EESTI
INFOTEHNOLOOGIA JA
TELEKOMMUNIKATSIOONI
LIIT

ITL-i arvamus NIS2 rakendusmääruse ettepaneku kohta

24.07.2024

Eesti Infotehnoloogia ja Telekommunikatsiooni Liit (ITL) esitab käesolevaga arvamuse Euroopa Komisjoni ettepaneku kohta võtta vastu direktiivi (EU) 2022/2555 (NIS2) rakendusakt, mis sätestab küberturvalisuse riskihalduse tehnilised ja metoodilised nõuded ning täpsustab, millal on intsident oluline seoses domeeninimede süsteemi teenuse osutajate, tippdomeeninimede registrite, pilvandmetöötlusteenuse osutajate, andmekeskusteenuse osutajate, sisulevivõrgu pakkujate, hallatud teenuse osutajate, turbetarnijate, internetipõhiste kauplemiskohtade, internetipõhiste otsingumootorite ning sotsiaalvõrguteenuse platvormide ja usaldusteenuse pakkujatega (edaspidi: „Ettepanek“).

ITL-i põhisõnumid:

1) Kuna juba täna kehtivad Ettepaneku skoobis olevatele ettevõtetele mitmed sektoriaalsed ja siseriiklikud standardid, siis tuleb tagada nendega kooskõla, mitte kehtestada uusi (topelt) nõudeid.
2) Intsidentide olulisuse kriteeriumid tuleb üle vaadata ning arvestada seejuures erinevate teenuste ja erinevate ettevõtetega, kuna raporteerimise mõttekuse ning efektiivsuse vaatest ei ole mõistlik igale intsidendile nii ühetaoliselt läheneda. Samuti tuleb tagada kooskõla olemasolevate toimepidevuse nõuetega.
3) Ettevõtted vajavad ülemineku aega, et valmistuda uute nõuete rakendamiseks, seda enam, et paljudes liikmesriikides ei ole NIS2 veel riigisisesesse õigusesse üle võetud. Lisaks palume Euroopa Komisjonil selgitada selle õigusakti õiguslikku staatust ja mõju siseriiklikele õigusaktidele.

Põhjalikumad selgitused:

1. Nõuete kooskõla kehtivate standarditega

Ettepaneku lisa sätestab kohustuse täita väga mitmeid äärmiselt detailseid tehnilisi ja metoodilisi nõudeid, mille eesmärk on kaitsta võrgu- ja infosüsteeme ning nende süsteemide füüsilist keskkonda intsidentide eest. Praktikas tähendab see, et ettevõtjad peavad hakkama järgima järjekordset standardit, mis tõstab oluliselt nende vastavuskoormust ja -kulusid. Samas on osadel teenuse osutajatel juba olemas sektoriaalsed standardid (näiteks usaldusteenuste osas ETSI EN 319 401 ja pilveteenuste osas CEN/TS 18026). Samuti on riikidel oma arusaamised, milline alusstandard sobib, et näidata vastavust NIS2-le. Näiteks Eestis on küberturvalisuse seaduses nimetatud teenuse osutajatel kohustus järgida Eesti infoturbe standardit (sellega on võrdsustatud ka ISO/IEC 27001 vastavussertifikaadi olemasolu).

Meie analüüs näitab, et paljud Ettepanekus sätestatud nõuded on võetud standardist ISO/IEC 27002 ja see tõstatab küsimuse, kas nõuete täiendav kehtestamine on tõesti vajalik ja kas see tõstab tegelikult kohaldamisalas olevate teenuste turvataset.

ESTONIAN ASSOCIATION OF INFORMATION
TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee

Oleme seisukohal, et teenusepakkuja vastavuse tõendamiseks on mõistlik kasutada olemasolevaid üldisi või valdkondlikke infoturbe standardeid (kui need on olemas). Seetõttu teeme ettepaneku analüüsida olemasolevate standardite nõuete vastavust NIS2-s sätestatule ning võtta eesmärgiks jõuda harmoniseeritud lähenemisele ja vältida sellega rakendusaktiga teenuseosutajatele järjekordse vastavusülesande panemist. Kui täiendavate nõuete kehtestamine osutub vältimatuks, siis on vajalik teha koostööd standardiorganisatsioonidega ja täiendada vastavalt olemasolevaid standardeid.

2. Intsidendi olulisuse kriteeriumid

Ettepaneku artiklis 3 toodud olulise intsidendi kriteeriumid on väga laiad ning vajavad ülevaatamist. Need on mõeldud väga erinevatele teenustele ja ettevõtetele, millele meie hinnangul ei saa niivõrd ühetaoliselt läheneda.

ITL ei saa nõustuda Ettepaneku lähenemisega, et mitmete erinevate teenuste puhul just 10 minutit katkestust tähendab olulist intsidenti. Leiame, et seejuures tuleb arvestada ka teenuse kriitilisust nii konteksti kui ka kasutajate hulga mõttes, mitte ainult aega. Teenuse katkestuse puhul ei näita olulisust ainult katkestuse pikkus, vaid ikkagi katkestuse mõju kasutajatele.

Näiteks usaldusteenuste puhul kui kvalifitseeritud elektrooniliste allkirjade sertifikaate ei väljastata 10 minuti jooksul (eeldusel, et väljastamine toimub tavapäraselt tööpäevadel ja tavapärasel tööajal), ei oleks 10 minuti mõju kriitiline. Samas on sertifikaadi kehtivusinfo (OCSP, CRL) edastamise katkestamisel kriitiline mõju nende sertifikaatide kasutamisele (kas sertifikaadid kehtivad elektroonilise allkirjastamise hetkel).

Sama kehtib mõjutatud kasutajate hulgas osas. Väiksema teenuse puhul ei pruugi Ettepanekus sätestatud lävend tuua kaasa kriitilist mõju. Seega arvestama peab ka mõju teenuse kättesaadavusele.

ITL-i ettepanek on raporteerimise mõttekuse ja efektiivsuse huvides Ettepaneku artiklid 3-14 üle vaadata ning arvestada rohkem erinevate teenuste, nende mõjude ja ulatustega. Intsidentide olulisuse määratlemisel tuleb meie hinnangul lähtuda olemasolevatest NIS2 direktiivis ning muudes õigusaktides kasutatud mõistetest ja olemasolevatest toimepidevuse nõuetest ning tagada kooskõla, mitte tekitada uut loogikat ja lisakohustusi.

3. Rakendamisaeg ja seos siseriiklike õigusaktidega

Ettepaneku väljatöötamine võttis Euroopa Komisjonil aega planeeritust kauem (rakendusakti kavand lubati avaldada käesoleva aasta esimeses kvartalis) ning nüüd plaanitakse rakendusakt jõustada ikkagi algse ajakava kohaselt ehk 18. oktoobril 2024. See ei ole kooskõlas hea õigusloome põhimõtetega. Ettevõtted vajavad aega, et valmistuda ette nõuete täitmiseks.

Lisaks on meile teadaolevalt mitmed riigid teatanud, et ei jõua NIS2 direktiivi riigisisesesse õigusesse tähtaegselt üle võtta, mis tähendab, et nendes riikides tegutsevate ettevõtete osas ei jõustu NIS2-s tulenevad kohustused käesoleva aasta oktoobris. Tekib küsimus, kuidas rakendusakt saab sel juhul jõustuda.

EESTI
INFOTEHNOLOOGIA JA
TELEKOMMUNIKATSIOONI
LIIT

ITL-i ettepanek on sätestada Ettepanekus ülemineku periood 2 aastat ehk mitte rakendada uusi nõudeid juba vähem kui kolme kuu pärast.

Lisaks teeme ettepaneku selgitada Ettepaneku preambulas selle õigusakti õiguslikku staatust, kuna hetkel jääb see ebaselgeks. NIS2 on direktiiv, mille liikmesriigid peavad üle võtma oma siseriiklikku õigusesse. Käesoleva Ettepaneku näol on aga tegemist otsekohalduva kohustusliku õigusaktiga. See tekitab küsimusi, mis saab sellega vastuolus olevatest siseriiklikest nõuetest. Seda enam, et liikmesriikidel, kes on juba NIS2 üle võtnud või sellega lähiajal valmis saamas, pole võimalik Ettepanekus sätestatut arvestada.

Kontakt:
Keilin Tammepärg
Jurist
Eesti Infotehnoloogia ja Telekommunikatsiooni Liit
Tel +3725060113
e-post keilin.tammeparg@itl.ee