõtted leppisid kohtuväliselt kokku kahjude hüvitamises. Sellegipoolest oli väikeettevõte oma konkurentsieelisest ilma jäänud ning sattus seetõttu majandusraskustesse.

Turvameetmed

- ► Ruumid ja hooned tuleb volitamata sissetungide eest kaitsta
- ► Tähtsad andmed tuleb eraldi krüpteerida

5 Kõige sagedasemad puudused

Tüüpiliste vigade ja eksimuste analüüsimine on näidanud, et ettevõtte suurusel ja tegevusalal on vaid väike osa infoturbe alaste probleemide tekkimises. Järgnevas ära toodud puuduste nimekirja abil saate ka oma ettevõttes välja selgitada, mis vajab tähelepanu ja mida tuleb muuta. Käesoleva juhendi 6. peatükis käsitletakse neid puudusi veelkord ja näidatakse, kuidas konkreetseid turvameetmeid rakendades, saab neid mõõdukate kulutustega kõrvaldada.

5.1 Ebapiisav infoturbe strateegia

Turvalisusele omistatakse liiga vähest tähtsust

Infoturbele omistatakse muude nõudmiste kõrval (kulud, mugavus, suur funktsionaalsus jne.) sageli liiga vähest tähtsust. Selle asemel nähakse IT turvameetmetes midagi kulukat ja ebamugavat. Eriti just mis puudutab uusi oste, siis jäetakse rakenduste või süsteemide turvalisuse omadused sageli hooletusse või nendega ei arvestata. Sellel on mitmeid põhjuseid, nagu näiteks liiga vähene juhatusepoolne toetus IT turvameetmete rakendamisele, ebapiisavad teadmised infoturbest, uued arengusuunad ettevõtte tegevusalal, keskendumine turundusele, vähene eelarve, jne. Turvapuudused ei ilmne reeglina kohe. Selle asemel suureneb “kõigest” selle puudujäägiga seotud risk! Halvemal juhul lükatakse turvameetmete rakendamine kogu aeg määramatusse kaugusse edasi, kuna neile omistatakse iga kord madalam prioriteet võrreldes vahele tulnud muude tegevustega.
Üheks selliseks näiteks on täiesti turvamata traadita internetiühenduste kiire kasv, kuna vastavad WLAN-võrgukaardid on nüüd kõigile kättesaadavad. Vaimustus uuest tehnoloogiast ja vabadus segavatest juhtmetest paneb paljud turvaaspektid täiesti unustama. Lugematud firmad avalikustavad sel viisil tahtmatult oma tundlikud andmed ja pakuvad kõigile soovijatele tasuta ligipääsu Internetti.

Puuduvad pikaajalised protsessid turvalisuse taseme hoidmiseks

Turvalisusega tegeldakse sageli ainult isoleeritud üksikprojektide raames, mis on vajalikud spetsiifiliste ülesannete täitmiseks ja oma alal piisava asjatundlikkusega tegelemiseks. Samas unustatakse sageli tähelepanu pöörata ka nendele kõrvalprotsessidele, mille käigus säilivad projekti tulemused pikema aja jooksul

väljaspool põhiprotsessi. Näiteks teostatakse põhjalik nõrkade kohtade analüüs ja koostatakse korralik turvapoliitika, mida aga hiljem enam nii põhjalikult ei järgita. Samuti pannakse uute süsteemide kasutuselevõtul nende algsed parameetrid ja ülesanded rangelt paika, kuid hilisema töö käigus võivad need põhjalikult muutuda. Sellegipoolest kontrollitakse esialgsetele parameetritele vastavust harva. Sedasorti näiteid on arvukalt. Paljudel juhtudel on nende puuduste põhjuseks halb ettevõttesisene infoturbe haldus – osalt puuduvad selged vastutuspiirid turvameetmete rakendamisel, osalt aga ei kontrollita kokkulepitud turvameetmete rakendamist regulaarselt.

Turvameetmed ei ole dokumenteeritud

Paljudel suurtel institutsioonidel on kirjalikult paika pandud turvakontseptsioon ja juhised vastavate turvameetmete rakendamiseks. Enamikus väikestes ja keskmise suurusega ettevõtetes need aga puuduvad. Paljud juhised on liiga abstraktselt sõnastatud ja annavad liiga palju mänguruumi erinevatele tõlgendustele. Kui juhised ka olemas on, ei teavitata neist sageli kõiki, keda need puudutavad. Sageli puudub juhistel sageli siduvus, s.t. töötajad ei ole nende järgimist allkirjaga kinnitanud. Üksikutel juhtudel võib tulemuseks olla isegi see, et turvaolukorra rikkumised jäävad karistamata või on nende puhul raske karistust määrata.

Puudub kontrolli ja uurimise mehhanism turvapoliitika rikkumiste jaoks

Kehtestatud turvapoliitikad ja turvameetmed on efektiivsed ainult siis, kui nende täitmist saab kontrollida. Praktikas aga jääb selline kontroll sageli teostamata, kas tehnilistel, administratiivsetel või hoopiski juriidilistel põhjustel. Sama problemaatiline on olukord, kus töötajad ei pea turvalisuse rikkumiste puhul karistusmeetmetega arvestama. Need mõlemad puudused toovad lõppkokkuvõttes endaga kaasa kehtestatud turvapoliitika rikkumise ja lõpuks ka tegelikud kahjud.

5.2 Vead IT süsteemide konfigureerimisel

Kasutajaõiguste jagamisel ei ole piisavalt rangeid piiranguid

Üks infoturbe alaseid kuldreegleid on niinimetatud „teadmisvajaduse põhimõte”, mille kohaselt igale kasutajale (ja ka igale administraatorile) antakse ligipääs ainult neile andmetele ja programmidele, mida tal tööks vaja on. Praktikas tähendab see aga

administratiivset ja tehnilist lisatööd. Seetõttu on paljudel töötajatel ligipääs paljudele tundlikele andmetele ja programmidele, mida neil tegelikult vaja ei ole. Kuna ettevõtte töökohaarvutid ja serverid on tavaliselt kõik omavahel ühenduses, siis saavad kasutajad sageli ilma piirangute ligi ka teistele arvutitele ja andmetele peale enda omade, ilma et see nende andmete ametlikele kasutajatele teatavaks saaks. Nii rikutakse kogemata või tahtlikult ligipääsureegleid.

IT süsteemid on halvasti konfigureeritud

Praktikas tekib enamik turvaauke administreerimisvigade tõttu, mitte tarkvaravigadest tulenevalt. Kui standardprogrammide poolt pakutavad turvavõimalused täiel määral ja õigesti ära kasutataks, siis oleks ettevõtete turvalisuse tase palju kõrgem. Standardsete kontoriprogrammide keerukus kasvab päev-päevalt. Administraatorite jaoks on turvalisus vaid üks paljudest aspektidest, millega neil igapäevaselt tegeleda tuleb. Nad on praktiliselt veel vaevalt võimelised valesid ja ebaturvalisi parameetrite seadistusi täielikult ära hoidma. See dilemma on paljudele teada, kuid ilma ülemuste piisava toetuseta ei ole muutused reaalselt võimalikud.

5.3 Kohalike arvutivõrkude ja internetiühenduste ebaturvalisus

Tundlikud arvutisüsteemid on sageli avalikust võrgust ligipääsemise eest ebapiisavalt kaitstud

Niikaua kui informatsioon ja andmed on ainult ettevõttesiseses arvutivõrgus saadaval, piirneb probleemide korral võimalike süüdlaste ring ettevõtte enda töötajatega. Kui aga arvutid ka internetiga ühendatud on, siis saavad nõrku kohti ära kasutada ka anonüümsed kolmandad isikud, näiteks häkkerid. Programmide ja andmete internetist ligipääsu eest kaitsmine eeldab administraatoritelt eriteadmisi, ilma milleta on seadistusvead praktiliselt vältimatud. Sageli on tundlikud andmed, süsteemid ja arvutivõrgud avalike võrkude osas ebapiisavalt või üldse mitte kaitstud. Isegi tulemüüri olemasolu ei taga tegelikult turvalisust, kui nende seadistus ei ole õige. Paljud IT osakonna vastutavad isikud arvavad, et nende arvutivõrk on piisavalt kaitstud, tegelikkuses aga näitaks lihtne väline ründetest, et paljudel juhtudel esinevad tõsised turvaaugud.

5.4 Turvanõuete mittetäitmine

Turvameetmed jäetakse mugavusest täitmata

Ka parimad turvapoliitikad ja turvameetmed ei tähenda midagi, kui neid ei täideta. Sageli jäetakse tundlikud dokumendid ja e-post krüpteerimata, isegi kui selleks on olemas vastavad süsteemid. Samuti leitakse turvalised ja sageli muudetavad paroolid, nagu ka näiteks parooliga ekraanisäästjad, ebamugavad olevat. Mistahes helistaja, kes esitleb ennast IT osakonna uue töötajana, võib paroolid teada saada, kui ta neid enesekindlalt ja viisakalt küsib.
Andmetest tehakse harva varukoopiaid või ei tehta neid üldse, kuigi asjaosalistele on sellega seotud kõrge andmete kaotsimineku risk teada. Eriti puudutab see sülearvuteid. Isegi kui andmetest regulaarselt varukoopiaid tehakse, on need sageli ebatäielikud või vigased. Automaatsete varukoopiate puhul ei tea töötajad sageli üldse, millistest andmetest ja millisel hulgal varukoopiaid tehakse ning kui kaua neid andmekandjaid säilitatakse. Sedasorti näiteid on veel arvukalt ning need näitavad kujukalt, et isegi kõige lihtsamad turvameetmed loetakse ebavajalikeks, kui nende rakendamisele ei ole juhatuse toetust või tehnilist sundust. See kehtib nii kasutajate kui ka administraatorite kohta. Viimased jälgivad vaid harva, et kõik parameetrite seadistused oleksid piisavalt turvalised. Lisaks on administraatoritel sageli kogu süsteemile juurdepääsu võimaldavad arvutiõigused, sest neile on ebamugav end teist korda sisse logida, kuigi see tehniliselt turvalisem oleks.

Kasutajad ja administraatorid ei ole läbinud piisavat väljaõpet

Pidevalt muutuvad IT süsteemid ja programmid eeldavad kõigilt asjaosalistelt kõrget eneseinitsiatiivi uute teadmiste omandamiseks, mis süsteemi kompetentseks kasutamiseks vajalikud on. Aina keerukamate süsteemide vajalikul määral tundmiseks aga ei piisa enam „mängulisest” õppimisest, seda eriti testkeskkondades.
Kasutusjuhendid ei ole alati kättesaadavad ja sageli pole nende lugemiseks aegagi. Väljaõppeprogrammid ei hõlma sageli neid spetsiifilisi alasid, mida osalejad hiljem kasutama peavad hakkama. Lisaks on seminarid sageli liiga kallid ja nendes osalejad jäävad nendeks päevadeks oma firma tööst kõrvale. Detailsed süvateadmised eraldi aladel, nagu näiteks *Windows 2000*, *Lotus Domino* või *Apache*, on sageli ebapiisavad, sest arvesse tuleb võtta ka nende omavahelist koostoimet.

5.5 IT süsteemide halb hooldus

Saadaolevaid turvauuendusi ei paigaldata

Sageli ei võta administraatorid programmide saadavalolevaid turvauuendusi õigeaegselt kasutusele. Paljud viiruste poolt tekitatavad kahjud ilmnevad alles mõni aeg pärast vastava viiruse esmakordset avastamist. Selleks ajaks on reeglina olemas juba ka viirustõrjeprogrammide vastavad uuendused. Enamiku programmide puhul tulevad turvauuendused suhteliselt sageli välja. Samas aga kulub kõigi nende uuenduste pidevale valimisele ja kasutuselevõtmisele lisaaega. Paljud administraatorid ootavad selle asemel kuni järgmise regulaarse tarkvarauuenduseni. Selline käitumine aga on hooletu.

5.6 Hooletu ümberkäimine paroolidega ja turvamehhanismidega

Paroolidega käiakse liiga hooletult ümber

Enamik juurdepääsukontrolle teostatakse paroolide abil. Selle juures tekivad probleemid, kui kasutatakse liiga lühikesi ja kergesti ära arvatavaid paroole. Iga päev toimuvad sissetungid IT süsteemidesse, sest sissetungija on vastava parooli välja selgitanud, seda kas süstemaatilise proovimise teel, lihtsalt ära arvates või spionaaži teel. See, et paroole hoitakse tõepoolest klaviatuuri all või ülemises sahtlis, teeb kõrvalistele isikutele juurdepääsu eriti lihtsaks.

Olemasolevaid turvamehhanisme ei rakendata

Paljudel programmidel on oma turvamehhanismid, mida aga mugavuse, usaldamatuse või ühilduvusprobleemide tõttu ei rakendata või rakendatakse ebapiisaval määral. Selle näiteks on traadita võrguühenduste (WLAN) puhul olemasolev krüpteerimise funktsioon, mida aga harva kasutatakse.

5.7 Ebapiisav kaitse füüsiliste sissetungide ja materiaalsete kahjude tekitamise vastu

Ruumid ja IT süsteemid ei ole varguste ja vandalismi vastu piisavalt hästi kaitstud

Sissetungijad ja vargad saavad sageli liigagi lihtsasti ruumidesse sisse, sest aknad jäetakse ööseks praokile või IT ruumid jäetakse lukust lahti. Külastajate üle järelevalve puudumine või autosse jäetud sülearvuti pakuvad soovimatutele külalistele häid võimalusi. Samas on vargusest või vandalismist tingitud riistvarakahjud palju väiksemad kui sellega kaasnevast andmete kadumaminekust tulenevad kahjud. Ühelt poolt on andmeid väga raske taastada, teiselt poolt aga on alati oht, et varas tundlikke andmeid ära kasutab. Sellised katastroofid nagu tulekahju või uputus tulevad küll harva ette, kuid nende põhjustatud kahjud on enamasti saatusliku ulatusega. Seetõttu peab ka tuleohutusreegleid, vee vastast kaitset ja elektriühenduse ohutust võtma kui infoturbe tähtsaid osi.

6 Olulisemad turvameetmed

6.1 Süstemaatiline lähenemine infoturbele

Vajalik tähelepanu infoturbele

1.	**Infoturbega seotud aspektid tuleb kõigi projektide puhul juba varakult ja piisava tähelepanuga arvesse võtta.**

Programmide võimalikult head kasutusvalikud ja kõrge funktsionaalsus, nende kasutusmugavus, madalad soetuskulud ja hoolduskulud ning infoturve on peaaegu alati omavahel vastuolus. Sellegipoolest on alati soovitatav juba projekti alguses (nt. uue tarkvara loomisel või äriprotsesside planeerimisel) pöörata tähelepanu infoturbele. Eriti just uusi tehnoloogiaid ei tohi ilma neid kriitilise pilguga üle vaatamata kasutusele võtta. Selle juures on hädavajalikuks eelduseks infoturbe selge toetamine juhtkonna poolt! Hiljem esile kerkivad turvapuudujäägid võivad endaga kaasa tuua ebameeldivaid tagajärgi. Kui projekteerimisvead või planeerimisvead alles hiljem välja tulevad, siis on nende kõrvaldamine sageli juba ebapraktiliselt kallis või hoopiski võimatu. Julgus mugavuse või funktsioonide osas kompromisse teha võib hiljem säästa palju kulusid seoses turvaprobleemidega või täiendavalt suuri investeeringuid infoturbesse.

2.	**Ebapiisavate ressursside korral tuleb otsida sobivaid alternatiivseid lahendusi.**

Sageli viib ühe eesmärgini mitu teed. Kulukad ja aeganõudvad projektid on vastuvõtlikumad riskile, et need rahanappuse, ajapuuduse või muutunud nõudmiste tõttu seisma jäävad. Seetõttu tuleb alati arvestada ka alternatiivsete lahendusvariantidega, mida saab vajadusel rakendada. Palju väikseid samme on lihtsam teostada kui üht suurt. Ka see on üks infoturbe aspekt.

Samm-sammult parema infoturbe suunas

3.	**Infoturbe eesmärgid tuleb kindlaks määrata, siis saab määrata ka turvameetmed nendeni jõudmiseks.**

Infoturbes esimeseks sammuks on olukorra kindlaksmääramine:

- ► Millised on olemasolevad raamtingimused (seadused, lepingud, klientide nõudmised, konkurentsiolukord)?
- ► Milline on IT osakonna ja infoturbe roll selles ettevõttes või ametkonnas?
- ► Milliseid väärtusi tuleb kaitsta (teadmised, ärisaladused, isiklikud andmed, IT süsteemid)? Millised on tekkida võivad kahjustavad sündmused?

Kaitsevajaduse kindlaksmääramine on igasuguse turvaanalüüsi hädavajalikuks osaks. Selle käigus tuleb tagada, et määratletud kaitseeesmärgid ja nendest tulenevad turvameetmed on piisavad ja sobivad olemasoleva olukorraga. Kuna raamtingimused võivad aja jooksul muutuda, siis tuleb regulaarselt kontrollida, kas kindlaks määratud kaitsevajadus vastab veel tegelikkusele. Kaitsevajaduse kindlaksmääramisel on abiks infoturbe kolmele põhiväärtusele orienteerumine: konfidentsiaalsus, käideldavus ja terviklus.

4.	**Igale olemasolevale turva-eesmärgile ja igale selle juurde kuuluvale turvameetmele tuleb määrata vastavad reeglid.**

“Infoturve on pikaajaline protsess.” See lause ütleb väga hästi ära põhilise probleemi: enamikku infoturbega seotud meetmeid tuleb regulaarselt üle vaadata ja uuendada. Iga turvameetme puhul tuleb kindlaks teha, kas seda tuleb rakendada üks kord või korduvalt (näide: viirustõrje programmi ja selle viiruste andmebaasi regulaarne uuendamine).

5. **Tuleb koostada tegevusprotseduur, mis sätestab selged prioriteedid nii turvaeesmärkidele kui turvameetmetele.**

Need, kes on mõnda aega mõelnud, milliseid mõistlikke samme infoturbe heaks ette võtta, leiavad varsti, et nad ei jõua ajaliselt ega finantsiliselt kõiki soovitud meetmeid rakendada. Seetõttu on vajalik määratletud turvaeesmärkidele ja turvameetmetele selged prioriteedid seada, mis võtavad arvesse ka kulude-kasulikkuse suhet.

6. **Eriti paljunõudvaid turvameetmeid tuleks vältida.**

Võimaluse korral tuleks alati valida sellised turvameetmed, mille rakendamine on praktiline ja mis ei tundu asjaosalistele ebareaalsed või mõttetud. Seejuures on iseenesestmõistetav, et soovitud turvameetmete rakendamiseks peab olemas olema ka sobiv tehniline ja organisatoorne infrastruktuur, muidu tekib oht, et kogu turvapoliitikat ei võeta enam tõsiselt ja hakatakse seda eirama. Kahtluste korral peaksid turvameetmed pigem natuke leebemad olema ja see-eest nende järgimise kontroll rangem olema. Samuti on soovitatav kõiki selliseid turvameetmeid, mis kellegi tööd eriti mõjutavad, asjaosalistega eelnevalt arutada.

7. **Vastutusalad tuleb kindlaks määrata.**

Iga turvameetme korral tuleb kindlaks määrata, kes selle rakendamise eest vastutama hakkab. Samuti tuleb iga turvameetme korral kindlaks määrata, millisele ringkonnale see siduv on: kas seda hakkavad rakendama ainult põhikohaga töötajad, ettevõtte mingi kindel osakond või kõik töötajad?
Igale vastutavale isikule tuleb kindlasti määrata asetäitja. Seejuures on tähtis, et asetäitja suudaks selle vastutava isiku ülesandeid kompetentselt täita. Kas ta tunneb neid ülesandeid? Kas vajalikud paroolid on hädakorra puhuks turvaliselt kõrvale pandud? Kas on vaja mingit täiendavat dokumentatsiooni?

8.	**Kehtivad turvapoliitikad ja vastutusalad tuleb kõigile teatavaks teha.**

Ettevõtetes korraldatavate infoturbe alaste töötajaküsitluste käigus tuleb sageli välja, et turvapoliitikast teatakse vähe või üldse mitte midagi. Samuti on nende olemasolu üldse vähetuntud. Seetõttu tuleb alati kindlaks teha, et kõik turvameetmega seotud isikud oleksid sellest meetmest ja meetme hetkekujust teadlikud. Kõik töötajad peavad teadma oma ettevõttesiseseid ja –väliseid kontaktisikuid ja nende kompetentsi. See võimaldab mitte ainult probleemide korral kiiresti abi saada, vaid ka väldib seda, et keegi kõrvaline isik töötajatelt hea veenmiskunsti või hirmutamise teel tundlikke andmeid, nt. paroole, teada saab.
Siinjuures tuleb arvesse võtta ka juriidilisi aspekte, et turvapoliitika rikkumisel ei ilmneks, et süüdlane oma teadmatusele rõhudes karistuseta jääb. Vajadusel tuleks lasta kõigil töötajatel turvapoliitikale selle läbilugemise järel alla kirjutada.

Infoturbe seire ja infoturbe taseme säilitamine:

9.	**IT turvalisust tuleb regulaarselt kontrollida.**

Infoturbe tegelikku taset tuleb regulaarselt kontrollida. Kui eelarve on selleks piisav, siis tuleks mõelda sellele, kas ehk korraldada igal aastal sõltumatute välisekspertide poolne ülevaatus eriti kriitilistele infoturbe alastele aspektidele. Alati tuleb tulevikku vaadata: kas on uusi turvastandardeid või uusi olulisi tehnoloogiad? Kas klientide või partnerite nõudmised on vahepeal muutunud?

10.	**Kehtivate töövõtete ja turvameetmete otstarbekust ja efektiivsust tuleb regulaarselt kontrollida.**

Protsesside ja juhiste pidev optimeerimine ei ole ainult IT alaste vastutavate isikute ülesanne. Turvapoliitika koostamisel on kolm peamist ohtu: see võib olla vananenud meetmetega, ebatäielik või ebapraktiline. Just omaksvõtmise huvides ei tohi turvapoliitika olla ebamugav ega mõttetu tunduda. Sellest vaatenurgast lähtudes tuleb

üle kontrollida kõik infoturbega seotud töövõtted. Siinjuures on asendamatu selle töövõttega tegelevate isikute individuaalne arvamus. Kui küsitluse tulemused näitavad, et mingi meede loetakse ebaotstarbekaks, siis tuleb koostööna selle põhjused ja lahendused leida.

Edasised sammud:

Kahe järgneva turvameetme tähtsus sõltub tugevasti ettevõtte või ametkonna suurusest. Mida rohkem töötajaid nendega seotud on, seda vajalikumad ja mõttekamad on need turvameetmed.

11.	**Pikas perspektiivis tuleb koostada kõikehõlmav turvapoliitika.**

Eriti just suurtes organisatsioonides saab head infoturbe taset alal hoida ainult siis, kui samm-sammult koostatakse kõikehõlmav turvapoliitika. See peab hõlmama eelnimetatud turvameetmeid, kuid mitte ainult neid, vaid peab minema veel palju kaugemale. Küsitlused on näidanud, et kõikehõlmava turvapoliitikaga organisatsioonides on turvaolukorra rikkumisi oluliselt vähem.

12.	**Kõik kehtivad turvameetmed peavad olema kirjalikult turvakontseptsioonis sätestatud.**

Soovitav on organisatsiooni turvapoliitika kirjalikult vormistada. Selleks on Internetis ja kirjanduses nüüdseks piisavalt näiteid, mida saab vabalt kasutada ja enda vajadustele kohandada. Vahel on lihtsam võõras ja hästi struktureeritud turvapoliitika üle võtta ja enda vajadustele kohandada kui oma ajalooliselt kasvanud, halva struktuuriga ja osaliselt iseendale vastukäivat turvapoliitikat parandama hakata.
Selliseid turvapoliitikaid on kõige parem üle võtta ja kohandada, kui need on hoolikalt mitmesse (vähemalt kolme) tasemesse jaotatud:
Kõige ülemine ja kõige abstraktsem tase kirjeldab ainult üldisi turvaeesmärke ja võtab kokku ettevõtte infoturbe alase filosoofia. See koosneb vaid mõnest leheküljest, on juhatusele vastuvõetav ja peakski juhatuse poolt välja antud olema.

Teine tase kirjeldab üksikasjalikult turvaeesmärke, tehnilisi nõudeid ja vastavaid turvameetmeid. See osa peab olema võimalikult üksikasjalik, ilma seejuures programmide tehnilisi üksikasju ja omadusi puudutamata. Nii ei ole programmide ja IT lahenduste muutumisel vaja iga kord turvaeesmärke ümber kirjutada.
Kolmandal tasemel kirjeldatakse teisel tasemel ära toodud turvameetmete konkreetset rakendamist konkreetsete programmidega ja mehhanismidega. Kui mingit kasutatavat programmi muudetakse, siis tuleb ka turvapoliitika seda kihti koheselt muuta. Kahjuks tuleb siin sageli ette olukordi, kus varem kirjeldatud turvameetmeid ei saa programmide funktsionaalsuse või ebapraktilisuse tõttu ellu rakendada. Sellisel juhul tuleb kas turvameetmed veel kord läbi vaadata või hakata kasutama mingit muud IT lahendust. Selge on see, et turvameetmete rakendamisel tekkivad puudujäägid tuleb igal juhul korrigeerida. Kõiki asjaosalisi tuleb sellest teavitada, et nad oskaksid tekkinud riski õigesti hinnata.

6.2 IT süsteemide turvalisus

13.	**Olemasolevaid turvamehhanisme tuleb kasutada.**

Paljudel kliendi ja serveri põhistes võrkudes andmesideks kasutatavatel programmidel on suurepärased turvamehhanismid. Peaaegu alati on turvaaukude põhjuseks valesti seadistatud programmiparameetrid või ebapiisavad teadmised turvamehhanismide kohta. Seetõttu tuleb programmidega kaasasolevaid turvamehhanisme analüüsida, tundma õppida ja kasutusele võtta. Nii saab ka selliseid turvameetmeid tehniliselt sunduslikuks teha, mida muidu ainult kokkuleppe alusel täidetakse.

14.	**Viirustõrje programmid peavad hõlmama kogu IT süsteemi.**

Uuendatud viirustõrje programmid on asendamatud. Arvutiviirused võivad levida andmekandjatel ning ka interneti ja kohaliku arvutivõrgu kaudu. Viirustõrje programmid on kohustuslikud ka ilma internetiühenduseta arvutites!
Soovitatav on kogu e-post ja igasugune andmeside kõigepealt keskserveris viirustõrje programmil üle kontrollida lasta. Lisaks peab igas arvutis olema kohalik viirustõrje

programm, mis kogu aeg taustal töötab. Reeglina piisab sellest, kui kohalik programm taustana töötades ainult parajasti kasutatavaid andmeid, programme, makrosid jne. jooksvalt kontrollib. Sellegi poolest on soovitatav lasta viirustõrje programmil regulaarselt kogu arvuti põhjalikult üle kontrollida (nt. enne igapäevast või igakuist andmetest varukoopiate tegemist). Tegeliku viirusejuhtumi korral on kogu arvuti põhjalik kontrollimine alati hädavajalik!
Ajakohased soovitused ja põhjaliku taustainformatsiooni leiate BSI veebilehelt pealkirja "*Computer-Viren*" ("Arvutiviirused") alt.

Tähelepanu:
Isegi juhul, kui Teie viirustõrje programm on alati uuendatud, ei paku see siiski kunagi absoluutset kaitset, sest teie arvuti on alati uutele viirustele vastuvõtlik niikaua, kui viirustõrje programmi autorid neid veel ei tunne ja vastavat uuendust välja ei ole andnud. Ka niisugused programmid on ohtlikud, mis ei ole küll viirused, kuid levivad Interneti teel ja on selliselt konstrueeritud, et suudavad end kõrvaldamata turvaaugu kaudu otse arvutisse paigaldada. Selliste programmide kuulsamaks näiteks on ussprogramm "Lovsan" (W32.Blaster.Worm), mis kasutas ära operatsioonisüsteemides Windows 2000 ja XP olemasolevat turvaauka. Selle ussprogrammi pidas kinni ainult rangelt seadistatud parameetritega tulemüür, e-posti kontrollimine tulemusi ei andnud.

15.	**Ligipääs andmetele tuleb viia minimaalsele tasemele, mis normaalseks tööks vajalik on.**

Üheks infoturbe kuldreegliks on teadmisvajaduse põhimõte ("*need-to-know*"): igal kasutajal ja administraatoril peab olema just selline ligipääs andmetele ja programmidele kui tal oma tööks vaja on, ja mitte rohkem. Siia juurde kuulub ka nõue, et ühe osakonna informatsioon ei ole nähtav teise osakonna töötajatele, kui nad seda oma normaalseks tööks ei vaja. Rakendusprogrammide, eriti süsteemi administreerimise programmide, kasutamine peab samuti olema piiratud nende töötajatega, kellel neid oma normaalseks tööks vaja on.
Selle põhimõtte rakendamine on suurema vaevata teostatav: vajalikud volitused võetakse sobivate volitusprofiilidena kokku ning nende põhjal määratletakse sobivad kasutajagrupid ja kasutajarollid. Iga kasutaja arvutiõigusi saab sel viisil volitusprofiili

kaudu lihtsasti reguleerida – kasutaja peab kuuluma vastavasse kasutajagruppi. Regulaarselt tuleb kontrollida, kas lubatavad arvutiõigused vastavad kasutajate tegelikele vajadustele. Arvutiõiguste kohta kergemini ülevaate saamiseks võib kasutada vastavaid programme, mis kogu arvutivõrgu regulaarselt üle kontrollivad. Nii leiate ka need ressursid, mis võiksid muidu kolmandatele isikutele kättesaadavateks osutuda. Paljud sellised programmid on tasuta saadaval.
Samuti tuleb kehtestada sobiv protsess töötajate töölevõtmisel ja nende lahkumisel arvutiõiguste komplektina andmiseks ja äravõtmiseks.

16.	**Kõigile süsteemi kasutajatele tuleb määrata kasutajaroll ja kasutajaprofiil.**

Juurdepääsuõiguste andmisel ei tohi uisapäisa toimida, muidu tekib suurte kasutajahulkade puhul varem või hiljem vaevaline kasutajate haldus, keerukad kasutajastruktuurid ja sellele vastavalt ka suured veavõimalused. Peaaegu kõigil standardprogrammidel on võimalus sobivaid kasutajaprofiile määratleda ja nende abil sobivad kasutajarollid luua. Igale kasutajale ja igale administraatorile antakse üks või mitu rolli, mida ta oma töös kasutada saab. Ühelt poolt on niimoodi kasutajate haldus lihtsam ja seega ka turvalisem ning teiselt poolt võimaldab see suuremat paindlikkust, sest ühele ja samale isikule saab sõltuvalt rollist erinevad kasutusõiguste komplektid määrata.

17.	**Ka administraatorite õigused tuleb viia miinimumini, mis neil normaalseks tööks vajalik on.**

Paljud süsteemiadministraatorid töötavad administraatori õigustes, mis annab neile praktiliselt piiramatu ligipääsu ja kõik süsteemiprivileegid. See annab aga samas ka administraatorile endale või tema rolli ülevõtmisel kellelegi volitamata isikule võimaluse süsteemi ärakasutamiseks. Seetõttu tuleks võimaluse korral erinevad administraatorite ülesanded üksteisest eristada ja erinevatele rollidele omistada, näiteks ühele administraatorile ainult printeritega tegelemine, teisele administraatorile ainult uute kasutajate loomine, kolmandale ainult andmetest varukoopiate tegemine. Ideaaljuhul on olemas ka eri-administraator, kes tegeleb protokollimisega ja jälgib teiste administraatorite tegevust.

18. Programmide juurdepääsuõigusi tuleb piirata.

Analoogselt kasutajatega on ka käivitatavatel programmidel oma juurdepääsuõigused ja süsteemiprivileegid. Paljudel juhtudel saab programm lihtsalt vastava kasutaja juurdepääsuõigused, kuid vahel ei piisa nendest programmi tööks või on tegemist serveriprotsessiga, millele tuleb kõrged privileegid anda. Sellistel juhtudel on programmidel vahel nn. juurkataloogi-õigused ning nad võivad kõikvõimsa süsteemiadministraatori kombel kõiki süsteemiressursse kasutada. Kui selline programm kellegi välise sissetungija poolt kasutusse võetakse, siis on ka temal kõik selle programmi suured võimalused. Seega tohib ka programmidele anda ainult sellised õigused, mis nende tööks hädavajalikud on.

19. Tehases konfigureeritud standardseadistused tuleb alati ära muuta.

Paljud operatsioonisüsteemid ja programmid on nende autorite poolt selliselt seadistatud, et nende arvutisse paigaldamise järel saaks neid võimalikult kohe ja mugavalt kasutama hakata. See kehtib ka IT komplektide ja sidesüsteemide kohta. Kahjuks ei ole autoripoolsete standardseadistuste valimisel IT turvalisusega üldse arvestatud. Kahtlemata on sellised standardseadistused mugavad neile, kes ei ole selle programmiga veel piisavalt tuttavad. Standardseadistuste puhul on programmi funktsionaalsus võimalikult vähe piiratud ja võimaldab vaba andmesidet kogu ümbritseva keskkonnaga. Sageli on kasutusel isegi standardparoolid ja standard-kasutajanimed. Turvalisuse huvides tuleb need kõik välja lülitada või ära muuta. Äsja paigaldatud ja veel kohalike turvameetmete kohaselt ümber seadistamata süsteemi ei tohi kunagi tegelikku kasutusse võtta!

Tähtsad serverid ja olulisemate arvutite operatsioonisüsteemid peavad olema tugevdatud turvalisusega. See tähendab kõigi niisuguste tarkvaraosade ja funktsioonide eemaldamist, mis programmi normaalseks tööks hädavajalikud ei ole. Sageli saab sissetungija serverisse ligipääsu mingi programmi kaudu, mis ei peaks üldse sellesse serverisse paigaldatud olema. Pealegi kulub arvuti regulaarseks

hooldamiseks ja uuendamiseks rohkem aega, kui selles on mingeid üleliigseid programme. Seetõttu tuleks kõik ebavajalikud programmid arvutitest eemaldada. Sama kehtib ka operatsioonisüsteemi enda töövahendite, draivertarkvarade, osade jne. kohta. Äärmusliku abinõuna saab eraldi eemaldada isegi ebavajalikud käsud, s.t. operatsioonisüsteemi mingid kindlad protsessid.

20.	**Kasutusjuhendid ja programmide dokumentatsioon tuleb enne kasutama hakkamist hoolikalt läbi lugeda.**

Kogenud administraator suudab paljudel juhtudel süsteemi ka ilma kasutusjuhendeid lugemata tööle saada. Selline edu on aga sageli petlik – nii võivad näiteks programmi autori poolsed hoiatused teadmata jääda ja hiljem võib nende põhjal probleeme tekkida: ühilduvusprobleemid, süsteemi seiskumised, avastamata turvaaugud. Programmi autori poolsete abivahendite ja informatsiooni tähelepanuta jätmine ja selle kaudu ebavajalike riskide tekitamine on hooletu ja ebaprofessionaalne.

21.	**Programmide paigaldamise ja süsteemi kui terviku kohta tuleb pidada dokumentatsiooni ja seda regulaarselt uuendada.**

Soovitatav on kõik programmi paigaldamisele eelnevad, käigushoidmise ja sellele järgnevad toimingud kirja panna. See aitab korduval paigaldamisel edaspidi kiiremini sihile jõuda ja probleemi korral võimaliku põhjuse leida. Samuti on tähtis, et programmi dokumentatsiooni vaataks üle keegi volitatud kolmas isik, näiteks abiadministraator või asetäitja, veendumaks, et dokumentatsioon on järgitav ja arusaadav. Nii on probleemid väiksemad kui põhiadministraator äkitselt töövõimetuks muutub. Samuti on häkkerirünnaku korral lihtsam volitamata süsteemimuudatusi leida.

6.3 Arvutivõrgud ja internetiühendused

Enamiku interneti ligipääsuga kasutajate jaoks on e-posti programm ja interneti brauser kaks kõige tähtsamat töövahendit. Pole ka ime, et just siin varitseb kõige rohkem ohte. Andmete internetist arvutisse salvestamisel võivad kaasa tulla ka kahjulikud programmid, mida viirustõrje programm ära ei tunne. Internetis liikudes

võidakse kogemata käivitada soovimatuid protsesse – eriti siis, kui aktiveeritakse riskantseid aktiivseid kirjalisandeid (vt. ka turvameedet nr. 26) ja neil töötada lastakse.

BSI kodulehelt leiate teema “*Internet-Sicherheit*” (“Turvalisus Internetis”) alt mitmesugust täiendavat informatsiooni, uuringuid ja näiteid.

22.	**Arvutivõrkude kaitseks tuleb kasutada tulemüüri.**

Ükski arvuti, mida äritegevuseks kasutatakse, ei tohi ilma kohaliku tulemüürita Internetiga ühendatud olla!
Ka suuremate kohtvõrkude puhul on enamasti mitmeid osavõrke omaette kasutajagruppidega ja erinevate kasutusvajadustega. Seetõttu tuleb kohalik võrguosa teistest tulemüüriga eraldada, et vältida võimalikke ohte, mis on võrreldavad ka interneti kaudu sissetungijate ohuga. Nii näiteks tuleks personaliosakonna võrguosa eraldada ülejäänud ettevõtte kohtvõrgust. Seetõttu tuleb ka nendele võrguüleminekutele paigaldada turvamehhanismid.

Mis on tulemüür?

Tulemüür on riistara või tarkvara, mis jälgib arvutite või arvutivõrkude vahelist ühendust ja hoiab ära eriti internetist tulevad rünnakud. Tulemüüride valik algab lihtsatest tasuta programmidest, mis kaitsevad põhiliselt seda arvutit, millesse nad paigaldatud on. Suurtes arvutivõrkudes aga kasutatakse keerukaid tulemüürisüsteeme, mis koosnevad mitmetest riistavalistest ja tarkvaralistest osadest.

23.	**Turvaline tulemüür peab vastama teatud miinimumnõuetele.**

Kohaliku võrguosa kaitsmiseks teiste võrkude (s.t. vähem usaldatavate võrkude) eest tuleb valida sobiv tulemüüritüüp. Tulemüüride süsteemi arhitektuuri valik ja tulemüüride paigaldamine peab jääma vastava ala spetsialistide hooleks.

Reeglina on soovitatav kasutada mitmeastmelise tulemüüri kontseptsiooni, mille puhul ühendatakse tulemüüri ette ja järele täiendavad filtreerivad elemendid, näiteks ruuterid. Kui näiteks tuleb kaitsta ainult ühte arvutit või kui keerukamat tulemüürisüsteemi ei saa mingil põhjusel kasutada, siis pakub lihtsama tulemüüriprogrammi kasutamine vähemalt minimaalset kaitset.
Tulemüüride filtreerimisreeglid kipuvad aja jooksul aina pikemaks ja ebaülevaatlikumaks muutuma. Tulemüüre haldavad administraatorid annavad kasutajate soovidele sageli liiga kergesti järele ja pehmendavad filtreerimisreegleid. Tegelikult ei tohiks erandeid teha ka firmajuhile! Seetõttu tuleb regulaarselt kontrollida, kas kehtivad filtreerimisreeglid on veel kooskõlas, kas neid saaks lihtsustada ja kas nad vastavad veel tegelikele filtreerimisvajadustele. Lisaks tuleb aeg-ajalt kontrollida, kas kehtiv tulemüürisüsteem sobib oma turvalisuselt juba kasutuselevõetud või lähitulevikus kasutuselevõetavatele uutele andmesideprotokollidele. Samuti võivad uued tehnoloogiad tulemüürisüsteemidele uusi nõudmisi esitada. Üksikasjalikku informatsiooni tulemüüride kohta saate IT etalonturbe juhendist ja BSI veebilehelt.

Lisainformatsioon tulemüürisüsteemi arhitektuuri kohta

Ka tulemüür võib rünnaku ohvriks langeda. Sellisteks puhkudeks ongi vajalikud mitmeastmelised tulemüürisüsteemid, et ühe tulemüüri äralangemisel ülejäänud süsteemiosad vähemalt minimaalset kaitset pakuksid.

Sellistele serveritele, mis oma tööülesannete tõttu Internetiga otsesuhtluses on ja Internetist ainult tulemüürisüsteemiga või muu kaitsemehhanismiga (nt. proxy) eraldatud on, paigutatakse niinimetatud “liivakasti” (“Demilitarised Zone”, DMZ). Sel juhul on väga tähtis sellise serveri õige hierarhia ja struktuur.

24.	**Ettevõttest väljapoole ligipääsetavaks tehtavate andmete hulk peab võimalikult minimaalne olema.**

Lugematul hulgal tundlikku informatsiooni tehakse volitatud kasutajatele ka avaliku võrgu kaudu kättesaadavaks. See aga tähendab, et sellele informatsioonile võib ligi pääseda ka volitamata isik. Nende andmete kaitse põhineb ainult tuvastamise ja volitamise mehhanismidel. Kui need aga on valesti seadistatud või on neis mingi

turvaauk, siis satuvad ka kaitsealused andmed kergesti valedesse kätesse. Sellised vead on kahjuks pigem reegel kui erand. Seetõttu tuleb kõigepealt määratleda, kas ja milliseid andmeid on üldse vaja väljaspool kohtvõrku kättesaadavaks teha.

25.	**Ettevõttest väljapoole ligipääsetavaks tehtavate teenuste ja programmifunktsioonide hulk peab võimalikult minimaalne olema.**

Kõik funktsioonid, serveriteenused ja avatud andmesideühendused (pordid) suurendavad võimaliku turvaaugu riski. Seetõttu tuleb iga kord hoolikalt üle vaadata, kas mingit potentsiaalset probleemide kandidaati on mõtet aktiveerida ja väljapoole ettevõtet kättesaadavaks teha. Sõltuvalt kasutatavast tehnoloogiast ja selle rakendamisest võib niisugustel juhtudel tegelik turvarisk väga erineva tõsidusega olla. Olemasolevate süsteemide korral tuleb regulaarselt kontrollida, ega mõni soovimatu teenus või funktsioon ei ole lihtsalt kogemata või ka mugavusest aktiveeritud, kuigi seda tegelikkuses keegi ei kasuta. Selle turvameetme kaudu väheneb administraatorite töökoormus ja nad saavad rohkem vajaminevate protsesside turvalisusele pühenduda.

26.	**Interneti-brauseri kasutamisel tuleb eriti ettevaatlik olla, kõik riskantsed tegevused tuleb ära jätta.**

Interneti-brauseri puhul tohib aktiivseks jätta ainult sellised aktiivsisud, skriptid ja multimeedia-lisad, mis on kasutaja tööks hädavajalikud. Eriti riskantsed skriptikeeled tuleb igal juhul välja lülitada.

Täiendav informatsioon

Uute tehniliste lahenduste ilmumisega võib ikka ja jälle muutuda, milliseid skripte, protokolle ja lisasid ei tohiks sisse lülitada. Uusimat informatsiooni riskantsete tehnoloogiate kohta leiate BSI veebilehelt. Praegusel hetkel on eriti ohtlikud ActiveX, Active Scripting ja JavaScript.

27.	**E-posti kirjalisandite puhul tuleb eriti ettevaatlik olla.**

Saadud e-posti kirjalisandid võivad eriti ohtlikeks osutuda, kui need soovimatult käivitatakse. Ükski kasutaja ei tohi ilma kontrollimata avada ühtki kirjalisandit, milles ta täiesti kindel ei ole. Viirustõrje programmi kasutamine on siinjuures kohustuslik! Kahtluste korral peab kirja saaja enne kirjalisandi avamist kirja saatjalt aru pärima. Eriti ohtlik on siinjuures asjaolu, et mõned e-postiprogrammid avavad kirjalisandeid automaatselt, ilma kasutaja käest küsimata. Selle tehnilisel viisil vältimiseks tuleb kasutada ilma seesuguse funktsioonita e-postiprogrammi, programmi vastavat seadistust või täiendavat lisaprogrammi.

28.	**Enamiku Interneti kasutamisega seotud turvaprobleemide vältimisel on odavaks lahenduseks eraldiseisva, ainult internetis liikumiseks mõeldud arvuti kasutamine.**

Lihtsaks ja odavaks võimaluseks Internetis liikumisega kaasnevate arvukate ohtude vähendamiseks on eraldi arvuti ülesseadmine, mis on ühendatud internetiga, kuid ei ole ühendatud kohtvõrguga. Seda saab internetist informatsiooni otsimiseks kasutada ilma seejuures funktsionaalsust ja mugavust ohvriks toomata. Siin saab arvutisse salvestatud andmete sisu ja võimalikku viiruste olemasolu rahulikult kontrollida, kartmata, et viirus Teist ette jõuab ja kohtvõrku laiali kandub, ning seejärel kontrollitud ja turvalised andmed andmekandja või e-posti teel kohtvõrku edastada.

Täiendav informatsioon

Rangelt soovitatav on turvasüsteemide kasutamine tehniliselt sunduslikuks teha, et vältida olukordi, kus kasutajad teadmatusest või mugavusest turvameetmeid välja lülitavad või eiravad.

Internetis liikumisel kohatavate ohtlike skriptide ja e-posti kahtlaste kirjalisandite edasikandumise vältimiseks saab kasutada ka süsteemi keskset tulemüüri või niinimetatud proxy't.

6.4 Inimtegur: turvameetmete tundmine ja rakendamine

29.	**Turvapoliitikat ja turvameetmeid tuleb järgida.**

Turvapoliitika on abiks ainult siis, kui seda järgitakse. Ka parimad turvafunktsioonid ja turvaprogrammid ei aita, kui neid ei kasutata. Kõigi vajalike turvameetmete kasutamine eeldab iga töötaja väljaõpetamist ja see hakkab toimima alles siis, kui turvameetmete kasutamine muutub kõigile rutiiniks. Kõigil töötajatel peab olema algne arusaam infoturbest, et suuta kaasa mõelda ja ohtusid hinnata, sest ka kõige täiuslikumad turvapoliitikad ei suuda arvesse võtta kõiki igapäevases tegevuses ettetulevaid turvaauke.

30.	**Töökohal peab valitsema kord ning ei tohi olla vaba ligipääsu mistahes tundlikule informatsioonile.**

“Kord on elu alus.” Selle lause tõesuse osas võivad inimesed erinevatel arvamustel olla, kuid infoturbe puhul on kord tõepoolest suurepärane vahend arvukate ohtude vältimiseks. Tundlikud kaustad peavad töökohalt lahkudes kapi või seifi lukustatud olema, andmekandjad, nagu lindid, flopikettad ja CD-plaadid, millel on tundlikku informatsiooni, ei tohi kunagi vabalt vedelema jääda. Vajadusel tuleb sellised andmekandjad asjakohaselt hävitada, et vältida neilt andmete volitamata taastamist. Tundlike andmetega väljatrükkide koht on paberihundis, mitte paberikorvis. Sellised andmekandjad nagu kõvakettad ja CD-plaadid tuleb kustutada või hävitada.
Selle turvameetme rakendamise eelduseks on loomulikult, et vastavad kaustad ja andmed on turvavajaduste kindlakstegemise käigus tundlikeks kuulutatud ning et töötajad on selle turvameetme rakendamisest teadlikud!

31.	**Hooldus- ja remonditööde puhul tuleb eriti ettevaatlik olla.**

Eriti siis, kui arvutit või selle kõvaketast remonti viiakse või ära visatakse, on võimalik andmeid isegi rikkis andmekandjatelt hiljem taastada. Seetõttu ei tohi hooldustehnikuid

kunagi IT süsteemide ja sidesüsteemide juurde järelevalveta jätta. Kui andmekandjad majast lahkuvad, siis tuleb neil olnud andmed hoolikalt kustutada.
Tähelepanu: Tavaviisil kustutatud andmeid saab vastavate programmide abil ikkagi osaliselt või täielikult lugeda. Seetõttu tuleb tähtsad andmed turvaliselt kustutada, kasutades selleks vastavaid programme.

32.	**Töötajaid tuleb regulaarselt koolitada.**

Paljude vigade põhjuseks on teadmatus turvameetmetest või probleemi olemasolust. See kehtib loomulikult ka infoturbe puhul.
Eriti just administraatorid ja infoturbe eest vastutavad isikud peavad regulaarselt läbima täiendõppe. Ka väiksema eelarvega perioodidel ei tohi väljaõppest täielikult loobuda, isegi kui kulukate seminaride külastamine on võimatu. Hea asjakohase kirjanduse ost tasub enda alati ära.
Samas ei tohi väljaõpe piirneda ainult tehnilise küljega, sest pea alati on süsteemi turvalisuse kõige nõrgemaks lüliks töötaja. Keegi “ekspert” teatas kord USA Kongressi ees, et ta on mitme nimeka suurettevõtte kohtvõrku sisse tunginud, et sealt informatsiooni varastada, kusjuures ta pidi vaid harva tehnilisi võtteid kasutama, sest enamasti oli kerge mõnda töötajat pehmeks rääkida, et too talle turvakoodid annaks. Seetõttu tuleb regulaarselt tõsta kõigi töötajate teadlikkust infoturbest. Selleks on palju võimalusi, näiteks ettevõttesisesed loengud, väljaõpe, ringkirjad, plakatid, näited, turvajuhtumite avalikustamine jne.
Samuti on väga tähtis töötajaid teavitada, millistel viisidel tohib äripartneritega suhelda: kes on äripartneriteks? Milline on nende kompetentsus? Kuidas toimub tuvastamine? Millist informatsiooni tohib edasi anda?
Ka sidekanalite kasutamist tuleb selgitada: Milliseid andmeid tohib e-posti kaudu vahetada? Millised on äripartnerite tegelikud täpsed telefoninumbrid ja veebiaadressid?
Aina sagedamini juhtub, et petturid meelitavad kasutajaid valeidentiteediga e-posti abil võlts-veebilehtedele, näiteks liba-pangalehele, et nood sinna PIN-koodi, parooli või mõne muu koodi sisestaksid (“*Phishing*”, õngevõtmine).

33. **Ainult aus enesehinnang viib edasi: vahel tuleb ekspertidelt abi paluda.**

Mitte alati ei ole kõigi infoturbe alaste aspektide kohta olemas ettevõttesisesed vajalikud teadmised. Praktika näitab, et kvalifikatsiooni tõstmise meetmed ei ole alati edukad, sest asjassepuutuvad isikud olid lihtsalt ajaliselt ülekoormatud. Sellisel juhul tuleb vastutusalad ümber vaadata ja optimaalsemaks määrata. Paljudel juhtudel on targem väljastpoolt abi tellida või vastava teenusepakkujaga leping sõlmida. Oma võimete ülehindamine ja vales kohas kokkuhoidmine võivad siin saatuslikke tagajärgi kaasa tuua.

34. **Kõigi kehtivate turvameetmete jaoks tuleb määrata ka kontrollmehhanismid.**

Kõigi turvameetmete puhul on kõrgeimaks eesmärgiks isiklik arusaamine, aktsepteerimine ja vabatahtlik täitmine. Samas on turvameetmete eiramisel mitmeid erinevaid põhjuseid. Teadlik eiramine on siin pigem erand, palju sagedamini on tegemist eksimustega ja hooletusega. Nende põhjuste kõrvaldamine on kõigi asjaosaliste huvides. Seetõttu peab iga kehtestatud turvameetme puhul mõtlema ka sellele, kuidas selle turvameetme täitmist kontrollida. See võib toimuda näiteks tehniliste programmide abil või siis auditite ja revisjonide kaudu, protokolliandmete kontrollimise teel, pistelise kontrolli abil jne. Loomulikult tuleb välja pakkuda ka enesekontrolli variant, näiteks vastavate kontrollnimekirjade väljajagamise teel. Sellised kontrollnimekirjad võib ka allakirjutatavateks teha ja kokku koguda.

35. **Turvaolukorra rikkumisel rakendatavad karistused tuleb kindlaks määrata ja avalikuks teha.**

Kõigile asjaosalistele peab teada olema, et turvapoliitika ja kordade kogemata või meelega rikkumisega kaasnevad süüdlasele kindlad tagajärjed. Selleks tuleb ametlikult ja selgelt teada anda (näiteks firma turvapoliitikas), millised on probleemide puhul vastavad karistused.

36.	**Ilmnenud turvapoliitika ja kordade rikkumiste eest tuleb ka tegelikkuses karistada.**

Kui ilmneb mingi turvapoliitika või korra rikkumine, siis tekib vältimatult ka küsimus selle kohta, kuidas ettevõtte juhtkond peaks süüdlasesse suhtuma. Kergete rikkumiste korral, eriti kui tegemist on esmakordse rikkumisega, on karmid sanktsioonid selgelt liialdus. Samas aga on ka vale raskete rikkumiste või kangekaelsete süüdlaste puhul sanktsioonidest loobuda, sest see annab vale arusaama nii süüdlasele kui ka kõigile teistele töötajatele. Seetõttu tuleb alati adekvaatselt reageerida. Asjaolu, et on toimunud turvapoliitika rikkumine, tuleb kõigile teada anda, niivõrd kui olukord seda lubab.

6.5 IT süsteemide hooldus – turvalisusega seotud uuenduste käsitlemine

37.	**Turvauuendusi tuleb regulaarselt paigaldada.**

Turvauuenduste puhul on kõige kõrgem prioriteet alati viirustõrje programmidel, kuna uued viirused levivad vahel väga kiiresti. Ka interneti brausereid, e-postiprogramme ja operatsioonisüsteeme tuleb regulaarselt uuendada. Samas ei tohi unustada ka muude programmide ja teatud riistvaraliste osade regulaarset hooldust.

38.	**Programmide turvalisusega seotud omaduste kohta tuleb regulaarselt ja põhjalikult lisainfot otsida.**

IT süsteemide turvalisuse tagamiseks on vajalik regulaarne täiendava informatsiooni otsimine uute leitud turvaaukude ja nende kõrvaldamise viiside kohta. Uuringute hõlbustamiseks saab kasutada Internetis antavaid ametlikke soovitusi ja asjakohaseid artikleid. Uutes programmiversioonides (nt. interneti brauseri puhul) on leitud turvaaugud reeglina programmi autorite poolt juba kõrvaldatud. See aga ei vabasta Teid isikliku hinnangu andmisest, sest enamasti on uutel programmiversioonidel ka uued funktsioonid ja uued vead, mis omakorda ohtusid kaasa toovad.
Iga süsteemi eest vastutav töötaja peab endale regulaarselt aega võtma, et internetis asjakohast informatsiooni otsida ja kolleegidega nõu pidada. Lisaks on olemas arvukalt

tasuta infoteenuseid, mille kvaliteet on sageli parem kui kommertslikel sama ala teenustel.
Uute programmiuuenduste ja turvauuenduste suur hulk teeb vajalikuks teatava valimise. Reeglina ei saa kõiki uuendusi paigaldada, eriti veel kohese abinõuna. Seetõttu tuleb juba ette selgeks teha, milliste kriteeriumide järgi uuendusi valida, milliseid uuendusi milliste ajaliste viivitustega paigaldada tohib ja milliseid uuendusi kindlasti kohe paigaldama peab.

39.	**Vajalike turvauuenduste paigaldamiseks tuleb koostada tegevusplaan.**

Isegi juhul, kui süsteemi eest vastutav isik ei paigalda uut turvauuendust kohe, ei jää sellepärast süsteem kohe seisma ega järgne ka minuti pärast kohutavat häkkerirünnakut. See aga tähendab, et uuenduste regulaarne paigaldamine nõuab ranget distsipliini ja see tuleb kohe algusest peale protsessina paika panna. Eriti just viirustõrje programmide puhul peab uuenduste võimalikult kiire paigaldamine rutiiniks muutuma.

40.	**Tarkvaramuutusi tuleb testida.**

Teoreetiliselt tuleks iga äritegevustega seotud programmide muudatust enne selle rakendamist testida, et olla kindel, et ka pärast selle muutuse rakendamist toimivad kõik süsteemid probleemideta. On juhtunud, et ka viirustõrje programmide uuendused on ettevõtte arvutisüsteemis kaose tekitanud, kuna viirustõrje programm pidas ettevõtte oma tarkvara ekslikult viiruseks ja lülitas selle välja.
Tähtsate turvauuenduste testimine toimub enamasti kiirustades, sest need uuendused tuleb ka võimalikult kiiresti paigaldada. Praktikas peavad administraatorid seetõttu eriti hoolikalt valima infoturbe alaste nõuete ja olemasolevate ressursside vahel, et mõistlikud kompromissid leida.

6.6 Turvamehhanismide kasutamine: paroolide ja krüpteerimise käsitlemine

41. **Turvamehhanismide valikul tuleb hoolikas olla.**

Paljud autorid on oma programmidesse juba sisse integreerinud soovi korral kasutatavad turvamehhanismid, nagu paroolide kasutamine või andmete krüpteerimine. Samas on turvaliste krüpteerimismehhanismide väljatöötamine äärmiselt keerukas teadus. Programmide autorid, kes ei ole vahepeal mitmeid aastaid krüpteerimismehhanismide väljatöötamisega intensiivselt tegelenud, ei saa olla sellel alal asjatundjad. Sellegipoolest on palju autoreid, kelle programmid pakuvad nende omaloodud krüpteerimismehhanisme, mis on aga reeglina ebaturvalised. Kui Teie ettevõttes sõltub palju turvalisest krüpteerimisest, siis uurige kriitilise pilguga, milliseid meetodeid programmi autor kasutab. Võimaluse korral tuleks kasutada standardiks muutunud ja üldsuse poolt turvaliseks tunnistatud algoritme.
Kui mingi turvafunktsiooni kvaliteet on kahtluse all ja kvaliteetsema turvafunktsiooni valimine ei tule kõne alla, siis on soovitatav kasutada vähemalt seda kahtlast turvafunktsiooni – halb kaitse on parem kui kaitse täielik puudumine. Sellisel juhul tuleb aga neid olemasolevaid turvamehhanisme kõige rangemal turvaseadistusel kasutada. Praktikas lubavad paljud e-teenuste pakkujad, kes kasutavad SSL krüpteerimist, endiselt 40 bitise võtmepikkusega krüpteerimist, et tagada vanemate versioonidega brauseritega kokkusobivust.

42. **Kasutada tuleb õigesti valitud turvalisi paroole.**

Halvasti valitud paroolid on infoturbe alaste puuduste hulgas esimeste seas. Eriti kasutavad seda asjaolu ära häkkerid. Oma süsteemi häkkerite töövahendite eest kaitsmiseks, mis poolautomaatselt kõiki võimalikke märgikombinatsioone proovivad või lausa terveid sõnastikke koos sõnade ja numbrite kombineerimisega kasutavad, peab parool vastama teatud kvaliteedinõuetele. Parool peab olema pikem kui seitse märki, see ei tohi olla mingi sõnastikes esinev sõna, ei tohi koosneda ühest ega mitmest nimest (eriti mitte kirjandusest ja filmidest tuntud lemmikute nimesid) ning peab sisaldama ka erimärke ja numbreid. Viimasel juhul tuleb vältida üldkasutatavate

variantide kasutamist, nagu näiteks lihtsalt parooli lõppu numbrite paigutamist või lihtsa parooli algusesse või lõppu mõne tavalise erimärgi, nagu $, !, ? või # lisamist.
Mõistlik nõue paroole regulaarselt muuta toob endaga kaasa dilemma – kuidas kõiki paroole meelde jätta? Seetõttu on pea kõikjal, välja arvatud mõnedes kõrgturvalisuse erandkohtades, lubatud parool üles kirjutada ja turvalises kohas hoida. Loomulikult aga ei tohi selliseks hoiukohaks olla kuvarialune ega ülemine kapisahtel.
Samuti tekitab probleeme harjumus samu paroole mitmes kohas kasutada. Kui selline parool valedesse kätesse satub, siis proovib targem pettur sama parooliga läbi ka teised rakendused. Seetõttu tuleb niisuguste “lihtsamate lahenduste” eelised ja puudused igal eraldi juhul põhjalikult läbi mõelda.

43.	**Standardina etteantud paroole ja tühje paroole tuleb vältida.**

Mõnedel programmidel on nende paigaldamise järel standardsed kõigile tuntud paroolid või tühjad paroolid. Paljud häkkerid teavad seda ning proovivad rünnaku puhul kõigepealt järgi, ega neid paroole pole muuta unustatud. Seetõttu tuleb uute programmide paigaldamise puhul alati ka nende kasutusjuhendid läbi lugeda, et saada teada, kas programmis kasutatakse selliseid algparoole. Ka hooldusfirmad, kus kasutatakse väliste hooldustööde puhul halvasti valitud või hoopiski alati samu paroole, kujutavad endast turvariski. Üksikutel juhtudel on isegi ilmnenud, et programmi autor on oma programmi dokumenteerimata juurdepääsuvõimalused (“tagauksed”) loonud, näiteks selleks, et klienditoena probleemide kõrvaldamisel lihtsamini administraatori-ligipääs saada. Seetõttu peavad programmide autorid ja IT hooldusfirmad suutma kaheldamatult tõestada, et nad selliseid meetodeid ei kasuta.
See hoiatus kehtib mitte ainult IT süsteemide, vaid ka sidesüsteemide puhul.

44.	**Tööarvutite juurest lahkumisel peavad need jääma parooliga kaitstud ekraanisäästjaga.**

Kõik uuemad operatsioonisüsteemid pakuvad võimalust klaviatuur ja kuvar teatud ooteaja järel lukustada. Lukustusest vabastamiseks tuleb sisestada kehtiv parool. Kui arvutitele võivad kasutaja eemaloleku ajal ligi pääseda volitamata isikud, siis tuleb kasutada parooliga kaitstud ekraanisäästjaid. Sellisel juhul ei tohiks lukustus liiga kiiresti

aktiveeruda, kuna see segaks kasutajaid pärast väikesi arvutikasutamise pause. Sageli kasutatakse 5 minuti pikkust perioodi alates viimasest sisestusest. Samuti peab olema võimalus lukustus käsitsi aktiveerida (nt. *Windowsis* vajutades <*CTRL+Alt+Del*> ja <*Lock Computer*>)

45.	**Tundlikud andmed ja süsteemid peavad kaitstud olema.**

Hiljemalt kui keegi saavutab otseligipääsu kõvakettale, millel tundlikke andmeid hoitakse, saab ta krüpteerimata andmeid takistamatult lugeda. Operatsioonisüsteemi sisseehitatud kaitsemehhanismid ja vastavad programmid pakuvad ekspertide rünnakute eest vaid piiratud ja ebapiisavat kaitset. Seetõttu tuleb tundlike andmete puhul kasutada lisaks ka krüpteerimise tarkvara. Sülearvutite sisu tuleks võimaluse korral täies mahus krüpteerida, kuna nende varastamine võib üsna lihtne olla. Selleks otstarbeks on head programmid saadaval soodsa hinnaga või hoopiski tasuta. Samas tuleb programmi valikul veenduda, et selle poolt kasutatavad krüpteerimismeetodid on tõesti turvalisteks tunnistatud. Programmi autorite omalooming on harva turvaline. Informatsioon turvaliste algoritmide ja koodipikkuste kohta on saadaval asjakohastes raamatutes, BSI veebilehel ja ka muudel vastavatel turvalisuse alastel veebilehtedel Internetis.

6.7 Katastroofide ja materiaalsete kahjude vastane kaitse

46.	**Tuleb koostada hädaolukorras tegutsemise juhendid ja töötajad peavad neid tundma.**

Kui arvuti streigib, printer ei prindi, elekter läheb ära, võrgus levib mingi viirus või vajalikud andmed on kogemata ära kustutatud, siis peab iga töötaja teadma, mida nüüd teha. Kõik vastutavad isikud peavad nende jaoks mõeldavad stsenaariumid läbi mängima ning vajalikud isikud ja nende telefoninumbrid endale üles kirjutama. Samuti tuleb kasuks tüüpilise stsenaariumi lühikirjelduse kirjapanek. Näiteks: Kuidas varukoopiat taastada? Kuidas printimisserverile taaskäivitust teha?

47.	**Kõigist tähtsatest andmetest tuleb regulaarselt varukoopiad teha.**

Andmetest varukoopiate tegemiseks on saadaval palju programme ja riistvaralisi lahendusi. On tähtis, et varukoopiasse kaasataks tõepoolest kõik vajalikud andmed. Selle nõude täitmine on väljakutseks eriti just jagatud heterogeensete keskkondade puhul. Samuti tuleb varukoopiate tegemisse kaasata mobiilsed lõppseadmed, nagu näiteks sülearvutid, võrku ühendamata üksikarvutid ja ka pihuarvutid. Regulaarselt tuleb kontrollida, et varundamine tegelikult toimib ja andmed tõepoolest varukoopiast taastatavad on.

Varukoopiatega andmekandjaid tuleb hoida turvalises kohas, võimalusel väljaspool ettevõtte hoonet või teenuse pakkumise hoonet. Lisaks peab varukoopiate hoidmise koht olema piisavalt hästi tulekahju, uputuse ja muude materiaalsete kahjude eest kaitstud.

Kõik kasutajad peavad teadma, millistest andmetest ja millal varukoopiaid tehakse ning kui kaua see aega võtab. Reeglina tehakse jooksev varukoopia teatud kataloogidest ja failidest, harvemini täielik varukoopia kogu süsteemist.

48.	**IT süsteemid peavad olema piisavalt kaitstud tulekahju, ülekuumenemise, uputuse ja voolukatkestuse eest.**

IT ettevõttele võivad materiaalsed kahjud tekkida mitte ainult kasutusvigade või tahtlike rünnakute kaudu. Sageli tekivad suured kahjud tule, vee või elektrivoolu otsese toime tõttu. Paljud seadmed tohivad töötada ainult teatud kindlates kliimatingimustes. Seetõttu tuleb eriti tähtsad IT seadmed (serverid, varukoopiatega seonduv, ruuterid jne.) paigutada piisavalt kaitstud ruumidesse. Lisaks tuleb need seadmed ühendada vooluvõrguga katkematu toite allika kaudu, millel on ka ülekoormuse vastane kaitse.

49.	**Rakendada tuleb sissepääsupiirangud ja sissemurdmise vastased kaitsesüsteemid.**

Ka väikeettevõtted ja riigiasutused peavad mõtlema sellele, kuidas kaitsta end sissemurdmise ja teiste kutsumata külaliste eest. Juba lihtsad meetmed võivad tuua kaasa turvalisuse taseme märkimisväärse tõusu. Tuleb läbi mõelda, kus külastajad ja

muud võõrad isikud reeglina viibivad ja millistele IT süsteemidele nad seal juurde võivad pääseda. Eriti just serverid ja sellised arvutid, mille kaudu võib ligi pääseda tundlikele andmetele, tuleb selliselt paigutada, et võõrad ei saaks neid märkamatult kasutada. Külastajaid tuleb mitte ainult viisakuse pärast igal pool hoolikalt saata. Teatud tingimustel on soovitatav tööruumid töötaja eemalviibimise ajaks lukustada ja akna sulgemine (näiteks lõunapausi ajaks) kohustuslikuks teha. Remondimeeste, tehnikute ja koristajate tegevus peab olema põhjalikult planeeritud ja kõigile töötajatele teada. Sülearvutit ei tohi kunagi ilma järelevalveta autosse jätta ja kui võimalik (vajalik), siis ööseks või pikemaks eemalviibimise ajaks lukustada. Siintoodud nõuanded ei ole kindlasti mitte ainukesed, mida silmas tuleb pidada – igal konkreetsel juhul tuleb need üle vaadata ja vajadusel täiendada.

Nõuanne:
Laske sissemurdmise vastane kaitsesüsteem eksperdil või politsei nõustajal üle vaadata, et sissemurdja tegevus ei oleks ülemäära lihtne.

50.	**Kogu ettevõttes kasutatav riistvara ja tarkvara tuleb inventarinimekirja kanda.**

Soovitatav on pidada inventarinimekirja, mida regulaarselt uuendatakse. Paljudel juhtudel saab need andmed ka raamatupidamisest, kuid siis on vahel ebaselge, kas asjade kirjapandud seis on enam aktuaalne ning kas mingi kadunud ese on juba pikemat aega kadunud olnud või läks kaduma alles äsja. Ka kindlustuse pakkujad vajavad kahjude hindamisel inventarinimekirja. Lisaks saab inventarinimekirja alusel kontrollida, kas kindlustussumma on ikka piisav.

7 Lisa

Kontrollnimekirjad

Allpool esitatud küsimused võtavad lühidalt kokku 50 turvameetme sisu ning võimaldavad saada kiire ülevaate ettevõtte või ametkonna nõrkadest kohtadest.

Infoturbe haldamine	
☐	Kas ettevõtte või ametkonna juhtkond on infoturbe eesmärgid defineerinud ja endale infoturbe alase vastutuse võtnud? Kas kõik vastavates kehtivates seadustes ja lepingutes sätestatud punktid on arvesse võetud?
☐	Kas infoturbe alale on määratud vastutav isik?
☐	Kas kõigi projektide puhul võetakse juba varases etapis (nt. uue võrgu planeerimisel, uute IT süsteemide ja rakenduste väljatöötamisel, alltöövõtulepingute ja teenuselepingute koostamisel) arvesse infoturbe alaseid nõudeid?
☐	Kas on olemas ülevaade tähtsamatest rakendustest ja IT süsteemidest ning nende kaitsevajadusest?
☐	Kas on olemas tegevusplaan, milles on sätestatud turvaprioriteedid ja konkreetsete IT turvameetmete rakendamine?
☐	Kas kõigi IT turvameetmete osas on sätestatud see, kas neid rakendatakse ühekordselt või regulaarselt (nt. viirustõrje tarkvara uuendamine)?
☐	Kas kõigi IT turvameetmete jaoks on defineeritud vastutavad isikud?
☐	Kas on paika pandud vastutavate isikute asendajad ja kas need asendajad on oma ülesannete kõrgusel? Kas tähtsamad paroolid on hädaolukorra puhuks hoiule pandud?
☐	Kas kõik asjakohased isikud tunnevad kehtivaid määrusi ja vastutusalasid?
☐	Kas on koostatud kontrollnimekirjad selle kohta, mida tuleb silmas pidada uue töötaja töölevõtmisel ja endise töötaja töölt vabastamisel (kasutajaõigused, võtmed, juurdepääsuloa, jne.)?
☐	Kas IT turvameetmete toimimist kontrollitakse regulaarselt?
☐	Kas on olemas dokumenteeritud IT turvakontseptsioon?

IT süsteemide turvalisus	
□	Kas kõiki rakenduste ja programmide olemasolevaid kaitsemehhanisme kasutatakse?
□	Kas kasutatakse kogu süsteemi hõlmavaid viirustõrje programme?
□	Kas kõigile süsteemi kasutajatele on määratud rollid ja profiilid?
□	Kas on kindlaks määratud, millistele andmetele millised kasutajad ligi pääseda tohivad? Kas on rakendatud mõistlikke piiranguid?
□	Kas erinevatele administraatoritele on määratud erinevad profiilid või tohib iga administraator teha kõike?
□	Kas on teada, millised privileegid ja õigused on programmidel?
□	Kas programmide ja IT süsteemide turvalisuse alased standardseadistused on ära muudetud või kasutatakse neid nende paigaldamise aegses seisundis?
□	Kas turvalisust mõjutavad ebavajalikud programmid on eemaldatud ja funktsioonid välja lülitatud?
□	Kas käsiraamatuid ja juhendeid loetakse enne tegutsema hakkamist?
□	Kas tarkvara paigaldamise ja IT süsteemide kohta peetakse põhjalikku ja regulaarselt uuendatavat dokumentatsiooni?

Arvutivõrgud ja internetiühendus	
□	Kas kasutatakse tulemüüri?
□	Kas tulemüüri seadistust ja toimimist kontrollitakse regulaarselt ja kriitilise pilguga?
□	Kas on loodud kontseptsioon selle kohta, milliseid andmeid väljapoole ettevõtet kättesaadavaks tehakse?
□	Kas on paika pandud, kuidas käituda ohtlike programmilisadega (*pluginitega*) ja aktiivsete kirjalisanditega?
□	Kas kõik ebavajalikud teenused ja programmifunktsioonid on välja lülitatud?
□	Kas brauserid ja e-postiprogrammid on turvaliselt seadistatud?
□	Kas töötajad on piisava koolituse läbinud?

Turvanõuete järgimine	
□	Kas tundlikku informatsiooni ja andmekandjaid hoitakse turvaliselt ja hoolikalt?
□	Kas tundlikud andmed kustutatakse andmekandjatelt ja IT süsteemidest enne hooldustööde või remonditööde tellimist?

□	Kas töötajad läbivad regulaarselt turvalisuse alase koolituse?
□	Kas töötajate turvalisuse alase teadlikkuse tõstmiseks on mingeid meetmeid rakendatud?
□	Kas kehtivate turvanõuete täitmist jälgitakse ja turvanõuete rikkumisi karistatakse?

IT süsteemide hooldus: programmiuuendused	
□	Kas turvauuendusi installeeritakse regulaarselt?
□	Kas on määratud vastutav isik, kes kogub regulaarselt täiendavat informatsiooni kasutatava tarkvara turvalisuse ja vastavate turvauuenduste kohta?
□	Kas tarkvaramuudatuste jaoks on paika pandud testimise kontseptsioon?

Paroolid ja krüpteerimine	
□	Kas kasutatavad programmid ja rakendused pakuvad turvamehhanisme, nagu paroolid või krüpteerimine? Kas need turvamehhanismid on kasutusel?
□	Kas kõik vaikimisi paroolid ja „tühjad" paroolid on ära muudetud?
□	Kas kõik töötajad on läbinud turvaliste paroolide valimise alase väljaõppe?
□	Kas kõik tööarvutid on töötaja lahkumisel parooliga ekraanisäästjaga kaitstud?
□	Kas tundlikud andmed ja eriti ohustatud süsteemid nagu sülearvutid on piisavalt hästi kaitstud kasutades krüpteerimist või muudel viisidel kaitstud?

Hädaolukordades tegutsemine	
□	Kas on koostatud hädaolukorras tegutsemise plaan, mis sisaldab tegevusjuhiseid ja kontaktandmeid?
□	Kas kõigi võimalike hädaolukordadega on arvestatud?
□	Kas kõik töötajad tunnevad hädaolukorra tegevusplaani ja kas see tegevusplaan on kõigile kättesaadav?

Andmete varundamine	
□	Kas on koostatud varukoopiate tegemise alane strateegia?
□	Kas on paika pandud, milliseid andmeid kui kaua säilitatakse?
□	Kas varukoopiate tegemine hõlmab ka sülearvuteid ja võrku mitteühendatud süsteeme?
□	Kas varukoopiatega andmekandjaid kontrollitakse regulaarselt?

□	Kas varukoopiate tegemine ja nendelt andmete taastamine on dokumenteeritud?

Infrastruktuuri turvalisus	
□	Kas IT süsteemid on piisavalt kaitstud tule, ülekuumenemise, vee, voolukõikumiste ja voolukatkestuste eest?
□	Kas juurdepääs tähtsatele IT süsteemidele ja ruumidele on reguleeritud? Kas külastajate, väliste tehnikute, hooldus personali jne. külastustel saadab neid isik ja kas neid jälgitakse?
□	Kas on rakendatud piisav sissemurdmiste vastane kaitse?
□	Kas riistvara ja tarkvara on regulaarselt uuendatavasse inventarinimekirja kantud?

Informatsioon BSI IT etalonturbe juhendi kohta

► **www.bsi.de/gshb**

Siit leiate kogu olemasoleva informatsiooni BSI IT etalonturbe juhendi kohta, GSTOOL töövahendi kohta ja IT etalonturbe juhendi alusel sertifitseerimise kohta.

Juuni 2004.aasta