CHEMICKÝ PRŮMYSL

KYBERNETICKÁ BEZPEČNOST CHEMICKÉHO PRŮMYSLU V ČESKÉ REPUBLICE

JOSEF BERNÁTEK

České vysoké učení technické v Praze, Fakulta biomedicínského inženýrství, nám. Sítná 3105, 272 01 Kladno
bernajo1@fbmi.cvut.cz

Došlo 17.4.19, přijato 7.11.19.

Klíčová slova: kyberbezpečnost, chemický průmysl, kritická infrastruktura, základní služba

1. Úvod

Kybernetické útoky z března 2019, které postihly tři velké společnosti z odvětví chemického průmyslu z Norska a Spojených států amerických, opětovně upozornily na zranitelnosti v zastaralých průmyslových řídících a kontrolních systémech užívaných v chemické výrobě. Dokonce ani společnosti, jejíž řídící systémy jsou odděleny od internetu, mohou být snadno napadeny škodlivým kódem např. z infikovaného USB disku nebo zařízení IoT (internet věcí). V případě kybernetických útoků finančně motivovaným aktérem, k jakým došlo v případě zmiňovaných útoků z března 2019 vedeným proti společnostem Norsk Hydro, Momentive a Hexion, byly dle odhadů způsobeny stamilionové škody[1]. Útok na chemickou továrnu prostřednictvím kybernetických technologií s úmyslem terorismu nebo aktu války může vyústit nejen ve finanční ztrátu, ale i značné oběti na životech.

Autorem byl pro získání aktuálních dat o provozovatelích základní služby a informačního systému služby v odvětví chemického průmyslu využit institut vyžádání informací dle zákona č. 106/1999 Sb., o svobodném přístupu k informacím u Národního úřadu pro kybernetickou a informační bezpečnost (dále jen NÚKIB). Rovněž byla autorem stanovena hypotéza předpokládající určení nejméně 15 provozovatelů základní služby z odvětví chemického průmyslu k obdržení odpovědi NÚKIB na vyžádanou žádost.

2. Definice základních pojmů a legislativní východiska EU a ČR

Bezpečnost představuje vlastnost objektu nebo subjektu určující stupeň jeho ochrany proti možným hrozbám. Hrozba je skutečnost, událost, síla nebo osoba, jejíž působení může způsobit poškození, ztrátu důvěry nebo hodnoty aktiva. Riziko vyjadřuje pravděpodobnost, s jakou bude hodnota aktiva poškozena působením hrozby[2]. Kybernetickou bezpečnost lze chápat jako souhrn právních, organizačních, technických a vzdělávacích prostředků pro zajištění ochrany digitálního prostředí a umožňujícího vznik, zpracování a výměnu informací[3].

Evropská unie se začala více zabývat otázkami spojenými s kritickou infrastrukturou po závažných mimořádných událostech a krizových situacích, které postihly jak členské, tak nečlenské země. Před 11. září 2001 byly na nadnárodní úrovni opomíjeny dopady spojené s útoky na kritickou infrastrukturu. Po teroristických útocích v New Yorku, Madridu a Londýně přijala Evropská komise 20. října 2004 sdělení Radě a Evropskému parlamentu o ochraně kritické infrastruktury při boji proti terorismu[4]. Sdělení obsahuje mj. definici hrozby, kritické infrastruktury, včetně výčtu stupňů dopadů a dále požadavek na vymezení, na úrovni členských států a na evropské úrovni[5].

V České republice byla problematika kritické infrastruktury do právního řádu zakotvena novelou zákona č. 240/2000 Sb., o krizovém řízení (dále jen krizový zákon) účinnou k 1. lednu 2011. Novelizace krizového zákona byla učiněna zejména na základě povinnosti ze směrnice Rady č. 2008/114/ES z 8. prosince 2008, o určování a označování evropských kritických infrastruktur a posuzování potřeby zvýšit jejich ochranu[6].

Pokud se zaměříme na českou legislativu, krizový zákon definuje ve vztahu ke kritické infrastruktuře následující pojmy:

- Kritická infrastruktura je prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, jehož narušení funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatel a zdraví osob nebo ekonomiku státu;
- Evropská kritická infrastruktura je kritická infrastruktura na území České republiky, jejíž narušení by mělo závažný dopad i na další členský stát Evropské unie;
- Prvek kritické infrastruktury je zejména stavba, zařízení, prostředek nebo veřejná infrastruktura, určený podle průřezových a odvětvových kritérií;
- Ochrana kritické infrastruktury představuje opatření zaměřená na snížení rizika narušení funkce prvku kritické infrastruktury;
- Subjektem kritické infrastruktury je provozovatel prvku kritické infrastruktury[7].

Krizový zákon stanovil subjektům kritické infrastruktury odpovědnost za ochranu prvků kritické infrastruktury a rovněž povinnost vypracování plánu krizové připravenosti subjektu kritické infrastruktury do 1 roku od určení prvku. Dále zákon stanovil povinnost oznámit příslušnému ministerstvu nebo jinému ústřednímu správnímu úřadu bez zbytečného odkladu informace o změnách, které mohou mít vliv na určení prvku kritické infrastruktury, zejména

informace o trvalém zastavení provozu, ukončení činnosti nebo restrukturalizaci[7].

Nařízením vlády č. 462/2000 Sb. k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení, jsou mj. stanoveny náležitosti a způsob zpracování plánu krizové připravenosti subjektu kritické infrastruktury[8].

Pro určení prvků kritické infrastruktury je klíčové nařízení vlády č. 432/2010 z 22. prosince 2010 o kritériích pro určení prvků kritické infrastruktury, které stanoví průřezová a odvětvová kritéria. Mezi průřezová kritéria řadíme dle ust. § 1 nařízení následující hlediska:

– Počet obětí s mezní hodnotou více než 250 osob nebo více než 2500 osob s následnou hospitalizací po dobu delší než 24 hodin;
– Ekonomický dopad s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu;
– Dopad na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 tisíc osob.

Mezi odvětvová kritéria pro určení prvku kritické infrastruktury se dle přílohy nařízení řadí odvětví energetika, vodní hospodářství, potravinářství a zemědělství, zdravotnictví, doprava, komunikační a informační systémy, finanční trh a měna, nouzové služby a veřejná správa. V rámci odvětví č. VI. Komunikační a informační systémy je pro určování prvků kritické informační infrastruktury klíčové pododvětví G. Oblast kybernetické bezpečnosti, které zahrnuje:

a) Informační systém, který významně nebo zcela ovlivňuje činnost určeného prvku kritické infrastruktury a který je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období přesahujícím 8 hodin;
b) Komunikační systém, který významně nebo zcela ovlivňuje činnost určeného prvku kritické infrastruktury a který je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období přesahujícím 8 hodin;
c) Informační systém spravovaný orgánem veřejné moci obsahující osobní údaje o více než 300 tisících osobách;
d) Komunikační systém, zajišťující připojení nebo propojení prvku kritické infrastruktury, s kapacitou garantovaného datového přenosu nejméně 1 Gbit/s.

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 naplňujícího tato kritéria nezbytná pro zajištění kybernetické bezpečnosti[9].

Prakticky se v případě prvků kritické informační infrastruktury jedná o takové informační nebo komunikační systémy, případně systémy ICS/SCADA, které naplní kritéria pro určení prvků kritické informační infrastruktury. Určování prvků poté probíhá po vzájemném jednání mezi potenciálními povinnými subjekty a zástupci NÚKIB. Zjednodušeně, pokud narušení bezpečnosti informací (důvěrnost, dostupnost, integrita) informačního nebo komunikačního systému subjektu může vyústit alespoň v 1 následek uvedený v průřezových kritériích (oběti, hospitalizace osob, hospodářské ztráty, omezení poskytování nezbytných služeb nebo jiný zásah do každodenního života) a zároveň informační nebo komunikační systém splňuje alespoň 1 z odvětvových kritérií (odvětví VI. Komunikační a informační systémy), část G. Oblast kybernetické bezpečnosti, písm. e), lze jej zařadit do kritické informační infrastruktury. Zařazení poté probíhá odlišně v případě organizačních složek státu a ostatních subjektů. Pokud je subjekt organizační složkou státu, informační nebo komunikační systém určí jako kritickou informační infrastrukturu NÚKIB vydáním opatření obecné povahy. Pokud není subjekt organizační složkou státu, NÚKIB navrhne Ministerstvu vnitra zařadit informační nebo komunikační systém do seznamu, který bude následně předložen vládě ČR. Vláda ČR poté rozhodne usnesením a navrhovaný informační nebo komunikační systém určí v příloze k tomuto usnesení prvkem kritické infrastruktury[10].

3. Provozovatelé základní služby

Odborná veřejnost mnohdy upozorňovala na neopodstatněnou absenci chemického průmyslu mezi odvětvími uvedenými v odvětvových kritériích pro určování prvků kritické infrastruktury, resp. kritické informační infrastruktury. Novelou zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „zákon o kybernetické bezpečnosti“), účinnou 1. července 2017, která transponovala směrnici Evropského parlamentu a Rady EU o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (dále jen NIS) byly definovány základní a digitální služby a rozšířeny oblasti, na které zákon o kybernetické bezpečnosti dopadá mj. výslovně i o odvětví chemického průmyslu.

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 by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v uvedených odvětvích (energetika, doprava, bankovnictví, infrastruktura finančních trhů, zdravotnictví, vodní hospodářství, digitální infrastruktura a chemický průmysl). Informační systém základní služby je informační systém, na jehož fungování je poskytování základní služby závislé. Provozovatelem základní služby je orgán nebo osoba poskytující základní službu a která je určena NÚKIB. Provozovatelé základní služby jsou mj. povinni zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti informačního systému základní služby a vést o nich bezpečnostní dokumentaci. Stejně tak jsou povinni zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smluv s dodavatelem uzavírané[11].

NÚKIB rozhodnutím určí provozovatele základní

služby a informační systém základní služby, pokud budou naplněna odvětvová a dopadová kritéria zohledňující významnost poskytovaných služeb a dopadů případného kybernetického bezpečnostního incidentu[11]. Kritéria pro určení provozovatele základní služby jsou uvedena ve vyhlášce č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby, která nabyla účinnosti 1. února 2018. Pokud se zaměříme na odvětví chemického průmyslu, tak v odvětvových kritériích se zohledňuje druh služby a druh subjektu, nikoliv však speciální kritérium druhu subjektu. Mezi druhy služby se řadí výroba technických plynů, hnojiv nebo dusíkatých sloučenin, pesticidů nebo jiných agrochemických přípravků, výbušnin, základních farmaceutických výrobků, farmaceutických přípravků, jiných základních anorganických látek, jiných základních organických chemických látek a zpracování jaderného paliva. Aby byla naplněna dopadová kritéria v případě odvětví chemického průmyslu, dopad kybernetického bezpečnostního incidentu v informačním systému nebo síti elektronických komunikací, na jejichž fungování je závislé poskytování služby, by mohl způsobit:

a) Závažné omezení či narušení druhu služby postihující více než 50 tisíc osob;
b) Závažné omezení či narušení jiné základní služby nebo omezení či narušení provozu prvku kritické infrastruktury;
c) Hospodářskou ztrátu vyšší než 0,25 % HDP;
d) Nedostupnost druhu služby pro více než 1600 osob, která není nahraditelná jiným způsobem bez vynaložení nepřiměřených nákladů;
e) Oběti na životech s mezní hodnotou více než 100 mrtvých nebo 1000 zraněných osob vyžadujících lékařské ošetření nebo
f) 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[12].

Ke dni 15. února 2019 NÚKIB určil dle dostupných dat, opatřením obecné povahy, celkem 30 provozovatelů základní služby a 30 informačních systémů základní služby. V případě určených provozovatelů základní služby se jednalo o 1 provozovatele z odvětví doprava, 16 z odvětví zdravotnictví a 13 z odvětví digitální infrastruktura. V odvětví chemický průmysl nebyl NÚKIB určen jediný provozovatel základní služby, ani informační systém provozovatele základní služby. K 15. únoru 2019 NÚKIB evidoval celkem 45 subjektů kritické informační infrastruktury, 114 prvků kritické informační infrastruktury a 178 významných informačních systémů. V rámci odvětví chemického průmyslu však nebyl NÚKIB evidován jediný subjekt nebo prvek kritické informační infrastruktury, ani významný informační systém. Není však vyloučeno, že v průběhu roku 2019 bude některý z provozovatelů základní služby v odvětví chemického průmyslu ze strany NÚKIB určen[13]. Od 1. května 2019 musí případní určení provozovatelé základní služby plnit povinnosti, vyplývající ze zákona o kybernetické bezpečnosti, z čehož rovněž vyplývá možnost kontrol ze strany NÚKIB.

4. Šíření nejlepší praxe a edukačních aktivit na národní úrovni

Národní institut pro standardy a technologii Spojených států amerických (dále jen NIST) vydal v roce 2014 dokument, označený jako rámec pro zlepšení kybernetické bezpečnosti v kritické infrastruktuře, sestávající ze standardů, doporučení a nejlepší praxe pro zvládání kybernetických rizik[14]. Ministerstvo vnitřní bezpečnosti Spojených států amerických navázalo na aktivity NIST a vydalo v roce 2015 rámec pro implementaci kybernetické bezpečnosti v chemickém sektoru. Implementace publikovaných rámců kybernetické bezpečnosti poskytuje mechanismus pro organizace, za účelem identifikace nedostatků, prioritizace příležitostí pro zefektivnění, vyhodnocení postupu, sjednocení s nejlepší praxí a další doporučení z oblasti kybernetické bezpečnosti[15]. Rámec pro implementaci kybernetické bezpečnosti v chemickém sektoru rovněž obsahuje odkaz na webovou aplikaci pro vlastní hodnocení bezpečnosti chemických provozů a na protiteroristické standardy v chemických provozech[16].

V České republice má v gesci problematiku kybernetické bezpečnosti z pozice ústředního správního úřadu NÚKIB. Pro oblast chemického průmyslu NÚKIB prozatím žádný implementační nebo edukační dokument veřejně nepublikoval, nicméně jeho zástupci uspořádali 21. února 2018 workshop pro členské organizace Svazu chemického průmyslu České republiky ke specifikům chemického průmyslu v kybernetické bezpečnosti, dopadovým kritériím i vyhlášce o kybernetické bezpečnosti. Svaz chemického průmyslu také vyvíjí aktivity pro zvýšení povědomí o kybernetické bezpečnosti, kdy již v roce 2016 v rámci svého výboru pro péči o hmotný majetek a jeho údržbu vznikla pracovní skupina decentralizovaných řídících systémů (dále jen DCS)[17]. Opomenout nelze ani aktivity české pobočky AFCEA prostřednictvím jí zřízené pracovní skupiny Kybernetická bezpečnost, jako vydání českého slovníku pojmů kybernetické bezpečnosti nebo pořádání osvětových seminářů na Policejní akademii ČR v Praze[18]. Nezbytná je nejen edukace manažerů kybernetické bezpečnosti a konkrétního kyber-bezpečnostního personálu, ale již studentů jakožto potenciálních zaměstnanců chemických provozů. Nejen na studenty cílí Středoškolská soutěž v kybernetické bezpečnosti pořádaná českou pobočkou AFCEA, které se v loňském druhém ročníku účastnilo více než 3000 studentů z 86 středních škol České republiky[19].

5. Závěr

Zajištění absolutní bezpečnosti, resp. kybernetické bezpečnosti není reálné. Lze však učinit opatření pro zajištění bezpečnosti, dle dodržování zásad nejlepší praxe za přijatelných nákladů, která mohou zajistit akceptovatelnou úroveň bezpečnosti. Mezi doporučení lze zařadit např. specifikace detailních požadavků pro hodnocení chemického provozu a bezpečnosti, zavedení auditních kontrol se stanovením sankcí při nedodržení bezpečnostních pravidel,

modernizace systémů nouzové komunikace, aktualizace plánů připravenosti a reakce na incidenty a školení všech pracovníků v oblastech kybernetické bezpečnosti[19]. Rovněž nelze opomenout pravidelná hodnocení bezpečnosti daného provozu, jakož i systému řízení bezpečnosti a kritérií rozvržení bezpečnosti, zaměřených na optimalizaci dostupných vrstev ochrany[20].

Z dostupných dat NÚKIB se nepotvrdila autorem stanovená hypotéza, jelikož na základě dostupných dat k 15. únoru 2019 NÚKIB neurčil ani jednoho provozovatele základní služby nebo informačního sytému základní služby z odvětví chemického průmyslu. Kybernetickou bezpečnost však nelze brát v potaz, pouze pokud k tomu má subjekt zákonnou povinnost. Stejně jako v případě některých vysokých škol, na které zákon o kybernetické bezpečnosti primárně nedopadá, je vhodné i u neurčených provozovatelů základní služby a informačního systému základní služby z odvětví chemického průmyslu aplikovat nejlepší praxi z oblasti kybernetické bezpečnosti.

LITERATURA

1. https://www.chemistryworld.com, staženo 2. 4. 2019.
2. Požár J.: *Informační bezpečnost*, Vydavatelství a nakladatelství Aleš Čeněk, Plzeň 2005.
3. Jirásek P., Novák L., Požár J.: *Výkladový slovník kybernetické bezpečnosti*, Policejní akademie ČR v Praze, Praha 2015.
4. *Ochrana kritické infrastruktury*, Česká asociace bezpečnostních manažerů, Praha 2011.
5. Sdělení Komise Radě a Evropskému parlamentu – *Ochrana kritické infrastruktury při boji proti terorismu*, Evropská komise, Brusel 2004.
6. *Směrnice Rady o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu*, Rada EU, Brusel 2008.
7. Vaníček J.: *Krizový zákon: komentář*, Wolters Kluwer, Praha 2017.
8. Nařízení vlády č. 462/2000 k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., *o krizovém řízení*. Praha 2000.
9. Nařízení vlády č. 432/2010 *o kritériích pro určení prvku kritické infrastruktury*. Praha 2010.
10. https://www.govcert.cz, staženo 2. 4. 2019.
11. Zákon č. 181/2014 sb. *o kybernetické bezpečnosti*. Sbírka zákonů 2014.
12. Vyhláška č. 437/2017 o *kritériích pro určení provozovatele základní služby*, Praha 2017.
13. https://www.nukib.cz, staženo 7. 4. 2019.
14. National Institute of Standards and Technology: *Cyber Security Framework*, 2019.
15. Department of Homeland Security: *Chemical Sector Cybersecurity Framework Implementation Guidance*. Washington 2015.
16. Department of Homeland Security: *Risk-Based Performance Standards Guidance: Chemical Facility Anti-Terrorism Standards*. Washington 2009.
17. https://www.schp.cz, staženo 10. 4. 2019.
18. https://afcea.cz/, staženo 10. 4. 2019.
19. Mae Lippin T., McQuiston T. H., Bradley-Bull K., Burns-Johnson T., Cook L., Gill M. L., Howard D., Seymour T. A., Stephens D., Williams B. K.: *Chemical Plants Remain Vulnerable to Terrorists: A Call to Action*. Environmental Health Perspectives. North Carolina 2006.
20. Moreno V. C., Reniers G., Salzano E., Cozzani V.: *Analysis of physical and cyber security-related events in the chemical and process industry*. Process Safety and Environmental Protection, 2018.

J. Bernátek *(Czech Technical University in Prague, Faculty of Biomedical Engineering, Kladno):* **Cybersecurity of Chemical Industry in the Czech Republic**

The paper deals with the legislative requirements and specifications of cybersecurity in the chemical industry, including the criteria for designating basic service operators under the Cyber Security Act. It also addresses the issue of the number of basic services designated operators by the National Cyber and Information Security Agency (NCISA). By February 15, 2019, NCISA has not designated a single basic service operator or the information system of the basic service operator. It can be expected that the NCISA will determine the entities on an ongoing basis in the coming years, which will require the obligated entities to comply with legal requirements. At the end of the paper, proposals for measures to increase the cybersecurity of chemical plants by dissemination of best practices and educational activities at the national level are set.

Keywords: cybersecurity, chemical industry, critical infrastructure, basic service