KAITSEMINISTEERIUM

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

Majandus- ja Kommunikatsiooniministeerium
Suur-Ameerika 1, 10122 Tallinn
info@mkm.ee

Meie: 19.02.2025 nr 5-7/24/173-4

Eelnõu kooskõlastamine

Olete edastanud Kaitseministeeriumile kooskõlastamiseks küberturvalisuse seaduse ja teiste seaduste muutmise eelnõu. Kaitseministeerium kooskõlastab eelnõu järgmiste märkustega:

1. Planeeritava § 2 punkti 33 kohaselt on risk küberintsidendist tingitud kahju või häire võimekus, mida tuleb väljendada sellise kahju või katkestuse ulatust ja kõnealuse küberintsidendi esinemise võimalikkust arvesse võtva kombineeritud näitajana. Juhime tähelepanu, et kahju või häire ei saa olla võimekus. Palume asendada sõna „võimekus“ sõnaga „võimalus“. Lisaks on definitsioon sarnane NIS2 direktiivis tooduga, kuid osa sõnu on erinevad. Kuigi erinevad sõnad ei ole otseselt väärad, palume mitmetimõistetavuse vältimiseks kaaluda võimalikult suures osas direktiivi sõnastuse kasutamist.

2. Euroopa Parlamendi ja nõukogu direktiivi (EL) 2022/2555 artikkel 14 kohaselt luuakse koostöörühm, et toetada ja hõlbustada strateegilist koostööd ja teabevahetust liikmesriikide vahel. Planeeritava § 5 lõike 2 kohaselt osalevad Justiits- ja Digiministeerium ning Riigi Infosüsteemi Amet koostöörühma tegevustes vastavalt koostöörühma ülesannetele. Koostöörühma ülesanne on tegeleda muuhulgas tarneahelakindluse, seonduvate õigusaktide, küberturvalisuse poliitikate, nõrkuste koordineeritud avaldamise ja teiste sarnaste tegevustega.

Selleks, et omada loetletud ülesannete täitmisel terviklikku ohupilti, on Justiits- ja Digiministeeriumil ning Riigi Infosüsteemi Ametil vaja sisendit julgeolekuasutustelt.
Vajadus julgeolekuasutuste kaasamise järele tuleneb ka „Küberturvalisuse strateegia 2024-2030“ rakenduskavast, kus muude tegevuste hulgas on välja toodud ootus, et elutähtsad taristu ja teenused on varustatud riikliku julgeoleku aspektist lähtuvate turvameetmetega, mis võimaldavad vastu seista nii praegustele kui ka tulevastele ohtudele.

Palume luua koostöömehhanism, mille kaudu on julgeolekuasutustel võimalus anda vajadusel sisendit Justiits- ja Digiministeeriumile ning Riigi Infosüsteemi Ametile. Sellise koostöömehhanismi reguleerimine seaduse tasandil ei ole meie hinnangul vajalik.

3. Planeeritava § 133 lõike 1 kohaselt võib Vabariigi Valitsus määrusega kohustada teenuse osutajat järgima käesoleva seaduse §-s 7 sätestatud nõuetele vastavuse tõenduseks teatavate IKT-toodete, IKT-teenuste ja IKT-protsesside kasutamist, mis on sertifitseeritud Euroopa Parlamendi ja nõukogu määruse (EL) 2019/881 artikli 49 kohaselt vastu võetud Euroopa küberturvalisuse sertifitseerimise kava alusel ning mis on:
1) töötatud välja teenuse osutaja poolt;

või
2) hangitud kolmandalt isikult.
Palume kaaluda võrgu- või infosüsteemi turvalisust tagavate IKT-toodete, IKT-teenuste ja IKTprotsesside puhul elutähtsa teenuse osutajatele kohustuse kehtestamist kasutada
sertifitseeritud või turbehinnatud tooteid.

Julgeoleku laiapindset käsitlust silmas pidades on ülimalt oluline, et elutähtsa teenuse osutajad lähtuvad oma võrgu- või infosüsteemide kaitsel sarnastest põhimõtetest nagu salastatud teabe töötlemiseks kasutatavate võrgu- ja infosüsteemide valdajad. Vähemalt need võrgu- või infosüsteemi komponendid, mille eesmärk on tagada teabe salajasus ja sidekanali turvalisus, peavad olema kaitstud toodetega, mis on saanud heakskiidu või mille turvalisust on hinnatud.

Ettepanekut toetab ka Eesti võetud kohustus Põhja-Atlandi Lepingu Organisatsiooni (NATO) Washingtoni tippkohtumiselt, mille deklaratsioonis on öeldud järgmist: "Lubame teha jätkuvaid jõupingutusi, et tugevdada riigi vastupanuvõimet, integreerides tsiviilplaneerimise riigi ja kollektiivkaitse planeerimisse rahu, kriisi ja konflikti ajal. Me jätkame oma vastupanuvõime suurendamist, suurendades alliansi kollektiivset teadlikkust, valmisolekut ja suutlikkust kõigis ohtudes ja kõikides valdkondades, et tegeleda kasvavate strateegiliste ohtudega, sealhulgas meie demokraatlike süsteemide, kriitilise infrastruktuuri ja tarneahelate vastu. Kasutame kõiki võimalusi pahatahtlike tegevuste avastamiseks, nende eest kaitsmiseks ja neile reageerimiseks.".

Lugupidamisega

(allkirjastatud digitaalselt)

Hanno Pevkur
minister

Johannes Randi
Johannes.Randi@kaitseministeerium.ee