SOOVITUSED

KOMISJONI SOOVITUS (EL) 2019/553,

3. aprill 2019,

küberturvalisuse kohta energeetikasektoris

(teatavaks tehtud numbri C(2019) 2400 all)

EUROOPA KOMISJON,

võttes arvesse Euroopa Liidu toimimise lepingut, eriti selle artiklit 292,

ning arvestades järgmist:

(1) Euroopa energeetikasektoris toimub oluline muutus vähese CO_2-heitega majanduse suunas, kus on tagatud ka varustuskindlus ja konkurentsivõime. Energiasüsteemi ümberkujundamise ja sellega seotud taastuvenergiatootmise detsentraliseerimise käigus muudavad tehnoloogia areng, sektorite ühendamine ja digitaliseerimine Euroopa elektrivõrgu tarkvõrguks. Samal ajal toob see kaasa ka uued ohud, sest digitaliseerimine muudab energiasüsteemi üha enam vastuvõtlikuks küberrünnetele ja intsidentidele, mis võivad ohustada energiavarustuskindlust.

(2) Kõigi kaheksa paketti „Puhas energia kõikidele eurooplastele“ kuuluva õigusakti ettepaneku ([1]) (sealhulgas energialiidu juhtimise kui hüppelaua kohta) vastuvõtmine võimaldab luua soodsa keskkonna energeetikasektori digitaliseerimiseks. Samuti tunnustatakse sellega küberturvalisuse olulisust energeetikasektoris. Eelkõige uuesti sõnastatud elektrienergia siseturu määrusega ([2]) nähakse ette selliste elektrialaste tehniliste eeskirjade vastuvõtmine nagu võrgueeskirjad piiriüleste elektrivoogude küberturvalisuse aspektide sektoripõhiste eeskirjade, ühiste miinimumnõuete, planeerimise, seire, aruandluse ja kriisiohje kohta. Ohuvalmidust elektrisektoris käsitlev määrus ([3]) järgib üldjoontes gaasivarustuskindluse määrusega ([4]) valitud lähenemisviisi; selles rõhutatakse vajadust hinnata nõuetekohaselt kõiki riske, sealhulgas küberturvalisusega seotud riske, ning tehakse ettepanek võtta vastu meetmed nende kindlakstehtud riskide ennetamiseks ja vähendamiseks.

(3) 2013. aastal ELi küberjulgeoleku strateegiat ([5]) vastu võttes kinnitas komisjon prioriteediks liidu kübervastupidavusvõime tugevdamise. Selle strateegia üks peamisi tulemusi on 2016. aasta juulis vastu võetud direktiiv võrgu- ja infosüsteemide turvalisuse kohta ([6]) (edaspidi „küberturvalisuse direktiiv“). Esimese küberturvalisust käsitleva horisontaalse ELi õigusaktina tõstab küberturvalisuse direktiiv küberturvalisuse üldist taset liidus liikmesriikide küberturvalisuse alase suutlikkuse arendamise, ELi tasandi koostöö suurendamise ning ettevõtetele ehk oluliste teenuste operaatoritele turvaohtudest ja küberintsidentidest teatamise kohustuse kehtestamise teel. Intsidentidest teatamine on esmatähtsates sektorites, sealhulgas energeetikasektoris, kohustuslik.

([1]) Euroopa Parlamendi ja nõukogu 11. detsembri 2018. aasta direktiiv (EL) 2018/2001 taastuvatest energiaallikatest toodetud energia kasutamise edendamise kohta (ELT L 328, 21.12.2018, lk 82), Euroopa Parlamendi ja nõukogu 11. detsembri 2018. aasta direktiiv (EL) 2018/2002, millega muudetakse direktiivi 2012/27/EL, milles käsitletakse energiatõhusust (ELT L 328, 21.12.2018, lk 210), Euroopa Parlamendi ja nõukogu 11. detsembri 2018. aasta määrus (EL) 2018/1999, milles käsitletakse energialiidu ja kliimameetmete juhtimist ning millega muudetakse Euroopa Parlamendi ja nõukogu määrusi (EÜ) nr 663/2009 ja (EÜ) nr 715/2009, Euroopa Parlamendi ja nõukogu direktiive 94/22/EÜ, 98/70/EÜ, 2009/31/EÜ, 2009/73/EÜ, 2010/31/EL, 2012/27/EL ja 2013/30/EL ning nõukogu direktiive 2009/119/EÜ ja (EL) 2015/652 ning tunnistatakse kehtetuks Euroopa Parlamendi ja nõukogu määrus (EL) nr 525/2013 (ELT L 328, 21.12.2018, lk 1), Euroopa Parlamendi ja nõukogu 30. mai 2018. aasta direktiiv (EL) 2018/844, millega muudetakse direktiivi 2010/31/EL hoonete energiatõhususe kohta ja direktiivi 2012/27/EL energiatõhususe kohta (ELT L 156, 19.6.2018, lk 75). Euroopa Parlament kinnitas 2019. aasta märtsis täiskogu istungil nõukoguga elektrituru korralduse ettepanekute kohta (ohuvalmiduse määrus, Energeetikasektorit Reguleerivate Asutuste Koostööameti (ACER) määrus, elektridirektiiv ja elektrimäärus) saavutatud poliitilisi kokkuleppeid. Ametlik vastuvõtmine nõukogus toimub eeldatavast aprillis ning varsti pärast seda avaldatakse õigusaktide tekstid *Euroopa Liidu Teatajas*.

([2]) COM(2016) 861.

([3]) COM(2016) 862.

([4]) Euroopa Parlamendi ja nõukogu 25. oktoobri 2017. aasta määrus (EL) 2017/1938, mis käsitleb gaasivarustuskindluse tagamise meetmeid ja millega tunnistatakse kehtetuks määrus (EL) nr 994/2010 (ELT L 280, 28.10.2017, lk 1).

([5]) JOIN(2013) 1.

([6]) Euroopa Parlamendi ja nõukogu 6. juuli 2016. aasta direktiiv (EL) 2016/1148 meetmete kohta, millega tagada võrgu- ja infosüsteemide turvalisuse ühtlaselt kõrge tase kogu liidus (ELT L 194, 19.7.2016, lk 1).

(4) Küberturvalisuse alase valmisoleku meetmete rakendamisel peaksid asjaomased sidusrühmad, sealhulgas küberturvalisuse direktiivi kohaste oluliste energiateenuste operaatorid võtma arvesse küberturvalisuse direktiivi artikli 11 kohaselt loodud võrgu- ja infoturbe koostöörühma välja antud horisontaalseid suuniseid. Kõnealune koostöörühm, millesse kuuluvad liikmesriikide, Euroopa Liidu Küberturvalisuse Ameti (edaspidi „ENISA“) ja komisjoni esindajad, on vastu võtnud juhenddokumendid turvameetmete ja intsidentidest teatamise kohta. 2018. aasta juunis lõi kõnealune töörühm spetsiaalse energeetikaalase töösuuna.

(5) 2017. aasta küberturvalisuse ühisteatises ([7]) tunnustatakse ELi tasandi sektoripõhiste (sh energeetikasektor) kaalutluste ja nõuete olulisust. Küberturvalisust ja selle võimalikku poliitilist mõju on viimaste aastate jooksul liidus põhjalikult arutatud. Sellest tulenevalt suureneb teadlikkus sellest, et üksikud majandussektorid seisavad silmitsi konkreetsete küberturvalisuse küsimustega ja peavad seetõttu üldise küberturvalisuse strateegia laiemas kontekstis arendama oma sektoripõhiseid lähenemisviise.

(6) Küberturvalisuse põhielemendid on teabe jagamine ja usaldus. Komisjoni eesmärk on suurendada teabe jagamist asjaomaste sidusrühmade vahel, korraldades spetsiaalseid üritusi, nagu olid näiteks energeetikasektori küberturvalisust käsitlev kõrgetasemeline ümarlaud Roomas 2017. aasta märtsis ja samateemaline kõrgetasemeline konverents Brüsselis 2018. aasta oktoobris. Samuti soovib komisjon tugevdada asjaomaste sidusrühmade ja spetsialiseerunud üksuste, nagu näiteks Euroopa energiavaldkonna teabe jagamise ja analüüsimise keskuse vahelist koostööd.

(7) Määrus ELi küberturvalisuse ameti (ENISA) ning info- ja kommunikatsioonitehnoloogia küberturvalisuse sertifitseerimise kohta ([8]) (edaspidi „määrus küberturvalisust käsitleva õigusakti kohta“) tugevdab ELi küberturvalisuse ameti volitusi, et liikmesriike küberturvalisusega seotud ohtude ja küberrünnakutega tegelemisel paremini toetada. Samuti luuakse sellega Euroopa küberturvalisuse raamistik toodete, protsesside ja teenuste sertifitseerimiseks, mis kehtib kogu liidus ja mis pakub eriti suurt huvi energeetikasektorile.

(8) Komisjon esitas soovituse, ([9]) milles käsitletakse küberturvalisusega seotud riske 5. põlvkonna (5G) võrgutehnoloogiate puhul, andes suuniseid riski asjakohaseks analüüsimiseks ja riskijuhtimismeetmete võtmiseks riiklikul tasandil, koordineeritud Euroopa riskianalüüsi väljatöötamiseks ning parimatest riskijuhtimismeetmetest ühiste töövahendite komplekti väljatöötamiseks vajaliku korra kehtestamiseks. Kui 5G võrgud on kord kasutusele võetud, moodustavad need põhistruktuuri suure hulga niisuguste teenuste jaoks, mis on hädavajalikud siseturu toimimiseks, ning samuti ühiskonnas ja majanduses oluliste teenuste, nt energiavarustuse jaoks.

(9) Käesolev soovitus peaks andma liikmesriikidele ja asjaomastele sidusrühmadele, eelkõige võrguoperaatoritele ja tehnoloogia tarnijatele mõningaid suuniseid suurema küberturvalisuse saavutamiseks, võttes arvesse energeetikasektori puhul kindlaks määratud reaalajalisi erinõudeid, doominoefekte ning vanemate ja tipptasemel tehnoloogiate kombineerimist. Käesolevate suuniste eesmärk on aidata sidusrühmadel rahvusvaheliselt tunnustatud küberturvalisuse standardite ([10]) rakendamisel meeles pidada energeetikasektori erinõudeid.

(10) Komisjon kavatseb käesolevat soovitust korrapäraselt läbi vaadata, lähtudes kogu liidus toimunud arengust ja konsulteerides ühtlasi liikmesriikide ja asjaomaste sidusrühmadega. Komisjon jätkab jõupingutusi küberturvalisuse tugevdamiseks energeetikasektoris, nimelt võrgu- ja infoturbe koostöörühma kaudu, mis tagab liikmesriikide strateegilise koostöö ja teabevahetuse küberturvalisuse valdkonnas.

ON VASTU VÕTNUD KÄESOLEVA SOOVITUSE:

REGULEERIMISESE

1. Käesolevas soovituses on esitatud peamised energeetikasektori küberturvalisusega seotud probleemid, nimelt reaalajalised nõuded, doominoefektid ning vanemate ja tipptasemel tehnoloogiate kombineerimine; samuti on kindlaks tehtud peamised toimingud asjakohaste küberturvalisuse valmisolekumeetmete rakendamiseks energeetikasektoris.

([7]) JOIN(2017) 450.

([8]) Euroopa Parlament võttis küberturvalisust käsitleva õigusakti vastu 2019. aasta märtsis. Ametlik vastuvõtmine nõukogus toimub eeldatavast aprillis ning varsti pärast seda avaldatakse õigusakti tekst *Euroopa Liidu Teatajas*.

([9]) C(2019) 2335.

([10]) Rahvusvahelised standardiorganisatsioonid on avaldanud mitmesuguseid küberturvalisuse (ISO/IEC 27000: Infotehnoloogia) ja riskijuhtimise standardeid (ISO/IEC 31000: Riskijuhtimise rakendamine). 2017. aasta oktoobris avaldati ISO/IEC 27000 seeria osana eristandard energeetikasektori jaoks (ISO/IEC 27019: Infoturbemeetodid energiatööstuses).

2. Käesoleva soovituse rakendamisel peaksid liikmesriigid julgustama asjaomaseid sidusrühmi suurendama energeetikasektori küberturvalisuse alaseid teadmisi ja oskusi. Vajaduse korral peaksid liikmesriigid lisama need kaalutlused oma riiklikku küberturvalisuse raamistikku, eeskätt strateegiate, seaduste, määruste ja muude haldussätete kaudu.

ENERGIATARISTU KOMPONENTIDE REAALAJALISED NÕUDED

3. Liikmesriigid peaksid tagama, et asjaomased sidusrühmad, nimelt energiavõrgu operaatorid ja tehnoloogia tarnijad ja eelkõige küberturvalisuse direktiivi kohased oluliste teenuste operaatorid rakendavad asjakohaseid küberturvalisuse valmisolekumeetmeid, mis on seotud energeetikasektori reaalajaliste nõuetega. Mõned energiasüsteemi elemendid peavad toimima reaalajas, st reageerima käsklustele mõne millisekundi jooksul, mistõttu küberturvalisuse meetmete võtmine on ajapuuduse tõttu keeruline või lausa võimatu.

4. Energiavõrkude operaatorid peaksid eelkõige:

   a) kohaldama uute käitiste suhtes kõige uuemaid turbestandardeid, kui see on asjakohane, ning kaaluma täiendavaid füüsilisi turvameetmeid, kui vanade käitiste seadmestiku kaitsmiseks ei piisa küberturvalisuse mehhanismidest;

   b) rakendama turvalise reaalajas toimuva teabevahetuse huvides rahvusvahelisi küberturvalisusstandardeid ja asjakohaseid spetsiaalseid tehnilisi standardeid kohe, kui asjaomased tooted müügile tulevad;

   c) kaaluma reaalaja nõuetest tingitud piiranguid varade üldises turvakontseptsioonis, eelkõige varade liigitamisel;

   d) kaaluma eraomandis olevate võrkude kasutamist kaugkaitseskeemides, et tagada reaalajaliste piirangute tõttu nõutav teenusekvaliteet; avalike sidevõrkude kasutamisel peaksid operaatorid kaaluma konkreetse ribalaiuse tagamist, nõudeid latentsusaja kohta ja sideturbemeetmeid;

   e) jaotama kogu süsteemi loogilisteks tsoonideks ja määrama igas tsoonis kindlaks aja ja protsessiga seotud piirangud, et oleks võimalik võtta sobivaid küberturvalisuse meetmeid või kaaluda alternatiivseid kaitsemeetodeid.

5. Kui see on võimalik, peaksid energiavõrkude operaatorid:

   a) valima turvalise sideprotokolli, võttes arvesse reaalajalisi nõudeid, näiteks käitise ja selle juhtimissüsteemide vahel (energiajuhtimissüsteem/jaotushaldussüsteem);

   b) võtma kasutusele reaalajalistele nõuetele vastava asjakohase autentimismehhanismi masinatevahelise side jaoks.

DOOMINOEFEKTID

6. Liikmesriigid peaksid tagama, et asjaomased sidusrühmad, nimelt energiavõrgu operaatorid ja tehnoloogia tarnijad ja eelkõige küberturvalisuse direktiivi kohased oluliste teenuste operaatorid rakendavad asjakohaseid küberturvalisuse valmisolekumeetmeid, mis on seotud doominoefektidega energeetikasektoris. Elektrivõrgud ja gaasijuhtmed on kogu Euroopas omavahel tihedalt seotud ning küberrünne, mis tekitab elektrikatkestuse või varustushäireid energiasüsteemi ühes osas, võib vallandada ulatusliku doominoefekti, mis jõuab süsteemi teiste osadeni.

7. Käesoleva soovituse rakendamisel peaksid liikmesriigid hindama elektrienergia tootmise ja paindliku nõudluse süsteemide, ülekande- ja jaotusalajaamade ja -liinide omavahelist sõltuvust ja olulisust ning seotud mõjutatavaid sidusrühmi (kaasa arvatud piiriüleste olukordade puhul), kui peaks toimuma edukas küberrünne või -intsident. Samuti peaksid liikmesriigid tagama, et energiavõrgu operaatorite ja kõigi peamiste sidusrühmade vahel on sidepidamise raamistik, mis võimaldab jagada varaseid hoiatusmärke ja teha kriisiohjamisel koostööd. Olemas peaksid olema struktureeritud sidekanalid ja kokkulepitud vormid tundliku teabe jagamiseks kõigi asjaomaste sidusrühmade, küberturbe intsidentide lahendamise üksuste ja asjaomaste asutustega.

8. Energiavõrkude operaatorid peaksid eelkõige:

   a) tagama, et uued seadmed, sealhulgas asjade interneti seadmed on rajatise olulisusele vastava küberturvalisuse tasemega ja see tase säilib;

   b) võtma talitluspidevuse kavade koostamisel ja regulaarsel läbivaatamisel asjakohaselt arvesse küberfüüsilist mõju;

c) kehtestama vastupidava võrgu projekteerimise kriteeriumid ja arhitektuuri, mida on võimalik saavutada järgmiselt:

— kehtestades iga rajatise kohta põhjalikud kaitsemeetmed, mis on kohandatud vastavalt rajatise olulisusele;

— tehes kindlaks kriitilised sõlmpunktid nii energiatootmisvõimsuse kui ka kliendile avalduva mõju seisukohast; võrgu olulised funktsioonid peaksid olema kavandatud nii, et doominoefekti põhjustavad riskid oleksid vähendatud, võttes arvesse liiasust, vastupidavust faasikõikumistele ja kaitset koormuse astmelise kadumise korral;

— tehes koostööd teiste asjaomaste operaatorite ja tehnoloogia tarnijatega, et ennetada doominoefekti, rakendades asjakohaseid meetmeid ja teenuseid;

— võttes side- ja juhtimisvõrkude projekteerimisel ja ehitamisel arvesse mis tahes füüsilise või loogilise rikke mõjude piiramist võrgu osades ning piisavate ja kiirete leevendusmeetmete tagamist.

VANEM JA TIPPTASEMEL TEHNOLOOGIA

9. Liikmesriigid peaksid tagama, et asjaomased sidusrühmad, nimelt energiavõrgu operaatorid ja tehnoloogia tarnijad ja eelkõige küberturvalisuse direktiivi kohased oluliste teenuste operaatorid rakendavad asjakohaseid küberturvalisuse valmisolekumeetmeid, mis on seotud vanemate ja tipptasemel tehnoloogiate kombineerimisega energeetikasektoris. Praeguses energiasüsteemis on kasutusel kaks eri tüüpi tehnoloogiat: vanem tehnoloogia, mille eluiga on 30–60 aastat ja mis on välja töötatud enne küberturvalisusega seotud aspektide tekkimist, ning moodsad seadmed, mis on nutikad ja peegeldavad tipptasemel digitaliseerimist.

10. Käesoleva soovituse rakendamisel peaksid liikmesriigid julgustama energiavõrguoperaatoreid ja tehnoloogia tarnijaid järgima võimaluse korral alati asjakohaseid rahvusvaheliselt tunnustatud küberturvalisuse standardeid. Sidusrühmad ja kliendid peaksid omalt poolt võtma seadmete võrku ühendamisel omaks küberturvalisust arvestava lähenemisviisi.

11. Tehnoloogia tarnijad peaksid eelkõige pakkuma kontrollitud lahendusi vanema ja uue tehnoloogiaga seotud turvalisusprobleemidele tasuta ja kohe, kui asjaomane probleem on ilmnenud.

12. Energiavõrkude operaatorid peaksid eelkõige:

a) analüüsima vanema tehnoloogia ning asjade interneti kontseptsioonide ühendamisega seotud riske ning olema teadlikud sise- ja välisliidestest ning nende haavatavustest;

b) võtma sobivaid meetmeid pahatahtlikke rünnete vastu, mille tegemiseks on kahju tekitamise eesmärgil haaratud kontroll paljude tarbijaseadmete või rakenduste üle;

c) arendama vanema tehnoloogia ja asjade interneti turvalisusega seotud sündmuste automaatseire- ja analüüsivõimekust; sellised sündmused on näiteks ebaõnnestunud sisselogimiskatse, kapiukse avamisel vallanduv alarm jms;

d) tegema kõigis vanema tehnoloogiaga käitistes regulaarselt küberturvalisuse eririskide analüüsi, eriti juhul, kui ühendatakse vana ja uut tehnoloogiat; kuna vanad käitised moodustavad sageli väga suure osa varadest, võib riskianalüüsi teha varaliikide kaupa;

e) ajakohastama vanemate ning asjade interneti süsteemide tarkvara ja riistvara uusimale versioonile alati, kui see on asjakohane; seejuures peaksid energiavõrgu operaatorid kaaluma täiendavaid meetmeid nagu süsteemi eraldamine või väliste turvatõkete paigaldamine, kui paikamine või ajakohastamine oleks asjakohane, kuid ei ole võimalik näiteks toodete puhul, mida ei toetata;

f) pidama pakkumuste koostamisel meeles küberturvalisust, st nõudma teavet turvaomaduste kohta, nõudma vastavust olemasolevatele küberturvalisuse standarditele, nõudma ettepanekuid selle kohta, kuidas tagatakse pidev hoiatamine, paikamine ja leevendamine, kui avastatakse haavatavusi, ning selgitama müüja vastutust küberrünnete või -intsidentide korral;

g) tegema koostööd tehnoloogia tarnijatega vanemate süsteemide asendamiseks alati, kui see on turvakaalutlustel kasulik, kuid võtma seejuures arvesse kriitilise tähtsusega süsteemi funktsioone.

SEIRE

13. Liikmesriigid peaksid 12 kuu jooksul pärast käesoleva soovituse vastuvõtmist ja seejärel iga kahe aasta möödudes esitama võrgu- ja infoturbe koostöörühma kaudu komisjonile üksikasjalike teabe käesoleva soovituse rakendamise seisu kohta.

LÄBIVAATAMINE

14. Komisjon vaatab liikmesriikide esitatud teabe põhjal käesoleva soovituse rakendamise läbi ja hindab, kas on vaja täiendavaid meetmeid, konsulteerides vajaduse korral liikmesriikide ja asjaomaste sidusrühmadega.

ADRESSAADID

15. Käesolev soovitus on adresseeritud liikmesriikidele.

Brüssel, 3. aprill 2019

Komisjoni nimel

komisjoni liige

Miguel ARIAS CAÑETE