DOPORUČENÍ

DOPORUČENÍ KOMISE (EU) 2019/553

ze dne 3. dubna 2019

o kybernetické bezpečnosti v odvětví energetiky

(oznámeno pod číslem C(2019) 2400)

EVROPSKÁ KOMISE,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 292 této smlouvy,

vzhledem k těmto důvodům:

(1) Evropské odvětví energetiky prochází důležitým přechodem na dekarbonizované hospodářství, přičemž se snaží zajistit bezpečnost dodávek energie a konkurenceschopnost. V rámci této transformace energetiky a související decentralizace výroby energie z obnovitelných zdrojů proměňuje technologický pokrok, integrace odvětví a digitalizace elektrickou síť Evropy v „inteligentní síť". Zároveň přináší nová rizika, jelikož digitalizace čím dál více vystavuje energetický systém kybernetickým útokům a incidentům, které mohou ohrozit bezpečnost dodávek energie.

(2) Přijetí všech osmi legislativních návrhů ([1]) v balíčku „Čistá energie pro všechny Evropany", jehož významnou součástí je i správa energetické unie, umožňuje vytvořit pro digitální transformaci odvětví energetiky příznivé podmínky. Rovněž uznává důležitost kybernetické bezpečnosti v tomto odvětví. Zejména přepracované znění nařízení o vnitřním trhu s elektřinou ([2]) upravuje přijímání technických pravidel pro elektřinu, jako je kodex sítě pro odvětvová pravidla týkající se aspektů kybernetické bezpečnosti v rámci přeshraničních toků elektřiny, pro společné minimální požadavky, plánování, monitorování, podávání zpráv a krizové řízení. Nařízení o rizikové připravenosti v odvětví elektřiny ([3]) se obecně řídí přístupem zvoleným v nařízení o bezpečnosti dodávek zemního plynu ([4]), přičemž klade důraz na to, že je třeba řádně posoudit všechna rizika, včetně rizik spojených s kybernetickou bezpečností, a navrhuje přijetí opatření za účelem prevence a zmírnění těchto zjištěných rizik.

(3) Když Komise přijala v roce 2013 strategii kybernetické bezpečnosti EU ([5]), určila jako prioritu posílení kybernetické odolnosti Unie. Jedním z klíčových výstupů této strategie je směrnice o bezpečnosti sítí a informací ([6]), která byla přijata v červenci 2016. Tato směrnice coby první horizontální právní předpis EU týkající se kybernetické bezpečnosti posiluje celkovou úroveň kybernetické bezpečnosti v Unii, a to rozvojem vnitrostátních schopností v oblasti kybernetické bezpečnosti, prohloubením spolupráce na úrovni EU a zavedením povinností v oblasti bezpečnosti a hlášení incidentů pro společnosti označené jako „provozovatelé základních služeb". Hlášení incidentů je povinné v klíčových odvětvích, mezi něž patří i odvětví energetiky.

([1]) Směrnice Evropského parlamentu a Rady (EU) 2018/2001 ze dne 11. prosince 2018 o podpoře využívání energie z obnovitelných zdrojů (Úř. věst. L 328, 21.12.2018, s. 82), směrnice Evropského parlamentu a Rady (EU) 2018/2002 ze dne 11. prosince 2018, kterou se mění směrnice 2012/27/EU o energetické účinnosti (Úř. věst. L 328, 21.12.2018, s. 210), nařízení Evropského parlamentu a Rady (EU) 2018/1999 ze dne 11. prosince 2018 o správě energetické unie a opatření v oblasti klimatu, kterým se mění nařízení Evropského parlamentu a Rady (ES) č. 663/2009 a (ES) č. 715/2009, směrnice Evropského parlamentu a Rady 94/22/ES, 98/70/ES, 2009/31/ES, 2009/73/ES, 2010/31/EU, 2012/27/EU a 2013/30/EU, směrnice Rady 2009/119/ES a (EU) 2015/652 a zrušuje nařízení Evropského parlamentu a Rady (EU) č. 525/2013 (Úř. věst. L 328, 21.12.2018, s. 1), směrnice Evropského parlamentu a Rady (EU) 2018/844 ze dne 30. května 2018, kterou se mění směrnice 2010/31/EU o energetické náročnosti budov a směrnice 2012/27/EU o energetické účinnosti (Úř. věst. L 156, 19.6.2018, s. 75). Evropský parlament potvrdil politické dohody dosažené s Radou ohledně návrhů na uspořádání trhu s elektřinou (nařízení o rizikové připravenosti, nařízení o agentuře pro spolupráci energetických regulačních orgánů (ACER), směrnice o elektřině a nařízení o elektřině) na plenárním zasedání v březnu 2019. Formální přijetí Radou se očekává v dubnu, brzy poté bude následovat zveřejnění právního textu v Úředním věstníku.

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

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

([4]) Nařízení Evropského parlamentu a Rady (EU) 2017/1938 ze dne 25. října 2017 o opatřeních na zajištění bezpečnosti dodávek zemního plynu a o zrušení nařízení (EU) č. 994/2010 (Úř. věst. L 280, 28.10.2017, s. 1).

([5]) JOIN(2013) 1.

([6]) Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Úř. věst. L 194, 19.7.2016, s. 1).

(4) Při provádění opatření pro zajištění připravenosti v oblasti kybernetické bezpečnosti by příslušné zúčastněné strany, včetně provozovatelů základních služeb v energetice určených podle směrnice o bezpečnosti sítí a informací, měly zohlednit horizontální pokyny vydané skupinou pro spolupráci v oblasti bezpečnosti sítí a informací, jež byla zřízena podle článku 11 směrnice o bezpečnosti sítí a informací. Skupina pro spolupráci, která je tvořena zástupci členských států, Evropské agentury pro kybernetickou bezpečnost (ENISA) a Komise, přijala pokyny týkající se bezpečnostních opatření a hlášení incidentů. V červnu 2018 skupina zahájila zvláštní oblast činností týkající se energetiky.

(5) Společné sdělení o kybernetické bezpečnosti z roku 2017 ([7]) uznává význam úvah a požadavků na úrovni EU specifických pro daná odvětví, včetně odvětví energetiky. Kybernetická bezpečnost a možné důsledky pro politiky byly v Unii v posledních letech předmětem komplexní diskuse. Díky tomu v současné době stoupá povědomí o tom, že jednotlivá hospodářská odvětví čelí specifickým otázkám v oblasti kybernetické bezpečnosti, a že tedy musí vytvořit své vlastní odvětvové přístupy v širším kontextu obecných strategií kybernetické bezpečnosti.

(6) Klíčovými prvky v oblasti kybernetické bezpečnosti jsou důvěra a sdílení informací. Cílem Komise je zintenzivnit sdílení informací mezi příslušnými zúčastněnými stranami, a to pořádáním specializovaných akcí, například jednání u kulatého stolu na vysoké úrovni o kybernetické bezpečnosti v energetice, které se uskutečnilo v březnu 2017 v Římě, a konference na vysoké úrovni o kybernetické bezpečnosti v energetice, která se uskutečnila v říjnu 2018 v Bruselu. Komise rovněž chce zlepšit spolupráci mezi příslušnými zúčastněnými stranami a specializovanými subjekty, jako je evropské středisko pro sdílení a analýzu informací v energetice.

(7) Nařízení o agentuře ENISA, Agentuře EU pro kybernetickou bezpečnost, a o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií („nařízení o aktu o kybernetické bezpečnosti“) ([8]) posílí mandát Agentury EU pro kybernetickou bezpečnost, aby lépe podporovala členské státy v boji proti kybernetickým bezpečnostním hrozbám a útokům. Rovněž vytváří evropský rámec v oblasti kybernetické bezpečnosti pro certifikaci produktů, procesů a služeb, který bude platný v celé EU a má zvláštní význam pro odvětví energetiky.

(8) Komise předložila doporučení ([9]), které se zabývá riziky v 5. generaci síťových technologií (5G) a stanoví za tímto účelem pokyny týkající se vhodné analýzy rizik a opatření k řízení rizik na vnitrostátní úrovni, vytvoření koordinované evropské analýzy rizik a zavedení procesu vypracování společné sady nástrojů s osvědčenými opatřeními k řízení rizik. Sítě 5G budou po svém zavedení páteří široké škály služeb nezbytných pro fungování vnitřního trhu a základních společenských a hospodářských funkcí, jako je energetika.

(9) Toto doporučení by mělo členským státům a příslušným zúčastněným stranám, zejména provozovatelům sítí a dodavatelům technologií, poskytnout orientační vodítko k dosažení vyšší úrovně kybernetické bezpečnosti s ohledem na zvláštní požadavky na práci v reálném čase identifikované v odvětví energetiky, kaskádové efekty a kombinaci starších a moderních technologií. Cílem těchto pokynů je pomoci zúčastněným stranám dbát na zvláštní požadavky odvětví energetiky při provádění mezinárodně uznávaných norem v oblasti kybernetické bezpečnosti. ([10])

(10) Komise má v úmyslu toto doporučení pravidelně přezkoumávat na základě pokroku dosaženého v celé Unii a v konzultaci s členskými státy a příslušnými zúčastněnými stranami. Komise se bude i nadále snažit o posílení kybernetické bezpečnosti v odvětví energetiky, zejména prostřednictvím skupiny pro spolupráci v oblasti bezpečnosti sítí a informací, která zajistí strategickou spolupráci a výměnu informací mezi členskými státy v oblasti kybernetické bezpečnosti,

PŘIJALA TOTO DOPORUČENÍ:

PŘEDMĚT

1) Toto doporučení uvádí hlavní problémy týkající se kybernetické bezpečnosti v odvětví energetiky (požadavky na práci v reálném čase, kaskádové efekty a kombinace starších a moderních technologií) a určuje hlavní akce pro provádění příslušných opatření pro zajištění připravenosti v oblasti kybernetické bezpečnosti v odvětví energetiky.

([7]) JOIN(2017) 450.

([8]) Evropský parlament přijal akt o kybernetické bezpečnosti v březnu 2019. Formální přijetí Radou se očekává v dubnu, brzy poté bude následovat zveřejnění právního textu v Úředním věstníku.

([9]) C(2019) 2335.

([10]) Mezinárodní organizace pro normalizaci zveřejnily různé normy v oblasti kybernetické bezpečnosti (ISO/IEC 27000: Informační technologie) a řízení rizik (ISO/IEC 31000: Management rizik). V říjnu 2017 byla jako součást řady ISO/IEC 27000 vydána zvláštní norma pro odvětví energetiky (ISO/IEC 27019: Řízení bezpečnosti informací pro odvětví energetických podniků).

2) Při uplatňování tohoto doporučení by členské státy měly vybízet příslušné zúčastněné strany, aby rozvíjely znalosti a dovednosti týkající se kybernetické bezpečnosti v odvětví energetiky. Členské státy by rovněž měly v příslušných případech začlenit tyto úvahy do svého vnitrostátního kybernetického bezpečnostního rámce, zejména prostřednictvím strategií a právních a správních předpisů.

POŽADAVKY SOUČÁSTÍ ENERGETICKÉ INFRASTRUKTURY NA PRÁCI V REÁLNÉM ČASE

3) Členské státy by měly zajistit, aby příslušné zúčastněné strany, především provozovatelé energetických sítí a dodavatelé technologií, a zejména provozovatelé základních služeb určení podle směrnice o bezpečnosti sítí a informací, prováděly příslušná opatření pro zajištění připravenosti v oblasti kybernetické bezpečnosti, jež souvisejí s požadavky na práci v reálném čase v odvětví energetiky. Některé prvky energetického systému musejí pracovat „v reálném čase“, tj. reagovat na povely během několika milisekund; v důsledku toho je zavádění opatření v oblasti kybernetické bezpečnosti z důvodu nedostatku času obtížné, či dokonce nemožné.

4) Provozovatelé energetických sítí by zejména měli:

a) u nových zařízení uplatňovat v příslušných případech nejnovější bezpečnostní normy a zvážit doplňková fyzická bezpečnostní opatření v případech, kdy nainstalovaná základna starých zařízení nemůže být dostatečně chráněna mechanismy kybernetické bezpečnosti;

b) implementovat mezinárodní normy týkající se kybernetické bezpečnosti a náležité zvláštní technické normy pro zabezpečenou komunikaci v reálném čase, jakmile budou příslušné produkty komerčně dostupné;

c) zohlednit omezení plynoucí z práce v reálném čase v celkové koncepci bezpečnosti týkající se aktiv, zejména při klasifikaci aktiv;

d) zvážit využití sítí v soukromém vlastnictví pro systémy dálkových ochran, aby byla zajištěna úroveň kvality služeb potřebná vzhledem k omezením plynoucím z práce v reálném čase; při používání veřejných komunikačních sítí by provozovatelé měli zvážit zajištění přidělené šířky pásma, požadavky na latenci a bezpečnostní opatření při komunikaci;

e) rozdělit celý systém do logických zón a v každé zóně stanovit časová a procesní omezení, aby mohli uplatnit vhodná opatření v oblasti kybernetické bezpečnosti nebo uvážit jiné metody ochrany.

5) V příslušných případech by provozovatelé energetických sítí rovněž měli:

a) zvolit, ohledem na požadavky na práci v reálném čase, zabezpečený komunikační protokol, například mezi zařízením a jeho systémy řízení (systém hospodaření s energií – EMS/systém řízení distribuční sítě – DMS);

b) zavést vhodný ověřovací mechanismus pro komunikaci stroj-stroj, který zohlední požadavky na práci v reálném čase.

KASKÁDOVÉ EFEKTY

6) Členské státy by měly zajistit, aby příslušné zúčastněné strany, především provozovatelé energetických sítí a dodavatelé technologií, a zejména provozovatelé základních služeb určení podle směrnice o bezpečnosti sítí a informací, prováděly příslušná opatření pro zajištění připravenosti v oblasti kybernetické bezpečnosti, jež souvisejí s kaskádovými efekty v odvětví energetiky. Elektrické soustavy a plynovody jsou v Evropě silně propojené a kybernetický útok, který by způsobil výpadek nebo narušení v jedné části energetického systému, by mohl vyvolat dalekosáhlé kaskádové efekty v dalších částech systému.

7) Při uplatňování tohoto nařízení by členské státy měly zhodnotit vzájemnou závislost a kritičnost výroby energie a systémů založených na flexibilní poptávce, přenosových a distribučních rozvoden a vedení a přidružených ovlivněných zúčastněných stran (včetně přeshraničních situací) v případě úspěšného kybernetického útoku nebo incidentu. Členské státy by rovněž měly zajistit, aby provozovatelé energetických sítí měli zaveden rámec pro komunikaci se všemi klíčovými zúčastněnými stranami za účelem sdílení varovných signálů a spolupráce na krizovém řízení. Měly by být zavedeny strukturované komunikační kanály a dohodnuté formáty za účelem sdílení citlivých informací se všemi relevantními zúčastněnými stranami, týmy CSIRT a příslušnými orgány.

8) Provozovatelé energetických sítí by zejména měli:

a) zajistit, aby nová zařízení, včetně zařízení internetu věcí, měla a udržovala si takovou úroveň kybernetické bezpečnosti, která odpovídá kritičnosti dané lokality;

b) při zavádění a pravidelném přezkumu plánů zachování kontinuity provozu dostatečně uvážit kybernetickofyzické účinky;

c) zavést konstrukční kritéria a architekturu pro odolnou síť, což lze dosáhnout:

— zavedením opatření hloubkové ochrany pro jednotlivé lokality, která budou přizpůsobena kritičnosti lokalit,

— určením klíčových uzlů, jak z hlediska kapacity výroby energie, tak z hlediska dopadu na zákazníky; zásadní funkce sítě by měly být projektovány tak, aby se zmírnilo riziko, které může způsobit kaskádové efekty, a to uvážením redundance, odolnosti vůči fázovým oscilacím a ochrany před kaskádovým odpojením zatížení,

— spoluprací s dalšími příslušnými provozovateli a s dodavateli technologií za účelem prevence kaskádových efektů uplatněním vhodných opatření a služeb,

— navrhováním a budováním komunikačních a řídicích sítí s cílem omezit účinky jakýchkoli fyzických a logických selhání na určité části sítí a zajistit přiměřená a rychlá zmírňující opatření.

STARŠÍ A MODERNÍ TECHNOLOGIE

9) Členské státy by měly zajistit, aby příslušné zúčastněné strany, především provozovatelé energetických sítí a dodavatelé technologií, a zejména provozovatelé základních služeb určení podle směrnice o bezpečnosti sítí a informací, prováděly příslušná opatření pro zajištění připravenosti v oblasti kybernetické bezpečnosti, jež souvisejí s kombinací starších a moderních technologií v odvětví energetiky. V dnešním energetickém systému souběžně existují dva různé druhy technologií: starší technologie s životností od 30 do 60 let projektovaná dříve, než se začala zohledňovat kybernetická bezpečnost, a moderní vybavení, které odráží moderní digitalizaci a inteligentní zařízení.

10) Při uplatňování tohoto doporučení by členské státy měly podněcovat provozovatele energetických sítí a dodavatele technologií, aby se vždy, kdy je to možné, řídili příslušnými mezinárodně uznávanými normami, jež se týkají kybernetické bezpečnosti. Zúčastněné strany a zákazníci by pak měli přijmout přístup zaměřený na kybernetickou bezpečnost při připojování zařízení do sítě.

11) Dodavatelé technologií by měli zejména poskytovat vyzkoušená řešení bezpečnostních problémů ve starších nebo nových technologiích, a to zdarma a jakmile je příslušný bezpečnostní problém zjištěn.

12) Provozovatelé energetických sítí by zejména měli:

a) analyzovat rizika spojení konceptů starších technologií a internetu věcí a mít povědomí o interních a externích rozhraních a jejich zranitelnostech;

b) přijmout vhodná opatření proti zlovolným útokům pocházejícím z velkého množství spotřebitelských zařízení či aplikací řízených se zlým úmyslem;

c) zavést schopnost automatizovaného monitorování a analýzy událostí souvisejících s bezpečností v prostředí starších technologií a internetu věcí, jako jsou neúspěšné pokusy o přihlášení, dveřní poplašná zařízení pro otevírání skříní a další události;

d) pravidelně provádět zvláštní analýzu rizik týkajících se kybernetické bezpečnosti u všech starších zařízení, a to zejména při spojování starých a nových technologií; vzhledem k tomu, že starší zařízení často představují značné množství aktiv, může být analýza rizik provedena podle tříd aktiv;

e) vždy, kdy je to vhodné, aktualizovat software a hardware starších systémů a systémů internetu věcí na nejnovější verze; přitom by provozovatelé energetických sítí měli uvážit doplňková opatření, jako je oddělení systémů nebo přidání vnějších bezpečnostních bariér v případech, kdy by instalace oprav či aktualizací byla vhodná, ale není možná, např. u nepodporovaných produktů;

f) vypisovat zadávací řízení s ohledem na kybernetickou bezpečnost, tj. požadovat informace o bezpečnostních prvcích, požadovat dodržování stávajících norem v oblasti kybernetické bezpečnosti, zajistit trvalé upozorňování a návrhy na opravy a migraci v případě zjištění zranitelností a upřesnit odpovědnost dodavatelů v případě kybernetických útoků či incidentů;

g) spolupracovat s dodavateli technologií na výměně starších systémů, kdykoli to bude prospěšné z bezpečnostních důvodů, avšak zohlednit zásadní funkce systému.

SLEDOVÁNÍ

13) Členské státy by měly do 12 měsíců od přijetí tohoto doporučení a poté každé dva roky podrobně informovat Komisi o stavu provádění tohoto doporučení prostřednictvím skupiny pro spolupráci v oblasti bezpečnosti sítí a informací.

PŘEZKUM

14) Komise na základě informací předložených členskými státy přezkoumá provádění tohoto doporučení a v příslušných případech po konzultaci s členskými státy a příslušnými zúčastněnými stranami posoudí, zda jsou nutná další opatření.

URČENÍ

15) Toto doporučení je určeno členským státům.

V Bruselu dne 3. dubna 2019.

Za Komisi
Miguel ARIAS CAÑETE
člen Komise