Juhised infoturbe halduse süsteemi loomiseks

Mai 2017

Euroopa Liit
Euroopa struktuuri- ja investeerimisfondid

Eesti
tuleviku heaks

Sisukord

Sissejuhatus **1**

1 Juhised infoturbe halduse süsteemi loomiseks **2**

1.1 JUHTKONNA VASTUTUS JA INFOTURBE ROLLID 2

1.2 RISKIANALÜÜSI LÄBIVIIMINE 2

1.3 INFOTURBE POLIITIKA KEHTESTAMINE 3

1.4 TURBEMEETMETE RAKENDAMINE 3

2 Infoturbe standardid ja raamistikud **5**

2.1 ISKE 5

2.2 CIS Critical Security Controls (CIS CSC) 5

2.3 NIST Framework for Improving Critical Infrastructure Cybersecurity 6

2.4 NIST Special Publication 800-53 7

2.5 COBIT 5 7

2.6 ISO/IEC 27001:2013 ja ISO/IEC 27002:2013 7

2.7 IASME Cyber Essentials Scheme 8

3 Näitlik turvameetmete kataloog ettevõtte elektroonilise turvalisuse tagamiseks **9**

Sissejuhatus

Tänapäeva maailmas on kõik ettevõtted ühel või teisel viisil ühendatud internetti ja on otseses sõltuvuses infosüsteemide käideldavuse, tervikluse ja konfidentsiaalsuse tagamisest. Küberturvalisuse olulisust tänapäeva maailmas on raske alahinnata. Seda toetavad faktid, et igapäevaselt satub rünnakute ohvriks tuhandeid infosüsteeme. Ohud ei ole ainult tehnilist laadi. Rünnete tehniline keerukus ja sotsiaalse manipuleerimise viimistletus suunatud rünnete kavandamisel on tekitanud olukorra, mille korral ei ole mõistlik panustada kogu infoturbe võimekust võrguperimeetri kaitsmisele, sest ründaja omab ründe planeerimisel alati tehnilist ja ajalist eelist. Järjest tähtsamal kohal on töötajate turvateadlikkuse tõstmine, kiire ja organiseeritud tegutsemine rünnete avastamisel ning taastevõimekuse parendamine.
Ründaja tegevus võib olla kannustatud poliitilistest motiividest, tööstusspionaažist või isiklikust motivatsioonist, kuid eelkõige organiseeritud küberkuritegevusest, eesmärgiga teenida rünnatava arvelt ebaseaduslikku tulu. Paraku kaasnevad ründe tagajärgedega tihti ründe alla sattunud ettevõtte IT süsteemide halvamisest tingitud teenusekatkestused, millest teatud juhtudel polegi võimalik täielikult taastuda. Elutähtsaid teenuseid osutavate ettevõtete puhul võib teenuse katkestus tähendada ohtu inimelule või riigikorralduse toimimisele. Ründe avalikuks tulemisega kaasneb mainekahju, mis võib sadades kordades ületada ründega tekitatud otsese majandusliku kahju. Täielikku turvalisust ei ole kunagi võimalik saavutada, ohud võivad realiseeruda kõige ebasoovitavamal hetkel.
Eestis sätestab elutähtsa teenuse osutajatele infosüsteemide turvalisuse tagamise kohustuse hädaolukorra seadus[1] ja määrus „Elutähtsa teenuse infosüsteemide ning nendega seotud infovarade turvameetmed“.

Elutähtsa teenuse infosüsteemide ning nendega seotud infovarade turvameetmed

§ 4. Turvameetmete rakendamine infoturbe halduse süsteemi alusel
(1) Elutähtsa teenuse osutaja loob oma põhitegevusi ja riske arvestades infoturbe halduse süsteemi, mida ta rakendab, seirab ja vajaduse korral täiustab.
(2) Elutähtsa teenuse osutaja järgib infoturbe halduse süsteemi rakendamisel soovitatavalt:
1) EVS-ISO/IEC 27001:2006 standardit;
2) Vabariigi Valitsuse 20. detsembri 2007. a määrusega nr 252 „Infosüsteemide turvameetmete süsteem” kehtestatud infosüsteemide kolmeastmelise etalonturbe süsteemi ISKE või
3) oma tegevusvaldkonnas kehtestatud infoturbe halduse erinõudeid ja head tava, mis tulenevad õigusaktist, välislepingust või muust lepingust ja on samaväärsed punktides 1 ja 2 nimetatud standarditega.
(3) Elutähtsa teenuse osutaja teeb infosüsteemi riskianalüüsi ja valib selle alusel infosüsteemi kaitseks vajalikud turvameetmed eesmärgiga tagada elutähtsat teenust korraldava asutuse kehtestatud teenuse toimepidevuse nõuete täitmine.

(4) Elutähtsa teenuse osutaja dokumenteerib turvameetmete rakendamise.

Turvameetmete rakendamiseks juurutab elutähtsa teenuse osutaja ettevõttes infoturbe halduse juhtimise süsteemi.

Infoturbe halduse juhtimise süsteem (ISMS- Information Security Management System) on tegevusriskikesksel metoodikal põhinev organisatsiooni üldise haldussüsteemi osa, mis tegeleb infoturbe rajamise, evitamise, rakendamise, seire, hoolduse ja täiustamisega; hõlmab organisatsiooni struktuuri, poliitikaid, plaanimistegevusi, kohustusi, tavasid, protseduure, protsesse ja ressursse [2]

[1] RT, Hädaolukorra seadus, vastu võetud 15.06.2009

[2] ISO/IEC 27000

1 Juhised infoturbe halduse süsteemi loomiseks

1.1 JUHTKONNA VASTUTUS JA INFOTURBE ROLLID

Infoturbe organisatsiooni suurus ja sellega tegelevate inimeste arv võib suurtes piirides varieeruda. Sellest tulenevalt võib väiksemates organisatsioonides üks inimene täita mitut erinevat rolli. Võimalikud rollid võiksid olla nt. järgmised:

- infoturbe juht
- infoturbe juhtrühm (infoturbekomitee)
- infoturbe spetsialist
- riskijuht
- IT juht
- IT haldusjuht
- IT administraator
- väline konsultant
- infovara omanik
- äriprotsessi omanik
- IT audiitor

Juhtkond peab selgelt määratlema, kes on infoturbe halduse toimimise eest, selle edendamise ja jooksva koordineerimistöö eest personaalselt vastutav. See võib olla infoturbe juht, kuid infoturbe juhi roll võib olla määratud ka mõni muu töötaja, nt IT juht. Sellist praktikat ei saa siiski heaks kiita, sest teatud juhtudel vähendab see ettevõtte kontrolli infoturbe meetmete rakendamise ja infoturbe toimimise üle.

Üldine vastutus ettevõttes infoturbe meetmete rakendamise eest on ettevõtte juhtkonnal. Juhtkond peab veenduma, et ettevõttes toimib efektiivne infoturbe halduse süsteem, mille rakendamisel infoturbe riske ning juurutatud kaitsemeetmeid perioodiliselt hinnatakse.

Juhtkond vastutab, et ettevõttes on piisavad vahendid infoturbega tegelemiseks, määratud vastutajad ja tagatud piisav aruandlus, mis võimaldab infoturbe olukorda ja tegevust hinnata ning analüüsida ja selle põhjal uuendusi kavandada. ISMS käivitamiseks on vajalik selge juhtkonna heakskiit.
Juhtkond peaks:

- teadma, millised on ettevõtte kriitilised äriprotsessid ja nende toimist toetavad infovarad;
- tuvastama võimalike ohtude realiseerimise tõenäosust ning kaaluma, milliseks võivad kujuneda intsidendi tagajärjed ja kogukulu;
- valima, milliseid riske aktsepteeritakse ja milliseid infoturbemeetmeid rakendatakse;
- koostama infoturbemeetmete rakendamise tegevuskava ja looma süsteemi tegevuste perioodiliseks ülevaatuseks.

Esmase hinnangu saamiseks infoturbe olukorrast ettevõttest soovitame juhtkonnal läbi viia esmase enesehindamise, kasutades selleks lisatud juhendit **Lisa 1 „Infoturbe küpsustaseme enesehindamise küsimustik ettevõtte juhtkonnale“.** Infoturbe hindamine on tegevus infoturbe hetketaseme väljaselgitamiseks. Hindamisel ilmnenud nõrkustega tuleb koheselt tegelema hakata. Alustada tuleb analüüsiga, et selgitada välja, milliseid ja kui olulisi riske need nõrkused ettevõttele võivad kaasa tuua.

1.2 RISKIANALÜÜSI LÄBIVIIMINE

Vastavalt hädaolukorra seadusele peab elutähtsa teenuse osutaja kaardistama ja analüüsima enda vastutusalas olevaid riske ja välja töötama võimalikud lahendused riskide vähendamiseks. Sama

põhimõte on kehtiv ka kõikidele muudele asutustele ja ettevõtetele. Infoturbe halduse süsteemi käivitamisel ja käigus hoidmise juures on perioodilisel riskide hindamisel oluline osa. Ettevõte peab hindama oma IT riske sarnaselt nagu hinnatakse muid ettevõtte riske, nt tegevus- ja finantsriske. Riskide tuvastamisel on oluline kõikide seotud osapoolte kaasamine. Enne riskide hindamist peab olema ettekujutus sellest, mis on ettevõtte jaoks olulised äriprotsessid ja millisel määral sõltuvad need IT-süsteemidest. Ettevõttele rakenduvad turvanõuded sõltuvad järgmistest asjaoludest:

- Millised tegevused on ettevõtte jaoks elutähtsad?
- Milline teave on ettevõtte jaoks elutähtis?
- Millised õiguslikud regulatsioonid ettevõttele kohalduvad?
- Millised kokkulepped ja lepingud käsitlevad infoturvet?
- Milliste ohtude vastu on vajalik ennast kaitsta?
- Mida peab tegema, et olla ettevõttena jätkusuutlik?

Riskianalüüsi peavad olema kaasatud äriüksuste juhid, infovarade omanikud, IT tugiisikud ja IT juhtkond. IT riskide metoodilisemaks kaardistamiseks ja detailsemaks analüüsiks tuleks kasutada mõnda spetsiaalselt IT riskide analüüsi ja hindamise metoodikat, nt ETO-dele mõeldud IT-riskianalüüsi juhend[3], mille tulemusena oskab ettevõtte veelgi paremini arvestada võimalike ohtude realiseerumise tõenäosuse ja võimalike intsidentide mõjuga.

1.3 INFOTURBE POLIITIKA KEHTESTAMINE

Ettevõtte peab kehtestama ja kõikidele töötajatele teatavaks tegema infoturbe poliitika. Infoturbe poliitika on kõrgema taseme dokument, mis defineerib kasutatavad mõisted, sätestab ettevõtte infoturbe strateegia ning infoturbe eesmärgid. Infoturbe poliitika peab sätestama infoturbe skoobi ja käsitlusala, seda nii käsitletavaid infosüsteeme kui ettevõtte füüsilisi asukohti silmas pidades. Infoturbe poliitika annab esmased suunised, kuidas neid eesmärke ellu viiakse. Infoturbe poliitika sätestab lisaks tegevusjuhenditele ka vastutused ja ametikohad, kes ettevõttes konkreetsete tegevuste eest vastutavad. Vastutuste osas peab olema infoturbe poliitikas selgelt välja toodud ka juhtkonna vastutus ning panus infoturbe halduse süsteemi toimimisse. Oluline on infoturbe poliitikas selgitada ka seda, mis juhtub siis, kui poliitikat või sellega seotud rakendusjuhiseid ettevõttes ei täideta. Infoturbe poliitika peab olema koostatud selliselt, et ta on kõigile mõistetav, asjakohane ja vajadusel kättesaadav.

1.4 TURBEMEETMETE RAKENDAMINE

Konkreetsed turvameetmed, mida ettevõte peaks kasutusele võtma, tulenevad eelnevalt määratletud turvanõuetest ja läbiviidud IT-riskide analüüsist.

Rakendamisele kuuluvate infoturbe meetmete valikul tuleb arvestada ettevõtte spetsiifikaga ja oluliste riskidega, mis selgitatakse välja meetmete valikule eelneva riskide hindamise käigus.

Aluseks, milliseid meetmeid oleks otstarbekas rakendada, võib võtta määruses soovitatud rahvusvahelise infoturvastandardi ISO/IEC 27001, etalonturbesüsteemi ISKE või muu samaväärse, soovitavalt valdkonnapõhise standardi või raamistiku (vt. ptk Infoturbe standardid ja raamistikud). Milliseid meetmeid rakendada, sõltub ettevõtte soovitavast infoturbe küpsustasemest. Osad allpooltoodud standarditest sisaldavad soovituslikke valikuid madala, keskmise ja kõrge turbevajaduse korral kasutamiseks (nt ISKE sisaldab L, M ja H-taseme nõudeid). Kõrgema taseme korral tuleb rakendada muuhulgas ka kõik madalamatele turvatasemetele ette nähtud meetmed. Ettevõte võib rakendatavate infoturbe meetmete kataloogi ettevõte koostada enda jaoks ise. Iga tuvastatud mittevastavuse puhul tuleks otsustada, kas sellega seotud riske aktsepteeritakse või tuleb meede rakendada. Meetmete rakendamiseks koostatakse riskikäsitluse tegevusplaan, kus märgitakse iga meetme kohta tema prioriteet, tegevuskava, rakendamise eest vastutav isik ja rakendamise tähtaeg. Oluline on, et tegevuskava on realistlik. Kui meetme rakendamine nõuab olulisel määral lisaressursse, tuleks enne selle rakendamist viia läbi tasuvushinnang.

[3] IT-riskianalüüsi koostamise juhend ETOdele, https://www.ria.ee/ee/kii-alusdokumendid.html

Infoturbe meetmete rakendamisel tuleb meeles pidada reeglit, mille kohaselt infoturbele kulutatud vahendite kogukulu peaks jääma alati väiksemaks kui võimalik kogukahju, mida meetmete rakendamisega püütakse vältida.

Kasud infoturbe halduse süsteemi sihipärasest rakendamisest:

- riskid on määratletud ja hallatud, organisatsioonis on võetud meetmed riskide vähendamiseks;
- ühtse metoodika kasutamisest tulenev läbipaistvus riskide juhtimisel ja infoturbe haldamisel üle kogu organisatsiooni;
- omanike, juhtkonna ja seotud osapoolte kindlustunne, et andmed ettevõttes on piisavalt hästi kaitstud;
- standardikohaste sisemiste protsesside juurutamisega on võimalik näidata välistele partneritele organisatsiooni tugevust ja küpsust.

2 Infoturbe standardid ja raamistikud

Tutvustame standardeid ja juhendmaterjale, mis käsitlevad kriitiliste teenuste pakkujate infoturbe halduse süsteemi (ingl *information security management system* – ISMS) väljatöötamist ja haldamist ning sisaldavad endas komplekti soovituslikke infoturbe meetmeid. Toodud standardid sobivad rakendamiseks eri valdkondade organisatsioonidele, samuti on need kasutatavad nii väikestes kui suurtes ettevõtetes. Neid juhendmaterjale on võimalik kombineerida omavahel ning muude infoturbestandardite, raamistike ja parimate meetodite (ingl *best practice*) juhenditega, ilma et tekiks nendevahelist vastuolu.

Elutähtsa teenuse osutajale sobivad abistavad materjalid infoturbe halduse süsteemi loomiseks ja käigushoidmiseks:

- RIA, Infosüsteemide kolmeastmeline etalonturbe süsteem ISKE, https://www.ria.ee/ee/iske-dokumendid.html
- The Center of Internet Security, The CIS Critical Security Controls for Effective Cyber Defence, Version 6.1, August 2016 (CCS CSC), https://www.cisecurity.org/controls/
- NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, National Institute of Standards and Technology, Veebruar 2014, https://www.nist.gov/cyberframework
- NIST Special Publication 800-53 rev4, Security and Privacy Controls for Federal Information Systems and Organizations, http://csrc.nist.gov/publications/
- ISO/IEC 27001:2013, ISO/IEC 27002:2013, https://www.iso.org/isoiec-27001-information-security.html
- ISACA, Framework for the governance and management of enterprise IT, COBIT 5, https://www.isaca.org/COBIT/Pages/Product-Family.aspx
- IASME Cyber Essentials Scheme, Requirements for basic technical protection from cyber attacks, Juuni 2014, https://www.iasme.co.uk/

2.1 ISKE

ISKE on Eesti avaliku sektori ettevõtetele ja riigiasutustele mõeldud kolmeastmeline etalonturbe süsteem, mis algselt võeti üle Saksamaa BSI poolt loodud analoogilisest infoturbe raamistikust. rakendamise eesmärk on tagada infosüsteemides töödeldavatele andmetele piisava tasemega turvalisus. Süsteem on loodud eelkõige riigi ja kohaliku omavalitsuse andmekogude pidamisel kasutatavatele infosüsteemidele ning nendega seotud infovaradele turvalisuse tagamiseks, kuid ISKE on kasutatav IT turvalisuse tagamise juhendmaterjalina ka muudes ettevõtetes. ISKE arendamisega tegeleb Riigi Infosüsteemi Amet, hetkel on jõutud juhendi 8-nda versioonini. ISKEga seotud materjalid on kättesaadavad veebiaadressilt https://www.ria.ee/ee/iske-dokumendid.html .
ISKEs on kirjeldatud kolm turbe taset – madal (L), keskmine (M) ja kõrge (H). Vastav turbetase määratakse andmetele turvaklasside (turvaosaklasside) määramise kaudu. Turvaklasside määramisel lähtutakse teabe konfidentsiaalsusest, teabe terviklikkusest, aegkriitilise teabe käideldavusest, teabe hilinemise tagajärgede lubatavast kaalukusest.

2.2 CIS Critical Security Controls (CIS CSC)

CIS (Centre of Internet Security) on Ameerika Ühendriikides 2008 aastal NSA poolt alustatud projekt, mis nüüdseks on välja kasvanud iseseisvaks, mittetulunduslikuks organisatsiooniks, mille missiooniks

on luua ja levitada küberturbe parimaid praktikaid ning seeläbi edendada turvalist internetikasutust. CIS CSC kontrollide koostamisel juhindutakse sellest, milliseid meetodeid ja turvanõrkuseid on kasutavad rünnete läbiviimiseks ründajad. Efektiivne kaitse tugineb peamiste nõrkuste kõrvaldamisele, mille tulemusena hoitakse ära suur osa (CIS andmetel 85% [4])levinumatest küberrünnetest. CIS infoturbe kontrollide näol on tegemist kogumikuga esmatähtsatest, kiiret tasuvust ja efektiivset kaitset pakkuvatest turvameetmetest. Suhteliselt lühikese turvameetmete nimekirja koostamisel on osalenud lai ring avaliku ja erasektori küberturbe spetsialiste. Kokku kahekümnesse kategooriasse kogutud meetmete kirjeldamisel on silmas peetud, et ettevõtte potentsiaalne kasu küberturbe investeeringutest oleks võimalikult suur**. CIS CSC läbivaks teemaks on kontroll olemasoleva riistvara, tarkvara ja võrguseadmete üle ning nende seadistamine turvaliseks kasutamiseks.** CIS CSC ei asenda tuntud turvastandardeid seadusandlusest tulenevate nõuete täitmisel, vaid annab praktilisi soovitusi, kuidas lahendada turvanõetest tulenevaid keerukaid ülesandeid. CIS küberturbesoovituste uuendamise ja ajakohastamise eest hoolitseb vabatahtlikkuse põhimõtte alusel toimiv rahvusvaheline küberturbe ekspertide kogukond.

2.3 NIST Framework for Improving Critical Infrastructure Cybersecurity

Ameerika Ühendriikide presidendi algatusest aluse saanud ja 2014 aastal riikliku institutsiooni *National Institute of Standards and Technology* (NIST) poolt loodud küberturbe raamistik (NIST CSF) loodi eesmärgiga aidata ettevõtteid tõhusate ja kuluefektiivsete infoturbemeetmete valimisel. Raamistik on arendatud olema sõltumatu kasutavatest tehnilistest lahendustest ning selle rakendamine on vabatahtlik. Raamistik peaks täiendama, mitte asendama, juba ettevõttes kasutusel olevaid infoturbe halduse süsteeme. NIST CSF loomisel on silmas peetud tegevusala parimate praktikate, standardite ja raamistike (nt. ISO 27001 ja COBIT 5) nõudeid, esitades need lihtsalt hoomatava loogika kohaselt funktsioonide kaupa *(Identify, Protect, Detect, Respond, Recover*) sektsioonidesse, mille sees omakorda kasutatakse teemakohaseid alamkategooriaid. Näiteks *Protect* domeen sisaldab juurdepääsuõigustega seotud kontrolle (PR.AC), töötajate turvateadlikkuse tõstmise ja koolitusega seotud meetmeid (PR.AT), andmekaitset(PR.DS), infoturbe protsesse ja protseduure (PR.IP), hooldusprotsesse (PR.MA) ning infoturbe tehnoloogiat (PR.PT) käsitlevaid nõudeid**. NIST CSF ei ole loodud kasutamiseks etalonturbesüsteemina, toodud turvameetmete rakendamine tervikuna ei pruugi kõikide ettevõtete jaoks sobida**. Kuigi raamistiku nimi viitab kriitilise infrastruktuuri ettevõtete küberturvalisuse raamistikule, on tegemist erinevate tegevusalade ja suurusega ettevõtete jaoks sobiliku informatiivse materjaliga. NIST CSF sobib kasutamiseks ühtviisi hästi nii avaliku sektori kui erasektori ettevõtetele. **NIST CSF on protsessipõhine meetmekataloog, mille juurutamisel tuleb kasutada riskipõhist lähenemist.** Meetmete valikul tuleb lähtuda ettevõtte eesmärkidest, protsessidest ja potentsiaalsetest ohtudest. NIST CSF kasutab küpsustaseme mudelile sarnanevat süsteemi. Juurutamiseks tuvastatakse infoturbe riskiprofiil antud hetkel, see järel analüüsitakse, milline on soovitav profiil, leitakse hetkeseisu ja soovitava taseme erinevused ning kavandatakse sammud ettevõtte küpsustaseme tõstmiseks. NIST soovitab selleks järgmist seitsmeastmelist tegevuskava:

1. Määra skoop ja prioriteedid.
2. Tee selgeks nõuded, seosed erinevate infovarade vahel ja riskitaluvus.
3. Loo hetkeseisu kajastav küberturbeprofiil.
4. Vii läbi riskide hindamine.
5. Määra soovitav küberturbe profiil.
6. Tee kindlaks, analüüsi ja prioritiseeri erinevused profiilide vahel.
7. Loo tegevuskava.

Eelpool toodud tegevusi tuleb perioodiliselt korrata, tagades niimoodi ettevõtte tasandil pideva infoturbe parendamise protsessi toimimise. Ka raamistik ise on mõeldud „elava dokumendina“, mida aja jooksul pidevalt täiendatakse ja muudetakse. Hetkel on raamistikust tehtud kättesaadavaks ka mustandversioon 1.1 (https://www.nist.gov/cyberframework/draft-version-11) .

[4] CIS Controls, https://learn.cisecurity.org/20-controls-download

2.4 NIST Special Publication 800-53

NIST 800-53 on NIST poolt Ameerika Ühendriikide riiklike infosüsteemide ning kriitilise infrastruktuuri ettevõtete kaitseks koostatud ühtne ja detailne infoturbe meetmete kataloog. NIST 800-53 arendamist koordineerib *Joint Task Force Transformation Initiative* töögrupp, kuhu kuuluvad esindajad kõigist olulistest riigistruktuuridest. See on osa laiapõhisest raamistikust, mis hõlmab täielikku infoturbe haldussüsteemi elutsüklit, alustades infoturbe halduse planeerimisest ja riskide kaardistamisest kuni detailsete meetmete valimiseni ja rakendamiseni. NIST SP 800-53 on üks juhend avaliku sektori IT-süsteemide kaitset reguleerivatest juhendmaterjalide süsteemist, mille rakendamiseks tuleb paralleelselt kasutada ka teisi NISTi, FISMA ja FIPS poolt publitseeritud juhendeid. NIST annab ka juhiseid juhendi rakendamiseks erinevates majandusvaldkondades (Smart Grid, ICS, tervishoid). NIST arvestab Ameerika Ühendriikide seadusandlusest tulenevate nõuetega, seetõttu pole NIST SP 800-53 täielik rakendamine väljaspool Ameerika Ühendriikide õigusruumi otstarbekas. Lisaks nõuete püstitamisele annab NIST SP 800-53 juhiseid ka infoturbe vastavuse hindamiseks.

2.5 COBIT 5

COBIT 5 on ISACA (varemalt tuntud kui *Information Systems Audit and Control Association, https://www.isaca.org*) poolt loodud ja aastatepikkuse arendustöö käigus oluliselt täiendatud ettevõtte IT halduse ja juhtimise (sh infoturbe halduse) parimate praktikate kogum. COBIT 5 on võimalik juurutada osade kaupa, alustades mõnede detailsete juhendite kasutamisest. Teisest küljest on COBIT 5 näol tegemist tervikliku lähenemisega terve ettevõtte IT korraldamisele, sisaldades kõiki selle aspekte alustades võimalikest mõjuteguritest, nagu ettevõtte eetika ja kultuur, kuni üksikute IT protsessideni välja. COBIT 5 eristab selgelt kahte tüüpi juhtimistegevusi:

- Valitsemine (ingl *governance*) – tegevused, mille eesmärk on omanike vajaduste elluviimine, tehes seda läbi ettevõtte eesmärkide ja detailsemaks minnes läbi IT eesmärkide seadmise.
- Juhtimine (ingl *management*) – planeerimise, evitamise, opereerimise ja seirega seotud tegevused, mille läbi tagatakse ettevõtte valitsemisega kehtestatud eesmärkide saavutamine

Infoturbe aspektist on oluline tähelepanu pöörata COBIT 5 protsessimudelile (COBIT 5 Process Reference Model), mis sisaldab 37 üldist IT protsessi, mida käsitletakse detailsemalt COBIT 5 juhendis „COBIT 5: Enabling Processes“. COBIT 5 protsessimudel kirjeldab IT protsesse ulatuses, nagu nad võiksid olla juurutatud standardses ettevõttes. Iga protsessi kohta lisatakse detailne kirjeldus, kvaliteedikriteeriumid, võimalikud sisendid ja väljundid ning seosed teiste protsessidega. Läbi protsessiga seotud IT eesmärkide seotakse iga protsess ühtlasi ettevõtte kui terviku eesmärkide saavutamisega. **COBIT 5 pöörab tähelepanu protsesside pideva täiustamise vajadusele**. ISACA annab suuniseid, juhendeid ja tööriistu COBITis kirjeldadud protsesside efektiivseks rakendamiseks, kuid maksimaalse kasu nendest saadakse ainult siis, kui protsessid on vastavuses organisatsiooni vajaduste ja keskkonnaga. Iga protsessi juurutamisel tuleb arvestada spetsiifiliste mõjuteguritega organisatsiooni küpsustasemega ning peamiste valupunktide ja arenguvõimalustega. Infoturvet käsitleb detailsemalt COBIT 5 koosseisus olev juhend „COBIT 5 for Information Security“. COBIT 5 raamistikku kuuluvad ka juhendid IT, sealhulgas infoturbe auditite läbiviimiseks.

2.6 ISO/IEC 27001:2013 ja ISO/IEC 27002:2013

Rahvusvahelise infoturbe halduse standardi ISO/IEC 27001:2013 „ Infotehnoloogia. Turbemeetodid. Infoturbe halduse süsteemid” kohaselt peab tippjuhtkond olema infoturbe alal eestvedaja ja kohustub sellega, et ta:

- tagab infoturvapoliitika ja infoturbe eesmärkide kehtestamise ning nende kooskõla organisatsiooni strateegia suunaga;
- tagab infoturbe halduse süsteemi nõuete lõimimise organisatsiooni protsessidesse;
- tagab infoturbe halduse süsteemile vajalikud ressursid;
- teeb teatavaks infoturbe toimiva halduse tähtsuse ning infoturbe halduse süsteemi nõuete järgimise tähtsuse;

- tagab, et infoturbe halduse süsteem saavutab sellele kavandatud tulemused;
- suunab inimesi andma panust infoturbe halduse süsteemi toimivusse ja toetab neid selles;
- edendab pidevat täiustamist;
- aitab teistel asjakohastel juhirollidel ilmutada samasugust eestvedu oma vastutusalal.

Standard „ISO 27002:2014. Infotehnoloogia. Turbemeetodid. Infoturbemeetodite tavakoodeks" kirjeldab infoturvameetmed ja nende rakendusjuhised järgnevates kategooriates:

- Infoturvapoliitikad
- Infoturbe korraldus
- Inimressursiturve
- Varade haldus
- Pääsu reguleerimine
- Krüptograafia
- Füüsiline ja keskkonna turve
- Käituse turve
- Side turve
- Süsteemide hankimine, väljatöötamine hooldus
- Tarnijasuhted
- Infoturvaintsidentide haldus
- Jätkusuutlikkuse halduse infoturbeaspektid
- Vastavus

2.7 IASME Cyber Essentials Scheme

Cyber Essentials on Ühendkuningriikides (UK) loodud, vabatahtlikuks kasutamiseks mõeldud infoturbe parim praktika, mis koondab endas peamisi kaitsemeetmeid kõige levinumate küberrünnete ärahoidmiseks. Igaüks võib Cyber Essentials dokumentatsiooni alla laadida (https://www.cyberaware.gov.uk/cyberessentials/docs.html) ja seda oma ettevõttes kasutada. Alates 2014 aastast peavad kõik UK isikuandmete töötlusega seotud ja teatud IKT teenuseid pakkuvad ettevõtted, mille partneriteks on riigiasutused, olema Cyber Essentials skeemi kohaselt auditeeritud ja sertifitseeritud. IASME Cyber Essentials nõuab, et esimeses järjekorras tuleb rakendada järgmised infoturbe kontrollid:

1. Välise perimeetri kaitsmine tulemüüriga
2. Seadmete turvaline konfigureerimine
3. Kasutajate juurdepääsuhaldus
4. Pahavaratõrje
5. Riist- ja tarkvara uuenduste paigaldamine

3 Näitlik turvameetmete kataloog ettevõtte elektroonilise turvalisuse tagamiseks

Antud juhend annab tegevuskava, kuidas läbi praktiliste sammude teha kindlaks infoturbe olukord ning aidata juhtidel teadlikult ja süstemaatiliselt keskenduda kõige olulisemate võrguturbe meetmete rakendamisele. Elektroonilise turvalisuse tagamine on oluline iga ettevõttesisesesse või avalikku arvutivõrku ühendatud seadme puhul. Erinevate hinnangute kohaselt on võimalik teadaolevate küberrünnete riski vähendada kuni 80%, kui rakendada inimeste, protsesside ja tehnoloogia kaitseks elementaarseid küberturvalisuse tagamise meetmeid. Lisatud meetmete kataloogis on esmataseme meetmed tähistatud küpsustasemega 1 (vt **lisa 2 „Küpsustasemete määramine“**). Soovitame nendele meetmetele tähelepanu pöörata koheselt, esimese sammuna enne EVS-ISO/IEC 27001, infosüsteemide kolmeastmelise etalonturbe süsteemi ISKE või mõne muu allpoolkirjeldatud raamistiku või infoturbestandardi täielikku rakendamist.
Näitlik turvameetmete kataloog (esitatud täielikul kujul **lisas 3 „Näitlik turvameetmete kataloog“**) koostamisel on lähtudud ülalpooltoodud infoturbe standarditest ja raamistikest. Meetmed on jaotatud neljaks loogiliseks meetmeteplokiks:

- **Planeerimine** - sisaldab meetmeid infoturbe käsitlusala määramiseks ja infoturbe halduse süsteemi loomiseks ning käigushoidmiseks
- **Kaitsmine** – sisaldab meetmeid mittesoovitavate infuturvaintsidentide ärahoidmiseks ja võimalikele ründajatele raskesti ligipääsetavaks muutmiseks. Kaitsemeetmed vähendavad andmelekete ja infoturva intsidentide tõenäosust
- **Avastamine** – sisaldab meetmeid intsidentide kiireks avastamiseks. Avastamismeetmed vähendavad ajavahemikku, mille jooksul ründaja saab segamatult tegutseda ja läbi selle minimiseerida tekitatud kahju.
- **Taastamine** – sisaldab meetmeid juhtumite menetlemiseks ja normaalse töökeskkonna taastamiseks pärast toimunud intsidente. Taastemeetmed vähendavad infoturvaintsidentide poolt tekitatud kahjusid.

Ajalooliselt on infoturbe fookus suunatud kaitsemeetmete, nt. võrguperimeetri, tugevdamisele ja kindlustamisele. Järjest enam pannakse rõhku nn. „mitmekihilise infoturbe“ juurutamisele , mille juures tuleb võrdselt tuleb panustada nii organisatsiooniliste kui erinevatele tehnoloogiliste infoturvameetmete rakendamisele. Kuna võrgu kaitsmisele suunatud meetmed ei suuda tagada efektiivset kaitset kõikide ründetüüpide vastu (nt sotsiaalne manipuleerimine – ingl *social engineering*), tuleb senisest enam panustada kiirele rünnete avastamisele, intsidendi lokaliseerimisele ja juhtumijärgsele normaalse töökeskkonna taastamisele koos kõigi olemasolevate andmetega.

PLANEERIMINE (PLAN)
Organisatsioon ja ärikeskkond
Infoturbe halduse süsteemi kehtestamine
Infoturvariskide analüüs
Infoturvariskide käsitlemine
Riistvara inventuur
Tarkvara inventuur
Turvateadlikkuse tõstmine
IT teenuste väljast tellimine
KAITSMINE (PROTECT)
Riist-ja tarkvara turvaline seadistamine

Pahavara tõkestamine
E-posti ja veebikasutuse turvamine
Võrguteenuste, -protokollide ja portide piiramine
Võrguseadmete turvaline seadistamine
Välisperimeetri kaitsmine
Traadita võrk (WiFi)
Rakenduste turve
Andmete kaitse
Teadmisvajadusel põhinev juurdepääs
Kasutajakontode haldus
Administraatoriõigustega kasutajad
AVASTAMINE (DETECT)
Turvanõrkuste avastamine ja analüüs
Logide seire ja analüüs
TAASTAMINE (SUSTAIN)
Infoturvaintsidentide haldus
Taastevõimekuse tagamine
Ründe- ja taastetestimised

Juhend sisaldab soovituslikku nimekirja infoturbe kontrollidest, mille rakendamine aitab tunduvalt vähendada riske sattuda rünnaku objektiks ning minimiseerida küberrünnete tagajärgedest tulenevat kahju. Infoturbe meetmete detailse nimekirja koostamisel on kasutatud eelpool nimetatud globaalselt tunnustatud ja riiklikke infoturbe standardeid, raamistikke, enesehindamise küsimustikke ja ettevõtete kogemusi. Toodud meetmete kataloog keskendub küberturvalisusele (st. arvutivõrk ja sellega ühendatud seadmed, ja arvutivõrgus kasutatav tarkvara). Võrguturvalisuse parendamine on oluline, sest enamik ründeid kas algatatakse Internetist või on aktiivne võrguühendus vajalik ründe käigushoidmiseks. Ka andmete varguse eelistatud viis on nende saatmine ettevõttest välja läbi avaliku võrguühenduse. Vähem tähelepanu on toodud meetmete näidiskataloogis pööratud füüsilise keskkonna (hooned ja seonduv infrastruktuur) turvalisuse parendamise meetmetele, mille rakendamine kahtlemata on ettevõttele samuti eluliselt tähtis.
Meetmete kataloogi on võimalik kasutada infoturbejuhi tööriista loomiseks (vt **Lisa 4 „Visioon interaktiivse infoturbe halduse tööriista tellimiseks“**), sidudes meetmetega:

- võimalikud riskid, mida konkreetne meede vähendab;
- vastutaja, kes meetme rakendamise eest vastutab;
- tegevuskava, mida tuleb meetme rakendamiseks teha;
- tähtajad, millal meede peab olema rakendatud või millal see uuesti üle vaadatakse;
- perioodilised tegevused, mis antud meetmega on seotud.

Kontakt

Teet Raidma
IT nõustamisteenuste juht
+372 6 676 814
traidma@kpmg.com

KPMG Baltics OÜ
Narva mnt 5
10117 Tallinn
Estonia

Tel +372 6 268 700
Fax +372 6 268 777

www.kpmg.com