REKOMENDACIJOS

KOMISIJOS REKOMENDACIJA (ES) 2019/553

2019 m. balandžio 3 d.

dėl energetikos sektoriaus kibernetinio saugumo

(pranešta dokumentu Nr. C(2019) 2400)

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo, ypač į jos 292 straipsnį,

kadangi:

(1) vyksta svarbus Europos energetikos sektoriaus perėjimas prie mažiau nuo iškastinio kuro priklausančios ekonomikos, kartu užtikrinant energijos tiekimo saugumą ir konkurencingumą. Vykstant tai energetikos pertvarkai ir susijusiam energijos gamybos iš atsinaujinančiųjų šaltinių decentralizavimui, dėl technologinės pažangos, sektorių susiejimo ir skaitmeninimo Europos elektros tinklas virsta pažangiuoju tinklu. Kartu šis procesas kelia ir naujų grėsmių, nes dėl skaitmeninimo energetikos sistema tampa vis labiau atvira kibernetiniams išpuoliams ir incidentams, galintiems pastatyti energijos tiekimo saugumą į pavojų;

(2) priėmus visus aštuonis dokumentų rinkinio „Švari energija visiems europiečiams“ pasiūlymus dėl teisės aktų ([1]), iš kurių svarbiausias – energetikos sąjungos valdymo teisės aktas, suteikiama galimybė užtikrinti palankias sąlygas energetikos sektoriaus skaitmeninei transformacijai. Be to, juo pripažįstama kibernetinio saugumo svarba energetikos sektoriui. Visų pirma, nauja Reglamento dėl elektros energijos vidaus rinkos ([2]) redakcija numatoma priimti elektros energijos technines taisykles, kaip antai tinklo kodeksą dėl tarpvalstybinių elektros energijos srautų kibernetinio saugumo aspektams taikomų sektoriaus taisyklių, dėl bendrų būtinųjų reikalavimų, planavimo, stebėsenos, informacijos teikimo ir krizių valdymo. Reglamente dėl pasirengimo valdyti riziką elektros energijos sektoriuje ([3]) iš esmės vadovaujamasi tuo pačiu požiūriu kaip ir Reglamente dėl dujų tiekimo saugumo ([4]), pabrėžiant poreikį tinkamai įvertinti visą riziką, įskaitant susijusią su kibernetiniu saugumu, ir siūlant priimti šios nustatytos rizikos prevencijos ir mažinimo priemones;

(3) 2013 m. priimtoje Europos Sąjungos kibernetinio saugumo strategijoje ([5]) Komisija prioritetą teikė Sąjungos kibernetinio atsparumo didinimui. Vienas iš pagrindinių strategijos įgyvendinimo rezultatų – 2016 m. liepos mėn. priimta Tinklų ir informacinių sistemų saugumo direktyva ([6]) (toliau – TIS direktyva). TIS direktyva, pirmuoju horizontaliuoju kibernetinio saugumo srities ES teisės aktu, Sąjungoje didinamas bendras kibernetinio saugumo lygis: plėtojami nacionaliniai kibernetinio saugumo gebėjimai ir didinamas ES lygmens bendradarbiavimas, o įmonėms (t. y. esminių paslaugų operatoriams) nustatoma informacijos apie saugumą ir incidentus teikimo prievolė. Teikti informaciją apie incidentus privaloma pagrindiniuose sektoriuose, įskaitant energetikos sektorių;

([1]) 2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos direktyva (ES) 2018/2001 dėl skatinimo naudoti atsinaujinančiųjų išteklių energiją (OL L 328, 2018 12 21, p. 82); 2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos direktyva (ES) 2018/2002, kuria iš dalies keičiama Direktyva 2012/27/ES dėl energijos vartojimo efektyvumo (OL L 328, 2018 12 21, p. 210); 2018 m. gruodžio 11 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1999 dėl energetikos sąjungos ir klimato politikos veiksmų valdymo, kuriuo iš dalies keičiami Europos Parlamento ir Tarybos reglamentai (EB) Nr. 663/2009 ir (EB) Nr. 715/2009, Europos Parlamento ir Tarybos direktyvos 94/22/EB, 98/70/EB, 2009/31/EB, 2009/73/EB, 2010/31/ES, 2012/27/ES ir 2013/30/ES, Tarybos direktyvos 2009/119/EB ir (ES) 2015/652 ir panaikinamas Europos Parlamento ir Tarybos reglamentas (ES) Nr. 525/2013 (OL L 328, 2018 12 21, p. 1); 2018 m. gegužės 30 d. Europos Parlamento ir Tarybos direktyva (ES) 2018/844, kuria iš dalies keičiama Direktyva 2010/31/ES dėl pastatų energinio naudingumo ir Direktyva 2012/27/ES dėl energijos vartojimo efektyvumo (OL L 156, 2018 6 19, p. 75). Europos Parlamentas patvirtino, kad per plenarinį posėdį 2019 m. kovo mėn. su Taryba pasiektas politinis susitarimas dėl pasiūlymų dėl elektros energijos rinkos modelio (Pasirengimo valdyti riziką reglamento, Energetikos reguliavimo institucijų bendradarbiavimo agentūros (ACER) reglamento), Elektros energijos direktyvos ir Elektros energijos reglamento. Numatoma, kad Taryba teisės aktus oficialiai priims balandžio mėn.; netrukus po to teisinis tekstas bus paskelbtas Oficialiajame leidinyje.

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

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

([4]) 2017 m. spalio 25 d. Europos Parlamento ir Tarybos reglamentas (ES) 2017/1938 dėl dujų tiekimo saugumo užtikrinimo priemonių, kuriuo panaikinamas Reglamentas (ES) Nr. 994/2010 (OL L 280, 2017 10 28, p. 1).

([5]) JOIN(2013) 1.

([6]) 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (OL L 194, 2016 7 19, p. 1).

(4) įgyvendindamos kibernetinio saugumo srities pasirengimo priemones atitinkamos suinteresuotosios šalys, įskaitant energetikos sektoriaus esminių paslaugų operatorius, kaip nustatyta TIS direktyva, turėtų atsižvelgti į TIS bendradarbiavimo grupės, įsteigtos TIS direktyvos 11 straipsniu, paskelbtas horizontaliąsias rekomendacijas. Bendradarbiavimo grupė, kurią sudaro valstybių narių, Europos Sąjungos kibernetinio saugumo agentūros (ENISA) ir Komisijos atstovai, yra priėmusi rekomendacinius dokumentus, susijusius su saugumo priemonėmis ir pranešimu apie incidentus. 2018 m. birželio mėn. ta grupė parengė specialią energetikos srities darbo procedūrą;

(5) 2017 m. bendrame komunikate dėl kibernetinio saugumo ([7]) pripažįstama sektoriams, įskaitant energetikos sektorių, aktualių argumentų ir ES lygmens reikalavimų svarba. Pastaraisiais metais Sąjungoje vyko išsamių diskusijų kibernetinio saugumo ir galimų politinių pasekmių temomis. Taigi šiuo metu tampa vis aiškiau, kad atskiri ekonomikos sektoriai susiduria su specifinėmis kibernetinio saugumo problemomis, todėl, atsižvelgdami į platesnį bendrųjų kibernetinio saugumo strategijų kontekstą, turi kurti specialius sektorinius metodus;

(6) pagrindiniai kibernetinio saugumo elementai – keitimasis informacija ir pasitikėjimas. Komisija siekia skatinti atitinkamų suinteresuotųjų šalių keitimąsi informacija, organizuodama specialius renginius, pavyzdžiui, 2017 m. kovo mėn. Romoje vykusią aukšto lygio apskritojo stalo diskusiją energetikos sektoriaus kibernetinio saugumo klausimais ir 2018 m. spalio mėn. Briuselyje surengtą aukšto lygio konferenciją energetikos sektoriaus kibernetinio saugumo klausimais. Be to, Komisija siekia skatinti atitinkamų suinteresuotųjų šalių ir specializuotų subjektų, kaip antai Europos keitimosi informacija ir jos analizės centro, bendradarbiavimą;

(7) ENISA (ES kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo reglamentu (Kibernetinio saugumo reglamentu) ([8]) bus padidinti ES kibernetinio saugumo agentūros įgaliojimai tinkamiau remti valstybes nares šalinant kibernetinio saugumo grėsmes ir reaguojant į išpuolius. Reglamentu taip pat nustatoma Europos kibernetinio saugumo sistema, skirta produktų, procesų ir paslaugų sertifikavimui, galiosiančiam visoje Sąjungoje ir ypač svarbiam energetikos sektoriui;

(8) Komisija pateikė rekomendaciją ([9]) dėl kibernetinio saugumo grėsmių, susijusių su 5-osios kartos (5G) tinklų technologijomis, kurioje išdėstė tinkamos nacionalinio lygmens rizikos analizės ir valdymo priemonių gaires, taip pat koordinuotos Europos rizikos analizės parengimo ir bendro geriausių rizikos valdymo priemonių sąvado sudarymo proceso gaires. Išplėtoti 5G tinklai taps įvairiausių paslaugų, svarbių vidaus rinkos veikimui ir esminių visuomeninių ir ekonominių funkcijų, kaip antai energetikos, vykdymui, centrine ašimi;

(9) šia rekomendacija valstybėms narėms ir atitinkamoms suinteresuotosioms šalims, visų pirma tinklų operatoriams ir technologijų tiekėjams, pateikiamos neišsamios aukštesnio lygio kibernetinio saugumo įgyvendinimo gairės, atsižvelgiant į specialius energetikos sektoriui nustatytus realiojo laiko reikalavimus, grandininį poveikį ir esamų bei moderniausių technologijų derinimą. Šiomis gairėmis siekiama suinteresuotosioms šalims padėti paisyti specialių energetikos sektoriaus reikalavimų įgyvendinant tarptautiniu mastu pripažintus kibernetinio saugumo standartus ([10]);

(10) konsultuodamasi su valstybėmis narėmis ir atitinkamomis suinteresuotosiomis šalimis, Komisija planuoja šią rekomendaciją reguliariai peržiūrėti atsižvelgdama į Sąjungoje padarytą pažangą. Komisija toliau dės pastangas siekdama didinti energetikos sektoriaus kibernetinį saugumą, visų pirma pasitelkdama TIS bendradarbiavimo grupę, užtikrinančią valstybių narių strateginį bendradarbiavimą ir keitimąsi informacija kibernetinio saugumo klausimais,

PRIĖMĖ ŠIĄ REKOMENDACIJĄ:

DALYKAS

1) Šioje rekomendacijoje nurodomos pagrindinės problemos, susijusios su energetikos sektoriaus kibernetiniu saugumu, konkrečiai, realiojo laiko reikalavimai, grandininis poveikis ir esamų bei moderniausių technologijų derinimas, ir nustatomi pagrindiniai veiksmai, reikalingi atitinkamoms kibernetinio saugumo pasirengimo priemonėms energetikos sektoriuje įgyvendinti.

([7]) JOIN(2017) 450.

([8]) Europos Parlamentas priėmė Kibernetinio saugumo teisės aktą 2019 m. kovo mėn. Numatoma, kad Taryba teisės aktus oficialiai priims balandžio mėn.; netrukus po to teisinis tekstas bus paskelbtas Oficialiajame leidinyje.

([9]) C(2019) 2335.

([10]) Tarptautinės standartizacijos organizacijos yra paskelbusios įvairių kibernetinio saugumo (ISO/IEC 27000: informacinės technologijos) ir rizikos valdymo (ISO/IEC31000: rizikos valdymo diegimas) standartų. 2017 m. spalio mėn. paskelbtas specialus energetikos sektoriui skirtas ISO/IEC 27000 serijos standartas (ISO/IEC 27019: energetikos komunalinių paslaugų sektoriaus informacinio saugumo kontrolės priemonės).

2) Taikydamos šią rekomendaciją valstybės narės turėtų skatinti atitinkamas suinteresuotąsias šalis kaupti žinias ir lavinti įgūdžius, susijusius su energetikos sektoriaus kibernetiniu saugumu. Atitinkamais atvejais valstybės narės šiuos argumentus turėtų įtraukti į savo nacionalines kibernetinio saugumo sistemas, visų pirma priimdamos strategijas, įstatymus ir kitus teisės aktus.

ENERGETIKOS INFRASTRUKTŪROS KOMPONENTAMS TAIKOMI REALIOJO LAIKO REIKALAVIMAI

3) Valstybės narės turėtų užtikrinti, kad atitinkamos suinteresuotosios šalys, konkrečiai energetikos tinklų operatoriai ir technologijų tiekėjai, o ypač TIS direktyva nustatyti esminių paslaugų operatoriai, energetikos sektoriuje diegtų atitinkamas kibernetinio saugumo pasirengimo priemones, susijusias su realiojo laiko reikalavimais. Kai kurie energetikos sistemos elementai turi dirbti realiuoju laiku, t. y. reaguoti į komandas per kelias milisekundes, todėl dėl laiko trūkumo kibernetinio saugumo priemones įdiegti yra sudėtinga ar net neįmanoma.

4) Visų pirma, energetikos tinklo operatoriai turėtų:

a) naujiems įrenginiams taikyti pačius naujausius saugumo standartus, jei tinka, ir apsvarstyti papildomas fizinio saugumo priemones, kai įrengtos senų įrengimų bazės kibernetinio saugumo mechanizmais pakankamai apsaugoti neįmanoma;

b) diegti tarptautinius kibernetinio saugumo standartus ir tinkamus specialius techninius standartus, skirtus saugiai komunikacijai realiuoju laiku, kai tik atitinkami produktai pasirodo prekyboje;

c) taikant bendrąją turto saugumo koncepciją, ypač klasifikuojant turtą, įvertinti realiojo laiko suvaržymus;

d) svarstyti galimybę naudoti privačius nuotolinės apsaugos sistemų tinklus, kad užtikrintų tokį paslaugų kokybės lygį, kokio reikia atsižvelgiant į realiojo laiko suvaržymus; viešuosius ryšių tinklus naudojantys operatoriai turėtų svarstyti galimybę užtikrinti specialios juostos paskyrimą, delsos reikalavimų laikymąsi ir ryšių saugumo priemonių taikymą;

e) suskirstyti bendrą sistemą į logines zonas ir kiekvienai zonai nustatyti laiko ir procesų suvaržymus, kad būtų galima taikyti tinkamas kibernetinio saugumo priemones arba svarstyti alternatyvius apsaugos metodus.

5) Jei įmanoma, energetikos tinklo operatoriai taip pat turėtų:

a) rinktis saugų ryšių protokolą, atsižvelgdami į realiojo laiko reikalavimus, taikomus, pavyzdžiui, įrenginių ir jų valdymo sistemų (energijos naudojimo vadybos sistemos, EMS, ir (arba) paskirstymo vadybos sistemos, DMS) ryšiui;

b) įdiegti tinkamą atpažinties mechanizmą, skirtą automatų ryšiams ir tenkinantį realiojo laiko reikalavimus.

GRANDININIS POVEIKIS

6) Valstybės narės turėtų užtikrinti, kad atitinkamos suinteresuotosios šalys, konkrečiai energetikos tinklų operatoriai ir technologijų tiekėjai, o ypač TIS direktyva nustatyti esminių paslaugų operatoriai energetikos sektoriuje diegtų atitinkamas kibernetinio saugumo pasirengimo priemones, susijusias su grandininiu poveikiu. Elektros tinklai ir dujotiekiai Europoje yra glaudžiai tarpusavyje sujungti, todėl vienos energetikos sistemos dalies atjungimą ar sutrikdymą sukėlęs kibernetinis išpuolis gali turėti platų grandininį poveikį kitoms tos sistemos dalims.

7) Pagal šią rekomendaciją valstybės narės turėtų įvertinti energijos gamybos ir lanksčių paklausos sistemų, perdavimo ir paskirstymo pastočių bei linijų tarpusavio priklausomybę ir kritinę svarbą, taip pat įvertinti susijusias suinteresuotąsias šalis, kurioms pavykusio kibernetinio išpuolio ar kibernetinio incidento atveju būtų daromas poveikis (taip pat tarpvalstybinėse situacijose). Be to, valstybės narės turėtų užtikrinti, kad energetikos tinklų operatoriai būtų nustatę ryšių su visomis pagrindinėmis suinteresuotosiomis šalimis sistemą, kad galėtų perduoti ankstyvojo perspėjimo signalus ir bendradarbiauti valdant krizę. Turėtų būti nustatyti struktūrizuoti ryšių kanalai ir sutarti formatai keistis slapta informacija su visomis atitinkamomis suinteresuotosiomis šalimis, reagavimo į kompiuterių saugumo incidentus tarnybomis ir atitinkamomis valdžios institucijomis.

8) Visų pirma, energetikos tinklo operatoriai turėtų:

a) užtikrinti, kad visų naujų prietaisų, įskaitant daiktų interneto prietaisus, kibernetinio saugumo lygis būtų dabar ir ateityje tinkamas atsižvelgiant į konkrečios vietos kritinę svarbą;

b) tinkamai atsižvelgti į kibernetinį ir fizinį poveikį, rengdami ir reguliariai peržiūrėdami veiklos tęstinumo planus;

c) nustatyti atsparaus tinklo kūrimo kriterijus ir architektūrą, pagal kuriuos tinklo atsparumo būtų galima siekti:

— kiekvienoje vietoje įdiegiant išsamias apsaugos priemones, pritaikytas pagal konkrečios vietos kritinę svarbą,

— nustatant kritinius mazgus, tiek susijusius su elektros energijos gamybos pajėgumu, tiek su poveikiu klientams. Tinklo ypatingos svarbos funkcijos turėtų būti kuriamos taip, kad būtų sumažinta grandininio poveikio rizika, t. y. apsvarstant dubliavimą, atsparumą fazės virpesiams ir apsaugos nuo grandininio apkrovos nutrūkimo priemones,

— bendradarbiaujant su kitais atitinkamais operatoriais ir technologijų tiekėjais siekiant tinkamomis priemonėmis ir paslaugomis užkirsti kelią grandininiam poveikiui,

— projektuojant ir diegiant ryšių ir kontrolės tinklus, kad bet kokių fizinių ir loginių gedimų poveikis paveiktų tik ribotas tinklų dalis ir būtų užtikrintos tinkamos ir greitos poveikio mažinimo priemonės.

ESAMOS IR MODERNIAUSIOS TECHNOLOGIJOS

9) Valstybės narės turėtų užtikrinti, kad atitinkamos suinteresuotosios šalys, konkrečiai energetikos tinklų operatoriai ir technologijų tiekėjai, o ypač TIS direktyva nustatyti esminių paslaugų operatoriai energetikos sektoriuje diegtų atitinkamas kibernetinio saugumo pasirengimo priemones, susijusias su esamų ir moderniausių technologijų derinimu. Iš tiesų šiandienos energetikos sistemoje sąveikauja dviejų skirtingų rūšių technologijos: senesnė technologija, kurios gyvavimo laikotarpis yra 30–60 metų ir kuri buvo kuriama iki kibernetinio saugumo sampratos susiformavimo, ir moderni įranga, suderinama su moderniausiais skaitmeninimo ir išmaniaisiais prietaisais.

10) Pagal šią rekomendaciją valstybės narės turėtų energetikos tinklo operatorius ir technologijų tiekėjus skatinti, kai įmanoma, laikytis atitinkamų tarptautiniu mastu pripažintų kibernetinio saugumo standartų. Kita vertus, jungdamos prietaisus į tinklą suinteresuotosios šalys ir klientai turėtų laikytis į kibernetinį saugumą orientuoto požiūrio.

11) Visų pirma, vos paaiškėjus atitinkamai saugumo problemai, technologijų tiekėjai turėtų nemokamai teikti išbandytų esamų arba naujų technologijų saugumo problemų sprendimo būdų.

12) Visų pirma, energetikos tinklo operatoriai turėtų:

a) analizuoti esamų technologijų ir daiktų interneto koncepcijų jungimo riziką ir išmanyti vidaus ir išorės sąsajas ir jų silpnąsias vietas;

b) imtis tinkamų kovos su piktavališkais išpuoliais priemonių atvejais, kai šie išpuoliai vykdomi iš daugybės piktavališkai kontroliuojamų klientų prietaisų ar taikomųjų programų;

c) nustatyti automatizuotą su saugumu susijusių įvykių, pavyzdžiui, nepavykusių bandymų prisijungti, skydinių durų atidarymo signalizacijos ar kitų įvykių, esamų įrenginių ir daiktų interneto aplinkose stebėsenos ir analizės sistemą;

d) reguliariai atlikti specialią esamų įrenginių kibernetinio saugumo rizikos analizę, ypač sujungiant senas ir naujas technologijas; kadangi esami įrenginiai dažnai sudaro labai didelę turto dalį, galima atlikti atskirų klasių turto rizikos analizę;

e) atnaujinti esamų ir daiktų interneto sistemų programinę ir aparatinę įrangą, kai įmanoma, įdiegiant pačią naujausią jų versiją. Tuo tikslu energetikos tinklo operatoriai turėtų apsvarstyti papildomas priemones, kaip antai sistemos atskyrimą arba išorinių saugumo barjerų įdiegimą, tais atvejais, kai reikėtų pataisų ar atnaujinimo, tačiau juos atlikti nėra galimybių (pavyzdžiui, kai produktų palaikymas nutrauktas);

f) rengiant konkursus atsižvelgti į kibernetinį saugumą, kitaip tariant, reikalauti informacijos apie saugumo priemones, reikalauti laikytis galiojančių kibernetinio saugumo standartų, užtikrinti nuolatinį perspėjimo, pataisų diegimo ir rizikos mažinimo pasiūlymų teikimą, jei nustatomos silpnosios vietos, ir paaiškinti pardavėjo atsakomybę kibernetinių išpuolių ar incidentų atveju;

g) bendradarbiauti su technologijų tiekėjais keičiant esamas sistemas, jei tai naudinga saugumo sumetimais, tačiau atsižvelgti į ypatingos svarbos sistemos funkcijas.

STEBĖSENA

13) Per 12 mėnesių nuo šios rekomendacijos priėmimo ir vėliau kas dvejus metus valstybės narės per TIS bendradarbiavimo grupę turėtų pateikti Komisijai išsamios informacijos apie šios rekomendacijos įgyvendinimo pažangą.

PERŽIŪRA

14) Remdamasi valstybių narių pateikta informacija Komisija peržiūrės šios rekomendacijos įgyvendinimą ir, pasikonsultavusi su valstybėmis narėmis ir suinteresuotosiomis šalimis, įvertins, ar reikėtų papildomų priemonių.

ADRESATAI

15) Ši rekomendacija skirta valstybėms narėms.

Priimta Briuselyje 2019 m. balandžio 3 d.

Komisijos vardu

Miguel ARIAS CAÑETE

Komisijos narys