# PRIPOROČILA

## PRIPOROČILO KOMISIJE (EU) 2019/553

**z dne 3. aprila 2019**

**o kibernetski varnosti v energetskem sektorju**

*(notificirano pod dokumentarno številko C(2019) 2400)*

EVROPSKA KOMISIJA JE –

ob upoštevanju Pogodbe o delovanju Evropske unije in zlasti člena 292 Pogodbe,

ob upoštevanju naslednjega:

(1) Evropski energetski sektor je sredi pomembnega prehoda na razogljičeno gospodarstvo, hkrati pa zagotavlja zanesljivost oskrbe in konkurenčnost. V okviru navedenega energetskega prehoda in s tem povezane decentralizacije proizvodnje električne energije iz obnovljivih virov, tehnološkega napredka, sektorskega povezovanja in digitalizacije se evropsko elektroenergetsko omrežje spreminja v „pametno omrežje“. Hkrati to prinaša tudi nova tveganja, saj je zaradi digitalizacije energetski sistem vse bolj izpostavljen kibernetskim napadom in incidentom, ki lahko ogrozijo zanesljivo oskrbo z energijo.

(2) Sprejetje vseh osmih zakonodajnih predlogov ([1]) svežnja „Čista energija za vse Evropejce“, vključno z upravljanjem energetske unije kot odskočno desko, omogoča ustvarjanje ugodnega okolja za digitalno preobrazbo energetskega sektorja. Dogovor priznava tudi pomen kibernetske varnosti v energetskem sektorju. Prenovljena uredba o notranjem trgu električne energije ([2]) zlasti določa sprejetje tehničnih pravil za električno energijo, kot je omrežni kodeks sektorskih pravil za vidike čezmejnih pretokov električne energije, povezane s kibernetsko varnostjo, o skupnih minimalnih zahtevah, načrtovanju, spremljanju, poročanju in kriznem upravljanju. Uredba o pripravljenosti na tveganja v sektorju električne energije ([3]) na splošno sledi pristopu, ki je bil izbran v uredbi o zanesljivosti oskrbe s plinom ([4]); v njej je poudarjeno, da je treba ustrezno oceniti vsa tveganja, vključno s tveganji, povezanimi s kibernetsko varnostjo, ter predlagano sprejetje ukrepov za preprečevanje in ublažitev navedenih ugotovljenih tveganj.

(3) Ko je Komisija leta 2013 sprejela strategijo EU za kibernetsko varnost ([5]), je kot prednostno nalogo opredelila krepitev kibernetske odpornosti Unije. Eden od ključnih rezultatov navedene strategije je direktiva o varnosti omrežij in informacijskih sistemov ([6]), ki je bila sprejeta julija 2016. Direktiva o varnosti omrežij in informacijskih sistemov kot prvi akt horizontalne zakonodaje EU o kibernetski varnosti spodbuja celotno raven kibernetske varnosti v Uniji z razvojem nacionalnih zmogljivosti na področju kibernetske varnosti, povečanjem sodelovanja na ravni EU ter uvedbo obveznosti poročanja o varnosti in incidentih za podjetja, imenovana „izvajalci bistvenih storitev“. Poročanje o incidentih je obvezno v ključnih sektorjih, vključno z energetskim sektorjem.

---

([1]) Direktiva (EU) 2018/2001 Evropskega parlamenta in Sveta z dne 11. decembra 2018 o spodbujanju uporabe energije iz obnovljivih virov (UL L 328, 21.12.2018, str. 82); Direktiva (EU) 2018/2002 Evropskega parlamenta in Sveta z dne 11. decembra 2018 o spremembi Direktive 2012/27/EU o energetski učinkovitosti (UL L 328, 21.12.2018, str. 210); Uredba (EU) 2018/1999 Evropskega parlamenta in Sveta z dne 11. decembra 2018 o upravljanju energetske unije in podnebnih ukrepov, spremembi uredb (ES) št. 663/2009 in (ES) št. 715/2009 Evropskega parlamenta in Sveta, direktiv 94/22/ES, 98/70/ES, 2009/31/ES, 2009/73/ES, 2010/31/EU, 2012/27/EU in 2013/30/EU Evropskega parlamenta in Sveta, direktiv Sveta 2009/119/ES in (EU) 2015/652 ter razveljavitvi Uredbe (EU) št. 525/2013 Evropskega parlamenta in Sveta (UL L 328, 21.12.2018, str. 1); Direktiva (EU) 2018/844 Evropskega parlamenta in Sveta z dne 30. maja 2018 o spremembi Direktive 2010/31/EU o energetski učinkovitosti stavb in Direktive 2012/27/EU o energetski učinkovitosti (UL L 156, 19.6.2018, str. 75). Evropski parlament je marca 2019 na plenarnem zasedanju potrdil politične dogovore, dosežene s Svetom, o predlogih v zvezi z zasnovo trga z električno energijo (uredba o pripravljenosti na tveganja, uredba o Agenciji za sodelovanje energetskih regulatorjev (ACER) ter direktiva in uredba o električni energiji). Svet naj bi jih uradno sprejel aprila, kmalu za tem pa bodo objavljeni tudi v *Uradnem listu Evropske unije*.

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

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

([4]) Uredba (EU) 2017/1938 Evropskega parlamenta in Sveta z dne 25. oktobra 2017 o ukrepih za zagotavljanje zanesljivosti oskrbe s plinom in o razveljavitvi Uredbe (EU) št. 994/2010 (UL L 280, 28.10.2017, str. 1).

([5]) JOIN(2013) 1.

([6]) Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL L 194, 19.7.2016, str. 1).

(4) Zadevne zainteresirane strani, vključno z izvajalci bistvenih storitev v energetskem sektorju, kot so opredeljeni v direktivi o varnosti omrežij in informacijskih sistemov, bi morale pri izvajanju ukrepov za pripravljenost na področju kibernetske varnosti upoštevati horizontalne smernice, ki jih je izdala skupina za sodelovanje na področju varnosti omrežij in informacijskih sistemov, ustanovljena na podlagi člena 11 direktive o varnosti omrežij in informacijskih sistemov. Navedena skupina za sodelovanje, ki jo sestavljajo predstavniki držav članic, Agencije Evropske unije za kibernetsko varnost (ENISA) in Komisije, je sprejela dokumente s smernicami o varnostnih ukrepih in priglasitvi incidentov. Junija 2018 je vzpostavila namenski delovni postopek v zvezi z energijo.

(5) V skupnem sporočilu o kibernetski varnosti iz leta 2017 ([7]) je priznan pomen premislekov in zahtev za posamezne sektorje na ravni EU, tudi v energetskem sektorju. Kibernetska varnost in morebitne posledice za politiko so bile v Uniji v zadnjih letih predmet obsežnih razprav. Zato se danes krepi zavedanje, da se posamezni gospodarski sektorji srečujejo s specifičnimi vprašanji, povezanimi s kibernetsko varnostjo, in da morajo zato v širšem okviru splošnih strategij za kibernetsko varnost razviti lastne sektorske pristope.

(6) Na področju kibernetske varnosti sta ključna elementa izmenjava informacij in zaupanje. Komisija si prizadeva povečati izmenjavo informacij med ustreznimi zainteresiranimi stranmi z organizacijo namenskih dogodkov, kot sta bili okrogla miza na visoki ravni o kibernetski varnosti v energetiki, ki je bila organizirana marca 2017 v Rimu, in konferenca na visoki ravni o kibernetski varnosti v energetiki, ki je bila organizirana oktobra 2018 v Bruslju. Komisija želi tudi okrepiti sodelovanje med ustreznimi zainteresiranimi stranmi in specializiranimi subjekti, kot je Evropski center za izmenjavo in analizo energetskih informacij.

(7) Uredba o agenciji EU za kibernetsko varnost (ENISA) ter certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti (v nadaljnjem besedilu: uredba o kibernetski varnosti ([8])) bo okrepila mandat agencije ENISA, da bo bolje podpirala države članice pri reševanju groženj in napadov na področju kibernetske varnosti. Vzpostavlja tudi evropski okvir za kibernetsko varnost za certificiranje izdelkov, procesov in storitev, ki bo veljal v vsej Uniji in je zlasti pomemben za energetski sektor.

(8) Komisija je predložila priporočilo ([9]) o obravnavi kibernetskih tveganj na področju omrežnih tehnologij pete generacije (5G), v katerem podaja smernice za ustrezno analizo in ukrepe za obvladovanje tveganj na nacionalni ravni, za uvedbo usklajene evropske analize tveganj ter za določitev postopka vzpostavitve skupnega nabora orodij za pripravo najboljših ukrepov za obvladovanje tveganj. Na omrežjih 5G bo temeljila široka paleta storitev, ki so bistvene za delovanje notranjega trga ter ključnih družbenih in ekonomskih dejavnosti, kot je oskrba z energijo.

(9) To priporočilo bi moralo državam članicam in ustreznim zainteresiranim stranem, zlasti operaterjem omrežij in dobaviteljem tehnologije, zagotoviti neizčrpne smernice za doseganje višje stopnje kibernetske varnosti glede na specifične zahteve v realnem času, ugotovljene v energetskem sektorju, kaskadne učinke ter kombinacijo starejših in najnovejših tehnologij. Namen teh smernic je zainteresiranim stranem pomagati, da pri izvajanju mednarodno priznanih standardov kibernetske varnosti upoštevajo specifične zahteve energetskega sektorja ([10]).

(10) Komisija namerava redno pregledovati to priporočilo na podlagi napredka, doseženega v Uniji, ter v posvetovanju z državami članicami in ustreznimi zainteresiranimi stranmi. Še naprej si bo prizadevala za krepitev kibernetske varnosti v energetskem sektorju, zlasti prek skupine za sodelovanje na področju varnosti omrežij in informacijskih sistemov, ki zagotavlja strateško sodelovanje in izmenjavo informacij med državami članicami na področju kibernetske varnosti –

SPREJELA NASLEDNJE PRIPOROČILO:

**PREDMET UREJANJA**

(1) V tem priporočilu so določena glavna vprašanja v zvezi s kibernetsko varnostjo v energetskem sektorju, in sicer zahteve v realnem času, kaskadni učinki ter kombinacija starejših in najnovejših tehnologij, in opredeljeni glavni ukrepi za izvajanje ustreznih ukrepov za pripravljenost na področju kibernetske varnosti v energetskem sektorju.

([7]) JOIN(2017) 450.

([8]) Uredbo o kibernetski varnosti je Evropski parlament sprejel marca 2019. Svet naj bi jo uradno sprejel aprila; kmalu za tem bo objavljena tudi v *Uradnem listu Evropske unije*.

([9]) C(2019) 2335.

([10]) Mednarodne organizacije za standardizacijo so objavile različne standarde kibernetske varnosti (ISO/IEC 27000: Informacijska tehnologija) in standarde obvladovanja tveganja (ISO/IEC 31000: Obvladovanje tveganja). Specifičen standard za energetski sektor (ISO/IEC 27019: Kontrole informacijske varnosti za industrijo energetskih storitev) je bil oktobra 2017 izdan kot del serije ISO/IEC 27000.

(2) Države članice bi morale pri uporabi tega priporočila ustrezne zainteresirane strani spodbujati, naj razvijajo znanje in veščine v zvezi s kibernetsko varnostjo v energetskem sektorju. Po potrebi bi morale države članice te vidike vključiti tudi v svoj nacionalni okvir za kibernetsko varnost, zlasti s strategijami ter zakoni in drugimi predpisi.

**ZAHTEVE KOMPONENT ENERGETSKE INFRASTRUKTURE V REALNEM ČASU**

(3) Države članice bi morale zagotoviti, da ustrezne zainteresirane strani, zlasti operaterji energetskih omrežij in dobavitelji tehnologije, predvsem pa izvajalci bistvenih storitev, opredeljeni v direktivi o varnosti omrežij in informacijskih sistemov, izvajajo ustrezne ukrepe za pripravljenost na področju kibernetske varnosti, povezane z zahtevami v energetskem sektorju v realnem času. Nekateri elementi energetskega sistema morajo delovati v „realnem času“, kar pomeni, da se morajo odzvati na ukaze v nekaj milisekundah, zato je zaradi pomanjkanja časa ukrepe za kibernetsko varnost težko ali celo nemogoče uvesti.

(4) Zlasti bi morali operaterji energetskih omrežij:

(a) uporabiti najnovejše varnostne standarde za nove obrate, kadar je to primerno, in razmisliti o dopolnilnih fizičnih varnostnih ukrepih, kadar nameščenih baz starih obratov ni mogoče zadostno zaščititi z mehanizmi za kibernetsko varnost;

(b) izvajati mednarodne standarde kibernetske varnosti in ustrezne posebne tehnične standarde za varno komunikacijo v realnem času, takoj ko zadevni proizvodi postanejo komercialno dostopni;

(c) upoštevati omejitve v realnem času v splošnem varnostnem konceptu za sredstva, zlasti pri razvrščanju sredstev;

(d) razmisliti o omrežjih za sheme zaščite na daljavo v zasebni lasti, da bi se zagotovila kakovost storitev, zahtevana za omejitve v realnem času; operaterji bi morali pri uporabi javnih komunikacijskih omrežij razmisliti o zagotavljanju dodeljevanja specifičnih pasovnih širin, zahtev glede latence in ukrepih za varno komunikacijo;

(e) razdeliti celoten sistem na logična območja ter znotraj vsakega območja opredeliti časovne in procesne omejitve, da bi se omogočila uporaba ustreznih ukrepov za kibernetsko varnost, ali razmisliti o alternativnih zaščitnih metodah.

(5) Kadar je na voljo, bi morali operaterji energetskih omrežij tudi:

(a) izbrati varen komunikacijski protokol ob upoštevanju zahtev v realnem času, na primer med obratom in njegovimi sistemi upravljanja (sistem upravljanja z energijo/upravljanje distribucijskega sistema);

(b) uvesti ustrezen mehanizem avtentikacije za komunikacijo stroj–stroj, ki obravnava zahteve v realnem času.

**KASKADNI UČINKI**

(6) Države članice bi morale zagotoviti, da ustrezne zainteresirane strani, zlasti operaterji energetskih omrežij in dobavitelji tehnologije, predvsem pa izvajalci bistvenih storitev, opredeljeni v direktivi o varnosti omrežij in informacijskih sistemov, izvajajo ustrezne ukrepe za pripravljenost na področju kibernetske varnosti, povezane s kaskadnimi učinki v energetskem sektorju. Električna omrežja in plinovodi po vsej Evropi so močno povezani, zato lahko kibernetski napad, ki povzroči izpad ali motnje v enem delu energetskega sistema, sproži daljnosežne kaskadne učinke v drugih delih navedenega sistema.

(7) Države članice bi morale na podlagi tega priporočila oceniti medsebojne odvisnosti ter kritičnost sistemov za proizvodnjo električne energije in sistemov prilagodljivega odjema, prenosnih in distribucijskih razdelilnih transformacijskih postaj in vodov ter s tem povezanih prizadetih zainteresiranih strani (vključno s čezmejnimi primeri) v primeru uspešnega kibernetskega napada ali kibernetskega incidenta. Zagotoviti bi morale tudi, da imajo operaterji energetskih omrežij z vsemi ključnimi zainteresiranimi stranmi komunikacijski okvir za izmenjavo zgodnjih opozorilnih znakov in sodelovanje pri kriznem upravljanju. Vzpostavljeni bi morali biti strukturirani komunikacijski kanali in dogovorjeni formati za izmenjavo občutljivih informacij z vsemi ustreznimi zainteresiranimi stranmi, skupinami za odzivanje na incidente na področju računalniške varnosti in ustreznimi organi.

(8) Zlasti bi morali operaterji energetskih omrežij:

(a) zagotoviti, da je raven kibernetske varnosti novih naprav, vključno z napravami v internetu stvari, primerna glede na kritičnost lokacije in da bo taka tudi ostala;

(b) pri pripravi in rednem pregledovanju načrtov neprekinjenega poslovanja ustrezno upoštevati kibernetsko-fizične učinke;

(c) določiti merila za načrtovanje in arhitekturo za odporno omrežje, kar bi bilo mogoče doseči z:

— vzpostavitvijo ukrepov poglobljene zaščite na posamezni lokaciji, ki so prilagojeni kritičnosti lokacije,

— opredelitvijo kritičnih vozlišč, tako glede zmogljivosti za proizvodnjo električne energije kot učinka na stranko; kritične funkcije omrežja bi morale biti zasnovane tako, da zmanjšajo tveganje, ki lahko povzroči kaskadne učinke, in sicer z upoštevanjem redundance, odpornosti proti faznim nihanjem in zaščite pred kaskadno prekinitvijo obremenitve,

— sodelovanjem z drugimi ustreznimi operaterji in dobavitelji tehnologije, da bi se z uporabo ustreznih ukrepov in storitev preprečili kaskadni učinki,

— načrtovanjem in izgradnjo komunikacijskih in nadzornih omrežij, da bi se učinki kakršnih koli fizičnih in logičnih napak omejili na omejene dele omrežij ter da bi se zagotovili ustrezni in hitri blažitveni ukrepi.

**STAREJŠA IN NAJNOVEJŠA TEHNOLOGIJA**

(9) Države članice bi morale zagotoviti, da ustrezne zainteresirane strani, zlasti operaterji energetskih omrežij in dobavitelji tehnologije, predvsem pa izvajalci bistvenih storitev, opredeljeni v direktivi o varnosti omrežij in informacijskih sistemov, izvajajo ustrezne ukrepe za pripravljenost na področju kibernetske varnosti, povezane s kombinacijo starejše in najnovejše tehnologije v energetskem sektorju. Dejansko v sedanjem energetskem sistemu soobstajata dve različni vrsti tehnologij: starejša tehnologija z življenjsko dobo od 30 do 60 let, ki je bila zasnovana pred premisleki o kibernetski varnosti, in sodobna oprema z najnovejšo digitalizacijo in pametnimi napravami.

(10) Države članice bi morale na podlagi tega priporočila operaterje energetskih omrežij in dobavitelje tehnologije spodbujati, naj upoštevajo ustrezne mednarodno sprejete standarde kibernetske varnosti, kadar je to mogoče. Medtem bi morale zainteresirane strani in stranke pri povezovanju naprav z omrežjem sprejeti pristop, usmerjen v kibernetsko varnost.

(11) Zlasti bi morali dobavitelji tehnologije preizkušene rešitve za varnostna vprašanja v zvezi s starejšimi ali novimi tehnologijami zagotoviti brezplačno in takoj, ko ustrezno varnostno vprašanje postane znano.

(12) Zlasti bi morali operaterji energetskih omrežij:

(a) analizirati tveganja povezovanja starejših konceptov in konceptov interneta stvari ter poznavati notranje in zunanje vmesnike in njihove ranljivosti;

(b) sprejeti ustrezne ukrepe proti zlonamernim napadom, ki izvirajo iz velikega števila zlonamerno upravljanih potrošniških naprav ali aplikacij;

(c) vzpostaviti avtomatizirane zmogljivosti za spremljanje in analizo dogodkov, povezanih z varnostjo, v starejših okoljih in okolju interneta stvari, kot so neuspešni poskusi prijave, sprožitev alarma za vrata v primeru odpiranja omaric ali drugi dogodki.

(d) redno izvajati specifične analize tveganja v zvezi s kibernetsko varnostjo v vseh starejših obratih, zlasti pri povezovanju starih in novih tehnologij; starejši obrati pogosto predstavljajo zelo veliko sredstev, zato se lahko analiza tveganja izvede po skupinah sredstev;

(e) posodabljati programsko in strojno opremo starejših sistemov in sistemov interneta stvari na najnovejšo različico, kadar koli je to primerno; pri tem bi morali operaterji energetskih omrežij razmisliti o dopolnilnih ukrepih, kot so ločevanje med sistemi ali dodajanje zunanjih varnostnih ovir, kadar bi nameščanje popravkov ali posodabljanje sicer zadoščalo, vendar ga ni mogoče izvesti, na primer pri nepodprtih izdelkih;

(f) razpise oblikovati ob upoštevanju kibernetske varnosti, tj. zahtevati informacije o varnostnih značilnostih in skladnost z obstoječimi standardi kibernetske varnosti, zagotavljati stalno obveščanje, nameščanje popravkov in predloge za blažitev, če se odkrijejo ranljivosti, ter pojasniti odgovornost dobavitelja v primeru kibernetskih napadov ali incidentov;

(g) sodelovati z dobavitelji tehnologije za nadomestitev starejših sistemov, kadar koli je to koristno iz varnostnih razlogov, vendar upoštevati kritične funkcionalnosti sistema.

**SPREMLJANJE**

(13) Države članice bi morale Komisiji v 12 mesecih po sprejetju tega priporočila in nato vsaki dve leti prek skupine za sodelovanje na področju varnosti omrežij in informacijskih sistemov sporočiti podrobne informacije o stanju izvajanja tega priporočila.

**PREGLED**

(14) Komisija bo na podlagi informacij, ki jih predložijo države članice, pregledala izvajanje tega priporočila ter po potrebi v posvetovanju z državami članicami in ustreznimi zainteresiranimi stranmi ocenila, ali so potrebni nadaljnji ukrepi.

**NASLOVNIKI**

(15) To priporočilo je naslovljeno na države članice.

V Bruslju, 3. aprila 2019

*Za Komisijo*
Miguel ARIAS CAÑETE
*Član Komisije*