Bundesamt
für Sicherheit in der
Informationstechnik

Riigi Infosüsteemide Arenduskeskus

IT-turbejuhend

Lühiülevaade olulisematest IT-turbe 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, kohalikes omavalitsustes, väikestes ja keskmistes ettevõtetes. Juhendit saavad kasutada ka asutuste juhtkonnad ja teisedki töötajad 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, mida on kohandatud Eesti oludele. 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 ISKE (Infosüsteemide kolmeastmelise etalonturbe süsteem, www.ria.ee/iske) rakendusjuhendi koostamisel. 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, Saksamaa infoturbeameti, BSI (*Bundesamt für Sicherheit in der Informationstechnik*) president.

Töö- ja äriprotsessid põhinevad üha enam IT-lahendustel. Seetõttu muutub üha tähtsamaks info- ja kommunikatsioonitehnoloogia turvalisus ja usaldusväärsus. Õige IT-turvakontseptsiooniga saab panna tugeva aluse usaldusväärse IT-turbeastme saavutamisele. Käesolev juhend aitab Teil saada kompaktses vormis ülevaate tähtsamatest turbemeetmetest. Praktikat kajastavad näited aitavad Teil näha ohtusid ning kirjeldavad hädavajalikke organisatoorseid, infrastruktuurilisi ja tehnilist laadi abinõusid. Oma hetkeolukorra analüüsimiseks on toodud kontrollnimekirjad. Kõik see kokku kinnitab tõsiasja:

suuremat turvalisust on võimalik saavutada ka ilma suure IT-eelarveta.

„IT-turbejuhend“ annab Teile kompaktse ülevaate tähtsamatest organisatoorsetest, infrastruktuurilistest ja tehnilistest IT-turvameetmetest. See on suunatud IT eest vastutavatele töötajatele ning nii väikese kui ka keskmise suurusega ettevõtete ja ametiasutuste administraatoritele.

Sisukord

1. Sissejuhatus

Elu 21. sajandil pole ilma info- ja kommunikatsioonitehnoloogiata peaaegu et enam ettekujutletav. Seetõttu muutub üha tähtsamaks ka igasuguste IT-süsteemide kaitse. Vajaduse IT-turvameetmete tõhususe tõstmiseks loovad ka muudatused seadusandluses, millel kohaselt peavad juhatused ja juhatuse esimehed puuduliku juhtimise ja ebapiisava riskiennetuse eest isiklikult vastutama.

Praktikas on aga mõistliku turbeastme saavutamine ja selle hoidmine tihti väga raske. Põhjuseid selleks on mitmeid: puudulikud ressursid, liiga piiratud eelarved ning viimaks, mida ei saa sugugi alahinnata, mängib selles oma rolli ka IT-süsteemide üha kasvav keerukus. Saadaval on kõige erinevamaid lahendusi nii IT-turvet pakkuvate toodete kui ka nõustajate näol. Valik on väga lai, mis muudab ülevaate säilitamise raskeks isegi ekspertidele.

Käesolev juhend annab kompaktse ja kõigile arusaadava ülevaate tähtsamatest IT-turvameetmetest. Kesksel kohal on organisatoorsed abinõud ja võimalike ohtude kirjeldamine praktikast kogutud näidete põhjal. Tehnilistest detailidest on siinkohal teadlikult loobutud.

Kokkuvõte: juba ainuüksi käesolevas juhendis toodud soovituste järjekindel ellurakendamine või selle järgimine IT-teenusepakkujatega sõlmitavate lepingute koostamisel loob kindla aluse usaldusväärse IT-turvalisuse taseme tekkeks.

2. Fookuses on IT-turve

Turvalisus on inimese ja seega terve meie ühiskonna üheks põhivajaduseks. Just globaliseerumisajastul, mil mobiilsus aina kasvab ning tööstusrahvaste sõltuvus info- ja kommunikatsioonitehnoloogiast üha suureneb, suureneb aina enam ka vajadus kaitse järele.

Haavatavus ja oht sattuda IT-riskide tagajärjel suurtesse majanduslikesse kahjudesse avaldavad survet ning sunnivad tegutsema aktiivse IT-turvahalduse suunas, mis oleks võimeline kahjusid ära hoidma ja jääkohtusid minimeerima. Asjakohane vastutus ei lasu mitte mingil juhul vaid puudutatud IT-osakondadel. Pigem kehtib siin tõsiasi, et IT-turvalisus on juhtide pärusmaa. Oma roll on selles ka seadusandlusel. Erinevad seadused ja ettekirjutused teevad juhatuste esimehed ja juhatused võimalike vajakajäämiste puhul isiklikult vastutavaks.

Küllaltki laialt on levinud arusaam, et IT-turvameetmed on ilmtingimata seotud kõrgete investeerimiskuludega, kuna raha tuleb paigutada nii turvatehnikasse kui ka kõrge kvalifikatsiooniga personali. See väide ei pea alati paika. Kõige olulisemateks edufaktoriteks on terve inimmõistus, läbimõeldud organisatoorne reeglistik ning usaldusväärsed ja motiveeritud töötajad, kes järgivad iseseisvalt, distsiplineeritult ja igapäevaselt turbealaseid ettekirjutusi. Toimiva ja efektiivse IT-turvakontseptsiooni loomine ei pea seega olema ilmtingimata kulutus, mida ei jõua mitte keegi kinni maksta. Kõige tõhusamad meetmed on üllatavalt lihtsad ja sellele lisaks veel ka tasuta!

Teiseks laialdaselt levinud väärarusaamaks on oma kaitsevajaduste hindamine. Tihti võib kuulda väiteid nagu:

„meil ei ole veel mitte kunagi midagi juhtunud“: See on väga julge väide. Võib-olla pole aset leidnud turvaintsidente seni veel tuvastatud!

„No mida meie käest ikka võtta on, meie andmed ju ei ole ju nii salajased“. Antud hinnang on paljudel juhtudel osutunud liiga pealiskaudseks. Võimalike kahjustsenaariumite põhjalikul hindamisel saab ruttu selgeks, et tegelikkuses töödeldakse siiski ka andmeid, mille sattumine valedesse kätesse võib endaga kaasa tuua nende andmete laiaulatusliku väärkasutuse.

„Meie võrk on kindel“. Tihti alahinnatakse potentsiaalsete ründajate võimeid. Lisaks kehtib tõsiasi, et ka kogenud võrgu- või turvaspetsialistid ei pruugi olla kõiketeadjad ning ka nemad ise võivad aeg-ajalt teha vigu. Väljast tellitud kontrollide käigus tuvastatakse peaaegu alati ka tõsiseid kitsaskohti, mistõttu on need head abivahendiks kaitseks organisatsioonisiseste „silmaklappide“ vastu.

„Meie töötajad on usaldusväärsed“. Erinevad statistilised andmed räägivad hoopis teist keelt: suurem osa turvanõuete rikkumistest pannakse toime organisatsiooni enda töötajate poolt. Need ei pruugi üldse olla teadlikud rikkumised. Kui võimalikest probleemidest ei olda piisavalt teadlikud, võivad laiaualatuslike tagajärgede põhjusteks olla ka hooletus, liigne agarus ja liigne uudishimu.

Kõik peaksid endale teadvustama, et turvalisus ei ole mitte staatiline seisund, vaid pidev protsess. Seetõttu peaksid kõik endalt ikka ja jälle küsima:

Millised võiksid olla erinevad väärkasutuse variandid juhul, kui teie ettevõtte või ametiasutuse konfidentsiaalne info peaks sattuma kolmandate isikute kätte?

Millised oleksid tagajärjed meie jaoks, kui leiaks aset olulise info muutmine, nt andmeedastuse käigus või meie serveril? Põhjusena võib kõne alla tulla mitte ainult kolmandate isikute pahatahtlik soov, vaid ka tehniline rike.

Mis juhtuks, kui organisatsiooni jaoks vajalikud arvutid või muud IT-komponendid ühtäkki rivist välja langeksid ja neid ei saaks enam pikema aja jooksul (päevi, kuid, …) kasutada? Kas tööd suudetaks jätkata? Kui suur oleks võimalik kahju?

Hästi läbimõeldud IT-turvakontseptsiooni juurutamise tagajärjel võite mõne aja möödudes märgata, kuidas lisaks turvalisuse kasvule hakkavad ilmnema veel ka muud eelised. IT-juhid täheldavad tihti järgnevaid „kõrvalmõjusid“:

Töötajad muutuvad enesekindlamaks, töö kvaliteet kasvab.

Igapäevane IT-turbega arvestamine loob tööl õhkkonna, mida iseloomustab vastutuskindel tegutsemine, orienteeritus oma klientidele töötajate samastumine organisatsiooni eesmärkidega.

Konkurentsieelised

Tõestatav IT-turve loob usaldusväärsust ka klientide ja teiste koostööpartnerite silmis ning viimased koguni nõuavad seda üha sagedamini.

IT-süsteemide hooldamiseks kulub märgatavalt vähem aega. Administraatorid töötavad efektiivsemalt.

Administraatorid ja kasutajad tunnevad oma süsteeme palju paremini. IT-süsteemid on hästi dokumenteeritud ning see lihtsustab administreerimistöid, planeerimist, tarkvara esmapaigaldamist ja vigade kõrvaldamist. Hea IT-turvakontseptsioon aitab muuhulgas vältida probleeme, mille all administraatorid tavaliselt väga kannatavad: kasutajad rakendavad ühe ja sama tööülesande täitmiseks erinevaid programme, hooldada tuleb erinevaid operatsioonisüsteeme, paralleelselt kasutatakse ühe tarkvara erinevaid versioone, igal kasutajal on individuaalsed volitused, kasutajad rakendavad isiklikku tarkvara ja koostavad oma töökohaarvuti ise, omamata asjakohast oskusteavet. Arvutipark on muutunud loomaaiaks, mille tsentraalne haldamine ei tule kõne allagi. Igat arvutit tuleb suure vaevaga eraldi analüüsida ja selle alusel hooldada.

3. IT-turvet puudutavad olulised mõisted

IT-turve koosneb kolmest põhiväärtusest: konfidentsiaalsus, käideldavus ja terviklus.

Konfidentsiaalsus: konfidentsiaalset infot tuleb kaitsta volitamata avalikustamise eest.

Käideldavus: kasutaja peab saama talle vajalikul hetkel kasutada talle vajaminevaid teenuseid, talle vajaliku IT-süsteemi funktsioone ja talle vajalikku infot.

Terviklus: andmed peavad olema täielikud ja muutmata. Mõistega „informatsioon“ tähistatakse infotehnoloogias „andmeid“, millele saab sõltuvalt kontekstist lisada erinevad täiendeid nagu autor või loomise aeg. Informatsiooni tervikluse kadu võib seega tähendada, et seda on volitamata kujul muudetud, on võltsitud selle autori andmeid või on manipuleerituid nende loomise ajaga.

Täiendavad tihtiesinevad mõisted on:

Autentimine: süsteemi sisse logides toimub autentimisprotsessi käigus sisselogiva isiku identiteedi kontrollimine. Antud mõistet kasutatakse ka IT-komponentide või rakenduste identiteedi kontrollimisel.

Autoriseerimine: autoriseerimise käigus kontrollitakse, kas teatud isikul, IT-komponendil või rakendusel on olemas vajalikud volitused, mis lubavad tal teatud tegevusega jätkata.

Andmekaitse: andmekaitse all peetakse silmas isiku isikuandmete kaitsmist kolmandate isikute poolt toime pandud väärkasutuse eest (mitte segi ajada andmeturbega).

Andmeturve: andmeturbe all peetakse silmas andmete kaitsmist eesmärgiga tagada nende konfidentsiaalsus, käideldavus ja terviklus. Sama asi teisisõnu kannab nimetust IT-turve.

Andmevarundus (ingl *Backup*): andmevarunduse käigus luuakse andmekao vältimiseks olemasolevatest andmehulkadest varukoopiad.

Penetratsiooni test: penetratsiooni test on sihipärane, reeglina simuleeritud, IT-süsteemi vastu suunatud ründekatse. Seda rakendatakse olemasolevate turvameetmete tõhususe kontrollimiseks.

Riskianalüüs (ingl *Risk Assessment / Analysis*): riskianalüüsi abil kontrollitakse, kui tõenäoline on teatud liiki kahju tekkimine ja hinnatakse vastava kahju võimalikke negatiivseid tagajärgi.

Turvapoliitika (ingl *Security Policy*): turvapoliitikaga sõnastatakse turbega seotud eesmärgid ja üldised turvameetmed, millest saavad ettevõtte või ametiasutuse ametlikud ettekirjutused. Turvameetmete detailsemad kirjeldused kajastuvad palju laialdasemas turvakontseptsioonis.

4. Seadused ja määrused

Järgnevalt on toodud olulisemad seadused ja määrused, mis otseselt või kaudselt reguleerivad infoturbe valdkonda Eestis.

Isikuandmete kaitse seadus – seadus reguleerib isikuandmete töötlemisel füüsilise isiku põhiõigusi ja põhivabadusi, eelkõige õigust eraelu puutumatusele.

Avaliku teabe seadus – seaduse eesmärk on tagada üldiseks kasutamiseks mõeldud teabele avalikkuse ja igaühe juurdepääsu võimalus, lähtudes demokraatliku ja sotsiaalse õigusriigi ning avatud ühiskonna põhimõtetest, ning luua võimalused avalikkuse kontrolliks avalike ülesannete täitmise üle.

Infosüsteemide turvameetmete süsteem – määrusega kehtestatakse riigi ja kohaliku omavalitsuse andmekogudes sisalduvate andmekoosseisude töötlemiseks kasutatavate infosüsteemide ning nendega seotud infovarade turvameetmete süsteem.

Digitaalallkirja seadus – seadus sätestab digitaalallkirja kasutamiseks vajalikud tingimused ning sertifitseerimisteenuse ja ajatempliteenuse osutamise üle järelevalve teostamise korra.

Infoühiskonna teenuse seadus – seadus sätestab nõuded infoühiskonna teenuse osutajale, järelevalve teostamise korralduse ja vastutuse seaduse rikkumise eest

Elektroonilise side seadus – seaduse eesmärk on luua elektroonilise side arenguks vajalikud tingimused, et soodustada elektroonilise side võrkude ja teenuste arengut konkreetseid tehnoloogiaid eelistamata ning tagada elektroonilise side teenuse kasutajate huvide kaitse vaba konkurentsi soodustamise teel ja raadiosageduste ning numeratsiooni otstarbekas ja õiglane planeerimine, eraldamine ning kasutamine.

Autoriõiguse seadus – Autoriõiguse seaduse eesmärk on tagada kultuuri järjepidevus ja kultuurisaavutuste kaitse, autoriõigusel põhinevate tootmisharude ja rahvusvahelise kaubanduse areng ning luua autoritele, teose esitajatele, fonogrammitootjatele, raadio- ja televisiooniorganisatsioonidele, filmi esmasalvestuse tootjatele, andmebaasi tegijatele ning teistele käesolevas seaduses nimetatud isikutele soodsad tingimused teoste ja muude kultuurisaavutuste loomiseks ja kasutamiseks.

Karistusseadustik – seadus sätestab süütegude eest karistamise korra.

5. Niimoodi ei tohi: hoiatavad näited kahjude kohta

Näide nr 1: Andmevarunduse (*Backup*-i) tegematajätmine

Advokaadibüroo kasutab oma väikeses võrgus tsentraalselt toimivat serverit, kuhu salvestatakse kõik andmed. Server sisaldab endas lindiajamit, millele salvestatakse regulaarsete ajavahemike tagant andmete varukoopia. Andmevarundusi sisaldavaid linte hoiab administraator oma büroo lukustatavas kapis. Ühel päeval, kui serveris tekib kõvaketta defekti tagajärjel avarii, on tarvis lintide peale varundatud andmed taastada. Taastamise käigus selgub, et lindiajam on olnud juba ilmselgelt pikemat aega katki ning lintidele pole mitte mingisuguseid andmeid üldse salvestatudki. Ainus töökorras varundatud andmetega lint pärineb viie aasta tagant. Kõik viimaste aastate andmed on kaotsi läinud.

Andmetest varukoopiate tegemise planeerimisel on administraatoril jäänud kahe silma vahele veel ka üks täiendav oht: isegi juhul, kui lindiajam oleks töötanud korralikult, oleks tulekahju või muu sarnase katastroofi korral lisaks originaalandmetele hävinud ka kapis hoitud andmete varukoopiad.

Turvameetmed

- ► Regulaarne andmevarunduslintide kontrollimine
- ► Andmetaastuse kontrollimine ja harjutamine
- ► Andmevarunduslintide hoidmine väljaspool oma büroruume, nt panga hoiulaekas.

Näide nr 2: Arvutiviiruste rünnaku alla sattumine

Ettevõte kasutab laialdaselt viirusetõrjeprogramme. Viirusesignatuuride värskendamine leiab aga aset vaid pisteliselt, nt ainult operatsioonisüsteemi täiendite paigaldamise käigus. Ühel päeval laekub IT-osakonda hoiatus teatud uut liiki e-maili viiruse kohta, mis levib kulutulena üle interneti ja nakatab aina uusi ja uusi adressaate. Ettevõttel ei ole kahjuks automaatselt toimivat täiendite laadimise mehhanismi, mille abil oleks võimalik kiirkorras paigaldada kõikidesse arvutitesse uued viirusesignatuurid. Avariilahendusena ühendatakse internetist lahti meiliserverid. Viirus on aga siiski jõudnud juba tungida sisevõrku ning selle edasilevimist ei ole võimalik enam peatada. Kuna kõnealune viirus kustutab Office-dokumente, tuleb kõik arvutid võrgust lahti ühendada ja välja lülitada, kuni IT eest vastutavatel töötajatel õnnestub paigaldada igasse arvutisse ükshaaval uued viirusesignatuurid ning viiruste rünnaku ohvriks langenud arvutid suure vaevaga viirustest ära puhastada. Kogu IT-kasutus on mitmeks päevaks peaaegu seisma pandud. Hävitatud andmed, viivitused tööülesannete täitmisel ja kaotsiläinud töötunnid on tekitanud märkimisväärne kahju. Vahetult pärast töö lõpetamist tekib Internetti sellest viirusest juba uus variant, mida ei suuda eelneva vaevarikka töö käigus värskendatud viirusetõrjeprogramm veel tuvastada. Kogu töö algab jälle otsast peale.

Turvameetmed

- ► Turvatäiendite värskendamise kontseptsiooni väljatöötamine
- ► Mitte unustada ettevõttes olevaid „üksikuid IT-saarekesi“ (nt sülearvuteid ja testimisarvuteid)

Näide nr 3: Administraatori töölt kõrvalejäämine

Keskmise suurusega ettevõttes töötab administraator, kes on juba aastaid ainuisikuliselt vastutav kõikide PCde installeerimise ja konfigureerimise ning võrgu käitamise eest. Ühel päeval satub administraator raskesse õnnetusse ja pole pärast seda enam töövõimeline.

Juba mõne päeva möödudes kuhjuvad võrgus serveritega seotud probleemid: süsteem väljastab veateateid ja hoiatusi, mida kaastöötajad ei ole võimelised korrektselt interpreteerima ega läbi töötama. Veidi aja pärast on juba mitmes arvutis tekkinud avarii, arvuteid pole enam võimalik kasutada ning pärast taaskäivitust ei toimi enam üldse mitte midagi. Alustatakse otsinguid administraatori tööalases dokumentatsioonis, mille järel selgub, et olemasolev süsteemikeskkond on praktiliselt dokumenteerimata. Hoiule pole antud isegi mitte administraatori paroole. Kiire lahenduse lootuses kohalekutsutud IT-tugiteenust pakkuv firma pole puuduva parooli ja dokumentatsiooni tõttu võimeline olemasolevat süsteemi uuesti käima saama. Suure vaevaga püütakse välja selgitada serveritele installeeritud rakendusi ning asukohti, kuhu need rakendused salvestasid firma jaoks olulisi andmeid. Protsessi tuleb kaasata täiendavaid väliseid eksperte, kuna lisaks laialdaselt levinud standardsetele rakendustele tuvastatakse süsteemis ka konkreetsete tootjate individuaalseid lahendusi, millega süsteemi tarnija, kellele on tehtud ülesandeks funktsioonid taastada, pole mitte kunagi varem kokku puutunud.

Ajaks, mil kõik suudetakse taastada ja kõik igapäevatööks vajalikud süsteemid uuesti tavapärasesse töökorda seada, on möödunud mitu nädalat. Vahepealsel ajal ei suutnud ettevõte täita oma olulisi tellimusi, kuna selleks vajalik info ja rakendused ei olnud kättesaadavad. Liites antud olukorrast tekkinud kahjule juurde kulutused, mis tuli kanda IT-tugiteenuse väljastpoolt sisseostmisega, jõutakse kuuekohalise summani. Ettevõte püsimajäämine on ohus. Lisaks muule tuleb puuduvale administraatorile leida veel ka sobiv järglane.

Turvameetmed

- Süsteemiseadete ja -parameetrite põhjalik dokumenteerimine
- Paroolide turvaline hoiuleandmine
- Olulisemate avariijuhtude protseduurilisi juhiseid sisaldava avariiplaani koostamine
- Töötajate asenduskorra määratlemine

Näide nr 4: Häkkerid ründavad läbi interneti

Psühholoogi praksis ühes väikelinnas. Oma patsientide toimikuid haldab ta arvutiga, mis on varustatud internetiühendusega. Ta tunneb oma arvutit hästi ja reeglina installeerib ta vajamineva tarkvara ise. Ta usub, et tema andmed on kaitstud, kuna süsteemi sisselogimiseks peab ta sisestama parooli. Ühel päeval levib linnakeses kulutulena kuuldus, et keegi anonüümne isik on avalikustanud linna kohalikus internetifoorumis tema patsientide konfidentsiaalsed andmed. Politsei algatab juhtunu osas psühholoogi suhtes juurdluse ja jõuab järeldusele, et praksise arvuti oli volitamata juurdepääsude eest ebapiisavalt kaitstud ning tõenäoliselt oli tegu mõne häkkeri rünnakuga. Prokurör esitab süüdistuse patsientide konfidentsiaalsete andmetega hooletus ümberkäimises. Patsientidele tekitatud kahju on väga suur ning selle lõpliku suuruse hindamine on peaaegu võimatu.

Turvameetmed

- Internetiühenduse turvamine
- Konfidentsiaalsete andmete krüpteerimine

Näide nr 5: Oma töötajad

Pikkade traditsioonidega väikeettevõte toodab juba aastaid spetsiaalseid värve ja lakke vastavalt oma salajasele koostisele. Ühel päeval asub üks endine turundusosakonna töötaja tööle konkureerivasse firmasse. Pool aastat hiljem toob konkureeriv ettevõte turule peaaegu identsed lakid. Esmalt ei ole kuidagi mõistetav, kuidas said ettevõtte saladused ettevõtte ruumidest väljuda, kuna turvakaalutlustel puudub arendusosakonnal nii intranet kui ka internetiühendus. Seetõttu kahtlustab ettevõte oma endise töötaja poolt toimepandud tööstusspionaaži ja esitab tema vastu süüdistuse.

Kriminaalpolitseil õnnestub erivarustuse abil tõestada, et kahtlustatava arvutisse on salvestatud ja hiljem kustutatud kahtlasi faile, mis võisid sisaldada kõnealuseid salajasi koostisi. Seistes silmitsi antud infoga, annab kahtlustatav oma tunnistuse. Arendusosakonna ruumid ei olnud öösiti lukus ning seetõttu oli neisse võimalik märkamatult siseneda kõigil töötajatel, kelle oli olemas majavõti. Pärast tööpäeva lõppu sisenes kõnealune isik arendusosakonda ja tekitas enesele *Boot*-disketi abil paroolkaitsest mööda minnes juurdepääsu vajaminevasse arvutisse. Tema uus tööandja oli nimelt tema käest töövestlusel küsinud, kas ta toob endaga kaasa ka „väärtuslikke lisateadmisi antud valdkonna kohta“, mis võiksid teda teiste kandidaatide seast esile tõsta.

Nii vargale kui ka tema uuele ülemusele esitatakse süüdistus ning nad saavad karistada. Kahjutasu osas jõuavad puudutatud ettevõtted kohtuvälisele kokkuleppele. Sellele vaatamata on ettevõte oma konkurentsieelise suures osas kaotanud, mis muudab ettevõtte majandusliku seisu üha kehvemaks.

Turvameetmed

- Ruumide ja hoone kaitsmine volitamata sissepääsu eest
- Oluliste andmete krüpteerimine

6. Sagedasemad vajakajäämised

Analüüsides tüüpilisi vigu ja vajakajäämisi, selgub, et need pole üldsegi väga tihedalt seotud ei ettevõtete suuruse ega nende tegutsemisvaldkonnaga. Koostatud nimekirja alusel saate ka ise kontrollida, millised spetsiaalsed vajakajäämised võivad muutuda oluliseks Teie töökeskkonnas ning kuidas selliseid olukordi hinnata. Järgnev peatükk käsitleb eelpool kirjeldatud puudujääke uuesti ja näitab, kuidas neile konkreetsete turvameetmete ja mõistliku töökoormusega vastu seista.

6.1 Ebapiisav IT-turvastrateegia

Turvalisusele ei pöörata piisavalt tähelepanu

IT-turvalisusele pööratakse võrreldes teiste valdkondadega (kulutustega, mugavusega, suure funktsionaalsusega, ...) tihti palju vähem tähelepanu. IT-turvalisuses nähakse vaid suurt kuluallikat ja takistust. Eriti vähe tähelepanu pööratakse turvaomadustele just uute rakenduste või süsteemide soetamisel ning vahel jäetakse see valdkond koguni läbimõtlemata. Selle põhjused on erinevad: IT-turbevaldkond ei saa juhatuselt piisavalt tuge, ebapiisav turvaaspektide uurimine, valdkonna uued trendid, turunduslikud põhjused, liiga väike eelarve jne. Nende puudujääkide tõttu kasvab ju „ainult“ võimalik risk! Kõige õnnetumatel juhtudel lükatakse hädavajalike turvameetmete rakendamine ikka ja jälle määramata tulevikku edasi, sest iga kord lasuvad prioriteedid neil töödel, mis on vahepeal uutena juurde tekkinud.

Üheks näiteks niisugusest olukorrast on kiiresti kasvav täiesti kaitseta traadita võrkude arv alates ajast, mil vastavad WLAN-kaardid muutusid igaühele taskukohaseks. Vaimustumine uuest tehnoloogiast ja võimalus loobuda tüütutest kaablitest jätavad turbeaspektid unarusse. Lugematul hulgal firmasid „avaldavad“ seeläbi vabatahtlikult oma konfidentsiaalseid andmeid ja võimaldavad mõnikord kõigile huvilistele tasuta internetiühendusi.

Puuduvad turbetaseme säilitamiseks vajalikud kestvad protsessid

Turvalisust luuakse tihti vaid isoleeritud üksikprojektide tarbeks. Vastavad projektid on vajalikud, et alustada spetsiifiliste ülesannete täitmist ja kontrollida vajalikke asjaolusid võimalikult sügavalt. Tihti jäetakse aga niisuguste protsesside raames välja töötamata usaldusväärsed protsessid, mis suudaksid tagada projekti raames saadud tulemuste ja eesmärkide järjepideva rakendamise. Näiteks analüüsitakse väga laialdaselt võimalike kitsaskohti ja sõnastatakse soovitused nende kõrvaldamiseks. Nende hilisemal ellurakendamisel puudub aga järjekindlus. Samamoodi koostatakse uute süsteemide juurutamisel tihti detailsed juhised, kuidas peaks toimuma turvaline alusinstallatsioon. Kogemused näitavad, et hiljem, töö käigus, võivad parameetrid pidevalt muutuda. Sellele vaatamata kontrollitakse vaid väga harva, kas kõik vastab algsetele ettekirjutustele. Sellekohaseid näiteid võib leida suurel hulgal. Paljud sellised vajakajäämised viitavad organisatsiooni halvale IT-turvahaldusele: mõnikord pole teada, kes vastutavad konkreetselt turbega seotud ülesannete eest ning mõnikord ei kontrollita kokkulepitud meetmeid regulaarselt.

Turvet puudutavad ettekirjutused on jäetud dokumenteerimata

Paljudes suurtes organisatsioonides on olemas kirjalikult fikseeritud turvapoliitika koos asjakohaste rakendusjuhistega. Enamikes väikestes ning keskmise suurusega ettevõtetes ja ametiasutustes seda aga ei ole. Lisaks on paljud suunised sõnastatud liiga abstraktselt ja jätavad liiga palju tõlgendamisvabadust. Isegi kui suunised on olemas, ei edastata neid tihti sugugi mitte kõikidele puudutatud osapooltele. Tihti puudub töötajatel ka konkreetne lepinguline kohustus kehtivatest suunistest täpselt kinni pidada. See võib viia olukorrani, kus turbealaseid rikkumisi pole kas võimalik või on väga raske karistada.

Puudulikud kontrollimehhanismid ja selgitustöö nõuete rikkumise puhul

Olemasolevatest turvapoliitikatest ja turvajuhenditest on kasu vaid siis, kui nende järgimine on kontrollitav. Praktikas niisuguseid kontrolle aga tihti ette ei võeta, seda kas tehnilistel, administratiivsetel või koguni õiguslikel põhjustel. Samuti on olukord problemaatiline siis, kui töötajad tunnevad, et ei pea turvarikkumiste eest vastutama. Mõlemad olukorrad toovad endaga kaasa kehtivate ettekirjutuste ühe kasvava eiramise, suurendades seeläbi turvariski, ja päädivad reaalsete kahjudega.

6.2 IT-süsteemide halb konfigureerimine

Volituste jagamisel ei rakendata piisavas mahus vajalikke piiranguid

IT-turbe üheks kuldseks reegliks on nn. parajasti piisava informeerituse põhimõte (nn. *need-to-know principle*): iga kasutaja (ja ka iga administraator) tohiks ligi pääseda ainult sellistele andmehulkadele ja käivitada ainult selliseid programme, mis on tema igapäevatööks otseselt vajalikud. Praktikas tähendab antud põhimõtte järgimine siiski täiendavat administratiivset ja tehnilist koormust. Seetõttu ongi paljudel töötajatel juurdepääs erinevale konfidentsiaalset liiki infole ja programmidele, mida neil tegelikult ei tohiks olla. Kuna töökoha PCd ja serverid on organisatsioonides reeglina omavahel võrguühenduses, võimaldatakse juurdepääsupiirangute kehtestamata jätmisega töötajatele tihti juurdepääs ka teiste töötajate andmetele ja arvutitele. Tihti pole andmete „omanikud“ sellest isegi teadlikud. Seetõttu võib laialdaste volituste väärkasutus aset leida ka kogemata, st vajalike teadmiste puudumise tõttu.

Halvasti konfigureeritud IT-süsteemid

Praktikas tekib vaieldamatult kõige rohkem turvaauke mitte tarkvaravigade tõttu, vaid administraatorite eksimuste läbi. Kui tüüptarkvara olemasolevaid turvafunktsioone kasutataks täies ulatuses ja õigesti, oleksid ettevõtete ja ametiasutuste IT-turbetase palju kõrgem. Standardsete büroorakenduste keerukus tõuseb aasta-aastalt. Turvalisus on administraatorite jaoks nende igapäevatöös vaid üks paljude teiste, osaliselt isegi konkureerivate tööülesannete seas. Administraatorid on reaalselt vaid vaevu suutelised valesid (ebaturvalisi) parameetriseadistusi täielikult vältima. Paljudele asjast puudutatutele on see dilemma väga tuttav, kuid ilma piisava ülemustepoolse toeta on positiivsetele muudatustele lootmine siinkohal ebareaalne.

6.3 Ebaturvalised võrgu- ja internetiühendused

Tundlikud süsteemid ei ole avalike võrkude eest piisavalt kaitstud

Senikaua, kuni info ja andmed tehakse kättesaadavaks vaid sisevõrgus, jääb turvaauguga seotud potentsiaalsete kahtlusaluste hulk veel küllaltki ülevaatlikuks (kaastöötajad). Internetiühenduse puhul tuleb aga arvestada sellega, et kitsaskohti võivad hakata otsima ja ära kasutama ka anonüümsed kolmandad osapooled nagu nt häkkerid. Olemasolevate rakenduste turvaline Internetti ühendamine eeldab asjaosalistelt administraatoritelt eriteadmisi, milleta on konfiguratsioonivead peaaegu vältimatud. Tundlik informatsioon, tundlikud süsteemid ja allvõrgud jäetakse tihti hoopis kaitseta või siis kaitstakse neid avalike võrkude eest vaid puudulikult. Isegi tulemüüri kasutamine ei ütle reaalse turvaolukorra kohta tegelikult mitte midagi. Paljud IT eest vastutavad töötajad arvavad, et nende hallatavad võrgud on väljapoole kaitstud. Väliste turbespetsialistide kontrollid avastavad aga paljudel juhtudel siiski tõsiseid turvaauke.

6.4 Turbealaste ettekirjutuste eiramine

Turbemeetmed jäetakse mugavusest täitamata

Ka kõige parematest turvapoliitikatest ja turbefunktsioonidest pole midagi kasu, kui neid eiratakse või kui neid ei rakendata. Tihti jäetakse konfidentsiaalsed dokumendid või e-mailid krüpteerimata isegi siis, kui sobivad mehhanismid on täiesti käepärast. Turvalisi, reeglipäraste ajavahemike tagant muudetavaid paroole peetakse sama tüütuks nagu parooliga kaitstud ekraani pimenduspilti. Täiesti suvalisel võõral helistajal, kes väidab ennast olevat IT-osakonna uus töötaja, piisab ainult „ilusti“ küsimisest ja talle avaldatakse kõik paroolid.

Vaatamata sellele, et andmekadudega seotud riskid on kõigile osapooltele teada, tehakse andmetest, eriti sülearvutite andmetest, varukoopiaid ainult harva või jäetakse üldse tegemata. Isegi kui andmetest tehakse regulaarselt varukoopiaid, on need tihti puudulikud või sisaldavad vigu. Automaatselt toimiva varukoopiate tegemise süsteemi puhul ei tea töötajad tihti üldse, milliste ajavahemike tagant varukoopiad luuakse ning kui pika aja jooksul varukoopiate andmekandjaid säilitatakse. Sarnaseid näiteid võiks loetleda veel palju rohkem ning need kinnitavad, et kui töötajad ei aktsepteeri turvameetmeid või kui neid pole võimalik tehnoloogia abil kohustuslikuks muuta, on isegi lihtsad turvameetmed määratud läbikukkumisele. See ei kehti mitte ainult tavakasutajate, vaid ka administraatorite puhul. Viimased pööravad vaid väga harva piisavalt tähelepanu parameetriseadistuste turvalisusele. Lisaks töötavad administraatorid sageli privilegeeritud süsteemivolitustega. Seda ka juhtudel, kus see pole tehniliselt üldse vajalik, kuna nii on palju mugavam kui ennast veel teist korda sisse logida.

Kasutajad ja administraatorid on puudulikult koolitatud

Kuna ettevõtetes ja ametiasutustes kasutatavad IT-süsteemid ja rakendused muutuvad pidevalt, nõuab see töötajatelt suurt omainitsiatiivi, et suuta nendega kompetentselt ümber käia. Üha keerukamaks muutuvate süsteemide valdamiseks ei sobi aga mänguline iseõppimine, kuna tihti ei tehta seda ka mitte testimiskeskkonnas. Käsiraamatuid pole alati kohapeal olemas. Tihti pole ka aega, et neid lugeda. Koolitused ei suuda alati katta neid spetsiifilisi teemavaldkondi, mida inimestel tarvis läheb. Pealegi on igasugused seminarid reeglina küllaltki kallid ning koolituse ajaks peavad töötajad oma igapäevatööst kõrvale jääma. Pealegi ei ole üksikasjalikud teadmised ainult väljavalitud valdkondadest (nt Windows 2000st, Lotus Dominost või Apachest) enamasti piisavad, kuna siinkohal ei tegelda sisuliste ristviidetega erinevate aspektide vahel.

6.5 IT-süsteemide halb hooldamine

Saadaolevad turvatäiendid jäetakse paigaldamata

Tihti jätavad administraatorid saadaolevad turvatäiendid õigeaegselt paigaldamata. Paljud viiruste või ussviiruste tekitatud kahjud ilmnevad alles mõne aja möödudes pärast nende ilmsikstulekut. Reeglina on tootjad selleks ajahetkeks oma tarkvara turvatäiendid juba väljastanud. Enamike toodete puhul ilmuvad asjakohased turvatäiendid juba väga lühikese aja möödudes. Oma kasutuskeskkonna jaoks vajalike täiendite väljavalimine ja testimine nõuab täiendavat aega. Paljud administraatorid ootavad seetõttu ära, kuni jõuab kätte aeg, mil tuleb teha järgmine plaanipärane tarkvaravärskenduse paigaldus. Selline teguviis on hoolimatu.

6.6 Hooletu ümberkäimine paroolide ja turvamehhanismidega

Paroolidega käiakse ümber liiga hoolimatult

Enamikel juhtudel kasutatakse juurdepääsude kaitsmiseks lahendusi, mis küsivad kasutajalt parooli. Antud lahendustega kaasnevad alati probleemid, kui paroolid valitakse ebaturvalised (nt kas liiga lühikesed või liiga kergesti äraarvatavad). IT-süsteemidesse murtakse iga päev sisse, kuna ründajal on õnnestunud teada saada parool, ükskõik, kas siis süstemaatilise läbiproovimise, äraarvamise või spioneerimise teel. Eriti kergeks muudab kurikaeltele, kel on sissepääs bürooruumidesse, konfidentsiaalse info kättesaamise see, kui paroole hoitakse sõna-sõnalt arvuti klaviatuuri all või kirjutuslaua ülemises sahtlis.

Olemasolevad turvamehhanismid jäetakse kasutamata

Paljud tooted tarnitakse juba sisseehitatud turvamehhanismidega, kuid mugavusest, umbusust või ühilduvusprobleemidest tingituna jäetakse need kas sisse lülitamata või seadistatakse need liiga nõrgatoimeliseks. Näiteks traadita võrkude (WLANide) olemasolevaid krüpteerimisfunktsioone kasutatakse ainult väga harva.

6.7 Ebapiisav kaitse sissemurdmiste ja looduskahjude eest

Ruume ja IT-süsteeme kaitstakse ebapiisavalt varguste ja looduskahjude eest

Murdvarastele ja näppajatele on nende töö tihti liigagi kergeks tehtud. Ööseks praokile jäetud aknad, lukustamata IT-ruumid, järelvalveta jäetud külalised või autosse unustatud sülearvutid pakuvad kutsumata külalistele suurel hulgal võimalusi. Võrreldes riistvara kaotsiminekuga näiteks varguse või vandalismi tõttu on andmete kaotsiminek üldjuhul palju raskemate tagajärgedega. Üheltpoolt on nende taastamine seotud väga suure vaevaga. Teiselt poolt ähvardab oht, et varas võib hakata konfidentsiaalseid andmeid oma huvides ära kasutama. Katastroofe nagu tulekahjusid või üleujutusi tuleb ette küll suhteliselt harva, aga kui need siiski aset leiavad, on nende tagajärjed tihti fataalsed. Seetõttu tuleb IT-turvalisuse oluliste koostisosadena käsitleda ka tuleohutuse ja veekahjude ärahoidmise suurendamiseks rakendatavaid meetmeid, samuti voolutoite tagamist.

7. Olulised turvameetmed

7.1 Süstemaatiline lähenemine IT-turvalisusele

Piisav arvestamine IT-turvalisusega:

1.	**IT-turbeaspektidega tuleb arvestada piisavas ulatuses ja võimalikult vara kõikide projektide puhul**

Võimalikult suur programmide hulk koos paljude funktsioonidega, kasutusmugavus, madalad soetamis- ja käitamiskulud on aspektid, mis on peaaegu alati konkureerivad IT-turvalisusega. Sellele vaatamata on alati ilmtingimata soovitatav arvestada IT-turbeaspektidega juba projekti algusest peale (nt uue tarkvara soetamisel või tööprotsesside planeerimisel). Eriti oluline on vaadata kriitilise pilguga just uusi tehnikalahendusi. Siinkohal on vältimatuks eelduseks juhatuse tasandi selge toetus IT-turvalisusele seatud eesmärkidele! Hiljem tekkivad turbepuudujäägid võivad viia ebasoovitud tagajärgedeni. Kui koostamisel ja planeerimisel tehtud vead tulevad ilmsiks alles hiljem, võib nende parandamine olla tihti seotud kas vastuvõetamatult suurte kuludega või osutuda isegi võimatuks. Julgus teha kärpeid mugavuse arvelt või loobuda teatud funktsioonidest võib ära hoida suuri turvaintsidentidest tekkivaid kulusid ja suuri investeeringuid täiendavatesse IT-turvaseadmetesse.

2.	**Puuduvate ressursside puhul tuleks kaaluda alternatiivseid lahendusi.**

Tihti viib soovitud eesmärgini mitu erinevat teed. Kulukate ja pikaajaliste projektidega kaasneb suurem risk, et need võivad kas aja, raha, või muutunud raamtingimuste tõttu pooleli jätta. Seetõttu tuleks kaaluda ka alternatiivseid lahendusi, mille eesmärgid on algul veidi tagasihoidlikumad. Palju väikesi samme on palju kergem teoks teha kui ühte suurt. Ka see on omaette turbeaspektiks.

Samm sammu järel kõrgema IT-turvalisuse suunas:

3.	**Tuleb määratleda IT-turvaeesmärgid, et töötada välja asjakohased abinõud.**

IT-turvalisusega tegelema hakates on esimeseks sammuks hetkeolukorrast ülevaate loomine:

Millised on kehtivad raamtingimused? (seadused, lepingud, klientide soovid, konkurentsiolukord)?
Millist rolli mängivad ettevõtte või ametiasutuse jaoks IT ja IT-turvalisus?
Milliseid väärtusi on tarvis kaitsta (oskusteavet, ärisaladusi, isikuandmeid, IT-süsteeme)? Millised võivad olla potentsiaalsed kahjud?

Iga turvaanalüüsi hädavajalikuks koostisosaks on kaitsevajaduse kindlaksmääramine. Selle eesmärgiks on välja selgitada, kas turbealased eesmärgid ja nendest tuletatud turvameetmed on piisavad ja sobivad kokku vastavate individuaalsete oludega. Kuna raamtingimised võivad aja jooksul muutuda, tuleks regulaarselt kontrollida, kas kaitsevajadusele antud hinnang vastab jätkuvalt hetkeolukorrale või mitte. Kaitsevajaduse kindlaksmääramisel on abiks, kui lähtuda kolmest IT-turbe põhiväärtusest, milleks on *konfidentsiaalsus, terviklus ja käideldavus*.

4. **Iga sõnastatud turvaeesmärgi ja iga selle juurde kuuluva meetme kohta tuleks kehtestada asjakohased reeglid.**

IT-turvalisus on pikaajaline protsess. See väide kirjeldab väga hästi käesoleva teema peamist probleemi: enamik IT-turvalisusega seotud ülesandeid tuleb regulaarselt korrata ja uuesti läbi töötada. Iga sõnastatud meetme puhul tuleks välja selgitada, kas seda on tarvis rakendada ainult üks kord või korduvalt (näide: viirusetõrjetarkvara viirusesignatuuride regulaarne värskendamine).

5. **Koostada tuleks tegevusplaan, mis kajastaks selgelt turvaeesmärgid ja turvameetmete prioriteete.**

Igaüks, kes on IT-turvalisuse tõstmiseks vajalike mõistlike sammude üle järele mõelnud, seisab peagi silmitsi rohkemate ülesannetega, kui ta on suuteline ajaliselt ja rahaliselt ellu viima. Seetõttu on vajalik seada sõnastatud turvaeesmärgid ja turvameetmed tähtsuse järjekorda. Prioriteetide määratlemisel tuleks arvestada ka tasuvusanalüüsi tulemusi.

6. **Vältida tuleks liiga üksikasjalikke turbenõudeid.**

Turbealased ettekirjutused tuleks koostada võimalikult sellised, et neid oleks võimalik ka reaalselt täita, mitte sellised, et suurem osa töötajatest peab neid kas ebareaalseteks või koguni kiuslikeks. Lisaks on iseenesest mõistetav, et ettekirjutuste ja meetmete rakendamiseks on tarvis luua nii tehniline kui ka organisatoorne infrastruktuur. Vastasel juhul tekib oht, et igasuguseid ettekirjutusi ei võeta enam tõsiselt ning neid hakatakse üha enam ja enam eirama. Kahtluse korral tuleks nõudeid pigem natuke pehmendada ning kontrollida selle eest veidi rangemalt nende täitmist. Samuti on soovitatav kõik meetmed, mis puudutavad juba sügavalt juurdunud tööharjumusi, kasutajatega eelnevalt läbi arutada.

7. Kindlaks tuleb määrata töötajate vastutusalad.

Iga tuvastatud ülesande puhul tuleb kindlaks määrata konkreetne isik, kes vastutab selle teostuse eest. Samamoodi tuleks kõikide üldistava sõnastusega turvapoliitikate puhul täpselt kindlaks määrata, millistele töötajatele need kehtivad: kas need puudutavad ainult püsikohaga töötajaid, ühte kindlat osakonda või kõiki?

Igal vastutaval töötajal peab olema ka asendaja. On oluline, et asendaja suudaks vastavaid tööülesandeid ka reaalselt täita. Kas töötaja sai oma ülesannete täitmiseks vajalikud juhised? Kas hädavajalikud paroolid on avariijuhtudeks hoiule antud? Kas tal läheb tarvis dokumentatsioone?

8. Olemasolevad poliitikad ja töötajate vastutusalad tuleb teha teatavaks.

Ettevõtetes küsitlusi läbi viies hakkab IT-turvalisuse puhul tihti silma, et töötajad ei tunne kehtivaid poliitikaid kas üldse või tunnevad neid ainult osaliselt. Aeg-ajalt ei ole töötajad nende olemasolust üleüldse teadlikud. Seetõttu tuleks tagada, et kõik puudutatud isikud tunneksid ettevõtte turvapoliitikat selle kõige uuemas versioonis. Kõik töötajad peaksid teadma, kes on nende kontaktisikud nii ettevõttes kui ka väljaspool ettevõtet ning teadma ka nende isikute kompetentsi piire. See ei aita mitte ainuüksi probleemide puhul kiiremini abi saada. See aitab vältida ka olukordi, kus töötajaid võidakse kas suure veenmisjõu või hirmutamise abil viia selleni, et nad annavad konfidentsiaalset infot (paroole jms) edasi volitamata isikutele.

Siinkohal tuleks arvestada ka õiguslike aspektidega, et turvanõuete rikkumiste eest karistamine ei saaks lõppeda ainuüksi sellega, et süüdistatav suudab oma teguviisi õigusega välja vabandada, viidates selleks üksnes oma teadmatusele. Vajadusel on küllaltki kasulik lasta töötajatel oluliste ettekirjutuse tundmist kirjalikult kinnitada.

IT-turbe kontroll ja säilitamine:

9. IT-turvet tuleks regulaarselt kontrollida.

IT-turvalisuse taset tuleks regulaarselt hinnata ja kontrollida. Piisava eelarveressursi korral tuleks kaaluda kord aastas sõltumatute ekspertide abi kasutamist, kes kontrolliksid eriti kriitilisi IT-valdkondi. Pilk peab olema suunatud tulevikku: kas vahepeal on tekkinud uusi turvastandardeid või uusi olulisi tehnoloogiaid? Kas klientide ja koostööpartnerite ootused võivad olla muutunud?

10. Olemasolevaid tööprotsesse ja turvapoliitikaid tuleks regulaarselt kontrollida, kas need on jätkuvalt otstarbekohased ja efektiivsed.

Olemasolevate protsesside ja suuniste optimeerimine ei ole mitte ainult IT turvalisuse eest vastutava töötaja kohustus. Turvapoliitikate sõnastamise käigus tuleb tegeleda kolme põhiküsimusega: kas need on vananenud, kas need on puudulikud ning kas need on reaalselt täidetavad? Selleks, et töötajad aktsepteeriksid turbealaseid ettekirjutusi, ei tohi need tunduda tülikate ega ebamõistlikena. Nimetatud lähtepunktidele toetudes tuleks kriitilise pilguga üle vaadata kõik IT-turbega seotud tööprotsessid. Mitte miski ei suuda siinkohal asendada hinnanguid, mida annavad tööprotsessidele töötajad, kes on kohustatud neid ise täitma. Kui küsitluse tulemusel peaks selguma, et üksikuid meetmeid ei peeta sugugi otstarbekaks, tuleks üheskoos välja selgitada võimalikud põhjused ja leida neile ka lahendused.

Edasiviivad sammud:

Kahe järgnevalt kirjeldatava meetme tähendus sõltub väga suurel määral konkreetse ettevõtte või ametiasutuse suurusest. Mida rohkem töötajaid on nendest puudutatud, seda hädavajalikum ja mõistlikum on nende rakendamine.

11. Pikemas perspektiivis tuleks üles ehitada laiaulatuslik turvahaldus.

Head IT-turbetaset on suuremates organisatsioonides võimalik saavutada eelkõige siis, kui samm-sammult seatakse sisse laiaulatuslik turvahaldus. See peaks sisaldama käesolevas juhendis toodud aspekte, kuid lisaks on see veel palju põhjalikum. Küsitlused on näidanud, et ettevõtetes, kus on loodud laialdane turvahaldus, on turvaintsidentide arv märgatavalt vähenenud.

12. Kõik olemasolevad turvapoliitikad tuleks kirja panna ühtse turvakontseptsioonina.

Organisatsiooni turvapoliitikad on soovitatav dokumenteerida. Selleks on nii Internetis kui ka erialases kirjanduses ilmunud piisavalt näiteid, mida võib vabalt kasutada ja muuta vastavalt oma otstarbele. Mõnikord võib olla lihtsamaks lahenduseks võtta üle võõras, hästi struktureeritud poliitika selle asemel, et hakata aja jooksul üha kasvanud, halvasti struktureeritud ja kohati vastuolulisi oma reeglistikke ümber töötama.

Kogemused näitavad, et kõige paremini saab niisuguseid poliitikaid täiendada ja ajakohaseks muuta seeläbi, et jagada need mitmesse (vähemalt kolme) tinglikku ossa:

kõige esimeses ja abstraktsemas osas sõnastatakse ainult üldised turvaeesmärgid ja võetakse põhijoontes kokku oma organisatsiooni IT-turbealane filosoofia. See koosneb ainult mõnest leheküljest, on „juhatuskõlbulik“ ning tuleks kõige kõrgema juhtorgani poolt vastu võtta.

Teises järgmises osas tuleks detailselt sõnastada turvaeesmärgid, anda põhjalik ülevaade tehnilistest nõuetest ja sinna juurde kuuluvatest meetmetest. See osa peaks olema võimalikult detailne, kuid samas ei peaks see lähemalt kajastama ei toote eripäradega seotud aspekte ega ka tooteomadusi. Juhul kui kasutuselevõetavates toodetes ja IT-lahendustes esineb muudatusi, tuleb ka turvaeesmärke pidevalt korrigeerida.

Kolmas osa peaks sisaldama teises osas sõnastatud ettekirjutuste lahendusi konkreetsete tooteseadistuste näol ning kirjeldama ka rakendatavaid mehhanisme. Niipea kui rakendatav toode on muutunud, tuleb sisse viia vajalikud muudatused. Kahjuks esineb siinkohal tihti olukord, et algselt sõnastatud nõuded jäävad ellu viimata, kuna tootel kas ei ole vajaminevaid funktsioone või neid on keeruline rakendada. Sellisel juhul tuleb nõuded kas uuesti läbi mõelda või võtta kasutusele mõni muu lahendus. Üks on kindel: realiseerimisel esinevad puudused tuleb ilmtingimata täpselt fikseerida. Olukorrast tuleb teavitada kõiki vastutavaid töötajaid, et neil oleks võimalik tekkinud riski hinnata.

7.2 IT-süsteemide turvalisus

13. Olemasolevaid turvamehhanisme tuleks ka reaalselt kasutada.

Paljud tänapäevased programmid, mida kasutatakse tavapärases klient-server põhimõttel toimivas büroo sidevõrgus, on varustatud arvukate suurepäraste turvamehhanismidega. Turvaaugud tekivad peaaegu alati kas valest konfigureerimistest või teadmatusest, kuidas olemasolevaid võimalusi õigesti ära kasutada. Seetõttu tuleks analüüsida tootjafirma poolt lisatud turvafunktsioone, need endale selgeks teha ja ellu rakendada, et vältida olukordi, kus olemasolevad turbenõuded jäetakse kas üldse ellu viimata või viiakse ellu ainult vähikäigul. Niimoodi on võimalik tehnoloogi abil kehtestada ka selliseid turbealaseid nõudeid, mille puhul tuleks vastasel korral loota ainult töötajate koostöövalmidusele.

14. Viirusetõrjetarkvara tuleb rakendada läbivalt.

Värskena hoitava viirusetõrjetarkvara kasutamine on vältimatu. Arvutiviirused võivad levida andmekandjatel ja üle võrkude (Interneti, intraneti). Viirusetõrjetarkvara kasutamine on kohustuslik ka neis arvutites, mis ei ole Internetti ühendatud!

E-mailide ja igasuguse muu läbi Interneti toimuva kommunikatsiooni korral on soovitatav rakendada tsentraalselt toimivat viirusekontrolli. Lisaks tuleks igasse arvutisse kohapeal paigaldada viirusetõrjetarkvara, mis töötaks pidevalt taustal (*resident*). Reeglina on piisav, kui kontrollida ainult käitatavaid faile, skripte, makrofaile jms. Sellele vaatamata on soovitatav regulaarsete ajavahemike tagant (nt enne päevas või kuus ettenähtud andmete varundamist) ka kõik failid siiski üle kontrollida. Seda tuleb alati teha ka siis, kui on tuvastatud viirusesse nakatumine!

Soovitusi arvutite turvalisuse kohta leiate muuhulgas ka Arvutikaitse kodulehelt http://www.arvutikaitse.ee .

Tähelepanu:

isegi neil juhtudel, kui Teie viirusetõrjetarkvara on kõige värskemas seisus, ei tähenda see veel sugugi, et oleksite arvutiviiruste, ussviiruste või muu pahavara eest absoluutselt kaitstud. Te peate arvestama, et uute viiruste eest on Teie süsteem vähemalt senikaua kaitseta, kuni tootjad suudavad oma viirusetõrjetarkvarale sobivad viirusesignatuurid välja töötada. Ohtu kujutab endast ka pahavara, mis levib üle Interneti ja on konstrueeritud tehniliselt selliselt, et nakatab sulgemata turvaaugu kaudu otse arvuti. Üheks kuulsaks näiteks selle kohta on ussviirus „Lovsan“ (W32.Blaster.Worm), mis kasutas ära Windows 2000 ja XP turvaauku. Antud ussviirust oli võimalik peatada ainult tulemüüriga, muutes selle seadistused võimalikult piiravaks, kuid mitte tsentraalselt e-postifiltrite abil.

15. Andmetele ligipääs tuleks piirata vajaliku miinimumini.

IT-turbe üheks kuldseks reegliks on parajasti piisava informeerituse põhimõte: iga kasutaja (ja ka iga administraator) tohiks ligi pääseda ainult sellistele andmehulkadele ja käivitada ainult selliseid programme, mis on tema igapäevatööks otseselt vajalikud. Muuhulgas tähendab see seda, et ühe konkreetse osakonna (nt müügiosakonna, arendusosakonna, personaliosakonna, juhatuse jne) töötajatel ei tohiks olla võimalust piiramatult tutvuda teiste osakondade töötajate infoga, välja arvatud juhul, kui neil on seda oma tööülesannete täitmiseks tarvis. Rakendusprogrammide, eriti süsteemihalduse programmide kasutamist tohiks samuti võimaldada ainult sellistele töötajatele, kes neid ka tõepoolest vajavad.

Antud põhimõtte rakendamine ei eelda ülemäära suurt töökoormust: vajalikud volitused võetakse kokku sobivatesse volituste profiilidesse. Neile toetudes luuakse vajalikud kasutajagrupid või rollid. Süsteemikasutaja individuaalseid volitusi saab juhtida läbi tema grupikuuluvuse või läbi erinevate rollide, mis kasutajale kas lubatakse või keelatakse. Regulaarsete ajavahemike tagant tuleks kontrollida, kas pääsuõigused, mida töötaja reaalselt kasutab, vastavad töötaja tegevuste profiilile, või oleks otstarbekas neid hoopis piirata. Juurdepääsuõigustest parema ülevaate saamiseks võib oma võrku regulaarselt kontrollida sobivate tarkvaratööriistade abil. See aitab tuvastada ressursse, mille ligipääs on jäänud võib-olla tahtmatult avatuks kõigile suvalistele kolmandatele osapooltele. Paljud selleks sobivad tarkvaratööriistad on saadaval tasuta.

Samuti on tarvis luua asjakohane protsess, mille abil saaks töötajatele nende volitusi tööleasumisel, tööfunktsioonide muutumisel või töötajate lahkumise järel vastavalt kas sisse seada või tühistada.

16. Kõik süsteemikasutajad tuleks liigitada rollide ja profiilide alla.

Üksikutele isikutele või isikurühmadele juurdepääsuõigusi andes tuleks jälgida, et neile ei antaks kompotti erinevatest volitustest. Suurema hulga inimeste haldamise puhul viib niisugune teguviis paratamatult kõrge halduskoormuseni, suurendab tööde keerukust ning vastuvõtlikkust kõikvõimalikele vigadele. Seetõttu pakuvad peaaegu kõik standardsed rakendused ka võimalust luua

sobivad volituste profiilid, mille abil saab omakorda luua vajalikud rollid. Igale kasutajale omistatakse (samamoodi nagu ka igale administraatorile) üks või mitu rolli, mida tal on lubatud oma töö vältel kasutada. Ühelt poolt lihtsustab see volituste haldamist, muutes selle ühtlasi ka turvalisemaks. Teiselt poolt jällegi suurendab see ka paindlikkust, kuna töötajal on võimalik sõltuvalt oma tööülesannetest või tegevustest kasutada erinevaid rolle.

17. Administraatorite volitusi tuleks piirata vajaliku miinimumini.

Paljud süsteemiadministraatorid töötavad üheainsa administratiivse rolli alt, millel puuduvad praktiliselt igasugused piirangud ning mis võimaldab kasutada kõiki süsteemiprivileege. Selline olukord suurendab administraatori enda poolt toimepandava väärkasutuse riski ja suurendab ohtu, et kolmandad, selleks volitamata isikud suudavad administraatorirolli edukalt üle võtta. Seetõttu tuleks administraatori töö jagada võimalusel erinevateks administratiivseteks rollideks. Sõltuvalt administratiivsest rollist võivad erinevad administraatorid tegeleda nt kas ainult printerite haldamisega, uute kasutajate loomisega või andmetest varukoopiate tegemisega. Ideaaljuhul võiks olla isegi eraldi administraator, kes tegeleb logiandmete analüüsimisega ja teiste administraatorite töö jälgimisega.

18. Programmiprivileege tuleks piirata.

Täitmisprogrammid on varustatud sarnaselt kasutajatega teatud juurdepääsuõiguste ja süsteemiprivileegidega. Paljudel juhtudel pärib programm lihtsalt selle kasutaja volitused, kes programmi parasjagu käivitas. Mõnikord nendest volitustest aga ei piisa. Või siis on tegu serveriprotsessidega, mis peavad olema varustatud kõrgete privileegidega. Niisugustel juhtudel on programmid mõnikord varustatud nn *Root*-volitustega ja need võivad kasutada samamoodi nagu üks „kõikvõimas“ süsteemiadministraator ka kõiki süsteemiressursse. Kui ründajal õnnestub selline programm oma käsutusse saada, pärib ta ka kõik vastava programmi volitused. Ka programmidele tohib anda vaid sellised volitused, mis on hädavajalikud nende veatuks funktsioneerimiseks.

19. Tootja standardsed algseadistused tuleb kohandada oma vajadustele sobivaks.

Paljud operatsioonisüsteemid ja tarkvararakendused on tootjate poolt väljastatud juba sellise algseadistusega, mis lubab neid pärast paigaldamist võimalikult sujuvalt ja mugavalt kasutama hakata. (Sama väide kehtib ka terviklike IT-süsteemide ja kodukeskjaamade kohta). Standardse installatsiooni koostamisel ei mängi IT-turbeaspektid tootja poolt tehtud valikute puhul mitte mingisugust rolli. Pakutav mugavus meeldib vaieldamatult kõikidele kasutajatele, kes ei tunne puudutatud süsteemi või pole sellega piisavalt tuttavad. Aluskonfiguratsiooniga piiratakse toote olemasolevaid funktsioone võimalikult vähe, mis lubab omas keskkonnas segamatult sidet pidada. Tihti on tootja poolt sisseseatud standardsed paroolid ja kasutajakontod. Väärkasutuse vältimiseks tuleb need desaktiveerida. Seega ei tohiks värskelt installeeritud süsteemi, mis ei ole veel oma (turbe-) vajadustega kooskõlla viidud, mitte kunagi otse igapäevasesse kasutusse üle võtta!

Eriti tuleks karastada avalike arvutite ja olulisemate serverite operatsioonisüsteeme. Niinimetatud karastamine (ingl *hardening*) tähendab IT-turbe puhul seda, et tootest eemaldatakse kõik sellised tarkvarakomponendid ja funktsioonid, mis ei ole vastava programmi tööks hädavajalikud. Tihti õnnestub ründajal serverisse sisse murda mõne programmi kaudu, mis ei peaks üldse olema sellele serverile installeeritud. Pealegi, mida rohkem programme arvuti sisaldab, seda rohkem kulub aega arvuti regulaarsele hooldusele ja värskendusele. Neil põhjustel tuleks kõik ebavajalikud rakendusprogrammid eemaldada. Sama kehtib ka üksikute tarkvaratööriistade, draiverite, komponentide jms kohta. Lõpliku lahendusena on võimalik eemaldada isegi üksikuid ebavajalikke käske (nt operatsioonisüsteemi rutiine ehk standardprogramme).

20.	**Käsiraamatuid ja toote dokumentatsiooni tuleks lugeda võimalikult varakult.**

Kogenud administraator võib olla paljudel juhtudel suuteline erinevaid süsteeme tööle panema ka ilma käsiraamatut lugemata. Selline edu osutub aga tihti petlikuks. Näiteks võivad tähelepanuta jääda tootja hoitavad teated, mille eiramisel võivad hiljem tekkida üllatavad probleemid: ühilduvusprobleemid, süsteemi avariid või avastamata jäänud kitsaskohad. Tootja poolt pakutavate abivahendite ja info ignoreerimine on märk hoolimatust ja ebaprofessionaalsest tegevusest, kuna sellega võetakse ebavajalikke riske.

21.	**Installeerimistööde ja süsteemi kohta on tarvis koostada põhjalik dokumentatsioon, mida tuleb regulaarselt värskendada..**

Enne installeerimistöödega alustamist, installeerimise käigus ja pärast installeerimise lõppemist on soovitatav vastavad tööetapid kirja panna. Korduvate tööde puhul aitab see jõuda kiiremini soovitud eesmärgini ja tuvastada probleemide korral kiiremini nende põhjuseid. Samuti on oluline, et süsteemi dokumentatsioon oleks mõistetav ka kolmandatele (nt „asendusadministraatorile“ või puhkuse ajaks leitud asendajale). Sellega vähendatakse avariide tekke ohtu juhtudel, kui vastutav administraator peaks töölt väga ootamatult kõrvale jääma. Õnnestunud häkkerirünnaku puhul suudetakse seeläbi kiiremini tuvastada ka süsteemis tehtud volitamata muudatusi.

7.3 Võrgu- ja internetiühendused

Enamikele kasutajatele, kes on varustatud internetiühendusega, on tähtsamateks internetirakendusteks nende e-mail ja veebilehitseja. Seetõttu pole ka ime, et just siin on varjul väga palju ohtusid. Failide allalaadimise käigus võidakse muuhulgas sisse tuua ka pahavara, mida viirusetõrjetarkvara ei pruugi alati tuvastada. Internetis surfates võidakse käivitada ebasoovitud protsesse, ennekõike siis, kui lubatakse käivitada igasugust kahtlase sisuga materjali (vt lisaks meede nr 26).

22. Võrkude kaitsmiseks tuleb kasutada tulemüüre.

Mitte ühtki arvutit, mida kasutatakse tööotstarbel, ei tohi ühendada Internetti, ilma et kasutataks sobivat tulemüüri!

Ka suurte sisevõrkude puhul leidub tavaliselt mitmeid, erinevate kasutajagruppide ja erinevate kaitsevajadusega alamvõrke. Seetõttu peab „oma" alamvõrku tihti naabervõrkude eest kaitsma, et ennetada ohtusid, mis on kvalitatiivselt võrreldavad Internetist tulenevate ohtudega (nt ettevõtte personaliosakonna võrgu eraldamine ettevõtte ülejäänud võrgu eest). Sel põhjusel peaksid kaitsemehhanismid olema installeeritud ka võrgu üleminekutesse.

Mis asi on tulemüür?

Tulemüür on riistvarast ja tarkvarast koosnev süsteem, mis kontrollib võrkudevahelisi ühendusi ning selle peamiseks eesmärgiks on kaitsta oma võrku (intranetti) rünnete eest, mida sooritatakse Interneti vahendusel. Tulemüürid algavad lihtsatest, osaliselt ka tasuta arvutiprogrammidest (ingl Personal Firewall), mis kaitsevad enamasti ainult seda arvutit, millesse need on installeeritud. Suuremates võrkudes kasutatakse seevastu juba keerukamaid tulemüürisüsteeme, mis koosnevad mitmetest riist- ja tarkvarakomponentidest.

23. Turvaline tulemüür peab täitma teatud miinimumnõudeid.

Sisevõrgu kaitsmiseks vähem usaldusväärsete naabervõrkude eest tuleb valida sobiv tulemüüri tüüp. Tulemüüri arhitektuuri puudutava kontseptsiooni väljatöötamine ja tulemüüri installeerimine peaks jääma spetsialistide pärusmaaks. Reeglina on soovitatav kasutada mitmeastmelist tulemüüri kontseptsiooni, mille puhul on võimalik järele ühendada veel ka täiendavaid filtrielemente (nt marsruutereid). Erijuhtumite puhul, kus on tegemist nt ühe ainsa arvutiga või kus keeruline tulemüürisüsteem ei tule muudel põhjustel kõne alla, suudab kaitset vajavale arvutile vähemalt baasturvet pakkuda ka nn *Personal Firewall*.

Tulemüüride filtreerimisreeglid muutuvad aja jooksul üha pikemaks ning nende ülevaatlikus kipub kaduma. Tulemüüride administraatorid annavad tihti liiga palju järele kasutajate poolt tagantjärele esitatud nõudmistele ja nõrgendavad reegleid. Ka ülemusele ei tohiks siinkohal teha mitte mingisuguseid erandeid! Seetõttu on vaja regulaarselt kontrollida, kas olemasolevad filtreerimisreeglid on piisavalt terviklikud, kas neid oleks võimalik lihtsustada ning kas need kehtestavad piisavas mahus vajalikke piiranguid. Peale selle tuleks aeg-ajalt kontrollida, kas olemasoleva tulemüüri kontseptsiooni poolt loodav IT-turvalisus vastab kas juba juurutatud või lähiajal kasutuselevõetavate sideprotokollide nõuetele. Samuti võivad kehtivatele tulemüüri kontseptsioonidele uusi nõudeid esitada ka uued kasutuselevõetavad tehnoloogiad. Põhjalikke tehnilisi juhiseid tulemüüride (turvalüüside) kohta leiate Riigi Infosüsteemide Arenduskeskuse internetilehel (http://www.ria.ee/ISKE) olevast ISKE rakendusjuhendi dokumendist.

Täiendavat infot tulemüüri arhitektuuri kohta

Ka tulemüür ise võib langeda rünnaku ohvriks. Mitmeastmeliselt koostatud turvastrateegiad on vajalikud selleks, et tagada minimaalse kaitse säilimine ka siis, kui tulemüüri üks komponent on langenud rünnaku ohvriks.

Kõikvõimalikud serverid, mis vajavad oma funktsiooni tõttu otsest internetiühendust ja on internetist eraldatud vaid tulemüüride või teiste kaitsemehhanismide (nt prokside) abil, tuleb paigutada nn demilitariseeritud tsooni (DMZ). Üldise turvalisuse tagamisel mängib siinkohal olulist rolli serverite õige asetus üksteise suhtes kaskaadis ja nende jaotamine DMZi erinevate alamvaldkondade vahel (koos oma IP-aadressidega).

24. Väljapoole pakutavate andmete hulka tuleks piirata vajaliku miinimumini.

Paljusid tundliku sisuga andmeid tehakse kasutajatele kättesaadavaks ka läbi avalike võrkude. Seeläbi muutuvad konfidentsiaalsed andmed väljast ligipääsetavaks. Nende kaitsmine sõltub eranditult vaid usaldusväärsetest autentimis- ja autoriseerimismehhanismidest. Kui viimased on aga valesti konfigureeritud või kui need sisaldavad turvaauku, satuvad kaitset vajavad andmed kergesti valedesse kätesse. Nimetatud vigade esinemine on pigem reegel kui erand. Seetõttu tuleks iga konkreetse juhtumi puhul kontrollida, kas tundlikke andmeid on üleüldse tarvis kättesaadavaks teha või töödelda väljaspool oma hästi kaitstud võrku.

25. Väljapoole pakutavaid teenuseid ja programmide funktsioone tuleks piirata vajaliku miinimumini.

Kõikvõimalikud väljapoole pakutavad funktsioonid, serveriteenused ja avatud sidepordid tõstavad turvaaukude tekkimise riski. Seetõttu tuleks iga juhtumi puhul hoolikalt kontrollida, kas potentsiaalseid ohuallikaid on üleüldse tarvis aktiveerida ja väljapoole pakkuda või mitte. Sellega kaasnev turvarisk võib olla sõltuvalt kasutatavast tehnoloogiast ja juurutamisviisist väga erinev. Kasutuses olevate lahenduste puhul tuleks regulaarselt kontrollida, kas leidub üksikuid teenuseid või funktsioone, mida mitte keegi ei kasuta, aga mis on siiski kas kogemata või mugavuse tõttu sisse lülitatud. Sarnaste piirangutega saavutatakse hoitakse muuhulgas kokku administraatori tööaega, mida on võimalik palju otstarbekamalt kulutada nt teiste protsesside administreerimiseks, mis tagab suurema turvalisuse.

26. Veebilehitsejatega ümberkäimisel tuleb olla eriti ettevaatlik ja riskantsed tegevused tuleks keelata.

Veebilehitsejates tohiks lubada kasutada ainult selliseid skriptikeeli ja multimeedia pistikprogramme (*PlugIn*), mis on tõepoolest tööks hädavajalikud. Eriti kriitilised skriptikeeled tuleks igal juhul desaktiveerida.

Täiendav info

Vastavad skriptid, protokollid või lisaprogrammid, mida Teil konkreetselt tuleks vältida, võivad tehnoloogia arengu tõttu korduvalt muutuda. Ajakohast infot riskantsete tehnoloogiate kohta leiate vastavatelt internetilehtedelt. Hetkel kuuluvad eriti ohtlike tehnoloogiate alla ActiveX, Active Scripting ja JavaScript.

27. Ettevaatust e-mailide manustega.

Sissetulnud meilidega kaasasolevad kahjulikud manused kujutavad endast suurt ohtu, kui need käivituvad soovimatult. Mitte ükski kasutaja ei tohiks selliseid manuseid sinisilmselt ilma kontrollimata avada. Viirusetõrjetarkvara kasutamine on kohustuslik! Kahtluse korral peaks adressaat enne manuse avamist konsulteerima meili saatjaga. Eriti ohtlikud on sellised e-maili-programmid, mis avavad manused automaatselt, ilma kasutajalt selleks eelnevalt luba küsimata. E-mailide manuste automaatset avamist saab tehniliselt vältida seeläbi, et valitakse e-maili-programm, millel puudub vastav funktsioon, tehakse vajalik konfiguratsioon või kasutatakse täiendavaid programme.

28. Paljude Internetiga seotud turvaprobleemide lahendamiseks piisab eraldiseisva surfamiseks mõeldud Interneti PC sisseseadmisest.

Üheks lihtsaks ja soodsaks lahenduseks, kuidas Internetis surfamisest tingitud arvukaid ohtusid minimeerida, on sisse seada eraldiseisev Interneti-PC, millel puudub ühendus kogu ülejäänud sisevõrguga. Sellist arvutit võib kasutada Internetis teostatavateks otsinguteks, ilma et peaks loobuma vajalikest funktsioonidest ja kasutusmugavusest. Sellises arvutis võib kontrollida ka allalaetud faile viiruste suhtes ning seejärel võib need kas andmekandjatel või e-maili vahendusel sisevõrku edasi transportida.

Täiendavad meetmed

Turbemeetmed on soovitatav muuta tehnoloogia abil kohustuslikuks, et kasutajad ei saaks turvamehhanisme kas väärkasutusest või koguni ettekavatsetult välja lülitada ega nendest mööda hiilida.

Ohtlike skriptide edasikandumist surfamise käigus ja potentsiaalselt ohtlike e-postimanuste levikut saab tõkestada tulemüüri tsentraalse seadistuse ehk niinimetatud proksi kasutamise abil.

7.4 Inimfaktor: turvanõuete tundmine ja järgimine

29. Turvapoliitikaid ja turvanõudeid tuleb järgida

Turvapoliitikatest on kasu vaid siis, kui neid järgitakse. Ka kõige paremates turvafunktsioonidest ja -programmidest pole mitte mingisugust kasu, kui neid ei kasutata. Kõikide vajalike turvanõuete järjepidev kasutamine eeldab igalt töötajalt pidevat osalemist õpiprotsessis ning see hakkab jätkusuutlikult funktsioneerima alles siis, kui nende järgimisest on saanud rutiinne tegevus. Kõikidel töötajatel peaksid olema IT-turbest vähemalt algteadmised, nad peaksid alati kaasa mõtlema ja suutma ohtusid hinnata. Ka kõige täiuslikumad turvapoliitikad ei suuda iialgi piisavalt arvestada kõikide igapäevatöös esineda võivate turbeaspektidega.

30. Töökohas peaks valitsema kord ning konfidentsiaalne info ei tohi olla vabalt ligipääsetav.

„Kord peab olema!“ Selle ütluse kohta võidakse olla eri meelt. IT-turbe puhul on korrast kinnipidamine kahtlemata tõhus vahend, mis võimaldab vältida arvukaid ohte. Konfidentsiaalset infot sisaldavad andmekaustad tuleks töökohalt lahkudes panna kas kappi või seifi luku taha. Kui andmekandjad nagu lindid, disketid või CD-ROMid sisaldavad konfidentsiaalset infot, ei tohiks ka need niisama avalikult ringi vedeleda. Vajadusel tuleks andmekandjad andmete volitamata taastamise vältimiseks nõuetekohaselt utiliseerida. Konfidentsiaalseid andmeid sisaldavad väljatrükid tuleb suunata purustisse, mitte visata tavalisse paberikorvi. Kõvakettad ja CD-ROMid tuleb kas turvalisel moel kustutada või hävitada.

Antud meetme rakendamise eelduseks on muidugi asjaolu, et turbevajaduse väljaselgitamise käigus on teatud andmed ja kaustad liigitatud konfidentsiaalseteks ning töötajad on vastavate ettekirjutustega kursis.

31. Hooldus- ja parandustööde käigus tuleb järgida spetsiaalseid ettevaatusabinõusid.

Suurim oht konfidentsiaalsete andmetega tutvumiseks või nende rekonstrueerimiseks kolmandate isikute poolt (reeglina isegi defektsetelt andmekandjatelt) esineb juhtudel, kus arvutid või kõvakettad viiakse kas parandusse või visatakse minema. Sel põhjusel ei tohiks mitte kunagi jätta hooldefirma tehnikuid IT-süsteemide või kodukeskjaama juurde järelvalveta. Kui andmekandjad lahkuvad majast, tuleb neist enne kõik andmed hoolikalt kustutada.

Tähelepanu: failid, mis on kustutatud tavapäraste meetoditega, on hiljem spetsiaalsete tööriistade abil jätkuvalt kas täielikult või osaliselt loetavad. Olulised failid tuleb seetõttu kustutada turvaliselt. Enamlevinud operatsioonisüsteemide jaoks on selleks saadaval lisaprogrammid.

32. Töötajaid tuleb regulaarselt koolitada.

Paljud vead tekivad kas teadmatusest või probleemide puudulikust teadvustamisest. See väide kehtib otse loomulikult ka IT-turbe kohta.

Regulaarne täiendõpe on vältimatu eriti just administraatorite ja IT-turbe eest vastutavate töötajate puhul. Ka kitsa eelarvega aegadel ei tohiks koolitusmeetmetest siiski täielikult loobuda, seda ka juhul, kui kallite meetmete rakendamine nagu nt seminaride külastus ei tule kõne allagi. Hea erialase kirjanduse ost tasub ennast alati.

Koolitused ei tohiks aga piirduda ainult tehniliste teemadega. Turvalisuse ahela kõige nõrgemaks lüliks on siiski peaaegu alati mõni kaastöötaja. USA kongressi ees esines kunagi üks laialdaselt tuntud „ekspert“ väitega, et tal õnnestus illegaalsel teel nimekate suurettevõtete võrkudesse tungida ja sealt infot varastada. Ainult harva kasutas ta selleks tehnilist laadi rünnet, enamjaolt olevat olnud küllaltki lihtne viia asutuste töötajaid selleni, et need talle vajalikud turvakoodid lihtsalt edasi annaks.

Seetõttu on tarvis regulaarselt rakendada meetmeid, mis suudaks tõsta kõigi kaastöötajate teadlikkust turbe olemusest (ingl *Security Awareness*). Selleni võib jõuda erinevaid teid pidi: organisatsioonisisesed loengud, ringkirjad, plakatid, näitlikustavad materjalid, turvaintsidentide avaldamine jms.

Väga oluline on töötajaid teavitada ka sellest, millisel kujul on võimalik suhelda oma koostööpartneritega: kes on kontaktisikud? Milline on nende kompetents? Kuidas toimub autoriseerimine? Millist infot tohib edasi anda organisatsioonivälistele töötajatele?

Ka sidekanalid peavad olema selged: millist infot tohib vahetada e-mailide vahendusel? Millised on koostööpartnerite õiged telefoninumbrid või veebiaadressid?

Üha sagedamini esineb olukordi, kus petturid püüavad vale identiteedi alusel loodud e-mailidega suunata pahaaimamatuid internetikasutajaid võltsitud veebilehtedele (nt pankade kodulehtedele) ja nõuavad seal salajase info nagu PIN-koodi, parooli või TANi *(Transaction authentication number)* sisestamist (*Phishing*).

33. Edasi aitab liikuda vaid aus enesehinnang: mõnikord tuleb pöörduda ekspertide poole.

Kõikide IT-turbeaspektide kohta ei pruugi olla organisatsioonis alati ilmtingimata kogu vajalikku oskusteavet. Praktiline kogemus näitab, et kvalifikatsiooni tõstmise meetmetest ei piisa, kuna kõnealused isikud on vastavate erialaste nõuetega juba ainuüksi ajaliselt üle koormatud. Siinkohal tuleks läbi mõelda ja uuesti kehtestada töötajate vastutusalad. Paljudel juhtudel on soodsamaks lahenduseks kasutada välist abi või jagada spetsiaalsed ülesanded ära erinevate teenusepakkujate vahel. Oma võimete ülehindamine või kokkuhoid vales kohas võivad olla väga raskete tagajärgedega.

34. Kõikide eksisteerivate turbealaste ettekirjutuste jaoks tuleb üles ehitada kontrollimehhanismid.

Kõikide turvet puudutavate ettekirjutuste ülimaks eesmärgiks on alati saavutada töötajatepoolne mõistmine, arusaam nende vajalikkusest ja nende vabatahtlik järgimine. Ettekirjutuste järgimine võib siiski ka erinevatel põhjustel läbi kukkuda. Teadlik eiramine on siinkohal pigem erand. Pigem on peamisteks põhjusteks hoopis eksimused ja järeleandmised. Nende vältimine sobivate abinõude abil on kõigi osapoolte huvides. Sel põhjusel tuleks iga olemasoleva turbeettekirjutuse korral kohe välja mõelda ka see, kuidas hakatakse kontrollima vastava ettekirjutuse täitmist. Kontrollimine võib olla lahendatud nt tehniliste kontrollitööriistade abil, audiitorite või revidentide kaasabil, olemasolevate logiandmete analüüsimise teel, ülemuste poolt läbiviidavate pisteliste kontrollidena jne. Enesekontroll, nt vastavate kontrollnimekirjade läbitöötamine, ei tohiks võimalikest valikutest kindlasti mitte olla viimane. Vajadusel võib kehtestada nõude, et töötajad peavad täidetud kontrollnimekirjad allkirjastama ja edasi andma.

35. Turvanõuete rikkumistega kaasnevad tagajärjed tuleks kindlaks määrata ja avalikustada.

Kõikidele puudutatud osapooltele peaks olema teada, et nii ettekavatsetult kui ka kogemata toimepandud turvameetmete rikkumistel on omad tagajärjed. Antud asjaolu rõhutamiseks tuleks selgesõnaliselt (nt organisatsioonisiseses turvapoliitikas) ära märkida, milliste tagajärgedega tuleb arvestada tõsiste juhtumite puhul.

36. Turvanõuete tuvastatud rikkumisi tuleks ka reaalselt karistada.

Turvanõuete rikkumiste tuvastamise korral tekib ikka ja jälle küsimus, kuidas peaksid ülemused oma alluvast rikkuja suhtes käituma. Karmid karistused ei ole kergete rikkumiste puhul kindlasti sobilikud, eriti veel, kui tegu on esimese korraga. Samamoodi on aga ka vale suured rikkumised või nende järjekindel eitamine hoopis karistamata jätta. Selline teguviis edastab ainult valesid signaale mitte ainult rikkujatele, vaid ka neile, kes sellest kuulevad. Seetõttu tuleb sündmustele adekvaatselt reageerida. Niipalju kui see on konkreetses olukorras võimalik, tuleks kõigile selgeks teha, et rikkumistele järgnevad ka sanktsioonid.

7.5 IT-süsteemide hooldamine: turvalisust puudutavate värskendustega ümberkäimine

37. **Turvatäiendeid tuleb paigaldada regulaarselt.**

Kõige suurema prioriteediga turvatäienditeks on mõnikord lausa ülikiirelt levivate arvutiviiruste tõttu viirusetõrjetarkvara turvatäiendid. Samuti tuleks regulaarselt värskendada veebilehitsejaid, e-posti-programme ja operatsioonisüsteeme. Regulaarselt tuleb värskendada ka kogu ülejäänud rakendustarkvara ja teatud riistvarakomponente.

38. **Turvakaalutlustel rakendatava tarkvara suhtes tuleks regulaarsete ajavahemike tagant läbi viia põhjalikud uuringud.**

IT-süsteemide turvalisuse tagamiseks on hädavajalik, et regulaarselt hangitaks uut informatsiooni avastatud turvaaukude ja nende likvideerimiseks kasutatavate abivahendite kohta. Otsinguid kergendavad värsked soovitused Internetis ja erialastes väljaannetes. Programmide „uuemates" versioonides (nt veebilehitsejate puhul) on turvaaugud reeglina tootja poolt juba kõrvaldatud. See aga ei tähenda, et võiksite individuaalsest lähenemisest loobuda, kuna uued versioonid sisaldavad reeglina ka uusi funktsioone ja vigu, mis võivad endaga kaasa tuua veel hoopis teistsuguseid ohtusid.

Iga töötaja, kes vastutab süsteemide eest, peaks regulaarsete ajavahemike tagant leidma endale vajaliku aja, et viia läbi vastavad internetiotsingud ja vahetada kogemusi oma ala spetsialistidega. Jätkuvalt on saadaval suur hulk tasuta infoteenuseid, mille kvaliteet on tihti palju kõrgem kui tasuliste pakkujate oma.

Kuna igasuguseid värskendusi ja uusi turvapaiku ilmub pidevalt suurel hulgal, on tarvis asjakohast valikuprotsessi. Reeglina ei ole kõiki neid võimalik installeerida kohe ja kindlasti mitte hädaabilahendusena. Seetõttu peaks juba eelnevalt olema välja töötatud põhimõtted, et oleks teada, missuguste valikukriteeriumite alusel otsustatakse, milliseid värskendusi tohib ja milliseid peab installeerima ning millises ajanihkes see peaks toimuma.

39. **Vajaminevate turvatäiendite paigaldamise jaoks tuleks koostada töökava.**

Isegi kui süsteemi eest vastutav töötaja jätab olulised turvatäiendid paigaldamata, ei tähenda see veel, et süsteem peaks selle tõttu automaatselt seisma jääma või et sellele järgneb vahetult mõni häkkerirünnak. Seega on kindel, et täiendite paigaldamine nõuab suurt distsipliini, mistõttu peaks see juba algusest peale olema juurutatud konkreetse protsessina. Eriti oluline on, et täiendite võimalikult kiirest paigaldamisest kujuneks välja rutiin just viirusetõrjetarkvara puhul.

40. Tarkvaramuudatusi tuleks testida.

Teoorias tuleks kõik tootmisrežiimi tarkvarasse sisseviidavaid muudatusi eelnevalt põhjalikult testimiskeskkonnas kontrollida, et kõik süsteemid töötaksid pärast muudatuste sisseviimist sujuvalt edasi. Ka viirusetõrjetarkvara täiendid ise on suutnud ettevõtete võrke täiesti seisma panna, kuna programm identifitseeris ettevõtte oma tarkvara ekslikult uue viirusena ja lülitas selle seetõttu välja.

Oluliste turvatäiendite testimine toimub suurel ajasurvel, kuna on väga oluline, et need saaksid paigaldatud võimalikult kiiresti. Praktikas tähendab see seda, et mõistliku kompromissi leidmiseks tuleb administraatoritel kõik IT-turvanõuded ja olemasolevad ressursid väga hoolikalt läbi kaaluda.

7.6 Turvamehhanismide kasutamine: paroolide ja krüpteerimisega ümberkäimine

41. Turvamehhanismide valikul tuleb olla väga põhjalik.

Paljud tootjad on oma toodetesse juba lisanud erinevaid valikuliselt kasutatavaid turvamehhanisme nagu paroolkaitset või krüpteerimist. Turvaliste krüpteerimisprotseduuride loomine on ülimalt keeruline teadus. On täiesti võimatu, et tootearendajad, kes pole antud valdkonnaga pikki aastaid tegelenud, suudaksid luua turvalisi protseduure. Sellele vaatamata leidub ikka veel suurel hulgal tootjaid, kes pakuvad oma toodetes enda poolt arendatud krüpteerimismehhanisme, mis on reeglina küllaltki ebaturvalised. Juhul kui turvalistest protseduuridest ollakse suuresti sõltuvad, tuleks vaadata kriitilise pilguga, millist protseduuri tootja kasutab. Võimalusel peaks olema tegu standardiseeritud, üldtunnustatud algoritmidega.

Isegi siis, kui teatud turvafunktsiooni suhtes ollakse kahtleval seisukohal, on soovitatav, kui parematoimelised ei tule kõne alla, seda siiski kasutada. Halb kaitse on siiski parem kui kaitse puudumine. Olemasolevaid kaitsemehhanisme tuleks aga sellisel juhul käitada kõige kõrgemas turvaastmes. Praktikas kasutavad paljud *online*-teenuste pakkujad nt SSL-krüpteeringu puhul, arvestades vanemate veebilehitsejate omadustega, ikka veel ebaturvalist 40-bitist võtmepikkust.

42. Kasutada tuleb hoolikalt valitud (turvalisi) paroole.

Halvasti valitud paroolid asuvad kõige sagedamaini esinevate IT-turvalisuse puudujääkide pingereas küllaltki tipus. Eriti kipuvad neid vajakajäämisi ära kasutama häkkerid. Selleks, et kaitsta ennast häkkerite tööriistade vastu, mis proovivad täiesti automatiseeritult läbi kõikvõimalikud tähemärkide kombinatsioonid või mis töötavad parooli leidmiseks läbi terveid sõnaraamatuid enamlevinud sõnakombinatsioonide ja neile lisatud numbrite kohta, peab parool vastama teatud kvaliteedinõuetele. Parool peaks olema pikem kui seitse tähemärki, seda ei tohiks esineda sõnaraamatutes, see ei peaks

sisaldama nime (kindlasti tuleks vältida kirjandusest või filmist pärit lemmikkangelase nime) ning see peaks sisaldama ka viitemärke või numbreid. Viimase puhul tuleks aga vältida liiga levinud variante, nagu lihtsalt numbrite lisamist parooli lõppu või mõne enamlevinud viitemärgi nagu „$, !, ?, #“ lisamist muidu väga lihtsa parooli algusesse või lõppu.

Vägagi mõistlik nõue, et parooli tuleks regulaarsete ajavahemike tagant muuta, tekitab suure dilemma: kõiki paroole on väga raske endale meelde jätta. Välja arvatud mõningate erandite puhul, mis jäävad kõrgturvalisuse valdkonda, on seetõttu lubatud oma paroole üles kirjutada ja need turvalisse kohta hoiule panna (mis ei tähenda otse loomulikult seda, et neid võiks hoida monitori küljes või kirjutuslaua ülemises sahtlis).

Probleemi kujutab endast harjumus kasutada ühesuguseid paroole paljudel erinevatel otstarvete ehk kasutajakontode puhul. Kui parool peaks ühest rakendusest valedesse kätesse sattuma, proovib oskaja ründaja selle parooli kindlasti läbi ka muudes rakendustes, mida see isik kasutab. Seetõttu tuleks iga kasutusjuhu puhul hinnata, millised võivad olla sellise „töö lihtsustamise“ võimalikud tagajärjed.

43. Eelseadistatud või tühjad paroolid tuleb ära muuta.

Mõningad tarkvaratooted lahkuvad tootja juurest seisundis, mille puhul on kontod ja nende paroolid kas tühjad või on kõik ühesugused ja kõigile teada. Paljud häkkerid teavad seda ja proovivad rünnete puhul esmalt läbi, kas kontode puhul pole unustatud neid uute paroolidega varustada. Seetõttu tuleks värskelt installeeritud toodete puhul käsiraamatutest järele uurida, kas tootel on sellised kontod või mitte. Turvaprobleemi kujutavad endast ka hooldefirmad, kes kasutavad välise hooldusjuurdepääsu jaoks kas halbu või koguni ühesuguselt seadistatud paroole. Üksikjuhtumitel on tuvastatud, et tootjad on jätnud programmi dokumentatsioonis kajastamata, et nende programm on varustatud nn tagaustega (ingl *backdoors*), mille eesmärgiks on nt tagada tugiteenuse osutamisel lihtne administreerimisjuurdepääs. Seetõttu peaks kas tootjafirma või hooldusfirma konkreetselt kinnitama, et nemad selliseid meetodeid ei kasuta.

Antud hoiatus ei kehti mitte ainult IT-süsteemide, vaid ka moodsate kodukeskjaamade puhul.

44. Töökohalt lahkudes peaksid töökohaarvutid olema kaitstud ekraani pimenduspildi ja paroolikaitsega.

Iga levinud operatsioonisüsteemiga kaasneb võimalus klaviatuuri ja monitori teatud ooteaja möödudes lukustada. Lahtilukustamine toimub alles pärast korrektse parooli sisestamist. Ekraani pimenduspilte tuleks kasutada juhtudel, kui volitamata kolmandatel isikutel on võimalus arvuti õiguspärase kasutaja lühikese eemalviibimise tõttu saada juurdepääs tema arvutile. Lukustusfunktsiooni ooteaega ei tohiks seadistada liiga lühikeseks, kuna vastasel korral hakkab see kasutajat ennast segama. Tihti kasutatakse ajalise piiranguna viit minutit alates viimasest kasutajasisestusest. Lisaks peaks olema võimalus lukustust vajadusel ka kohe sisse lülitada (Windowsi all jõutakse antud valikuni klahvikombinatsiooniga Ctrl+Alt+Del).

45. **Tundlikke andmeid ja süsteeme tuleb kaitsta.**

Hiljemalt siis, kui kellelgi õnnestub luua endale otsene juurdepääs konfidentsiaalset infot sisaldavale kõvakettale, on kõik krüpteerimata andmed vabalt loetavad. Ekspertidest ründajate vastu pakuvad operatsioonisüsteemide või rakenduste enda sisseehitatud kaitsemehhanismid vaid vähe kaitset. Seepärast tuleks konfidentsiaalsete failide puhul kaaluda nende krüpteerimist. Sülearvutid tuleks võimalusel krüpteerida täielikult, kuna neid on eriti lihtne varastada. Häid tooteid leiab nii vähese raha eest kui ka päris tasuta. Tootevalikul tuleks arvestada, et selleks kasutatud kaitsemehhanismid oleksid hinnatud turvaliseks. Tootjate omaarendused on harva turvalised. Informeerige ennast turvaliste algoritmide ja võtmepikkuste kohta erialase kirjanduse või vastavate turvet käsitlevate netilehekülgede abil.

7.7 Kaitse katastroofide ja looduskahjude eest

46. **Välja tuleks töötada avarii kontrollnimekirjad ja need igale töötajale laiali jagada.**

Juhtudel, kus arvuti streigib, printer enam ei prindi, kui tekib voolukatkestus, kui võrk satub viiruse küüsi või kui andmeid on kogemata ära kustutatud, peaks iga töötaja teadma, mida tal teha tuleb. Kõik vastutavad töötajad peaksid neile mõeldavad stsenaariumid läbi mängima ja koostama nimekirja vastutavatest töötajatest ja nende telefoninumbritest. Tüüpiliste stsenaariumite lühike kirjeldus oleks samuti kasulik. Näited: kuidas toimub andmete taastamine varundatud andmete (*backup*i) hulgast? Kuidas toimub printimisserveri taaskäivitamine?

47. **Kõiki olulisi andmeid tuleb regulaarselt varundada (*backup*).**

Andmevarunduseks (*backup*iks) saab kasutada hulgaliselt erinevaid tarkvara- j riistvaralahendusi. On tähtis, et sisseseatud *backup* kataks ka tõepoolest kogu olulise info. Jagatud heterogeensetes keskkondades kujuneb sellest aga suur väljakutse. Lahendusse tuleb kaasata ka mobiilsed lõppseadmed nagu sülearvutid, võrguühenduseta üksikarvutid ja pihuarvutid. Regulaarselt tuleks järele kontrollida, kas *backup* ka reaalselt toimib ja kas varundatud andmeid on võimalik taastada.

Backup-andmekandjad tuleb panna hoiule kuhugi turvalisse kohta, võimalikult väljaspool ettevõtte või ametiasutuse enda hoonet. Hoiukoht peaks olema piisavalt kaitstud igasuguste looduskahjude nagu nt tule, vee jms mõjude eest.

Kõik kasutajad peavad teadma, millistest andmetest kunas ja kuidas varukoopiaid tehakse. Reeglina tehakse varukoopiad ainult teatud valitud kaustadest ja failidest, vaid harva tehakse *backup* kogu olemasolevast materjalist.

48. IT-süsteeme tuleb sobival moel kaitsta tule, ülekuumenemise, veekahjustuste ja elektrikatkestuste eest.

IT-varades ei pruugi kahjusid tekitada mitte ainult IT-väärkasutus ja IT vastu suunatud tahtlikud ründed. Tihti tekivad märkimisväärsed kahjud ka tule, vee või elektri füüsikaliste mõjude tõttu. Paljusid seadmeid tohib käitada ainult teatud kindlates siseruumi kliimatingimustes. Seetõttu tuleks eriti tähtsad IT-komponendid (serverid, varukoopiate tegemise seadmed, marsruuterid jms) paigutada piisavalt kaitstud ruumidesse. Lisaks peaksid niisugused seadmed olema veel ühendatud ka katkematu toiteallikaga, millel on lisaks ka liigpinge kaitse. Kasulikke näpunäiteid saab antud valdkonna kohta nii Päästeameti nõuannete veebilehelt (www.rescue.ee) kui ka ISKE rakendusjuhendis toodud nõuannetest.

49. Rakendada tuleb sissepääsu turvamise ja murdvaraste vastaseid kaitsemeetmeid.

Ka väikesed ettevõtted ja ametiasutused peaksid mõtlema selle peale, kuidas kaitsta ennast murdvaraste ja muude kutsumata külaliste eest. Juba mõningad lihtsad meetmed võivad siinkohal kaasa tuua turvalisuse märgatava kasvu. Tuleks luua ülevaade, millistes kohtades viibivad külastajad ja võõrad isikud reeglina kõige rohkem ning millistele IT-süsteemidele on neil võimalik sel ajal ligi pääseda. Eriti oluline on, et serverid ja arvutid, millega pääsetakse ligi konfidentsiaalsetele andmetele, seataks üles selliselt, et võõrastel ei oleks võimalik neid märkamatult kasutama hakata. Külalisi tuleks saata kogu nende külastusaja vältel ja seda mitte ainult viisakusest. Sõltuvalt olukorrast võib olla mõttekas teatud büroouumid töötajate eemaloleku ajaks lukku panna ja aknad (nt lõunapausi ajaks) sulgeda, mitte irvakile jätta. Igasuguste meistrimeeste, hooldetehnikute ja puhastusteenindajate kutsumist tuleks teadlikult ette planeerida ja kõigile töötajatele teada anda. Sülearvuteid ei tohiks mitte kunagi jätta järelvalveta autosse või ööseks või pikema eemalviibimise korral niisama büroosse jätta. Siinkohal toodud soovituste loetelu pole kindlasti mitte täielik, st kõik konkreetsed juhtumid tuleb hoolikalt läbi mõelda ja neid vastavalt täiendada.

Soovitus:

küsige murdvaraste vastase kaitse juurutamisel nõu ekspertidelt või laske see politseil üle kontrollida, veendumaks, et Te ei tee murdvarastele nende tööd liiga lihtsaks.

50. Kõik olemasolev riistvara ja tarkvara tuleb kirja panna inventari loetelusse.

Inventarist on soovitav koostada nimekiri, mida tuleks ka regulaarselt värskendada. Paljudel juhtudel on selleks võimalik kasutada raamatupidamisest saadud andmeid. Kuid ka sellistel juhtudel jääb siiski tihti ebaselgeks, kus vastavad asjad viimati asusid, kas mõni kadunud ese on teatud ajaks juba pikka aega kadunud olnud või on see alles äsja kaotsi läinud. Inventari loetelu, milles kajastuks muuhulgas ka esemete hinnanguline väärtus, vajavad ka kindlustusfirmad, et kahju korral nõuetekohaselt toimida. Sellele lisaks saab inventari loetelu alusel regulaarselt kontrollida, et esemete väärtus ei oleks kindlustatud oma tegelikust väärtusest väiksema summa peale.

8. ISKE

Eelnevates peatükkides sai valgustatud ja selgitatud erinevaid IT-turbe aspekte, tuues välja põhjuseid, miks korraliku turbe tagamiseks ei piisa ainult tehniliste mehhanismide ja funktsioonide rakendamisest. Tehnilisi turbefunktsioone on tarvis ümbritseda organisatoorsete, personali- ja ehituslik-füüsikaliste meetmetega. Soov IT-turvalisust süstemaatiliselt ja laiaulatuslikult parandada seab Teie ette väljakutse, kuidas tuleks saavutada võimalikult optimaalne turbealane funktsionaalsus ja hoida seejuures kulutused kontrolli all. Lisaks peavad lahendused olema ka reaalselt kasutatavad ja piisavalt mugavad, et nendest puudutatud töötajad neid oma igapäevatöös ka aktsepteeriksid. Käesolev peatükk annab üldiseid juhised professionaalse IT-turvakontseptsiooni koostamiseks ja püüab selgitada, kuidas võiks RIA poolt arendatav ISKE rakendusjuhend Teile seejuures kasulik olla.

8.1 ISKE kasutamine professionaalse IT-turvakontseptsiooni väljatöötamise alusmaterjalina

Põhjalik, aga kallis: riskianalüüs

Üheks turvakontseptsiooni koostamise võimaluseks on viia läbi traditsiooniline riskianalüüs. Selle raames töötatakse olemasolevate IT-varade jaoks välja individuaalsed turvameetmed. Luuakse ülevaade kaitset vajavatest väärtustest (IT-süsteemidest, andmetest, oskusteabest jms) ning analüüsitakse täpselt läbi, millistele ohtudele on need avatud. Lõpetuseks analüüsitakse, kui suur on turvaintsidendi esinemise tõenäosus, milliste kahjudega tuleks sellisel juhul arvestada, milliseid turvameetmeid võiks rakendada selle kaitseks ning kui suur on loodava turvakontseptsiooni rakendamise tagajärjel alles jääv jääkrisk.

Riskianalüüsid annavad väärtuslikku infot, kuid individuaalse lähenemise tõttu nõuavad need väga palju tööd. Tarvis on eksperte, kes valdaksid vajalikku oskusteavet. Pealegi on olulised lähteandmed nagu turvaintsidendi esinemise tõenäosus või kahju suurus väga raskesti mõõdetavad, mistõttu jäävad need hinnangud väga umbkaudseteks. Neil põhjustel on riskianalüüside tegemine seotud suurte kuludega.

ISKE pakub efektiivset alternatiivi

Alternatiivse lahendusena riskianalüüsile saab turvakontseptsiooni koostamiseks kasutada ISKE rakendusjuhendit. ISKE rakendusjuhend koosneb ISKE rakendamise metoodika kirjeldusest ja kataloogidest, mis sisaldavad endas moodulite, ohtude ja turvameetmete katalooge. Etalonturve toetub tõsiasjale, et suurt osa IT-süsteemidest ja rakendustest rakendatakse kasutajate poolt sarnasel moel ja neid käitatakse võrreldavates kasutuskeskkondades. Näidetena võib siinkohal tuua Unixil töötavad serverid, Windowsi klient-PCd või andmebaasirakendused. Tüüpsete komponentide kasutamise tõttu tekivad IT-käitamises ikka ja jälle sarnased ohud. Kui spetsiaalseid turvanõudeid ei kasutata, pole vastavad ohud suures osas üldsegi seotud konkreetse kasutusvaldkonnaga. Sellest on tuletatud kaks metodoloogilist põhimõtet:

- ☐ laiaulatuslik riskianalüüs ei ole alati hädavajalik: IT-süsteemide käitamisel tekkivaid ohtusid ja ohtudest tekkivate kahjude tõenäosust on võimalik teatud eelduste täitmisel üldistavalt hinnata.
- ☐ Iga rakendusjuhtumi puhul ei ole täiesti uute turvameetmete väljatöötamine alati hädavajalik: standardsetest turvameetmetest on võimalik tuletada meetmepaketid, mis suudavad tavapäraste turbenõuete puhul tagada sobiva ja piisava kaitse võimalike ohtude vastu.

Nimetatud oletustele toetudes pakub ISKE rakendusjuhend välja oma IT-turvakontseptsioonide loomise ja kontrollimise metoodika. ISKE rakendusjuhendis on samm-sammult toodud erinevad etapid, mille alusel saab IT-turvahaldust praktikas üles ehitada ja käitada. ISKE käsitleb väga

põhjalikult seda, kuidas tuleks IT-turvakontseptsiooni praktikas koostada ning kuidas tuleks välja töötada ja rakendada asjakohased ISKE turvameetmed. Sellega käsitleb etalonturve ka väga üldsõnalisi nõudeid kehtestavaid ISO-standardeid nr 13335, 27001 ja 27002 ning annab kasutajatele palju juhiseid, taustateadmisi ja näiteid, kuidas seda kõike ellu rakendada. Etalonturbe üheks tähtsamaks eesmärgiks on vähendada IT-turbeprotsessi käigushoidmisele kuluvat tööd, pakkudes komplekssselt ja jätkusuutlikult infoturbe parandamiseks teadaolevat metoodikat. Seetõttu kajastavad ISKE kataloogid tüüpiliste IT-süsteemidega kaasnevaid standardseid ohtusid ja nende turvameetmeid, mida vajadusel ellu rakendada. Materjalidest leiate tüüpiliste IT-süsteemide jaoks mõeldud, praktikas läbiproovitud standardsed turvameetmed, mida tuleb mõistliku turbeastme saavutamiseks juurutada vastavalt kaasaegsetele tehnilistele nõuetele. Selle raames käsitletakse erinevaid valdkondi nagu infrastruktuur, organisatsioon, personal, tehnoloogia ja avariiplaanid, ja luuakse niimoodi terviklik lähenemine. Erilist tähelepanu pööratakse vajalike tehniliste teadmiste edasiandmisele. Seega saab etalonturbe katalooge kasutada muuhulgas ka võrdlus- ja infomaterjalina.

ISKE rakendamine toob kasutajatele eelise

ISKE abil on IT-turvakontseptsiooni ellurakendamine lihtne ning selleks ei kulu ülemäära palju tööd. Saavutatav turbeaste on piisav madala (L), keskmise (M) ja kõrge (H) kaitsevajaduste katmiseks. Kui tuleb kaitsta süsteeme, mida ISKE rakendusjuhendi kataloogides ei käsitleta, tuleb läbi viia täiendav turvaanalüüs. Kokkuvõtlikult võib välja tuua järgmised **IT-etalonturbest lähtumise eelised**:

- ☐ Standardseid turvameetmeid kirjeldatakse konkreetselt ja detailselt.
- ☐ Töö tulemusena valmivaid IT-turvakontseptsioone on võimalik täiendada ja värskendada ning need on kompaktsed, kuna viitavad olemasolevatele võrdlusallikatele.
- ☐ Soovitatavad turvameetmed on praktikas läbi proovitud ja välja valitud selliselt, et nende juurutamine toimuks võimalikult väikeste kuludega.
- ☐ Kuna IT-etalonturve kui tehniline juhend ja nõuandja käsitleb erinevaid turbealaseid küsimusi moodulite kaupa, saavad seda edukalt kasutada ka need, kes soovivad luua otsast peale tervet uut turvakontseptsiooni.

ISKE on riigi ja kohaliku omavalitsuse andmekogude töötlemisel seatud kohustuslikuks rakendamiseks määrusega nr 252 **Infosüsteemide turvameetmete süsteem**.

ISKE rakendustööriist, Teie professionaalne abimees

Lisaks kõikvõimalikele IT-etalonturvet käsitlevatele materjalidele võimaldab RIA kasutada ka spetsiaalset tööriista - ISKE rakendustööriista. Selle, ISKE rakendusjuhendil põhineva tööriista näol on kasutajatel võimalik saada abi turvameetmete valimisel ja rakendamisel. ISKE rakendustööriist võimaldab struktureeritult analüüsida kõiki kogutud andmeid. Tarkvara täisfunktsionaalne versioon erinevatele platvormidele on saadaval tasuta. Täiendavat infot ISKE rakendustööriista kohta leiate veebilehelt http://www.ria.ee/isketooriist

Allikad

ISKE rakendusjuhendit uuendatakse kord aastas. Lisaks on nii saksa kui ka inglise keeles tasuta kättesaadavad BSI IT-etalonturbe juhendid ja kataloogid.

ISKEga seotud küsimuste, arvamuste, ettepanekute korral pöörduda meili teel iske@ria.ee

Kogu ISKE-t puudutav informatsioon on toodud Internetis aadressil www.ria.ee/iske

8.2 ISKE kataloogide ülesehitus

Etalonturbe kataloogide moodulid jagunevad vastavalt teemakäsitlustele viide ossa:

1. **Üldised IT-turbeaspektid**
   Siia alla kuuluvad nt moodulid nagu personal, IT-turvahaldus ja andmevarunduse kontseptsioon.
2. **Ehituslikud ja tehnilised tingimused (infrastruktuur)**
   Sellesse ossa kuuluvad nt moodulid, mis käsitlevad hooneid, serveriruumi ja kodust töökohta.
3. **IT-süsteemid**
   IT-etalonturbe kataloogides on olemas asjakohased moodulid tüüpiliste IT-süsteemide kohta nagu nt Unix-süsteem, kaasaskantav PC, kodukeskjaam.
4. **IT-süsteemide erinevad võrguühenduste aspektid**
   Antud moodulites käsitletakse nt heterogeensete võrkude ühendamist ning võrgu- ja süsteemihaldust.
5. **IT-rakendused**
   Teatud rakenduste nagu e-maili, veebiserveri ja andmebaaside kohta on olemas spetsiaalsed moodulid.

Iga IT-etalonturbe kataloogides olev moodul sisaldab lühikest teemakirjeldust ja nimekirja viidetega antud valdkonnas olulistele ohtudele ning ka nende ärahoidmiseks mõeldud standardsetele turvameetmetele.

8.3 IT-etalonturbeanalüüsi läbiviimine

ISKE rakendusjuhend kirjeldab, kuidas luua erinevatele IT-lahendustele standardsete turvameetmete baasil IT-turvakontseptsioone ja kuidas neid kontrollida. Samuti antakse laialdast infot selle kohta, kuidas igapäevatöös turvameetmeid ellu rakendada ja tagada vajalik IT-turve. ISKE kataloogide standardsed turvameetmed loovad madala (L), keskmise (M) või kõrge (H) turbeastme turvalisuse. Vajadusel tuleb neile lisaks rakendada veel ka täiendavaid IT-turvameetmeid. Täiendavad turvameetmed võivad osutuda vajalikuks nt ka juhtudel, kus kasutatakse spetsiaalseid komponente, mida ISKE kataloogid ei kajasta, kuid mis on vaadeldavate IT-varade turbe jaoks väga olulised.

ISKE rakendamise sammudest loe täpsemalt ISKE rakendusjuhendi punktist 1.5.

9. Lisa

9.1 Kontrollnimekirjad

Käesoleva peatüki küsimused võtavad lühidalt kokku 50 IT-turvameetme sisu ja võimaldavad saada ülevaate oma ettevõtte või ametiasutuse võimalikest kitsaskohtadest.

IT-turvahaldus	
☐	Kas ettevõtte või ametiasutuse juhtkond on kehtestanud IT-turbega seotud eesmärgid ja saanud aru oma vastutusest IT-turbe tagamisel? Kas kõikide seadustest ja lepingutest tulenevate aspektidega on piisavalt arvestatud?
☐	Kas IT-turvajuhi (või IT-turvaeksperdi) ametikoht on olemas?
☐	Kas kõikide projektide puhul (nt uute võrkude planeerimisel, uute IT-süsteemide ja rakenduste ostmisel, väljasttellimise- ja teenuselepingute sõlmimisel) arvestatakse piisavalt varakult ka IT-turvanõuetega?
☐	Kas on olemas ülevaade olulisemate rakenduste ja IT-süsteemide ning nende kaitsevajaduste kohta?
☐	Kas on olemas tegutsemiskava, mis seab prioriteediks turvaeesmärgid ja reguleerib vastuvõetud IT-turvameetmete ellurakendamist?
☐	Kas kõikide IT-turvameetmete puhul on kindlaks määratud, kas neid tuleb rakendada ühekordselt või regulaarsete intervallide tagant (nt viirusetõrjetarkvara täiendite laadimine)?
☐	Kas kõikide IT-turbemeetmete puhul on kindlaks määratud töötajate pädevused ja vastutusalad?
☐	Kas vastutavate töötajate puhul on kindlaks määratud ka nende asendajad ning kas asendajad on nende tööülesannetega kursis? Kas olulisemad paroolid on avariijuhtudeks turvaliselt hoiule pandud?
☐	Kas olemasolevad ettekirjutused ja vastutusalad on kõikidele puudutatud isikutele teada?
☐	Kas on loodud kontrollnimekirjad, mida tuleb järgida uute töötajate töölevõtmisel või vanade töötajate lahkumisel (volitused, võtmed, juhendamine jne)?
☐	Kas IT-turvameetmete efektiivsust kontrollitakse regulaarselt?
☐	Kas on olemas dokumenteeritud IT-turvakontseptsioon?
IT-süsteemide turvalisus	
☐	Kas kasutatakse rakendustes ja programmides olemasolevaid kaitsemehhanisme?
☐	Kas viirustõrjetarkvara kasutatakse laialdaselt?
☐	Kas kõikidele süsteemikasutajatele on määratud oma rollid ja profiilid?
☐	Kas on kindlaks määratud, millistele andmetele tohivad erinevad kasutajad ligi pääseda? Kas on rakendatud mõistlikke piiranguid?
☐	Kas administraatorid on jaotatud erinevate rollide ja profiilide alla või tohib iga administraator teha kõike?
☐	Kas on teada ning kas on kehtestatud normid, millised privileegid ja õigused tohivad programmidel olla?
☐	Kas programmide ja IT-süsteemide standardsed turvaseadistused on kohandatud

	vastavalt vajadustele või kasutatakse neid jätkuvalt tootjafirma tarneseisundis?
☐	Kas turvalisust mõjutavad ebavajalikud programmid deinstalleeritakse ja nende funktsioonid lülitatakse järjekindlalt välja?
☐	Kas käsiraamatuid ja toote dokumentatsiooni loetakse piisavalt varakult?
☐	Kas installeerimistööde ja süsteemi üle peetakse põhjalikku dokumentatsiooni ning kas seda värskendatakse regulaarselt?

Võrgu- ja internetiühendused	
☐	Kas kasutatakse tulemüüri?
☐	Kas tulemüüri konfiguratsiooni ja toimimist kontrollitakse regulaarselt piisava põhjalikkusega?
☐	Kas on loodud kontseptsioon, millised andmed tehakse kättesaadavaks välistele kasutajatele?
☐	Kas on määratletud, kuidas käituda ohtlike lisaprogrammidega (*PlugIn*idega) ja aktiivsisuga?
☐	Kas kõik ebavajalikud teenused ja programmide funktsioonid on desaktiveeritud?
☐	Kas veebilehitsejad ja meiliprogramm on konfigureeritud turvaliselt?
☐	Kas töötajad on saanud piisava koolituse?

Turvanõuete järgimine	
☐	Kas tundliku informatsiooni ja andmekandjatega käiakse hoolikalt ümber?
☐	Kas enne andmekandjate ja IT-süsteemide hooldustööde või remonditööde tellimist kustutatakse nendest kõik tundlikud andmed?
☐	Kas töötajaid koolitatakse turbega seotud teemade osas regulaarselt?
☐	Kas töötajate turbealase teadlikkuse tõstmiseks on rakendatud mingisuguseid meetmeid?
☐	Kas kehtivate turvanõuete täitmist kontrollitakse ning kas turvanõuete rikkumisi karistatakse?

IT-süsteemide hooldamine: värskendustega ümberkäimine	
☐	Kas turvavärskendusi paigaldatakse regulaarselt?
☐	Kas ametisse on määratud vastutav isik, kes peab regulaarselt koguma täiendavat infot rakendatava tarkvara turvalisuse ja selle olulisemate turvavärskenduste kohta?
☐	Kas tarkvaramuudatuste kasutamise jaoks on olemas vastav testimiskontseptsioon?

Paroolid ja krüpteerimine	
☐	Kas kasutatavad programmid ja rakendused võimaldavad kasutada turvamehhanisme nagu paroole või krüpteerimist? Kas vastavad turvamehhanismid on sisse lülitatud?

☐	Kas algseadistusega paroolid või tühjad paroolid on ära muudetud?
☐	Kas kõik töötajad on läbinud koolituse, kuidas valida endale turvalisi paroole?
☐	Kas töökohalt lahkudes kaitstakse töökohaarvuteid ekraani pimenduspildi ja paroolkaitsega?
☐	Kas tundlikud andmed ja eriti ohustatud süsteemid nagu sülearvutid on krüpteerimise või muude kaitsemeetmete abil piisavalt hästi kaitstud?

Valmisolek hädaolukorraks	
☐	Kas on koostatud avariiplaan, mis sisaldab tegevusjuhiseid ja kontaktandmeid?
☐	Kas kõigi võimalike avariiolukordadega on arvestatud?
☐	Kas kõik töötajad tunnevad avariiplaani sisu ning kas avariiplaan on hästi kättesaadav?

Andmete varundamine	
☐	Kas andmevarunduse kohta on olemas strateegia?
☐	Kas on kindlaks määratud, kui kaua säilitatakse erinevat liiki andmeid?
☐	Kas andmete varundamisse on kaasatud ka sülearvutid ja ilma võrguühenduseta süsteemid?
☐	Kas andmevarunduslinte kontrollitakse regulaarselt?
☐	Kas andmete varundamise ja taastamise protseduurid on dokumenteeritud?

Infrastruktuuri turvalisus	
☐	Kas IT-süsteemid on piisavalt kaitstud tulekahju, ülekuumenemise, veekahjustuste, liigpinge ja elektrikatkestuste eest?
☐	Kas juurdepääs tähtsatele IT-süsteemidele ja ruumidele on reguleeritud? Kas külastajaid, remonditöölisi, hooldetehnikuid jne tuleb alati saata ning kas neid isikuid jälgitakse?
☐	Kas infrastruktuur on murdvaraste eest piisavalt kaitstud?
☐	Kõik olemasolev riistvara ja tarkvara on kantud inventari loetellu?

9.2 Näide: valdkonnad, mis peaksid olema reguleeritud kodukeskjaama turvakontseptsioonis

► Ametisse peaksid olema nimetatud kodukeskjaama eest vastutav töötaja ja tema asendaja.

► Süsteemis tuleks tuvastada ebavajalikud funktsioonid ja need sulgeda.

► Tehaseparoolid tuleks ära muuta.

► Konfigureerimis- ja hooldustöödeks vajalikud paroolid tuleks avariijuhtudeks turvaliselt deponeerida.

► Koostada tuleks ettekirjutused, mis kehtivad tasuliste numbrite ja välismaale helistamise kohta (nt tasulistele teenusenumbritele helistamise sulgemine).

► Regulaarselt tuleks analüüsida logifaile, et tuvastada võimalikud kõrvalekalded. Kõrvalekalleteks on nt volitamata sissevalimised hoolduseks reserveeritud ühenduste kaudu, ühenduse loomine pärast tööpäeva lõppu, korduvad helistamised PIN-koodide süstemaatiliseks läbiproovimiseks, ruumide jälgimissüsteemi sisselülitamine jms tegevus.

► Kodukeskjaama konfiguratsioonist tuleks regulaarselt luua varukoopia.

► Tootja käest tuleks muretseda või siis ise koostada tehniline dokumentatsioon ja lühike juhend igapäevase kasutamise kohta.

► Kodukeskjaam tuleb sisse töötada avariiolukordade käsiraamatusse (nt loetleda veatuvastuse võimalused, märkida ära hooldetehniku telefoninumber jne).

► Töötajatele tuleks selgitada võimalikke ohtusid (nt ruumi pealtkuulamise võimalust mobiiltelefoni abil, püsivõrguseadmete ja automaatvastajate võimaliku väärkasutust salajaste kõneluste pealtkuulamiseks).

► Võimalusel tuleks lasta välistel ekspertidel regulaarselt kontrollida kodukeskjaama turvalisust.

9.3 Täiendav informatsioon

Internetis on vabalt saadaval põhjatu hulk informatsiooni erinevate IT-turvet puudutavate küsimuste kohta ning selle hulka kuuluvad tihti ka väga head infoallikad.
Looge enda jaoks otsingumootorite abil teemast oma ülevaade!
Peagi näete, et ratast ei ole tarvis enam ise leiutama hakata, vaid et eksisteerib juba suur hulk dokumente, mis moodustavad hea aluse nende iseseisvaks kasutamiseks. Järgnevalt on toodud mõningad huvitavad aadressid.

Informatsioon ISKE kohta

www.ria.ee/iske neilt lehekülgedelt leiate kogu info ISKE kohta.

CERT (*Computer Emergency Response Teams*)

Infot arvutiviiruste ja teiste uute nii riist- kui ka tarkvaras ilmsiks tulnud turvaprobleemide kohta avaldatakse nn CERTide (*Computer Emergency Response Teams*) infolehekülgedel. CERTid vastavad IT-turbega seotud teemadele preventiivselt, hoiatavad turvaaukude eest ja levitavad infot turvalisust puudutavate sündmuste kohta. Nende informatsioonile toetudes on süsteemi eest vastutavatel töötajatel ja lõppkasutajatel võimalik astuda kiireid asjakohaseid samme potentsiaalsete ohtude ennetamiseks. Niimoodi on võimalik ennetada kahjude tekkimist.

Turvaintsidentide ilmsikstulekul pakuvad CERTid sõltuvalt oma eripärast ka tagantjärele rakendatavaid abiteenuseid, mis aitavad vähendada sündmuste negatiivseid tagajärgi, toetavad nende kõrvaldamist või aitavad teil olukorda vahetult mõista ja lahendada väärarusaamu.

www.cert.ee CERT-EE käsitleb Eesti arvutivõrkudes toimuvaid turvaintsidente, teostab ennetavaid tegevusi nende ärahoidmiseks ning tõstab kasutajate turvateadlikkust. Tuge osutatakse asutuste või interneti teenuse pakkuja süsteemiadministraatoritele, võrguadministraatoritele või klienditoele. Koostööd tehakse nii riigiasutuste kui erasektoriga. Lõppkasutajad peaksid turvaintsidentide korral pöörduma oma interneti teenuse pakkuja poole või siis oma organisatsiooni süsteemiadministraatorite poole, kes vajadusel teevad koostööd CERT Eestiga.

Info seisuga: juuli 2009