SISEMINISTEERIUM

Majandus- ja Kommunikatsiooniministeerium Teie: 02.12.2023 nr MKM/23-1602/-1K

Meie: 04.01.2024 nr 1-7/305-4

Eelnõu kooskõlastamine märkustega

Siseministeerium (edaspidi *SIM*) on tutvunud kooskõlastamiseks esitatud ettevõtlus- ja infotehnoloogiaministri 12. detsembri 2022. a määruse nr 101 „Eesti infoturbestandard" muutmise eelnõuga (edaspidi määruse eelnõu). Siseministeeriumi tähelepanekud on esitatud mitmes osas. Kooskõlastame määruse eelnõu esimeses ja teises punktis kirjeldatud märkustega arvestamisel.

1. Märkused:
   1.1. Määruse eelnõu lisa 1 punktis 10.2 on esitatud nõuded infoturbe halduse süsteemile. Palun täpsustada millist eesmärki kannab regulaarne sõltumatu läbivaatus, kui organisatsioon peab regulaarselt korraldama ka E-ITS-i auditit? Kas sellisel juhul on sõltumatu läbivaatus veel täiendavalt vajalik? Antud meede tähendab suurt lisahalduskoormust. Samas E-ITS-i eel-, põhi-, järel- ja vaheauditite täidetakse juba sarnast eesmärki.
   1.2. Määruse eelnõu seletuskirjas (lk 3) on kirjas, et E-ITS-i uuendamine toimub iga aasta sügisel – ettepanek uuendada standardit nt 3–5 aastase intervalliga, sest iga-aastase uuendamisega kaasneb asutustele järjepidev ajaga võidu jooks. Teisisõnu, asutused ei pruugi jõuda veel varasema versiooni meetodeid kasutusele võtta / nende rakendamiseks plaani teha, kui juba koostatakse uut versiooni. Eriti keeruline on see suurtes organisatsioonides, kus on palju protsesse. Samuti avaldub mõju ka väikestes organisatsioonides, kus sageli täidab üks inimene paljusid erinevaid rolle.
   1.3. Üldine tähelepanek: E-ITS ei kirjelda, kuidas käsitleda protsessile/teenusele määratud kaitsetarvet infosüsteemile määratava turvaklassi osas. Ehk kas need on 1:1 samad või peaks teatud juhul määrama kaitsetarbe infosüsteemile eraldi? Näiteks, kuidas määratleda infosüsteemi turvaklassi, kui see sisaldab kõiki neid tundlikke andmeid, mille tõttu on ka protsessi kaitsetarve suur? Samas, kuidas määratleda infosüsteemi turvaklassi juhul, kui protsessi kaitsetarve on suur või väga suur, aga infosüsteemile nii suuri nõuded ei pea kohaldama (nt infosüsteem ei pea olema 24 h kättesaadav, ei mõjuta teisi infosüsteeme või ei sisalda selliseid isikuandmeid, mida protsessi käigus muul moel ja teises asukohas töödeldakse). Kirjeldatud juhul võib olla majanduslikult ebamõistlik rakendada infosüsteemile meetmeid suure või väga suure kaitsetarbe järgi.
   1.4. Praegu on asutustele pandud kohustus koormavam, kui võimalus seda tagada olukorras, kus organisatsioon (rakendab E-ITS-i) ise ei taga IKT teenuseid, vaid seda teeb eraldiseisva asutusena n-ö IT-maja (rakendab ISO-t). Taustakirjeldusena saab välja tuua, et dokumendi „E-ITS – Nõuded infoturbe halduse süsteemile" kohaselt on E-ITS-i eesmärk tagada avalike ülesannete täitmiseks kasutatavate äriprotsesside ja infosüsteemide kõikehõlmav kaitse ning saavutada infoturbe ühtlane tase nende kõigis

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

osades kogu elutsükli jooksul (lisa 1, lk 8). Samas dokumendis on viidatud, et E-ITS-i rakendamisega standardturbe ulatuses saavutatakse vastavus rahvusvahelise standardiga ISO/IEC 27001. See vastavus võimaldab E-ITS-i rakendajatel oma kaitsealale taotleda rahvusvahelist tunnustamist ISO/IEC 27001 sertifikaadiga. Siinjuures, ISO/IEC 27001 vastavussertifikaat ilma E-ITS-i rakendusplaanita E-ITS-i rakendatust ei kinnita. (lisa 1, lk 8). Standardturbe korral rakendatakse lisaks esmajärjekorras rakendatud põhimeetmetele standardmeetmeid ning veendutakse etalonturbe välise riskihaldusega etalonturbe meetmete piisavuses. Vajaduse korral rakendatakse olenevalt kaitsetarbest kõrgmeetmeid ja etalonturbe välise id lisameetmeid. Väljajäetud põhimeetmeid ja standardmeetmeid põhjendatakse, lähtudes eelkõige riskide aktsepteerimise kriteeriumitest (lisa 1, lk 8).
Samas, Eesti Infoturbestandardi lehelt on leitav praegu kehtiv tabel E-ITS-i 2022 versiooni vastavusest ISO/IEC 27001:2017 standardi nõuetele, mille enam kui 4000+ meetmest umbes pooled s.o 2000+ on üksnes osaliselt vastavuses. Neist valdav enamus on põhi- ja standardmeetmed. Seetõttu palume õigusselguse huvides selgitada, kas ISO meetmed hakkavad lähiaastal vastama kõigile E-ITS-i meetmetele. Kui ei, siis millise erisusega käsitletakse organisatsioonile pandud vastutuskohustust (lisa 1, lk 10), kui vastavuse tagamine ei sõltu organisatsioonist endast? Või alternatiivselt, kuidas vastutus ja ülesanded vastavuserisuste kaotamata jätmisel jaotatakse?

1.5. Palume kaaluda antud määruse alusel muuta Riigi Kinnisvara AS-i (edaspidi RKAS) E-ITS-i kohuslaseks. Seda põhjusel, et RKAS haldab väga suurt osa riigi kinnisvarast, kus on kasutusel mitmesuguseid taristu ja infotehnoloogia komponente. Need mõjutavad klientide infoturvet ja halvemal juhul võivad kaasa tuua suure mõjuga intsidente. Teiseks on RKAS-il märkimisväärne roll turvalise tarneahela tagamisel, millega seotud riske võimaldab kirjeldatud meede maandada.

2. Meetmed:
   2.1. Miks nii CON.2.M2 Andmekaitsespetsialisti (andmekaitseametniku) määramine kui ka kõik CON.2 meetmed on sisustatud kitsalt isikuandmete kaitse üldmääruse (IKÜM) kaudu? Ka muus osas pole mainitud näiteks isikuandmete kaitse seaduse (IKS) või muu asjakohase regulatsiooni kohaldumist. Interpoli andmetöötlusreeglite alusel peab olema määratud ka andmekaitseametnik ja infoturbejuht ning rakendatud turvameetmeid jne. Näiteks CON.2.M29 on sisse toodud avaliku sektori erisusena avaliku teabe seadus (AvTS).
   2.2. Kui E-ITS on infoturvapoliitika ja -protsessi keskne, andmekaitse on konkreetselt fookuses CON.2, siis kas või miks pole infoturvapoliitika ja -protsessi teemades andmekaitset/andmekaitsespetsialisti eraldi välja toodud.
   2.3. CON.2.M26 b. järgi korraldatakse andmekaitseaudit vähemalt kord nelja aasta jooksul. Kas see on sama süsteem, mida on nimetatud lisas 3 (eel-, põhi-, järel- ja vaheaudit)? Näiteks SIS ja VIS audit oli Andmekaitse Inspektsioonil (AKI) üles ehitatud ISO standardile, samuti on nende tulevased (2024. a alguse saavad) logide auditid ISO meetmete põhised. EL-i õigusaktidest tuleneb aga mitte vastutavale töötlejale, vaid järelevalveasutusele kohustus korraldada konkreetselt määratletud või umbkaudse intervalli järel auditeid. Kas praktikas vaadatakse üle, et Politsei- ja Piirivalveameti ning AKI auditid toimuksid vaheldumisi? Asutustel on juba iga-aastaseid auditeid ning iga lisaaudit on dubleerimine ja täiendav koormus. Palume täiendavalt tuua välja selgitused ja arvestada ka teiste võimalike auditite ga.

3. Täiendavad tähelepanekud määruse eelnõu ja sõnastuse kohta:
   3.1. Palume täpsustada määruse lisa 1 punkti 4 sõnastust. Praegu tekitab segadust sõnastuses, mille järgi E-ITS vastab ISO standardile. Sellest jääb mulje, et ISO standard on midagi väga detailset ja spetsiifilist ning E-ITS proovib sellele vastata. Tegelikkus

on ju vastupidine. ISO on palju üldisem. Kas saame selle alusel öelda, et üks vastab teisele?

3.2. Palun täpsustada määruses, millal kasutada infoturva ja millal infoturbe (infoturve) mõistet. Lisaselgitust on vajalik, sest probleemid tekivad nt muukeelsete dokumentide tõlkimisel eesti keelde. Tõlk võib tõesti aru saada, milline on semantiline vahe, kuid tavainimese jaoks on see keeruline. Eriti, kui tekstis on läbivalt kasutusel mõlemad.

3.3. Lisa 1 punktis 7.1.3 tuuakse välja tarneahela hindamine väljast tellitavatele teenustele. Palume täpsustada või sõnastada antud punkt selgemalt. Milliseid väljast tellitavaid teenuseid on mõeldud ja kus tuleb vajalik osa kirjeldada?

Lugupidamisega

(allkirjastatud digitaalselt)

Lauri Läänemets
siseminister

info- ja varahaldusosakond