Väljaandja:	Vabariigi Valitsus
Akti liik:	määrus
Teksti liik:	algtekst-terviktekst
Redaktsiooni jõustumise kp:	12.08.2017
Redaktsiooni kehtivuse lõpp:	22.05.2018
Avaldamismärge:	RT I, 09.08.2017, 3

Elutähtsa teenuse infosüsteemide ning nendega seotud infovarade turvameetmed

Vastu võetud 03.08.2017 nr 133

Määrus kehtestatakse hädaolukorra seaduse§ 41 lõike 3 alusel.

§ 1. Määruse reguleerimisala ja eesmärk

(1) Määrusega reguleeritakse elutähtsa teenuse osutamiseks kasutatavate infosüsteemide ja nendega seotud infovarade turvameetmete rakendamise korraldust.

(2) Määruse eesmärk on tagada elutähtsa teenuse osutamiseks kasutatavate infosüsteemide järjepideva toimimise suutlikkus ja taastamise võime pärast katkestust.

(3) Määrus, välja arvatud selle § 3, kohaldub lisaks elutähtsa teenuse osutajale ka muu teenuse osutajale, kui määruse nõuete rakendamise kohustus on sätestatud seaduses.

§ 2. Terminid

Määruses kasutatakse termineid järgmises tähenduses:
1) teenuse osutamise kriitiline tegevus (edaspidi *kriitiline tegevus*) – teenuse osutaja tegevus, mille puudumine toob kaasa teenuse katkestuse või häire;
2) infosüsteemi riskianalüüs – analüüs, mille käigus selgitatakse välja võimalikud ohud ja nõrkused infosüsteemile, hinnatakse ohtude realiseerumise tõenäosust ja nendega kaasnevaid kahjusid ning valitakse sobivad turvameetmed ohtude realiseerumise mõju vähendamiseks;
3) olulise mõjuga turvaintsident – teenuse osutamiseks kasutatava infosüsteemiga seotud sündmus, mis ohustab teenuse toimepidevust või toob kaasa teenuse katkestuse või häire või võib mõjutada teise teenuseosutaja teenuse osutamiseks vajaliku infosüsteemi toimimist;
4) oluline sõltuvus infosüsteemist – kriitilise tegevuse sõltuvus infosüsteemist, kui infosüsteemi, sealhulgas tööstusliku automaatjuhtimissüsteemi tõrge, võib põhjustada kriitilise tegevuse katkestuse või häire.

§ 3. Kriitilise tegevuse sõltuvus infosüsteemist

(1) Elutähtsa teenuse osutaja hädaolukorra seaduse § 38 lõike 3 punkti 1 alusel koostatavas toimepidevuse riskianalüüsis selgitatakse, kas ja millisel määral sõltub kriitilise tegevuse toimimine infosüsteemist.

(2) Kui kriitilise tegevuse sõltuvus infosüsteemist on oluline, kuid kriitilise tegevuse toimimise tagamiseks on alternatiivne lahendus, peab elutähtsa teenuse osutaja kirjeldama toimepidevuse riskianalüüsis hädaolukorra seaduse § 38 lõike 3 punktis 2 nimetatud ennetavaid meetmeid kriitilise tegevuse toimimise tagamiseks.

§ 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 vajadusel täiustab.

(2) Elutähtsa teenuse osutaja lähtub infoturbe halduse süsteemi rakendamisel vähemalt ühest järgnevast standardist, kui seadus ei sätesta teisiti:
1) EVS-ISO/IEC 27001 seeria infoturbe standard;
2) Vabariigi Valitsuse 20. detsembri 2007. a määrusega nr 252 „Infosüsteemide turvameetmete süsteem” kehtestatud infosüsteemide kolmeastmeline etalonturbe süsteem ISKE;
3) oma tegevusvaldkonnas kehtestatud infoturbe halduse erinõuded, mis tulenevad õigusaktist, välislepingust või muust lepingust ja on samaväärsed käesoleva lõike punktides 1 ja 2 nimetatud standarditega, ja heast tavast.

(3) Elutähtsa teenuse osutaja koostab valdkonna iseäralikke riske ja muid olulisi asjaolusid arvestades infosüsteemi riskianalüüsi.

(4) Elutähtsa teenuse osutaja rakendab käesoleva paragrahvi lõikes 3 nimetatud infosüsteemi riskianalüüsi alusel valitud infosüsteemi kaitseks ja teenuse toimepidevuse tagamiseks vajalikke turvameetmeid.

(5) Elutähtsa teenuse osutaja dokumenteerib rakendatud turvameetmed ja rakendamise protseduuri.

(6) Elutähtsa teenuse osutaja tagab turvameetmete rakendamisega vähemalt:
1) ligipääsu teenuse infosüsteemile vaid selleks õigustatud isikule;
2) õigustatud isiku turvalise tuvastamise;
3) kontrolljälje olemasolu, mis võimaldab tagantjärele kindlaks teha katkestuse toimumise aja ja muu kontrolliks või uurimiseks tähtsust omava asjaolu;
4) olulise mõjuga turvaintsidendi raporti olemasolu, mis sisaldab teenuse taastamise käiku pärast katkestust ja meetmeid katkestuse edasiseks vältimiseks;
5) elutähtsa teenuse osutamiseks vajalike andmete koopia säilitamise elektromagnetilise kiirguse eest kaitstud ruumis;
6) elutähtsa teenuse osutamiseks vajalike andmete salvestamisel andmekandjale tagama selle säilitamise asukohtades, mis on üksteisest piisaval kaugusel, arvestades võimalikke ohtusid ja nendest tulenevaid riske.

(7) Elutähtsa teenuse osutaja määrab isiku, kes vastutab turvameetmete rakendamise eest ning teavitab regulaarselt asutuse või ettevõtte juhti toimunud olulise mõjuga turvaintsidendist ja toimepidevuse häirest.

§ 5. Turvaintsidendi toimumisest ja lahendamisest teavitamine

(1) Elutähtsa teenuse osutaja teavitab olulise mõjuga turvaintsidendi toimumisest viivitamatult Riigi Infosüsteemi Ametit.

(2) Olulise mõjuga turvaintsidendi lahendamise järel edastab teenuse osutaja Riigi Infosüsteemi Ametile turvaintsidendi lahendamist kirjeldava raporti.

§ 6. Rakendussäte

Elutähtsa teenuse osutaja ja muu teenuse osutaja, kui käesoleva määruse nõuete rakendamise kohustus on sätestatud seaduses, koostab määruse § 4 lõike 3 alusel infosüsteemi riskianalüüsi 1. juuliks 2018. a.

Jüri Ratas
Peaminister

Urve Palo
Ettevõtlus- ja infotehnoloogiaminister

Aivar Rahno
Riigikantselei istungiosakonna juhataja riigisekretäri ülesannetes