IETEIKUMI

KOMISIJAS IETEIKUMS (ES) 2019/553

(2019. gada 3. aprīlis)

par kiberdrošību enerģētikas nozarē

(izziņots ar dokumenta numuru C(2019) 2400)

EIROPAS KOMISIJA,

ņemot vērā Līgumu par Eiropas Savienības darbību un jo īpaši tā 292. pantu,

tā kā:

(1) Eiropas enerģētikas nozarē, vienlaikus nodrošinot energoapgādes drošību un konkurētspēju, tiek īstenotas būtiskas pārmaiņas saistībā ar pāreju uz dekarbonizētu ekonomiku. Līdz ar šo enerģētikas pārkārtošanu un ar to saistīto atjaunojamo energoresursu elektroenerģijas ražošanas decentralizāciju, tehnoloģiju attīstību, nozaru sasaisti un digitalizāciju Eiropas elektrotīkls tiek pārveidots par "viedu energotīklu". Taču tajā pašā laikā tas rada arī jaunus riskus, jo digitalizācija arvien vairāk pakļauj enerģētikas sistēmu kiberuzbrukumiem un incidentiem, kas var apdraudēt energoapgādes drošību.

(2) Pieņemot visus astoņus tiesību aktu priekšlikumus ([1]), kas veido paketi "Tīru enerģiju ikvienam Eiropā", kur galvenais jautājums ir Enerģētikas savienības pārvaldība, tiek sagatavota labvēlīga augsne enerģētikas nozares digitālajai pārveidei. Tāpat ar šiem tiesību aktiem tiek atzīta kiberdrošības nozīme enerģētikas nozarē. Konkrēti, regulas par elektroenerģijas iekšējo tirgu pārstrādātajā redakcijā ([2]) ir paredzēts pieņemt elektroenerģijas tehniskos noteikumus, piemēram, tīkla kodeksu par nozaru noteikumiem attiecībā uz pārrobežu elektroenerģijas plūsmu kiberdrošības aspektiem, par kopīgām minimālajām prasībām, plānošanu, uzraudzību, ziņošanu un krīžu pārvarēšanu. Regulā par elektroenerģijas nozares riskgatavību ([3]) pamatā izmantota tā pati pieeja, kas Gāzes piegādes drošības regulā ([4]), proti, uzsvērta vajadzība pienācīgi novērtēt visus riskus, tostarp tos, kas saistīti ar kiberdrošību, un ierosināt tādu pasākumu pieņemšanu, ar kuriem varētu novērst un mazināt šos apzinātos riskus.

(3) Kad Komisija 2013. gadā pieņēma ES kiberdrošības stratēģiju ([5]), tā par prioritāti noteica Savienības kibernoturības stiprināšanu. Par vienu no galvenajiem ar šo stratēģiju sasniedzamajiem rezultātiem tika noteikta Tīklu un informācijas drošības direktīva ([6]) (turpmāk "TID direktīva"), kas tika pieņemta 2016. gada jūlijā. TID direktīva, kas bija pirmais horizontālais ES tiesību akts kiberdrošības jomā, paaugstina vispārējo kiberdrošības līmeni Savienībā, attīstot valstu kiberdrošības spējas, paplašinot ES līmeņa sadarbību un ieviešot drošības un incidentu ziņošanas pienākumus, kuri jāievēro uzņēmumiem – tā sauktajiem pamatpakalpojumu sniedzējiem. Ziņošana par incidentiem ir obligāta galvenajās nozarēs, tostarp enerģētikas nozarē.

([1]) Eiropas Parlamenta un Padomes 2018. gada 11. decembra Direktīva (ES) 2018/2001 par no atjaunojamajiem energoresursiem iegūtas enerģijas izmantošanas veicināšanu (OV L 328, 21.12.2018., 82. lpp.); Eiropas Parlamenta un Padomes 2018. gada 11. decembra Direktīva (ES) 2018/2002, ar ko groza Direktīvu 2012/27/ES par energoefektivitāti (OV L 328, 21.12.2018., 210. lpp.); Eiropas Parlamenta un Padomes 2018. gada 11. decembra Regula (ES) 2018/1999 par enerģētikas savienības un rīcības klimata politikas jomā pārvaldību un ar ko groza Eiropas Parlamenta un Padomes Regulas (EK) Nr. 663/2009 un (EK) Nr. 715/2009, Eiropas Parlamenta un Padomes Direktīvas 94/22/EK, 98/70/EK, 2009/31/EK, 2009/73/EK, 2010/31/ES, 2012/27/ES un 2013/30/ES, Padomes Direktīvas 2009/119/EK un (ES) 2015/652 un atceļ Eiropas Parlamenta un Padomes Regulu (ES) Nr. 525/2013 (OV L 328, 21.12.2018., 1. lpp.); Eiropas Parlamenta un Padomes 2018. gada 30. maija Direktīva (ES) 2018/844, ar ko groza Direktīvu 2010/31/ES par ēku energoefektivitāti un Direktīvu 2012/27/ES par energoefektivitāti (OV L 156, 19.6.2018, 75. lpp.). Eiropas Parlaments 2019. gada marta plenārsēdē apstiprināja ar Padomi panākto politisko vienošanos par priekšlikumiem par elektroenerģijas tirgus modeli (Riskgatavības regula; regula, ar ko izveido Energoregulatoru sadarbības aģentūru (*ACER*), Elektroenerģijas direktīva un Elektroenerģijas regula. Plānots, ka Padome oficiāli tos pieņems aprīlī, drīz pēc tam sekos tiesību akta publicēšana *Oficiālajā Vēstnesī*.

([2]) COM(2016) 861 final.

([3]) COM(2016) 862 final.

([4]) Eiropas Parlamenta un Padomes 2017. gada 25. oktobra Regula (ES) 2017/1938 par gāzes piegādes drošības aizsardzības pasākumiem un ar ko atceļ Regulu (ES) Nr. 994/2010 (OV L 280, 28.10.2017., 1. lpp.).

([5]) JOIN(2013) 1.

([6]) Eiropas Parlamenta un Padomes 2016. gada 6. jūlija Direktīva (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā (OV L 194, 19.7.2016., 1. lpp.).

(4) Īstenojot sagatavotības pasākumus kiberdrošības jomā, attiecīgajām ieinteresētajām personām, tostarp pamatpakalpojumu sniedzējiem enerģētikas nozarē, kuri noteikti saskaņā ar TID direktīvu, būtu jāņem vērā horizontālie norādījumi, ko izdevusi ar TID direktīvas 11. pantu izveidotā TID Sadarbības grupa. Šī sadarbības grupa, kuru veido dalībvalstu pārstāvji, Eiropas Savienības Kiberdrošības aģentūra (*ENISA*) un Komisija, ir pieņēmusi norādījumus par drošības pasākumiem un incidentu paziņošanu. 2018. gada jūnijā minētā grupa izveidoja specializētu vienību darbam enerģētikas jomā.

(5) 2017. gada kopīgajā paziņojumā par kiberdrošību ([7]) atzīts, cik svarīgi ir sagatavot konkrētai nozarei specifiskus apsvērumus un prasības ES līmenī, tostarp enerģētikas nozarē. Pēdējo gadu laikā Savienībā par kiberdrošību un iespējamu politikas ietekmēšanu ir notikušas visaptverošas diskusijas. Tagad ir pieaugusi izpratne par to, ka atsevišķas ekonomikas nozares saskaras ar īpašām kiberdrošības problēmām un ka tāpēc tajās jāveido pašām sava specifiska pieeja plašākā kiberdrošības vispārējo stratēģiju kontekstā.

(6) Informācijas apmaiņa un uzticēšanās ir galvenie kiberdrošības elementi. Komisijas mērķis ir palielināt informācijas apmaiņu starp attiecīgajām ieinteresētajām personām, tādēļ tā ir organizējusi īpašus pasākumus, piemēram, 2017. gada martā Romā augsta līmeņa apaļā galda sarunas par kiberdrošību, bet 2018. gada oktobrī Briselē – augsta līmeņa konferenci par kiberdrošību enerģētikas jomā. Komisija arī vēlas uzlabot sadarbību starp attiecīgajām ieinteresētajām personām un specializētajām struktūrām, piemēram, Eiropas Enerģētikas informācijas apmaiņas un analīzes centru.

(7) Regula par *ENISA* jeb ES Kiberdrošības aģentūru un par informācijas un komunikācijas tehnoloģiju kiberdrošības sertifikāciju ("Kiberdrošības akta regula" ([8])) stiprinās ES Kiberdrošības aģentūras pilnvaras, lai tādējādi labāk atbalstītu dalībvalstis draudu un uzbrukumu novēršanā kiberdrošības jomā. Tā arī izveido ES kiberdrošības produktu, procesu un pakalpojumu sertifikācijas regulējumu, kas būs izmantojams visā Savienībā un jo īpaši enerģētikas nozarē.

(8) Komisija ir nākusi klajā ar ieteikumu ([9]), kurā tā risina jautājumu par kiberdrošības riskiem piektās paaudzes (5G) tīklu tehnoloģiju izmantošanā, proti, sniedz norādes par atbilstīgiem riska analīzes un pārvaldības pasākumiem valsts līmenī, par koordinētas riska analīzes ieviešanu Eiropas līmenī un par tāda procesa izveidi, kas vajadzīgs, lai izstrādātu vienotu labāko riska pārvaldības pasākumu kopumu. Pēc tam, kad būs izvērsti 5G tīkli, uz to pamata tiks veidots plašs klāsts pakalpojumu, kas vajadzīgi, lai nodrošinātu iekšējā tirgus darbību un tādas sabiedriski un ekonomiski svarīgas funkcijas kā energoapgāde.

(9) Šajā ieteikumā būtu jāsniedz dalībvalstīm un attiecīgajām ieinteresētajām personām, jo īpaši tīklu operatoriem un tehnoloģiju piegādātājiem, neizsmeļoši norādījumi par to, kā panākt augstāku kiberdrošības līmeni enerģētikas nozarē, ņemot vērā enerģētikas nozarē noteiktās īpašās reāllaika prasības, ķēdes reakciju, kā arī novecojušo un modernāko tehnoloģiju kombināciju. Šo norādījumu mērķis ir palīdzēt ieinteresētajām personām starptautiski atzītu kiberdrošības standartu īstenošanā ņemt vērā enerģētikas nozares īpašās prasības ([10]).

(10) Komisija plāno regulāri pārskatīt šo ieteikumu, pamatojoties uz visā Savienībā panākto progresu un apspriežoties ar dalībvalstīm un attiecīgajām ieinteresētajām personām. Komisija turpinās savus kiberdrošības stiprināšanas centienus enerģētikas nozarē, jo īpaši ar TID Sadarbības grupas starpniecību, kas nodrošina stratēģisku sadarbību un informācijas apmaiņu starp dalībvalstīm kiberdrošības jomā,

IR PIEŅĒMUSI ŠO IETEIKUMU.

PRIEKŠMETS

1. Šajā ieteikumā ir izklāstīti galvenie jautājumi, kas saistīti ar kiberdrošību enerģētikas nozarē, proti, par reāllaika prasībām, ķēdes reakciju, kā arī novecojušo un modernāko tehnoloģiju kombināciju, un noteikts, kas jādara, lai enerģētikas nozarē īstenotu sagatavotības pasākumus attiecībā uz kiberdrošību.

([7]) JOIN(2017) 450.

([8]) Eiropas Parlaments Kiberdrošības aktu pieņēma 2019. gada martā. Plānots, ka Padome oficiāli to pieņems aprīlī, drīz pēc tam tiesību akts tiks publicēts *Oficiālajā Vēstnesī*.

([9]) COM(2019) 2335.

([10]) Starptautiskā Standartizācijas organizācija ir publicējusi dažādus kiberdrošības standartus (ISO/IEC 27000: Informācijas tehnoloģijas) un riska pārvaldības standartus (ISO/IEC31000: Riska pārvaldības īstenošana). 2017. gada oktobrī ISO/IEC 27000 standartu sērijā tika izdots īpašs standarts enerģētikas nozarē (ISO/IEC 27019: Informācijas drošības kontrole enerģētikas komunālo pakalpojumu nozarē).

2. Piemērojot šo ieteikumu, dalībvalstīm būtu jāmudina attiecīgās ieinteresētās personas vairot zināšanas un izkopt prasmes, kas saistītas ar kiberdrošību enerģētikas nozarē. Vajadzības gadījumā dalībvalstīm šie apsvērumi būtu jāiekļauj arī valsts kiberdrošības regulējumā, jo īpaši stratēģijās, tiesību aktos un citos administratīvos noteikumos.

ENERGOINFRASTRUKTŪRAS KOMPONENTU REĀLLAIKA PRASĪBAS

3. Dalībvalstīm būtu jānodrošina, ka attiecīgās ieinteresētās personas, jo īpaši energotīklu operatori un tehnoloģiju piegādātāji, sevišķi TID direktīvā definētie pamatpakalpojumu sniedzēji, īsteno attiecīgos sagatavotības pasākumus kiberdrošības jomā, kuri saistīti ar reāllaika prasībām enerģētikas nozarē. Dažiem enerģētikas sistēmas elementiem jādarbojas "reāllaikā", t. i., tiem jāspēj reaģēt uz komandām dažās milisekundēs, un tas laika trūkuma dēļ apgrūtina vai pat padara neiespējamu kiberdrošības pasākumu ieviešanu.

4. Konkrēti, energotīklu operatoriem būtu:

   a) jāpiemēro jaunākie drošības standarti jaunām iekārtām, kad tas ir atbilstoši, un jāapsver papildu fiziskās drošības pasākumi, ja veco iekārtu uzstādīto bāzi ar kiberdrošības mehānismiem nevar pietiekami aizsargāt;

   b) tiklīdz attiecīgie produkti kļūst komerciāli pieejami, jāievieš starptautiski kiberdrošības standarti un atbilstīgi īpaši tehniskie standarti attiecībā uz drošu saziņu reāllaikā;

   c) jāņem vērā reāllaika ierobežojumi vispārējā drošības koncepcijā attiecībā uz aktīviem, jo īpaši aktīvu klasifikāciju;

   d) jāņem vērā privātā īpašumā esošie sakaru tīkli, lai nodrošinātu tādu pakalpojumu kvalitātes līmeni, kāds jāpanāk reāllaika ierobežojumu dēļ; izmantojot publiskos sakaru tīklus, operatoriem būtu jāapsver iespēja nodrošināt īpašu joslas platumu, latentuma prasības un sakaru drošības pasākumi;

   e) vispārējā sistēma jāsadala loģiskās zonās, un katrā zonā jānosaka laika un procesa ierobežojumi, lai varētu piemērot atbilstīgus kiberdrošības pasākumus, vai jāapsver alternatīvas aizsardzības metodes.

5. Ja iespējams, energotīklu operatoriem arī būtu:

   a) jāizvēlas drošu sakaru protokols, ņemot vērā reāllaika prasības, piemēram, starp iekārtu un tās vadības sistēmām (energovadības sistēma jeb *EMS*/sadales vadības sistēma jeb *DMS*);

   b) jāievieš tāds piemērots autentifikācijas mehānisms mašīnas-mašīnas sakariem, kas ļautu izpildīt reāllaika prasības.

ĶĒDES REAKCIJA

6. Dalībvalstīm būtu jānodrošina, ka attiecīgās ieinteresētās personas, jo īpaši energotīklu operatori un tehnoloģiju piegādātāji, sevišķi TID direktīvā definētie pamatpakalpojumu sniedzēji, īsteno attiecīgos sagatavotības pasākumus kiberdrošības jomā, kuri saistīti ar ķēdes reakciju enerģētikas nozarē. Elektrotīkli un gāzes cauruļvadi ir savstarpēji cieši saistīti visā Eiropā, tādēļ kiberuzbrukums, kas rada pārtraukumu vai traucējumus kādā no energosistēmas daļām, var izraisīt plašu ķēdes reakciju citās šīs sistēmas daļās.

7. Piemērojot šo ieteikumu, dalībvalstīm būtu jānovērtē elektroenerģijas ražošanas un elastīgu pieprasījumu sistēmu, pārvades un sadales apakšstaciju un līniju savstarpējā atkarība un kritiskums, kā arī saistītās ieinteresētās personas (tostarp pārrobežu situācijās), ko skāris sekmīgi īstenots kiberuzbrukums vai kiberincidents. Dalībvalstīm būtu arī jānodrošina, ka energotīkla operatoriem ir sakaru sistēma, kas izmantojama saziņai ar visām galvenajām ieinteresētajām personām, lai informētu par agrīnām apdraudējuma pazīmēm un sadarbotos krīžu pārvarēšanas jomā. Būtu jāizveido un jāievieš strukturēti sakaru kanāli un saskaņoti formāti, kas ļautu apmainīties ar sensitīvu informāciju ar visām attiecīgajām ieinteresētajām personām, datordrošības incidentu reaģēšanas vienībām un attiecīgajām iestādēm.

8. Konkrēti, energotīklu operatoriem būtu:

   a) jānodrošina, ka jaunajām ierīcēm, tostarp lietu interneta ierīcēm, ir objekta kritiskuma pakāpei atbilstīgs kiberdrošības līmenis un tāds arī tiek saglabāts;

   b) darbības nepārtrauktības plānu izstrādē un periodiskā pārskatīšanā pienācīgi jāņem vērā kiberfiziskā ietekme;

c) jāizstrādā projektēšanas kritēriji un arhitektūra noturīgai energosistēmai, ko varētu sasniegt:

— uz vietas ieviešot padziļinātus aizsardzības pasākumus, kas pielāgoti objekta nozīmīguma pakāpei,

— apzinot kritiskos mezglus gan attiecībā uz elektroenerģijas ražošanas jaudu, gan ietekmi uz patērētājiem; tīkla kritiskās funkcijas būtu jāizstrādā tā, lai, ņemot vērā redundanci, noturību pret fāzes svārstībām un aizsardzību pret pakāpenisku jaudas atslēgšanu, mazinātu ķēdes reakcijas rašanās risku,

— sadarbojoties ar citiem attiecīgajiem operatoriem un ar tehnoloģiju piegādātājiem, lai ar attiecīgiem pasākumiem un pakalpojumiem novērstu ķēdes reakciju,

— projektējot un veidojot sakaru un kontroles tīklus tādā veidā, lai fiziskas un loģiskas atteices ietekmētu tikai ierobežotu tīklu daļu un būtu nodrošināti pienācīgi un ātri ietekmes mazināšanas pasākumi.

NOVECOJUŠĀS UN MODERNĀKĀS TEHNOLOĢIJAS

9. Dalībvalstīm būtu jānodrošina, ka attiecīgās ieinteresētās personas, jo īpaši energotīklu operatori un tehnoloģiju piegādātāji, sevišķi TID direktīvā definētie pamatpakalpojumu sniedzēji, īsteno attiecīgos sagatavotības pasākumus kiberdrošības jomā, kuri saistīti ar novecojušo un modernāko tehnoloģiju kombināciju enerģētikas nozarē. Pašlaik energosistēmā paralēli tiek izmantoti divi dažādi tehnoloģiju veidi: vecākas tehnoloģijas, kuru ekspluatācijas termiņš ir 30–60 gadi un kuras izstrādātas pirms kiberdrošības jautājumu aktualizēšanās, un modernās iekārtas, kas veidotas atbilstīgi mūsdienu digitalizācijas un viedierīču prasībām.

10. Piemērojot šo ieteikumu, dalībvalstīm būtu jāmudina energotīklu operatori un tehnoloģiju piegādātāji, kad vien iespējams, ievērot attiecīgos starptautiski pieņemtos standartus attiecībā uz kiberdrošību. Tajā pašā laikā ieinteresētajām personām un klientiem, ierīces pieslēdzot tīklam, būtu jāizmanto kiberdrošības principiem atbilstoša pieeja.

11. Tehnoloģiju piegādātājiem būtu bez maksas jānodrošina pārbaudīti drošības risinājumi novecojušajām vai modernajām tehnoloģijām, tiklīdz attiecīgā drošības problēma parādās.

12. Konkrēti, energotīklu operatoriem būtu:

a) jāanalizē riski, ko rada novecojušo tehnoloģiju un lietu interneta koncepcijas sasaiste, un jāapzinās iekšējās un ārējās saskarnes un to vājās vietas;

b) jāveic piemēroti pasākumi tādu ļaunprātīgu uzbrukumu atvairīšanai, kuru veikšanai tiek izmantots liels skaits ļaunprātīgi pārņemtu patērētāju ierīču vai lietojumu;

c) jāizveido automatizēta uzraudzības un analīzes spēja ar drošību saistītiem risinājumiem vidē, kur tiek izmantotas gan novecojušās, gan lietu interneta tehnoloģijas, piemēram, saistībā ar neveiksmīgiem pieteikšanās mēģinājumiem, durvju atvēršanas signalizācijām vai citām situācijām;

d) regulāri jāveic īpaša kiberdrošības riska analīze attiecībā uz visām novecojušajām iekārtām, jo īpaši situācijās, kad tiek apvienotas vecās un jaunās tehnoloģijas; tā kā novecojušās iekārtas bieži nozīmē ļoti lielu aktīvu skaitu, riska analīzi var veikt pa aktīvu klasēm;

e) vajadzības gadījumā atbilstoši jaunākajām versijām jāatjaunina novecojušo tehnoloģiju un lietu interneta sistēmu programmatūra un aparatūra; šajā procesā energotīklu operatoriem būtu jāapsver papildu pasākumi, piemēram, jānodala sistēmas vai papildus jāizveido ārējās drošības barjeras, kad meklēšana vai atjaunināšana būtu piemērota, bet nav iespējama, piemēram, neatbalstītiem produktiem;

f) konkursu paziņojumu sagatavošanā jāņem vērā kiberdrošības aspekti, proti, jāpieprasa informācija par drošības elementiem, par atbilstību spēkā esošajiem kiberdrošības standartiem, pastāvīgi jāsniedz brīdināšanas, ielāpošanas un apdraudējumu samazināšanas priekšlikumi, ja ir konstatētas vājās vietas, kā arī jāprecizē pārdevēja atbildība kiberuzbrukumu vai incidentu gadījumā;

g) jāsadarbojas ar tehnoloģiju piegādātājiem, lai aizstātu novecojušās sistēmas, ja vien tas ir lietderīgi drošības apsvērumu dēļ, bet jāņem vērā sistēmas kritiski svarīgās funkcijas.

UZRAUDZĪBA

13. Dalībvalstīm 12 mēnešu laikā pēc šā ieteikuma pieņemšanas un pēc tam reizi divos gados ar TID sadarbības grupas starpniecību būtu jāsniedz Komisijai detalizēta informācija par šā ieteikuma īstenošanas gaitu.

PĀRSKATĪŠANA

14. Pamatojoties uz dalībvalstu iesniegto informāciju, Komisija pārskatīs šā ieteikuma īstenošanu un noskaidros, vai pēc apspriešanās ar dalībvalstīm un attiecīgajām ieinteresētajām personām ir vajadzīgi turpmāki pasākumi.

ADRESĀTI

15. Šis ieteikums ir adresēts dalībvalstīm.

Briselē, 2019. gada 3. aprīlī

Komisijas vārdā –

Komisijas loceklis

Miguel ARIAS CAÑETE