| | |
|---|---|
| Väljaandja: | Ettevõtlus- ja infotehnoloogiaminister |
| Akti liik: | määrus |
| Teksti liik: | algtekst-terviktekst |
| Redaktsiooni jõustumise kp: | 13.07.2018 |
| Redaktsiooni kehtivuse lõpp: | Hetkel kehtiv |
| Avaldamismärge: | RT I, 10.07.2018, 6 |

# Võrgu- ja infosüsteemide riskianalüüsi nõuded ning turvameetmete kirjeldus

Vastu võetud 05.07.2018 nr 40

Määrus kehtestatakse küberturvalisuse seaduse§ 7 lõike 4 alusel.

**§ 1. Reguleerimisala**

Määrusega kehtestatakse nõuded küberturvalisuse seaduse § 3 lõikes 1 loetletud teenuste osutamiseks kasutatavate võrgu- ja infosüsteemide (edaspidi *süsteemid*) riskianalüüsi koostamisele ning organisatsiooniliste, infotehniliste ja füüsiliste turvameetmete (edaspidi *turvameetmed*) kirjeldus.

**§ 2. Terminid**

(1) Süsteemide riskianalüüs käesoleva määruse tähenduses on süsteemide turvalisust ja teenuse toimepidevust ohustavate riskide ja nende haldamiseks rakendatavate meetmete kirjeldus.

(2) Ressurss käesoleva määruse tähenduses on kõik süsteemide pidamiseks kasutatavad ja nende toimimist mõjutavad vahendid, sealhulgas ruumid, ruume teenindavad ventilatsiooni-, jahutus- ja kütteseadmed, ruume ja süsteeme elektrienergiaga varustavad seadmed, süsteemide käitamiseks kasutatav tarkvara ja teenuse osutaja personal.

(3) Kriitiline tegevus käesoleva määruse tähenduses on teenuse osutaja tegevus, mis sõltub vähemalt ühest süsteemist ja mis on oluline teenuse osutamiseks ning mille puudumisel võib teenus katkeda.

(4) Nõrkus käesoleva määruse tähenduses on süsteemide või süsteemidega seotud ressursside turvalisuse puudus, mis muudab süsteemid või süsteemidega seotud ressursid ohule vastuvõtlikuks.

(5) Oht käesoleva määruse tähenduses on sündmus või asjaolu, mis on võimeline süsteemide või nendega seotud ressursside nõrkust ära kasutama.

(6) Risk käesoleva määruse tähenduses on hinnanguline määratlus, mis kujuneb ohu poolt nõrkuse ärakasutamise tõenäosuse ja tekkida võiva küberintsidendi tagajärgede kombinatsioonist.

**§ 3. Nõuded süsteemide riskianalüüsi koostamisele**

(1) Teenuse osutaja esitab süsteemide riskianalüüsis vähemalt järgmised andmed:
1) süsteemide riskianalüüsis kasutatud metoodika lühikirjeldus ning viited riskianalüüsiga seotud lisadokumentidele;
2) loetelu teenuse osutamiseks vajalikest kriitilistest tegevustest koos nende toimimiseks vajalike süsteemidega;
3) loetelu süsteemidega seotud ressurssidest;
4) loetelu ohtudest;
5) loetelu nõrkustest;
6) hinnang ohtude realiseerumise tõenäosusele, arvestades tuvastatud nõrkusi ja rakendatud meetmeid;
7) hinnang võimaliku küberintsidendi tagajärgedele ning tagajärgede raskusaste, arvestades tagajärgede raskusastme määramise kriteeriumitena küberintsidendist mõjutatud isikute ligikaudset arvu, teenuse katkemise kestust, küberintsidendist mõjutatud piirkonna ulatust, võimalikku kahju liiki ja määra ning süsteemi turvalisuse või teenuse toimepidevuse taastamise keerukust;
8) loetelu riskidest koos iga riski kriitilisuse määraga;
9) riske maandavate abinõude kirjeldus.

(2) Teenuse osutaja tagab riskide pideva seire ja uuendab süsteemide riskianalüüsi iga uue riski ilmnemisel, mida teenuse osutaja hindab oluliseks.

(3) Teenuse osutaja võib süsteemide riskianalüüsi koostada muu õigusakti alusel koostatava dokumendi osana.

**§ 4. Turvameetmete kirjeldus süsteemide turvalisuse tagamiseks**

(1) Teenuse osutaja peab turvameetmetega hõlmama teenuse osutaja juhtorgani poolt kinnitatud:
1) protseduure, ressursse, tegevusi ning küberintsidendi lahendamise korraldust;
2) personali tööülesandeid ja vastutust.

(2) Turvameetmetega nähakse ette vähemalt:
1) süsteemide juurdepääsuõiguste haldamine, süsteemi kasutajate identifitseerimine ja autoriseerimine;
2) teenuse osutamiseks vajalikest andmetest regulaarsete varukoopiate tegemine ja protseduurid andmete varukoopiatest taastamiseks;
3) süsteeme käitava ja süsteemides käideldava tarkvara ajakohasus;
4) süsteemides läbiviidavate toimingute logid toimingu teostaja, toimingu liigi ja toimingu teostamise ajaga;
5) tarkvaralised ja riistvaralised lahendused süsteemide turvalisust ohustava tegevuse ja tarkvara tuvastamiseks ning tõrjumiseks;
6) protseduurid süsteemide turvalisuse või teenuse toimepidevuse taastamiseks.

(3) Teenuse osutaja rakendab, seirab ja ajakohastab turvameetmeid, et tagada § 3 alusel koostatud süsteemide riskianalüüsis loetletud riskide haldamine.

**§ 5. Määruse rakendamine**

Teenuse osutaja koostab § 3 alusel süsteemide riskianalüüsi hiljemalt 31. detsembriks 2018. a.

Urve Palo
Ettevõtlus- ja infotehnoloogiaminister

Merike Saks
Kantsler