29.12.2020

Väliskaubandus- ja infotehnoloogiaministri määruse „Küberintsidentide registri põhimäärus“ eelnõu seletuskiri

1. Sissejuhatus

1.1. Sisukokkuvõte

Määruse eelnõu kohaselt asutatakse riigi infosüsteemi mitte kuuluv andmekogu ametliku nimetusega küberintsidentide register ning kehtestatakse selle pidamise põhimäärus.

Määrus kehtestatakse küberturvalisuse seaduse (edaspidi *KüTS)* § 13 lõike 3 alusel.

KüTS § 13 kohaselt on küberintsidentide register Riigi Infosüsteemi Ameti peetav andmekogu, kuhu kantakse küberintsidenti kirjeldavad andmed eesmärgiga pidada küberintsidentide üle arvestust nende tuvastamiseks, analüüsimiseks, lahendamiseks, ohuteadete edastamiseks ja järelevalve teostamiseks. Küberintsidentide register koondab endas informatiivset teavet Eesti arvutivõrkudes toimuvate ja Riigi Infosüsteemi Ametile edastatud või Riigi Infosüsteemi Ameti tuvastatud võrgu- ja infosüsteemides küberintsidentide kohta.

Eelnõuga sätestatakse muu hulgas registri nimetus, eesmärk, registri vastutav töötleja, registri andmed, registriandmete kaitse, registriandmete säilitamine, registri finantseerimine ja likvideerimine.

1.2. Ettevalmistajad

Määruse eelnõu ja seletuskirja on koostanud ning keeletoimetuse teinud Riigi Infosüsteemi Ameti õigusnõunik Silver Lusti (silver.lusti@ria.ee) ning Majandus- ja Kommunikatsiooniministeeriumi küberturvalisuse õigusnõunik Kea Kohv (kea.kohv@mkm.ee). Eelnõu juriidilise ekspertiisi teostas Majandus- ja Kommunikatsiooniministeeriumi õigusosakonna õigusnõunik Ave Henberg.

2. Eelnõu sisu ja võrdlev analüüs

Eelnõu koosneb neljast peatükist ja 14-st paragrahvist.

Eelnõu 1. peatükis on üldsätted.

Paragrahvis 1 sätestatakse Riigi infosüsteemi Ameti loodava andmekogu nimetus, milleks on „Küberintsidentide register“.

Paragrahvis 2 nähakse ette registri pidamise eesmärk. Registri pidamisel ja andmete töötlemisel lähtutakse avaliku teabe seaduse (edaspidi *AvTS*) §-s 43^1 ja KüTS §-s 13 sätestatud

eesmärgist, mille kohaselt on küberintsidentide registri puhul tegemist Riigi Infosüsteemi Ameti peetava ja infosüsteemis töödeldava korrastatud andmete kogumiga, kuhu kantakse küberintsidenti kirjeldavad andmed, eesmärgiga pidada küberintsidentide üle arvestust ning analüüsida neid nende lahendamiseks, ohuteadete edastamiseks ja järelevalvetoimingute läbiviimise toetamiseks. Küberintsident käesoleva põhimääruse mõistes on vastavalt KüTS § 2 punktile 3 süsteemis toimuv sündmus, mis ohustab või kahjustab süsteemi turvalisust.

Paragrahvis 3 sätestatakse registri vastutav töötleja ehk registripidaja, kelleks on Riigi Infosüsteemi Amet. Vastavalt AvTS § 43^4 lõikele 1 korraldab vastutav töötleja andmekogu kasutusele võtmist ja andmete haldamist ning vastutab andmekogu haldamise seaduslikkuse ja andmekogu arendamise eest. KüTS § 13 lõike 1 kohaselt on tegemist Riigi Infosüsteemi Ameti peetava andmekoguga. Riigi Infosüsteemi Amet majutab küberintsidentide registrit ning korraldab registri teenuste ja tehnoloogilise keskkonna haldamise. Registril ei ole volitatud töötlejat.

Paragrahvis 4 kohaselt on andmekogusse kantud andmetel informatiivne tähendus.

Paragrahvis 5 sätestatakse andmete säilitamise kord, millega nähakse ette registri pidamine ja andmete säilitamine elektroonilisel kujul.

Paragrahvis 6 sätestatakse registri turvaklass ja turbeaste. Registri turvaklass ja turbeaste on määratud vastavalt Vabariigi Valitsuse 20. detsembri 2007. a määrusele nr 252 „Infosüsteemide turvameetmete süsteem". Turvaosaklassid on määratud järgnevalt: andmete käideldavuse alusel K1, kuivõrd töökindlus peab olema tagatud vähemasti 90% ulatuses; terviklikkuse alusel T1, kuivõrd info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad; konfidentsiaalsuse alusel S2, kuivõrd info kasutamine on lubatud ainult teatud kindlatele kasutajate gruppidele ja juurdepääs teabele on lubatav üksnes juurdepääsu taotleva isiku õigustatud huvi korral. Registri turbeaste on seega vastavalt ISKE rakendusjuhendile keskmine (M).

Eelnõu 2. peatükis on reguleeritud andmete koosseis ja andmete esitamine registrisse.

Paragrahv 7 lõige 1 sätestab, et küberintsidentide registrisse kantakse andmed küberintsidendi ja andmeandja kohta. Lõige 2 sätestab registris sisalduda võivate andmete loetelu. Tegemist on ammendava loeteluga registris sisalduda võivatest andmetest. Samas ei ole kõik loetelus olevad andmed kohustuslikud, kuna alati ei pruugi olla iga loetelus oleva punkti kohta informatsiooni. Lõikes 3 sätestatakse registrisse sisestatav informatsioon küberintsidendi andmeandja ja lahendaja kohta.

Paragrahvis 8 sätestatakse küberintsidentide kohta vastutavale töötlejale teavet esitavate isikute ehk andmeandjate ring. Andmeandjateks ehk küberintsidendist teatajaks on teenuse osutaja KüTS-i tähenduses või riigi- või kohaliku omavalitsuse üksus või muu isik, kes esitab vastutavale töötlejale teavet küberintsidendi kohta. Küberintsidendist teatanud isik ei pruugi tingimata olla ise mõjutatud isik. Andmeandjaks saab pidada ka Riigi Infosüsteemi Ametit

(vastutav töötleja), kelle poolt küberintsidentide ennetamiseks teostatav seire võib välja tuua teavet küberintsidentide registri eesmärgipäraseks toimimiseks.

Paragrahv 9 sätestab vastutava töötleja kohustuse kanda registrisse kõik temale esitatud teavitused või raportid küberintsidentide kohta.

Teatiste ja raportite esitamise vorminõuet ei ole senini teadlikult sisustatud selleks, et kogu vajalik teave küberintsidentide toimumise ja lahendamise osas jõuaks viivitamatult vastutava töötlejani ning teatamise kohustuslik vorm takistuseks ei muutuks, näiteks juhtudel, kui teatatakse telefoni või e-maili teel. Vastavalt KüTS § 8 lõikele 8 võib teavitamise korra ja raporti vormi võib kehtestada valdkonna eest vastutav minister määrusega, kuid kehtestamine pole kohustuslik.

Raporti esitamise kohustus tuleneb KüTS § 8 lõikest 7, mille järgi teenuse osutaja on olulise mõjuga küberintsidendi lahendamisel kohustatud edastama Riigi Infosüsteemi Ametile raporti, mis sisaldab informatsiooni küberintsidendi tekkepõhjuste, selle lahendamiseks kulunud aja ja rakendatud abinõude ning küberintsidendi mõju kohta. Seega raportit eristab teavitusest see, et raport esitatakse peale intsidendi lahendamist ja raportis peab sisalduma kindlasti informatsioon tekkepõhjuste, lahendamiseks kulunud aja, rakendatud abinõude kohta ja küberintsidendi mõju. Neid ei pruugita intsidendi alguses teada, kui küberintsidendist teavitatakse.

Registrisse kantakse kõik CERT-il jõudnud teave. Selline teave on registris oluline, et teha laiapindsemaid järeldusi üht või teisti liiki intsidentide leviku osas perioodiți/regionaalselt/domeeni kaupa või mis iganes muul moel liigitatud kujul. See võimaldab näiteks anda aimu sihitud rünnetest.

Eelnõu 3. peatükis sätestatakse registri andmete kaitse.

Registriandmed on mõeldud asutusesiseseks kasutamiseks lähtudes eelkõige avaliku teabe seaduse § 35 lõike 1 punktides 2 ning 9-12 sätestatud juurdepääsupiirangute alustest. Registriandmed võivad sisaldada teavet poolelioleva järelevalvemenetluse, turvasüsteemide või turvameetmete kirjelduse või tehnoloogiliste lahenduste kohta. Samuti võib registrisse kantud teave sisaldada isikuandmeid. Olenevalt küberintsidendi asjaoludest võib olla juurdepääsupiirangu seadmine põhjendatud ka muudel alustel kooskõlas avaliku teabe seadusega.

Kuna tegemist on piiratud juurdepääsuga registriga, on juurdepääs registriandmetele teatud kindlatel kasutajate gruppidel, kellel on selleks seadusest või seaduse alusel antud õigusaktist tulenev õigus ja õigustatud huvi.

Paragrahv 10 sätestab andmetele juurdepääsu. Lõike 1 kohaselt määrab vastutav töötleja isikud, kellel on õigus töödelda registriandmeid töö- või teenistusülesannete täitmiseks. Samuti määratakse nende isikute kasutajakonto õiguste klass. Reeglina saadakse lihtkasutaja õigused, kuid kindlatel isikutel on ka eeliskasutaja õigused.

Lõige 2 sätestab vastutava töötleja kohustuse pidada arvestust registrist väljastatud andmete üle, säilitades andmed kellele, millisel eesmärgil, millal, millisel viisil ja missuguseid andmeid registrist väljastatakse.

Lõigk 3 kohaselt säilitades iga registrisse tehtud päringu või kande, andmete lisamise, muutmise, sulgemise või kustutamise kohta vähemalt päringu või kande tegija andmed, päringu või kande tegemise sisu, kuupäeva ja kellaaja kohased andmed.

Paragrahvis 11 sätestatakse lõikega 1, et andmeandjad vastutavad küberintsidentide registrisse esitatud andmete õigsuse eest. Lõike 2 kohaselt võtab vastutav töötleja küberintsidentide registris andmete ebaõigsuse kindlaks tegemisel kasutusele vajalikud meetmed ebaõigete andmete parandamiseks.

Paragrahv 12 määrab andmete säilitamise tähtajaks viis aastat alates intsidendi lahendamisest või viis aastat alates intsidendi tuvastamisest, kui intsidendil pole mõju. Mõjuta intsident on sündmus, mille eesmärk on avaldada mõju süsteemi käideldavusele, terviklusele või konfidentsiaalsusele, aga see ei ole õnnestunud. Näiteks õngitsuskirjad, mille ohvriks ei ole keegi langenud. Registri logisid säilitatakse üks aasta.

Eelnõu 4. peatükk on reguleeritud registri finantseerimine ja likvideerimine.

Paragrahv 13 kohaselt rahastatakse registri pidamist riigieelarvest Riigi Infosüsteemi Ameti eelarve kaudu. Tänaseni on registri arendus- ja hooldustöödeks kaasatud osaliselt struktuurifondide (SF) või Euroopa ühendamise (CEF) rahastust, kuid pidades silmas registri olulisust kogu riigi küberturvalisuse tagamise vaatest, on mõistlikum ja jätkusuutlikum rahastada registri arendus- ja hooldustöid ning pidamist riigieelarvelistest vahenditest Riigi Infosüsteemi Ameti eelarve kaudu.

Paragrahvis 14 sätestatu kohaselt toimub registri likvideerimine seaduse alusel. Likvideerimisel tuleb otsustada andmete teise andmekogusse või avalikku arhiivi üleandmise või andmete hävitamisele kuulumine ja nende üleandmise või hävitamise tähtaeg.

Seadusest tulenevalt teostab registri pidamise üle järelevalvet Andmekaitse Inspektsioon, mistõttu seda määruses ei korrata.

3. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõu on vastavuses Euroopa Liidu õigusega.

4. Määruse mõjud

Määruse kehtestamisega ei kaasne otsest sotsiaalset ega demograafilist mõju, olulist mõju riigi julgeolekule ega välissuhetele, majanduslikku mõju ega mõju elu- ja looduskeskkonnale,

regionaalarengule, riigiasutuste ja kohaliku omavalitsuse korraldusele ega muud otsest ja kaudset mõju. Eelnõu rakendamisega võib ette näha mõju riigiasutuste ja kohaliku omavalitsuse korraldusele, täpsemalt Riigi Infosüsteemi Ametile.

Kaasnev mõju: mõju riigiasutuste ja kohaliku omavalitusese korraldusele
Sihtrühm: Riigi Infosüsteemi Ameti teenistujad
Mõju ulatus: Tuvastatud mõju on väike. Määrust rakendab Riigi Infosüsteemi Amet ehk registripidaja. Märkimisväärseid muutusi töös ei toimu.
Mõju avaldumise sagedus: mõju avaldumise sagedus sõltub sellest, kui palju küberintsidentidest teatatakse ja kui palju küberintsidente registripidaja ise tuvastab. Hetkel on saadav ja tuvastatav küberintsidentide arv hallatav.
Ebasoovitavate mõjude risk: väike, kuna negatiivset mõju andmete esitamisega ei kaasne.

5. Määruse rakendamisega seotud tegevused, vajalikud kulud ja määruse rakendamise eeldatavad tulud

Määruse rakendamine ei too kaasa täiendavaid kulusid ega tulusid. Määrust rakendatakse olemasolevate ressursside raames. Eelnõu ei puuduta registrite arendamist, kasutusele võtmist või likvideerimist, mis tooksid kaasa rahalisi mõjusid.

6. Määruse jõustumine

Määrus jõustub üldises korras ehk kolmandal päeval pärast Riigi Teatajas avaldamist.

7. Määruse eelnõu kooskõlastamine, huvirühmade kaasamine ja avalik konsultatsioon

Määruse eelnõu saadetakse kooskõlastamiseks Kaitseministeeriumile, Siseministeeriumile, Justiitsministeeriumile, Välisministeeriumile, Andmekaitse Inspektsioonile, Riigi Infosüsteemi Ametile, Statistikaametile ning arvamuse andmiseks Eesti Infotehnoloogia ja Telekommunikatsiooni Liidule ja Eesti Infoturbe Assotsiatsioonile.