Lisa 1 - Infoturbe küpsustaseme enesehindamise küsimustik ettevõtte juhtkonnale

SISSEJUHATUS

Vastavalt 14.03.2013 jõustunud määrusele „Elutähtsa teenuse infosüsteemide ning nendega seotud infovarade turvameetmed“ peab elutähtsa teenuse osutaja (ETO), juhul kui ETO elukriitilise tegevuse sõltuvus infosüsteemist on oluline, looma oma põhitegevusi ja riske arvestades infoturbe halduse süsteemi, mida ta rakendab, seirab ja vajaduse korral täiustab. Turvameetmete rakendamiseks soovitab määrus aluseks võtta rahvusvaheliselt tuntud infoturbe standardi ISO/IEC 27001, Eesti avaliku sektori jaoks kohandatud etalonturbesüsteemi ISKE või nendega samaväärseid tegevusvaldkonna infoturbenõuded. Infosüsteemi kaitseks vajalike turvameetmete valimiseks teeb ETO eelnevalt infosüsteemi riskianalüüsi.

2016 aastal RIA poolt tellitud uuringu[1] kohaselt elutähtsa teenuse osutajad kas rakendavad ülaltoodud standardeid vähesel määral või ei rakenda neid üldse. Peamiste takistusena näevad ETOd järgmisi probleeme:

- infoturbe halduse süsteemi süstemaatiline rakendamine ei ole majanduslikult otstarbekas;
- infoturbe riskide analüüsi ja hindamine on keeruline;
- infoturbe standardid on mõeldud suurematele ettevõtetele;
- standardis toodud meetmete rakendamine on väga kallis ja ajamahukas;
- ei oska hinnata, millised standardi meetmed on ettevõttele olulised ja millised mitte;
- puuduvad vajalike äriliste, IT ja infoturbe teadmistega töötajad.

Arvestades pidevalt suurenevaid küberriske[2], on oluline tagada ETOde võimekus vähemalt kõige kriitilisemates infoturbe valdkondades, sh võrguturbe meetmete rakendamises. Infoturbe halduse olukorra välja selgitamiseks ettevõtetes pakume välja järgmise, infoturbe kriitilisi aspekte käsitleva ning infoturbe elutsüklil põhineva küsimustiku. Küsimustikul on järgmised eesmärgid:

- saada ülevaatlik hinnang infoturbe olukorrast ettevõttes;
- hinnata ettevõtte infoturbe küpsustaset infoturbe elutsükli lõikes (planeerimine, kaitsmine, avastamine, taastamine);
- analüüsides erinevate ettevõtete tulemusi, on võimalik leida süstemaatilisi puudusi ning planeerida juhendeid ja koolitusi konkreetsete riskide vähendamiseks
- Juhtida tähelepanu ettevõtte infoturbe nõrkadele külgedele ning pakkuda lahendusi olukorra parendamiseks.

Infoturbe tegevuskava koostamiseks soovitame pärast enesehinnangu andmist kasutada detailset kriitiliste infoturbe meetmete nimekirja, millel antud küsimustik põhineb.

---

[1] Elutähtsate teenuste osutamist mõjutavate tegurite kaardistamise uuring, https://www.ria.ee/public/Kuberturvalisus/Elutahtsate-teenuste-osutamist-mojutavate-tegurite-uuringu-kokkuvote.pdf

[2] Riigi Infosüsteemi Ameti küberturvalisuse teenistuse 2016. aasta kokkuvõte, https://www.ria.ee/public/Kuberturvalisus/RIA-kuberturbe-aastaraport-2016.pdf

INFOTURBE KÜPSUSTASEME ENESEHINDAMISE KÜSIMUSTIK

Küsimustik on koostatud juhtkonna enesehindamise küsimustikuna. Küsimustik on jaotatud infoturbe valdkondade kaupa kolmeks küsimuste blokiks, igaühes 10 küsimust. Küsimustele vastamisel eeldame, et juhtkond vastab küsimustikublokis **A** esitatud küsimustele iseseisvalt, kuid küsimustikublokkide **B** ja **C** puhul võib vajadusel hankida vastuseid ettevõttes turvameetmete rakendamise eest vastutavalt isikult.

Igale küsimusele tuleb valida sobivaim vastus järgnevatest variantidest:

JAH	OSALISELT	EI	EI OSKA HINNATA
1	0,5	0	0

Vastates igale küsimusele ja summeerides punktid (maksimaalselt 10 igas valdkonnas), saab ettevõtte juhtkond anda esmase ning üldise hinnangu ettevõtte infoturbe olukorrale asutuses. Võrreldes sarnastest ettevõtetest saadud enesehindamise tulemusi, on võimalik leida ettevõttes infoturbe valdkonnad, millega tegelemine nõuab senisest enam tähelepanu.

A. PLANEERIMINE

1. Kas infoturbe halduseks on kehtestatud ettevõttes konkreetsed vastutused ja määratud töökohustused?
2. Kas omate ülevaadet seadusest tulenevatest ja lepingulistel kohustustel põhinevatest nõuetest infoturbe korraldamisele ja infoturvameetmete rakendamisele?
3. Kas on kehtestatud infoturbe eesmärgid ja indikaatorid infoturbe hindamiseks?
4. Kas ettevõte on koostanud ja kinnitanud infoturvapoliitika ja sellest lähtuvad protseduurijuhendid?
5. Kas ettevõte omab ülevaadet ettevõttes kasutatavast tarkvarast ja riistvarast?
6. Kas te teate, mis on ettevõtte kõige väärtuslikumad andmeid?
7. Kas ettevõtte töötajatele korraldatakse perioodiliselt infoturbe koolitusi?
8. Kas olete kaardistanud infoturbe ohud, nõrkused ja infoturbega seotud riskid?
9. Kas olete koostanud tegevuskava infoturbe riskidega tegelemiseks?
10. Kas ettevõte on määratlenud infoturbe nõuded IT teenuste väljast tellimiseks?

B. KAITSMINE

1. Kas teate, millised infosüsteemid ja andmed on ettevõtte põhitegevuse jaoks kriitilise tähtsusega?
2. Kas ettevõte seadmete ja tarkvara soetamine ja seadistamine toimub tsentraalselt ja standardiseeritult?
3. Kas ettevõte kasutab keskselt hallatavaid pahavara tõkestamise ja viirustõrje lahendusi?
4. Kas on kehtestatud reeglid nutiseadmete kasutamiseks ning tööks andmetega väljaspool ettevõtet?
5. Kas on kehtestatud kasutusreeglid ja kasutatakse tehnilisi piiranguid turvaliseks e-posti ja interneti kasutamiseks?

6. Kas on kehtestanud infoturbe nõuded infosüsteemide arendamisele ja hankimisele?
7. Kas ettevõte paigaldab regulaarselt tarkvarauuendusi?
8. Kas ettevõtte on rakendanud turvameetmed tundlikele andmetele juurdepääsu tõkestamiseks?
9. Kas ettevõttes viiakse läbi perioodiliselt infosüsteemi kasutajakontode ja kasutusõiguste kontrolle, tuvastamaks liigselt antud või mittevajalikke kasutusõigusi?
10. Kas te hindate enne tundlikele andmetele juurdepääsu lubamist selle tegelikku vajadust, töötajate tausta, vajalikke teadmisi ja oskusi?

C. AVASTAMINE JA TAASTAMINE

1. Kas arvutivõrgus toimuvate kahtlust äratavate tegevuste avastamiseks kasutatakse automaatseid seirelahendusi?
2. Kas ettevõttes viiakse läbi turvanõrkuste avastamise ja arvutivõrgu ründetestimisi?
3. Kas võrguperimeetri seadmed logivad ja talletavad informatsiooni toimunud sündmuste kohta?
4. Kas ettevõte teostab volitamata juurdepääsude ja andmelekete avastamiseks jooksvalt infosüsteemi logianalüüsi?
5. Kas on loodud protseduurireeglid infoturvaintsidentide raporteerimiseks ja lahendamiseks?
6. Kas on määratud konkreetne vastutus ja meeskond kriisiolukordade lahendamiseks?
7. Kas ettevõttel on infoturbe tagamiseks piisavalt tehnilisi vahendeid ja vajalike teadmiste ja oskustega töötajaid?
8. Kas ettevõte on koostanud taasteplaanid oluliste infosüsteemide normaalse tegevuse taastamiseks pärast toimunud intsidenti?
9. Kas vähemalt üks varukoopia andmetest asub serveritest füüsiliselt eemal asuvas, pideva võrguühenduseta asukohas?
10. Kas ettevõtte viib perioodiliselt läbi andmete varunduse ja taastamise testimisi?