Kybernetická bezpečnost v českém cukrovarnictví: výzvy a příležitosti v kontextu nového zákona

CYBERSECURITY IN CZECH SUGAR INDUSTRY: CHALLENGES AND OPPORTUNITIES IN CONTEXT OF NEW LAW

Veronika Kolek Netolická
Fakulta sociálních studií, Masarykova Universita, Brno
Národní úřad pro kybernetickou a informační bezpečnost, Brno

Kybernetická bezpečnost již dávno není oblastí pouze tradiční kritické infrastruktury, jako jsou energetické sítě či finanční instituce. S rostoucí digitalizací napříč sektory se bezpečnostní rizika stávají stále více propojenými s reálným světem a ovlivňují i oblasti, které byly dříve považovány za méně náchylné k digitálním hrozbám. Zajištění bezpečnosti v systémech potravinářského průmyslu tak nemá pouze technologický rozměr, ale přímo ovlivňuje potravinovou soběstačnost a ekonomickou stabilitu (1).

Tento posun ve vnímaní reflektuje i aktuální legislativní vývoj v České republice, kde došlo k nedávnému přijetí nového zákona o kybernetické bezpečnosti, který lze nyní najít pod oficiálním názvem jako zákon č. 264/2025 Sb., o kybernetické bezpečnosti. Nejde o první právní úpravu této oblasti (účinná legislativa existuje již od roku 2015), ale o zákon reagující na požadavky unijní směrnice NIS 2 a související změny národní úpravy k posílení ochrany informační infrastruktury ČR. Nový zákon však přináší zásadní rozšíření okruhu regulovaných odvětví i služeb nově dopadající i na cukrovary.

Zařazení cukrovarnického průmyslu do nové regulace kybernetické bezpečnosti ilustruje širší trend rostoucí digitalizace a automatizace v průmyslových odvětvích. Podle studie *Cost and Quality Control: Digitalisation in Sugar Sector is the Need of the Hour* je digitalizace v cukrovarnictví nezbytná pro efektivní řízení nákladů a kvality produkce, což je klíčové nejen pro udržitelnost podniků, ale i pro ochranu před kybernetickými hrozbami (3). Se zvyšující se závislostí na informačních a komunikačních technologiích roste i potřeba systematického řízení kybernetických rizik. Regulace, jako je směrnice NIS 2 a tedy i nový zákon o kybernetické bezpečnosti, představují klíčový mechanismus pro zajištění odolnosti kritických a významných podniků vůči kybernetickým hrozbám. Cukrovary, jejichž provoz je ve značné míře založen na automatizovaných řídicích systémech, se tímto stávají součástí širšího bezpečnostního ekosystému, kde je státem definovaná minimální úroveň kybernetické ochrany nezbytnou podmínkou pro stabilitu a kontinuitu výroby.

Teoretický rámec kybernetické bezpečnosti v průmyslu

Kybernetická bezpečnost si vyžaduje komplexní přístup, který zahrnuje technologické a organizační aspekty i legislativní opatření zaměřená na ochranu kritické infrastruktury (4). Tento holistický model je nezbytné vnímat v kontextu kritické kaskády, která ukazuje, jak i malá zranitelnost v jednom segmentu systému může vyvolat řetězovou reakci, jež ohrozí stabilitu celého provozu (5). Ochrana průmyslových systémů tedy nevyžaduje pouze prevenci proti vnějším hrozbám, ale i rozvoj schopnosti rychle a efektivně reagovat na interní rizika, jako jsou selhání lidského faktoru nebo nedostatečná údržba a aktualizace zařízení. Tento přístup reflektuje komplexní povahu kybernetické triády, která je postavena na pilířích dostupnosti, integrity a důvěrnosti (6).

Kritická infrastruktura, včetně cukrovarů, zahrnuje systémy, jejichž poškození nebo ztráta funkčnosti by měla zásadní dopad na národní ekonomiku, bezpečnost nebo veřejné zdraví (6). V případě cukrovarů, které jsou závislé na vysoce automatizovaných výrobních systémech, mohou kybernetické útoky nejen narušit výrobu prostřednictvím manipulace s výrobními procesy, což má přímý dopad na kvalitu produkce a kontinuitu provozu, ale mohou ohrozit i širší dodavatelské řetězce. S rostoucí mírou digitalizace se tato problematika stává ještě urgentnější, neboť rizika spojená s kybernetickými hrozbami rostou úměrně s mírou propojení a závislosti systémů.

Jako příklad reálných hrozeb pro tento sektor lze uvést incident z roku 2017, kdy Amalgamated Sugar Company, druhý největší výrobce cukru z cukrové řepy v USA, čelil spear-phishing útoku. Útočník napodobil e-mail generálního ředitele a získal daňové formuláře za rok 2016, což mělo dopad na 2 858 zaměstnanců společnosti. Tento incident vyzdvihl rizika spojená s digitalizací citlivých informací (7). V širším kontextu potravinářského průmyslu byly v posledních dvou letech zaznamenány útoky na globální společnosti, jako jsou Campbell Soup, Dole Foods, Heineken nebo Krispy Kreme (8).

Klíčovým konceptem pro zajištění kybernetické bezpečnosti v těchto odvětvích je ochrana kritické informační infrastruktury, která zahrnuje nejen informační technologie (IT), ale i operační technologie (OT), nezbytné pro řízení fyzických procesů v průmyslových odvětvích. V tomto kontextu je nutné zmínit normy a rámce zaměřující se na bezpečnost v těchto oblastech. Mezi nejvýznamnější rámce patří norma IEC 62443 (9), která se zaměřuje na kybernetickou bezpečnost v automatizačních a řídicích systémech. Tato norma pokrývá všechny klíčové aspekty kybernetické bezpečnosti, včetně návrhu, implementace a údržby automatizovaných systémů, a stanovuje požadavky na ochranu před zneužitím, řízení přístupu, monitorování a obnovu po kybernetickém incidentu. Dalšími klíčovými normami pro průmyslové sektory jsou ISO/IEC 27001 (10), která poskytuje rámec pro správu bezpečnosti informací, implementaci kontrolních opatření a hodnocení rizik, a NIST SP 800-82 (11), která

specifikuje bezpečnostní pokyny pro průmyslové kontrolní systémy, včetně dispečerského řízení, sběru dat a programovatelných automatů.

Pro zajištění kybernetické bezpečnosti v těchto prostředích je nezbytné implementovat adekvátní bezpečnostní opatření, mezi něž patří například segmentace sítí mezi IT a OT infrastrukturou, pravidelná aktualizace a patchování systémů, šifrování dat a silné autentifikační a přístupové řízení. Kromě toho je nezbytné klást důraz na testování bezpečnosti těchto systémů pomocí simulací kybernetických útoků a pravidelné školení zaměstnanců. Tato opatření nejenže minimalizují riziko lidské chyby, ale také zajišťují stabilitu organizačních procesů a efektivní rozhodování v krizových situacích.

Tento multidimenzionální přístup ke kybernetické bezpečnosti je nezbytný pro ochranu průmyslových systémů před rychle se vyvíjejícími kybernetickými hrozbami a pro zajištění dlouhodobé odolnosti kritické infrastruktury. V kontextu tohoto přístupu se objevuje i významný legislativní krok, který má zásadní dopad na potravinářský průmysl. S přijetím nového zákona o kybernetické bezpečnosti totiž přicházejí nové povinnosti, které ovlivní nejen technologickou stránku, ale i organizační a procedurální rámec kybernetické bezpečnosti v tomto odvětví.

Dopady nového zákona o kybernetické bezpečnosti na cukrovarnické společnosti

Zákon o kybernetické bezpečnosti zavádí nové regulatorní povinnosti pro subjekty napříč různými odvětvími, včetně potravinářského průmyslu. Cukrovarnické společnosti, jako strategičtí aktéři v tomto sektoru, mohou být zařazeny mezi regulované subjekty jako poskytovatelé regulovaných služeb, pokud splní stanovené podmínky pro registraci (2). Mezi klíčové parametry posuzování patří působnost v regulovaném sektoru (nově 22 odvětví), poskytování regulované služby (nejde pouze o působení v regulovaném sektoru) a v neposlední řadě významnost této služby. Odpovědnost za analýzu těchto kritérií leží primárně na samotném subjektu. O registraci subjektu jako poskytovatele regulované služby rozhoduje (na základě podnětu z výše uvedené samostatně identifikační analýzy) Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB; Úřad) (12).

Přímý dopad na rozsah povinností regulovaných subjektů bude po úspěšné registraci dále záviset na režimu. Dle významnosti subjektu se jedná o dva režimy – vyšší a nižší. Oba režimy, byť v odlišné míře, ukládají povinnost implementace adekvátních bezpečnostních opatření, kontinuálního monitorování kybernetických incidentů a udržování efektivní komunikační linky s příslušnými regulačními orgány. Tyto povinnosti jsou dále konkretizovány prostřednictvím závazných lhůt a metodických postupů (13).

Ohlášení regulované služby (§ 6)

Každý subjekt, který poskytuje regulovanou službu, je povinen tuto skutečnost nahlásit NÚKIB do 60 dnů od splnění podmínek pro registraci. Ohlášení probíhá prostřednictvím Portálu NÚKIB, na jehož základě Úřad vydá rozhodnutí o registraci.

Hlášení kontaktních a dalších údajů (§ 11)

Po obdržení rozhodnutí o registraci musí subjekt do 30 dnů prostřednictvím Portálu NÚKIB poskytnout aktuální kontaktní a další relevantní informace nezbytné pro efektivní komunikaci. Tyto údaje musí být v případě změn aktualizovány.

Stanovení rozsahu řízení kybernetické bezpečnosti (§ 12)

Organizace je povinna identifikovat primární a podpůrná aktiva spojená s poskytováním regulované služby a na základě této analýzy určit rozsah aplikace bezpečnostních opatření. Pokud subjekt tento rozsah nestanoví, předpokládá se, že rozsahem aplikace bezpečnostních opatření je celá organizace a všechna její aktiva.

Zavádění bezpečnostních opatření (§ 13–14)

V návaznosti na přidělený režim povinností (vyšší/nižší) musí organizace implementovat příslušná bezpečnostní opatření, jejichž konkrétní požadavky jsou stanoveny v prováděcích vyhláškách. Zahájení implementace je povinné do jednoho roku od doručení rozhodnutí o registraci, přičemž jednotlivá opatření lze zavádět postupně.

Hlášení kybernetických bezpečnostních incidentů (§ 15–16)

Organizace musí v souladu se stanovenými postupy reportovat kybernetické bezpečnostní incidenty odpovědným orgánům prostřednictvím Portálu NÚKIB. V případě režimu vyšších povinností se jedná o reportování Vládnímu CERT u režimu nižších povinností Národnímu CERT (CSIRT.CZ).

V případě závažných bezpečnostních incidentů a hrozeb mohou být regulované subjekty povinny informovat své zákazníky. NÚKIB si vyhrazuje pravomoc rozhodnout o povinnosti takové informování provést v závislosti na závažnosti incidentu.

Provádění protiopatření vydaných NÚKIB (§ 20–23)

Protiopatřeními jsou úkony Úřadu, kterými reaguje na aktuální hrozby a zranitelnosti v kybernetickém prostoru. Cílem je jim předcházet a využít zkušenosti z minulých incidentů pro prevenci budoucích problémů. Regulované subjekty jsou povinny na tato protiopatření adekvátně reagovat.

Povinnosti v oblasti bezpečnosti dodavatelských řetězců (§ 24–32)

Poskytovatelé strategicky významné služby (úzká množina poskytovatelů regulovaných služeb spadající do vyššího režimu v odvětvích veřejná správa, energetika, doprava a digitální infrastruktura a služby) musí zajistit bezpečnost dodavatelského řetězce prostřednictvím prověřování bezpečnostně relevantních dodávek. Tato povinnost se uplatní v případech, kdy regulovaná služba získá strategický význam.

Zajištění dostupnosti strategicky významné služby z ČR (§ 33)

Poskytovatelé strategicky významných služeb musí garantovat dostupnost těchto služeb v nezbytném rozsahu a kvalitě na území ČR.

Závěr

Implementace nových požadavků kybernetické bezpečnosti podle zákona představuje pro cukrovary nejen právní povinnost, ale také příležitost k posílení jejich kybernetické odolnosti. Zařazení cukrovarů mezi provozovatele regulované služby v daném režimu povinností bude mít zásadní dopad na

rozsah a přísnost aplikovaných bezpečnostních opatření, kterému budou podléhat.

Pro komplexní porozumění dopadům legislativy je nezbytné posoudit veškeré související normy a vyhlášky, které detailně upravují jednotlivé regulatorní požadavky. Tento článek představuje základní přehled změn, které cukrovarnický průmysl čekají v oblasti kybernetické bezpečnosti.

Díky přechodným obdobím, která legislativa poskytuje, mají regulované subjekty dostatečný čas na adaptaci. Klíčovou roli v podpoře regulovaných subjektů sehrává Portál NÚKIB, který již nyní poskytuje metodické materiály, nástroje pro vyhodnocení regulatorního statusu a doporučení ohledně souladu s legislativními požadavky.

Souhrn

Příspěvek se zaměřuje na dopady implementace unijní kybernetické legislativy do českého právního rámce, konkrétně na zařazení cukrovarnického průmyslu mezi nově regulované subjekty. Analyzuje specifická kybernetická rizika v tomto strategicky klíčovém odvětví a hodnotí nové regulatorní požadavky, včetně vyhodnocení regulačního statusu, povinností v oblasti řízení rizik a zavádění bezpečnostních opatření. Cílem tohoto příspěvku je zvyšování povědomí o kybernetických výzvách v cukrovarnictví a podpora implementace odpovídajících bezpečnostních opatření k zajištění ochrany kritické infrastruktury v souladu s novými regulacemi.

Klíčová slova: kybernetická bezpečnost, cukrovarnický průmysl, kritická infrastruktura, regulace, zákon o kybernetické bezpečnosti.

Literatura

1. Bernátek, J.: Kybernetická bezpečnost řepařského a cukrovarnického sektoru. *Listy cukrov. řepař.*, 11, 2019 (11), s. 375–376.
2. *Sněmovní tisk 759: Vládní návrh zákona o kybernetické bezpečnosti – historie tisku*. Poslanecká sněmovna Parlamentu ČR [online] https://www.psp.cz/sqw/historie.sqw?o=9&t=759, cit. 28. 3. 2025.
3. Medhe, P. G.: *Cost and quality control: Digitalisation in sugar sector is the need of the hour*. Chinimandi, 2024, [online]. https://www.chinimandi.com/cost-and-quality-control-digitalisation-is-the-need-of-the-hour-in-sugar-sector/, cit. 28. 3. 2025.
4. Hossain, M. S.; Liu, L.: Cybersecurity for Critical Infrastructure Protection. *Int. J. Cybersecurity*, 14, 2021 (4), s. 99–112.
5. Bodeau, D. J. et al.: Critical Cascades: An Integrated Model for Cybersecurity. *Cybersecurity Journal*, 12, 2020 (2), s. 55–72.
6. Von Solms, R.; Van Niekerk, J.: From information security to cyber security. *Computers & Security*, 38, 2013, s. 97–102.
7. Bertel, S.: *Amalgamated Sugar suffers cyber security breach; 2,858 workers' personal info stolen*. Idaho News 6, 2017, [online] https://www.kivitv.com/news/amalgamated-sugar-suffers-cyber-security-breach-workers-personal-info-stolen-in-phishing-attack, 28. 3. 2025.
8. Eastlake, D.: *Hackers targeting weak food and beverage industry*. Foodnavigator, 2025, [online] https://www.foodnavigator.com/Article/2025/03/24/cyber-attack-threat-not-taken-seriously-by-food-and-beverage/, cit. 28. 3. 2025.
9. IEC 62443: Industrial communication networks – Network and system security – Part 1-1: Terminology, concepts, and models. International Electrotechnical Commission, 2009.
10. ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements.
11. NIST SP 800-82: Guide to Industrial Control Systems (ICS) Security. National Institute of Standards and Technology, 2011.
12. *Koho se týká nový zákon o kybernetické bezpečnosti*. Portál NÚKIB, [online]. Dostupné https://portal.nukib.gov.cz/informacni-servis/podpurne-materialy/67b316bdc3c48e2492025682, cit. 28. 3. 2025.
13. *Povinnosti dle nového zákona o kybernetické bezpečnosti*. Portál NÚKIB, [online] https://portal.nukib.gov.cz/informacni-servis/podpurne-materialy/67877cf2e8e3c7573907a549, cit. 28. 3. 2025.

Kolek Netolická V.: Cybersecurity in Czech Sugar Industry: Challenges and Opportunities in Context of New Law

The paper focuses on the impact of implementing EU cybersecurity legislation into the Czech legal framework, specifically regarding the inclusion of the sugar industry among the newly regulated entities. It analyzes the specific cybersecurity risks within this strategically critical sector and evaluates the new regulatory requirements, including the assessment of regulatory status, risk management obligations, and the implementation of security measures. The paper aims to raise awareness of cybersecurity challenges in the sugar industry and to support the implementation of appropriate security measures to ensure the protection of critical infrastructure in line with new regulations.

Key words: cyber security, sugar industry, critical infrastructure, regulation, cyber security act.

Kontaktní adresa – Contact adress:

Mgr. Veronika Kolek Netolická, MPP, Masarykova univerzita v Brně, Fakulta sociálních studií, Joštova 10, 602 00 Brno, Česká republika, e-mail: 414896@mail.muni.cz