KRÍZOVÝ MANAŽMENT
DOI: 10.26552/krm.C.2020.1.34-38
ISSN: 1336 - 0019

ÚPRAVA KRITÉRIÍ PRO URČOVÁNÍ KRITICKÉ INFORMAČNÍ INFRASTRUKTURY ČESKÉ REPUBLIKY

MODIFICATION OF CRITERIA FOR DETERMINING CRITICAL INFORMATION INFRASTRUCTURE OF THE CZECH REPUBLIC

JOSEF BERNÁTEK

ABSTRACT: *The paper defines the fundamental concepts of cybersecurity concerning the critical information infrastructure of the Czech Republic. The practical part of the paper contains an adjustment of the currently set impact and sectoral criteria for determining the elements of critical information infrastructure. In connection with the adaptation of these criteria, measures are proposed to abolish the domain of essential service and incorporate the criteria for identifying essential service information systems into the criteria for identifying critical information infrastructure elements in order to harmonize the current state.*

KEYWORDS: *Critical information infrastructure. Cybersecurity. Crisis management. Population protection.*

ÚVOD

Prvky kritické informační infrastruktury každým rokem více prostupují do našich každodenních aktivit a běžného způsobu života. Mnohdy si dopady jejich zničení nebo kompromitace ani neuvědomujeme. Vyřazení systému řídícího distribuci vody nebo elektřiny může vyústit ve způsobení veřejných nepokojů, škod velkého rozsahu, ale i ztrát na životech. Z hlediska bezpečnosti státu je na místě zajistit nejen přiměřená opatření pro ochranu těchto pro stát existenčně důležitých prvků, ale i nastavení vhodných kritérií pro jejich určování. Zákon č. 240/2000 Sb., o krizovém řízení nebyl původně koncipován pro řešení krizových situací majících původ v kyberprostoru. Krizové řízení v České republice má primárně v gesci Hasičský záchranný sbor České republiky (HZS ČR), kybernetickou bezpečnost Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB). Spolupráce těchto dvou subjektů je nejen pro řešení, ale i přípravu na krizové situace a mimořádné události klíčová.

Ne všechny informační systémy pro stát kritické, jsou určeny jako prvky kritické informační infrastruktury. Některé z nich jsou určeny jako informační systémy základní služby, tudíž již nespadají pod zákon o krizovém řízení. Určitá část kritických systémů není určena ani jako informační systémy základní služby, ačkoliv by z povahy věci přinejmenším do této kategorie spadat měla. Cílem příspěvku je definice základních pojmů kybernetické bezpečnosti ve vztahu ke kritické informační infrastruktuře, zhodnocení současných právními předpisy stanovených odvětvových a dopadových kritérií pro určování prvků kritické informační infrastruktury České republiky s navržením případných úprav, které mohou mít pozitivní dopad nejen na úroveň bezpečnosti státu, ale i jeho ekonomiku, životní prostředí, zdraví a životy obyvatel.

1. DEFINICE ZÁKLADNÍCH POJMŮ

Aktivum představuje hmotný i nehmotný statek s hodnotou pro provozovatele prvku kritické informační infrastruktury (Požár, 2005). Pod hmotná aktiva lze zařadit řídící kontrolní systémy pro monitoring a řízení prvků kritické informační infrastruktury, síťové prvky zajišťující výměnu dat mezi technologickými zařízeními a výpočetní technikou, ale i pracovní stanice administrativního personálu nebo jejich komunikační zařízení. U nehmotných aktiv se jedná například o informační systémy určené pro interpretaci dat z řídících kontrolních systémů nebo informace, jež jsou pro chod podniku nepostradatelné. Aktiva by měla být chráněna pro zajištění jejich důvěrnosti, integrity a dostupnosti (Promyslov et al. 2019).

V obecné rovině je bezpečnost definována dvěma způsoby – negativním a pozitivním. Při negativním vymezení se jedná o absenci hrozby a tedy stav, kdy není prvek nebo provozovatel kritické informační

infrastruktury zatížen nebezpečím a je zajištěn vůči případnému útoku. Pozitivní vymezení bezpečnosti je vždy vztaženo ke konkrétnímu objektu, který je mimo dosah hrozeb, případně je před nimi chráněn. Bezpečnost není nikdy absolutní, ale vždy relativní. Lze ji také definovat jako vlastnost prvku kritické informační infrastruktury, určující stupeň jeho ochrany proti hrozbám (Požár 2005; Ouyang 2016).

Kyberprostor představuje virtuální svět, charakterizovaný užitím elektronických zařízení k ukládání, úpravám a výměně dat prostřednictvím systémů zapojených do sítě a spojených s fyzickou infrastrukturou (Akart 2015). Může se jednat o počítače, servery, směrovače, ale i zařízení internetu věcí a další komponenty prvků kritické informační infrastruktury (Encyclopædia Britannica 2013). Kybernetickou bezpečnost lze definovat jako stav, kdy na prvek kritické informační infrastruktury nepůsobí hrozby, které by mohly narušit jeho důvěrnost, integritu nebo dostupnost (Refsdal et. al. 2015). Stejně jako v případě obecně formulované bezpečnosti, ani kybernetická bezpečnost nemůže být absolutní, ale pouze relativní.

S pojmem kybernetická bezpečnost jsou úzce spojeny pojmy důvěrnost, integrita, dostupnost a nepopíratelnost. Důvěrnost je zajištěna, pokud k datům mohou přistupovat jen oprávnění uživatelé. Identita oprávněného uživatele je ověřována pomocí širokého spektra opatření v autentizačním procesu. Integrita vyjadřuje garanci stavu, že data nebyla neoprávněně změněna. Dostupnost představuje možnost oprávněného uživatele nebo informačního systému přistupovat k datům bez nežádoucího přerušení. Úroveň dostupnosti je obvykle vyjadřována v procentech. Nepopíratelnost zajišťuje garanci skutečnosti, že zápis nebo změnu dat učinil konkrétní uživatel (Cordero 2018).

Kritickou infrastrukturu představují systémy a služby, jejichž vyřazení případně omezení funkčnosti by představovalo závažný dopad pro ekonomiku státu, jeho bezpečnost, veřejnou správu a v důsledku i zajištění základních životních potřeb obyvatelstva (Jirásek et. al. 2015). Přestože neexistuje obecně přijímaná definice kritické infrastruktury, všechny definice zdůrazňují její roli pro společnost, případně dopady v případě jejího narušení nebo omezení funkce (Setola et. al. 2017). Kritická informační infrastruktura je dle českého právního řádu kritická infrastruktura v odvětví komunikační a informační systémy a oblasti kybernetické bezpečnosti dle přílohy k nařízení vlády č. 432/2010 o kritériích pro určení prvku kritické infrastruktury (Vláda ČR 2010). Lze ji definovat jako informační a komunikační systémy, které jsou samy o sobě prvkem kritické infrastruktury nebo jsou nezbytné pro správnou funkci ostatních kategorií prvků kritické infrastruktury, jako například přenosové soustavy elektrické energie (Theron & Bologna 2013).

Základní služba je v zákonu o kybernetické bezpečnosti definována jako služba, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení může mít významný dopad na zabezpečení společenských nebo ekonomických činností v definovaných odvětvích. Jedná se o odvětví dopravy, energetiky, zdravotnictví, bankovnictví, infrastruktury finančních trhů, vodního hospodářství, digitální infrastruktury a chemického průmyslu (Maisner 2015).

2. DOPADOVÁ A ODVĚTVOVÁ KRITÉRIA

Dopadová kritéria, označovaná v právních předpisech jako průřezová, představují soubor parametrů pro hodnocení dopadů narušení funkce prvku kritické infrastruktury s mezními hodnotami zahrnujícími ztráty na životech obyvatelstva, dopad na jejich zdraví, mimořádně vážný ekonomický dopad nebo dopad na veřejnost v důsledku rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do běžného způsobu života (NÚKIB 2018). Mezi dopadová kritéria řadíme dle ustanovení § 1 nařízení vlády ze dne 22. prosince 2010 č. 432/2010 Sb., o kritériích pro určení prvků kritické infrastruktury počet obětí nebo osob vyžadující hospitalizaci, ekonomický dopad, dopad na veřejnost, omezení poskytování nezbytných služeb nebo jiný závažný zásah do běžného způsobu života (Vláda ČR 2010).

Odvětvová kritéria představují technické nebo provozní parametry k určování prvku kritické infrastruktury v odvětvích potravinářství, zemědělství, energetika, doprava, vodní hospodářství, zdravotnictví, finanční trh a měna, nouzové služby, veřejná správa a komunikační a informační systémy (Vaníček 2017). V rámci odvětví č. „VI. komunikační a informační systémy“ je pro určení prvku kritické informační infrastruktury klíčové pododvětví „G. Oblast kybernetické bezpečnosti“.

Nařízení dále stanoví, že odvětvová kritéria pro určení prvku kritické infrastruktury uvedená v písmenech A. až F. pododvětví VI. komunikační a informační systémy se použijí přiměřeně pro oblast kybernetické bezpečnosti, pokud je ochrana prvku splňujícího tato kritéria nutná pro zajištění kybernetické bezpečnosti (Vláda ČR 2010).

Pro určování provozovatelů základní služby jsou kritéria uvedena ve vyhlášce č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby, která nabyla účinnosti 1. února 2018 a jsou pro každý typ subjektu odlišná. Pokud si jako příklad vezmeme odvětví chemického průmyslu, tak v odvětvových kritériích se zohledňuje druh služby a druh subjektu, nikoliv však speciální kritérium. Aby byla naplněna dopadová kritéria v případě odvětví chemického průmyslu, mohl by dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jejichž fungování je poskytování služby závislé způsobit závažné omezení nebo narušení služby, hospodářskou ztrátu, nedostupnost služby, oběti na životech, zraněné, případně narušení veřejné bezpečnosti (NÚKIB 2017).

3. ÚPRAVA ODVĚTVOVÝCH KRITÉRIÍ

Směrnice Rady č. 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu definovala pouze dvě odvětví, energetiku a dopravu (Evropská rada, 2008). Česká republika pojala problematiku kritické infrastruktury šířeji, kdy definovala celkem devět odvětví a rovněž stanovila pro její území dopadová kritéria. V současné době obsahuje nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury celkem devět odvětví. Jedná se o energetiku, vodní hospodářství, potravinářství a zemědělství, zdravotnictví, dopravu, komunikační a informační systémy, finanční trh a měnu, nouzové služby a veřejnou správu. Ke zvážení je zahrnutí do odvětví chemického nebo obranného průmyslu, jako je tomu například ve Spojených státech amerických.

Žádoucí je vypracování analýz současně stanovených odvětvových kritérií a jejich případná redefinice. Jako příklad lze uvést odvětví zdravotnictví, kdy u zdravotnického zařízení je vyžadován celkový počet akutních lůžek nejméně 2 500, ačkoliv již při stanovení tohoto kritéria bylo zřejmé, že žádné takové zařízení se v České republice nenachází. Pokud se kybernetický útočník rozhodne infiltrovat všechny velké (v krajním případě všechny) nemocnice v České republice škodlivým kódem, tak se v souhrnu překoná kritérium 2 500 lůžek a budou vyřazeny tyto nemocnice z provozu na blíže nestanovenou dobu. Legislativně by měl být stanoven minimální počet lůžek na vyšší územně samosprávný celek a hustotu zalidnění, aby měl stát k dispozici jako prvky kritické infrastruktury alespoň čtrnáct nemocničních zařízení.

Obdobná situace nastává i u odvětví potravinářství a zemědělství, kde dle přílohy k typovému plánu Narušení bezpečnosti informací kritické informační infrastruktury nebyl k 1. lednu 2018 určen jediný prvek kritické informační infrastruktury (HZS Ústeckého kraje, 2020). Dnešní potravinářská a zemědělská produkce se přitom již téměř neobejde bez průmyslových řídicích systémů, které zajišťují značnou část výrobních procesů. Do budoucna se s vývojem precizního zemědělství a implementací zařízení internetu věcí budou tyto technologické procesy ještě významněji závislé na kybernetickém prostoru a tím i více zranitelné vůči kybernetickým hrozbám.

4. ÚPRAVA DOPADOVÝCH KRITÉRIÍ

Dopadová kritéria, označovaná v nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury jako průřezová, byla pro určování prvků kritické infrastruktury převzata z dopadových kritérií pro živelní pohromy, což může při určování prvků kritické informační infrastruktury činit potíže. Pro jejich naplnění jsou stanovena kritéria 250 mrtvých nebo více než 2 500 osob s následnou hospitalizací delší než 24 hodin, ekonomický dopad vyšší než 0,5 % hrubého domácího produktu nebo dopad na veřejnost omezením poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života více než 125 000 osob.

Inspiraci pro redefinici dopadových kritérií lze nalézt například v Maďarsku, jako zemi s obdobným počtem obyvatel, rozlohou i hustotou zalidnění (Rostek 2014). V rámci vládního nařízení upravujícího určování prvků kritické infrastruktury státu jsou v Maďarsku nastavena dopadová kritéria zohledňující ztráty na životech nebo zdraví, ekonomický, sociální, politický dopad, včetně dopadu na životní prostředí (Vláda Maďarska, 2013).

5. ZMĚNA INSTITUTU ZÁKLADNÍ SLUŽBY

V rámci institutu základní služby, který v českém právním řádu nabyl účinnosti 1. srpna 2017 a jednotlivé informační systémy základní služby jsou určovány od doby účinnosti vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby, bylo k 31. prosinci 2019 určeno celkem 38 provozovatelů základní služby s 56 informačními systémy základní služby. Institut byl zaveden na základě požadavků ze Směrnice Evropského parlamentu a Rady (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Uni (Směrnice NIS), kdy pro účely České republiky byla rozšířena odvětvová kritéria (o chemický průmysl a pododvětví teplárenství, nakládání s odpadní vodou), stanovená směrnicí a upraveny dopadová kritéria.

Směrnice NIS je významná zejména pro státy, které obdobnou regulaci neměly zavedenu. Pro provozovatele základní služby vyplývají požadavky zejména dle zákona o kybernetické bezpečnosti na rozdíl od provozovatelů kritické informační infrastruktury, které mají povinnosti dané i zákonem o krizovém řízení. Cílem by měla být harmonizace současného stavu. Provozovatelé základní služby byly určováni zejména tam, kde současná kritéria pro určení kritické informační infrastruktury nebyla dostatečná. Jedná se například o odvětví zdravotnictví.

Zjednodušeně řečeno se jedná o pro stát základní informační infrastrukturu, ve které jsou mírnější dopadová kritéria a širší odvětvová kritéria ve srovnání s kritickou informační infrastrukturou. Pokud jde o povinnosti pro provozovatele základní služby, dopadá na ně mírnější regulace i v otázce zavedení bezpečnostních opatření v kybernetické bezpečnosti. Nemusí tak být zavedena stejná úroveň kybernetické bezpečnosti jako u provozovatelů prvků kritické informační infrastruktury.

Pokud by byl institut základní služby zrušen a odvětvová a dopadová kritéria transponována do oblasti kritické informační infrastruktury, jednalo by se o nárůst pouze o 56 prvků kritické informační infrastruktury. V rámci odvětví kritické informační infrastruktury by bylo klíčové rozšíření zejména o chemický průmysl.

V rámci dopadových kritérií pro určování prvků kritické informační infrastruktury by se mohlo po úpravě jednat o následující hranice:

- závažné omezení nebo narušení prvku postihující více než 25 000, 50 000 nebo 500 000 osob (v závislosti na odvětví);
- omezení či narušení provozu prvku kritické infrastruktury;
- hospodářská ztráta vyšší než 0,25 % hrubého domácího produktu;
- nedostupnost prvku pro více než 1 600 osob, který je nenahraditelný jiným způsobem bez vynaložení nepřiměřených nákladů;
- oběti na životech s mezní hodnotou více než 100 nebo 200 mrtvých (v závislosti na odvětví) nebo 1 000 zraněných osob vyžadujících lékařské ošetření;
- narušení veřejné bezpečnosti na významné části správního obvodu obce s rozšířenou působností, které by mohlo vyžadovat provedení záchranných a likvidačních prací složkami integrovaného záchranného systému;
- kompromitace citlivých osobních údajů o více než 200 000 osobách.

Zrušením institutu základní služby a návaznou úpravou odvětvových a dopadových kritérií by se vyřešil dosud přetrvávající problém s neurčením nemocnic jako kritické infrastruktury státu a harmonizace povinností a gescí u provozovatelů kritické informační infrastruktury a základní služby. Pokud by nebylo přistoupeno ke zrušení institutu základní služby, měla by být provedena přinejmenším analýza implementace dopadových kritérií pro prvky kritické infrastruktury v otázkách sociálních a politických dopadů a rovněž dopadů na životní prostředí.

ZÁVĚR

V první části příspěvku byly definovány základní pojmy ve vztahu ke kybernetické bezpečnosti jako je kyberprostor nebo kritická informační infrastruktura. Následovala definice dopadových a odvětvových kritérií pro určování prvků kritické informační infrastruktury a informačních systémů základní služby podle současně platných právních předpisů v České republice. V praktické části příspěvku byla navržena úprava odvětvových a dopadových kritérií pro určování prvků kritické informační infrastruktury, a to rozšířením odvětvových kritérií a snížením dopadových kritérií. S daným se pojí návrh na zrušení institutu základní služby a jeho integraci do současných právních předpisů o kritické informační infrastruktuře.

Pokud by byl institut základní služby zrušen a odvětvová a dopadová kritéria transponována do oblasti kritické informační infrastruktury, jednalo by se o nárůst pouze o 56 prvků kritické informační infrastruktury. Přínosem by byla harmonizace současného stavu, kdy HZS ČR by mohl k těmto systémům přistupovat v oblasti krizového řízení, jako k prvkům kritické informační infrastruktury. Pro zvýšení kybernetické bezpečnosti České republiky je mimo úpravu odvětvových a dopadových kritérií rovněž žádoucí kontinuální ověřování stanovených opatření pro zabezpečení již určených prvků kritické informační infrastruktury a harmonizace systému krizového řízení u HZS ČR v oblasti kybernetické bezpečnosti.

LITERATURA

Akart, B. (2015) Cyber Warfare: Prepping for Tomorrow Book 3, Freedom Preppers.

Cordero, P. D. (2018). Hacking the Cyber Threat A Cybersecurity Primer for Business Leaders and Executives, CreateSpace Independent Publishing Platform.

Cyberspace (2013, Mar 12). Encyclopædia Britannica. Retrieved July 3, 2019, from https://www.britannica.com/topic/cyberspace

Informace 2/2020 - HSUL- 635/KKŘ-2020. Retrieved February 23, 2020, from https://www.hzscr.cz/clanek/informace-2-2020-hsul-635-kkr-2020.aspx

Jirásek, P., Novák, L., & Požár, J. (2015). Výkladový slovník kybernetické bezpečnosti, Policejní akademie ČR v Praze.

Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról. Magyarország Kormánya.

Maisner, M. (2015). Zákon o kybernetické bezpečnosti: komentář, Wolters Kluwer.

Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

Ouyang, A. (2016). Security. Critical Quarterly, 58(3), 107-109. https://doi.org/10.1111/criq.12286

Požár, J. (2005). Informační bezpečnost, Vydavatelství a nakladatelství Aleš Čeněk.

Proces určování kritické informační infrastruktury (2018). NÚKIB. Retrieved June 3, 2019-06-03, from https://www.govcert.cz/cs/regulace-a-kontrola/podpurne-materialy/

Promyslov, V. G., Semenkov, K. V., & Shumov, A. S. (2019). A clustering method of asset cybersecurity classification. Ifac Papersonline, 52(13), 928-933. https://doi.org/10.1016/j.ifacol.2019.11.313

Refsdal, A., Soulhaug, B., & STØLEN, K. (2015). Cyber-Risk Management, Springer.

Rostek, P., Adamec V. Porovnání a návrh kritérií pro určení prvků kritické infrastruktury. Krízový manažment. Žilina: Žilinská univerzita v Žiline, 2014, 13(2), 69. ISSN 1336-0019.

Setola, R., Rosato, V., Kyriakides, E., & Rome, E. (2017). Managing the Complexity of Critical Infrastructures: A Modelling and Simulation Approach, SpringerOpen.

Směrnice Rady 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu.

Theron, P., Bologna, S. (2013). Critical Information Infrastructure Protection and Resilience in the ICT Sector, IGI Global.

Vaníček, J. (2017). Krizový zákon: komentář, Wolters Kluwer.

Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby.

Josef Bernátek, Ing.

České vysoké učení technické v Praze, Fakulta biomedicínského inženýrství, nám. Sítná 3105, 272 01 Kladno

e-mail: bernajo1@fbmi.cvut.cz