Časopis výzkumu a aplikací v profesionální bezpečnosti (JOSRA). JOSRA 4 - 2020, roč. 13.

Kybernetický útok jako hrozba pro BOZP v podnicích

30.12.2020

Cyber attack as OHS threat in enterprises

Pavel Danihelka, Lenka Schreiberova, Jan Jurásek

Vysoká škola báňská - Technická univerzita Ostrava; pavel.danihelka@vsb.cz, lenka.schreiberova@vsb.cz

bezpečnost provozu | BOZP | kybernetická bezpečnost | kybernetické útoky

Abstrakt

Provozovatel je povinen zajistit bezpečnost svých zaměstnanců a ostatních osob s jeho vědomím se vyskytujících v provozech nejen za běžných pracovních podmínek, ale také v mimořádných situacích, které lze předvídat. Jednou z takovýchto situací je kybernetický útok, ať už vedený jen na informační systémy, nebo zaměřený i na fyzické ovládnutí technologií a sabotáž. Význam těchto akcí pak poroste s přechodem na Průmysl 4.0. Příspěvek se zabývá historií kybernetických útoků na podniky v cizině i u nás s vytýčením významných milníků v jejich vývoji, jejich dopady na podnik i bezpečnost a nutností tento problém řešit.

Klíčová slova: kybernetický útok, bezpečnost provozu, BOZP

Abstract

Operator of any facility is responsible for ensuring the safety of employee as well as other persons present with his/her agreement in the facility and this rule is valid not only in normal working conditions, but also in emergencies. One from newly aroused emergency is the cyber-attack, which can be oriented to information system only or can involve cyber – physical action with the control of technology and sabotage. Importance of this type of actions will grow with implementation of Industry 4.0. This contribution deals with the history of cyber-attacks oriented to enterprises and the description of milestones, with cyber-attack impacts to enterprise and OHS. The necessity to mitigate this risk is the conclusion.

Keywords: cybernetic attack, process safety, OHS

Přijat k publikování / Received for publication 2. 11. 2020

1. Úvod

V měnícím se prostředí současné doby se objevují a dynamicky vyvíjejí různé nové hrozby, které se mohou promítat nejen do ekonomických a provozních podmínek, ale také v oblasti bezpečnosti práce. Jednou z nově se objevujících možností vnějších hrozeb vůči podniku jsou kybernetické útoky a mimořádné situace s nimi spojené. Požadavky na provozovatele dle Zákoníku práce ve smyslu jeho § 102 odst. (6) zahrnují povinnost přijmout opatření pro případ zdolávání mimořádných událostí, jako jsou havárie, požáry a povodně, jiná vážná nebezpečí a evakuace zaměstnanců včetně pokynů k zastavení práce a k okamžitému opuštění pracoviště a odchodu do bezpečí. Je tedy zřejmé, že i mimořádné stavy a události způsobené kybernetickými útoky by měly být do tohoto požadavku zahrnuty a zákoník práce myslí v následujícím odstavci - § 102, odst. (3) – i na změny a vývoj, kde udává, že zaměstnavatel je povinen přizpůsobovat opatření měnícím se skutečnostem, kontrolovat jejich účinnost a dodržování a zajišťovat zlepšování stavu pracovního prostředí a pracovních podmínek. Tento článek se proto zabývá rozborem toho, zda lze kybernetické útoky chápat jako ohrožení bezpečnosti práce a nakolik jsou podniky na tuto situaci připraveny.

2. Útoky v kybernetickém prostoru

V průběhu posledních dvou desetiletí došlo k dramatickému, až explozivnímu nárůstu využívání výpočetní techniky a jak společnost, tak ekonomika se staly na informačních a komunikačních technologiích (ICT) natolik závislé, že si nyní lze jen velmi obtížně představit situaci jejich úplného selhání. Daleko pravděpodobnější však je selhání jen části funkcí, a to nejen v oblasti „safety“, tedy selhání IT technologie nebo náhodný proces nesprávné funkce digitálního systému, ale hlavně v oblasti „security“, kdy jsou prostředky informační a komunikační techniky zneužity ke zlovolnému činu, tedy ke kybernetickému útoku. Ten je nejčastěji definován jako úmyslné jednání útočníka v kybernetickém prostoru, které směřuje proti zájmům jiné osoby nebo organizace.

Informace a data představují významný konkurenční potenciál. Informace a jejich obsah mohou rozhodovat nejen o prosperitě či úpadku podniku či jednotlivce z ekonomických a politických důvodů, ale ve své podstatě jsou schopny ovlivnit také fyzické dění v podniku samém, včetně bezpečnosti jeho zaměstnanců. Pokud však chce v současné společnosti podnik prosperovat, není možné se od informačních technologií oprostit a nemá smysl tyto technologie nevyužívat. V poslední době se navíc začala rozvíjet čtvrtá průmyslová revoluce (Industry 4.0), jejíž hlavním vektorem je digitalizace a Internet věcí – Internet of Things (IoT). Propojená zařízení a stroje tak mezi sebou navzájem stále více komunikují, a to i prostřednictvím sítí elektronických komunikací, což usnadňuje přístup útočníka k nechráněným zařízením či informacím, ale také zvyšuje možnost fyzického ohrožení osob.

Informační a komunikační technologie jsou oborem, který se nejdynamičtěji a nejmasivněji vyvíjí, avšak otázkám bezpečnosti či zabezpečení není obvykle věnována taková pozornost jako například tomu, jaký bude design výrobků, kapacita úložného prostoru, možnosti telekomunikace s dalšími zařízeními [1]. To vysoce kontrastuje s tím, že například Globální ekonomické fórum zařadilo v roce 2020 kybernetické útoky mezi deset nejvýznamnějších globálních rizik s ohledem jak na dopady, tak na pravděpodobnost vzniku.

3. Případové studie v zahraničí

Na rozdíl od hackerských aktivit cílených na získání citlivých dat nebo přístupů k finančním prostředkům, kterým je věnována poměrně velká mediální pozornost, jsou kybernetické útoky na podniky jen málo reportovány v médiích, ačkoliv jsou průmyslové řídící a kontrolní systémy již dlouhou dobu cílem kybernetických útoků, jejichž komplexita navíc roste [2]. V následujících případových studiích jsou ukázány některé významné příklady.

3.1 Maroochy Water

Australská vodohospodářská firma v roce 2000 po zjištění nestandardního chování čerpacích systémů odpadních vod zahájila pátrání, jehož výsledkem bylo odhalení, že odmítnutý uchazeč o zaměstnání, Vitek Boden, s cílem se pomstít ovládnul dálkově ovládaný systém SCADA (Supervisory Control and Data Acquisition) a postupně vypustil milióny litrů nevyčištěné odpadní vody do vodních recipientů [3]. Tento případ ukázal, patrně jako první v historii, že lze pomocí informačních technologií provést fyzický útok včetně uvolnění nebezpečných látek do prostředí, tedy ohrozit zdraví.

3.2 Exploze ropovodu Baku-Tbilisi-Ceyhan (BTC) v Refahiye

Tato exploze (Turecko, 2008) byla vyvolána přetlakem v potrubí a vyvolala zpočátku rozsáhlou diskusi, zda byla iniciována technickým selháním nebo kybernetickým útokem [2]. Stopy po útoku, vymazání záznamů kontrolních kamer a další indicie vedly postupně k přesvědčení, že se opravdu jednalo o kybernetický útok, jak konstatuje zpráva Bloomberg „Mysterious 08 Turkey Pipeline blast opened new cyberwar“ [4]. Existuje také podezření, že se jednalo o akt ruských hackerů, a poprvé tak bylo použito kybernetického útoku na fyzické zařízení ze zahraničí [5]. Rozsah takto vyvolané havárie plně odpovídá definicím závažné havárie dle směrnice Seveso a přináší tak přímé ohrožení životů, zdraví a životního prostředí.

3.3 STUXNET – Destrukce centrifug na obohacení uranu v Natanz (Írán, 2010)

Je považována za „vlajkovou loď“ kybernetické války a změnila nejen pohled na bezpečnost technologických zařízení se sofistikovaným řízením pomocí informačních technologií, ale také koncept moderní asymetrické války. Na tomto kybernetickém útoku se ukázala anatomie kyberneticko-fyzického útoku ve svých třech vrstvách, tedy proniknutí do informačního systému, zmanipulování řídících funkcí (např. SCADA, v Natanz se jednalo hlavně o ovladače S7-315 a S7-417) a detailní znalost vlastní napadené technologie a její zranitelnosti [6]. Původ malware STUXNET nebyl nikdy prokázán, v podezření je spolupráce tajných služeb Izraele a USA. Další, nejasnou událostí v jaderném programu Íránu s potenciálním dopadem na BOZP je letošní exploze v Natanz, u které je sice zřejmé, že se jednalo o sabotáž, není však prokázáno, zda to byl kybernetický útok. Íránská vláda kybernetický útok popírá, což může být motivováno snahou nepřipustit veřejně zranitelnost tak citlivé technologie, ale v materiálech izraelského Begin-Sadatova centra pro strategické studie [7] je naznačen opak. Kybernetická válka mezi Íránem a Izraelem pokračuje i útoky na civilní cíle, typicky na infrastruktury. V květnu 2020 uskutečnil Írán několik pokusů o napadení dodávky vod v Izraeli a Izrael zaútočil několikahodinovým kybernetickým vyřazením íránského přístavu Shahid Rajaae z provozu narušením dodávky vody a energie [7],[8]. O tom, že se jednalo o kybernetický útok vedený z Izraele, není pochyb, neboť krátce poté, 24. 6. 2020, byla speciální izraelská jednotka Unit 8200, Military Intelligence’s Research Division vyznamenána velitelem tajných služeb Tamirem Hyamanem za „jedinečný a působivý výsledek“ [9]. Z hlediska BOZP je významný fakt to, že útoky byly vedeny proti běžným firmám, a i když byly evidentně cíleny tak, aby více prokázaly schopnost napadnout protivníka víceméně kdekoliv v citlivých oblastech infrastruktury, než aby ohrozily zdraví a životy, výpadky energií a médií mohou ohrozit zdraví i životy.

3.4 Německá ocelárna

Německý spolkový úřad pro informační bezpečnost (BSI) ve své výroční zprávě z roku 2014 [10] uvádí případ, kdy došlo v nejmenovaném ocelářském podniku k vyřazení prakticky celého systému kontroly a řízení kybernetickým útokem, takže například nebylo možné ani monitorovat, ani ovládat stav vysoké pece. Případné nebezpečné stavy by tak nebylo možné ovládat. I když případ skončil vyjma ekonomických a technologických ztrát bez závažných problémů, ukazuje na nebezpečí jak pro provoz, tak pro zaměstnance.

3.5 Útoky na infrastruktury na Ukrajině

Vzhledem ke svému charakteru včetně rozsáhlému využívání informačních a komunikačních technologií, a velkým dopadům jejich selhání, jsou infrastruktury různého druhu lákavým cílem pro kybernetické útoky. Ilustrativní jsou útoky na ukrajinskou energetickou síť [2], kdy před Vánocemi roku 2015 byl na Ukrajině kyberneticky vyvolán blackout, který zasáhnul 230 000 lidí a velké množství podniků, když vyřadil 30 elektrických stanic a pro ně určený systém SCADA. Dodávku energie se podařilo obnovit až za 6 hodin, a to manuálně. Necelý rok později se útok opakoval v oblasti Kyjeva se stejně velkým rozsahem, ale ačkoliv byl útok sofistikovanější, podařilo se obnovit dodávku energie za poloviční čas. Pokusů o ovládnutí infrastruktur, hlavně energetické, je známo velké množství.

Vyvolání blackoutu má velký význam z hlediska bezpečnosti podniku a jeho zaměstnanců, zvláště pak v případech, kdy podnik nemá dostatečně výkonný a disponibilní náhradní zdroj energie. Ohroženy jsou nejen kontrolní a řídící funkce provozu, ale také bezpečná odstávka a mnozí pracovníci v rizikových provozech, kde jsou využívána nejrůznější kontrolní měření zajišťující bezpečnost provozu i pracovního prostředí.

4. Zkušenosti z České republiky

4.1 Stav v České republice

Česká republika není v oblasti kybernetické bezpečnosti výjimkou a ani jí se kybernetické incidenty nevyhýbají. Národní ústav pro informační a kybernetickou bezpečnost (NÚKIB) ve své výroční zprávě za rok 2019 uvádí graf vyobrazující rostoucí počet případů kyberkriminality v České republice [11].

Obr. 1: Nárůst počtu případů kybernetické kriminality v ČR v letech 2011 až 2019. Zdroj: [11]

Zpráva NÚKIB také konstatuje, že v České republice se v roce 2019 vyděračský malware nejvíce projevil v prosinci v podobě kampaně ransomwaru Ryuk. Ten například napadl sítě Nemocnice Rudolfa a Stefanie Benešov a těžební společnosti OKD (viz níže). V roce 2019 došlo k dalšímu nárůstu počtu kybernetických útoků proti naší zemi, z nichž některé lze označit za velmi vážné. Řada veřejných i soukromých institucí se musela vyrovnávat s obranou před těmito útoky a odstraňováním jejich následků. Podle průzkumu provedeného NÚKIB se v oblasti kybernetické bezpečnosti řada dotazovaných organizací potýkala s nedostatkem financí ve vlastních rozpočtech a nedostatkem odborníků.

Téměř žádný z respondentů neměl obsazené všechny potřebné pozice v oblasti kybernetické bezpečnosti.

Z hlediska bezpečnosti práce a možného ohrožení zdraví nejen zaměstnanců jsou klíčové události v kybernetické bezpečnosti dva loňské útoky pomocí ransomwaru Ryuk na nemocnici v Benešově a na OKD.

4.2 Útok na nemocnici Rudolfa a Stefanie Benešov

Nemocnice Rudolfa a Stefanie v Benešově byla napadena kybernetickým útokem 11. prosince 2019 v noci. Po dobu sedmi dní byl provoz nemocnice zcela paralyzován, všechny akutní i plánované operace byly na konci roku 2019 zrušeny, nefungoval ambulantní provoz a byla poskytována péče pouze těm pacientům, kteří byli již hospitalizováni. Nejtěžší pacienti byli přeloženi do jiných nemocnic.

Zdravotnický personál pracoval řadu dní ve velmi improvizovaném provozu a téměř měsíc po události neměl plně funkční všechny potřebné počítačové systémy a aplikace. Náběh nemocnice při obnovování počítačové sítě byl složitý, pomalý a finančně náročný. Naštěstí nedošlo k ohrožení zdraví pacientů ani personálu.

Kybernetický útok způsobil škodu přes 59 milionů korun. Největší ztráty nemocnice zaznamenala v souvislosti s omezením lékařských výkonů, nemocnice nedostala proplacené finanční prostředky od zdravotních pojišťoven na původně plánovaná vyšetření, zákroky a operace.

Na nemocnici zaútočil ransomware, tedy počítačový vir, který zašifruje data na počítači a serverech a následně požaduje po napadeném výkupné, obvykle ve formě obtížně stopovatelné kryptoměny. Nejednalo se však o cílený útok přímo na tuto konkrétní nemocnici, současně s tímto útokem byly napadeny i další počítače některých institucí státní správy.

Kriminalisté na případu spolupracovali s IT specialisty benešovské nemocnice, s pracovníky Národní centrály proti organizovanému zločinu (NCOZ), zaměstnanci Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) a zaměstnanci společnosti ESET. Pachatele se nepodařilo dohledat, policie případ odložila.

4.3 Kybernetický útok na Ostravsko-karvinské doly

Počítače OKD ochromil těsně před Vánocemi roku 2019 hackerský útok, který způsobil okamžitou nefunkčnost celé sítě těžařské firmy a všech jejich serverů. Společnost OKD proto z bezpečnostních důvodů přerušila těžbu ve všech svých dolech na Karvinsku. Ochromena byla počítačová síť firmy, a tím také všechny významné prvky monitoringu a zajištění BOZP, například měření koncentrace explozivního metanu, oxidu uhelnatého, stav větrání pracovišť atd. Z bezpečnostních důvodů proto byli horníci z šachet evakuováni.

Firma postupně zajistila reinstalace nejdůležitějších stanic a obnovu systémů, jež kvůli zajištění těžby a bezpečnosti zpočátku pracovaly v oddělené malé síti, kterou vytvořili počítačoví experti. Postup připomíná regeneraci elektrické sítě po rozsáhlém blackoutu, využívající tzv. ostrovní provozy. Jedním z klíčových prvků pak bylo zajištění bezpečnosti práce. Tato událost ukázala, že kybernetické útoky, i když nejsou prvotně plánovány jako kyberneticko – fyzický akt, se nutně promítají také do stavu BOZP. Psychologicky vzato, právě bezpečnost, spolu s omezenou nebo ztracenou schopností monitoringu a řízení a možností zneužití dat, jsou hlavními motivačními nástroji útočníka při jeho snaze získat výkupné za odblokování viru. Aspekty bezpečnosti práce tak musejí být nedílnou součástí krizových plánů podniku pro případ kybernetického útoku, a to nejen kyberneticko-fyzického (sabotáže), ale i čistě informačního (např. vydírání spojené s informacemi).

Právně vzato, kybernetický útok obdobného charakteru jako loňský v OKD naplňuje všechny znaky trestného činu poškození a ohrožení provozu obecně prospěšného zařízení podle § 276 odst. 1, odst. 2 písm. b) trestního zákoníku. Jako precedent lze chápat rozhodnutí Krajského soudu Ostrava ze dne 27. června 2018, č. j. 5To 178/2018 – 110, kdy

byl vynesen dvouletý podmíněný trest za to, že pachatel oddělil a odcizil celkem 32 metrů telefonního a datového kabelu sloužícího k přenosu dat, signalizace a provozu vnitřních telefonních linek dolu z podzemních pracovišť, kdy tímto jednáním vyřadil z provozu celkem 18 čidel pro měření hladiny důlních plynů, a to metanu a oxidu uhelnatého, 11 tzv. binárních čidel pro sledování funkce ventilátorů, hladiny vody a signalizace otevření dveří skladu střeliva, 12 telefonních linek v podzemní části dolu, 3 automatické systémy pro vypínání důlní elektrické sítě při překročení hladiny důlního plynu metanu a systém ISI pro sledování jednotlivých horníků při práci v rizikové tzv. otřesové sloji, následkem čehož muselo být odvoláno ze dvou pracovišť celkem 10 horníků, neboť nebylo zřejmé, zda jsou jejich pracoviště po vyřazení chodu ventilátoru dostatečně odvětrávána. Horníci mohli být ohroženi škodlivými plyny a ztrátou spojení s povrchem.

5. Závěry

Moderní ekonomika nemůže existovat bez kybernetiky, ta však s sebou přináší nová rizika, například kybernetické útoky na podniky. Světové ekonomické fórum považuje kybernetické útoky za jednu z deseti nejhorších hrozeb moderní doby celkově, a to jak s ohledem na závažnost, tak s ohledem na pravděpodobnost vzniku. NÚKIB, jakožto vrcholná autorita v kybernetické bezpečnosti v České republice, upozorňuje na nedostatečnost ochrany proti kybernetickým útokům u velké části organizací a na jejich rostoucí počet i sofistikovanost. Kybernetické útoky se pak neomezují jen na informace a informační systémy přímo, ale zahrnují také fyzické dopady v provozech, ať už cíleně myšlené sabotáže, nebo sekundární dopady ztráty kontroly nad zařízením (podnikem), což se nutně promítá do bezpečnosti práce i bezpečnosti provozu. Přímo cílené sabotáže pak mohou zneužít i potenciál nebezpečných materiálů a technologií v podniku samém, a to nejen v oblasti jaderného průmyslu, ale také v oblasti nebezpečných chemických látek, kdy by kyberneticko-fyzický útok mohl sloužit k úmyslnému vyvolání závažné chemické havárie s dopady na zdraví a životy nejen v podniku, ale také v jeho okolí.

Jako nezbytnost se tak ukazuje zařazení otázek kybernetické bezpečnosti s ohledem na prevenci a na řešení mimořádných stavů nejen do přímé agendy informační bezpečnosti, ale také do managementu kontinuity činností (Business Continuity Management dle ISO 22301) a do managementu bezpečnosti práce dle ISO 45001.

Poděkování

Vznik tohoto příspěvku byl podpořen projektem Bezpečnostního výzkumu ČR VI20172020060 s názvem „Teroristická hrozba vyvolané chemické havárie a zranitelnost společnosti“.

Literatura

[1] KOLOUCH, Jan ...[et al.]. *Cybersecurity*. Praha: CZ.NIC, 2019. ISBN 978-80-88168-34-8.

[2] HEMSLEY, Kevin E.; FISHER, Ronald E. *History of Industrial Control System Cyber Incidents*. Idaho National Laboratory, 2018.

[3] The cyberspace invaders. *The Age: Independent. Always.* [online]. June 22, 2003 [cit. 2020-06-02]. Dostupné z: https://www.theage.com.au/national/the-cyberspace-invaders-20030622-gdvx44.html.

[4] ROBERTSON, Jordan; RILEY, Michael. Mysterious ’08 Turkey Pipeline Blast Opened New Cyberwar: Cybersecurity. *Bloomberg* [online]. NYC, 2014 [cit. 2020-06-02]. Dostupné z: https://www.bloomberg.com/news/articles/2014-12-10/mysterious-08-turkey-pipeline-blast-opened-new-cyberwar.

[5] Russian hackers now thought to have caused 2008 Turkish oil pipeline explosion. *Hazardex* [online]. 2014 [cit. 2020-06-02]. Dostupné z: http://www.hazardexonthenet.net/article/88497/Russian-hackers-now-thought-to-have-caused-2008-Turkish-oil-pipeline-explosion.aspx

.

[6] LANGER, R. To Kill a Centrifuge: a Technical Analysis of What Stuxnet's Creators Tried to Achieve [online]. The Langner Group, 2013 [cit. 2020-06-02]. Dostupné z: https://www.semanticscholar.org/paper/To-Kill-a-Centrifuge-A-Technical-Analysis-of-What-%E2%80%99-Langner/50988101501366324c11e9e7a199e88a9a899bec.

[7] OFER, Raphael. Was the Iranian Uranium Enrichment Plant at Natanz Sabotaged?: BESA Center for Strategic Studies Perspectives Paper No. 1,658 [online]. BESA, July 24, 2020 [cit. 2020-06-02]. Dostupné z: https://besacenter.org/perspectives-papers/iran-uranium-natanz-sabotage/.

[8] GOL, Jiyar. Iran blasts: What is behind mysterious fires at key sites? *BBC: News* [online]. 6 July 2020 [cit. 2020-07-06]. Dostupné z: https://www.bbc.com/news/world-middle-east-53305940.

[9] AHRONHEIM, Anna. IDF honors troops for successful operation after Iran cyberattack. *The Jerusalem Post* [online]. June 25, 2020 [cit. 2020-06-02]. Dostupné z: https://www.jpost.com/israel-news/following-iran-cyberattack-idf-honors-troops-for-successful-operation-632728.

[10] Bundesamt für Sicherheit in der Informationstechnik (BSI), Die Lage der IT-Sicherheit in Deutschland 2014, Bonn, 2014

[11] *Zprávy o stavu* [online]. Národní úřad pro kybernetickou a informační bezpečnost [cit. 2020-06-02]. Dostupné z: https://www.nukib.cz/cs/infoservis/dokumenty-a-publikace/zpravy-o-stavu-kb/.

Vzorová citace

DANIHELKA, Pavel; SCHREIBEROVÁ, Lenka; JURÁSEK, Jan. Kybernetický útok jako hrozba pro BOZP v podnicích. *Časopis výzkumu a aplikací v profesionální bezpečnosti* [online]. 2020, roč. 13, č. 4. Dostupný z: https://www.bozpinfo.cz/josra/kyberneticky-utok-jako-hrozba-pro-bozp-v-podnicich. ISSN 1803-3687.

Autor článku:
Prof. RNDr. Pavel Danihelka, CSc.
Ing. Lenka Schreiberova, Ph.D.
Mgr. Jan Jurásek