SISEMINISTEERIUM

Liisa-Ly Pakosta
Justiits- ja Digiministeerium

Teie: 09.12.2024 nr MKM/24-1266/-1K

Meie: 10.02.2025 nr 1-7/279-5

Vastuskiri

Lugupeetud justiits- ja digiminister

Siseministeerium kooskõlastab „Küberturvalisuse seaduse ja teiste seaduste muutmise seadus (küberturvalisuse 2. direktiivi ülevõtmine)“ eelnõu alljärgnevate märkustega.

1. Eelnõu sätestab teenuse osutaja juhtorganile kohustuse läbida korrapäraselt erikoolitusi. Siseministeeriumi hinnangul on juhtorgani liikmete koolituste kohustus samm õiges suunas, kuid koolituste sisu ja kvaliteet on jäetud määratlemata. Samuti puudub selgus, kuidas koolituste läbimist jälgitakse.

   Tekib küsimus, mida tähendab, et teenuse osutaja juhtorgani liige peab läbima korrapäraselt erikoolitusi, mille õpiväljunditeks on piisavate teadmiste ja oskuste omandamine, et mõista ja hinnata küberturvalisuse riske, nendest tulenevat mõju teenuse osutaja osutatavatele teenustele ning viise riskide käsitlemiseks? Siseministeeriumi hinnangul peab juhtorgani kohustuste osas olema seletuskirjas erikoolituse õpiväljundid detailsemalt lahti kirjeldatud.

2. Samuti ei ole välja toodud erikoolituse vajaduse ajaline kriteerium. Kuivõrd NIS2 direktiiv ei määratle, mis on erikoolituste läbimise välp ehk mis aja tagant tuleks taolisi koolitusi teha, siis õigusselguse tagamiseks teeb Siseministeerium ettepaneku määrata koolituse läbimise välbaks 3 aastat, kuna ka E-ITSis (Eesti infoturbestandard) määratletud audititsükkel on käesolevalt 3 aastat.

3. Eelnõu § 7 lg 2 punktid 1-3 näevad ette teenuse osutajale kohustused turvameetmete rakendamisel. Käesolevalt on turvameetmete rakendamine kirjeldatud E-ITSis, mis annab juhtkonnale kaalutlusõiguse erinevate meetmete rakendamise ulatuses. Palume eelnõu seletuskirjas välja tuua hinnang kõigi turvameetmete rakendamisega lisanduvate kulude osas, et oleks võimalik planeerida eelarvelisi kulutusi.

4. Siseministeerium nõustub, et subjektide laiendamine on vajalik, kuid suurenev subjektide hulk toob kaasa järelevalve ja nõustamise mahu kasvu, mis võib ületada RIA võimekuse. On risk, et järelevalve ja toe pakkumise võimekus väheneb. Tekib küsimus, kas RIA-l on piisavalt ressursse uute nõuete täitmise tagamiseks? Kuidas planeerib RIA teha nii suurele subjektide arvule järelevalvet? Nimelt on täna subjektide arv väga suur ja audiitorid ei jõua E-ITSi auditeid teha, siis kuidas on tagatud efektiivne ja pidev järelevalve tegevus?
   Siseministeerium teeb ettepaneku hinnata nimekirja laiendamise tegelikku mõju järelevalveasutusele.

5. Eelnõu § 8^1 lõike 1 ja 2 kohaselt Riigi Infosüsteemi Ametile (edaspidi RIA) võib: 1) teenuse osutaja teavitada küberintsidendist, nõrkusest ja küberohust; 2) muu isik kui teenuse osutaja teavitada olulise mõjuga küberintsidendist, nõrkusest ja küberohust.

   Sätte sõnastusest jääb ebaselgeks, miks on vabatahtliku teavitamise võimalus sätestatud seaduses just RIA suunal. Kui eesmärgiks on teadlikult luua konkreetne teabevahetuse ahel, tuleks kaaluda ka võimalusi, kuidas RIA saaks kogutud informatsiooni edastada asjakohastele partnerasutustele, nagu Politsei- ja Piirivalveamet (edaspidi PPA), Kaitsepolitseiamet või Andmekaitse Inspektsioon.

6. NIS2 direktiivi põhjenduspunktis 106 sätestab, et direktiivi alusel nõutava teabe esitamise lihtsustamiseks ja üksuste halduskoormuse vähendamiseks peaksid liikmesriigid asjakohase teabe esitamiseks ette nägema tehnilised vahendid, nagu ühtne kontaktpunkt, automatiseeritud süsteemid, veebipõhised vormid, kasutajasõbralikud liidesed, teatevormid, spetsiaalsed platvormid, mida üksused saavad kasutada, olenemata sellest, kas nad kuuluvad käesoleva direktiivi kohaldamisalasse. PPA on täna koos RIA-ga saamas küberintsidentide osas kontaktpunktiks.

   Antud kontekstis tekib küsimus, et kuidas ja mismoodi oleks mõistlik ühtset kontaktpunkti Eestis luua ja lisaks ei selgu, et mis õigusnormid juurde tulevad, mis täpsed kohustusi, mis mahus ja mis eelarvelisi vahendeid see asutuselt nõuaks PPA küberüksuselt. Siseministeerium teeb ettepaneku, et juhtivaks kontaktiks ENISA-le jätta RIA. PPA oleks toetav osapool ning protseduurid lepitakse eraldi kokku.

7. Eelnõu paragrahvis 4^2 on edaspidi vaja RIA taotlusel esitab teenuse osutaja vahearuande olulise mõjuga küberintsidendi lahendamise seisu kohta. Siseministeerium teeb ettepaneku täiendada seletuskirjas vahearuande eesmärki, sisu, ajalist raami (nt nädala jooksul pärast intsidenti) ja kirjutada soovitud sisu lahti sarnaselt intsidenditeatele.

8. Eelnõus on välja toodud, et mõju majandustegevusele ja riigiasutustele on teatav ja sellest tulenevalt palume veelkord mõelda ja kaaluda täiendavaid rahastusallikaid NIS2 rakendamisele, sest varasemalt Eesti infoturbe standardi rakendamisel on MKM öelnud, et mõju puudub, kuid tegelikkuses on auditi hind märkimisväärselt kõrgem eelnõu seletuskirjas pakutuga ja infoturbe personali halduskoormus ebamõistlikult suur.

9. Juhime tähelepanu asjaolule, et kolme aasta jooksul ei ole lahenenud audiitorite vähesuse probleem, mis toob tulevikus suure tõenäosusega kaasa auditi hangete ebaõnnestumisi ja märkimisväärse hinnatõusu. Lisaks ei jätku kõikidele subjektidele audiitoreid, sest E-ITS auditeid peab tegema 3 aastase tsükliga ja iga aasta peaks pea kõikidele subjektidele tegema auditi. Riigil ei ole mõistlik tekitada olukorda, kus subjektid rikuvad tahtmatult seadust (ei suuda auditi kohustust täita endast mitteolenevatel põhjustel).

Lugupidamisega

(allkirjastatud digitaalselt)

Lauri Läänemets
siseminister