ODPORÚČANIA

ODPORÚČANIE KOMISIE (EÚ) 2019/553

z 3. apríla 2019

o kybernetickej bezpečnosti v odvetví energetiky

[oznámené pod číslom C(2019) 2400]

EURÓPSKA KOMISIA,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 292,

keďže:

(1) Európske odvetvie energetiky prechádza dôležitou zmenou, ktorá smeruje k dekarbonizovanému hospodárstvu, pričom zároveň zaisťuje bezpečnosť dodávok energie a konkurencieschopnosť. Ako súčasť tohto energetického prechodu a súvisiacej decentralizácie výroby elektriny z obnoviteľných zdrojov energie, technologický pokrok, prepájanie odvetví a digitalizácia menia elektrickú sieť Európy na „inteligentnú sieť". Súčasne to však prináša nové riziká, keďže digitalizácia čoraz viac vystavuje energetický systém kybernetickým útokom a incidentom, ktoré môžu ohroziť bezpečnosť dodávok energie.

(2) Prijatie všetkých ôsmich legislatívnych návrhov ([1]) balíka opatrení v oblasti čistej energie pre všetkých Európanov vrátane riadenia energetickej únie ako odrazového mostíka umožňuje vytvoriť priaznivé prostredie pre digitálnu transformáciu odvetvia energetiky. Uznáva tiež dôležitosť kybernetickej bezpečnosti v odvetví energetiky. Najmä v prepracovanom znení nariadenia o vnútornom trhu s elektrinou ([2]) sa stanovuje prijatie technických pravidiel pre elektrinu ako napr. sieťového predpisu o osobitných odvetvových pravidlách týkajúcich sa aspektov kybernetickej bezpečnosti pri cezhraničných tokoch elektriny, o spoločných minimálnych požiadavkách, plánovaní, monitorovaní, podávaní správ a krízovom riadení. Nariadenie o pripravenosti na riziká v oblasti elektrickej energie ([3]) vo všeobecnosti nadväzuje na prístup zvolený v nariadení o bezpečnosti dodávok plynu ([4]); zdôrazňuje potrebu riadne posúdiť všetky riziká vrátane tých, ktoré súvisia s kybernetickou bezpečnosťou, a navrhnúť prijatie opatrení na predchádzanie týmto zisteným rizikám a na ich zmiernenie.

(3) Keď Komisia prijala stratégiu kybernetickej bezpečnosti Európskej únie ([5]) v roku 2013, posilnenie kybernetickej odolnosti Únie stanovila ako prioritu. Jedným z kľúčových výsledkov stratégie je smernica o bezpečnosti sietí a informačných systémov ([6]) (ďalej len „smernica NIS"), ktorá bola prijatá v júli 2016. Ako prvý horizontálny právny predpis EÚ o kybernetickej bezpečnosti smernica NIS zvyšuje celkovú úroveň kybernetickej bezpečnosti v Únii prostredníctvom rozvoja vnútroštátnych spôsobilostí v oblasti kybernetickej bezpečnosti, zvýšenia spolupráce na úrovni EÚ a zavedenia povinnosti oznamovania bezpečnosti a incidentov pre spoločnosti nazývané „prevádzkovatelia základných služieb". Oznamovanie incidentov je povinné v kľúčových odvetviach vrátane odvetvia energetiky.

([1]) Smernica Európskeho parlamentu a Rady (EÚ) 2018/2001 z 11. decembra 2018 o podpore využívania energie z obnoviteľných zdrojov (Ú. v. EÚ L 328, 21.12.2018, s. 82); smernica Európskeho parlamentu a Rady (EÚ) 2018/2002 z 11. decembra 2018, ktorou sa mení smernica 2012/27/EÚ o energetickej efektívnosti (Ú. v. EÚ L 328, 21.12.2018, s. 210); nariadenie Európskeho parlamentu a Rady (EÚ) 2018/1999 z 11. decembra 2018 o riadení energetickej únie a opatrení v oblasti klímy, ktorým sa menia nariadenia Európskeho parlamentu a Rady (ES) č. 663/2009 a (ES) č. 715/2009, smernice Európskeho parlamentu a Rady 94/22/ES, 98/70/ES, 2009/31/ES, 2009/73/ES, 2010/31/EÚ, 2012/27/EÚ a 2013/30/EÚ, smernice Rady 2009/119/ES a (EÚ) 2015/652 a ktorým sa zrušuje nariadenie Európskeho parlamentu a Rady (EÚ) č. 525/2013 (Ú. v. EÚ L 328, 21.12.2018, s. 1); smernica Európskeho parlamentu a Rady (EÚ) 2018/844 z 30. mája 2018, ktorou sa mení smernica 2010/31/EÚ o energetickej hospodárnosti budov a smernica 2012/27/EÚ o energetickej efektívnosti (Ú. v. EÚ L 156, 19.6.2018, s. 75). Európsky parlament potvrdil politické dohody s Radou týkajúce sa návrhov koncepcie trhu s elektrinou [nariadenie o pripravenosti na riziká, nariadenie týkajúce sa Agentúry pre spoluprácu regulačných orgánov v oblasti energetiky (ACER), smernica o elektrine a nariadenie o elektrine] na plenárnom zasadnutí v marci 2019. Formálne prijatie Radou sa očakáva v apríli; čoskoro potom bude nasledovať uverejnenie právneho textu v úradnom vestníku.

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

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

([4]) Nariadenie Európskeho parlamentu a Rady (EÚ) 2017/1938 z 25. októbra 2017 o opatreniach na zaistenie bezpečnosti dodávok plynu a o zrušení nariadenia (EÚ) č. 994/2010 (Ú. v. EÚ L 280, 28.10.2017, s. 1).

([5]) JOIN(2013) 1.

([6]) Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (Ú. v. EÚ L 194, 19.7.2016, s. 1).

(4) Pri vykonávaní opatrení týkajúcich sa pripravenosti v oblasti kybernetickej bezpečnosti by mali príslušné zainteresované strany vrátane prevádzkovateľov základných energetických služieb podľa smernice NIS zohľadniť horizontálne usmernenie vydané skupinou pre spoluprácu v oblasti bezpečnosti sietí a informačných systémov zriadenou podľa článku 11 smernice NIS. Táto skupina pre spoluprácu, ktorú tvoria zástupcovia členských štátov, Agentúry Európskej únie pre kybernetickú bezpečnosť (ďalej len „ENISA“) a Komisie, prijala usmernenia týkajúce sa bezpečnostných opatrení a oznamovania incidentov. V júni 2018 skupina vytvorila samostatný pracovný okruh týkajúci sa energetiky.

(5) V spoločnom oznámení o kybernetickej bezpečnosti ([7]) z roku 2017 sa uznáva dôležitosť úvah a požiadaviek špecifických pre dané odvetvie na úrovni EÚ vrátane odvetvia energetiky. Kybernetická bezpečnosť a možné politické dôsledky sú v posledných rokoch predmetom rozsiahlej diskusie v Únii. V dôsledku tejto diskusie sa v súčasnosti zvyšuje povedomie o tom, že jednotlivé hospodárske odvetvia čelia špecifickým otázkam v oblasti kybernetickej bezpečnosti, a preto potrebujú rozvíjať vlastné odvetvové prístupy v širšom kontexte všeobecných stratégií kybernetickej bezpečnosti.

(6) Výmena informácií a dôvera sú kľúčovými prvkami kybernetickej bezpečnosti. Cieľom Komisie je zvýšiť výmenu informácií medzi príslušnými zainteresovanými stranami prostredníctvom organizovania osobitných podujatí, ako boli okrúhly stôl na vysokej úrovni o kybernetickej bezpečnosti v energetike organizovaný v Ríme v marci 2017 a konferencia na vysokej úrovni o kybernetickej bezpečnosti v energetike organizovaná v Bruseli v októbri 2018. Komisia chce tiež posilniť spoluprácu medzi príslušnými zainteresovanými stranami a špecializovanými subjektmi, ako je napríklad Európske stredisko pre výmenu a analýzu informácií v oblasti energetiky.

(7) Nariadenie o Agentúre EÚ pre kybernetickú bezpečnosť (agentúra ENISA) a certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií („nariadenie o kybernetickej bezpečnosti“) ([8]) posilní mandát Agentúry EÚ pre kybernetickú bezpečnosť s cieľom lepšie podporovať členské štáty pri riešení kybernetických hrozieb a útokov. Vytvára tiež európsky rámec kybernetickej bezpečnosti pre certifikáciu výrobkov, postupov a služieb, ktorý bude platný v celej Únii a má osobitný význam pre odvetvie energetiky.

(8) Komisia predložila odporúčanie ([9]) týkajúce sa rizík v oblasti kybernetickej bezpečnosti v prípade sieťových technológií 5. generácie (5G) a stanoví na tieto účely usmernenia o vhodných analýzach rizík a opatreniach na riadenie rizík na vnútroštátnej úrovni, o vypracovaní koordinovanej európskej analýzy rizík a o vytvorení postupu na vypracovanie spoločného súboru najlepších opatrení na riadenie rizík. Po svojom zavedení budú siete 5G tvoriť základ širokej škály služieb, ktoré sú nevyhnutné pre fungovanie vnútorného trhu a vykonávanie dôležitých spoločenských a hospodárskych funkcií, ako je energetika.

(9) Toto odporúčanie by malo poskytnúť členským štátom a príslušným zainteresovaným stranám, najmä prevádzkovateľom sietí a dodávateľom technológií, demonštratívne usmernenie na dosiahnutie vyššej úrovne kybernetickej bezpečnosti vzhľadom na osobitné požiadavky v reálnom čase stanovené pre odvetvie energetiky, kaskádové efekty a kombináciu starších a najmodernejších technológií. Cieľom tohto usmernenia je pomôcť zainteresovaným stranám zohľadniť osobitné požiadavky odvetvia energetiky pri vykonávaní medzinárodne uznávaných noriem v oblasti kybernetickej bezpečnosti ([10]).

(10) Komisia má v úmysle pravidelne preskúmavať toto odporúčanie na základe pokroku dosiahnutého v celej Únii po konzultácii s členskými štátmi a príslušnými zainteresovanými stranami. Komisia bude naďalej pokračovať vo svojom úsilí o posilnenie kybernetickej bezpečnosti v odvetví energetiky, najmä prostredníctvom skupiny pre spoluprácu v oblasti bezpečnosti sietí a informačných systémov, ktorá zabezpečí strategickú spoluprácu a výmenu informácií medzi členskými štátmi v oblasti kybernetickej bezpečnosti,

PRIJALA TOTO ODPORÚČANIE:

PREDMET

1. V tomto odporúčaní sa stanovujú hlavné problémy týkajúce sa kybernetickej bezpečnosti v odvetví energetiky, konkrétne požiadavky v reálnom čase, kaskádové efekty a kombinácie starších a najmodernejších technológií a určujú sa hlavné postupy na vykonávanie príslušných opatrení týkajúcich sa pripravenosti v oblasti kybernetickej bezpečnosti v odvetví energetiky.

([7]) JOIN(2017) 450.

([8]) Európsky parlament prijal akt o kybernetickej bezpečnosti v marci 2019. Formálne prijatie Radou sa očakáva v apríli; čoskoro potom bude nasledovať uverejnenie právneho textu v úradnom vestníku.

([9]) C(2019) 2335.

([10]) Medzinárodná organizácia pre normalizáciu uverejnila viaceré normy v oblasti kybernetickej bezpečnosti (ISO/IEC 27000: Informačné technológie) a normy riadenia rizík (ISO/IEC31000: Vykonávanie riadenia rizík). Osobitná norma pre odvetvie energetiky (ISO/IEC 27019: Kontroly bezpečnosti informácií pre energetický priemysel) bola vydaná ako súčasť série ISO/IEC 27000 v októbri 2017.

2. Pri vykonávaní tohto odporúčania by členské štáty mali povzbudiť príslušné zainteresované strany, aby rozvíjali znalosti a zručnosti súvisiace s kybernetickou bezpečnosťou v odvetví energetiky. V prípade potreby by členské štáty mali zahrnúť tieto úvahy aj do svojho vnútroštátneho rámca pre kybernetickú bezpečnosť, najmä prostredníctvom stratégií, zákonov, iných právnych predpisov a správnych opatrení.

POŽIADAVKY ZLOŽIEK ENERGETICKEJ INFRAŠTRUKTÚRY V REÁLNOM ČASE

3. Členské štáty by mali zabezpečiť, aby príslušné zainteresované strany, predovšetkým prevádzkovatelia energetických sietí a dodávatelia technológií, a najmä prevádzkovatelia základných energetických služieb podľa smernice NIS, vykonávali príslušné opatrenia týkajúce sa pripravenosti v oblasti kybernetickej bezpečnosti v súvislosti s požiadavkami v odvetví energetiky v reálnom čase. Niektoré prvky energetického systému musia fungovať v „reálnom čase“, to znamená reagovať na príkazy v priebehu niekoľkých milisekúnd, čo spôsobuje, že zavedenie opatrení v oblasti kybernetickej bezpečnosti je z dôvodu nedostatku času náročné alebo dokonca nemožné.

4. Prevádzkovatelia energetických sietí by mali najmä:

   a) uplatňovať najnovšie bezpečnostné normy pre nové zariadenia všade, kde je to primerané, a zvážiť doplnkové opatrenia fyzickej bezpečnosti tam, kde zavedené staré zariadenia nemôžu byť dostatočne chránené mechanizmami kybernetickej bezpečnosti;

   b) uplatňovať medzinárodné normy v oblasti kybernetickej bezpečnosti a primerané osobitné technické normy pre zabezpečenú komunikáciu v reálnom čase, hneď ako sa príslušné výrobky stanú komerčne dostupné;

   c) zvážiť obmedzenia v reálnom čase v celkovej bezpečnostnej koncepcii pre aktíva, najmä pri klasifikácii aktív;

   d) zvážiť použitie sietí v súkromnom vlastníctve pre systémy ochrany na diaľku, aby sa zabezpečila kvalita úrovne služieb požadovaná v súvislosti s obmedzeniami v reálnom čase; pri využívaní verejných komunikačných sietí by prevádzkovatelia mali zvážiť zabezpečenie osobitného prideľovania šírky pásma, požiadavky na oneskorenie a komunikačné bezpečnostné opatrenia;

   e) rozdeliť celkový systém na logické zóny a v rámci každej zóny definovať časové a procesné obmedzenia s cieľom umožniť uplatňovanie vhodných opatrení v oblasti kybernetickej bezpečnosti alebo zvážiť alternatívne spôsoby ochrany.

5. Ak je to možné, prevádzkovatelia energetických sietí by takisto mali:

   a) zvoliť zabezpečený komunikačný protokol, ktorý zohľadní požiadavky v reálnom čase, napríklad medzi zariadením a jeho systémami riadenia (systém energetického manažérstva/systém riadenia distribúcie);

   b) zaviesť vhodný mechanizmus autentifikácie pre komunikáciu medzi strojmi, ktorý rieši požiadavky v reálnom čase.

KASKÁDOVÉ EFEKTY

6. Členské štáty by mali zabezpečiť, aby príslušné zainteresované strany, predovšetkým prevádzkovatelia energetických sietí a dodávatelia technológií, a najmä prevádzkovatelia základných energetických služieb podľa smernice NIS, vykonávali príslušné opatrenia týkajúce sa pripravenosti v oblasti kybernetickej bezpečnosti v súvislosti s kaskádovými efektmi v odvetví energetiky. Elektrizačné sústavy a plynovody sú v celej Európe silne prepojené a kybernetický útok, ktorý spôsobí odstávku alebo prerušenie v časti energetického systému, by mohol spustiť ďalekosiahle kaskádové efekty v ďalších častiach tohto systému.

7. Pri vykonávaní tohto odporúčania by členské štáty mali zhodnotiť vzájomnú prepojenosť a dôležitosť systémov výroby elektriny a pružného dopytu, prenosových a distribučných rozvodní a vedení a príslušných dotknutých zainteresovaných strán (vrátane cezhraničných prípadov) v prípade úspešného kybernetického útoku alebo kybernetického incidentu. Členské štáty by takisto mali zabezpečiť, aby prevádzkovatelia energetických sietí mali komunikačný rámec so všetkými kľúčovými zainteresovanými stranami, aby si navzájom mohli poskytovať včasné varovné signály a spolupracovať na krízovom riadení. Mali by byť zavedené štruktúrované komunikačné kanály a dohodnuté formáty s cieľom poskytovať citlivé informácie všetkým príslušným zainteresovaným stranám, jednotkám pre riešenie počítačových bezpečnostných incidentov a príslušným orgánom.

8. Prevádzkovatelia energetických sietí by mali najmä:

   a) zabezpečiť, aby nové zariadenia vrátane zariadení internetu vecí mali a dodržiavali úroveň kybernetickej bezpečnosti, ktorá je primeraná dôležitosti lokality;

   b) primerane zvážiť kyberneticko-fyzické účinky pri stanovení a pravidelnom preskúmaní plánu na zabezpečenie kontinuity činností;

c) stanoviť kritériá projektovania a architektúru pre odolnú sieť, čo sa môže dosiahnuť:

— zavedením hĺbkových obranných opatrení pre jednotlivé lokality, ktoré by boli prispôsobené dôležitosti lokality;

— určením kritických uzlov z hľadiska kapacity výroby elektriny, ako aj z hľadiska vplyvu na odberateľa; kritické funkcie siete by mali byť navrhnuté tak, aby zmierňovali riziká, ktoré by mohli mať kaskádový efekt tým, že sa vezme do úvahy nadbytočnosť, odolnosť voči fázovej oscilácii a ochrana proti kaskádovému odpojeniu zaťaženia;

— spoluprácou s inými príslušnými prevádzkovateľmi a dodávateľmi technológií na zabránenie kaskádovému efektu prostredníctvom uplatňovania vhodných opatrení a služieb;

— navrhovaním a budovaním komunikačných a kontrolných sietí s cieľom obmedziť účinky akýchkoľvek fyzických a logických porúch na obmedzené časti sietí a zabezpečením primeraných a rýchlych zmierňujúcich opatrení.

STARŠIE A NAJMODERNEJŠIE TECHNOLÓGIE

9. Členské štáty by mali zabezpečiť, aby príslušné zainteresované strany, predovšetkým prevádzkovatelia energetických sietí a dodávatelia technológií, a najmä prevádzkovatelia základných energetických služieb podľa smernice NIS, vykonávali príslušné opatrenia týkajúce sa pripravenosti v oblasti kybernetickej bezpečnosti v súvislosti s kombináciou starších a najmodernejších technológií v odvetví energetiky. V dnešnom energetickom systéme totiž existujú naraz dva odlišné typy technológií: staršia technológia, ktorá má 30 až 60 rokov a ktorá bola navrhnutá pred tým, ako sa začalo uvažovať o kybernetickej bezpečnosti, a moderné zariadenia, ktoré odzrkadľujú najmodernejšiu digitalizáciu a inteligentné zariadenia.

10. Pri vykonávaní tohto odporúčania by členské štáty mali podporovať prevádzkovateľov energetických sietí a dodávateľov technológií, aby vždy, keď je to možné, dodržiavali príslušné medzinárodne uznávané normy v oblasti kybernetickej bezpečnosti. Zainteresované strany a odberatelia by medzitým mali pri pripájaní zariadení do siete postupovať tak, aby sa zamerali na kybernetickú bezpečnosť.

11. Najmä dodávatelia technológií by mali bezplatne poskytovať overené riešenia pre bezpečnostné otázky týkajúce sa starších alebo najmodernejších technológií, hneď ako sa príslušný bezpečnostný problém objaví.

12. Prevádzkovatelia energetických sietí by mali najmä:

a) analyzovať riziká spájania starších koncepcií a koncepcií internetu vecí a byť si vedomí interných a externých rozhraní a ich zraniteľných miest;

b) prijať vhodné opatrenia proti škodlivým útokom, ktoré pochádzajú z veľkého počtu spotrebiteľských zariadení alebo aplikácií riadených so zlým úmyslom;

c) zaviesť automatizované monitorovanie a analýzu prípadov súvisiacich s bezpečnosťou v starších prostrediach a prostredí internetu vecí, ako sú neúspešné pokusy o prihlásenie, poplachy v prípade otvorenia dverí rozvodnej skrinky alebo iné prípady;

d) pravidelne vykonávať špecifickú analýzu rizík pre kybernetickú bezpečnosť na všetkých starších zariadeniach, najmä pri prepájaní starých a nových technológií; keďže staršie zariadenia často predstavujú veľmi veľký počet aktív, analýza rizík sa môže vykonať podľa skupín aktív;

e) aktualizovať softvér a hardvér starších systémov a systémov internetu vecí na najnovšiu verziu vždy, keď je to primerané; prevádzkovatelia energetických sietí by pritom mali zvážiť doplnkové opatrenia, ako je oddelenie systémov alebo pridanie vonkajších bezpečnostných bariér tam, kde by oprava alebo aktualizácia bola primeraná, ale nie je možná, napríklad v prípade nepodporovaných výrobkov;

f) formulovať ponuky vzhľadom na kybernetickú bezpečnosť, teda požadovať informácie o bezpečnostných prvkoch, požadovať súlad s existujúcimi normami pre kybernetickú bezpečnosť, zabezpečiť neustále výstrahy, opravy a návrhy na zmiernenie v prípade zistenia zraniteľných miest a objasniť zodpovednosť predajcu v prípade kybernetických útokov alebo incidentov;

g) spolupracovať s dodávateľmi technológií, aby sa nahradili staršie systémy vždy, keď je to z bezpečnostných dôvodov prospešné, ale zohľadniť kritické systémové funkcie.

MONITOROVANIE

13. Členské štáty by mali Komisii do 12 mesiacov po prijatí tohto odporúčania a následne každé dva roky oznámiť podrobné informácie o stave vykonávania tohto odporúčania prostredníctvom skupiny pre spoluprácu v oblasti bezpečnosti sietí a informačných systémov.

PRESKÚMANIE

14. Komisia na základe informácií poskytnutých členskými štátmi preskúma vykonávanie tohto odporúčania a po konzultácii s členskými štátmi a príslušnými zainteresovanými stranami posúdi, či sú prípadne potrebné ďalšie opatrenia.

ADRESÁTI

15. Toto odporúčanie je určené členským štátom.

V Bruseli 3. apríla 2019

Za Komisiu
Miguel ARIAS CAÑETE
člen Komisie