SISEMINISTEERIUM

Majandus- ja Kommunikatsiooniministeerium Teie: 19.01.2021 nr MKM/21-0078/-1K

Meie: 15.02.2021 nr 1-7/18-5

Vastuskiri

Väliskaubandus- ja infotehnoloogia minister esitas kooskõlastamisele määruse "Küberintsidentide registri põhimäärus" eelnõu.

Siseministeerium kooskõlastab eelnõu märkustega.

Küberintsidentide registri põhimäärus luuakse küberturvalisuse seaduse (KüTS) § 13 alusel. Seaduses ja määruses on sätestatud eesmärkideks küberintsidentide üle arvestuse pidamine ja intsidentide analüüsimine nende lahendamiseks, ohuteadete edastamiseks ning järelevalve-toimingute teostamiseks. Siseministeeriumi hinnangul on register ka meie haldusala asutustele nii kuritegevuse kui sisejulgeoleku ohtude tõkestamiseks potentsiaalselt väga oluliseks tööriistaks.

1. Määruse §-s 7 sätestatud andmekoosseis on teoorias üsna põhjalik ja ulatuslik. Eelnõu § 6 on välja toodud registri ISKE turvaklass K1T1S2 ja turbeaste M. Siseministeeriumi hinnangul ei ole see turvatase piisav.

Esiteks juhime tähelepanu, et koondina on see informatsioon väga tundlik ning seda on vaja proportsionaalsete meetmetega kaitsta. Teiseks on eelnõu § 8 loetletud andmeandjate hulgas on ka Siseministeerium ning tema hallatavad asutused ning riigisaladuse ja salastatud välisteabe seaduse (RSVS) § 10 lg 1 ja lg 9 koosmõjus võib antud asutuste poolt edastatud küberintsidente käsitlev teave ning selle kogumina hoidmine RSVS mõistes infrastruktuuri ja teabe riigisaladus, mida tuleb salastada kas konfidentsiaalsel või madalamal tasemel kuni 30 aastat. Kolmandaks kattuvad osaliselt eelnõu § 2 välja toodud registri eesmärgid ja eelnõu § 7 lg 2 loetletud registrisse kantavad andmed riigisaladuse ja salastatud välisteabe kaitse korra (RSVKK) § 8 lg 1 p 32 nimetatud Riigi Infosüsteemide Ameti (RIA) poolt kogutava teabega, milline salastatakse piiratud tasemel 10 aastaks. Riigisaladuse esinemisel tuleb registrile kohaldada RSVKK § 39 lg 2 p 3 ehk arvutite ja kohtvõrkude kaitse nõuete määrust (AKKN).

2. Eelnevaga seoses palume RIA-l täiendavalt hinnata peetava registri eesmärki. Probleem tuleneb eelnõu seletuskirja §-st 12, milles selgitatakse, et registris kajastuvad ka mõjuta intsidendid ehk „õngitsuskirjad, mille ohvriks ei ole keegi langenud“. See selgitus ei haaku KüTS intsidendi definitsiooniga, mis on selgitatud ka seletuskirjas § 12 all. Ebaõnnestunud õngitsuskirjad, mida saabub nii avaliku- kui erasektori meiliaadressidele üleriigiliselt tuhandeid, siia sellisel kujul ei kvalifitseeru. Siseministeerium ei väida, et sellist infot ei oleks vajalik süstematiseerida, vaid peab vajalikuks see eelnõus ja seletuskirjas selgemalt eristada.

Pikk 61 / 15065 Tallinn / 612 5008 / info@siseministeerium.ee / www.siseministeerium.ee
Registrikood 70000562

Eelnevast kahest märkusest lähtuvalt teeb Siseministeerium ettepaneku kajastada registris üksnes intsidentide arvestust, kaitstes seda seejuures rangemate ISKE nõuetega, kui K1T1S2. Selline lähenemine võimaldab kajastada intsidentide tundlikumat informatsiooni eraldi süsteemis, mis oleks kooskõlas ka riigisaladuse kaitse nõuetega, kui intsidendiga seotud haavatavus ja intsidendi koondanalüüs seda nõuavad. Juhul, kui RIA registri pidajana siiski soovib registris käsitleda oluliselt sisulisemat informatsiooni (nagu sätestatud eelnõu §-s 7, mh piiratud tasemel riigisaladust), peab register vastama ka AKKN nõuetele.

3. Eelnõu seletuskirjas on märgitud, et registri loomisega kulusid ei kaasne. Siseministeerium näeb vajadust registri tervikliku eesmärgi täpsustamisega seoses täiendavalt üle hinnata ka kulud.

4. Eelnõu § 5 sätestab registri pidamise elektroonilisel kujul. Eelnõus ei ole ettenähtud, et loodav register oleks liidestatud infosüsteemide andmevahetuskihiga (edaspidi X-tee). Ka eelnõu seletuskirjas ei ole selgitatud, miks ei ole peetud vajalikuks, et loodav register oleks riigi infosüsteemi kuuluv andmekogu, st andmekogu, mis registreeritakse riigi infosüsteemi halduse infosüsteemis (RIHA) ning liidestatakse X-teega. Sellega seoses palub Siseministeerium selgitusi, miks ei ole X-teega liidestamist peetud vajalikuks.

5. Eelnõu § 10 sätestab andmetele juurdepääsu. Siseministeeriumi hinnangul ei ole õiguslikult üheselt selge, kas eelnõu § 10 võimaldab vastutaval töötlejal ehk RIA-l anda juurdepääse iseseisvalt. Siseministeeriumi haldusalas omavad kindlasti ligipääsuvajadust Politsei- ja Piirivalveameti Keskkriminaalpolitsei (PPA) ning Kaitsepolitseiamet (KAPO). PPA tegeleb intsidentide menetlemisega ning KAPO teeb järjepidevalt tööd Eesti riiklikku julgeolekut ohustavate küberrünnete tuvastamisel ja tõkestamisel.

Sellest tulenevalt teeb Siseministeerium ettepaneku sätestada eelnõu §-s 10 konkreetsed asutused, kellele on juurdepääs õiguslikult tagatud või sõnastada asutuste ja isikute juurdepääs läbi seadusest tulenevate ülesannete täitmise pädevuse.

6. KüTS § 8 sätestab teenuse osutajate kohustuse teavitada Riigi Infosüsteemide Ametit intsidentidest. Sama paragrahvi lõige 8 annab õigusliku aluse kehtestada küberintsidentidest teavitamise kord ja raporti vorm. Siseministeeriumi hinnangul oleks asjakohane registri loomisel kaaluda ka ühise edastamise korra ja intsidendi vormi kehtestamist, et tagada intsidentide andmete ühetaolisus ja selgem struktuur.

Lugupidamisega

(allkirjastatud digitaalselt)

Kristian Jaani
siseminister

Martin Reissar 6125018
martin.reissar@siseministeerium.ee