Kybernetická bezpečnost řepařského a cukrovarnického sektoru

CYBERSECURITY OF BEET AND SUGAR SECTOR

Josef Bernátek – České vysoké učení technické v Praze

Finančně motivované kybernetické útoky z března 2019, které postihly výrobní závody chemického průmyslu z Norska a Spojených států amerických a způsobily stamilionové škody, opětovně upozornily na zranitelnosti v zabezpečení řídicích kontrolních systémů (1). Subjekty zajišťující výrobu v oblasti cukrovarnického průmyslu jsou v dnešní době, rovněž jako subjekty z potravinářského (chemického) průmyslu, závislé na průmyslových řídicích systémech označovaných jako dispečerské řízení a sběr dat (SCADA). Tyto systémy zajišťují nejen automatizaci výroby, ale sběrem dat v reálném čase a jejich následnou grafickou interpretací umožňují operátorům výroby včasnější korekce pro optimalizaci produkce (2). Sběr dat a kontrola výroby probíhá za využití programovatelných automatů (PLC) přenášejících data do hlavní stanice. Operátor výroby může sledovat, případně upravit hodnoty výrobního procesu prostřednictvím rozhraní člověk-stroj (HMI) na hlavní stanici. Relevance zobrazovaných dat na HMI je pro operátory výroby klíčová. V průběhu kybernetického útoku mohou být nejen zobrazována nerelevantní data na HMI, ale i útočníkem vzdáleně ovládány PLC.

Výrobu cukru lze zařadit mezi nejvíce energeticky náročné procesy v agrárním sektoru (3). Pro zajištění konkurenceschopnosti je ze strany provozovatelů cukrovarů klíčová implementace technologií, které umožní vyšší míru automatizace. Mezi výhody automatizace v cukrovarnickém průmyslu lze zařadit snížení personálu o 30–40 %, úsporu spotřeby elektrické energie o 5–10 %, zvýšení podílu extrakce, vyšší spolehlivost procesů a snížení pochybení způsobených lidským faktorem (4). Automatizaci prakticky není možno realizovat bez průmyslových řídicích systémů, tudíž je na místě počítat s nutností implementace opatření pro zajištění jejich bezpečnosti.

Za nejznámější příklad kybernetického útoku na průmyslový řídicí systém lze označit působení škodlivého kódu Stuxnet na íránská zařízení pro obohacování uranu. V daném případě, publikovaném v roce 2010, se jednalo o technologicky velmi sofistikovanou a cíleně vykonstruovanou kybernetickou zbraň mající za cíl způsobit poškození výrobních zařízení, za kterou byl s největší pravděpodobností odpovědný státní aktér (5). Pokud se zaměříme na Evropu, v roce 2014 došlo v Německu k infiltraci řídicího kontrolního systému ocelárny a následnému neplánovanému odstavení vysoké pece. Útočníci zpočátku využili techniku sociálního inženýrství při rozesílání podvodných e-mailů, pomocí které vylákali od zaměstnanců ocelárny přihlašovací údaje, jež následně využili k přístupu do produkčních systémů provozu a způsobili selhání komponent řídicího systému (6).

Výrobní zařízení v cukrovarnickém průmyslu nebudou s největší pravděpodobností cílem kybernetických útoků ze strany státních aktérů. Nejpravděpodobnější hrozbu pro tyto systémy mohou představovat útoky typu Ransomware ze strany finančně motivovaných aktérů, jako v případě v úvodu citovaných útoků vůči chemickým společnostem. V případě útoků typu Ransomware dochází k infikaci počítačových systémů a jejich následné blokaci, v krajním případě zašifrování dat v počítačovém systému uložených, s výzvou k uhrazení výkupného pro odblokování počítače, resp. dešifrování dat, nejčastěji ve formě virtuálních měn.

Vyloučit nelze ani zasažení zařízení cukrovaru škodlivým kódem, který nebude cílen na konkrétní subjekt. K obdobné události došlo v roce 2017, kdy Ransomware WannaCry infikoval více než 230 000 zařízení ve 150 zemích bez ohledu na jejich provozovatele. Mezi infikovanými byla jak zařízení soukromých společností jako Bank of China či FedEx, tak i státní organizace jako ruské ministerstvo vnitra nebo Britská národní zdravotní služba. Příčinou značného rozsahu úspěšnosti útoku byly dlouhodobě neaktualizované operační systémy Microsoft Windows na infikovaných zařízeních (7).

U řepařství se v souvislosti s moderními technologiemi můžeme velmi často setkat s pojmem „precizní zemědělství". To zahrnuje takový přístup k agrotechnickým opatřením, který vede ke snížení vstupů pesticidů i hnojiv a snižování negativních dopadů zemědělské činnosti na životní prostředí, a který v konečném důsledku přispívá ke zvýšení konkurenceschopnosti zemědělských podniků (8). V případě produkce cukrové řepy se může jednat o řízení jízdy zemědělské techniky podle družicových polohových systémů, mapování výnosů v průběhu sklizně, automatickou regulaci dávky hnojiva dle mapových podkladů, příp. o využití bezpilotních letounů pro aplikaci pesticidů (9).

Ministerstvo vnitřní bezpečnosti Spojených států amerických vydalo v říjnu 2018 analýzu hrozeb pro technologie precizního zemědělství užívané v rostlinné a živočišné výrobě. Analýza identifikovala hrozby pro důvěrnost, integritu a dostupnost precizního zemědělství za využití vektorů útoku od nesprávného zacházení s USB disky po podvodné e-maily. Jako hrozba pro důvěrnost je uvedeno neoprávněné zpřístupnění dat, pro integritu neoprávněné pozměnění dat a pro dostupnost technologie pak narušení příjmu signálu GPS nebo komunikačních sítí (10).

Pro prevenci hrozeb jak vůči technologiím precizního zemědělství užívaných při produkci cukrové řepy, tak i řídicích kontrolních systémů cukrovarnických závodů lze doporučit široké spektrum kyber-bezpečnostních opatření. Na straně koncových stanic je vhodná implementace ochrany webových prohlížečů, užití širokospektrálních antivirových řešení, omezení

a kontrola síťových portů, protokolů a služeb. Dále sestavení přehledu povoleného hardware a povoleného software, včetně pravidelných aktualizací operačních systémů a užívaného software. Opomenout nelze monitoring a kontrolu před neoprávněným přístupem do počítačových systémů a oddělení výrobních a kontrolních technologií od činností administrativního a obchodního charakteru (10). Je zřejmé, že při současném nedostatku expertů na kybernetickou bezpečnost lze v podmínkách cukrovaru nebo řepařského podniku obtížně zavádět všechna doporučení interními zaměstnanci. Jejich implementaci, včetně případného reálného vykonávání monitoringu, kontroly neoprávněných přístupů a analýz rizik, lze řešit bez větších obtíží outsourcingem u vybraných dodavatelů bezpečnostních řešení.

Na subjekty cukrovarnického a řepařského sektoru v Česku primárně nedopadá zákon č. 181/2014 Sb., o kybernetické bezpečnosti v souvislosti s vykonáváním obvyklé činnosti v těchto oborech. Pro uložení povinností vyplývajících z tohoto zákona musí subjekty naplnit kritéria uvedená v příslušné legislativě. Bylo by však mylné se domnívat, že se v případě absence zákonné povinnosti není nutno kybernetickou bezpečností zabývat. Pro každý podnikatelský subjekt by mělo být samozřejmostí provedení analýz rizik a s tím souvisejícího přijetí příslušných opatření k jejich snížení na akceptovatelnou úroveň. Inspiraci pro nejlepší praxi v zavádění kybernetické bezpečnosti bez ohledu na zákonné požadavky lze získat z vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).

Závěr

Pro udržení konkurenceschopnosti v cukrovarnickém průmyslu je vhodné zvyšování podílu automatizace v rámci všech fází produkce. U řepařského sektoru lze doporučit implementaci prvků precizního zemědělství. V obou výše uvedených případech se bude jednat o řešení závislá na řídicích kontrolních systémech a dalších zařízeních náchylných vůči kybernetickým útokům. Představa zajištění absolutní kybernetické bezpečnosti je stejně jako v případě bezpečnosti práce mylná. Rovněž je mylná představa, že se v případě cukrovarnického nebo řepařského sektoru kybernetickou bezpečností nemusíme zabývat. Implementací nejlepší praxe v zabezpečení užívaných technologií, pravidelnými analýzami rizik a přijetím opatření z těchto analýz vyplývajících, periodickým školením personálu i dalšími bezpečnostními opatřeními lze dosáhnout akceptovatelné úrovně rizika. Dosažení této úrovně by mělo být cílem každého výrobního podniku, nejen v oblastech kritické informační infrastruktury státu, ale i v podnicích produkujících cukrovou řepu a cukr.

Souhrn

Příspěvek pojednává o kybernetických rizicích pro řepařský a cukrovarnický sektor. V případě cukrovarnického průmyslu představuje hlavní riziko napadení řídicích kontrolních systémů škodlivým kódem finančně motivovaného aktéra. V případě řepařského sektoru představují riziko napadení nově zaváděné technologie precizního zemědělství. Cílem příspěvku je rovněž stanovení návrhů opatření pro zvýšení kybernetické bezpečnosti u řepařství a cukrovarnictví jako oblastí, na které primárně nedopadá zákon o kybernetické bezpečnosti.

Klíčová slova: kyberbezpečnost, cukrovarnický průmysl, řepařský průmysl, precizní zemědělství, škodlivý kód.

Literatura

1. Stupp, C.: Norsk Hydro Repairs Systems and Investigates After Ransomware Attack; Norwegian aluminum and energy company confirms LockerGoga virus was used in strike that crippled operations. *The Wall Street Journal*, 9. 4. 2019, [online] https://www.wsj.com.
2. Castaldini, S.: Control system Pcs7 and M.I.S. together for the complete automation of the process in the sugar beet factory of Co.Pro.B. – Minerbio – Italy. In *17th European Symposium on Computer Aided Process Engineering*, 24, 2007, s. 841–846.
3. Rajaeifar, M. A. et al.: A review on beet sugar industry with a focus on implementation of waste-to-energy strategy for power supply. *Renewable and Sustainable Energy Reviews*, 103, 2019, s. 423–442.
4. Balwinder, S.; Lini M.; Sumit P.: Design and Implementation of Smart SCADA in Sugar Mill using LabVIEW. *European Journal of Advances in Engineering and Technology*, 2015, 2, s. 61–65.
5. Fidler, D. P.: Was Stuxnet an Act of War? Decoding a Cyberattack. *IEEE Security & Privacy*. 9, 2011 (4), s. 56–59.
6. Lee, R. M.; Assante, M. J.; Conway, T.: *German Steel Mill Cyber Attack*. SANS Industrial Control Systems, 30. 12. 2014 [online] https://ics.sans.org.
7. Adams, C.: Learning the lessons of WannaCry. *Computer Fraud & Security*, 2018 (9), s. 609.
8. Shannon, D. K.; Clay, D.; Kitchen, R. N.: *Precision agriculture basics*. Madison, WI: ACSESS Publications, 2018, ISBN 978-0891183662.
9. Mahmood, S. A.; Murdoch, A. J.: Adaptation of precision agriculture to root crops (sugar beet and potato). *CAB Reviews*, 13, 2018 (61), s.1–12.
10. *Threats to Precision Agriculture*. 2018 Public-Private Analytic Exchange Program, U. S. Department of Homeland Security, 2018, s. 1–25, 3. 10. 2019, [online] https://www.us-cert.gov.

Bernátek J.: Cybersecurity of Beet and Sugar Sector

The paper deals with the cyber risks for the beet and sugar sectors. In the case of sugar industry, the main risk of industrial control systems attack is a malicious code by a financially motivated actor. In the case of beet sector, there is a risk of attack targeting the newly introduced precision farming technologies. The aim of the paper is also to set out proposals for measures to increase cybersecurity of the beet and sugar sectors as areas not primarily covered by the Cyber Security Act.

Key words: cyber security, sugar industry, beet industry, precision farming, malicious code.

Kontaktní adresa – Contact address:

Ing. Josef Bernátek, České vysoké učení technické v Praze, Fakulta biomedicínského inženýrství, nám. Sítná 3105, 272 01 Kladno, Česká republika, e-mail: bernajo1@fbmi.cvut.cz