Mezinárodní bezpečnostní instut, z.ú.,

Na Ořechovce 580/4, Praha 6, PSČ 162 00

IČO: 07313209

Kybernetická bezpečnost kritické energetické infrastruktury Evropské Unie

Zdroj:
https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2019)642274

České relevantní právní zdroje prostřednictvím:

https://www.zakonyprolidi.cz/cs/2000-240?text=kritick%C3%A1+infrastruktura:

- 432/2010 Sb. - Nařízení vlády o kritériích pro určení prvku kritické infrastruktury
- 240/2000 Sb. - Krizový zákon
- 181/2014 Sb. - Zákon o kybernetické bezpečnosti
- 462/2000 Sb. - Nařízení vlády k provedení krizového zákonu
- 82/2018 Sb. - Vyhláška o kybernetické bezpečnosti
- 317/2014 Sb. - Vyhláška o významných informačních systémech a jejich určujících kritériích
- 194/2017 Sb. - Zákon o opatřeních ke snížení nákladů na zavádění vysokorychlostních sítí elektronických komunikací
- 320/2015 Sb. - Zákon o hasičském záchranném sboru
- 140/2013 Sb. - Rozhodnutí vlády ČR o vyhlášení nouzového stavu
- 387/2012 Sb. - Vyhláška o státní autorizaci na výstavbu výrobny elektřiny
- 585/2004 Sb. - Branný zákon

Autor:

EPRS (European Parliamentary Research Service) , Gregor Erbach with Jack O'Shea Members' Research Service, (Říjen 2019)

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

Evropská unie (dále jen „EU“) má vysokou úroveň energetické bezpečnosti, umožněné zásobami ropy a zemního plynu a také jednou z nejspolehlivějších elektrických sítí na světě. Řada zavedených a vznikajících trendů však představuje nové výzvy pro zabezpečení dodávek energie, zejména v odvětví elektřiny. Hackeři se stávají stále více schopnými a již zkoumají a využívají zranitelnosti v energetickém systému, jak již prokázalo množství incidentů mimo EU.

Směrnice z roku 2008 o evropských kritických infrastrukturách byla základem přístupu EU. EU nedávno posílila svůj přístup ke kybernetické bezpečnosti prostřednictvím právních předpisů, norem a posílení Evropské agentury pro bezpečnost sítí a informací, která převezme nové koordinační a operační úlohy v kybernetické bezpečnosti.

Současné trendy v zabezpečení energetických systémů.

Bezpečný energetický systém má pro moderní společnosti zásadní význam. Elektřina, plyn a ropa nejsou nutné pouze pro naše každodenní činnosti, ale umožňují také fungování další kritické infrastruktury, zejména dopravy, telekomunikací, zdravotnictví, financí a obrany. EU má jednu z nejspolehlivějších elektrických sítí na světě a její možná zranitelnost dosud nebyla zneužita k přerušení dodávek energie ve velkém měřítku. Jinde však už byly zneužity zranitelnosti energetického systému v různých kybernetických útocích. Přírodní katastrofy, jako jsou bouře, zemětřesení, sopečné erupce, povodně a elektromagnetické impulsy, mohou rovněž způsobit vážné narušení energetických systémů, což vyžaduje silnější infrastrukturu.

Důsledky těchto nově vznikajících hrozeb jsou četné: protože všechna odvětví hospodářství se spoléhají na energii, aby mohla fungovat, využívání slabých míst v kritické infrastruktuře

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

sítě má potenciál iniciovat „kaskádový efekt“, který brání nebo zastavuje provoz v jiných odvětvích, jako je doprava, finance a zdravotnictví. Vypnutí energetické sítě může vyvolat občanské nepokoje, narušit komunikační řetězce, zhoršit vojenskou připravenost a obecně bránit vládní schopnosti rychle a účinně reagovat v krizových situacích.

Evropský energetický systém prochází zásadní transformací směrem k modelu s vysokým podílem variabilní distribuované obnovitelné energie, flexibilní poptávky, zařízení pro skladování energie a propojení odvětví. Všechny trendy vedou k rostoucí digitalizaci energetického systému a rostoucímu počtu síťových zařízení a řídicích systémů, což vede ke zvýšeným příležitostem pro kybernetické útoky. Očekává se, že počet síťových zařízení v energetickém systému poroste s rozšířením „průmyslového internetu věcí“ umožněného zavedením bezdrátových komunikačních sítí 5G. Na druhé straně se využívání elektřiny stává také „inteligentní“, a to pomocí inteligentních spotřebičů připojených k internetu, inteligentních domácností, inteligentních měřičů elektřiny a plynu.

Energetický systém má řadu zvláštností, které vyžadují specializovaný odvětvový přístup ke kybernetické bezpečnosti, nad rámec standardů kybernetické bezpečnosti a opatření uplatňovaná na systémy informačních technologií:

• **Požadavky v reálném čase**: V elektrické síti musí být nabídka a poptávka v každém okamžiku vyvážené, což znamená, že průmyslové řídicí systémy musí reagovat během zlomků vteřiny, což nezanechává čas na sofistikované autentizační postupy.

• **Mix pokročilých a starších technologií**: Komponenty energetického systému mají velmi dlouhou životnost, několik desetiletí. Je tedy velmi pravděpodobné, že mřížka bude řízena kombinací pokročilých technologií s certifikací kybernetické bezpečnosti a starších zařízení, která je třeba chránit jiným způsobem.

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

• **Kaskádové účinky narušení**: Vzhledem k propojené povaze elektrické soustavy se může vážné narušení v jedné části sítě rozšířit i na vzájemně propojené rozvodné sítě, což může vést k výpadku proudu v široké oblasti. To by mělo rovněž dopad na další služby, které jsou závislé na elektřině, zejména doprava, telekomunikace, zásobování vodou a finance.

Mezi opatření, která mají útočníkům zabránit v přístupu, patří pravidelná aktualizace systémů, silné autentizační protokoly, šifrování komunikace, soukromé sítě, které nejsou připojeny
k internetu, fyzická ochrana sítí, bezpečnostní postupy a pravidelné bezpečnostní audity a školení zaměstnanců ke zvýšení informovanosti.

Politika a právní předpisy EU.

Evropský program na ochranu kritické infrastruktury (EPCIP), který Komise přijala v roce 2006, stanoví rámec pro opatření zaměřená na zlepšení ochrany kritické infrastruktury ve všech členských státech EU a ve všech příslušných hospodářských odvětvích. Mezi hrozby, které program řeší, patří terorismus, trestná činnost, přírodní katastrofy a další příčiny nehod. Členské státy si pravidelně vyměňují informace v rámci schůzí kontaktních míst. Klíčovým právem EU na ochranu kritické infrastruktury je směrnice Rady 2008/114 / ES o kritických evropských infrastrukturách. Stanovuje postupy pro identifikaci a označování evropských kritických infrastruktur (ECI) a zavádí společný přístup k posuzování jejich ochrany a potřeby jej zlepšit. Směrnice se vztahuje pouze na **odvětví energetiky a dopravy**. Vyžaduje, aby vlastníci nebo provozovatelé určené ECI připravili pokročilé plány kontinuity činnosti (plány bezpečnosti provozovatele) a jmenovali styčné důstojníky pro bezpečnost, kteří působí jako kontaktní místa k vnitrostátnímu orgánu odpovědnému za ochranu kritické infrastruktury.

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

V červnu 2019 Komise zveřejnila hodnocení směrnice o kritické infrastruktuře (2008), v níž zjistila, že význam této směrnice se snížil s ohledem na nové a vyvíjející se výzvy vyvolané technologickým, hospodářským, sociálním, politickým a environmentálním vývojem. Dospívá k závěru, že směrnice byla částečně účinná, ale nezavedla společný přístup k posuzování opatření na ochranu kritické infrastruktury. Mezi možnosti určené pro budoucí přezkum směrnice patří přístup zaměřený více na systémy a lepší sladění s dalšími příslušnými právními předpisy EU.

Nařízení o bezpečnosti dodávek plynu: Nařízení (EU) 2017/1938 se zabývá nedostatkem dodávek plynu způsobeným řadou rizikových faktorů, včetně počítačových útoků, války, terorismu a sabotáže. Stanoví pravidla pro posuzování regionálních rizik a nouzové plánování a zavádí mechanismus vzájemného hodnocení a nouzové plánování a zavádí mechanismus vzájemné pomoci v případě vážné krize v dodávkách plynu na základě zásady solidarity.

Nařízení o připravenosti na riziko elektřiny: Nařízení (EU) 2019/941 je zaměřeno konkrétně na předcházení krizím a řešení krizí v odvětví elektřiny. Předpokládá vývoj společných metod pro hodnocení rizik pro zabezpečení dodávek elektřiny, včetně rizik kybernetických útoků; společná pravidla pro řešení krizových situací a společný rámec pro lepší hodnocení a sledování bezpečnosti dodávek elektřiny. Evropská komise pořádá pravidelné akce ke sdílení informací, jako je například akce na vysoké úrovni o kybernetické bezpečnosti v odvětví energetiky, která se konala dne 9. července 2019.

Probíhající vývoj.

Přepracování nařízení o elektřině (nařízení (EU) 2019/943) dává Komisi mandát k vypracování síťového předpisu pro kybernetickou bezpečnost. Pracovní skupina pro inteligentní sítě provádí přípravné práce od roku 2017 a v červenci 2018 vydala svou druhou průběžnou zprávu. Zpráva doporučuje zřídit systém včasného varování pro energetický

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

sektor v Evropě, přeshraniční a nadnárodní řízení rizik, minimum bezpečnostní požadavky na kritické komponenty infrastruktury, minimální úroveň ochrany pro provozovatele energetických systémů, evropský rámec energetické kybernetické bezpečnosti a řízení rizik v dodavatelském řetězci.

Zapojení odborníků a zúčastněných stran.

Kybernetická bezpečnost v energetickém sektoru zahrnuje několik klíčových zúčastněných organizací a v posledních letech bylo vyvinuto úsilí o začlenění těchto aktérů do fór pro sdílení osvědčených postupů a zavedení jednotných norem kybernetické bezpečnosti. Pracovní skupiny, jako je pracovní skupina pro inteligentní sítě, koordinační skupina pro elektřinu (ECG) a Evropské středisko pro sdílení informací a analýzu energie (EE-ISAC), fungují jako fóra pro veřejné služby, agentury a další relevantní aktéry k budování pracovních vztahů a vyměňovat si osvědčené postupy pro kybernetickou bezpečnost. Skupina zúčastněných stran v oblasti bezpečnosti kritické energetické infrastruktury (CEIS-SG) byla zřízena jako fórum pro výměnu názorů a informací, které má vést a koordinovat úsilí o zlepšení bezpečnosti
a odolnosti kritické energetické infrastruktury (CEI). EU je podporována prostřednictvím rámcového programu pro výzkum Horizont 2020 (projekt Defender). CEIS-SG si klade za cíl definovat plán bezpečnosti CEI nové generace podle návrhu a ve výchozím nastavení, rozvíjet bezpečnostní certifikace a propagovat osvědčené postupy na celoevropské úrovni.

Přístupy v některých jiných jurisdikcích.

Spojené státy americké.

Ve Spojených státech byl prvním významným právním předpisem, který se zabýval rostoucí výzvou kybernetické bezpečnosti v odvětví energetiky, zákon o energetické politice z roku

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

2005. Zákon udělil Federální energetické regulační komisi (FERC) možnost jmenovat Organizaci pro elektrickou spolehlivost (ERO), která se bude vyvíjet a prosazovat závazné standardy spolehlivosti pro všechny elektrické rozvodné sítě v zemi. Severoamerická společnost pro elektrickou spolehlivost (NERC) byla v roce 2006 jmenována ERO pro Spojené státy a několik kanadských provincií. NERC odpovídá za vypracování seznamu norem na ochranu kritické infrastruktury (NERC-CIPs), které jsou doručeny FERC ke kontrole. Z jedenácti CIP, které jsou v současné době předmětem vymáhání, je deset věnováno standardům kybernetické bezpečnosti a jeden se týká fyzické bezpečnosti energetických sítí. NERC-CIP, které se zabývají infrastrukturami pro výrobu a přenos elektřiny, patří mezi nejpodrobnější a nejobsáhlejší standardy kybernetické bezpečnosti na světě. Tyto standardy lze také v případě potřeby rychle aktualizovat a efektivně se přizpůsobit kolísajícímu prostředí kybernetické bezpečnosti. Vládní agentury v USA přijímají holistický přístup k problému energetické kybernetické bezpečnosti, spolupracují s průmyslovými a místními činiteli v boji proti vznikajícím hrozbám. Například nový Úřad pro kybernetickou bezpečnost, energetickou bezpečnost a reakci na mimořádné situace (CESER) má vést koordinovanou reakci ministerstva energetiky na narušení prostřednictvím partnerství s národním laboratorním systémem, koordinačními organizacemi soukromého sektoru a státními a místními vládami. Program sdílení informací o riziku kybernetické bezpečnosti (CRISP) je dobrovolné partnerství veřejného a soukromého sektoru, které je financováno především průmyslem. Cvičení jako Clear Path VI-roční simulace kybernetického útoku na energetickou infrastrukturu v Severní Americe vedené NERC mohou také pomoci rozvinout meziagenturní koordinaci během krizí.

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

Austrálie.

Australská vláda zřídila australské středisko kybernetické bezpečnosti (ACSC) se společnými středisky kybernetické bezpečnosti (JCSC) rozmístěnými po celé zemi ve velkých městech. V průběhu roku 2019 bude ACSC dohlížet na celostátní program aktivit v oblasti kybernetické odolnosti a reakce v elektroenergetickém průmyslu a na vládní agentury, které mají energetickou a kybernetickou bezpečnost, včetně výměny informací a školení. Tyto aktivity vyvrcholí dvoudenním funkčním cvičením pro australský elektroenergetický průmysl v listopadu 2019.

Výhled.

Bezpečnost a odolnost evropského energetického systému zůstane v dohledné budoucnosti zásadním problémem. Řada současných trendů zvýší potřebu silných bezpečnostních opatření a politik, zejména v odvětví elektřiny.

- **Digitalizace a automatizace**: Tento trend ovlivňuje energetický systém přechodem k inteligentní síti s více a více síťovými komponenty sítě, od výrobců elektřiny, přes přenosové a distribuční sítě až po inteligentní měřiče v domácnosti. Na internet věcí bude připojen rostoucí počet zařízení spotřebovávajících elektřinu v domácnostech a průmyslu, což umožní zavádění telekomunikačních sítí 5G. Všechna tato zařízení představují potenciální příležitosti k útokům nebo neúmyslnému narušení.
- **Udržitelná energie**: S cílem dosáhnout energeticky neutrálního energetického systému bude elektrická soustava stále více decentralizovaná (distribuované větrné, solární a vodní elektrárny). Rovněž bude stále více propojena, aby se rovnováha mezi variabilní výrobou energie mezi regiony vyvážila. Kromě toho všechna elektrická vozidla, skladování, inteligentní spotřebiče a flexibilní průmyslová poptávka vedou k dramatickému nárůstu potenciálně zranitelných síťových zařízení v elektrické síti.

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

- **Reforma trhu a posílení postavení spotřebitelů**: Reformy trhu s elektřinou umožňují účast nových aktérů. Patří sem energetické společnosti, agregátory, energetické komunity a jednotliví občané. Mnoho z nich nebude mít odpovídající dovednosti v oblasti kybernetické bezpečnosti, a proto se musí spolehnout na certifikované poskytovatele vybavení, softwaru a služeb.
- **Schopnosti protivníků**: Znalosti a nástroje hackerů se neustále vyvíjejí. Mezi potenciální protivníky patří kybernetičtí zločinci, hackeři sponzorovaní vládou, teroristické skupiny a vojenské kybernetické příkazy. Nástroje automatizovaného útoku se mohou šířit v síti a způsobit poškození za zamýšlený cíl. Umělá inteligence má potenciál posílit schopnosti útočníků i obránců a může se ukázat jako zásadní výhoda.
- **Dovednosti a investiční pobídky**: Se zvyšující se potřebou dovedností v oblasti kybernetické bezpečnosti bude pravděpodobně přetrvávat současný nedostatek kvalifikovaných pracovníků. Sdílení informací a znalostí, jakož i automatizace, budou nápomocny při co nejlepším využití dostupné základny dovedností. Trh navíc dostatečně nepodněcuje investice do bezpečnosti a odolnosti, což může znamenat nutnost regulace a veřejných investic.

Očekává se, že s rychlým vývojem v energetickém systému a v informačních i komunikačních technologiích zůstane v nadcházejících letech prioritou agendy EU kybernetická bezpečnost energetického systému. Bude třeba neustále přizpůsobovat bezpečnostní opatření a politiky neustále se vyvíjejícím hrozbám a posilovat odolnost energetických systémů vůči záměrným útokům a neúmyslnému narušení. Adekvátní investice do kybernetické bezpečnosti, rozvoje příslušných dovedností a sdílení informací a znalostí jsou jedním z klíčových předpokladů pro zajištění bezpečného a odolného zásobování energií. V reakci na vznikající hrozbu zařízení manipulovaných výrobcem přijal Evropský parlament v březnu 2019 usnesení, v němž vyzval k přijetí opatření na úrovni EU ohledně bezpečnostních rizik spojených s dominantní rolí Číny

MBI MEZINÁRODNÍ BEZPEČNOSTNÍ INSTITUT

Mezinárodní bezpečnostní instut, z.ú.,
Na Ořechovce 580/4, Praha 6, PSČ 162 00
IČO: 07313209

jako dodavatele telekomunikačních zařízení 5G, který bude pravděpodobně hrát klíčová podpůrná role v inteligentních sítích a distribuovaný, udržitelný energetický systém