PREPORUKE

PREPORUKA KOMISIJE (EU) 2019/553

od 3. travnja 2019.

o kibersigurnosti u energetskom sektoru

(priiopćeno pod brojem dokumenta C(2019) 2400)

EUROPSKA KOMISIJA,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov članak 292.,

budući da:

(1) Europski energetski sektor uvelike se mijenja prelaskom na dekarbonizirano gospodarstvo uz istodobno osiguravanje sigurnosti opskrbe i konkurentnosti. U okviru te energetske tranzicije i s njom povezane decentralizacije proizvodnje električne energije iz obnovljivih izvora, tehnološki napredak, povezivanje sektora i digitalizacija pretvaraju europsku mrežu u „pametnu mrežu". Zbog toga nastaju i novi rizici jer je zbog digitalizacije energetski sustav sve izloženiji kibernapadima i incidentima koji mogu ugroziti sigurnost opskrbe energijom.

(2) Donošenjem svih osam zakonodavnih prijedloga ([1]) iz paketa „Čista energija za sve Europljane", što uključuje upravljanje energetskom unijom kao ključan korak u tom smjeru, omogućuje se stvaranje povoljnog okruženja za digitalnu transformaciju energetskog sektora. Prepoznaje se i važnost kibersigurnosti u energetskom sektoru. Među ostalom, preinakom Uredbe o unutarnjem tržištu električne energije ([2]) predviđa se donošenje tehničkih pravila za električnu energiju, kao što su posebna sektorska mrežna pravila za aspekte kibersigurnosti prekograničnih tokova električne energije, mrežna pravila o zajedničkim minimalnim zahtjevima, planiranju, praćenju, izvješćivanju i upravljanju u kriznim situacijama. U Uredbi o pripravnosti na rizike u području električne energije ([3]) u širem se smislu slijedi pristup odabran u Uredbi o sigurnosti opskrbe plinom ([4]), naglašavanjem potrebe za odgovarajućom procjenom svih rizika, uključujući one povezane s kibersigurnošću, te predlaganjem mjera za sprečavanje i ublažavanje utvrđenih rizika.

(3) Prilikom donošenja Strategije EU-a za kibersigurnost ([5]) 2013. Komisija je kao prioritet odredila jačanje kiberotpornosti Unije. Direktiva o sigurnosti mrežnih i informacijskih sustava ([6]) (dalje u tekstu „Direktiva NIS"), donesena u srpnju 2016., jedan je od ključnih rezultata te strategije. Kao prvi horizontalni zakonodavni akt EU-a u području kibersigurnosti, Direktiva NIS povećava ukupnu razinu kibersigurnosti u Uniji razvojem nacionalnih kapaciteta u području kibersigurnosti, povećanjem suradnje na razini EU-a i uvođenjem obveza izvješćivanja o sigurnosti i incidentima za trgovačka društva koja se nazivaju „operatori ključnih usluga". Izvješćivanje o incidentima obvezno je u ključnim sektorima, uključujući energetski sektor.

([1]) Direktiva (EU) 2018/2001 Europskog parlamenta i Vijeća od 11. prosinca 2018. o promicanju uporabe energije iz obnovljivih izvora (SL L 328, 21.12.2018., str. 82.); Direktiva (EU) 2018/2002 Europskog parlamenta i Vijeća od 11. prosinca 2018. o izmjeni Direktive 2012/27/EU o energetskoj učinkovitosti (SL L 328, 21.12.2018., str. 210.); Uredba (EU) 2018/1999 Europskog parlamenta i Vijeća od 11. prosinca 2018. o upravljanju energetskom unijom i djelovanjem u području klime, izmjeni uredaba (EZ) br. 663/2009 i (EZ) br. 715/2009 Europskog parlamenta i Vijeća, direktiva 94/22/EZ, 98/70/EZ, 2009/31/EZ, 2009/73/EZ, 2010/31/EU, 2012/27/EU i 2013/30/EU Europskog parlamenta i Vijeća, direktiva Vijeća 2009/119/EZ i (EU) 2015/652 te stavljanju izvan snage Uredbe (EU) br. 525/2013 Europskog parlamenta i Vijeća (SL L 328, 21.12.2018., str. 1.); Direktiva (EU) 2018/844 Europskog parlamenta i Vijeća od 30. svibnja 2018. o izmjeni Direktive 2010/31/EU o energetskim svojstvima zgrada i Direktive 2012/27/EU o energetskoj učinkovitosti (SL L 156, 19.6.2018., str. 75.). Na plenarnom zasjedanju u ožujku 2019. Europski parlament potvrdio je političke sporazume postignute s Vijećem o prijedlozima modela tržišta električne energije (Uredba o pripremljenosti za rizike, Uredba o Agenciji za suradnju energetskih regulatora (ACER) te Direktiva o električnoj energiji i Uredba o električnoj energiji). Očekuje se da će ih Vijeće formalno donijeti u travnju; objava pravnog teksta u Službenom listu uslijedit će ubrzo nakon toga.

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

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

([4]) Uredba (EU) 2017/1938 Europskog parlamenta i Vijeća od 25. listopada 2017. o mjerama zaštite sigurnosti opskrbe plinom i stavljanju izvan snage Uredbe (EU) br. 994/2010 (SL L 280, 28.10.2017., str. 1.).

([5]) JOIN(2013) 1

([6]) Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194, 19.7.2016., str. 1.).

(4) Pri provedbi mjera pripravnosti u području kibersigurnosti relevantni dionici, uključujući operatore ključnih usluga u području energetike utvrđene u skladu s Direktivom NIS, trebali bi uzeti u obzir horizontalne smjernice koje je izdala Skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava osnovana na temelju članka 11. Direktive NIS. Ta skupina za suradnju, koja se sastoji od predstavnika država članica, Europske agencije za mrežnu i informacijsku sigurnost (ENISA) i Komisije, donijela je smjernice za sigurnosne mjere i obavješćivanje o incidentima. Skupina je u lipnju 2018. osnovala posebnu radnu skupinu za područje energetike.

(5) U Zajedničkoj komunikaciji o kibersigurnosti ([7]) iz 2017. prepoznaje se važnost razmatranja i zahtjeva svojstvenih pojedinim sektorima na razini EU-a, uključujući i za energetski sektor. U EU-u je tijekom posljednjih godina pokrenuta sveobuhvatna rasprava o kibersigurnosti i mogućim posljedicama za politike. Stoga danas raste svijest o tome da se pojedinačni gospodarski sektori suočavaju s posebnim pitanjima kibersigurnosti i da zato moraju razviti vlastite sektorske pristupe u širem kontekstu općih strategija za kibersigurnost.

(6) Razmjena informacija i povjerenje ključni su elementi kibersigurnosti. Komisija nastoji povećati razmjenu informacija među relevantnim dionicima organiziranjem posebnih događaja, kao što su, primjerice, okrugli stol na visokoj razini o kibersigurnosti u području energetike održan u Rimu u ožujku 2017. i konferencija na visokoj razini o kibersigurnosti u području energetike održana u Bruxellesu u listopadu 2018. Komisija također želi poboljšati suradnju između relevantnih dionika i specijaliziranih subjekata kao što su Europski centar za razmjenu i analizu informacija o energetici.

(7) Uredbom o ENISA-i (Agenciji EU-a za kibersigurnost) i o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije („Uredba o kibersigurnosti") ([8]) ojačat će se mandat Agencije EU-a za kibersigurnost kako bi se bolje pomoglo državama članicama u borbi protiv prijetnji i napada u području kibersigurnosti. Njome se također uspostavlja europski okvir za kibersigurnost za certifikaciju proizvoda, postupaka i usluga koja će biti valjana u čitavoj Uniji te je od posebnog interesa za energetski sektor.

(8) Komisija je predstavila Preporuku ([9]) kojom se nastoje riješiti pitanja kibersigurnosnih rizika u petoj generaciji (5G) mrežnih tehnologija davanjem smjernica o odgovarajućoj analizi rizika i mjerama upravljanja na nacionalnoj razini, o razvoju usklađene europske analize rizika i o utvrđivanju postupka za razvoj skupa zajedničkih alata s najboljim mjerama za upravljanje rizicima. Nakon što se uvedu, mreže 5G bit će okosnica brojnih usluga koje su ključne za funkcioniranje unutarnjeg tržišta i iznimno važnih društvenih i ekonomskih djelatnosti kao što je energetika.

(9) Ovom bi se Preporukom državama članicama i relevantnim dionicima, posebno mrežnim operatorima i dobavljačima tehnologije, trebale pružiti neke od smjernica za postizanje više razine kibersigurnosti s obzirom na posebne zahtjeve u stvarnom vremenu utvrđene za energetski sektor, kaskadne učinke i kombinaciju naslijeđenih i najnovijih tehnologija. Cilj je ovih smjernica pomoći dionicima da vode računa o posebnim zahtjevima energetskog sektora pri provedbi međunarodno priznatih normi kibersigurnosti ([10]).

(10) Komisija namjerava redovito preispitivati ovu Preporuku na temelju napretka postignutog diljem Unije uz savjetovanje s državama članicama i relevantnim dionicima. Komisija će i dalje nastojati ojačati kibersigurnost u energetskom sektoru, posebno putem Skupine za suradnju u području sigurnosti mrežnih i informacijskih sustava, koja osigurava stratešku suradnju i razmjenu informacija među državama članicama u području kibersigurnosti,

DONIJELA JE OVU PREPORUKU:

PREDMET

1. U ovoj se Preporuci iznose glavna pitanja povezana s kibersigurnošću u energetskom sektoru, odnosno zahtjevi u stvarnom vremenu, kaskadni učinci i kombinacija naslijeđene i najnovije tehnologije, te se određuju glavne mjere za provedbu relevantnih mjera pripravnosti u području kibersigurnosti u energetskom sektoru.

([7]) JOIN(2017) 450

([8]) Akt o kibersigurnosti donio je Europski parlament u ožujku 2019. Očekuje se da će ga Vijeće formalno donijeti u travnju; objava pravnog teksta u Službenom listu uslijedit će ubrzo nakon toga.

([9]) C(2019)2335

([10]) Međunarodne organizacije za normizaciju objavile su niz normi za kibersigurnost (ISO/IEC 27000: Informacijske tehnologije) i upravljanje rizikom (ISO/IEC31000: Provedba upravljanja rizicima). Posebna norma za energetski sektor (ISO/IEC 27019: Kontrole informacijske sigurnosti za elektroenergetsku industriju) izdana je u listopadu 2017. u okviru serije ISO/IEC 27000.

2. Pri primjeni ove Preporuke države članice trebale bi poticati relevantne dionike da razviju znanja i vještine povezane s kibersigurnošću u energetskom sektoru. Države članice bi, prema potrebi, trebale uključiti ta pitanja u svoje nacionalne okvire za kibersigurnost, posebno putem strategija, zakona i drugih propisa.

ZAHTJEVI U STVARNOM VREMENU ZA KOMPONENTE ENERGETSKE INFRASTRUKTURE

3. Države članice trebale bi osigurati da relevantni dionici, posebno operatori energetskih mreža i dobavljači tehnologije, a osobito operatori ključnih usluga utvrđeni u skladu s Direktivom NIS, provode odgovarajuće mjere pripravnosti u području kibersigurnosti povezane sa zahtjevima u stvarnom vremenu u energetskom sektoru. Neki elementi energetskog sustava moraju raditi u „stvarnom vremenu", odnosno reagirati na naredbe u roku od nekoliko milisekundi, što otežava ili čak onemogućuje uvođenje mjera kibersigurnosti zbog nedostatka vremena.

4. Konkretno, operatori energetskih mreža trebali bi:

   (a) primjenjivati najnovije sigurnosne standarde za nova postrojenja gdje god je to primjereno i razmotriti komplementarne mjere fizičke sigurnosti ako se instalirana stara postrojenja ne mogu dovoljno zaštititi mehanizmima kibersigurnosti;

   (b) provoditi međunarodne norme o kibersigurnosti i odgovarajuće posebne tehničke standarde za sigurnu komunikaciju u stvarnom vremenu čim odgovarajući proizvodi postanu dostupni na tržištu;

   (c) razmotriti ograničenja u stvarnom vremenu u ukupnom sigurnosnom konceptu za sredstva, posebno u pogledu njihova razvrstavanja;

   (d) razmotriti mreže u privatnom vlasništvu za sustave zaštite na daljinu kako bi se osigurala razina kvalitete usluge potrebna za ograničenja u stvarnom vremenu; pri uporabi javnih komunikacijskih mreža operatori bi trebali razmotriti osiguravanje posebne raspodjele pojasne širine, zahtjeve u pogledu kašnjenja i mjere komunikacijske sigurnosti;

   (e) podijeliti cjelokupni sustav na logičke zone i u svakoj zoni odrediti vremenska i procesna ograničenja kako bi se omogućila primjena odgovarajućih mjera kibersigurnosti ili kako bi se razmotrile alternativne metode zaštite.

5. Gdje je to moguće, operatori energetskih mreža trebali bi također:

   (a) odabrati siguran komunikacijski protokol, uzimajući u obzir zahtjeve u stvarnom vremenu, primjerice između postrojenja i njegovih sustava upravljanja (sustav za upravljanje energijom – EMS/sustav za upravljanje distribucijom – DMS);

   (b) uvesti odgovarajući mehanizam autentifikacije za komunikaciju između strojeva, za rješavanje zahtjeva u stvarnom vremenu.

KASKADNI UČINCI

6. Države članice trebale bi osigurati da relevantni dionici, posebno operatori energetskih mreža i dobavljači tehnologije, a osobito operatori ključnih usluga utvrđeni u skladu s Direktivom NIS, provode odgovarajuće mjere pripravnosti u području kibersigurnosti povezane s kaskadnim učincima u energetskom sektoru. Elektroenergetske mreže i plinovodi izrazito su međusobno povezani diljem Europe, a kibernapad koji dovodi do prekida ili poremećaja u dijelu energetskog sustava mogao bi potaknuti dalekosežne kaskadne učinke na druge dijelove tog sustava.

7. Pri primjeni ove Preporuke države članice trebale bi ocijeniti međuovisnosti i kritičnost sustava za proizvodnju energije i fleksibilnu potražnju, prijenosnih i distribucijskih podstanica i vodova te povezanih pogođenih dionika (uključujući prekogranične situacije) u slučaju uspješnog kibernapada ili kiberincidenta. Države članice trebale bi također osigurati da operatori energetskih mreža imaju okvir za komunikaciju sa svim ključnim dionicima radi razmjene ranih znakova upozorenja i suradnje u upravljanju kriznim situacijama. Trebalo bi uspostaviti strukturirane komunikacijske kanale i dogovorene formate za razmjenu osjetljivih informacija sa svim relevantnim dionicima, timovima za odgovor na računalne sigurnosne incidente i relevantnim tijelima.

8. Konkretno, operatori energetskih mreža trebali bi:

   (a) osigurati da novi uređaji, uključujući uređaje za internet stvari, imaju i da će održati razinu kibersigurnosti primjerenu kritičnosti lokacije;

   (b) primjereno razmotriti kiberfizičke učinke pri utvrđivanju i periodičnom preispitivanju planova kontinuiteta poslovanja;

(c) utvrditi kriterije projektiranja i arhitekturu za otpornu mrežu, što bi se moglo postići sljedećim:

— uspostavom detaljnih obrambenih mjera za svaku lokaciju, prilagođenih kritičnosti lokacije,

— utvrđivanjem kritičnih čvorišta, kako u pogledu kapaciteta proizvodnje energije tako i u pogledu utjecaja na korisnike. Ključne funkcije mreže trebale bi biti osmišljene tako da ublaže rizike koji mogu prouzročiti kaskadne učinke uzimajući u obzir redundanciju, otpornost na fazne oscilacije i zaštitu od kaskadnih ispada zbog opterećenja,

— suradnjom s drugim relevantnim operatorima i s pružateljima tehnologije radi sprečavanja kaskadnih učinaka primjenom odgovarajućih mjera i usluga,

— projektiranjem i izgradnjom komunikacijskih i kontrolnih mreža radi ograničavanja učinaka eventualnih fizičkih i logičkih kvarova na ograničenim dijelovima mreža te osiguravanja odgovarajućih i brzih mjera ublažavanja.

NASLIJEĐENA I NAJNOVIJA TEHNOLOGIJA

9. Države članice trebale bi osigurati da relevantni dionici, posebno operatori energetskih mreža i dobavljači tehnologije, a osobito operatori ključnih usluga utvrđeni u skladu s Direktivom NIS, provode odgovarajuće mjere pripravnosti u području kibersigurnosti povezane s kombinacijom naslijeđene i najnovije tehnologije u energetskom sektoru. Naime, u današnjem energetskom sustavu istodobno postoje dvije različite vrste tehnologija: starija tehnologija s vijekom trajanja od 30 do 60 godina, koja je osmišljena prije razmatranja pitanja kibersigurnosti, i moderna oprema, koja odražava najnoviju digitalizaciju i pametne uređaje.

10. Pri primjeni ove Preporuke države članice trebale bi poticati operatore energetskih mreža i dobavljače tehnologije da slijede odgovarajuće međunarodno prihvaćene norme o kibersigurnosti kad god je to moguće. U međuvremenu bi dionici i potrošači pri povezivanju uređaja s mrežom trebali primijeniti pristup usmjeren na kibersigurnost.

11. Dobavljači tehnologije posebno bi trebali osigurati ispitana rješenja za sigurnosna pitanja u naslijeđenim ili novim tehnologijama besplatno i čim se pojavi relevantan sigurnosni problem.

12. Konkretno, operatori energetskih mreža trebali bi:

(a) analizirati rizike povezivanja naslijeđenih koncepata i koncepata interneta stvari te biti svjesni unutarnjih i vanjskih sučelja i njihovih ranjivosti;

(b) poduzeti odgovarajuće mjere za obranu od zlonamjernih napada velikog broja zlonamjerno kontroliranih potrošačkih naprava ili aplikacija;

(c) uspostaviti automatsku mogućnost praćenja i analize kad je riječ o događajima povezanima sa sigurnošću u naslijeđenom okruženju i okruženju interneta stvari, kao što su neuspješni pokušaji prijavljivanja, alarmi na vratima pri otvaranju ormara ili drugi događaji;

(d) redovito provoditi posebne analize rizika u području kibersigurnosti u svim naslijeđenim postrojenjima, posebno pri povezivanju starih i novih tehnologija; budući da naslijeđena postrojenja često čine vrlo velik dio sredstava, analiza rizika može se provesti po kategorijama sredstava;

(e) ažurirati softver i hardver naslijeđenih sustava i sustava interneta stvari na najnoviju verziju kad god je to primjereno; pritom bi operatori energetskih mreža trebali razmotriti dodatne mjere, kao što su odvajanje sustava ili dodavanje vanjskih sigurnosnih prepreka, ako bi sigurnosni popravci ili ažuriranja bili odgovarajući, ali nisu mogući, primjerice za nepodržane proizvode;

(f) sastavljati javne natječaje imajući na umu kibersigurnost (tj. zahtijevati informacije o sigurnosnim značajkama, zahtijevati sukladnost s postojećim normama za kibersigurnost, osigurati stalno upozoravanje, sigurnosne popravke i prijedloge za ublažavanje ako se otkriju ranjivosti te pojasniti odgovornost prodavatelja u slučaju kibernapada ili incidenata);

(g) surađivati s dobavljačima tehnologije radi zamjene naslijeđenih sustava kad god je to korisno iz sigurnosnih razloga, ali uzeti pritom u obzir kritične funkcije sustava.

PRAĆENJE

13. Države članice trebale bi dostaviti Komisiji u roku od 12 mjeseci od donošenja ove Preporuke, a zatim svake dvije godine, detaljne informacije o stanju provedbe ove Preporuke putem Skupine za suradnju u području sigurnosti mrežnih i informacijskih sustava.

PREISPITIVANJE

14. Na temelju podataka koje dostave države članice Komisija će u dogovoru s državama članicama i relevantnim dionicima preispitivati provedbu ove Preporuke i prema potrebi procijeniti jesu li potrebne dodatne mjere.

ADRESATI

15. Ova je Preporuka upućena državama članicama.

Sastavljeno u Bruxellesu 3. travnja 2019.

Za Komisiju
Miguel ARIAS CAÑETE
Član Komisije