MASARYKOVA
UNIVERZITA

PRÁVNICKÁ FAKULTA

Kybernetická bezpečnost kritické infrastruktury

Diplomová práce

PETRA VARGOVÁ

Vedoucí práce: JUDr. Mgr. Jakub Harašta, Ph.D.

Ústav práva a technologií
Program Právo a právní věda

Brno 2024

MUNI
LAW

Bibliografický záznam

Autor: Petra Vargová
Právnická fakulta
Masarykova univerzita
Ústav práva a technologií

Název práce: Kybernetická bezpečnost kritické infrastruktury

Studijní program: Právo a právní věda

Vedoucí práce: JUDr. Mgr. Jakub Harašta, Ph.D.

Rok: 2024

Počet stran: 142

Klíčová slova: Kyberbezpečnost, Kritická infrastruktura, Směrnice NIS 2, Nařízení CRA, Směrnice CER, Cybersecurity Act, Cyber Solidarity Act, Směrnice NIS

Bibliographic record

Author: Petra Vargová
Faculty of Law
Masaryk University
Institute of Law and Technology

Title of Thesis: Cybersecurity of Critical Infrastructure

Degree Programme: Law and Legal Science

Supervisor: JUDr. Mgr. Jakub Harašta, Ph.D.

Year: 2024

Number of Pages: 142

Keywords: Cyber security, Critical infrastructure, NIS 2 Directive, CRA, CER Directive, Cybersecurity Act, Cyber Solidarity Act, NIS Directive

Anotace

Tato diplomová práce se zaměřuje na roli právních nástrojů v oblasti kybernetické bezpečnosti kritické infrastruktury v kontextu rostoucí digitální závislosti a komplexnosti kybernetických hrozeb. Analyzuje implementaci směrnice NIS 2, směrnice o odolnosti kritických subjektů, a nařízení o kybernetické odolnosti v České republice a EU. Součástí práce jsou případové studie kybernetických útoků a jejich dopady na kritickou infrastrukturu. Závěrem jsou navržena doporučení pro zlepšení právního rámce, zvýšení odolnosti kritických systémů vůči kybernetickým hrozbám a zlepšení koordinace mezi státními a soukromými subjekty.

Popis využití AI

Prohlašuji, že při tvorbě této diplomové práce nebyla využita žádná forma umělé inteligence (AI).

Abstract

This thesis focuses on the role of legal instruments in the area of critical infrastructure cybersecurity in the context of growing digital dependence and the complexity of cyber threats. It analyses the implementation of the NIS 2 Directive, the Critical Entities Resilience Directive, and the Cyber Resilience Act in the Czech Republic and the EU. The thesis includes case studies of cyber attacks and their impact on critical infrastructure. Lastly, recommendations for improving the legal framework, increasing the resilience of critical systems to cyber threats and improving coordination between public and private actors are proposed.

Description of how AI was used

I declare that no form of artificial intelligence (AI) was used in the creation of this thesis.

Čestné prohlášení

Prohlašuji, že jsem diplomovou práci na téma **Kybernetická bezpečnost kritické infrastruktury** zpracovala sama. Veškeré prameny a zdroje informací, které jsem použila k sepsání této práce, byly citovány v poznámkách pod čarou a jsou uvedeny v seznamu použitých pramenů a literatury. Popsán je též způsob a rozsah využití nástrojů umělé inteligence.

V Brně 30. června 2024 .....

Petra Vargová

Poděkování

Chtěla bych vyjádřit své upřímné díky vedoucímu této diplomové práce, JUDr. Mgr. Jakubu Haraštovi, Ph.D., za jeho cenné rady, odborné vedení a trpělivost během psaní práce. Jeho expertní znalosti a podnětné připomínky výrazně přispěly ke zlepšení kvality této práce.
Dále děkuji Mgr. Jakubu Vostoupalovi za jeho roli konzultanta, který mi poskytl užitečné zpětné vazby a pomoc při zdolávání obtížných technických výzev spojených s touto prací. Jeho podpora byla neocenitelná při dosahování stanovených cílů.

Obsah

Obsah 10

Seznam pojmů a zkratek 12

1 Úvod 14

2 Základní pojmy a kritická infrastruktura 18

2.1 Kyberbezpečnost ... 18
2.2 Kybernetický bezpečnostní incident ... 19
2.3 Kritická infrastruktura ... 20
2.4 Evropská kritická infrastruktura ... 26
2.5 Pojmy KI a EKI na praktickém příkladu ... 27
2.6 Proces určení prvků KI a EKI a určení subjektů KI ... 29
2.7 Dílčí závěr ... 33

3 Vývoj kyberbezpečnosti kritické infrastruktury 35

3.1 Dílčí závěr ... 45

4 Právní předpisy v oblasti kyberbezpečnosti kritické infrastruktury 47

4.1 Cybersecurity Act ... 47
4.2 Critical Entities Resilience ... 52
4.3 Cyber Resilience Act ... 57
4.4 Směrnice NIS 2 ... 62
4.5 Směrnice CER a směrnice NIS 2 na praktickém případě ... 67
4.6 Cyber Solidarity Act ... 70
4.7 Dílčí závěr ... 72

5 Případová studie 76

5.1 Vícepřípadová studie ... 77
5.2 Závěr případové studie ... 110

6 Závěr **118**

Použité zdroje **121**

Seznam pojmů a zkratek

Směrnice NIS	–	Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii
Směrnice NIS 2	–	Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148
Směrnice CER	–	Směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES
Nařízení CRA	–	Návrh Nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020
Cybersecurity Act	–	Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013 („akt o kybernetické bezpečnosti“)
Cyber Solidarity Act	–	Návrh Nařízení Evropského parlamentu a Rady, kterým se stanoví opatření k posílení solidarity a kapacit v Unii pro odhalování kybernetických bezpečnostních hrozeb a incidentů a pro připravenost a reakci na ně
NÚKIB	–	Národní úřad pro kybernetickou a informační bezpečnost

BSI	– Spolkový úřad pro bezpečnost informační techniky
BKA	– Spolkový kriminální úřad
ENISA	– Agentura Evropské unie pro kybernetickou bezpečnost
CERT	– Computer Emergency Response Team
CSIRT	– Computer Security Incident Response Team
NCKB	– Národní centrum kybernetické bezpečnosti
KI	– Kritická infrastruktura
EKI	– Evropská kritická infrastruktura
ICT	– Informační a komunikační technologie
IoT	– Internet věcí
EUCSS	– Strategie kybernetické bezpečnosti EU
DEP	– Zabránění spuštění dat
EU	– Evropská Unie
DRP	– Plánování obnovy po havárii
BCP	– Plán kontinuity podnikání
UKD	– Univerzitní nemocnice v Düsseldorfu
FN Brno	– Fakultní nemocnice Brno
AgID	– Agentura pro digitální Itálii
ACN	– Národní agentura pro kybernetickou bezpečnost

1 Úvod

Tato diplomová práce se zaměřuje na roli právních nástrojů v kontextu zajištění kybernetické bezpečnosti kritické infrastruktury. V dnešní digitální éře, kde digitální technologie pronikly do každodenního života a infrastruktury, je kybernetická bezpečnost nezbytným prvkem pro zachování stability a fungování společnosti. Kritická infrastruktura, jakožto systémy a služby nezbytné pro fungování společnosti a hospodářství, jsou zranitelné vůči kybernetickým hrozbám, které mohou mít katastrofální důsledky. Jako příklad může být uveden kybernetický útok BlackEnergy na Ukrajinu. V roce 2015 se Ukrajina stala terčem významného kybernetického útoku, který způsobil značné výpadky elektrické energie. Tento útok, známý jako BlackEnergy, byl pravděpodobně koordinován hackerskou skupinou Sandworm Team a mohl být reakcí na předchozí útoky pro-ukrajinských separatistů na Krymu, které vedly k výpadkům elektřiny pro dva miliony obyvatel a klíčovou námořní základnu v Sevastopolu. [1] [2] Útočníci začali své přípravy již v březnu 2015, což naznačuje, že čekali na vhodný politický moment, aby mohli Ukrajině vyslat varování o schopnosti vážně poškodit její infrastrukturu, nebo jako demonstraci moci Ruska v oblasti kybernetických schopností. [3]

Útok začal spear-phishingovou kampaní zaměřenou na různé cíle, přičemž v prosinci 2015 zacílil na zaměstnance energetických společností.[4] E-maily obsahovaly přílohy ve formátech Word, Excel nebo PowerPoint s makry, která nainstalovala malware BlackEnergy 3.[5] Tento malware umožnil útočníkům špehovat zaměstnance a získávat

[1] MITRE. 2015 Ukraine Electric Power Attack [online]. *MITRE ATT&CK*. [cit. 15.06.2024]. https://attack.mitre.org/campaigns/C0028/

[2] Baezner, M., Robin, P. *Cyber and Information warfare in the Ukrainian conflict*. Zürich, 2018, s. 15.

[3] ibidem

[4] Cherepanov, A., Lipovsky, R. BlackEnergy – What We Really Know About the Notorious Cyber Attacks. *Virus Bulletin*. 2016, s. 1-3.

[5] Cherepanov, A., Lipovsky, R. BlackEnergy – What We Really Know About the Notorious Cyber Attacks. *Virus Bulletin*. 2016, s. 3.

informace.[6] Útočníci poté použili software Radmin k získání přístupu do řídicích center energetických společností a provedli synchronizovaný pětinásobný útok: otevření všech přepínačů napájení, narušení záložního napájení, deaktivaci ethernetových převodníků, telefonní denial-of-service (TDoS) útok a použití programu KillDisk k mazání důležitých souborů.[7] [8] Tento koordinovaný útok způsobil výpadky napájení v různých oblastech po dobu jedné až šesti hodin, což naznačuje, že cílem nebylo způsobit trvalé škody, ale spíše demonstrovat schopnosti útočníků.[9]

Zabezpečení kritických infrastruktur se tak stává jedním z nejdůležitějších úkolů pro vlády po celém světě. Evropská unie se v posledních letech intenzivně zabývá otázkou kybernetické bezpečnosti a ochrany kritické infrastruktury. Úsilí o posílení kybernetické bezpečnosti je reflektováno v různých legislativních opatřeních a strategiích, které mají za cíl zvýšit odolnost a ochranu kritických systémů před kybernetickými hrozbami.

Volba daného tématu pro diplomovou práci byla motivována několika klíčovými faktory. Prvním důvodem byla pozorovatelná tendence společností k rostoucí závislosti na digitální infrastruktuře.[10] Za druhé, s tímto nárůstem závislosti roste i riziko a komplexnost kybernetických útoků, které mohou mít zničující dopady na ekonomickou stabilitu a bezpečnost společnosti. Třetím důležitým faktorem je skutečnost, že v posledních letech přibývá čím dál tím více právních předpisů v oblasti kybernetické bezpečnosti kritické infrastruktury, což způsobuje

[6] Kaspersky, BlackEnergy APT Attacks in Ukraine [online]. *kaspersky.com.* [cit. 15.06.2024]. https://www.kaspersky.com/resource-center/threats/blackenergy

[7] CISA. Cyber-Attack Against Ukrainian Critical Infrastructure [online]. *cisa.gov.* [cit. 15.06.2024]. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

[8] Cherepanov, A., Lipovsky, R. BlackEnergy – What We Really Know About the Notorious Cyber Attacks. *Virus Bulletin*. 2016, s. 5–6.

[9] Pollard, M. A Case Study of Russian Cyber-Attacks on the Ukrainian Power Grid: Implications and Best Practices for the United States. *Pepperdine Policy Review*. 2024, Vol. 16, článek 1, s. 12.

[10] Vzestup závislosti společnosti na digitální infrastruktuře (včetně technologií jako Internet věcí (IoT), 5G sítě, umělá inteligence, cloud computing, a blockchain) je zřejmý díky jejich rychlému rozvoji, který umožňuje propojení a optimalizaci všeho od domácích spotřebičů po průmyslové výrobní linky, čímž se zvyšuje efektivita, ale také rizika spojená s kybernetickou bezpečností.

nepřehlednost v právní úpravě kyberbezpečnosti. Tyto faktory dohromady představují zásadní impulz k hlubšímu zkoumání této problematiky nejenom v akademickém prostředí, ale i v praxi, s cílem identifikovat klíčové výzvy a navrhnout účinná opatření pro ochranu kritické infrastruktury a prevenci kybernetických hrozeb.

V obecné části jsou nejprve definovány základní pojmy a kritická infrastruktura, včetně rozdílů mezi kritickou infrastrukturou a evropskou kritickou infrastrukturou. Tyto pojmy budou sloužit jako základní rámec pro pochopení problematiky, kterou se bude práce dále zabývat.

V následující kapitole bude zmapován a rozebrán vývoj právních předpisů dopadajících na kyberbezpečnost v kritické infrastruktuře. Tato kapitola sleduje vývoj právních předpisů týkajících se kybernetické bezpečnosti kritické infrastruktury od počátků digitální éry po současnost. Analyzuje klíčové momenty, jako je přijetí směrnice o evropské kritické infrastruktuře v roce 2008, směrnice NIS v roce 2016 či směrnice o odolnosti kritických subjektů z roku 2022. Kapitola poskytuje kontext pro pochopení současného stavu ochrany kybernetické bezpečnosti kritické infrastruktury.

Třetí kapitola se bude věnovat analýze současných právních požadavků, které jsou zaměřeny na zajištění kybernetické bezpečnosti kritické infrastruktury. Zvláštní pozornost je věnována účinným právním předpisům, jako jsou směrnice 2022/2555 a nařízení 881/2019, a také připravované legislativě, zejména návrhu Aktu o kybernetické odolnosti. Tato analýza má za cíl poskytnout komplexní pohled na současný stav právního rámce a identifikovat případné mezery a nedostatky.

Zvláštní část práce se bude zaměřovat na analýzu kybernetických útoků prostřednictvím vícepřípadové explanatorní studie. Jejím cílem je poskytnout komplexní pohled na to, jak různé organizace a země reagují na kybernetické hrozby, identifikovat zranitelnosti a nabídnout doporučení pro zlepšení kybernetické bezpečnosti. Bude zde analyzováno, jak různé sektory kritické infrastruktury reagují na kybernetické útoky, a jaké strategie a opatření používají k minimalizaci rizik a následků těchto útoků. Kapitola se konkrétně zaměří na reakce organizací, krizové řízení, komunikační strategie a dlouhodobá opatření k prevenci, přičemž bude kladen důraz na specifika České republiky ve srovnání s Itálií a Německem. Analyzovány budou čtyři významné kybernetické útoky na kritickou infrastrukturu: útok na Deutsche Bahn, nemocnici v Düsseldorfu, Enel a Fakultní nemocnici v Brně. Výběr těchto případů umožní

pochopení různých aspektů kybernetické bezpečnosti v dopravě, zdravotnictví a energetice. Kapitola rovněž vyhodnotí vliv evropské legislativy na zvládání kybernetických incidentů, konkrétně směrnice NIS a dalších relevantních nařízení, a jejich dopad na úspěšnost a efektivitu reakcí na kybernetické útoky.

Diplomová práce si tak klade za cíl přispět k lepšímu porozumění právního rámce pro kybernetickou bezpečnost kritické infrastruktury a poskytnout ucelený přehled o současném stavu a dosavadním vývoji právního rámce v této oblasti. Kromě toho je jejím záměrem identifikovat klíčové oblasti, které vyžadují další pozornost a zdokonalení. Analyzování současných právních nástrojů a jejich aplikace v praxi nám pomůže lépe porozumět výzvám v oblasti kybernetické bezpečnosti a navrhnout účinnější opatření pro ochranu kritických systémů v Evropské unii.

2 Základní pojmy a kritická infrastruktura

V dnešní době je kyberbezpečnost považována za rozsáhlé téma, ve kterém je stále obtížnější se orientovat, ať již z právního, technického nebo laického hlediska. S rozvojem technologií je zaváděno stále více nových pojmů, jejichž pochopení je nezbytné pro efektivní ochranu před neustále se vyvíjejícími hrozbami.

Tato část práce je zaměřena na vysvětlení základních pojmů v oblasti kybernetické bezpečnosti kritické infrastruktury. Nejprve je definována samotná kybernetická bezpečnost, následně jsou zkoumány související pojmy, jako je kybernetický bezpečnostní incident. Poté je věnována pozornost konceptu kritické infrastruktury a jsou identifikovány její klíčové charakteristiky. Dále jsou analyzovány rozdíly v pojetí kritické infrastruktury v českém právu a evropském kontextu, což pomáhá lépe porozumět specifikům ochrany a zabezpečení těchto systémů na kontinentální úrovni. Tato kapitola poskytuje základní rámec pro další zkoumání kybernetické bezpečnosti v kontextu kritické infrastruktury, které je dále rozvíjeno v této práci. Vzhledem k dynamice této oblasti existuje mnoho definic jednotlivých pojmů, které se mohou lišit v závislosti na zdroji a kontextu. Proto je důležité přistupovat k výběru definic systematicky a s důrazem na jejich přesnost a srozumitelnost. Definice jsou vybrány s ohledem na jejich relevanci k probíranému tématu, přičemž musí být přesné a odpovídat odborným a legislativním standardům. Současně dbát na to, aby byly formulovány jasně a srozumitelně, což usnadňuje jejich pochopení širokému publiku, včetně těch, kteří nemají odborné právní znalosti. Preferují se definice z oficiálních a důvěryhodných zdrojů, jako jsou právní předpisy a oficiální dokumenty od agentur a úřadů. Upřednostňují se aktuální definice, které odrážejí nejnovější právní a odborné vývoje v dané oblasti. Tento přístup se snaží zajistit, aby vybrané definice byly nejen odborně správné, ale také snadno pochopitelné pro co nejširší okruh uživatelů.

2.1 Kyberbezpečnost

Jedna z možných definic se nachází v dokumentu od agentury ENISA pod názvem Definition of Cybersecurity - Gaps and overlaps in standardisation: *„Kyberbezpečnost se vztahuje na bezpečnost kyberprostoru, kde*

samotný kybernetický prostor odkazuje na soubor vazeb a vztahů mezi objekty, které jsou přístupné prostřednictvím všeobecné telekomunikační sítě, a na samotnou sadu objektů, jejichž rozhraní umožňující jejich dálkové ovládání, vzdálený přístup k datům, anebo jejich zapojení do řídících akcí v rámci kyberprostoru. Kyberbezpečnost bude zahrnovat paradigma ‚CIA' triády pro vztahy a objekty v rámci kyberprostoru a zároveň bude toto paradigma rozšiřováno z důvodu zajištění ochrany soukromí subjektů (fyzických a právnických osob) a odolnosti [‚zotavení se' (recovery) z útoku]." [11] Jedná se tedy o určitá opatření či prostředky k ochraně a zabezpečení kyberprostoru. Kyberbezpečnost se vztahu na všechny, kteří ve svém životě používají informační technologie, tedy každý jednotlivý člověk, který informační technologie využívá je prvkem kyberbezpečnosti. Pro kyberbezpečnost je tedy důležitý každý prvek, jelikož jakýkoliv slabý článek může vést k úspěšnému kybernetickému útoku ze strany hackerů. Ovšem kyberbezpečnost chrání nejen před útoky, ale i před širokým spektrem dalších hrozeb, např. přírodní katastrofy či změny technologického prostředí.

2.2 Kybernetický bezpečnostní incident

Důležitým pojmem, se kterým se setkáme v rámci daného tématu je kybernetický bezpečnostní incident, jehož možnou definici nalezneme v zákoně č. 181/2014 Sb. (zákon o kybernetické bezpečnosti): *„narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.*" [12] V souvislosti s navrhovanými změnami v legislativě v oblasti kybernetické bezpečnosti (návrh nového zákona o kybernetické bezpečnosti) byla tato definice upravena tak, že nyní hovoří o *„narušení bezpečnosti informací v rámci aktiv"*.[13] Může vzniknout otázka týkající se rozdílu mezi kybernetickým útokem a kybernetickým bezpečnostním incidentem. Hlavní rozdíl spočívá v tom, že kybernetický bezpečnostní incident zahrnuje širší škálu

[11] Brookson, Ch., et al. *Definition of Cybersecurity - Gaps and overlaps in standardisation*. ENISA, 2015, s. 30.

[12] § 7 odst. 2 zákona č. 181/2014 Sb., zákon o kybernetické bezpečnosti, ve znění pozdějších předpisů.

[13] § 2 odst. 2 písm. f) návrhu zákona o kybernetické bezpečnosti.

událostí než pouze kybernetický útok (úmyslné napadení systému). Může se jednat jak o kybernetické útoky, tak i jiné události, jako jsou chyby v systémech, technické závady, neoprávněný přístup k datům či přirozené katastrofy.

Rozdíl mezi kybernetickým bezpečnostním incidentem a událostí spočívá v tom, že kybernetická bezpečnostní událost je pouze potenciální možnost narušení bezpečnosti informací, služeb či integrity sítí elektronických komunikací.[14] Na rozdíl od toho, kybernetický bezpečnostní incident představuje skutečné a reálné narušení těchto bezpečnostních prvků.

2.3 Kritická infrastruktura

Kritická infrastruktura je klíčovým faktor pro stabilitu a bezpečnost celé společnosti.[15] Kritická infrastruktura zahrnuje širokou škálu systémů a zařízení, které jsou nezbytné pro chod státu a ekonomiky, včetně energetických sítí, dopravních systémů, telekomunikací, zdravotnictví a dalších. Zabezpečení této infrastruktury se stává prioritou pro vlády a organizace, protože jakékoli selhání nebo útok na ni by mohlo mít katastrofální důsledky. Například výpadek energetického systému by mohl vést k masivním hospodářským škodám, přerušení komunikací a ohrožení životů občanů. Proto je nezbytné vyvinout a implementovat komplexní bezpečnostní opatření. Mezi taková opatření patří plány krizového řízení, které umožňují rychlou a efektivní reakci v případě mimořádných událostí, monitorování kritických systémů pro detekci potenciálních hrozeb a zranitelností a také zabezpečení používání citlivých systémů a dat. Spolupráce a inovativní přístupy jsou klíčové pro úspěšné zabezpečení kritické infrastruktury. To zahrnuje spolupráci mezi vládními a soukromými subjekty, výzkumnými institucemi a odborníky na bezpečnost, stejně jako investice do nových technologií a postupů, které mohou pomoci minimalizovat rizika a zlepšit reakci na možné hrozby.

[14] § 7 odst. 1 zákona č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů.

[15] Kritická infrastruktura v ČR: Přehled klíčových odvětví a jejich význam pro stát [online]. *arpki.cz.* [cit. 16.04.2024]. https://www.arpki.cz/kriticka-infrastruktura/kriticka-infrastruktura/

Celkově lze říci, že pro bezpečnost kritické infrastruktury je nutné pečlivé plánování a investice do bezpečnostních opatření, aby byla zajištěna stabilita a bezpečnost společnosti v době nejistoty a rizik.

K přiblížení a porozumění konceptu kritické infrastruktury je využit základní právní předpis týkající se kritické infrastruktury v České republice, konkrétně zákon č. 240/2000 Sb. o krizovém řízení (krizový zákon). V § 2 daného zákona je kritická infrastruktura upravena v písmenu g), jako *„prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu“.* [16] Dle definice kritické infrastruktury platné ke květnu 2024 je tedy kladen důraz na prvek kritické infrastruktury. Příkladem můžou být elektrárny a síť pro přenos a distribuci elektřiny, jež jsou zásadními komponentami kritické infrastruktury. Poruchy v těchto systémech by měly závažné dopady na dodávky elektřiny, což by ovlivnilo veřejné služby, průmysl a domácnosti. To bylo možné vidět např. při kybernetickém útoku BlackEnery na Ukrajinu. Ale může se jednat i o dopravní infrastrukturu, včetně silnic, železnic, letišť a přístavů. Její poškození by mohlo způsobit přerušení přepravních a logistických toků, což by ovlivnilo dodávky zboží, mobilitu obyvatelstva a ekonomiku.

Prvky jsou identifikovány v souladu s nařízením vlády č. 432/2010 Sb., které je rozděluje na průřezové prvky (s ohledem na oběti, dopad na ekonomiku a veřejnost) a odvětvové prvky (v rámci 9 odvětví). Generální ředitelství Hasičského záchranného sboru ČR má povinnost vést seznam prvků KI. Aby byl prvek zapsán na seznam, tak musí splňovat určitá kritéria, která jsou přesněji upravena v nařízení vlády č. 432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury.

Klasifikace podle prvků kritické infrastruktury vykazuje jak výhody, tak nevýhody, jež budou nyní diskutovány. Mezi výhody patří například umožnění specializované ochrany, neboť každý prvek může vyžadovat specifický přístup k zabezpečení, a tedy jejich identifikace a kategorizace umožňuje individualizovaný přístup a poskytnutí specializované ochrany. Dále také identifikace jednotlivých prvků kritické infrastruktury umožňuje efektivní cílení investic do modernizace a zajištění, což zvyšuje celkovou odolnost a bezpečnost. Navíc, definice kritické

[16] Zákon č. 240/2000 Sb. o krizovém řízení, ve znění pozdějších předpisů.

infrastruktury podle prvků může podporovat lepší spolupráci mezi různými sektory a subjekty, což přispívá k efektivnější ochraně a správě.

Na druhou stranu, mezi nevýhody patří riziko přehlédnutí nebo nedostatečného zabezpečení některých klíčových prvků kvůli složitosti detailní identifikace kritické infrastruktury podle jednotlivých prvků.[17] Další nevýhodou jsou administrativní nároky, neboť správa a aktualizace rozsáhlého seznamu kritické infrastruktury podle jednotlivých prvků vyžaduje čas a zdroje.[18] Nejvýznamnějším problémem tohoto přístupu k definici kritické infrastruktury je nedostatečná flexibilita, jelikož pevné definice jednotlivých prvků mohou být nepružné a nedokáží adekvátně reagovat na rychle se měnící technologické a společenské trendy.[19]

Ovšem v souvislosti se směrnicí o odolnosti kritických subjektů (směrnice CER) se v České republice připravuje nový právní rámec. Tento návrh zákona reaguje na požadavky uvedené ve směrnici a zahrnuje samostatný zákon o odolnosti subjektů kritické infrastruktury (návrh zákona o kritické infrastruktuře), který je záměrně oddělen od stávajícího krizového zákona. Současně je plánována revize krizového zákona s cílem identifikovat nedostatky v reakci na současné i budoucí moderní a nepředvídatelné hrozby a události, včetně postkrizového období. Nový právní předpis čerpá ze zkušeností s předchozími krizovými situacemi, jako jsou pandemie COVID-19 a ruská válka proti Ukrajině, a usiluje o lepší připravenost státu na podobné události v budoucnosti.[20]

Návrh zákona o kritické infrastruktuře se primárně zaměřuje na zajištění odolnosti základních služeb a poskytovatelů kritické infrastruktury, s důrazem na reakci na kybernetické útoky a přerušení dodávek surovin. Zavádí nový přístup k identifikaci subjektů kritické infrastruktury a zdůrazňuje význam poskytování základních služeb pro stabilitu společnosti. Kromě toho navrhuje opatření pro zvýšení odolnosti a sdílení informací mezi subjekty kritické infrastruktury a navazuje na nový právní

[17] Důvodová zpráva k návrhu zákonu o kritické infrastruktuře [online]. *odok.cz.* [cit. 20.05.2024]. https://odok.cz/portal/veklep/material/ALBSD2AH4CXO/

[18] Důvodová zpráva k návrhu zákonu o kritické infrastruktuře [online]. *odok.cz.* [cit. 20.05.2024]. https://odok.cz/portal/veklep/material/ALBSD2AH4CXO/

[19] ibidem

[20] Důvodová zpráva k návrhu zákonu o kritické infrastruktuře [online]. *odok.cz.* [cit. 20.05.2024]. https://odok.cz/portal/veklep/material/ALBSD2AH4CXO/

rámec v oblasti kybernetické bezpečnosti. K návrhu zákona o kybernetické bezpečnosti blíže v kapitole 4.4.

Nicméně, jsou zde i aspekty, které mohou být předmětem diskusí v rámci procesu přijetí zákona. Podle Michala Moroziho, který je výkonným ředitelem Asociace kritické infrastruktury ČR, může vyvolat kritiku výše navrhovaných pokut, protože některé subjekty kritické infrastruktury mohou vnímat tyto sankce jako příliš přísné nebo neadekvátní, jelikož nejsou v souladu se směrnicí CER a ignoruje individuální kontext.[21] Dále, ustanovení, které umožňuje ministerstvu vnitra získat pravomoc zakazovat subjektům kritické infrastruktury jejich dodavatele, což by mohlo vyvolat obavy z možného zneužití moci a politického tlaku na soukromé subjekty.[22] Jedná se o ustanovení § 14 návrhu zákona o kritické infrastruktuře, které se zabývá bezpečností dodavatelského řetězce, a umožňuje Ministerstvu vnitra ČR rozhodnout o podmínkách, omezeních, nebo zákazu dodávek či poskytování služeb od dodavatelů a poskytovatelů služeb subjektům kritické infrastruktury, pokud tito představují významné ohrožení bezpečnosti České republiky. Směrnice CER pouze stanovuje, prostřednictvím harmonizovaných minimálních pravidel a podpůrných opatření, že členské státy mají povinnost provádět pravidelné hodnocení rizik a identifikovat kritické entity, které poskytují základní služby pro společnost a ekonomiku.[23] Na základě těchto hodnocení pak mají členské státy přijmout opatření ke zvýšení odolnosti těchto entit, což by mohlo zahrnovat i kontrolu a regulaci dodavatelských řetězců. Tento návrh ovšem vzbudil kritiku kvůli obavám z netransparentnosti a potenciální zneužitelnosti, protože postrádá funkční kontrolní

[21] Nonnemann, F. Před mikrofonem: Jak se připravuje nová legislativa o kritické infrastruktuře [online]. *gdpr.cz.* [cit. 27.04.2024]. https://www.gdpr.cz/pred-mikrofonem-jak-se-pripravuje-nova-legislativa-o-kriticke-infrastrukture

[22] ibidem

[23] Čl. 6 a 12 směrnice Evropského parlamentu a rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES.

mechanismy.[24] [25] Kritika je také zaměřena na nedostatečné definování kritérií významnosti. Přičemž kritérium významnosti se týká stanovení důležitosti jednotlivých základních služeb poskytovaných subjekty kritické infrastruktury. Nejasná definice kritéria významnosti může vést k netransparentnosti a nespravedlivým rozhodnutím.[26] Kritici, včetně Asociace kritické infrastruktury ČR a Svazu průmyslu a dopravy ČR, upozorňují, že nejasná definice významnosti může způsobit právní nejistotu a zvýšit administrativní zátěž pro subjekty kritické infrastruktury, které musí splnit nové povinnosti bez jasného rámce.[27] [28] Navrhovaná kritéria významnosti a seznam základních služeb budou stanoveny prováděcím právním předpisem, což znamená, že detaily budou upřesněny až v budoucnu, což přispívá k současné nejistotě a kritice návrhu zákona. Další problém je shledáván v nejasnosti role Generálního ředitelství Hasičského záchranného sboru v kontextu plnění úkolů definovaných

[24] Proksch, J. Stanovisko Svazu průmyslu a dopravy ČR k Návrhu zákona o odolnosti subjektů kritické infrastruktury a o změně dalších zákonů (zákon o kritické infrastruktuře) [online]. *Svaz průmyslu a dopravy České republiky*. [cit. 15.05.2024]. https://www.spcr.cz/images/Stanovisko_SP_%C4%8CR_k_n%C3%A1vrhu_z%C3%A1kona_o_KI_final.pdf

[25] Moroz, M. Stanovisko Asociace kritické infrastruktury ČR k Návrhu zákona o odolnosti subjektů kritické infrastruktury a o změně dalších zákonů [online]. *AKI ČR*. [cit. 15.05.2024]. https://www.akicr.cz/2024/03/01/zakon-o-kriticke-infrastrukture-pripominky-aki-cr-k-navrhu-zakona/

[26] Moroz, M. Stanovisko Asociace kritické infrastruktury ČR k Návrhu zákona o odolnosti subjektů kritické infrastruktury a o změně dalších zákonů [online]. *AKI ČR*. [cit. 15.05.2024]. https://www.akicr.cz/2024/03/01/zakon-o-kriticke-infrastrukture-pripominky-aki-cr-k-navrhu-zakona/

[27] Moroz, M. Stanovisko Asociace kritické infrastruktury ČR k Návrhu zákona o odolnosti subjektů kritické infrastruktury a o změně dalších zákonů [online]. *AKI ČR*. [cit. 15.05.2024]. https://www.akicr.cz/2024/03/01/zakon-o-kriticke-infrastrukture-pripominky-aki-cr-k-navrhu-zakona/

[28] Proksch, J. Stanovisko Svazu průmyslu a dopravy ČR k Návrhu zákona o odolnosti subjektů kritické infrastruktury a o změně dalších zákonů (zákon o kritické infrastruktuře) [online]. *Svaz průmyslu a dopravy České republiky*. [cit. 15.05.2024]. https://www.spcr.cz/images/Stanovisko_SP_%C4%8CR_k_n%C3%A1vrhu_z%C3%A1kona_o_KI_final.pdf

v navrhovaném zákoně o kritické infrastruktuře, což může vést k netransparentnosti, riziku zneužití pravomocí a kompetenčním sporům mezi úřady, přičemž související náklady jsou plně přenášeny na subjekty kritické infrastruktury.[29] [30] Existuje také problém s překrýváním navrhovaného zákona s legislativním návrhem týkajícím se kybernetické bezpečnosti, což zdůrazňuje potřebu koherentního právního rámce a sjednocení terminologie pro efektivní ochranu kritické infrastruktury.[31] Někteří autoři též upozorňují na související změny v krizovém zákoně, kde má dojít k omezení práv na soukromí, vzdělání, vlastnictví či ochranu osobních údajů v případě nouzového stavu či stavu ohrožení státu.[32] Konkrétně, návrh zákona umožňuje vládě omezit práva fyzických a právnických osob na nedotknutelnost obydlí, vlastnická a užívací práva, svobodu pohybu a pobytu, právo na shromažďování a podnikání, a také právo na stávku, pokud by tato stávka narušovala krizová opatření.[33] V praxi by to znamenalo, že vláda by mohla dočasně zabavit nebo omezit užívání majetku fyzických a právnických osob. Například by mohla

[29] Proksch, J. Stanovisko Svazu průmyslu a dopravy ČR k Návrhu zákona o odolnosti subjektů kritické infrastruktury a o změně dalších zákonů (zákon o kritické infrastruktuře) [online]. *Svaz průmyslu a dopravy České republiky*. [cit. 15.05.2024]. https://www.spcr.cz/images/Stanovisko_SP_%C4%8CR_k_n%C3%A1vrhu_z%C3%A1kona_o_KI_final.pdf

[30] Moroz, M. Stanovisko Asociace kritické infrastruktury ČR k Návrhu zákona o odolnosti subjektů kritické infrastruktury a o změně dalších zákonů [online]. *AKI ČR*. [cit. 15.05.2024]. https://www.akicr.cz/2024/03/01/zakon-o-kriticke-infrastrukture-pripominky-aki-cr-k-navrhu-zakona/

[31] Proksch, J. Stanovisko Svazu průmyslu a dopravy ČR k Návrhu zákona o odolnosti subjektů kritické infrastruktury a o změně dalších zákonů (zákon o kritické infrastruktuře) [online]. *Svaz průmyslu a dopravy České republiky*. [cit. 15.05.2024]. https://www.spcr.cz/images/Stanovisko_SP_%C4%8CR_k_n%C3%A1vrhu_z%C3%A1kona_o_KI_final.pdf

[32] ProLibertate. Vnitro chystá zásadní omezení lidských práv [online]. *prolibertate.cz.* [cit. 03.05.2024]. https://www.prolibertate.cz/2024/03/vnitro-chysta-zasadni-omezeni-lidskych-prav/

[33] ProLibertate. Vnitro chystá zásadní omezení lidských práv [online]. *prolibertate.cz.* [cit. 03.05.2024]. https://www.prolibertate.cz/2024/03/vnitro-chysta-zasadni-omezeni-lidskych-prav/

zabavit vozidla nebo jiné vybavení pro účely krizových opatření. Novela by také měla změnit podmínky pro náhradu škody způsobené krizovými opatřeními, již by nebyl nárok na ušlý zisk.[34] Tedy podnikatelé a jednotlivci by mohli zůstat bez kompenzace za ušlý zisk a byli by např. odkázáni na sociální příspěvky.

Klíčovým bodem změny je přechod od pohledu na jednotlivé fyzické prvky infrastruktury k zaměření na subjekty, které poskytují základní služby.[35] Tento přístup lépe reflektuje moderní hrozby a umožňuje efektivnější ochranu a reakci v případě potřeby.

2.4 Evropská kritická infrastruktura

Je důležité nezaměňovat pojmy kritická infrastruktura (národní úroveň) a evropská kritická infrastruktura (unijní úroveň). Podobně jako je tomu u kritické infrastruktury, tak i definice EKI platná ke květnu 2024 je upravena v krizovém zákoně, a to jako *„kritická infrastruktura na území České republiky, jejíž narušení by mělo závažný dopad i na další členský stát Evropské unie"*[36] Směrnice 2008/114/ES, z níž pojem EKI vychází, se zaměřovala výhradně na sektory dopravy a energetiky. Nicméně již v této směrnici bylo naznačeno budoucí rozšíření působnosti na další odvětví, zejména na informační a komunikační technologie. Tato směrnice bude zrušena a nahrazena směrnicí CER k 17.10.2024.

S transpozicí směrnice CER do českého právního řádu dojde ke změně v regulaci EKI. Tento pojem již nebude začleněn do krizového zákona, ale bude zahrnut do zákona o kritické infrastruktuře. Podle návrhu zákona platného ke dni 2.5.2024 bude existovat pouze pojem subjekt evropské kritické infrastruktury, který je definován jako *„subjekt kritické infrastruktury, který poskytuje stejnou nebo podobnou základní službu alespoň v 6 členských státech Evropské unie a byl označen Evropskou komisí*

[34] ProLibertate. Vnitro chystá zásadní omezení lidských práv [online]. *prolibertate.cz.* [cit. 03.05.2024]. https://www.prolibertate.cz/2024/03/vnitro-chysta-zasadni-omezeni-lidskych-prav/

[35] § 2 písm. g) návrhu zákona o kritické infrastruktuře.

[36] § 2 písm. h) zákona č. 240/2000 Sb., krizový zákon, ve znění pozdějších předpisů.

za subjekt zvláštního evropského významu".[37] Název "evropská kritická infrastruktura" byl ve směrnici CER nahrazen pojmem "kritický subjekt zvláštního evropského významu".[38] Kritický subjekt je subjekt náležející do některé z kategorií subjektů uvedených v příloze směrnice CER. Jak bylo již uvedeno, tato změna reflektuje posun pozornosti od samotných prvků kritické infrastruktury směrem k individuálním subjektům poskytujícím základní služby v rámci širšího konceptu odolnosti. Nicméně s uvedením tohoto nového termínu se objevují určité kritické připomínky, které naznačují, že tato změna může vyvolat zmatky v rámci překladů mezi jednotlivými členskými státy EU.[39] Na rozdíl od své předchůdkyně se směrnice CER zabývá kritickými subjekty poskytujícími základní služby v 11 odvětvích.

2.5 Pojmy KI a EKI na praktickém příkladu

V předchozí podkapitole jsme podrobně popsali pojmy kritická infrastruktura a evropská kritická infrastruktura. V této podkapitole se zaměříme na praktický příklad, který ilustruje význam těchto pojmů v reálném světě.

V případě, že dojde k závažné kybernetické útoku na hlavní elektrárenskou společnost v České republice, která je hlavním provozovatelem distribuční soustavy elektřiny pro regiony v České republice. Tento útok způsobí rozsáhlé výpadky elektřiny, které ovlivní nejen domácnosti, ale i kritické služby jako nemocnice, dopravní systémy a zásobování vodou. V tomto případě by elektrárenská společnost byla považována za součást kritické infrastruktury, protože její funkce je zásadní pro národní bezpečnost a ekonomickou stabilitu. Zde může být uvedena například distribuční společnost ČEZ:

---

[37] § 2 písm. d) návrhu zákona o kritické infrastruktuře.

[38] Pursiainen, C., Kytömaa, E. From European critical infrastructure protection to the resilience of European critical entities: what does it mean? *Sustainable and Resilient Infrastructure*. 2023, č. 8, s. 89.

[39] Pursiainen, C., Kytömaa, E. From European critical infrastructure protection to the resilience of European critical entities: what does it mean? *Sustainable and Resilient Infrastructure*. 2023, č. 8, s. 89–90.

- ČEZ Distribuce, a.s. je jedním z hlavních provozovatelů distribuční soustavy v České republice a představuje klíčový prvek kritické infrastruktury v elektroenergetice.
- ČEZ Distribuce zajišťuje provoz, údržbu a rozvoj distribuční sítě, která zahrnuje vysoko- a nízkonapěťové vedení a distribuční trafostanice.[40]
- Společnost dodává elektrickou energii milionům domácností a podniků v ČR.[41]
- Ochrana této infrastruktury je nezbytná pro zajištění kontinuity a bezpečnosti dodávek elektřiny, což má přímý dopad na každodenní život obyvatel a fungování ekonomiky.

Pokud by její činnost ovlivňovala více států a způsobila by přeshraniční výpadky, stává se také součástí evropské kritické infrastruktury (subjekt zvláštního evropského významu). Evropská unie by v takové situaci mohla aktivovat mechanismy na ochranu a obnovu této infrastruktury, včetně sdílení informací, společných opatření na zmírnění dopadů a koordinaci obnovy kritických služeb. Příkladem subjektu zvláštního evropského významu může být propojená přenosová síť ENTSO-E:

- ENTSO-E se skládá ze 40 členských provozovatelů přenosových soustav, kteří zastupují 36 zemí. Ti jsou zodpovědní za bezpečný a koordinovaný provoz evropské elektrické soustavy, největší propojené elektrické sítě na světě.[42]
- ENTSO-E (European Network of Transmission System Operators for Electricity) je příkladem subjektu zvláštního evropského významu, protože koordinuje provoz přenosových sítí ve více než šesti členských státech EU.
- Ochrana této sítě vyžaduje spolupráci mezi všemi zapojenými státy, aby byla zajištěna stabilita a kontinuita dodávek elektřiny

[40] ČEZ. O společnosti [online]. *cezdistribuce.cz.* [cit. 14.05.2024]. https://www.cezdistribuce.cz/cs/o-spolecnosti

[41] ČEZ. O společnosti [online]. *cezdistribuce.cz.* [cit. 14.05.2024]. https://www.cezdistribuce.cz/cs/o-spolecnosti

[42] ENTSO-E. ENTSO-E Mission Statement [online]. *entsoe.eu.* [cit. 20.05.2024]. https://www.entsoe.eu/about/inside-entsoe/objectives/

napříč Evropou. Směrnice 2022/2557 vyžaduje, aby byly zavedeny společné krizové plány a systémy včasného varování.

2.6 Proces určení prvků KI a EKI a určení subjektů KI

V této podkapitole se budeme zabývat procesem identifikace a určení prvků KI a EKI, se zaměřením na energetický sektor, konkrétně oblast elektřiny. Prozkoumáme, jakým způsobem jsou klíčové prvky a subjekty identifikovány, jaké metody a kritéria jsou při tomto procesu využívány. Proces určení prvků kritické infrastruktury je rozdělen do 4 fází.[43]
Fáze 1: Návrh na určení prvku KI

- Navrhování: Hodnotitel (Ministerstvo průmyslu a obchodu (pro elektroenergetiku) nebo Ministerstvo vnitra (pro nestátní prvky)) navrhne provoz, u kterého lze předpokládat splnění prvků KI/EKI.
- Získání podkladů: Hodnotitel získá od navrhovatele nebo provozovatele potřebné podklady pro hodnocení.
- Vypracování protokolu: Po získání dokumentů a údajů hodnotitel vygeneruje Protokol o návrhu na určení prvku kritické infrastruktury.

Fáze 2: Analýza podkladových dat

- Analýza a porovnání: Hodnotitel analyzuje poskytnutá data s odvětvovými a průřezovými kritérii, včetně kritéria kontinuity provozuschopnosti:[44] [45]
    1. Posouzení podle národních odvětvových kritérií
        a) Zařízení pro výrobu elektřiny:

[43] Řehák, D., Hadáček, L. Metodika jednotného určování zařízení pro výrobu, přenos a distribuci elektřiny národní a evropskou kritickou infrastrukturou a zajišťování fyzické ochrany těchto zařízení. In: Řehák, D., Hadáček, L. *Objektivizace hrozeb a rizik zařízení pro výrobu a přenos elektřiny*. Praha, 2013, s. 8-12.

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

[45] Řehák, D., Hadáček, L. Metodika jednotného určování zařízení pro výrobu, přenos a distribuci elektřiny národní a evropskou kritickou infrastrukturou a zajišťování fyzické ochrany těchto zařízení. In: Řehák, D., Hadáček, L. *Objektivizace hrozeb a rizik zařízení pro výrobu a přenos elektřiny*. Praha, 2013, s. 10-11.

- výrobna s celkovým instalovaným elektrickým výkonem nejméně 500 MW,
- výrobna poskytující podpůrné služby s celkovým instalovaným elektrickým výkonem nejméně 100 MW,
- vedení pro vyvedení výkonu a zabezpečení vlastní spotřeby výrobny elektřiny,
- dispečink výrobce elektřiny.

b) Zařízení pro přenos elektřiny:
- vedení přenosové soustavy o napětí nejméně 110 kV,
- elektrická stanice přenosové soustavy o napětí nejméně 110 kV,
- technický dispečink provozovatele přenosové soustavy.

c) Zařízení pro distribuci elektřiny:
- elektrická stanice distribuční soustavy a vedení o napětí 110 kV (stanice typu 110/10 kV, 110/22 kV a 110/35 kV a k nim patřící vedení se posuzují podle jejich strategického významu v distribuční soustavě),
- technický dispečink provozovatele distribuční soustavy.

2. Posouzení podle národních průřezových kritérií
   a) obětí s mezní hodnotou více než 250 mrtvých nebo více než 2500 osob s následnou hospitalizací po dobu delší než 24 hodin,
   b) ekonomického dopadu s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu, nebo
   c) dopadu na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125000 osob.
3. Posouzení podle evropských odvětvových kritérií
   a) Zařízení pro výrobu elektřiny.
   b) Zařízení pro přenos elektřiny.

4. Posouzení podle evropských průřezových kritérií
    a) Hledisko dopadu významného dopadu na dva a více členských států.

- Hodnocení nenahraditelnosti: Pokud je zařízení hodnoceno jako nenahraditelné, je považováno za prvek KI.

Fáze 3: Posouzení návrhu hodnotící komisí

- Složení komise: Hodnotící komise zahrnuje hodnotitele, navrhovatele, zástupce odboru elektroenergetiky a další relevantní subjekty.
- Posouzení návrhu: Komise posuzuje a vydává verdikt o navržených prvcích KI.

Fáze 4: Vydání opatření obecné povahy

- Určení prvků: Hodnotitel určí prvky KI a prvky EKI a zašle návrhy Ministerstvu vnitra.
- Informování Evropské komise: Ministerstvo vnitra informuje Evropskou komisi o prvcích EKI a pravidelně předkládá zprávy o zranitelnosti a rizicích.
- Aktualizace seznamu: Proces určování prvků KI je kontinuální a seznam je pravidelně aktualizován.

Podle návrhu zákona o kritické infrastruktuře by se již nepostupovalo podle těchto fází. Navrhovaný zákon má totiž za cíl centralizovat proces a bude se řídit novými kritérii, jako je poskytování základních služeb a jejich významnost. Následně jsou uvedeny 4 fáze procesu určení subjektů KI, dle návrhu zákona o kritické infrastruktuře.

Fáze 1: Návrh na určení subjektu kritické infrastruktury

- Ministerstvo (Ministerstvo průmyslu a obchodu - elektroenergetika), jiný ústřední správní úřad nebo Česká národní banka (hodnotitel) zhodnotí, zda je subjekt poskytovatelem základní služby.
- Poskytovatel základních služeb je povinen poskytnout hodnotiteli potřebné informace (skrze Portál kritické infrastruktury)
    - o poskytované základní službě a naplnění kritéria významnosti,
    - o své kritické infrastruktuře na území nebo mimo území České republiky,
    - o základní službě poskytované mimo území České republiky.

Fáze 2: Analýza informací poskytovatele

- Hodnotitel analyzuje data poskytnutá poskytovatelem základních služeb.
- Kritérium významnosti stanoví prováděcí právní předpis, který zohlední[46]:
    - počet uživatelů závislých na základní službě,
    - závislost jiných odvětví a pododvětví na základní službě,
    - možný dopad incidentů na ekonomiku, společnost, životní prostředí, veřejnou bezpečnost, obecnou bezpečnost nebo zdraví obyvatelstva,
    - tržní podíl poskytovatele základní služby,
    - území ovlivněné incidentem včetně přeshraničních dopadů,
    - důležitost poskytovatele pro udržování základní služby,
    - jedinečnost poskytovatele základní služby.

Fáze 3: Doporučení na určení subjektu KI

- Hodnotitel zašle Ministerstvu vnitra doporučení na určení poskytovatele základní služby subjektem kritické infrastruktury.

Fáze 4: Zařazení na seznam KI

- Ministerstvo vnitra určí subjekt kritické infrastruktury zařazením na seznam subjektů kritické infrastruktury, který je neveřejný.
- Ministerstvo vnitra informuje subjekt kritické infrastruktury, Národní úřad pro kybernetickou a informační bezpečnost, věcně příslušné ministerstvo, jiný ústřední správní úřad nebo Českou národní banku o zařazení na seznam subjektů kritické infrastruktury do jednoho měsíce ode dne tohoto určení.
- Informování Evropské komise: Ministerstvo vnitra informuje Evropskou komisi o seznamu základních služeb, subjektech evropské kritické infrastruktury a pravidelně předkládá souhrnnou zprávu o incidentech a posouzení rizik.

[46] § 9 návrhu zákona o kritické infrastruktuře.

2.7 Dílčí závěr

Závěr této kapitoly diplomové práce uvádí důležitost porozumění kyberbezpečnosti a kritické infrastruktuře v dnešní digitální éře. Kybernetická bezpečnost je klíčovým prvkem pro ochranu jak jednotlivců, tak i organizací před rostoucími kybernetickými hrozbami. Zabezpečení této infrastruktury se stále více stává prioritou, protože jakékoli selhání nebo útok na ni by mohlo mít katastrofální důsledky, například výpadek energetického systému by mohl vést k masivním hospodářským škodám a ohrožení životů občanů. Proto je nezbytné vyvinout a implementovat komplexní bezpečnostní opatření, která zahrnují plány krizového řízení, monitorování kritických systémů a zabezpečení používání citlivých systémů a dat. V této kapitole jsou vysvětleny základní pojmy v oblasti kybernetické bezpečnosti, včetně kybernetických událostí a kybernetických bezpečnostních incidentů, a také je zde zdůrazněn význam kritické infrastruktury pro stabilitu společnosti a ekonomiky.

V rámci Evropské unie je klíčové rozlišovat mezi národní a evropskou kritickou infrastrukturou. Přestože přístup založený na prvcích kritické infrastruktury má své výhody, jako je lepší ochrana, současně s sebou nese i určité nevýhody, jako je administrativní zátěž a nedostatečná flexibilita. V současnosti se připravují návrhy zákona o kritické infrastruktuře a zákona o kybernetické bezpečnosti, které mají za cíl reflektovat aktuální a budoucí hrozby, podporovat spolupráci a inovaci, a přinést lepší ochranu pro občany, efektivnější reakci na kybernetické útoky a zvýšenou odolnost kritických systémů.

Nový právní rámec v České republice odpovídá evropským směrnicím a zdůrazňuje význam odolnosti a sdílení informací mezi subjekty kritické infrastruktury. Tento rámec přináší některé přísnější požadavky na ochranu a zároveň zachovává některé stávající prvky, což umožňuje lepší integraci národních a unijních norem. Pro občany to znamená zvýšenou bezpečnost a stabilitu kritických služeb, jako je dodávka energie, vody a doprava. Nicméně, nový přístup přináší i určité výzvy, například kritiku výše navrhovaných pokut a možnost ministerstva vnitra zakazovat subjektům kritické infrastruktury jejich dodavatele, což může vést k obavám z možného zneužití moci. Je však důležité zvážit různé aspekty a připomínky, které vznikly během přípravy nového právního rámce.

Navrhovaný nový přístup k identifikaci a ochraně subjektů kritické infrastruktury v souladu se směrnicí CER představuje změnu zaměření

od samotných prvků kritické infrastruktury směrem k individuálním subjektům poskytujícím základní služby. Tato změna má za cíl zvýšit odolnost a efektivitu ochrany kritických systémů v době nejistoty a rizik. Nicméně, s tímto novým přístupem se pojí určité výzvy a kritické připomínky, které musí být řešeny v rámci přípravy a implementace nového právního rámce. Při implementaci je nezbytné zajistit vyváženost a propojení směrnice CER se směrnicí NIS 2. Obě směrnice jsou navrženy tak, aby se vzájemně doplňovaly, přičemž mají za cíl dosáhnout vysoké úrovně kybernetické bezpečnosti a posílit odolnost kritických subjektů vůči kybernetickým útokům a hrozbám v rámci Evropské unie. Je tedy zapotřebí, aby i návrhy zákonů o kritické infrastruktuře a kybernetické bezpečnosti docílily sjednocení terminologie pro efektivní ochranu kritické infrastruktury.

Analyzování těchto právních nástrojů a jejich aplikace v praxi nám pomůže lépe porozumět výzvám v oblasti kybernetické bezpečnosti a navrhnout účinnější opatření pro ochranu kritických systémů v Evropské unii. Mezi klíčové výzvy patří složitost detailní identifikace kritické infrastruktury podle jednotlivých prvků, administrativní zátěž spojená se správou a aktualizací rozsáhlého seznamu kritické infrastruktury a nedostatečná flexibilita pevně stanovených definic, které nemusí adekvátně reagovat na rychle se měnící technologické a společenské trendy.

Návrhy účinnějších opatření pro ochranu kritických systémů zahrnují zavedení komplexního monitorovacího systému, který umožní včasnou detekci potenciálních hrozeb a zranitelností, posílení spolupráce mezi vládními a soukromými subjekty, výzkumnými institucemi a odborníky na bezpečnost, a investice do nových technologií a postupů, které mohou pomoci minimalizovat rizika. Dále je navrhováno zvýšení odolnosti kritických systémů prostřednictvím lepšího plánování krizového řízení a sdílení informací mezi subjekty kritické infrastruktury, což umožní rychlou a efektivní reakci v případě mimořádných událostí.

Tento přístup lépe reflektuje moderní hrozby a umožňuje efektivnější ochranu a reakci v případě potřeby, což přináší lepší ochranu a stabilitu základních služeb pro občany. Závěrem je třeba zdůraznit, že pro úspěšné odolání moderním hrozbám a zabezpečení kritických systémů v Evropě jsou klíčové budoucí právní úpravy a inovativní postupy.

3 Vývoj kyberbezpečnosti kritické infrastruktury

Prvním významným bodem v oblasti kyberbezpečnosti bylo založení agentury ENISA v roce 2004.[47] V roce 2008 byla vydána směrnice o evropské kritické infrastruktuře (směrnice ECI), která se vztahovala na odvětví dopravy a energetiky. Ovšem tato směrnice zatím neznala pojem kyberbezpečnost, přesto je stále účinná, a to až do 17. října 2024, kdy bude transponována směrnice CER. Větším milníkem kyberbezpečnosti byl rok 2013, kdy v rámci první strategie kybernetické bezpečnosti EU (EUCSS) bylo poprvé volně použito slovo kybernetická bezpečnost[48]. Cílem EUCSS byl otevřený, bezpečný a chráněný kyberprostor. Otevřený, bezpečný a chráněný kyberprostor EU přináší, dle EUCSS, Evropské unii několik významných výhod. EUCSS se snažila vytvořit bezpečné prostředí online.[49] To vedlo, spolu s přijetím jednotlivých předpisů (jak je rozebráno dále), k podpoře stále se rozvíjející digitální ekonomiky a stimulaci ekonomického růstu a inovací díky bezpečnému online obchodu a poskytování služeb, což přineslo nové příležitosti pro podniky.[50] Dále se snažila zvýšit důvěru občanů a podniků v digitální služby a technologie, což je klíčové pro širší přijetí těchto služeb.[51] Strategie měla rovněž

[47] ENISA. O agentuře ENISA – Agentuře Evropské unie pro kybernetickou bezpečnost [online]. *enisa.europa.eu.* [cit. 16.05.2024]. https://www.enisa.europa.eu/about-enisa/about/cs

[48] Společné sdělení Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů. Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor. Dokument 52013JC0001 – v konečném znění.

[49] Opinion of the European Economic and Social Committee on the 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: the Digital Agenda for Europe — Driving European growth digitally'. Dokument COM (2012) 784 – v konečném znění.

[50] Bogoslov, A., Stoica, E. A. Europe's Struggle and Transformation in an Almost Fully Digitized World. *Revista Economică*. 2019, č. 71(4), s. 31-32.

[51] European Commission. Tisková zpráva: EU Cybersecurity plan to protect open internet and online freedom and opportunity ze dne 07. února 2013 [online].

za cíl zajistit, že digitální technologie jsou používány v souladu s demokratickými hodnotami a lidskými právy, čímž posílila postavení EU na globální scéně jako jednoho z lídrů v oblasti kybernetické bezpečnosti a digitální ekonomiky.[52] Dle EUSCC měly jednotlivé členské státy vytvořit národní tým pro počítačové nouzové reakce (CERT), v ČR plní funkci vládního CERTu Národní centrum kybernetické bezpečnosti (NCKB). NCKB je výkonnou sekcí Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). [53] Návrh směrnice NIS byl již součástí první strategie kybernetické bezpečnosti EU (EUCSS). Tato strategie položila základy pro koordinovaný přístup k řešení kybernetických hrozeb a zdůraznila potřebu harmonizace kybernetické bezpečnosti napříč členskými státy EU. Návrh směrnice NIS se zaměřil na zajištění vysoké úrovně bezpečnosti sítí a informačních systémů, a to jak ve veřejném, tak i soukromém sektoru. Tímto krokem chtěla EU podpořit sdílení informací a spolupráci mezi členskými státy v oblasti kybernetické bezpečnosti.

Dalším krokem byla směrnice 2016/1148 (směrnice NIS), schválená Evropskou unií v roce 2016, která přinesla do praxe několik zásadních změn v oblasti kybernetické bezpečnosti v Evropské unii. Tato směrnice vytvořila společný právní rámec, který měl zajistit vysokou úroveň bezpečnosti sítí a informačních systémů napříč členskými státy. Jednalo se o první legislativní nástroj na úrovni EU, který se specificky zaměřoval na kybernetickou bezpečnost. Stanovuje povinnost, aby operátoři základních služeb a digitální poskytovatelé služeb dodržovali požadavky na bezpečnost sítě a informací. Operátoři základních služeb zahrnují subjekty v oblastech jako je energie, bankovnictví, zdravotnictví atd.[54], zatímco digitální poskytovatelé služeb zahrnují cloudové služby,

ec.europa.eu. [cit. 19.05.2024]. https://ec.europa.eu/commission/presscorner/detail/en/IP_13_94

[52] Bogoslov, A., Stoica, E. A. Europe's Struggle and Transformation in an Almost Fully Digitized World. *Revista Economică*. 2019, roč. 71, č. 4, s. 34.

[53] NÚKIB. Kybernetická bezpečnost [online]. *nukib.gov.cz.* [cit. 25.04.2024]. https://nukib.gov.cz/cs/kyberneticka-bezpecnost/

[54] Čl. 4 odst. 4 směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

online tržiště atd[55]. Cílem bylo zvýšit odolnost vůči kybernetickým hrozbám, zejména u základních služeb, které jsou klíčové pro fungování společnosti a ekonomiky.[56] Směrnice zaváděla povinnost pro provozovatele základních služeb a digitálních služeb přijímat přiměřená bezpečnostní opatření a hlásit závažné incidenty.[57] Ovšem pouze 11 států splnilo požadavky směrnice před lhůtou, což vyvolává otázky ohledně jejího vlivu na evropskou kybernetickou bezpečnost.[58]

Jedním z největších přínosů směrnice bylo, že sloužila jako katalyzátor pro změnu regulačního prostředí v oblasti kybernetické bezpečnosti v celé EU. Povinnost určovat provozovatele základních služeb vedla k detailnímu posouzení rizik spojených s jejich činností a k vytvoření strukturovaných bezpečnostních opatření.[59] [60] Směrnice také podpořila kulturu řízení rizik mezi poskytovateli těchto služeb.[61]

---

[55] Čl. 4 odst. 5 směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

[56] Adami. M., et al. Summary of First Interim Study Report (D1). In: Adami. M., et al. *Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) - No. 2020- 665*. CEPS, 2021, s. 9.

[57] Zpráva Komise Evropskému parlamentu a Radě hodnotící konzistentnost přístupů členských států při určování provozovatelů základních služeb v souladu s čl. 23 odst. 1 směrnice 2016/1148/EU o bezpečnosti sítí a informačních systémů. Dokument COM(2019) 546 - v konečném znění.

[58] Irwin, L. Majority of EU member states missed NIS Directive deadline [online]. *IT Governance Blog En.* [cit. 20.06.2024]. https://www.itgovernance.eu/blog/en/majority-of-eu-member-states-missed-nis-directive-deadline

[59] Adami. M., et al. Summary of First Interim Study Report (D1). In: Adami. M., et al. *Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) - No. 2020- 665*. CEPS, 2021, s. 12 a 15.

[60] Zpráva Komise Evropskému parlamentu a Radě hodnotící konzistentnost přístupů členských států při určování provozovatelů základních služeb v souladu s čl. 23 odst. 1 směrnice 2016/1148/EU o bezpečnosti sítí a informačních systémů. Dokument COM(2019) 546 - v konečném znění.

[61] Adami. M., et al. Summary of First Interim Study Report (D1). In: Adami. M., et al. *Study to support the review of Directive (EU) 2016/1148 concerning*

Přestože směrnice přinesla významné pozitivní změny, čelila také několika výzvám. Implementace směrnice v jednotlivých členských státech nebyla konzistentní, což vedlo k roztříštěnosti přístupů.[62] Tento nedostatek jednotnosti mohl způsobit nestejné úrovně kybernetické odolnosti a zvýšit riziko, že přeshraniční incidenty způsobí rozsáhlé škody. Další slabinou byla nejednotnost v určení provozovatelů základních služeb a mezních hodnot pro jejich určení, což komplikovalo porovnání výsledků mezi státy a vedlo k nerovným podmínkám na vnitřním trhu.[63]

Navzdory těmto problémům směrnice NIS položila základy pro další rozvoj kybernetické bezpečnosti v EU a zvýšila povědomí o nutnosti koordinovaného přístupu. Skupina pro spolupráci v oblasti bezpečnosti sítí a informací, složená ze zástupců členských států, Komise a agentury ENISA, sehrála klíčovou roli v poskytování pokynů a výměně osvědčených postupů mezi státy.[64] Výzvou do budoucna zůstává dosažení větší konzistentnosti v implementaci směrnice a sladění bezpečnostních opatření napříč celou EU.

Směrnice NIS měla vztah k dalším předpisům v oblasti kybernetické bezpečnosti. Například, směrnice ECI byla jedním z rámců, na který členské státy navazovaly při určování provozovatelů základních služeb.[65]

---

measures for a high common level of security of network and information systems across the Union (NIS Directive) - No. 2020- 665. CEPS, 2021, s. 12 a 15.

[62] Adami. M., et al. Summary of First Interim Study Report (D1). In: Adami. M., et al. *Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) - No. 2020- 665*. CEPS, 2021, s. 26-27.

[63] Adami. M., et al. Summary of First Interim Study Report (D1). In: Adami. M., et al. *Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) - No. 2020- 665*. CEPS, 2021, s. 26-27.

[64] Adami. M., et al. Summary of First Interim Study Report (D1). In: Adami. M., et al. *Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) - No. 2020- 665*. CEPS, 2021, s. 10.

[65] Zpráva Komise Evropskému parlamentu a Radě hodnotící konzistentnost přístupů členských států při určování provozovatelů základních služeb v souladu s čl. 23

Směrnice NIS také zohledňuje zásadu lex specialis, což znamená, že pokud existují specifické sektoriální předpisy (např. v oblasti telekomunikací podle směrnice 2002/21/ES), směrnice NIS se na tyto oblasti nevztahuje, pokud sektoriální předpisy zajišťují rovnocennou úroveň bezpečnosti.[66] Tímto způsobem směrnice NIS integrovala a doplňovala stávající legislativní rámce, čímž zajistila komplexnější přístup k ochraně kritických služeb a infrastruktury v EU.

Přestože tyto iniciativy nejsou specificky zaměřeny na kyberbezpečnost kritické infrastruktury, tak stále poskytují důležitý kontext pro vývoj kyberbezpečnosti v EU, protože digitální trh a kybernetická odolnost jsou klíčovými aspekty celkové bezpečnosti a stability unie. Dále také tyto iniciativy značí první kroky k zintenzivnění úsilí o posílení kyberbezpečnosti.

Strategie pro jednotný digitální trh z roku 2015 byla iniciativou Evropské komise, jejímž cílem bylo vytvořit jednotný digitální prostor v EU. Strategie se zaměřila na tři hlavní oblasti: zlepšení přístupu k digitálnímu zboží a službám, vytvoření vhodných podmínek pro rozvoj digitálních sítí a služeb, a maximalizaci růstového potenciálu digitální ekonomiky.[67] Cíle strategie zahrnovaly lepší dostupnost online služeb pro spotřebitele, podporu inovací a zvýšení konkurenceschopnosti evropských podniků.[68] Slabiny však zahrnovaly složitost harmonizace právních předpisů mezi členskými státy, problémy z implementací v jednotlivých členských státech a obavy ohledně ochrany osobních údajů.[69] Implementace této

odst. 1 směrnice 2016/1148/EU o bezpečnosti sítí a informačních systémů. Dokument COM(2019) 546 - v konečném znění.

[66] Čl. 1 odst. 3 Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

[67] Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu Výboru a Výboru regionů. Strategie pro jednotný digitální trh v Evropě. Dokument COM(2015) 192 - v konečném znění.

[68] Farkač, M. Jednotný digitální trh – atraktivní, leč problematický návrh [online]. *tvorimevropu.cz.* [cit. 25.05.2024]. https://tvorimevropu.cz/2015/04/08/jednotny-digitalni-trh-atraktivni-lec-problematicky-navrh/

[69] Rosati, E. The DSM Directive 3 years on: have we found our digital single market yet? *Journal of Intellectual Property Law & Practice*. 2022, roč. 17, č. 5, s. 397-398.

strategie vedla k významným změnám, jako je například zavedení GDPR, ale také poukázala na nutnost další koordinace.[70]

Společná zpráva a sdělení Evropské komise o odolnosti z roku 2017 se zaměřila na posílení kyberbezpečnost prostřednictvím několika klíčových opatření a cílů. Mezi hlavní cíle patří zvýšení kybernetické odolnosti, kde je zdůrazněna potřeba posílit bezpečnostní opatření v rámci EU, a zlepšení spolupráce prostřednictvím zřízení a využívání sítě bezpečnostních týmů typu CSIRT a skupiny CERT-EU pro strategickou spolupráci.[71] EU také usiluje o posílení důvěry v digitální společnost a ekonomiku tím, že zajistí efektivnější meziodvětvovou reakci na kybernetické hrozby.[72] Dalším významným krokem je smluvní partnerství veřejného a soukromého sektoru na vývoji a zkoušení technologií k ochraně před kybernetickými hrozbami.[73] Ve společné zprávě byla rovněž naplánována revize mandátu agentury ENISA, která má za cíl jasně vymezit její funkce v rámci nového prostředí kybernetické bezpečnosti.[74] Tento cíl byl v praxi dosažen směrnicí CRA. Další opatření se týkají vlastníků inteligentních sítí, aby zlepšili kybernetickou bezpečnost svých zařízení a vytvořili plány připravenosti na rizika v energetickém sektoru.[75] To bylo v praxi realizováno několika předpisy a dokumenty, mezi které patří Cybersecurity Act, směrnice NIS, Doporučení Komise 2019/553, nařízení 2019/943 a nově přijaté Nařízení Komise v přenesené pravomoci 2024/1366.

---

[70] Thouvenin, F., Tamò-Larrieux, A. Data Ownership and Data Access Rights: Meaningful Tools for Promoting the European Digital Single Market? In: Burri, M. (eds). *Big Data and Global Trade Law*. Cambridge University Press, 2021, s. 319.

[71] Společné sdělení Evropskému parlamentu a Radě. Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU. Dokument JOIN(2017) 450 - v konečném znění.

[72] Společná zpráva Evropskému parlamentu a Radě o provádění společného rámce pro boj proti hybridním hrozbám – reakce Evropské unie. Dokument JOIN(2017) 30 - v konečném znění.

[73] Společná zpráva Evropskému parlamentu a Radě o provádění společného rámce pro boj proti hybridním hrozbám – reakce Evropské unie. Dokument JOIN(2017) 30 - v konečném znění.

[74] ibidem

[75] ibidem

Po roce 2019 Evropská unie postoupila k posílení kybernetické bezpečnosti kritické infrastruktury prostřednictvím řady významných legislativních a strategických iniciativ. Legislativní rámec kybernetické bezpečnosti kritické infrastruktury v EU se od té doby významně rozvinul, aby reagoval na rostoucí a stále sofistikovanější kybernetické hrozby. Tyto iniciativy jsou zaměřeny na posílení schopností členských států v oblasti prevence, detekce a reakce na kybernetické hrozby, čímž se zajišťuje bezpečnost a odolnost klíčových odvětví napříč Evropskou unií.

V červnu 2019 byla přijetím nařízení 2019/881 (Cybersecurity Act) zlepšena transparentnost a důvěryhodnost kybernetické bezpečnosti v EU. Cybersecurity Act představuje významný krok Evropské unie směrem k jednotnému a harmonizovanému systému certifikace ICT produktů, služeb a procesů napříč členskými státy.[76] Jeho primárním účelem je posílení ochrany kybernetické bezpečnosti v rámci EU a zároveň umožnit výrobcům a poskytovatelům služeb používat jeden vzájemně uznávaný certifikát.[77] Ovšem předpis má i své slabé stránky, jako je např. problém s implementací certifikátu z důvodu různorodosti a nestálosti IoT zařízení, či zastarání certifikovaných produktů z důvodu rychlého vývoje technologií.[78] [79] Důsledky pro praxi, včetně přínosů a nevýhod, budou podrobněji rozebrány v podkapitole 4.1.

Nová kybernetická strategie EU (EUCSS), uveřejněná v prosinci 2020, má za cíl zvýšit odolnost proti kybernetickým hrozbám v době rostoucího počtu útoků a digitalizace. Je zaměřena na tři hlavní aspekty: zvýšení odolnosti a vedení, budování operační kapacity a posílení globální

[76] European Commission. The EU Cybersecurity Act [online]. *digital-strategy.ec.europa.eu.* [cit. 18.05.2024]. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act

[77] ENISA. Cybersecurity Certification Framework [online]. *enisa.europa.eu.* [cit. 18.05.2024]. https://www.enisa.europa.eu/topics/certification/cybersecurity-certification-framework

[78] Kowalski, B., Intemann, M., Mühlenbruch, T. Bedeutung des Cybersecurity Acts für die IT-Sicherheitszertifizierung in Deutschland und Europa. *Schwerpunkt.* 2021, roč. 45, s. 247-248.

[79] Khurshid, A., et al. EU Cybersecurity Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme. *IEEE Access*. 2022, roč. 10, s. 129934.

spolupráce.[80] EUCSS představuje legislativní kroky, jako jsou směrnice NIS 2 a CER, pro posílení kybernetické bezpečnosti napříč různými odvětvími. Klade důraz na vytvoření Evropského kybernetického štítu a Společného kybernetického útvaru pro lepší výměnu informací a řízení krizí. S ohledem na globální rozměr se EUCSS snaží prosazovat evropské hodnoty na mezinárodní úrovni.[81] V oblasti obrany a bezpečnosti se zavazuje posílit Kybernetický diplomatický toolbox a zdokonalit obranné schopnosti EU v kybernetické sféře pomocí iniciativ, jako je Rámcová politika kybernetické obrany. Ačkoli není právně závazná, EUCSS představuje klíčové kroky k řešení rostoucích kybernetických hrozeb.

V roce 2022 byla přijata směrnice 2022/2557 (směrnice CER), která představovala významný krok v oblasti kyberbezpečnosti a fyzické odolnosti kritické infrastruktury. Tato směrnice se zaměřila na jedenáct klíčových odvětví, včetně energetiky, dopravy, bankovnictví a zdravotnictví, s cílem snížit jejich zranitelnost vůči různým hrozbám, jako jsou přírodní katastrofy, terorismus a sabotáž.[82] Jedním z hlavních požadavků směrnice bylo, aby členské státy vypracovaly národní strategie pro odolnost kritických infrastruktur.[83] To zahrnovalo zavedení aktualizovaných hodnocení rizik, provádění stresových testů a zajištění koordinovaných reakcí na případná přerušení služeb.[84] Klíčovou součástí bylo také zajištění, že subjekty v těchto sektorech přijmou vhodná bezpečnostní

[80] Lété, B. The Relevance of Multistakeholder Input for the EU Cybersecurity Strategy. In: Lété, B. *Implementing the EU Cybersecurity Strategy.* The European Cyber Agora, 2021, s. 9.

[81] ibidem

[82] Cyber Risk GmbH. Healthcare - Critical Entities Resilience Directive (CER) [online]. *european-health-data-space.com.* [cit. 20.11.2023]. https://www.european-health-data-space.com/CER_Training.html

[83] European Commission. Critical infrastructure resilience [online]. *home-affairs.ex.europa.eu.* [cit. 16.04.2024]. https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience_en

[84] Cyber Risk GmbH. The Critical Entities Resilience Directive (CER) [online]. *critical-entities-resilience-directive.com.* [cit. 12.04.2024]. https://www.critical-entities-resilience-directive.com/

opatření k posílení své odolnosti.[85] Přestože směrnice přinesla významné pokroky v oblasti připravenosti a mezinárodní spolupráce, její implementace nebyla bez problémů. Členské státy se potýkají s výzvami při harmonizaci přístupů, což vede k rozdílné úrovni připravenosti napříč Evropskou unií.[86] Tato rozdílnost ukazuje na potřebu větší koordinace a sdílení osvědčených postupů mezi státy, aby bylo dosaženo jednotné úrovně ochrany kritických infrastruktur. Tato problematika bude podrobněji rozebrána v podkapitole 4.2.

V roce 2023 byl přijat návrh nařízení 2019/1020 (nařízení CRA), zaměřený na posílení bezpečnosti softwarových produktů a digitálních služeb v celé EU. Tento legislativní krok zavedl povinnost nejen výrobců, ale také poskytovatelů služeb a distributorů zajistit, aby jejich produkty splňovaly určité bezpečnostní standardy po celou dobu svého životního cyklu.[87] Cílem bylo vytvořit jednotné kybernetické požadavky napříč celou EU, které by pokrývaly širokou škálu hardwaru a softwaru.[88] Tento akt měl za úkol zajistit vyšší ochranu před kybernetickými útoky a zvýšit důvěru uživatelů v digitální technologie, což je klíčové pro fungování moderní společnosti závislé na digitální infrastruktuře.[89] [90] Vzhledem k současnému nesourodému regulačnímu prostředí v rámci Unie nařízení

[85] European Commission. Critical infrastructure resilience [online]. *home-affairs.ec.europa.eu*. [cit. 16.04.2024]. https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience_en

[86] Sickinghe, F., Karniyevich, N. CER Directive [online]. *twobirds.com.* [cit. 26.05.2024]. https://www.twobirds.com/en/trending-topics/cybersecurity/rce-directive

[87] Limbergová, Z. Akt o kybernetické odolnosti. *Revue pro právo a technologie*. 2023, roč. 14, č. 27, s. 8.

[88] Chin, K. The EU Cyber Resilience Act: Securing Digital Products [online]. *upguard.com*. [cit. 12.05.2024]. https://www.upguard.com/blog/eu-cyber-resilience-act-cra

[89] Eckhardt, P., Kotovskaia, A. The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive. *International Cybersecurity Law Review*. 2023, roč. 4, s. 148 -149.

[90] Chiara, P. G. The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. *International Cybersecurity Law Review*. 2022, roč. 3, s. 270.

CRA usiluje o poskytnutí jasnosti a konzistence prostřednictvím stanovení jednotných kybernetických požadavků, které platí pro téměř všechny digitální produkty (výjimka lékařské přístroje, motorová vozidla, či vojenský hardware).[91] Implementace tohoto aktu však naráží na řadu problémů. Podniky se potýkají se sladěním nových bezpečnostních standardů s již existujícími normami a s finančními a technickými aspekty jejich dodržování.[92] Tyto výzvy a jejich konkrétní dopady budou podrobněji rozebrány v podkapitole 4.3.

Směrnice 2022/2555 (směrnice NIS 2) vstoupila v platnost 16. ledna 2023 a aktualizovala původní směrnici z roku 2016. Tato nová směrnice rozšířila spektrum sektorů, které musí splňovat přísnější bezpečnostní požadavky, včetně veřejné správy a digitální infrastruktury. To znamená, že více podniků v různých odvětvích, jako jsou energetika, doprava, zdravotnictví a digitální infrastruktura, bude muset dodržovat přísnější bezpečnostní opatření a povinnosti hlášení incidentů.[93] Hlavním cílem bylo zlepšit spolupráci mezi členskými státy a efektivněji reagovat na nové kybernetické hrozby a technologie.[94] Nicméně, implementace směrnice NIS 2 přináší i některé výzvy a negativa. Některé členské státy se potýkají s problémy při implementaci této směrnice a potřebují více času na přizpůsobení svých národních předpisů.[95] Organizace navíc často upozorňují na administrativní a finanční náročnost spojenou s novými bezpečnostními opatřeními.[96] Blíže k této problematice v podkapitole 4.4.

---

[91] Chiara, P. G. The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. *International Cybersecurity Law Review*. 2022, roč. 3, s. 259.

[92] European Cyber Security Organisation. *Challenges of the industry to implement the CRA*. ECSO, 2024, s. 7 a 10.

[93] Sievers, T. Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations. *International Cybersecurity Law Review. 2021, roč. 2, s*. 225.

[94] Božić, V. *The Network and Information Systems (NIS) Directive 2: A Comprehensive Analysis*. 2024, s. 8.

[95] Božić, V. *The Network and Information Systems (NIS) Directive 2: A Comprehensive Analysis*. 2024, s. 12-14.

[96] Božić, V. *The Network and Information Systems (NIS) Directive 2: A Comprehensive Analysis*. 2024, s. 13.

Poslední významnou iniciativou byl návrh nařízení o kybernetické solidaritě (Cyber Solidarity Act) z roku 2023. Tento akt se zaměřil na posílení kybernetické bezpečnosti napříč členskými státy prostřednictvím spolupráce, harmonizace a rychlé reakce na kybernetické hrozby. Cyber Solidarity Act zavádí mechanismy pro sdílení informací a poskytování podpory v případě rozsáhlých kybernetických incidentů, což by mělo zlepšit schopnost EU efektivně reagovat na kybernetické útoky a minimalizovat jejich dopady.[97] Konkrétně zahrnuje tři klíčové prvky: evropský kybernetický štít, nouzový kybernetický mechanismus a mechanismus pro přezkoumání kybernetických incidentů.[98] Cyber Solidarity Act by mohl mít významný dopad na kybernetickou bezpečnost kritické infrastruktury v EU tím, že by podporoval vytvoření jednotného a odolného bezpečnostního prostředí schopného čelit stále sofistikovanějším útokům. Nicméně, zavedení těchto opatření vyžaduje značné investice a některé členské státy se potýkají s nedostatečnými zdroji na zavedení opatření, která jsou povinna již z dříve probraných předpisů, natož na plnou implementaci tohoto nařízení. Financování implementace bude probíhat v rámci programu Digital Europe Programme (DEP), avšak na Cyber Solidarity Act bude k dispozici pouze omezené množství finančních prostředků z celkového rozpočtu určeného na kybernetickou bezpečnost.[99]

Z výše uvedeného vyplývá, že EU, především po roce 2019, posiluje a aktualizuje své předpisy týkající se kybernetické bezpečnosti kritické infrastruktury v reakci na nové výzvy a hrozby. Harmonizace pravidel a spolupráce mezi členskými státy jsou klíčovými prvky tohoto úsilí.

3.1 Dílčí závěr

Od založení agentury ENISA v roce 2004 se Evropská unie neustále snaží posilovat právní rámec pro kybernetickou bezpečnost kritické

[97] European Parliamentary Research Service. *Cyber solidarity act.* European Union, 2024, s. 4.

[98] European Parliamentary Research Service. *Cyber solidarity act.* European Union, 2024, s. 5.

[99] European Parliamentary Research Service. *Cyber solidarity act.* European Union, 2024, s. 5-6.

infrastruktury. Přijetí směrnice ECI v roce 2008 bylo prvním významným krokem, který se zaměřoval na fyzickou bezpečnost v sektorech dopravy a energetiky, avšak neřešil kybernetickou bezpečnost. Tento nedostatek byl postupně odstraněn přijetím směrnice NIS v roce 2016, která poprvé stanovila povinnosti v oblasti kybernetické bezpečnosti pro operátory základních služeb a digitálních poskytovatelů služeb.

Navzdory tomu, že směrnice NIS přinesla mnoho pozitivních změn, její implementace nebyla bez problémů. Pouze 11 členských států splnilo požadavky směrnice před stanovenou lhůtou, což vedlo k nejednotnosti přístupů a rozdílné úrovni kybernetické odolnosti mezi státy. Tento problém byl částečně řešen návrhem směrnice NIS 2, která rozšířila spektrum sektorů, které musí splňovat bezpečnostní požadavky, a zavedla přísnější pravidla pro sdílení informací a spolupráci mezi členskými státy.

Další významný krok představovalo přijetí Cybersecurity Act v roce 2019, které posílilo roli ENISA a zavedlo evropský rámec pro certifikaci kybernetické bezpečnosti ICT produktů, služeb a procesů. Tento rámec má za cíl poskytnout jednotné standardy napříč EU a zvýšit důvěru v digitální technologie, což je klíčové pro ochranu kritické infrastruktury.

Směrnice CER z roku 2022 rozšířila odolnost na 11 odvětví kritické infrastruktury, zatímco návrh nařízení CRA zlepšuje bezpečnost digitálních produktů. Návrh nařízení o kybernetické solidaritě z roku 2023 pak podporuje spolupráci a rychlou reakci na kybernetické hrozby. Celkově tyto legislativní a strategické iniciativy posilují schopnost členských států EU předcházet, detekovat a reagovat na kybernetické hrozby, čímž zajišťují bezpečnost a odolnost kritické infrastruktury v Evropě.

Vývoj legislativy kybernetické bezpečnosti kritické infrastruktury v EU ukazuje na postupný přístup, který reaguje na rostoucí hrozby a technologické změny. Od počátečních strategických dokumentů přes první právní rámce až po aktuální iniciativy zaměřené na posílení spolupráce a solidarity mezi členskými státy, EU neustále zvyšuje své úsilí o zajištění bezpečnosti a odolnosti své kritické infrastruktury. Analyzování současných právních nástrojů a jejich aplikace v praxi odhaluje výzvy, jako je nejednotnost implementace předpisů a potřeba větší koordinace a sdílení osvědčených postupů mezi členskými státy. Problematika nejednotné implementace předpisů v jednotlivých členských státech a spolupráce mezi organizacemi a úřady při hlášení incidentů bude podrobněji analyzována v kapitole 5, prostřednictvím případových studií.

4 Právní předpisy v oblasti kyberbezpečnosti kritické infrastruktury

Tato kapitola se zaměřuje na analýzu právních požadavků, které jsou klíčové pro zajištění kybernetické bezpečnosti kritické infrastruktury. Vzhledem k rostoucímu počtu a sofistikovanosti kybernetických hrozeb je právní regulace v této oblasti nezbytná pro ochranu národních zájmů a veřejné bezpečnosti. Analyzována bude zejména směrnici NIS 2 a Cybersecurity Act, které tvoří základní právní rámec pro kybernetickou ochranu v současnosti. V této kapitole bude zkoumána nejen platná legislativa, ale i připravované právní předpisy, které mají za cíl zvýšit odolnost infrastruktury vůči kybernetickým útokům. Podíváme na jednotlivé aspekty těchto právních dokumentů a jejich implementaci v praxi.

4.1 Cybersecurity Act

Tato podkapitola se blíže věnuje Cybersecurity Actu. Přestože Cybersecurity Act, přijatý Evropskou unií, se specificky nezaměřuje na kritickou infrastrukturu, jeho zavedení má nepřímý vliv na její bezpečnost. Cybersecurity Act posiluje roli agentury ENISA a zavádí jednotné evropské schéma pro certifikaci kybernetické bezpečnosti ICT produktů, služeb a procesů. Certifikované produkty a služby, které splňují vyšší bezpečnostní standardy, mohou zvýšit celkovou odolnost podniků, včetně těch, které jsou dodavateli či součástí kritické infrastruktury, vůči kybernetickým hrozbám.[100] Tento právní rámec, po zavedení certifikačního schématu do praxe, bude přispívat k lepší připravenosti a schopnosti reagovat na kybernetické incidenty, což je klíčové pro ochranu kritické infrastruktury.

Cybersecurity Act je klíčovým legislativním krokem Evropské unie v oblasti kybernetické bezpečnosti. Jeho hlavními cíli jsou zajistit trvalý mandát Evropské agentuře pro kybernetickou bezpečnost (ENISA)

[100] European Parliamentary Research Service. *ENISA and a new cybersecurity act*. European Union, 2019, s. 11 a 15.

a vytvořit evropský systém pro certifikaci kybernetické bezpečnosti ICT produktů, služeb a procesů.[101] [102]

Nařízení významně posiluje mandát ENISA, která se stává stálou agenturou s rozšířenými pravomocemi. ENISA je pověřena poskytováním poradenství a podpory členským státům, institucím EU a dalším subjektům v otázkách kybernetické bezpečnosti a také koordinací reakcí na kybernetické incidenty. Spolupracuje s národními orgány na zlepšení celkové úrovně kybernetické bezpečnosti v celé EU. Mezi její klíčové úkoly patří poskytování odborné pomoci při vývoji a implementaci evropských politik kybernetické bezpečnosti, podpora výzkumu a inovací, zvyšování povědomí o kybernetických hrozbách a podpora vzdělávacích iniciativ zaměřených na kybernetickou bezpečnost.

Nařízení zavádí celoevropský systém pro certifikaci kybernetické bezpečnosti produktů, služeb a procesů. Evropské certifikační schéma má zajistit splnění přísných bezpečnostních standardů u certifikovaných produktů. Přičemž systém certifikace bude platný po dobu max. 5 let.[103] Potřeba evropského systému vychází z existence mnoha různých certifikačních schémat a standardů kybernetické bezpečnosti v Evropě, což ztěžuje jednotlivcům a organizacím přesné hodnocení kybernetických rizik spojených s používáním ICT produktů, procesů nebo služeb.[104] Evropský systém stanovuje celoevropské parametry pro pravidla, technické požadavky, standardy a postupy obsažené v certifikačních

[101] MergeBase. EU Cybersecurity Act [online]. *mergebase.com.* [cit. 15.05.2024]. https://mergebase.com/compliance/eu-cybersecurity-act/

[102] Vostoupal, J. *Certifikace kyberbezpečnostních technologií*. 2018/2019, diplomová práce, Masarykova univerzita, Právnická fakulta, s. 48.

[103] Čl. 49 odst. 8 nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013.

[104] IT Governance Ltd. The EU Cybersecurity Act [online]. *itgovernance.co.uk*. [cit. 12.05.2024]. https://www.itgovernance.co.uk/eu-cybersecurity-act

schématech.[105] Tato schémata jsou založena na hodnocení rizik a týkají se různých kategorií ICT produktů, procesů a služeb.[106]

Existuje několik bodů, kterých tyto schémata musejí dosáhnout. Mezi ně patří ochrana dat před náhodným nebo neoprávněným ukládáním, zpracováním, přístupem, zveřejněním, zničením, ztrátou, změnou nebo nedostupností během celého životního cyklu ICT produktu, služby nebo procesu.[107]

Cybersecurity Act dále ve svém rámci stanovuje tři úrovně záruky, a to základní, významná a vysoká. Přičemž úroveň záruky odpovídá míře rizika, která vychází z pravděpodobnosti a dopadu incidentu spojeného s plánovaným využitím produktu, služby nebo procesu ICT.

Certifikace podle nových schémat začne jako dobrovolná, avšak Evropská komise bude pravidelně vyhodnocovat její účinnost a využívání. Na základě těchto hodnocení může rozhodnout, zda certifikace bude povinná. První hodnocení se musí uskutečnit do 31. prosince 2023 a následná hodnocení budou probíhat každé dva roky.[108] Jednotlivci a organizace mají právo podat stížnost na vydavatele evropského certifikátu kybernetické bezpečnosti, a také mají právo na soudní ochranu proti rozhodnutím orgánů pro posuzování shody nebo národních certifikačních

[105] IT Governance Ltd. The EU Cybersecurity Act [online]. *itgovernance.co.uk.* [cit. 12.05.2024]. https://www.itgovernance.co.uk/eu-cybersecurity-act

[106] Kohler, C. The EU Cybersecurity Act and European standards: an introduction to the role of European standardization. *International Cybersecurity Law Review*. 2020, roč. 1, s. 7 a 10.

[107] Čl. 51 odst. 1 nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013.

[108] Čl. 56 odst. 3 nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost“), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013.

autorit.[109] Zákon rovněž stanovuje, že za porušení budou uplatňovány sankce, které budou „účinné, přiměřené a odrazující".[110]

Implementace Cybersecurity Actu přináší řadu výzev, ale také přináší výhody jak pro organizace, tak pro členské státy EU.

Jedním z hlavních problémů implementace je fragmentace kybernetického prostoru v EU. Před platností nového nařízení byly certifikace kybernetické bezpečnosti realizovány hlavně na národní úrovni, což vedlo k neuznávání certifikátů mezi členskými státy.[111] [112] Společnosti působící v několika zemích tak musely opakovaně certifikovat své produkty a služby v různých členských státech.[113] [114] Tento problém byl dále komplikován rozdílnými úrovněmi kybernetické bezpečnosti v jednotlivých členských státech, což vedlo k nerovnoměrnému zabezpečení napříč celou Unií.[115] Implementace jednotného certifikačního rámce vyžaduje harmonizaci těchto rozdílů. Ovšem díky harmonizovanému přístupu, dle Cybersecurity Act budou organizace moci získat certifikace platné po

[109] IT Governance Ltd. The EU Cybersecurity Act [online]. *itgovernance.co.uk.* [cit. 12.05.2024]. https://www.itgovernance.co.uk/eu-cybersecurity-act

[110] IT Governance Ltd. The EU Cybersecurity Act [online]. *itgovernance.co.uk*. [cit. 12.05.2024]. https://www.itgovernance.co.uk/eu-cybersecurity-act

[111] Ananda, S., Putranti, I., Dir, A. Analysis Of The EU Cybersecurity Act Under The Theory Of Neoliberal Institutionalism. *Arena Hukum*. 2022, roč. 15, č. 1, s. 192.

[112] Kohler, C. The EU Cybersecurity Act and European standards: an introduction to the role of European standardization. *International Cybersecurity Law Review*. 2020, roč. 1, s. 7-8.

[113] Kohler, C. The EU Cybersecurity Act and European standards: an introduction to the role of European standardization. *International Cybersecurity Law Review*. 2020, roč. 1, s. 9-10.

[114] Kohler, C. The EU Cybersecurity Act and European standards: an introduction to the role of European standardization. *International Cybersecurity Law Review*. 2020, roč. 1, s. 7-8.

[115] ENISA. National Cyber Security Strategies - Interactive Map [online]. *enisa.europa.eu.* [cit. 20.06.2024]. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

celé EU, což sníží administrativní zátěž spojenou s dodržováním různých certifikací na trzích.[116]

Další výzvou jsou zařízení IoT. Ty jsou v současné době pokryta především certifikačním schématem EUCC (pro ICT produkty obecně), zatímco schémata EUCS (pro cloudové služby) a EU5G (pro 5G sítě) je pokrývají jen velmi okrajově.[117] Tato schémata zahrnují některé aspekty zabezpečení IoT zařízení, ale nejsou specificky navržena pro jejich jedinečné potřeby a rizika.[118] Vzhledem k rychlému vývoji a rozmanitosti IoT zařízení bude v budoucnu nezbytné vytvořit nové, specifické certifikační schéma zaměřené výhradně na IoT.[119] Toto schéma by mělo pokrývat specifické bezpečnostní požadavky a technologické výzvy, které IoT zařízení přinášejí.

Co se týče dopadů na praxi, Cybersecurity Act zvyšuje důvěru a bezpečnost ICT produktů, služeb a procesů, což je klíčové pro rozvoj digitálního jednotného trhu. Podniky a spotřebitelé mohou mít větší důvěru ve výrobky, které prošly přísným certifikačním procesem.[120] Dále jednotná certifikace eliminuje potřebu vícenásobné certifikace v různých členských státech, což může vést ke zjednodušení a zlevnění přeshraničního obchodu pro podniky.[121]

Pro organizace přináší Cybersecurity Act výhody v podobě snížení nákladů díky eliminaci potřeby vícenásobné certifikace a zvýšené důvěry

[116] IT Governance Ltd. The EU Cybersecurity Act [online]. *itgovernance.co.uk.* [cit. 12.05.2024]. https://www.itgovernance.co.uk/eu-cybersecurity-act

[117] Hassan, S., et al. Real-Time Investigation of Cross-Technology Interference in Heterogeneous IoT Networks. *IEEE Access*. 2017, s. 5-6.

[118] Hassan, S., et al. Real-Time Investigation of Cross-Technology Interference in Heterogeneous IoT Networks. *IEEE Access*. 2017, s. 5–6.

[119] Hassan, S., et al. Real-Time Investigation of Cross-Technology Interference in Heterogeneous IoT Networks. *IEEE Access*. 2017, s. 8-9.

[120] Kohler, C. The EU Cybersecurity Act and European standards: an introduction to the role of European standardization. *International Cybersecurity Law Review*. 2020, roč. 1, s. 10-11.

[121] Ananda, S., Putranti, I., Dir, A. Analysis Of The EU Cybersecurity Act Under The Theory Of Neoliberal Institutionalism. *Arena Hukum*. 2022, roč. 15, č. 1, s. 189.

zákazníků, což zvyšuje atraktivitu jejich produktů a služeb.[122] [123] Organizace také získají zjednodušený přístup na trhy v různých členských státech díky uznání certifikace napříč EU. Pro členské státy pak harmonizace standardů zajišťuje konzistentní úroveň kybernetické bezpečnosti napříč EU a posiluje národní bezpečnost díky spolupráci na úrovni EU.[124]

4.2 Critical Entities Resilience

Tato podkapitola se zaměřuje na směrnici CER, která představuje klíčový nástroj EU pro posílení odolnosti kritické infrastruktury. Směrnice CER je úzce propojena s kritickou infrastrukturou, neboť stanovuje konkrétní požadavky na ochranu a odolnost entit, které jsou považovány za nezbytné pro fungování společnosti a ekonomiky. Tato podkapitola doplňuje a navazuje na informace uvedené v kapitole "Základní pojmy a kritická infrastruktura," kde byly představeny základní koncepty a význam kritické infrastruktury. Obecně lze říci, že směrnice CER přispěje k efektivnější reakci na kybernetické útoky na kritickou infrastrukturu tím, že zavádí harmonizovaná pravidla a postupy pro identifikaci, prevenci, ochranu, detekci, reakci a zotavení se z těchto incidentů. Tím se zvýší celková odolnost kritických entit vůči různým typům hrozeb a zajistí se kontinuita poskytování základních služeb.

Směrnice CER, platná od 16. ledna 2023, přináší nový rámec pro ochranu kritické infrastruktury, který zohledňuje širokou škálu hrozeb, včetně přírodních katastrof, kybernetických útoků a teroristických

[122] Two Birds. The EU Cybersecurity Act [online]. *twobirds.com.* [cit. 15.05.2024]. https://www.twobirds.com/en/capabilities/practices/digital-rights-and-assets/european-digital-strategy-developments/cybersecurity/cybersecurity/the-eu-cybersecurity-act

[123] Dunkelberger, D. Understanding the EU Cybersecurity Act and Its Effect on Businesses [online]. *ispartnersllc.com.* [cit. 15.05.2024]. https://www.ispartnersllc.com/blog/eu-cybersecurity-act-effects-businesses/

[124] Ananda, S., Putranti, I., Dir, A. Analysis Of The EU Cybersecurity Act Under The Theory Of Neoliberal Institutionalism. *Arena Hukum*. 2022, roč. 15, č. 1, s. 192.

akcí.[125] Jedním z hlavních přínosů směrnice CER je rozšíření rozsahu pokrytých sektorů z původních dvou (energetika a doprava) na jedenáct.[126] Toto rozšíření zavazuje kritické entity v daných sektorech provádět hodnocení rizik a přijímat technická, bezpečnostní a organizační opatření, která jsou adekvátní a odpovídající rizikům, jimž čelí.[127] Tímto způsobem budou schopny předcházet incidentům, reagovat na ně, odolávat jim, přizpůsobovat se jim a zotavovat se z nich.[128] Dodržování, těchto povinností a opatření kritickými subjekty, má za cíl zajistit vyšší úroveň kybernetické odolnosti a bezpečnosti. Například posouzení rizik, která mohou ohrozit jejich činnost, by se mělo provádět nejméně každé čtyři roky.[129]

Jak již bylo uvedeno, směrnice CER stanovuje kritéria pro identifikaci kritických subjektů. To zahrnuje poskytování jednoho nebo více základních služeb, provozování kritických infrastruktur v území členského státu a možnost, že narušení těchto subjektů by mohlo ovlivnit jednu nebo více základních služeb (viz kapitola 2). V případě bezpečnostního

[125] Kastrati, B., Pavleski, A., Spasov, N. Cyber-security as an issue of the contemporary security agenda. In: Dujovski, N. (eds). *The strategic and security concept for the countries of southest europe*. International scientific conference, Skopje, 2023, roč. 8, č. 1, s. 303.

[126] Kastrati, B., Pavleski, A., Spasov, N. Cyber-security as an issue of the contemporary security agenda. In: Dujovski, N. (eds). *The strategic and security concept for the countries of southest europe*. International scientific conference, Skopje, 2023, roč. 8, č. 1, s. 303.

[127] Kastrati, B., Pavleski, A., Spasov, N. Cyber-security as an issue of the contemporary security agenda. In: Dujovski, N. (eds). *The strategic and security concept for the countries of southest europe*. International scientific conference, Skopje, 2023, roč. 8, č. 1, s. 303-304.

[128] Kastrati, B., Pavleski, A., Spasov, N. Cyber-security as an issue of the contemporary security agenda. In: Dujovski, N. (eds). *The strategic and security concept for the countries of southest europe*. International scientific conference, Skopje, 2023, roč. 8, č. 1, s. 303-304.

[129] Čl. 12 odst. 1 směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES.

incidentu musí kritický subjekt oznámit tento incident kompetentním orgánům členského státu do 24 hodin od jeho zjištění.[130]

Pro zhodnocení povinnosti oznámit bezpečnostní incident do 24 hodin je zapotřebí důkladně zvážit několik klíčových faktorů. Rychlé oznámení incidentů je zásadní, protože zajišťuje, že informace o potenciálních hrozbách jsou rychle sdíleny mezi organizacemi a úřady. To umožňuje efektivní koordinaci a rychlou reakci na kybernetické útoky, což přispívá k lepšímu monitorování situace a poskytuje úřadům přehled o aktuálních hrozbách a trendech. Navíc mohou úřady postiženým organizacím poskytovat podporu a zdroje, čímž se zkrátí doba obnovy a sníží celkové dopady incidentů.

Pro splnění této povinnosti musí organizace mít nastavené interní procesy pro detekci a oznámení incidentů. To zahrnuje monitorování systémů, identifikaci potenciálních hrozeb a jejich rychlé nahlášení odpovědným úřadům. Nicméně, samotné nastavení procesů nestačí. Je nezbytné, aby zaměstnanci byli řádně proškoleni na postupy spojené s detekcí a hlášením bezpečnostních incidentů. Bez dostatečného proškolení zaměstnanců by nebylo možné zajistit, že detekované hrozby budou správně a včas hlášeny, což by mohlo vést k opožděné reakci a zvýšeným škodám.

Úřady hrají klíčovou roli při poskytování podpory a koordinaci reakce, což zahrnuje i sdílení informací s dalšími relevantními subjekty, aby se minimalizoval dopad incidentu a zabránilo se jeho šíření.[131] Proto je důležité, aby zaměstnanci byli informováni nejen o základních typech bezpečnostních incidentů, ale také o správných postupech pro jejich detekci, hlášení a následnou komunikaci. Efektivní a dobře informovaný personál je klíčem k minimalizaci škod a rychlé obnově bezpečnosti v případě incidentu.

Avšak povinnost oznámit incidenty do 24 hodin je možná až přespříliš ambiciózní a může být obtížné ji vždy dodržet, zejména u komplexních útoků, kde identifikace a analýza hrozby může trvat déle.

---

[130] ČL. 15 směrnice Evropského parlamentu a Rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES.

[131] NÚKIB. Incident Reporting [online]. *nukib.gov.cz.* [cit. 14.06.2024]. https://nukib.gov.cz/en/cyber-security/government-cert/incident-reporting/

Organizace mohou mít různé schopnosti a zdroje pro detekci a reakci na incidenty, což může vést k nerovnoměrnému plnění této povinnosti. Rychlé oznámení incidentu nemusí vždy zahrnovat dostatečně podrobné informace pro efektivní reakci. Kvalita a úplnost oznámení jsou klíčové pro správné posouzení situace a koordinaci reakce. Nedostatek standardizovaných formátů pro oznámení incidentů může vést k nekonzistentním informacím, což může zpomalit reakci.

Zavedení systémů pro rychlou detekci a oznámení incidentů může být nákladné, zejména pro menší organizace.[132] To zahrnuje investice do technologií, školení personálu a vytvoření odpovídajících procesů. Organizace mohou také čelit výzvám při integraci nových požadavků do stávajících bezpečnostních systémů a procesů.

Celkově lze konstatovat, že povinnost oznámit incidenty do 24 hodin je přínosná pro zajištění rychlé a efektivní reakce na kybernetické hrozby. Nicméně, její reálná implementace v praxi bude záviset na schopnosti organizací překonat výzvy spojené s rychlou detekcí, oznámením a koordinací reakcí na incidenty. Úspěšná realizace této povinnosti bude vyžadovat podporu a spolupráci mezi organizacemi a úřady, včetně poskytování potřebných zdrojů, školení zaměstnanců a technické pomoci menším organizacím.

Směrnice CER dále stanovuje, že každý členský stát musí vypracovat strategii obsahující strategické cíle, priority a rámec řízení, stejně jako opatření nezbytná k zvýšení celkové odolnosti. Členské státy mají také povinnost poskytovat kritickým subjektům podporu, včetně metodických materiálů, asistence při implementaci strategie a podpora testování odolnosti.[133] K dosažení cílů směrnice je důležitá spolupráce mezi členskými státy, zejména pokud je kritický subjekt propojen mezi dvěma nebo více členskými státy, má propojenou korporátní strukturu nebo poskytuje základní služby v jiném členském státu.

---

[132] Sordyl, J. Meeting the Challenges of a Changing Threat Landscape with the CER Directive [online]. *insights.pecb.com*. [cit. 22.05.2024]. https://insights.pecb.com/meeting-the-challenges-of-a-changing-threat-landscape-with-the-cer-directive/

[133] Fernandez, J. M. Navigating the EU Critical Entities Resilience Directive [online]. *deloitte.com*. [cit. 12.06.2024]. https://www.deloitte.com/lk/en/services/risk-advisory/perspectives/navigating-the-eu-critical-entities-resilience-directive.html

Implementace směrnice CER vyvolává zvýšenou pozornost kritických subjektů a organizací na ochranu svých systémů a infrastruktury před kybernetickými hrozbami. Některé kritické subjekty budou nuceny investovat do bezpečnostních opatření, jako jsou aktualizace softwaru, školení zaměstnanců a nasazení moderních bezpečnostních technologií, což pro ně může znamenat zvýšenou finanční zátěž. Tato opatření jsou nezbytná pro posílení kybernetické odolnosti a minimalizaci rizik spojených s kybernetickými útoky. Ovšem takové investice budou záležet na organizaci od organizace, jelikož některé organizace měly dostatečná bezpečnostní opatření již před směrnicí CER. K zjištění stavu bezpečnosti v organizaci slouží i povinnost pravidelně provádět posouzení rizik stanovená směrnicí CER.[134] Posouzení rizik klade důraz na monitorování a hodnocení možných bezpečnostních hrozeb a zranitelností. Organizace musí identifikovat potenciální hrozby a přijmout opatření k jejich omezení nebo eliminaci, čímž se posiluje kybernetická strategie organizace.

Směrnice CER poskytuje harmonizovaná minimální pravidla, která zajišťují poskytování základních služeb na vnitřním trhu, zvyšují odolnost kritických entit a zlepšují přeshraniční spolupráci mezi kompetentními orgány.[135] Směrnice CER také podporuje lepší spolupráci mezi kritickými subjekty a členskými státy v oblasti kybernetické bezpečnosti. Tato spolupráce zahrnuje výměnu informací o bezpečnostních hrozbách, sdílení osvědčených postupů a společné cvičení a testování odolnosti.[136] Posílení spolupráce je klíčové pro efektivní reakci na kybernetické hrozby a zajištění celkové kybernetické odolnosti.

Mezi hlavní problémy při implementaci směrnice patří absence jasného návodu, jak implementovat všechny požadavky směrnice, což může vést k rozdílným přístupům mezi členskými státy a komplikacím při

[134] Nonnemann, F. Před mikrofonem: Nový zákon o kritické infrastruktuře se blíží! [online]. *gdpr.cz.* [cit. 05.06.2024]. https://www.gdpr.cz/pred-mikrofonem-novy-zakon-o-kriticke-infrastrukture-se-blizi

[135] Mikac, R. Protection of the EU's Critical Infrastructures: Results and Challenges. *Applied Cybersecurity & Internet Governance*. 2023, roč. 2, č. 1, s. 13.

[136] Fernandez, J. M. Navigating the EU Critical Entities Resilience Directive [online]. *deloitte.com.* [cit. 12.06.2024]. https://www.deloitte.com/lk/en/services/risk-advisory/perspectives/navigating-the-eu-critical-entities-resilience-directive.html

koordinaci na unijní úrovni.[137] Bylo by vhodné, nejen v případě směrnice CER, stanovit jasné podmínky a postupy pro transpozici a implementaci směrnic.

4.3 Cyber Resilience Act

Tato podkapitola se zabývá nařízením CRA, které je klíčovou legislativou Evropské unie zaměřenou na regulaci kybernetické bezpečnosti digitálních produktů a služeb. Tato legislativa se vztahuje na všechny produkty a služby s digitálními prvky po celou dobu jejich životního cyklu s cílem vytvořit jednotný rámec pro dodržování kybernetických bezpečnostních norem v EU. Nařízení CRA má zásadní vliv na kritickou infrastrukturu, neboť stanoví přísné bezpečnostní standardy pro produkty s digitálními prvky, což zvyšuje odolnost kybernetické bezpečnosti této infrastruktury. Dále může nařízení CRA významně ovlivnit schopnost předcházet bezpečnostním incidentům a efektivně na ně reagovat díky zavedení koordinovaného mechanismu pro řízení kybernetických rizik a incidentů.

Nařízení CRA má několik klíčových cílů. Patří mezi ně posílení digitální důvěry, podpora proaktivního řízení kybernetických rizik, zajištění přísné ochrany dat a zavedení koordinovaného mechanismu pro řízení kybernetických incidentů.[138] Toto nařízení se týká různorodých subjektů, včetně provozovatelů základních služeb, poskytovatelů digitálních služeb, v některých bodech i veřejné správy. Platí také pro společnosti, které vyvíjejí nebo prodávají ICT produkty, služby nebo procesy v rámci EU.

Implementace nařízení CRA v praxi přináší mnoho výzev, které zahrnují technické, organizační a právní aspekty. Jedním z hlavních problémů je sladění nařízení CRA s dalšími nařízeními, jako je směrnice NIS 2. Integrace nařízení CRA a směrnice NIS 2 posiluje kybernetickou bezpečnost v EU tím, že se zaměřuje na různé aspekty ochrany. Směrnice

[137] Pursiainen, C., Kytömaa, E. From European critical infrastructure protection to the resilience of European critical entities: what does it mean? *Sustainable and Resilient Infrastructure*. 2023, č. 8, s. 90.

[138] Kiteworks. Introduction to the EU's Proposed Cyber Resilience Act [online]. *kiteworks.com.* [cit. 15.06.2024]. https://www.kiteworks.com/risk-compliance-glossary/eu-cyber-resiliency-act/

NIS 2 se soustředí na zabezpečení organizací v kritické infrastruktuře, vyžaduje od nich ochranu sítí, systémů a dodavatelských řetězců, zatímco nařízení CRA stanovuje bezpečnostní požadavky pro digitální produkty na trhu, včetně chytrých spotřebičů a softwaru. Nařízení CRA může podpořit směrnici NIS 2 tím, že usnadní subjektům, podléhajícím směrnici NIS 2, plnění povinností v oblasti kybernetické bezpečnosti a zároveň přinutí výrobce dodávat bezpečnější produkty splňující vysoké standardy.[139] Tento způsob může vést k tomu, že obě regulace společně zvýší odolnost jak samotných organizací, tak i produktů, které používají, což by vedlo k celkově vyšší úrovni kybernetické bezpečnosti v celé EU. Podniky musí navíc sladit požadavky nařízení CRA s existujícími bezpečnostními opatřeními a zajistit, že všechny produkty s digitálními prvky splňují nové standardy kybernetické bezpečnosti.[140]

Nařízení CRA v čl. 10 zavádí nové povinnosti pro výrobce. Výrobci při uvedení produktu s digitálním prvkem na trh zajistí jeho návrh, vývoj a výrobu v souladu se základními požadavky na kybernetickou bezpečnost. Provedou posouzení kybernetických rizik, které začlení do technické dokumentace a zajistí bezpečnost při použití součástí od třetích stran. Dokumentují relevantní aspekty kybernetické bezpečnosti, systematicky aktualizují posouzení rizik a řeší zranitelnosti po dobu životnosti produktu. Nařízení také rozlišuje mezi různými typy produktů. První, výchozí kategorie, zahrnuje nekritická zařízení, jako jsou chytré reproduktory, software pro zpracování textu, pevné disky, a umožňuje výrobcům samohodnocení bez potřeby třetí strany (tvoří ji cca 90 % IoT

[139] Eckhardt, P., Kotovskaia, A. The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive. *International Cybersecurity Law Review*. 2023, roč. 4, s. 155.

[140] Simola, J., et al. Impact of Cyber Security Operations on Hardware Requirements for Stable and Workable Industrial Environments. *International Conference on Cyber Warfare and Security*. 2024, roč. 19, č. 1, s. 350–351.

zařízení).[141] [142] Druhou kategorii tvoří důležité produkty, které jsou rozděleny na třídy I a II podle úrovně kritičnosti a vyžadují přísnější posouzení shody (nezávislý audit), jedná se o správce hesel, VPN, firewally a operační systémy.[143] Do třetí kategorie patří kritické produkty, které mají významné kyberbezpečnostní funkce, a vyžadují nezávislý audit.[144] [145]

Tento akt vyvolal debatu, zejména mezi open source projekty, které se obávají, že by mohl zkomplikovat vývoj softwaru s otevřeným zdrojovým kódem.[146] I když open source projekty nejsou přímo zahrnuty do působnosti aktu, některé jsou finančně podporovány nebo účtují poplatky za servisní služby.[147] Splnění povinností nařízení CRA může být pro vývojáře open source softwaru obtížné, protože nezohledňuje skutečnost, že tito vývojáři často neznají všechny uživatele svého softwaru,

[141] Nabto. Understanding the EU Cyber Resilience Act and What It Means for You [online]. *nabto.com.* [cit. 20.06.2024]. https://www.nabto.com/eu-cyber-resilience-act/

[142] Eckhardt, P., Kotovskaia, A. The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive. *International Cybersecurity Law Review*. 2023, roč. 4, s. 157.

[143] Eckhardt, P., Kotovskaia, A. The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive. *International Cybersecurity Law Review*. 2023, roč. 4, s. 157–158.

[144] Nabto. Understanding the EU Cyber Resilience Act and What It Means for You [online]. *nabto.com*. [cit. 20.06.2024]. https://www.nabto.com/eu-cyber-resilience-act/

[145] Eckhardt, P., Kotovskaia, A. The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive. *International Cybersecurity Law Review*. 2023, roč. 4, s. 158.

[146] Amler, P., Lupač, T. Evropa brání svou digitální budoucnost: Akt o kybernetické odolnosti [online]. *havelpartners.blog.* [cit. 14.05.2024]. https://www.havelpartners.blog/evropa-brani-svou-digitalni-budoucnost-akt-o-kyberneticke-odolnosti

[147] Ramaswami, A., Boehm, M. Understanding the Cyber Resilience Act: What Everyone involved in Open Source Development Should Know [online]. *linuxfoundation.org.* [cit. 20.06.2024]. https://www.linuxfoundation.org/blog/understanding-the-cyber-resilience-act

což činí povinnosti jako opravy zranitelností a poskytování bezpečnostních aktualizací nepraktickými.[148] To by mohlo vést k omezení počtu dostupných open source projektů, což by mohlo negativně ovlivnit inovace[149] a dostupnost bezpečnostních řešení pro kritickou infrastrukturu.

Organizace jsou povinny splnit určité kybernetické normy, pravidelně provádět posouzení rizik a včas hlásit významné kybernetické incidenty.[150] Nedodržení může mít pro organizace vážné důsledky, včetně značných peněžních pokut a reputační škody[151]. Nedodržení základních bezpečnostních požadavků může vést k pokutám až do výše 15 milionů EUR nebo 2,5 % celosvětového ročního obratu podniku.[152]

V souvislosti s nařízením CRA je také zapotřebí zmínit pojmy security by design a security by default. Security by Design znamená, že produkty jsou navrženy s ohledem na bezpečnost od samého počátku jejich

[148] Ramaswami, A., Boehm, M. Understanding the Cyber Resilience Act: What Everyone involved in Open Source Development Should Know [online]. *linuxfoundation.org.* [cit. 20.06.2024]. https://www.linuxfoundation.org/blog/understanding-the-cyber-resilience-act

[149] Dionysopoulos, C., et al. Open Letter on the Significance of Free and Open Source Software in the EU's Proposed Cyber Resilience Act [online]. *typo3.org.* [cit. 15.05.2024]. https://typo3.org/fileadmin/t3o_common_storage/documents/press_releases/2023-07_Open_Letter_to_EU_Legislators/Open_Letter_on_the_Significance_of_Free_and_Open_Source_Software_in_the_EU_s_Proposed_Cyber_Resilience_Act.pdf

[150] Jara, A. J., Martinez, I. C., Sanchez, J. *CyberSecurity Resilience Act (CRA) in practice for IoT devices: Getting ready for the NIS2*. Conference: IEEE Smart Cities Futures Summit, Marrakech, Morocco, 2024, s. 2.

[151] Kiteworks. Introduction to the EU's Proposed Cyber Resilience Act [online]. *kiteworks.com.* [cit. 15.06.2024]. https://www.kiteworks.com/risk-compliance-glossary/eu-cyber-resiliency-act/

[152] Čl. 55 odst. 3 návrh Nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020.

vývoje.[153] Tento přístup zahrnuje identifikaci a zmírnění bezpečnostních rizik v každé fázi vývojového procesu, což zahrnuje používání bezpečnostních rámců, kontrolu kódu a implementaci bezpečnostních funkcí ještě před uvedením produktu na trh.[154] Hlavní myšlenkou je zabránit vzniku zranitelností, než aby byly řešeny až poté, co jsou objeveny v produkci.[155] Security by Default znamená, že produkty jsou dodávány s výchozími nastaveními, která maximalizují bezpečnost bez nutnosti dalších konfigurací od uživatele.[156] To zahrnuje například eliminaci výchozích hesel, implementaci vícefaktorové autentizace pro privilegované uživatele, podporu jednotného přihlašování a poskytování kvalitních auditních logů.[157] Nařízení CRA klade důraz na to, aby výrobci začlenili bezpečnostní opatření do celého životního cyklu produktu, což přímo souvisí s principy Security by Design a Security by Default.[158] Implementace principů Security by Design a Security by Default v rámci nařízení CRA má zásadní dopad na kritickou infrastrukturu. Začleněním bezpečnostních opatření již od počátku vývoje produktů se významně zvyšuje odolnost systémů vůči kybernetickým útokům. Tento přístup znamená, že produkty jsou navrhovány tak, aby minimalizovaly bezpečnostní rizika ještě před tím, než se dostanou k uživatelům, což vede ke snížení počtu zranitelností, které by jinak mohly být zneužity. Nařízení CRA také stanovuje povinnosti ohledně informování uživatelů a orgánů v případě zjištění aktivně zneužívaných zranitelností majících dopad na

[153] Young, T. Security by Design and by Decree [online]. *securitycompass.com.* [cit. 19.06.2024]. https://www.securitycompass.com/blog/security-by-design-and-by-decree/

[154] Cybersecurity and Infrastructure Security Agency. *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-byDesign and -Default*. CISA, 2023, s. 8-9.

[155] Cybersecurity and Infrastructure Security Agency. *Shifting the balance of cybersecurity risk: Principles and approaches for secure by design software*. CISA, 2023, s. 8.

[156] National Cyber Security Centre. Secure by Default [online]. *ncsc.gov.uk.* [cit. 15.05.2024]. https://www.ncsc.gov.uk/information/secure-default

[157] Cybersecurity and Infrastructure Security Agency. *Shifting the balance of cybersecurity risk: Principles and approaches for secure by design software*. CISA, 2023, s. 15.

[158] Cybersecurity and Infrastructure Security Agency. *Shifting the balance of cybersecurity risk: Principles and approaches for secure by design software*. CISA, 2023, s. 4.

bezpečnost produktu. To znamená, že při vzniku bezpečnostního incidentu mají organizace lepší nástroje a informace pro rychlé a účinné řešení situace, což minimalizuje dopady na kritickou infrastrukturu a zajišťuje kontinuitu poskytování klíčových služeb.

Dodržování nařízení CRA může vést k lepšímu postavení v oblasti kybernetické bezpečnosti a důvěře trhu. Je důležité se nejen připravit na dodržování nařízení CRA, ale také sledovat aktualizace a dodatky k nařízení CRA, vzhledem k neustále se vyvíjející povaze kybernetických hrozeb a technologií.

Nařízení CRA poskytuje jednotný rámec pro kybernetickou bezpečnost napříč celou EU, což usnadňuje podnikům dodržování předpisů a zvyšuje právní jistotu. Nařízení stanoví jasné požadavky na bezpečnost, které musí nové produkty splňovat od počátku svého vývoje. To by mělo vést k vyšší úrovni bezpečnosti produktů, což je výhodné jak pro podniky, tak pro spotřebitele.

Nicméně, implementace nařízení CRA má také své nevýhody. Může být pro mnoho podniků nákladná, zejména pro malé a střední podniky, které mohou mít omezené zdroje pro splnění nových požadavků.[159] Pro mnoho podniky může být obtížné přizpůsobit své systémy a procesy, aby splnily stanovené bezpečnostní standardy, což může zahrnovat náklady na školení zaměstnanců, zavedení nových technologií a úpravy produktového vývoje. Navíc komplexnost požadavků může být pro některé podniky obtížná, což může vést k administrativní zátěži.

4.4 Směrnice NIS 2

Tato podkapitola se zaměřuje na směrnici NIS 2, která byla přijata na úrovni Evropské unie, a její implementaci v České republice prostřednictvím nového návrhu zákona o kybernetické bezpečnosti. Směrnice NIS 2 je významným legislativním krokem, jehož cílem je posílit ochranu kritické infrastruktury a zvýšit odolnost proti kybernetickým hrozbám napříč celou Evropskou unií. Byla zavedena v reakci na nejednotnost a nedostatečný účinek předchozí směrnice NIS, čímž se usiluje o sjednocení

[159] European Cyber Security Organisation. *Position paper: Cyber Resilience Act*. ECSO, 2022, s. 2.

přístupů k ochraně kritické infrastruktury. Směrnice NIS 2 a nový zákon mají za cíl sjednotit přístupy k ochraně kritické infrastruktury, zlepšit prevenci a reakci na bezpečnostní incidenty, a tím zvýšit celkovou kybernetickou odolnost.

V lednu 2023 vstoupila v platnost směrnice NIS 2, která by měla docílit posílení ochrany kritické infrastruktury pro celou EU. Směrnice NIS 2 klade důraz na sjednocení pravidel pro všechny členské státy EU, navíc je ochrana rozšířena i na další sektory (celkem 11 sektorů), jako je finanční sektor, zásobování vodou a potravinami, či zdravotnictví, předchozí směrnice se zabývala jen dopravou a energetikou. Jednotlivé členské státy mají 21 měsíců na přijetí směrnice NIS 2 do národního právního rámce. Povinností členských států je určit kritické subjekty určující základní služby, přijetí národní strategie na zvýšení odolnosti kritické infrastruktury a provádění pravidelných analýz rizik. Směrnice NIS 2 je rozšířením předchozí směrnice NIS, s cílem odstranit nedostatky původního dokumentu. Jedním z hlavních problémů implementace směrnice NIS 2 v praxi je nedostatečná harmonizace mezi členskými státy, což může vést k různým úrovním ochrany a různým postupům při řešení incidentů.[160] Navíc se objevují obavy z vysokých nákladů na implementaci, zejména pro menší podniky, které mohou mít omezené zdroje na splnění nových požadavků.[161]

NIS 2 má za cíl zvýšit bezpečnost síťových a informačních systémů v EU tím, že ukládá provozovatelům kritické infrastruktury a základních služeb povinnost zavést odpovídající bezpečnostní opatření a hlásit incidenty.[162] [163] Výhodou nové směrnice je její širší záběr, který zahrnuje

[160] Božić, V. *Strengthening Cybersecurity Resilience: Collaborative Efforts in the NIS2 Framework*. 2024, s. 8-9.

[161] Božić, V. *Strengthening Cybersecurity Resilience: Collaborative Efforts in the NIS2 Framework*. 2024, s. 8-9.

[162] Uniqkey. What Is The NIS2 Directive? [online]. *nis2directive.eu.* [cit. 12. 02.2024]. https://nis2directive.eu/what-is-nis2/

[163] Schmitz-Berndt, S. Refining the Mandatory Cybersecurity Incident Reporting Under the NIS Directive 2.0: Event Types and Reporting Processes. In: Onwubiko, C., et al. (eds). *Proceedings of the International Conference on Cybersecurity, Situational*

více sektorů a umožňuje lepší koordinaci a spolupráci na úrovni EU.[164] Na druhou stranu, nevýhodou může být zvýšená administrativní zátěž pro organizace a potřeba vysokých investic do kybernetické bezpečnosti.[165] Rozšiřuje bezpečnostní požadavky na celou EU a různé organizace a odvětví. Cílem je zvýšit bezpečnost dodavatelského řetězce, zjednodušit ohlašovací povinnosti a prosadit přísnější opatření a sankce v celé Evropě.[166] [167]

Směrnice zavádí rámec pro posílení kybernetické bezpečnosti v EU, včetně národních strategií kybernetické bezpečnosti, určení příslušných orgánů a jednotných kontaktních míst, a zřízení týmů pro řešení počítačových bezpečnostních incidentů (CSIRT). Stanovuje také spolupráci na úrovni EU a mezinárodní úrovni prostřednictvím skupiny pro spolupráci, sítě národních CSIRT a EU-CyCLONe.

Dále se směrnice NIS 2 zabývá opatřeními pro řízení rizik a oznamovacími povinnostmi souvisejícími s kybernetickou bezpečností. Subjekty podléhající směrnici musí přijmout vhodná opatření k řízení rizik a hlásit významné incidenty do 24 hodin[168]. To zahrnuje i incidenty, které mají potenciál způsobit značné škody, což umožňuje získat úplný obraz

Awareness and Social Media. Springer Proceedings in Complexity, Singapore, 2023, s. 344-345.

[164] Božić, V. *Strengthening Cybersecurity Resilience: Collaborative Efforts in the NIS2 Framework*. 2024, s. 8.

[165] Božić, V. *Strengthening Cybersecurity Resilience: Collaborative Efforts in the NIS2 Framework*. 2024, s. 8–9.

[166] Uniqkey. What Is The NIS2 Directive? [online]. *nis2directive.eu.* [cit. 12. 02.2024]. https://nis2directive.eu/what-is-nis2/

[167] Schmitz-Berndt, S. Refining the Mandatory Cybersecurity Incident Reporting Under the NIS Directive 2.0: Event Types and Reporting Processes. In: Onwubiko, C., et al. (eds). *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media.* Springer Proceedings in Complexity, Singapore, 2023, s. 349.

[168] Rozdíl od směrnice NIS, kde bylo stanoveno pouze hlásit incidenty bez zbytečného odkladu.

o hrozbách a lépe chránit veřejnost a podniky.[169] Směrnice také upravuje využití evropských systémů certifikace kybernetické bezpečnosti a podporuje standardizované přístupy ke kybernetické bezpečnosti.[170]

Jedním z významných prvků směrnice je požadavek na samoidentifikaci organizací, které podléhají novým předpisům.[171] To znamená, že organizace budou muset samy zhodnotit svou úroveň kybernetické bezpečnosti a přijmout opatření k jejímu zlepšení. Pokud organizace poruší bezpečnostní předpisy, mohou být vystaveny tvrdým sankcím, včetně vysokých finančních pokut a pozastavení povolení k provozování určitých služeb.

Organizace budou muset zajistit, aby i jejich dodavatelé splňovali požadavky na kybernetickou bezpečnost.[172] To znamená, že organizace budou muset prověřovat bezpečnostní opatření svých dodavatelů a případně požadovat audit jejich bezpečnostních postupů. S narůstajícími požadavky na kybernetickou bezpečnost se očekává zvýšená poptávka po odbornících a specialistech v oblasti kybernetické bezpečnosti.[173] Organizace budou potřebovat kvalifikované pracovníky, kteří budou schopni implementovat a spravovat bezpečnostní opatření.

[169] Schmitz-Berndt, S. Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive. *Journal of Cybersecurity*. 2023, roč. 9, č. 1, s. 9.

[170] Sievers, T. Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations. *International Cybersecurity Law Review*. 2021, roč. 2, s. 229.

[171] Růžková, P. NIS2 a novinky pro české firmy: Co se mění v oblasti kybernetické bezpečnosti [online]. *master.cz.* [cit. 16.05.2024]. https://www.master.cz/blog/nis2-a-novinky-pro-ceske-firmy-co-se-meni-v-oblasti-kyberneticke-bezpecnosti/

[172] Růžková, P. NIS2 a novinky pro české firmy: Co se mění v oblasti kybernetické bezpečnosti [online]. *master.cz.* [cit. 16.05.2024]. https://www.master.cz/blog/nis2-a-novinky-pro-ceske-firmy-co-se-meni-v-oblasti-kyberneticke-bezpecnosti/

[173] ibidem

Směrnice NIS 2 má významné dopady na celou organizaci, a za implementaci je zodpovědný management.[174] [175] Organizace musí navrhnout a zavést opatření k posílení kybernetické bezpečnosti, nejenom na úrovni ochrany a šifrování dat. Zavedení bezpečnostních procesů, organizace školení a korekce bezpečnosti napříč dodavatelským řetězcem jsou povinnostmi, za které ponese odpovědnost vedení organizace.[176] [177]

V ČR proběhne implementace směrnice NIS 2 pomocí rekodifikace zákona o kybernetické bezpečnosti a na to navázané vyhlášky. Přičemž prováděcí vyhlášky budou projednány samostatně. Návrh zákona o kybernetické bezpečnosti předložil NÚKIB i k veřejné diskuzi, kdy se veřejnost skrze podněty mohla podílet na doplňování návrhu zákona, který byl zveřejněn na internetových stránkách nis2.nukib.cz. Předseda Legislativní rady vlády v červnu doporučil vládě návrh zákona ke schválení.[178] Předpokládaná doba vstoupení zákona v účinnost je říjen 2024, což je i závěr transpoziční lhůty pro přijetí směrnice NIS 2.[179]

Nový návrh zákona o kybernetické bezpečnosti přináší výrazné změny v regulaci. Jednou z hlavních novinek je rozšíření povinností

[174] Šilarová, J. Jak se připravit na NIS2: Nový zákon o kybernetické bezpečnosti pro střední a velké podniky [online]. *alvao.com.* [cit. 18.05.2024]. https://www.alvao.com/cs/blog/jak-se-pripravit-na-nis2

[175] Sievers, T. Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations. *International Cybersecurity Law Review*. 2021, roč. 2, s. 228.

[176] Šilarová, J. Jak se připravit na NIS2: Nový zákon o kybernetické bezpečnosti pro střední a velké podniky [online]. *alvao.com.* [cit. 18.05.2024]. https://www.alvao.com/cs/blog/jak-se-pripravit-na-nis2

[177] Sievers, T. Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations. *International Cybersecurity Law Review*. 2021, roč. 2, s. 228.

[178] NÚKIB. Legislativní rada vlády doporučila návrh zákona [online]. *nukib.gov.cz.* [cit. 20.06.2024]. https://nukib.gov.cz/cs/infoservis/aktuality/2125-legislativni-rada-vlady-doporucila-navrh-zakona/

[179] NÚKIB. Návrh nového zákona o kybernetické bezpečnosti vstupuje do další fáze [online]. *nukib.gov.cz.* [cit. 20.06.2024]. https://nukib.gov.cz/cs/infoservis/aktuality/2125-legislativni-rada-vlady-doporucila-navrh-zakona/

týkajících se bezpečnosti dodavatelského řetězce. To znamená, že organizace budou muset aktivně sledovat bezpečnost svých dodavatelů a zajistit, aby dodavatelský řetězec byl zabezpečen dostatečně.[180] Navíc návrh obsahuje nová pravidla pro umístění dat, zejména pro organizace s vyššími povinnostmi, které musí zaručit, že data jsou uložena na území České republiky nebo Evropské unie.[181]

Další důležitou inovací je rozšíření povinnosti hlásit kybernetické incidenty nejen NÚKIBu, ale také uživatelům postižených služeb. Současně jsou navrhovány vyšší pokuty za porušení předpisů, což by mohlo motivovat organizace k lepší ochraně svých informačních systémů.

4.5 Směrnice CER a směrnice NIS 2 na praktickém případě

Hypotetická situaci, ve které by společnost „SqiMed“ spadala pod obě směrnice – CER i NIS 2. SqiMed je velká firma, která poskytuje kritické digitální infrastruktury pro zdravotnický sektor, což ji činí důležitým subjektem dle směrnice NIS 2 a zároveň kritickým subjektem dle směrnice CER.

SqiMed musí dodržovat řadu opatření vyplývajících z obou směrnic. Podle směrnice CER by společnost byla identifikována jako kritický subjekt, protože poskytuje služby nezbytné pro udržení důležitých společenských funkcí v oblasti zdravotnictví. Směrnice NIS 2 ji klasifikuje jako základní subjekt, protože její služby spadají pod kritickou digitální infrastrukturu.

Hodnocení rizik podle směrnice CER by zahrnovalo komplexní posouzení jak fyzických, tak kybernetických hrozeb, včetně přírodních katastrof, teroristických útoků, hybridních hrozeb a jiných fyzických incidentů. Naopak směrnice NIS 2 se zaměřuje konkrétně na kybernetická

[180] Šimsa, P., Michalcová, L., Ptáček, O. Směrnice NIS2 a nový Zákon o kybernetické bezpečnosti [online]. *pwc.com.* [cit. 03.06.2024]. https://www.pwc.com/cz/cs/temata/smernice-nis2.html

[181] Šimsa, P., Michalcová, L., Ptáček, O. Směrnice NIS2 a nový Zákon o kybernetické bezpečnosti [online]. *pwc.com.* [cit. 03.06.2024]. https://www.pwc.com/cz/cs/temata/smernice-nis2.html

rizika a vyžaduje implementaci specifických opatření pro řízení těchto rizik a zajištění bezpečnosti sítí a informačních systémů.

SqiMed by musela podle směrnice CER vypracovat a implementovat bezpečnostní plány pro zajištění fyzické bezpečnosti svých zařízení a provozů. Směrnice NIS 2 by pak vyžadovala zavedení opatření pro kybernetickou bezpečnost, včetně monitorování, detekce, reakce na incidenty a obnovy systémů po kybernetických útocích.

Spolupráce a sdílení informací by byla dalším klíčovým aspektem. Směrnice CER by vyžadovala zapojení společnosti do centralizované platformy pro sdílení informací s příslušnými orgány a dalšími kritickými subjekty, aby podporovala osvědčené postupy a výměnu zkušeností. Směrnice NIS 2 by zlepšila spolupráci mezi členskými státy prostřednictvím strukturovaného rámce zahrnujícího spolupracující skupiny a síť CSIRTs, zaměřenou na kybernetickou bezpečnost.

Regulační a implementační mechanismy se v těchto směrnicích také liší. Směrnice CER zahrnuje státem regulované odpovědnosti, kde členské státy identifikují kritické subjekty a zajišťují jejich soulad s národními předpisy, s podporou Evropské komise. Směrnice NIS 2 naopak zdůrazňuje koordinovaný regulační rámec v celé EU, aby se zmírnily rozdíly v kybernetických bezpečnostních opatřeních mezi členskými státy.

V hypotetické situaci, kdy by SqiMed čelila kybernetickému incidentu – například ransomware útoku[182], který by ochromil jejich sítě a zablokoval přístup ke kritickým datům zdravotnických zařízení – by společnost musela okamžitě aktivovat svůj incident response plán. Tento plán by zahrnoval izolaci napadených systémů, identifikaci rozsahu útoku, odstranění hrozby a obnovení dat ze záloh. Společnost by také musela informovat své klienty a partnery o incidentu a přijmout opatření k minimalizaci škod.

Podle směrnice NIS 2 by SqiMed musela nahlásit incident národnímu CSIRT a relevantním úřadům do 24 hodin od zjištění incidentu. Hlášení by mělo obsahovat podrobnosti o povaze útoku, jeho rozsahu, postižených systémech a přijatých opatřeních. Protože incident má významný dopad na poskytování kritických služeb, musela by společnost také informovat příslušné orgány odpovědné za fyzickou bezpečnost a odolnost

[182] To je typ škodlivého softwaru, který šifruje data oběti a požaduje výkupné za jejich dešifrování.

kritických subjektů dle směrnice CER. Toto hlášení by mělo obsahovat informace o tom, jak kybernetický incident ovlivnil fyzickou infrastrukturu a provozní kontinuitu.

SqiMed by musela úzce spolupracovat s CSIRT a dalšími národními a evropskými kybernetickými bezpečnostními orgány, poskytovat jim potřebné informace a podporu při vyšetřování incidentu. Současně by se musela zapojit do koordinace s orgány odpovědnými za fyzickou bezpečnost, aby zajistila, že jsou přijata všechna potřebná opatření k ochraně kritické infrastruktury před dalšími hrozbami nebo potenciálními útoky.

Po incidentu by SqiMed musela provést důkladnou analýzu a implementovat dodatečná bezpečnostní opatření, aby se zabránilo opakování podobných útoků. Společnost by také musela pravidelně aktualizovat své bezpečnostní plány a trénovat zaměstnance v oblasti kybernetické bezpečnosti. Podle směrnice CER by SqiMed musela aktualizovat své bezpečnostní plány a provést cvičení, která by simulovala podobné incidenty, aby se zlepšila připravenost na budoucí hrozby.

SqiMed by tedy musela dodržovat komplexní soubor požadavků podle obou směrnic – CER i NIS 2. To zahrnuje hodnocení rizik, implementaci bezpečnostních opatření, spolupráci a sdílení informací a pravidelné hlášení incidentů. V případě kybernetického incidentu by společnost musela okamžitě reagovat a hlásit incident příslušným úřadům podle obou směrnic, spolupracovat při vyšetřování a přijmout opatření k obnově a zlepšení své bezpečnostní infrastruktury. Tento integrovaný přístup by měl zajistit, že SqiMed zůstane odolná vůči fyzickým i kybernetickým hrozbám.

Komplexní požadavky obou směrnic mohou představovat značnou regulační zátěž pro veřejné orgány i soukromé subjekty. Zajištění souladu s opatřeními pro fyzickou i kybernetickou odolnost může napnout zdroje, zejména u menších subjektů. Řešení složitých propojení mezi fyzickými a kybernetickými systémy, zejména v kontextu hybridních hrozeb, vyžaduje koordinovaný přístup, který integruje cíle obou směrnic.[183] To může být v praxi náročné, protože to vyžaduje vysokou úroveň

[183] Pursiainen, Ch., Kytömaa, E. Sustainable and Resilient Infrastructure ISSN: (Print) From European critical infrastructure protection to the resilience of European critical entities: what does it mean? *Sustainable and Resilient Infrastructure.* 2022, roč. 8, č. 6, s. 93-94.

spolupráce a komunikace mezi různými regulačními orgány a zainteresovanými stranami.

Celkově lze říci, že směrnice CER a NIS 2 mají za cíl zvýšit odolnost a bezpečnost kritické infrastruktury a informačních systémů v EU. Jejich úspěšná implementace však vyžaduje pečlivou koordinaci k řešení překryvů, regulačních zátěží a vývojových hrozeb. Efektivní spolupráce mezi členskými státy, spolu s jasnými pokyny a dostatečnými zdroji, bude klíčová pro překonání těchto výzev a dosažení cílů těchto směrnic.

4.6 Cyber Solidarity Act

V této kapitole bude rozebráno Cyber Solidarity Act, jeho význam a dopady na kybernetickou bezpečnost Evropské unie. Cyber Solidarity Act usiluje o posílení odpovědnosti členských států za ochranu jejich kybernetických infrastruktur, zlepšení koordinace mezi nimi a umožnění rychlejší a efektivnější reakce na kybernetické útoky. Podle tohoto nařízení by měla být přijata opatření ke zvýšení schopnosti detekovat hrozby, zlepšení situačního povědomí a rozvoji reakčních schopností. To v praxi znamená vytvoření evropské kybernetické rezervy, investice do technologií pro kybernetickou obranu a zavedení mechanismů pro sdílení informací a společná cvičení. Tento přístup by měl vést k lepší ochraně kritických infrastruktur, zvýšení připravenosti a odolnosti vůči kybernetickým útokům a posílení kolektivní bezpečnosti v rámci EU.

Cyber Solidarity Act, schválené v roce 2022, představuje zásadní posun v přístupu ke kybernetické bezpečnosti, je zaměřený na zlepšení připravenosti, detekce a reakce Evropské unie na kybernetické hrozby a incidenty. Tento akt si klade za cíl posílit společné evropské schopnosti detekce, situačního povědomí a reakce, postupně vybudovat rezervu na úrovni EU pro kybernetickou bezpečnost s pomocí služeb od důvěryhodných soukromých poskytovatelů a podpořit testování kritických subjektů.[184]

[184] Two Birds. Cyber Solidarity Act [online]. *twobirds.com.* [cit. 15.05.2024]. https://www.twobirds.com/en/capabilities/practices/digital-rights-and-assets/european-digital-strategy-developments/cybersecurity/cybersecurity/cyber-solidarity-act

Cyber Solidarity Act vychází z poznatků o rostoucí složitosti a rozsahu kybernetických hrozeb, které čelí nejenom jednotlivé státy, ale celé regiony a kontinenty. Jeho hlavními cíli jsou posílení odpovědnosti členských států v oblasti kybernetické bezpečnosti, zlepšení koordinace mezi nimi v případě kybernetických incidentů a posílení schopnosti EU rychle reagovat na nové a rozmanité hrozby.[185]

Konkrétně se Cyber Solidarity Act zaměřuje na prevenci kybernetických útoků a zlepšení schopnosti detekce a reakce v případě, že k útoku dojde. Zavádí opatření na posílení ochrany kritické infrastruktury, podporuje investice do technologií pro kybernetickou obranu a navrhuje mechanismy pro sdílení informací a společné cvičení členských států. Jedním z hlavních bodů je zřízení Evropského kybernetického štítu, který bude sestávat z národních a přeshraničních operačních center propojených napříč EU.[186] Tyto centra budou využívat moderní technologie, jako je umělá inteligence a analýza dat, k detekci a sdílení varování o kybernetických hrozbách.[187] Mechanismus pro mimořádné události v kybernetické oblasti bude podporovat přípravné akce, vzájemnou finanční pomoc postiženým subjektům a vytvoření „kybernetické rezervy", která bude sestávat z incidentních reakčních služeb ze soukromého sektoru.[188] Mechanismem přezkumu kybernetických bezpečnostních incidentů bude provedeno zhodnocení účinnosti kybernetického mechanismu s cílem zajistit jeho neustálé zlepšování.[189]

V praxi to znamená, že členské státy musí přijmout větší odpovědnost za ochranu svých kybernetických infrastruktur a aktivně spolupracovat s ostatními státy na úrovni EU. Tato spolupráce je klíčová pro

[185] European Parliamentary Research Service. *Cyber solidarity act.* European Union, 2024, s. 4.

[186] European Commission. The EU Cyber Solidarity Act [online]. *digital-strategy.ec.europa.eu.* [cit. 24.05.2024]. https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity

[187] ibidem

[188] Coker, J. EU Agrees 'Cyber Solidarity Act' to Bolster Incident Response and Recovery [online]. *infosecurity-magazine.com.* [cit. 29.04.2024]. https://www.infosecurity-magazine.com/news/eu-cyber-solidarity-incident/

[189] ibidem

rychlé sdílení informací o kybernetických hrozbách a koordinovanou reakci v případě útoku.

Dopady implementace Cyber Solidarity Act jsou značné. Zlepšuje se ochrana kybernetických infrastruktur, zvyšuje se schopnost rychlé reakce na kybernetické incidenty a posiluje se pocit kolektivní bezpečnosti v rámci EU.[190]

Nicméně, i přes tyto ambiciózní cíle, Cyber Solidarity Act může čelit několika výzvám. Jednou z hlavních výzev je koordinace různých národních zájmů v oblasti kybernetické bezpečnosti. Některé členské státy mohou mít odlišné priority a politické agendy, což může zpomalit proces rozhodování a implementace opatření.

Přesto však Cyber Solidarity Act přináší značné bonusy v podobě posílené kybernetické bezpečnosti a ochrany infrastruktur EU. Investice do spolupráce a koordinace v této oblasti mohou vést k efektivnějšímu a odolnějšímu kybernetickému prostředí v celé Unii.[191]

4.7 Dílčí závěr

Evropská unie podnikla několik klíčových legislativních kroků v oblasti kybernetické bezpečnosti, které mají za cíl posílit ochranu digitálního prostředí, infrastruktury a služeb v celé Unii. Tyto kroky zahrnují nařízení a směrnice, které zajišťují komplexní přístup k řízení kybernetických rizik a zvyšování odolnosti proti kybernetickým hrozbám.

Cybersecurity Act představuje významný posun v přístupu k řízení kybernetické bezpečnosti v EU. Tento akt poskytuje stálý mandát agentuře ENISA, což jí umožňuje nejen koordinovat reakce na kybernetické incidenty, ale také aktivně přispívat k tvorbě politik a standardů kybernetické bezpečnosti. ENISA se stává klíčovým hráčem při vytváření rámců pro certifikaci kybernetické bezpečnosti ICT produktů, služeb a procesů. Tento rámec je navržen tak, aby poskytoval tři úrovně záruky (základní, významná, vysoká), což umožňuje flexibilitu a přizpůsobení

[190] Headmind Partners. The Cyber Solidarity Act [online]. *headmind.com.* [cit. 16.05.2024]. https://www.headmind.com/en/cyber-solidarity-act/

[191] European Parliamentary Research Service. *Cyber solidarity act.* European Union, 2024, s. 7.

podle konkrétních potřeb různých sektorů a typů produktů. Certifikace, ačkoli zpočátku dobrovolná, může být povinná v budoucnu na základě hodnocení Evropské komise, což by mohlo výrazně ovlivnit trh a přístup organizací ke kybernetické bezpečnosti.

Směrnice CER představuje další klíčový krok v ochraně kritické infrastruktury v EU. Tato směrnice rozšiřuje povinnosti kritických subjektů, které nyní musí provádět pravidelná posouzení rizik a implementovat adekvátní opatření k zajištění své odolnosti. Významný je požadavek na oznámení bezpečnostních incidentů do 24 hodin, což zvyšuje transparentnost a umožňuje rychlejší reakci na potenciální hrozby. Směrnice rovněž podporuje spolupráci mezi členskými státy a kritickými subjekty, výměnu informací o hrozbách a společné testování odolnosti, čímž se zvyšuje celková úroveň bezpečnosti a připravenosti na případné incidenty.

Nařízení CRA klade důraz na kybernetickou bezpečnost digitálních produktů a služeb po celou dobu jejich životního cyklu. Výrobci jsou nyní povinni uvádět na trh pouze produkty splňující základní bezpečnostní standardy a pravidelně provádět hodnocení kybernetických rizik. Tento akt rozlišuje mezi nekritickými zařízeními a kritickými produkty, pro které je vyžadován nezávislý audit, což zajišťuje vyšší úroveň bezpečnosti pro klíčové technologie. Nedodržení bezpečnostních požadavků může vést k vysokým pokutám, což motivuje výrobce k dodržování stanovených standardů. CRA také klade důraz na proaktivní řízení kybernetických rizik, čímž posiluje důvěru spotřebitelů v digitální produkty a služby a podporuje inovace v oblasti kybernetické bezpečnosti. Principy security by design a security by default zajišťují, že produkty jsou navrženy s ohledem na bezpečnost od počátku jejich vývoje. Významné dopady na open source projekty a nutnost sladění nařízení CRA s dalšími nařízeními, jako je směrnice NIS 2, vyvolávají potřebu dalších úprav a harmonizace.

Směrnice NIS 2 rozšiřuje a posiluje ochranu kritické infrastruktury v EU. Tato směrnice zahrnuje nové sektory, jako je finanční sektor, zdravotnictví a zásobování potravinami, což zajišťuje širší pokrytí a ochranu před kybernetickými hrozbami. Směrnice NIS 2 sjednocuje pravidla pro všechny členské státy a vyžaduje, aby přijaly národní strategie na zvýšení odolnosti kritické infrastruktury. Organizace musí zavést odpovídající bezpečnostní opatření a hlásit incidenty, což podporuje

transparentnost a rychlou reakci na hrozby. Směrnice podporuje spolupráci na úrovni EU a mezinárodní úrovni a vyžaduje, aby organizace zajistily, že i jejich dodavatelé splňují požadavky na kybernetickou bezpečnost. Tato směrnice také ukládá organizacím povinnost provádět pravidelné analýzy rizik a zajišťuje tvrdé sankce za porušení bezpečnostních předpisů.

Fragmentace kybernetického prostoru v EU stále představuje výzvu, přestože Cybersecurity Act harmonizuje certifikační standardy. Je nutné zlepšit uznávání certifikátů mezi členskými státy a snížit administrativní zátěž spojenou s vícenásobnou certifikací. Současné certifikační schémata nedostatečně pokrývají specifické bezpečnostní požadavky IoT zařízení, a proto je nezbytné vytvořit nové certifikační schéma zaměřené výhradně na IoT. Povinnost oznámit incidenty do 24 hodin je ambiciózní a může být obtížné ji vždy dodržet, zejména u komplexních útoků. Standardizace formátů pro oznámení incidentů a posílení podpory pro organizace při detekci a hlášení incidentů je nezbytná. Nařízení CRA a směrnice NIS 2 by měly být lépe sladěny, aby se minimalizovala administrativní zátěž pro podniky a zajistila konzistentní úroveň kybernetické bezpečnosti napříč EU.

Harmonizace certifikačních standardů a rozšíření specifických schémat pro IoT zařízení zlepší celkovou kybernetickou bezpečnost. Poskytnutí finanční a technické podpory malým a středním podnikům, které mohou mít omezené zdroje na splnění nových bezpečnostních požadavků, je klíčové. Zavedení standardizovaných formátů pro oznámení incidentů a poskytování školení zaměstnancům v oblasti kybernetické bezpečnosti zajistí rychlejší a efektivnější reakci na incidenty.

Školení zaměstnanců je kritické pro zvýšení kybernetické odolnosti organizací. Zaměstnanci musí být pravidelně informováni o aktuálních hrozbách a nejnovějších metodách ochrany. Školení by mělo zahrnovat praktické cvičení zaměřená na detekci, hlášení a reakci na bezpečnostní incidenty. Je důležité, aby zaměstnanci byli schopni rychle a správně reagovat na kybernetické hrozby, což výrazně snižuje riziko úspěšného útoku. Organizace by měly také investovat do kontinuálního vzdělávání, aby udržely krok s rychle se vyvíjejícím prostředím kybernetických hrozeb.

Posílení spolupráce mezi členskými státy a kritickými subjekty je klíčové pro efektivní ochranu kritické infrastruktury. Centralizované

platformy pro sdílení informací a osvědčených postupů mohou významně přispět k lepší koordinaci a rychlejší reakci na incidenty. Výměna informací o aktuálních hrozbách a incidentech mezi členskými státy a kritickými subjekty umožňuje lepší přehled o kybernetické situaci v celé EU a podporuje efektivní a jednotnou reakci. Společné cvičení a testování odolnosti systémů posilují schopnost členských států a kritických subjektů reagovat na kybernetické incidenty a zvyšují celkovou odolnost kritické infrastruktury. Tento integrovaný přístup zajišťuje, že kritické systémy zůstanou chráněny a kontinuita poskytování základních služeb nebude narušena. Tímto komplexním přístupem lze dosáhnout lepší ochrany kritických systémů a zajistit kontinuitu poskytování základních služeb v Evropské unii.

Evropská unie prostřednictvím těchto legislativních aktů výrazně posílila rámec kybernetické bezpečnosti, který zahrnuje certifikaci produktů a služeb, ochranu kritické infrastruktury, regulaci digitálních produktů a sjednocení pravidel kybernetické bezpečnosti napříč členskými státy. Tyto kroky podporují inovace, posilují důvěru spotřebitelů a zajišťují vyšší úroveň ochrany proti kybernetickým hrozbám, čímž přispívají k rozvoji digitální ekonomiky a odolnější společnosti v EU.

5 Případová studie

Tato kapitola se zaměřuje na analýzu kybernetických útoků prostřednictvím jedné vícepřípadové explanatorní studie. Tato kapitola poskytne komplexní pohled na to, jak se různé organizace a země vypořádaly s kybernetickými hrozbami, a nabídne poznatky pro zlepšení kybernetické bezpečnosti a implementaci legislativních opatření v praxi. Cílem kapitoly je podrobně prozkoumat, jak různé sektory kritické infrastruktury reagují na kybernetické útoky a jaké strategie a opatření používají k minimalizaci rizik a následků těchto útoků. Konkrétně se kapitola zaměří na analýzu reakcí organizací, identifikaci zranitelností, porovnání geografických a odvětvových rozdílů, doporučení pro zlepšení kybernetické bezpečnosti a poučení z incidentů. Tato analýza zahrnuje krizové řízení, komunikační strategie, obnovení činnosti a dlouhodobá opatření k prevenci. Přičemž také klade důraz na specifika České republiky ve srovnání s Itálií či Německem. Případová studie analyzuje čtyři významné kybernetické útoky: útok na německou železniční společnost Deutsche Bahn, útok na nemocnici v Düsseldorfu v Německu, útok na italskou energetickou společnost Enel a kyberútok na Fakultní nemocnici v Brně v České republice.

Výběr těchto konkrétních případů nebyl náhodný. Každý z nich reprezentuje různá odvětví kritické infrastruktury – dopravu, zdravotnictví a energetiku – a ukazuje různé aspekty kybernetické bezpečnosti a její zranitelnosti. Útok na Deutsche Bahn demonstruje dopad na dopravní sektor, a byl vybrán kvůli jeho významu pro německou dopravní infrastrukturu, i když jeho dopad na veřejnost nebyl rozsáhlý, ukazuje důsledky kybernetických hrozeb na klíčovou dopravní síť. Incident v nemocnici v Düsseldorfu odhaluje závažné důsledky kybernetických útoků na zdravotnictví, kde může být ohrožen nejen majetek, ale i lidské životy. Útok na Enel byl vybrán kvůli jeho rozsáhlým operacím a významu pro evropský energetický sektor, čímž ukazuje zranitelnost energetické infrastruktury vůči kybernetickým hrozbám a jejich dopad na kontinuitu dodávek energie. A konečně, útok na Fakultní nemocnici v Brně poskytuje specifický pohled na situaci v České republice a umožňuje srovnání s předchozími případy. Explanatorní typ případové studie byl zvolen, protože umožňuje hlubší analýzu a porozumění příčinným souvislostem, které vedly k těmto incidentům. Tento přístup pomáhá identifikovat

slabá místa a faktory, které přispěly k úspěšnosti kybernetických útoků, a poskytuje přehled o reakcích a opatřeních přijatých postiženými organizacemi.

Pro sběr dat byly využity především elektronické zdroje, včetně odborných článků, zpráv o kybernetických útocích, oficiálních dokumentů a dalších relevantních publikací. Vzhledem k povaze zkoumaných incidentů a omezeným možnostem přístupu k přímým účastníkům nebylo možné využít jiné metody sběru dat, jako jsou dotazníky nebo rozhovory. Tyto metody nebyly zvoleny ani pro případ útoku na Fakultní nemocnici v Brně. Důvodem je snaha o zachování konzistence a objektivity výzkumu.

5.1 Vícepřípadová studie

Kybernetické útoky na kritickou infrastrukturu představují stále rostoucí hrozbu, která vyžaduje kvalitní legislativní a technologická opatření. Tato vícepřípadová studie se zaměřuje na čtyři významné kybernetické incidenty v Evropě: útok na německou železniční infrastrukturu (Deutsche Bahn) v roce 2017, útok na německý zdravotnický systém (nemocnice v Düsseldorfu) v roce 2020, ransomware útok na italskou energetickou společnost Enel v roce 2020 a kybernetický útok na Fakultní nemocnici v Brně v roce 2020.

Cílem této studie je analyzovat vliv evropské legislativy pro zvládání kybernetických incidentů, konkrétně směrnice NIS, směrnice NIS 2, nařízení CRA a směrnice CER, a jejich ekvivalentů v jednotlivých zemích, na úspěšnost těchto útoků. Klíčovou otázkou je, zda jsou úspěšné kybernetické útoky zaviněny nedostatečnou úpravou a implementací legislativy nebo lidskými chybami.

Každý případ je analyzován s ohledem na právní úpravu a její implementaci v dané zemi, důvody a průběh útoku, identifikované nedostatky a úspěchy v reakci na útok. V případě útoku na Fakultní nemocnici v Brně je navíc poskytován přehled o specifické situaci v České republice a srovnání s ostatními státy EU. V závěru je prozkoumáno, zda lze mezi Českou republikou a ostatními státy EU pozorovat rozdíly při reakci na kybernetické útoky.

Tato studie poskytuje komplexní pohled na různé aspekty kybernetické bezpečnosti a zranitelnosti v kritické infrastruktuře a nabízí

poznatky pro zlepšení kybernetické bezpečnosti a implementaci legislativních opatření v praxi.

5.1.1 Případ 1: Útok na německou železniční infrastrukturu (2017 - Deutsche Bahn)

Deutsche Bahn AG (DB) je německý státní železniční podnik, který se řadí mezi největší poskytovatele dopravních služeb na světě. Společnost vznikla v roce 1994 sloučením západoněmecké Deutsche Bundesbahn a východoněmecké Deutsche Reichsbahn a má své sídlo v Berlíně.[192] DB nabízí široké spektrum služeb v oblasti osobní a nákladní dopravy a správy železniční infrastruktury. Je rozdělena do několika divizí, které zahrnují DB Fernverkehr (dálková osobní doprava), DB Regio (regionální a příměstská doprava), DB Cargo (nákladní doprava) a DB Netze (správa železniční infrastruktury).[193] Tato struktura umožňuje DB efektivně obsluhovat jak domácí, tak mezinárodní trhy a zajišťovat komplexní dopravní řešení.

Deutsche Bahn se aktivně zapojuje do inovací a modernizace své infrastruktury a služeb. Společnost investuje do digitalizace a automatizace provozu, implementuje pokročilé systémy řízení dopravy, vyvíjí a nasazuje elektrické a hybridní vlaky a modernizuje železniční stanice s využitím digitálních technologií.[194] DB se také zavazuje k udržitelnému rozvoji a ekologickým iniciativám, s cílem dosáhnout klimatické neutrality do roku 2040.[195] Tyto kroky jsou zásadní pro zajištění efektivního, bezpečného a ekologického provozu železniční dopravy.

---

[192] Deutsche Bahn AG. The foundation of Deutsche Bahn AG [online]. *deutschebahn.com.* [cit. 19.06.2024]. https://www.deutschebahn.com/en/group/history/topics/foundation-6929102#

[193] Deutsche Bahn. Business Units [online]. *deutschebahn.com.* [cit. 19.06.2024]. https://www.deutschebahn.com/en/group/business_units

[194] Deutsche Bahn. Deutsche Bahn invests a record EUR 7.6 bn in Strong Rail in Germany in 2023 [online]. *deutschebahn.com.* [cit. 19.06.2024]. https://www.deutschebahn.com/en/presse/press_releases/Deutsche-Bahn-invests-a-record-EUR-7-6-bn-in-Strong-Rail-in-Germany-in-2023-12760244

[195] Deutsche Bahn Engineering and Consulting. Sustainable mobility: DB to achieve climate neutrality ten years early [online]. *db-engineering-consulting.com.* [cit.

Nicméně, Deutsche Bahn čelí řadě výzev, včetně stárnoucí infrastruktury, nutnosti modernizace, konkurence na dopravním trhu a zajištění kvality služeb. Klíčovým problémem je také kybernetická bezpečnost, jak ukázal útok na společnost v roce 2017. Tento případ poukazuje na potřebu silných bezpečnostních opatření a neustálé inovace. Tato opatření jsou nezbytná nejen pro ochranu před kybernetickými hrozbami, ale i pro celkovou modernizaci společnosti, která musí být schopna čelit novým technologickým výzvám a zajistit bezpečný a spolehlivý provoz své infrastruktury. Příkladem mohou být inteligentní systémy řízení dopravy, které jsou navrženy tak, aby optimalizovaly provoz na železnicích, snižovaly zpoždění a zvyšovaly kapacitu tratí.[196] Tyto systémy jsou nezbytnou součástí modernizace, avšak jejich zabezpečení proti útokům je klíčové.[197] Útočníci by mohli tyto systémy zneužít k narušení provozu, například změnou signálů, manipulací s trasami vlaků nebo vytvářením falešných alarmů, což by mohlo vést k nehodám nebo rozsáhlým zpožděním. Proto je nutné implementovat bezpečnostní opatření, která budou tyto systémy chránit před kybernetickými hrozbami.

Právní úprava a její implementace v Německu

V roce 2017 byla právní úprava kybernetické bezpečnosti v Německu primárně formována Zákonem o bezpečnosti IT (IT-Sicherheitsgesetz), který vstoupil v platnost v roce 2015.[198] Tento zákon měl za cíl posílit bezpečnost IT systémů v sektorech kritické infrastruktury, mezi něž patří doprava, energetika, vodní hospodářství a zdravotnictví.[199] Hlavním regulačním orgánem odpovědným za dohled nad opatřeními

19.06.2024]. https://db-engineering-consulting.com/en/news/sustainable-mobility-db-to-achieve-climate-neutrality-ten-years-early/

[196] Prasad, N., Jain, S. Intelligent Technologies in High-Speed Rail Transit Systems. In: Upadhyay, R. K., Sharma, S. K., Kumar, V. (eds). *Intelligent Transportation System and Advanced Technology*. Springer Singapore, 2024, s. 217.

[197] Predescu, S. G., Savu, D., Badea, V. E. Cybersecurity in the Railway Sector. *Romanian Cyber Security Journal*. 2022, roč. 4, č. 2, s. 98.

[198] Sinner, F. IT-Sicherheitsgesetz [online]. *link11.com.* [cit. 25.05.2024]. https://www.link11.com/de/glossar/it-sicherheitsgesetz/

[199] ibidem

v oblasti kybernetické bezpečnosti a jejich dodržování v těchto kritických sektorech byl Spolkový úřad pro bezpečnost informační techniky (BSI).

Zákon o bezpečnosti IT vyžadoval, aby provozovatelé kritické infrastruktury zavedli přiměřená bezpečnostní opatření a hlásili významné IT bezpečnostní incidenty BSI.[200] Dále zákon požadoval pravidelné bezpečnostní audity a dodržování stanovených IT bezpečnostních standardů. Navzdory těmto předpisům se implementace a prosazování těchto opatření lišily napříč různými sektory a organizacemi.

Proč a jak se útok stal

Kybernetický útok na Deutsche Bahn se stal součástí celosvětového útoku WannaCry ransomwarem, který vypukl 12. května 2017.[201] WannaCry zneužíval zranitelnost v operačních systémech Microsoft Windows, která byla společností Microsoft identifikována a opravena již v březnu 2017.[202] Ransomware se rychle šířil, šifroval soubory na napadených systémech a požadoval výkupné v bitcoinech za jejich odšifrování.[203] V důsledku zobrazování vyděračské zprávy na panelech železničních stanic získal tento útok širokou pozornost po celém Německu.[204]

Systémy Deutsche Bahn byly zasaženy kvůli zpožděné implementaci potřebných bezpečnostních záplat.[205] Ransomware infikoval digitální displeje, prodejní automaty na jízdenky a zákaznické služby, což způsobilo značné narušení provozu.[206] I když samotné vlakové spoje nebyly

[200] Sinner, F. IT-Sicherheitsgesetz [online]. *link11.com.* [cit. 25.05.2024]. https://www.link11.com/de/glossar/it-sicherheitsgesetz/

[201] Fordoński, R., Kasprzak, W. WannaCry ransomware cyberattack as violation of international law. *Studia Prawnoustrojowe.* 2019, č. 44, s. 47-48.

[202] Federal Office for Information Security. *The State of IT Security in Germany 2017*. BSI, 2017, s. 26.

[203] ibidem

[204] ibidem

[205] ibidem

[206] Spiegel. 450 railway computers affected by "WannaCry" virus [online]. *spiegel.de.* [cit. 12.05.2024]. https://www.spiegel.de/netzwelt/web/wannacry-450-bahn-computer-von-cyber-attacke-betroffen-a-1147921.html

přímo ovlivněny, útok vážně narušil schopnost společnosti komunikovat s cestujícími a efektivně řídit služby.

Útok vyvolal okamžité kroky národních i mezinárodních kybernetických bezpečnostních orgánů. BSI vydal veřejná varování a pokyny, jak zmírnit účinky ransomwaru a zabránit dalším infekcím.[207] Tento incident zdůraznil důležitost proaktivních opatření v oblasti kybernetické bezpečnosti, včasných aktualizací a potřebu kvalitní strategie reakce na incidenty. Klíčové strategie zahrnují plán obnovy po havárii (DRP) a plán kontinuity podnikání (BCP). DRP se zaměřuje na rychlou obnovu kritických systémů a dat po incidentu pomocí pravidelných záloh a jasně definovaných postupů pro jejich obnovu, což minimalizuje dobu výpadku a škody způsobené incidentem.[208] BCP se soustředí na udržení provozu organizace během a po incidentu, zahrnuje analýzu dopadů na podnikání, plánování potřebných zdrojů a jasné komunikační plány, které zajistí informovanost všech zainteresovaných stran.[209] Tyto plány jsou nezbytné pro zajištění kontinuity a rychlé obnovy provozu organizace po kybernetickém útoku. BCP a DRP jsou úzce provázané se směrnicí NIS 2, která vyžaduje robustní opatření v oblasti kybernetické bezpečnosti, včetně správy záloh a obnovy po havárii, aby byla zajištěna ochrana a kontinuita kritických síťových a informačních systémů.[210] [211]

Okolnosti útoku

Kybernetický útok WannaCry na Deutsche Bahn se odehrál uprostřed většího globálního útoku, který zasáhl řadu organizací ve více než 150

[207] Federal Office for Information Security. *The State of IT Security in Germany 2017*. BSI, 2017, s. 26.

[208] Alhazmi, O., Malaiya, Y. *Evaluating Disaster Recovery Plans Using the Cloud.* IEEE, 2013, s. 3-6.

[209] Kumar, A., Prasad, P. Business continuity plan. *South Asian Journal of Engineering and Technology*. 2020, č. 102, s. 1-2.

[210] Oxfeldt, M. NIS2 Directive: A key to compliance is business continuity [online]. *keepit.com*. [cit. 16.04.2024]. https://www.keepit.com/blog/nis2-key-to-compliance/

[211] Barrat, J., Dupont, H. NIS 2: Developing Cyber Maturity and Compliance through Cyber Risk Quantification (CRQ) [online]. *citalid.com.* [cit. 03.05.2024]. https://citalid.com/resources/nis-2-cyber-directive/

zemích. Útok začal 12. května 2017 a rychle se šířil díky schopnosti ransomwaru šířit se jako červ, což mu umožnilo pronikat do zranitelných systémů bez zásahu uživatele.[212] Ransomware WannaCry využil zranitelnost známou jako EternalBlue, kterou původně vyvinula NSA jako nástroj pro kybernetické útoky.[213] EternalBlue cílil na chybu v protokolu Windows Server Message Block (SMB), což umožňovalo šíření malwaru mezi síťovými systémy.[214] Tento exploit byl uniknut hackerskou skupinou známou jako Shadow Brokers, což vedlo k jeho širokému využití v útoku WannaCry, který způsobil významné narušení globálně.[215]

Deutsche Bahn byla obzvláště zranitelná kvůli zpožděné implementaci bezpečnostních aktualizací, navzdory varováním od odborníků na kybernetickou bezpečnost o kritické povaze zranitelnosti v Microsoft Windows.[216] Načasování útoku, který současně zasáhl různé sektory po celém světě, zdůraznilo provázanost globálních IT systémů a kaskádové efekty takových rozsáhlých kybernetických hrozeb.

Nedostatky a úspěchy

Jedním z hlavních problémů, které WannaCry zneužil, byla opožděná aplikace bezpečnostních záplat od společnosti Microsoft. I když byla kritická zranitelnost opravena dva měsíce před útokem, mnoho systémů, včetně těch u Deutsche Bahn, nebylo aktualizováno, což odhalilo

[212] Kaspersky. What is WannaCry ransomware? [online]. *kaspersky.com.* [cit. 20.05.2024]. https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

[213] Liu, Z., et al. Working Mechanism of Eternalblue and Its Application in Ransomworm. In: Chen, X., Shen, J., Susilo, W. (eds). *Cyberspace Safety and Security*. Xi'an, China, 2022, 14th International Symposium, s. 178-179.

[214] Liu, Z., et al. Working Mechanism of Eternalblue and Its Application in Ransomworm. In: Chen, X., Shen, J., Susilo, W. (eds). *Cyberspace Safety and Security*. Xi'an, China, 2022, 14th International Symposium, s. 179-180.

[215] Burdova, C. What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant? [online]. *avast.com.* [cit. 16.06.2024]. https://www.avast.com/c-eternalblue

[216] Selvaraj, K., et al. WannaCrypt ransomware worm targets out-of-date systems [online]. *microsoft.com.* [cit. 18.06.2024]. https://www.microsoft.com/en-us/security/blog/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/

významné mezery v praxi správy záplat.[217] Tento incident také ukázal na širší problém uvnitř organizace týkající se povědomí o kybernetických hrozbách a školení zaměstnanců.[218] Zaměstnanci nebyli dostatečně připraveni rozpoznat a reagovat na takové hrozby, což přispělo k rozsahu útoku. Prvotní reakce na kybernetický útok odhalila mezery v plánu reakce na incidenty Deutsche Bahn. Informační panely a video dohled na mnoha nádražích přestaly fungovat a zobrazovaly vyděračské zprávy. Opravy systémů a obnovení plné funkčnosti trvalo několik dní[219], což vedlo společnost k přijetí opatření k zabezpečení a modernizaci IT infrastruktury. V reakci na útok Deutsche Bahn zahájila projekt Cyber Security @ DB, který zahrnoval zřízení krizového výboru a zavedení nových bezpečnostních protokolů pro zvýšení odolnosti proti podobným hrozbám.[220]

Mezi úspěchy je možné zařadit to, že po zjištění rozsahu kybernetického útoku Deutsche Bahn okamžitě oznámila incident BSI a Spolkovému kriminálnímu úřadu (BKA).[221] [222] Tato spolupráce usnadnila koordinovanou reakci na zmírnění dopadů a zahájení vyšetřování narušení. IT tým Deutsche Bahn pracoval efektivně na izolaci postižených systémů, obnovení služeb ze záloh a aplikaci potřebných záplat.[223] Nicméně, větším škodám zabránil bezpečnostní výzkumník v Londýně, který v pátek 12. května 2017 objevil a zaregistroval doménu, kterou WannaCry

[217] Federal Office for Information Security. *The State of IT Security in Germany 2017*. BSI, 2017, s. 26.

[218] Kaspersky. What is WannaCry ransomware? [online]. *kaspersky.com.* [cit. 20.05.2024]. https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

[219] Spiegel. 450 railway computers affected by "WannaCry" virus [online]. *spiegel.de.* [cit. 12.05.2024]. https://www.spiegel.de/netzwelt/web/wannacry-450-bahn-computer-von-cyber-attacke-betroffen-a-1147921.html

[220] Deutsche Bahn. *2017 Integrated Report: Departure into a new era!* Deutsche Bahn AG, 2017, s. 154.

[221]Bundeskriminalamt. *Cybercrime: Bundeslagebild 2017*. BKA, 2017, s. 29.

[222] Federal Office for Information Security. *The State of IT Security in Germany 2017*. BSI, 2017, s. 26.

[223]Deutsche Bahn. *2017 Integrated Report: Departure into a new era!* Deutsche Bahn AG, 2017, s. 200.

využíval k šíření, čímž účinně zastavil první vlnu útoku.[224] Tímto úsilím se minimalizoval dlouhodobý dopad útoku na provoz vlaků a zákaznické služby. Během následujících dní však hackeři vytvořili nové verze, které tuto slabinu (kill switch) již neobsahovaly a byly obtížněji zastavitelné.[225] Útok WannaCry posloužil jako varování, které přimělo Deutsche Bahn a další provozovatele kritické infrastruktury k tomu, aby upřednostnili opatření v oblasti kybernetické bezpečnosti, provedli důkladné revize svých IT bezpečnostních praktik a zvýšili svou obranu proti budoucím hrozbám (Cyber Security @ DB).[226]

5.1.2 Případ 2: Útok na německý zdravotnický systém (2020 - nemocnice v Düsseldorfu)

Nemocnice v Düsseldorfu, známá jako Universitätsklinikum Düsseldorf (UKD), je jednou z předních zdravotnických institucí v Německu. Jako univerzitní nemocnice nabízí širokou škálu lékařských služeb a je významným centrem pro výzkum, vzdělávání a klinickou péči.[227] UKD poskytuje komplexní zdravotní péči pro obyvatele Düsseldorfu a okolních regionů (samotný Düsseldorf má kolem 640 000 obyvatel[228], celkově tedy může být nemocnice spádovou oblastí pro cca 1 – 1,5 mil. obyvatel), přičemž spolupracuje s lékařskou fakultou Heinrich Heine University.

[224] Khomami, N., Solon, O. 'Accidental hero' halts ransomware attack and warns: this is not over [online]. *theguardian.com.* [cit. 17.05.2024]. https://www.theguardian.com/technology/2017/may/13/accidental-hero-finds-kill-switch-to-stop-spread-of-ransomware-cyber-attack

[225] Norton Rose Fulbright. WannaCry Ransomware Attack Summary [online]. *dataprotectionreport.com.* [cit. 20.05.2024]. https://www.dataprotectionreport.com/2017/05/wannacry-ransomware-attack-summary/

[226] Deutsche Bahn. *2017 Integrated Report: Departure into a new era!* Deutsche Bahn AG, 2017, s. 200.

[227] The University Hospital Düsseldorf. Innovation and transparency [online]. *uniklinik-duesseldorf.de.* [cit. 10.06.2024]. https://www.uniklinik-duesseldorf.de/ueber-das-ukd/unternehmen

[228] Düsseldorf. Office for Statistics and Elections [online]. *duesseldorf.de.* [cit. 10.06.2024]. https://www.duesseldorf.de/statistik-und-wahlen/statistik-und-stadtforschung/statistics

Nemocnice zahrnuje široké spektrum specializovaných oddělení, včetně kardiologie, onkologie, neurologie a dalších klíčových oblastí medicíny, což z ní činí důležité zdravotnické centrum pro pacienty s různými zdravotními problémy.[229]

UKD se rovněž angažuje v pokročilém lékařském výzkumu a inovacích.[230] Nemocnice využívá moderní technologie a postupy, aby zajistila nejvyšší úroveň péče. Investice do digitalizace a modernizace infrastruktury jsou klíčovými aspekty jejího provozu. Vzhledem k tomu, že UKD funguje jako univerzitní nemocnice, hraje také významnou roli ve vzdělávání budoucích lékařů a zdravotnického personálu.[231] Nemocnice se zapojuje do mezinárodních výzkumných projektů a spolupracuje s dalšími předními zdravotnickými institucemi.

Nicméně, stejně jako mnoho jiných zdravotnických zařízení, čelí i UKD řadě výzev. Mezi hlavní problémy patří financování zdravotní péče, zajištění dostatečných zdrojů pro modernizaci technologií a infrastruktury a také otázka kybernetické bezpečnosti.[232] Útok na nemocnici v roce 2020 vedl k významnému narušení zdravotnických služeb, což mělo přímý dopad na pacienty, včetně jednoho úmrtí kvůli zpožděné péči.[233] Útočníci použili ransomware k zašifrování dat nemocnice, což vyřadilo z provozu klíčové systémy.[234] Útok pravděpodobně využil zranitelnosti v softwaru Citrix nebo nedostatečně zabezpečené přístupové body.[235] Útok, který vážně narušil provoz UKD, zdůraznil potřebu

[229] The University Hospital of Düsseldorf. About us [online]. *uniklinik-duesseldorf.de.* [cit. 10.06.2024]. https://www.uniklinik-duesseldorf.de/international-patients/english/about-us

[230] ibidem

[231] ibidem

[232] Knight, B. How to save Germany's hospitals [online]. *dw.com.* [cit. 15.05.2024]. https://www.dw.com/en/how-to-save-germanys-hospitals/a-63634230

[233] Ralston, W. The untold story of a cyberattack, a hospital and a dying woman [online]. *wired.com.* [cit. 14.06.2024]. https://www.wired.com/story/ransomware-hospital-death-germany/ /

[234] Prucková, M. German hospital ransomware attack (2020) [online]. *cyberlaw.ccdcoe.org.* [cit. 13.06.2024]. https://cyberlaw.ccdcoe.org/wiki/German_hospital_ransomware_attack_(2020)

[235] ibidem

posílení bezpečnostních opatření a lepší připravenosti na kybernetické hrozby. Tento incident ukázal na zranitelnosti v nemocničním systému, které je nutné řešit, aby byla zajištěna kontinuita a bezpečnost zdravotní péče.

Právní úprava a její implementace v Německu

Během útoku na Universitätsklinikum Düsseldorf v roce 2020 byl hlavním legislativním rámcem pro kybernetickou bezpečnost v Německu „IT-Sicherheitsgesetz", který byl přijat v roce 2015.[236] Směrnice NIS a německý zákon o bezpečnosti IT vyžadovaly, aby poskytovatelé kritických služeb, včetně zdravotnictví, přijali vhodná bezpečnostní opatření a oznamovali závažné incidenty. Navzdory těmto požadavkům nebyla implementace bezpečnostních opatření v nemocnicích dostatečně důsledná, pravděpodobně kvůli problémům německého zdravotnického systému s financováním a prioritizací kybernetické bezpečnosti, což vedlo k slabé realizaci požadovaných opatření.[237] [238]

V roce 2020, během útoku na Universitätsklinikum Düsseldorf, byl platný BSI Critical Infrastructure Regulation (BSI-KritisV), který vyžadoval, aby nemocnice implementovaly minimální standardy a opatření k zajištění dostatečné IT bezpečnosti. Nemocnice v Düsseldorf byla klasifikována jako subjekt kritické infrastruktury, jelikož splňuje podmínky pro nemocnice v příloze 5 části 3 BSI-KritisV.[239]

Po útoku na Universitätsklinikum Düsseldorf bylo zdůrazněno, že existuje potřeba posílit stávající právní rámec. V roce 2021 proto

[236] Sinner, F. IT-Sicherheitsgesetz [online]. *link11.com.* [cit. 25.05.2024]. https://www.link11.com/de/glossar/it-sicherheitsgesetz/

[237] Simsek, A. German hospitals protest lack of funds, warn of looming crisis [online]. *aa.com.tr.* [cit. 14.06.2024]. https://www.aa.com.tr/en/europe/german-hospitals-protest-lack-of-funds-warn-of-looming-crisis/2996922

[238] Klick, J., Brandstetter, T., Koch, R. Epidemic? The Attack Surface of German Hospitals during the COVID-19 Pandemic. In: Jančárková, T., et al. (eds). *2021 13th International Conference on Cyber Conflict: Going viral*. Tallinn, Estonia, NATO CCDCOE Publications, 2021, s. 74 a 89.

[239] The University Hospital of Düsseldorf. History of the University Hospital Düsseldorf [online]. *uniklinik-duesseldorf.de.* [cit. 12.05.2024]. https://www.uniklinik-duesseldorf.de/ueber-das-ukd/geschichte-des-ukd

Německo přijalo nový IT-Sicherheitsgesetz 2.0, který dále zpřísnil požadavky na kybernetickou bezpečnost a rozšířil pravomoci BSI.[240]

Proč a jak se útok stal

V září 2020 došlo k závažnému kybernetickému útoku na nemocnici v Düsseldorfu, kdy útočníci použili ransomware Doppelpaymer k zašifrování nemocničních dat, čímž paralyzovali klíčové systémy.[241] Tento incident způsobil selhání nemocničních sítí a následný postupný kolaps počítačových systémů. To vedlo k úplnému omezení zaměstnanců v přístupu k potřebným datům, což mělo za následek neschopnost provádět operace a nutnost přepravy pacientů do okolních nemocnic.[242]

Po zjištění incidentu nemocnice neprodleně informovala BSI, který následující den zahájil vyšetřování s podezřením na kybernetický útok.[243] Vyšetřování odhalilo, že útočník využil zranitelnost ve VPN softwaru od společnosti Citrix Systems, který je určen k optimalizaci provozu nemocničních systémů.[244] Tato zranitelnost byla odhalena koncem roku 2019 a začátkem roku 2020 byla vydána aktualizace, která tento

[240] Federal Office for Information Security. Second Act to Increase the Security of Information Technology Systems [online]. *bsi.bund.de.* [cit. 28.05.2024]. https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html

[241] Ralston, W. The untold story of a cyberattack, a hospital and a dying woman [online]. *wired.com*. [cit. 14.06.2024]. https://www.wired.com/story/ransomware-hospital-death-germany/

[242] Ralston, W. The untold story of a cyberattack, a hospital and a dying woman [online]. *wired.com.* [cit. 14.06.2024]. https://www.wired.com/story/ransomware-hospital-death-germany/

[243] Federal Office for Information Security. Cyber attack on Düsseldorf University Hospital: BSI warns of acute exploitation of known vulnerability [online]. *bsi.bund.de.* [cit. 28.05.2024]. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2020/UKDuesseldorf_170920.html

[244] ibidem

bezpečnostní problém řešila.[245] Podle dostupných informací nemocnice v Düsseldorfu svůj software aktualizovala již v lednu 2020.[246]

Navzdory této aktualizaci útočník dokázal proniknout do nemocniční sítě, což naznačuje, že se mu podařilo vstoupit do systému ještě před provedením aktualizace a následně využil zadní vrátka, která mu umožnila opětovný přístup.[247] Útočník byl v systému nemocnice v Düsseldorfu přítomen dostatečně dlouho na to, aby si připravil půdu pro útok, což naznačuje, že se jednalo o pokročilého útočníka, možná i o tzv. Advanced Persistent Threat (APT)[248]. Schopnost útočníka zůstat dlouho neodhalený a systematicky se připravovat na nasazení ransomwaru svědčí o vysoké úrovni odbornosti a strategického plánování.[249] Tato pokročilost útoku odhalila kritické slabiny v bezpečnostních opatřeních nemocnice, ale zároveň ukazuje na nedostatečné kapacity nemocnice v oblasti detekce a reakce na takové sofistikované hrozby. Navíc je třeba zdůraznit, že původním cílem útočníka nebyla samotná nemocnice, ale univerzita.[250] Po útoku, když byl kontaktován policií, útočník údajně poskytl

[245] Federal Office for Information Security. Cyber attack on Düsseldorf University Hospital: BSI warns of acute exploitation of known vulnerability [online]. *bsi.bund.de.* [cit. 28.05.2024]. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2020/UKDuesseldorf_170920.html

[246] Ralston, W. The untold story of a cyberattack, a hospital and a dying woman [online]. *wired.com.* [cit. 14.06.2024]. https://www.wired.com/story/ransomware-hospital-death-germany/

[247] Schirrmacher, D. Workaround available: Critical vulnerability in Citrix ADC and Gateway [online]. *heise.de.* [cit. 17.05.2024]. https://www.heise.de/news/Workaround-verfuegbar-Kritische-Luecke-in-Citrix-ADC-und-Gateway-4627525.html

[248] APT je označení pro vysoce kvalifikovaného útočníka s dostatečnými zdroji, který využívá různé metodiky útoků, aby pronikl a trvale operoval v IT infrastrukturách organizací. Jeho cílem je často krádež dat, narušení provozu nebo příprava na budoucí akce, přičemž se adaptuje na obranná opatření po dlouhou dobu.

[249] Federal Office for Information Security. Cyber attack on Düsseldorf University Hospital: BSI warns of acute exploitation of known vulnerability [online]. *bsi.bund.de.* [cit. 28.05.2024]. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2020/UKDuesseldorf_170920.html

[250] Miliard, M. Hospital ransomware attack leads to fatality after causing delay in care [online]. *healthcareitnews.com.* [cit. 24.05.2024].

dešifrovací klíč, což naznačuje, že neměl v úmyslu způsobit škodu nemocnici.[251] Tento fakt dodává útoku další vrstvu složitosti a ukazuje na to, že i přes nedostatečnou připravenost nemocnice byla samotná pokročilost útočníka klíčovým faktorem úspěchu útoku. Útočníkova ochota komunikovat s policií a poskytnout dešifrovací klíč naznačuje určitou úroveň etiky nebo alespoň úmysl minimalizovat škody způsobené neúmyslným zásahem.

K úspěchu kybernetických útoků na nemocnice může též přispět komplexnost a zastaralost jejich systémů. Zdravotnická zařízení často používají širokou škálu přístrojů připojených k internetu, které mohou mít různé bezpečnostní nedostatky.[252] Mnohé z těchto přístrojů jsou velmi drahé a kritické pro lékařskou péči, což znamená, že je nelze snadno nahradit nebo aktualizovat.[253] Starší zařízení mohou být náchylnější k útokům, protože výrobci již neposkytují bezpečnostní aktualizace. Tento problém je umocněn tím, že nemocnice používají mnoho různých systémů a zařízení, což zvyšuje komplexnost a obtížnost udržování všech systémů aktuálních a bezpečných. Nemocnice navíc fungují nepřetržitě, což ztěžuje plánování a provádění údržby a aktualizací bez narušení poskytování zdravotní péče. Tento nedostatek času na údržbu a zajištění kybernetické bezpečnosti může vést k tomu, že zranitelnosti zůstanou neopravené po dlouhou dobu.

Analýza incidentu zdůrazňuje důležitost pravidelných a důsledných aktualizací softwaru a nutnost kontinuálního monitorování

---

https://www.healthcareitnews.com/news/hospital-ransomware-attack-leads-fatality-after-causing-delay-care

[251] Miliard, M. Hospital ransomware attack leads to fatality after causing delay in care [online]. *healthcareitnews.com.* [cit. 24.05.2024]. https://www.healthcareitnews.com/news/hospital-ransomware-attack-leads-fatality-after-causing-delay-care

[252] Ikeda, S. Ransomware Attack at German Hospital Responsible for First Documented Death [online]. *cpomagazine.com.* [cit. 14.05.2024]. https://www.cpomagazine.com/cyber-security/ransomware-attack-at-german-hospital-responsible-for-first-documented-death/

[253] Klick, J., Brandstetter, T., Koch, R. Epidemic? The Attack Surface of German Hospitals during the COVID-19 Pandemic. In: Jančárková, T., et al. (eds). *2021 13th International Conference on Cyber Conflict: Going viral*. Tallinn, Estonia, NATO CCDCOE Publications, 2021, s. 74.

a zabezpečení systémů. Současně je důležité nezapomenout na nezbytnost zvyšování povědomí o kybernetických hrozbách mezi zaměstnanci, aby byli schopni lépe rozpoznat a reagovat na potenciální rizika. Tento incident rovněž podtrhuje potřebu posílení bezpečnostních protokolů a implementace kvalitnějších opatření kybernetické bezpečnosti v nemocničních zařízeních, aby se předešlo podobným událostem v budoucnosti. Prvním krokem by mělo být zvýšení finančních prostředků alokovaných na kybernetickou bezpečnost v rámci zdravotnických zařízení. Vzhledem k již nyní nedostatečnému financování nemocnic je důležité zaměřit se na efektivní využití dostupných zdrojů a identifikovat oblasti s největšími riziky, které vyžadují okamžitou pozornost. Dále by bylo vhodné zavést jedno z klíčových opatření, a to pravidelnou aktualizaci veškerého softwaru a systémů používaných v nemocnicích. To by mělo zahrnovat nejen operační systémy a aplikace, ale také zdravotnické přístroje připojené k síti, které často bývají zanedbávány.

Okolnosti útoku

Útok se odehrál v době, kdy nemocnice čelila značnému tlaku kvůli pandemii COVID-19. Zvýšené používání digitálních systémů a náhlé změny v pracovních postupech mohly vést k přehlédnutí aktualizace kritických bezpečnostních záplat.[254] Tento případ zdůraznil potřebu lepšího zabezpečení zdravotnických systémů a pravidelných aktualizací softwaru.

Kromě technických aspektů hrála roli i koordinace mezi různými úrovněmi řízení a jejich reakce na varování o zranitelnostech. I když byla aktualizace provedena, došlo k útoku, protože útočník pronikl do systému ještě před její aplikací. Tento případ ilustruje důležitost nejen rychlé aktualizace softwaru, ale také kontinuální opatření pro monitorování a reakci. Nemocnice by měly zavést rámec pro řízení rizik a kontrolu v oblasti kybernetické bezpečnosti, který zahrnuje identifikaci a hodnocení rizik, zavedení kontrolních opatření a pravidelné přezkoumávání jejich efektivity. Je nutné implementovat základní bezpečnostní opatření, jako jsou šifrování dat, vícefaktorová autentizace, segmentace sítě a pravidelná aktualizace softwaru a systémů. Pravidelné hodnocení vyspělosti bezpečnostních opatření a vytváření plánů pro neustálé zlepšování kybernetické bezpečnosti, schvalovaných vedením nemocnice, jsou klíčové.

[254] He, Y., et al. Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. *J Med Internet Res.* 2021, roč. 23, č. 4, s. 14-15.

Nemocnice v Düsseldorfu oznámila, že při útoku nedošlo ke zničení ani odcizení dat, ale výrazně narušil její provoz. Oddělení pohotovostní péče nebylo plně funkční ještě několik dní po útoku.[255] BSI vydal varování a doporučení pro všechny uživatele softwaru Citrix, aby prováděli důkladné revize své infrastruktury a posílili bezpečnostní opatření.[256]

Během kybernetickému útoku na nemocnici v Düsseldorfu zemřela pacientka, která byla z důvodu útoku poslána do vzdálenější nemocnice.[257] Vyšetřovatelé zkoumali, zda za její smrt bude odpovědný útočník.[258] Hlavní státní zástupce v Kolíně nad Rýnem, Markus Hartmann, uvedl, že samotný útok nebyl přímou příčinou smrti pacientky.[259] Po několika měsících vyšetřování dospěli vyšetřovatelé k závěru, že pacientka byla v tak špatném zdravotním stavu, že by pravděpodobně zemřela i bez zpoždění způsobeného kybernetickým útokem.[260]

Nedostatky a úspěchy

Mezi hlavní nedostatky patřilo slabé zabezpečení zdravotnických systémů, nedostatečná záloha dat a chybějící krizový plán pro kybernetické útoky. Zdravotnické zařízení nemělo dostatečné zálohovací systémy, což vedlo k tomu, že ransomware útok způsobil značné narušení provozu. Kdyby byly implementovány pravidelné a bezpečné zálohy dat, nemocnice by mohla rychleji obnovit své systémy a minimalizovat dopad útoku. Zdravotnické zařízení nemělo implementované pokročilé bezpečnostní opatření, jako jsou systémy pro detekci a reakci na kybernetické hrozby. Tyto systémy jsou schopny rychle identifikovat a reagovat na podezřelé

[255] Federal Office for Information Security. Cyber Security in Healthcare. *BSI Magazine*. 2020, č. 2, s. 13.

[256] Federal Office for Information Security. Cyber attack on Düsseldorf University Hospital: BSI warns of acute exploitation of known vulnerability [online]. *bsi.bund.de.* [cit. 28.05.2024]. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2020/UKDuesseldorf_170920.html

[257] Goodin, D. A patient dies after a ransomware attack hits a hospital [online]. *wired.com.* [cit. 16.05.2024]. https://www.wired.com/story/a-patient-dies-after-a-ransomware-attack-hits-a-hospital/

[258] ibidem

[259] ibidem

[260] ibidem

aktivity v síti, čímž mohou zabránit rozsáhlým škodám a minimalizovat dopady útoků.

Naopak, rychlé varování a koordinace s jinými nemocnicemi pomohlo minimalizovat další škody a zajistit, že pacienti dostali potřebnou péči v jiných zařízeních. I když nemocnice čelila vážným problémům kvůli útoku, schopnost rychle informovat a spolupracovat s dalšími zdravotnickými zařízeními byla klíčová pro zvládnutí krize a minimalizaci negativních dopadů na pacienty

5.1.3 Případ 3: Ransomware útok na energetickou společnost v Itálii (2020 - Enel)

Enel S.p.A. je jednou z největších energetických společností na světě, se sídlem v Římě, Itálie. Společnost byla založena v roce 1962 a postupně se rozrostla do globálního lídra v oblasti elektrické energie a plynu.[261] Enel působí ve více než 30 zemích na pěti kontinentech, kde poskytuje širokou škálu služeb od výroby a distribuce elektřiny po prodej a obchodování s energií.[262] Společnost je známá svým důrazem na obnovitelné zdroje energie a inovace v energetickém sektoru, což jí umožňuje hrát klíčovou roli v globálním přechodu na udržitelnou energetiku.[263]

Enel se zaměřuje na rozvoj a implementaci pokročilých technologií a digitálních řešení, aby zefektivnila své operace a zlepšila služby pro své zákazníky. Investice do obnovitelných zdrojů, jako jsou solární, větrné a vodní elektrárny, jsou klíčovou součástí strategie společnosti.[264] Enel také aktivně pracuje na rozvoji chytrých sítí (smart grids) a inteligentních měřících systémů, které zvyšují efektivitu a spolehlivost dodávek energie.[265] Společnost se rovněž angažuje v projektech zaměřených na energetickou účinnost a dekarbonizaci průmyslu.

---

[261] Enel. Our story [online]. *enel.com.* [cit. 12.06.2024]. https://www.enel.com/company/about-us/our-story

[262] ibidem

[263] Enel. Enel Group [online]. *enel.com.co.* [cit. 12.06.2024]. https://www.enel.com.co/en/the-companies/enel-group.html

[264] ibidem

[265] Enel. Enel Group [online]. *enel.com.co.* [cit. 12.06.2024]. https://www.enel.com.co/en/the-companies/enel-group.html

Navzdory svým úspěchům a inovačním snahám čelí Enel řadě výzev, včetně geopolitických rizik, regulací v energetickém sektoru a rostoucí konkurence na globálním trhu. Jedním z nejvýznamnějších problémů je však otázka kybernetické bezpečnosti.

Právní úprava a implementace v Itálii

V době kybernetického útoku na společnost Enel v říjnu 2020 byla právní úprava kybernetické bezpečnosti kritické infrastruktury v Itálii založena na několika klíčových zákonech a regulacích. Itálie přijala NIS směrnici, která byla implementována v roce 2018.[266] V Itálii byla směrnice implementována zákonem o kybernetické bezpečnosti (Decreto Legislativo 65/2018), který definoval opatření pro ochranu kritické infrastruktury.[267] Tento zákon vyžadoval, aby poskytovatelé kritických služeb, včetně energetických společností, přijali vhodná bezpečnostní opatření a oznamovali závažné incidenty, avšak přestože italská vláda přijala určité kroky k implementaci těchto pravidel, nejen energetický sektor čelil výzvám s jejich plnou implementací. Zvláště malé a střední podniky měly problémy s financováním a realizací potřebných bezpečnostních opatření. Náklady zahrnují nejen finanční výdaje na nové technologie a systémy, ale také na školení zaměstnanců, najímání odborníků na kyberbezpečnost a udržování aktuálních seznamů a zpráv požadovaných zákony. Italská legislativa, zahrnující prováděcí dekrety a prezidentské dekrety, přináší určitou míru flexibility, což může být výhodné, ale také představuje výzvy. Národní legislativa, založená na vládních dekretech, je relativně snadno a rychle upravitelná, což umožňuje rychle reagovat na nové hrozby a potřeby.[268] Na druhé straně, složitý legislativní rámec může vést k vysoké administrativní zátěži a nejistotě pro společnosti. Nutnost pravidelných aktualizací a udržování seznamů ICT aktiv a komponent může být zvláště náročná pro operátory s vysokou

[266] Tugnoli, F., et al. At a glance: cybersecurity best practices in Italy [online]. *lexology.com*. [cit. 14.05.2024]. https://www.lexology.com/library/detail.aspx?g=d3975429-3d0d-4b24-b9c0-9102f2cc9f5e

[267] ibidem

[268] Schmitz-Berndt, S., Chiara, P. G. One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive. *International Cybersecurity Law Review*. 2022, roč. 3, s. 298.

mírou digitalizace.[269] Právní nejistota může vzniknout z nejasné interpretace, co zahrnuje například sektor "digitálních služeb".[270] Tento nedostatek konkrétního vymezení může vést k různým interpretacím a následně ke zvýšeným nákladům na dosažení souladu s předpisy.[271]

Implementace požadavků směrnice NIS v Itálii, stejně jako v ostatních členských státech, zahrnovala založení specializovaných institucí, poskytujících podporu a koordinaci v oblasti kybernetické bezpečnosti. V Itálii se jednalo o Agenzia per l'Italia Digitale (AgID) a Computer Emergency Response Team (CERT).[272]

Proč a jak se útok stal

V roce 2020 se společnost Enel stala obětí kybernetického útoku pomocí ransomwaru. Kybernetický útok na společnost Enel byl proveden pomocí ransomwaru Netwalker.[273] Ransomware Netwalker se šíří přes phishingové[274] e-maily nebo zranitelnosti v softwaru, které útočníci využijí k infiltraci do systému společnosti.[275] Tedy jestli např. zaměstnanci společnosti Enel na tyto e-maily klikli, ransomware se nainstaloval do jejich systémů.

---

[269] Schmitz-Berndt, S., Chiara, P. G. One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive. *International Cybersecurity Law Review*. 2022, roč. 3, s. 299.

[270] ibidem

[271] Schmitz-Berndt, S., Chiara, P. G. One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive. *International Cybersecurity Law Review*. 2022, roč. 3, s. 299.

[272] Tugnoli, F., et al. At a glance: cybersecurity best practices in Italy [online]. *lexology.com*. [cit. 14.05.2024]. https://www.lexology.com/library/detail.aspx?g=d3975429-3d0d-4b24-b9c0-9102f2cc9f5e

[273] Šlekytė, I. What is Netwalker ransomware? [online]. *nordvpn.com.* [cit. 16.05.2024]. https://nordvpn.com/blog/netwalker-ransomware/

[274] Phishingový útok je forma kybernetického útoku, při které útočník spustí škodlivý kód na zařízení oběti či získává citlivé informace od oběti pod záminkou legitimního podnětu, často prostřednictvím falešných e-mailů, webových stránek nebo jiných komunikačních kanálů.

[275] Baig, Z., Mekala, S. H., Zeadally, S. Ransomware Attacks of the COVID-19 Pandemic: Novel Strains, Victims, and Threat Actors. *IT Professiona*. 2023, roč. 25, č. 5, s. 40.

Netwalker se poté rychle rozšířil v celé síti společnosti Enel, šifroval soubory a způsobil značné narušení provozu. Útočníci požadovali výkupné ve výši 14 milionů dolarů v bitcoinech za dešifrovací klíč.[276] Společnost Enel nahlásila incident Národnímu centru pro kybernetickou bezpečnost (CSIRT Italia), které fungovalo pod Ministerstvem hospodářského rozvoje (MiSE).[277] Toto centrum bylo zodpovědné za koordinaci a reakci na kybernetické incidenty před vznikem Národní agentury pro kybernetickou bezpečnost (ACN) v roce 2021.[278] Útok byl dobře naplánovaný a koordinovaný, využíval slabých míst v bezpečnostních opatřeních společnosti a byl proveden v době, kdy byla společnost zranitelná. Tento útok využíval kombinace pokročilých technik, včetně fileless metod a reflective DLL injection.[279] Útočníci využili nedostatečnou ochranu proti fileless útokům, kdy malware nebyl uložen na disku, ale byl spuštěn přímo v paměti systému pomocí PowerShell skriptů.[280] Tyto skripty byly vysoce obfuskované[281] a šifrované, což znemožňovalo jejich snadnou detekci a analýzu.[282] Reflektovaná injekce DLL umožnila útočníkům injektovat škodlivé kódy přímo do běžících procesů, jako je explorer.exe, aniž by bylo nutné ukládat DLL soubor na disk.[283] Tato technika obchází tradiční detekční mechanismy, které monitorují načítání modulů a DLL

[276] GFI Software. Enel hit by ransomware [online]. *techgenix.com*. [cit. 15.05.2024]. https://techgenix.com/enel-hit-by-ransomware/

[277] Štorek, D. Pracoviště typu CSIRT a CERT v Evropě. *Ochrana & Bezpečnost.* 2018, roč. 7, č. 1, s. 51.

[278] National Cybersecurity Agency. About ACN [online]. *acn.gov.it.* [cit. 16.06.2024]. https://www.acn.gov.it/portale/en/chi-siamo

[279] Victor, K. Reflective Loading Runs Netwalker Fileless Ransomware [online]. *trendmicro.com.* [cit. 16.06.2024]. https://www.trendmicro.com/en_us/research/20/e/netwalker-fileless-ransomware-injected-via-reflective-loading.html

[280] ibidem

[281] Obfuskování je proces, při kterém se záměrně komplikuje čitelnost a srozumitelnost kódu nebo dat, aby bylo obtížnější je analyzovat nebo reverzním inženýrstvím zpětně pochopit jejich funkci.

[282] Victor, K. Reflective Loading Runs Netwalker Fileless Ransomware [online]. *trendmicro.com.* [cit. 16.06.2024]. https://www.trendmicro.com/en_us/research/20/e/netwalker-fileless-ransomware-injected-via-reflective-loading.html

[283] ibidem

souborů do procesů.[284] V rámci útoku byly využity také techniky, které odstranily Shadow Volume Copies, čímž bylo oběti zabráněno v obnovení dat z těchto záloh.[285] Dále útočníci zastavili procesy související se zálohováním a bezpečností, což znesnadnilo obnovu dat a ochranu před útokem[286]

Aby se předešlo útokům podobným těm, kterým čelila společnost Enel v roce 2020, je nezbytné implementovat několik klíčových bezpečnostních opatření. Tato opatření mohou významně zvýšit celkovou bezpečnost organizace a minimalizovat rizika spojená s ransomware útoky. PowerShell je nástroj, který útočníci často využívají ke spuštění škodlivých skriptů přímo v paměti systému.[287] Proto je důležité využívat jeho možnosti logování k monitorování podezřelého chování. Konkrétně může použití režimu ConstrainedLanguageMode omezit schopnost spuštění škodlivých skriptů tím, že zamezí přístupu k pokročilým funkcím PowerShellu, které nejsou běžně potřebné pro každodenní úlohy.[288] Jedním z nejúčinnějších způsobů, jak se chránit před ransomware útoky, je pravidelné zálohování kritických dat.[289] Zálohy by měly být prováděny pravidelně a ukládány mimo hlavní síť, aby byly k dispozici i v případě, že je síť kompromitována.[290] Je také důležité pravidelně ověřovat a testovat zálohy, aby bylo jisté, že je lze v případě potřeby úspěšně obnovit. Pravidelná aplikace aktualizací a bezpečnostních záplat pro operační systémy a software třetích stran je klíčová pro minimalizaci rizika využití známých zranitelností. Útočníci často hledají neaktualizované systémy, které mohou napadnout, takže udržování všech systémů aktuálních je

[284] Victor, K. Reflective Loading Runs Netwalker Fileless Ransomware [online]. *trendmicro.com.* [cit. 16.06.2024]. https://www.trendmicro.com/en_us/research/20/e/netwalker-fileless-ransomware-injected-via-reflective-loading.html

[285] ibidem

[286] ibidem

[287] ibidem

[288] ibidem

[289] Manjezi, Z., Botha, R. A. Preventing and Mitigating Ransomware. In: Venter, H., et al. (eds). *Information Security*. Pretoria, South Africa, 17th International Conference, ISSA 2018, s. 155.

[290] ibidem

základním preventivním opatřením.[291] Zaměstnanci jsou často první linií obrany proti kybernetickým útokům. Pravidelné školení o bezpečnostních hrozbách a technikách sociálního inženýrství může výrazně zvýšit schopnost zaměstnanců rozpoznat a reagovat na podezřelé e-maily a soubory.[292] Informovaní zaměstnanci mohou zabránit mnoha útokům jednoduše tím, že neotevřou podezřelé přílohy nebo nekliknou na škodlivé odkazy. Multifaktorová autentizace výrazně zvyšuje bezpečnost přístupů do kritických systémů tím, že vyžaduje více forem ověření identity.[293] I když útočník získá heslo, stále potřebuje další faktor (například mobilní telefon nebo biometrický údaj), aby mohl získat přístup. Tím se snižuje riziko neautorizovaného přístupu.

Dalším důležitým faktorem byla sofistikovanost útočníků, kteří využívali pokročilé metody k obcházení bezpečnostních opatření.[294] Taktika ransomwaru, jako je Netwalker, zahrnovala nejen šifrování dat, ale i krádež informací a hrozby jejich zveřejnění, což zvyšovalo tlak na oběti, aby zaplatily výkupné.

Okolnosti útoku

Kybernetický útok na společnost Enel byl ovlivněn několika klíčovými faktory. Pandemie COVID-19 vedla k masivnímu přesunu zaměstnanců na práci z domova, což zvýšilo zranitelnost organizací vůči kybernetickým útokům. Domácí sítě a zařízení často postrádají stejnou úroveň

[291] Manjezi, Z., Botha, R. A. Preventing and Mitigating Ransomware. In: Venter, H., et al. (eds). *Information Security*. Pretoria, South Africa, 17th International Conference, ISSA 2018, s. 155-156.

[292] Manjezi, Z., Botha, R. A. Preventing and Mitigating Ransomware. In: Venter, H., et al. (eds). *Information Security*. Pretoria, South Africa, 17th International Conference, ISSA 2018, s. 156-157.

[293] AlAnsary, S. A., Latif, R., Saba, T. Multi Factor Authentication as a Service (MFAaaS) for Federated Cloud Environments. In: Daimi, K., Sadoon, A. A. (eds*). Proceedings of the Second International Conference on Innovations in Computing Research (ICR'23).* Springer, 2023, s. 227.

[294] Baig, Z., Mekala, S. H., Zeadally, S. Ransomware Attacks of the COVID-19 Pandemic: Novel Strains, Victims, and Threat Actors. *IT Professiona*. 2023, roč. 25, č. 5, s. 40.

zabezpečení jako firemní prostředí.[295] Během pandemie došlo ke zvýšení aktivity kyberzločinců, kteří využívali chaosu a zvýšené závislosti na digitálních technologiích.[296] Netwalker byl jedním z nejaktivnějších ransomware útoků v té době. Netwalker ransomware, také známý jako MailTo, vyniká mezi jinými ransomwary díky své sofistikované vícefázové útočné strategii.[297] Začíná infiltrací do sítě oběti prostřednictvím různých metod, jako jsou phishingové e-maily, exploatační nástroje, zranitelnosti vzdáleného desktopového protokolu a metody hrubé síly.[298] Jakmile je uvnitř, provádí laterální pohyby napříč sítí a strategicky identifikuje cenná data k zašifrování.[299] Kromě šifrování dat používá techniku dvojité extorze, kdy nejen že šifruje data, ale také exfiltruje[300] citlivé informace a hrozí jejich zveřejněním nebo prodejem, pokud není zaplaceno výkupné.[301]

Útok na Enel, který je subjektem kritické infrastruktury v Itálii, se odehrál v kontextu rostoucího počtu kybernetických útoků na energetický sektor. Energetické společnosti se stávají stále častějším cílem útočníků kvůli své důležitosti pro národní bezpečnost a ekonomiku. Společnost Enel, která má globální přítomnost, je odpovědná za dodávku elektřiny milionům zákazníků, což z ní činí atraktivní cíl pro kybernetické útoky. Nejčastější motivací kybernetických útoků na energetický sektor jsou geopolitické zájmy, finanční zisk a destabilizace cílových

[295] Asure. Cybersecurity: Is the Office Safer than Remote? [online]. *asuresoftware.com.* [cit. 20.06.2024]. https://www.asuresoftware.com/blog/cybersecurity-is-the-office-safer-than-remote/

[296] Baig, Z., Mekala, S. H., Zeadally, S. Ransomware Attacks of the COVID-19 Pandemic: Novel Strains, Victims, and Threat Actors. *IT Professiona*. 2023, roč. 25, č. 5, s. 37.

[297] Baig, Z., Mekala, S. H., Zeadally, S. Ransomware Attacks of the COVID-19 Pandemic: Novel Strains, Victims, and Threat Actors. *IT Professiona*. 2023, roč. 25, č. 5, s. 40.

[298] ibidem

[299] ibidem

[300] Exfiltrace dat je proces, při kterém útočník nelegálně získává a přenáší data z počítače nebo sítě oběti na své vlastní úložiště.

[301] Baig, Z., Mekala, S. H., Zeadally, S. Ransomware Attacks of the COVID-19 Pandemic: Novel Strains, Victims, and Threat Actors. *IT Professiona*. 2023, roč. 25, č. 5, s. 40.

zemí.[302] Státem sponzorované skupiny, jako například ruská GRU prostřednictvím skupiny APT28, se zaměřují na energetickou infrastrukturu s cílem oslabit národní bezpečnost a destabilizovat společnost. [303]

Útok se odehrál v době, kdy byla společnost Enel zapojena do rozsáhlých modernizačních projektů a digitalizace svých operací.[304] Navzdory zavedeným bezpečnostním protokolům a postupům se ukázalo, že úroveň kybernetické bezpečnosti nebyla dostatečná k odvrácení útoku. Tento incident podtrhuje důležitost neustálého zlepšování bezpečnostních opatření, včetně aktualizací systémů, a také potřebu vzdělávání zaměstnanců v oblasti kybernetických hrozeb.

Přestože společnost Enel neuvedla přesné finanční ztráty, tak lze předpokládat, že byly rozsáhlé, jelikož zahrnovaly náklady na výpadky v provozu a obnovu systémů. Společnost navíc utrpěla poškození své reputace jako důvěryhodného poskytovatele energetických služeb, což mohlo ovlivnit její vztahy s klienty a partnery. Nicméně, útok vedl k posílení bezpečnostní kultury ve společnosti, zvýšení povědomí o kybernetických hrozbách a zavedení přísnějších bezpečnostních protokolů, což může do budoucna pomoci při prevenci podobných incidentů.[305]

Nedostatky a úspěchy

Mezi nedostatky patřila neschopnost zabránit útočníkům v přístupu k citlivým datům a neadekvátní ochrana před ransomwarovými útoky (již v červnu daného roku utrpěla společnost kybernetický útok za pomoci ransomwaru Snake[306]). Zásadním problémem byla také absence

[302] DFMG. Kybernetické útoky v energetice [online]. *ceskovdatech.cz.* [cit. 14.05.2024]. https://www.ceskovdatech.cz/clanek/46-kyberneticke-utoky-v-energetice/#article-content

[303] MITRE. APT28 [online]. *MITRE ATT&CK*. [cit. 15.06.2024]. https://attack.mitre.org/groups/G0007/

[304] Enel. Sustainability plan 2024-2026 and results 2023 [online*]. beyondreporting.enel.com.* [cit. 20.06.2024]. https://beyondreporting.enel.com/content/dam/enel-beyondreporting/2023/bds/en/performance-2023/digitalization/pdf/digitalization.pdf

[305] Enel Communications. *Integrated annual report 2020*. Enel SpA, 2021, s. 176.

[306] Ilascu, I. Power company Enel Group suffers Snake Ransomware attack [online]. *bleepingcomputer.com.* [cit. 15.05.2024].

efektivní reakce na incident, což vedlo k tomu, že útočníci mohli vyhrožovat zveřejněním ukradených dat, pokud nebude výkupné zaplaceno.

Na druhé straně lze za úspěch považovat schopnost společnosti Enel udržet kontinuitu poskytování služeb během útoku. Firma dokázala minimalizovat dopady na své zákazníky a pokračovat v provozu navzdory útoku. Tento incident také vedl k výraznému posílení kybernetické bezpečnosti uvnitř společnosti, což snížilo riziko budoucích útoků.[307]

5.1.4 Případ 4: Kybernetický útok na nemocnici v Česku (2020 - Fakultní nemocnice Brno)

Fakultní nemocnice Brno (FN Brno) je jedním z největších a nejvýznamnějších zdravotnických zařízení v České republice. Nachází se v Brně a zahrnuje několik specializovaných pracovišť, která poskytují široké spektrum zdravotnických služeb. Mezi klíčové součásti nemocnice patří Bohunický kampus, Dětská nemocnice a Porodnice.[308] Nemocnice je silně propojena s Masarykovou univerzitou, zejména s její Lékařskou fakultou, a je centrem pro výuku mediků a dalších zdravotnických odborníků.[309] FN Brno také hraje významnou roli v oblasti výzkumu a vývoje, s důrazem na inovace a pokročilé zdravotnické technologie. V rámci své činnosti se nemocnice soustředí také na klinický výzkum a inovace v medicíně, což ji činí důležitým hráčem v oblasti zdravotní péče a vědeckého výzkumu v České republice.[310]

Založena v roce 1998 sloučením několika předních brněnských nemocnic, FN Brno se stala důležitým zdravotnickým centrem, které

https://www.bleepingcomputer.com/news/security/power-company-enel-group-suffers-snake-ransomware-attack/

[307] Enel Communications. *Integrated annual report 2020*. Enel SpA, 2021, s. 100.

[308] Fakultní nemocnice Brno. Prezentační publikace o FN Brno [online]. *fnbrno.cz.* [cit. 06.06.2024]. https://www.fnbrno.cz/prezentacni-publikace-o-fn-brno/f3642

[309] ibidem

[310] Fakultní nemocnice Brno. Spuštění Centra inovací FN Brno s Prusa Research a.s. jako strategickým partnerem – Memorandum o spolupráci [online]. *fnbrno.cz.* [cit. 06.06.2024]. https://www.fnbrno.cz/areal-bohunice/interni-gastroenterologicka-klinika/spusteni-centra-inovaci-fn-brno-s-prusa-research-a-s-jako-strategickym-partnerem-memorandum-o-spolupraci/t7764

poskytuje péči nejen obyvatelům Brna a Jihomoravského kraje, ale i jiných krajů ČR.[311] Nemocnice se specializuje na širokou škálu lékařských oborů, včetně onkologie, kardiologie, pediatrie, gynekologie a porodnictví, a nabízí také komplexní akutní péči a specializované chirurgické zákroky.[312]

Právní úprava a její implementace v České republice

V roce 2020 byla právní úprava kybernetické bezpečnosti v České republice formována zejména zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, který implementoval směrnici NIS.[313] V rámci této legislativy je NÚKIB hlavním orgánem odpovědným za koordinaci a podporu národní kybernetické bezpečnosti.

Kromě směrnice NIS obsahuje česká legislativa také různé nařízení vlády a vyhlášky vydané NÚKIB, které specifikují technické a organizační požadavky na zajištění kybernetické bezpečnosti. V roce 2020 NÚKIB vydal několik varování a doporučení týkajících se aktuálních kybernetických hrozeb, včetně ransomwarových útoků.[314]

---

[311] Fakultní nemocnice Brno. Historie FN Brno [online]. *fnbrno.cz.* [cit. 06.06.2024]. https://www.fnbrno.cz/historie-fn-brno/t5760

[312] Fakultní nemocnice Brno. Areál Bohunice, Jihlavská 20 [online]. *fnbrno.cz.* [cit. 06.06.2024]. https://www.fnbrno.cz/areal-bohunice-jihlavska-20/k274

[313] NÚKIB. Legislativa KB [online]. *nukib.gov.cz.* [cit. 16.06.2024]. https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

[314] NÚKIB. Upozornění na hrozbu ransomware útoků [online]. *nukib.gov.cz.* [cit. 16.06.2024]. https://nukib.gov.cz/cs/infoservis/hrozby/1428-upozorneni-na-hrozbu-ransomware-utoku/; NÚKIB. NÚKIB vydal Varování před hrozbou a doporučil opatření [online]. *nukib.gov.cz.* [cit. 16.06.2024]. https://nukib.gov.cz/cs/infoservis/hrozby/1491-nukib-vydal-varovani-pred-hrozbou-a-doporucil-opatreni/; NÚKIB. Nová vlna vyděračských e-mailů [online]. *nukib.gov.cz.* [cit. 16.06.2024]. https://nukib.gov.cz/cs/infoservis/hrozby/1521-nova-vlna-vyderacskych-e-mailu/; NÚKIB. NXNSAttack - zranitelnost protokolu DNS [online]. *nukib.gov.cz.* [cit. 16.06.2024]. https://nukib.gov.cz/cs/infoservis/hrozby/1438-nxnsattack-zranitelnost-protokolu-dns/; NÚKIB. Upozornění na zranitelnost SAP NetWeaver [online]. *nukib.gov.cz*. [cit. 16.06.2024]. https://nukib.gov.cz/cs/infoservis/hrozby/1595-upozorneni-na-zranitelnost-sap-netweaver/; NÚKIB. Upozornění na zranitelnost Windows DNS server [online]. *nukib*.gov.cz. [cit. 16.06.2024]. https://nukib.gov.cz/cs/infoservis/hrozby/1596-upozorneni-na-zranitelnost-windows-dns-server/; NÚKIB. Upozornění na zranitelnost Zerologon [online]. *nukib.gov.cz.* [cit. 16.06.2024]. https://nukib.gov.cz/cs/infoservis/hrozby/1636-

Před rokem 2020 musely nemocnice, aby byly považovány za prvky základní služby podle vyhlášky č. 437/2017 Sb., mít více než 800 lůžek nebo status traumacentra (např. právě Fakultní nemocnice v Brně). Po útoku byla vyhláška změněna vyhláškou č. 573/2020 Sb., která snížila požadovaný počet lůžek na 400 a zahrnula také vysoce specializovaná centra, urgentní příjmy s minimálně 40 lůžky intenzivní péče a poskytovatele s více než 100 000 unikátními pacienty ročně. Tato změna rozšířila působnost zákona na více nemocnic, které nyní musí dodržovat přísnější pravidla kybernetické bezpečnosti a spolupracovat s NÚKIB.

Vyhláška č. 317/2014 Sb. stanovuje významné informační systémy a jejich určující kritéria. Zároveň definuje, které informační systémy jsou považovány za významné a stanovuje kritéria pro jejich určení.

Nařízení vlády č. 432/2010 Sb. definuje kritéria pro určení prvku kritické infrastruktury, včetně kritické informační infrastruktury. Toto nařízení bylo novelizováno nařízením vlády č. 61/2022 Sb. Sb. s účinností od 22. března 2022. V rámci zdravotnických zařízení se do kritické infrastruktury nemocnice dostaly jen díky vyhlášce č. 437/2017 Sb., protože v nařízení vlády č. 432/2010 Sb. byly stanoveny podmínky příliš neadekvátně. Požadavek na více než 2500 akutních lůžek by nesplňovalo snad žádné zdravotnické zařízení v ČR.[315]

Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a náležitostech hlášení kybernetických bezpečnostních incidentů, specifikuje konkrétní požadavky na technické a organizační zabezpečení informačních systémů. Mezi tyto požadavky patří například pravidelná aktualizace softwaru, školení zaměstnanců a zavedení vhodných nástrojů pro detekci a prevenci kybernetických útoků.

V souvislosti se zákonem o kybernetické bezpečnosti je na místě ještě zmínit vyhlášky, které se týkají využívání cloudových služeb.

---

upozorneni-na-zranitelnost-zerologon/; NÚKIB. Upozornění na zvýšenou aktivitu malwaru Emotet [online]. *nukib.gov.cz.* [cit. 16.06.2024]. https://nukib.gov.cz/cs/infoservis/hrozby/1638-upozorneni-na-zvysenou-aktivitu-malwaru-emotet/; NÚKIB. Upozornění na rizika softwaru firmy SolarWinds [online]. *nukib.gov.cz.* [cit. 16.06.2024]. https://nukib.gov.cz/cs/infoservis/hrozby/1665-upozorneni-na-rizika-softwaru-firmy-solarwinds/

[315] Největší nemocnicí v ČR je Fakultní nemocnice v Motole, která má kolem 2200 lůžek, ale tato kapacita zahrnuje všechna lůžka, nejen ta akutní.

Vyhláška č. 316/2021 Sb. stanovuje požadavky pro zápis do katalogu cloud computingu. Jejím cílem je zajistit, aby poskytovatelé cloudových služeb splňovali určité bezpečnostní požadavky, které jsou rozděleny do různých bezpečnostních úrovní. Jedná se o prováděcí předpis k zákonu č. 365/2000 Sb., o informačních systémech veřejné správy.

Vyhláška č. 315/2021 Sb. definuje bezpečnostní úrovně pro využívání cloud computingu orgány veřejné moci. Stanovuje kritéria pro hodnocení významnosti informačních nebo komunikačních systémů a jejich zařazení do jedné ze čtyř bezpečnostních úrovní, aby orgány veřejné moci mohly využívat cloudové služby splňující příslušné bezpečnostní požadavky.

Vyhláška č. 190/2023 Sb. zavádí bezpečnostní pravidla pro orgány veřejné moci využívající služby poskytovatelů cloud computingu. Vyhláška stanoví specifické požadavky, které musí orgány veřejné moci splňovat při využívání cloudových služeb.

Česká právní úprava kybernetické bezpečnosti má několik slabin, mezi které patří nedostatek odborníků v oblasti kybernetické bezpečnosti. Stát není schopen tyto odborníky adekvátně finančně ohodnotit, což vede k tomu, že mnozí z nich odcházejí do soukromého sektoru, kde jsou jejich dovednosti lépe oceněny.[316] Zákon č. 181/2014 Sb. o kybernetické bezpečnosti, ačkoliv poskytuje základní rámec, je relativně stručný a neřeší všechny aspekty kybernetických hrozeb. Efektivita kontrol a sankcí, které provádí NÚKIB, je dalším slabým místem. I když NÚKIB má pravomoc kontrolovat dodržování stanovených povinností a ukládat nápravná opatření či pokuty, praktická realizace těchto kontrol může být omezená, a ne vždy účinná. Finanční omezení rovněž představují vážný problém.[317] Omezené finanční prostředky na personál a technické vybavení, které jsou nezbytné pro zajištění efektivní kybernetické obrany, limitují schopnost státu čelit kybernetickým hrozbám.

[316] Flek, L. *Právní problémy české kybernetické bezpečnosti*. 2018, diplomová práce, Masarykova univerzita, Právnická fakulta, s. 20.

[317] Procházka, R. *Kontrolní závěr z kontrolní akce 19/26: Budování kybernetické bezpečnosti České republiky*. NKÚ, 2019, s. 4–5.

Proč a jak se útok stal

Kybernetický útok na Fakultní nemocnici v Brně se odehrál v březnu 2020. Útočníci použili ransomware Defray k zašifrování dat nemocnice, čímž vyřadili z provozu klíčové systémy.[318] Tento útok začal tím, že se ransomware dostal do interní sítě nemocnice, pravděpodobně prostřednictvím phishingového e-mailu nebo jiného škodlivého kódu.[319] Jakmile byl ransomware aktivován, začal šifrovat důležité soubory a data, což paralyzovalo provoz nemocnice.

Phishingový e-mail, který obsahoval škodlivý kód, byl pravděpodobně odeslán zaměstnanci nemocnice, který nevědomky otevřel přílohu nebo klikl na odkaz, čímž umožnil ransomwaremu infikovat systém.[320]Tento typ útoku je běžný a spoléhá na lidskou chybu, kdy zaměstnanci nejsou dostatečně vyškoleni, aby rozpoznali phishingové e-maily. Jakmile byl ransomware v systému, začal se šířit do dalších zařízení v síti, šifrovat soubory a způsobovat postupný kolaps počítačových systémů nemocnice.

Zaměstnancům byl zcela odepřen přístup k potřebným datům, což znemožnilo realizaci operací a vyžádalo převoz pacientů do okolních

[318] Horák, J. Obecné ohrožení, vydírání a škoda 150 milionů. Vyšetřování kyberútoku míří do ciziny [online]. *zpravy.akutalne.cz.* [cit. 15.05.2024]. https://zpravy.aktualne.cz/domaci/obecne-ohrozeni-vydirani-a-skoda-150-milionu-vysetrovani-kyb/r~6e02e8a881ad11eb89ccac1f6b220ee8/

[319] Horák, J. Na nemocnici v Brně zaútočil vyděračský virus, špitál povolal krizového IT manažera [online]. *zpravy.akutalne.cz.* [cit. 15.05.2024]. https://zpravy.aktualne.cz/domaci/na-nemocnici-v-brne-zautocil-vyderacsky-virus-spital-povolal/r~ff91a02c6aa011eab1110cc47ab5f122/

[320] Horák, J. Na nemocnici v Brně zaútočil vyděračský virus, špitál povolal krizového IT manažera [online]. *zpravy.akutalne.cz.* [cit. 15.05.2024]. https://zpravy.aktualne.cz/domaci/na-nemocnici-v-brne-zautocil-vyderacsky-virus-spital-povolal/r~ff91a02c6aa011eab1110cc47ab5f122/

nemocnic.[321] Nemocnice o incidentu informovala NÚKIB, který zahájil vyšetřování jako kybernetický útok.[322]

Nemocnice neměla dostatečně kvalitní systém záplatování ani dostatečnou ochranu proti phishingovým útokům. Tato zranitelnost byla, podobně jako u předešlých případů, zneužita útočníky, kteří použili ransomware k zašifrování systémů nemocnice a požadovali výkupné za jejich odšifrování.[323] V nemocnici chybělo adekvátní školení zaměstnanců na rozpoznávání kybernetických hrozeb.

Reakce na tento incident zahrnovala okamžitá opatření ke zmírnění útoku a zlepšení preventivních opatření, což zahrnovalo posílení interních bezpečnostních politik a zvýšení povědomí o kybernetických hrozbách mezi zaměstnanci.[324]

Reakce na kybernetický útok na Fakultní nemocnici Brno v roce 2020 byla rozsáhlá a zahrnovala spolupráci několika klíčových institucí a odborníků. NÚKIB okamžitě po útoku vydal reaktivní opatření zaměřená na ochranu dalších zdravotnických zařízení.[325] Tato opatření zahrnovala zvýšení bezpečnostních standardů a kontrolu zabezpečení IT

[321] Porter, S. Cyberattack on Czech hospital forces tech shutdown during coronavirus outbreak [online]. *healthcareitnews.com.* [cit. 18.05.2024]. https://www.healthcareitnews.com/news/emea/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak

[322] NÚKIB. FN v Brně Bohunicích dnes nahlásila NÚKIBu kybernetický bezpečnostní incident [online]. *nukib.gov.cz.* [cit. 19.06.2024]. https://nukib.gov.cz/cs/infoservis/aktuality/1417-fn-v-brne-bohunicich-dnes-nahlasila-nukibu-kyberneticky-bezpecnostni-incident/

[323] ČT24. Policie odložila případ kybernetického útoku na FN Brno. Nejsou důkazy k obvinění konkrétního pachatele [online]. *ct24.ceskatelevize.cz.* [cit. 15.05.2024]. https://ct24.ceskatelevize.cz/clanek/regiony/policie-odlozila-pripad-kybernetickeho-utoku-na-fn-brno-nejsou-dukazy-k-obvineni-konkretniho-pachate-18896

[324] NÚKIB. NÚKIB vydal reaktivní opatření pro vybrané subjekty ve zdravotnictví [online]. *nukib.gov.cz.* [cit. 19.05.2024]. https://nukib.gov.cz/cs/infoservis/aktuality/1418-nukib-vydal-reaktivni-opatreni-pro-vybrane-subjekty-ve-zdravotnictvi/

[325] ibidem

systémů. NÚKIB také vydal varování o zvýšeném riziku kybernetických útoků na zdravotnická zařízení v kontextu pandemie COVID-19.[326]

Masarykova univerzita (MUNI) poskytla technickou podporu při obnově napadených systémů.[327] IT odborníci a studenti z této univerzity se zapojili do analýzy útoku, identifikace zranitelností a implementace bezpečnostních opatření. Jejich spolupráce přispěla k obnovení funkčnosti nemocnice a posílení celkového zabezpečení.

Nemocnice musela přejít na krizový režim, což zahrnovalo odložení plánovaných operací a přesměrování akutních případů do jiných nemocnic v regionu.[328] [329] Nemocniční personál byl instruován, aby neotevíral počítače a nevyužíval digitální záznamy pacientů, což vedlo k návratu k manuálním metodám práce, včetně psaní receptů a vedení zdravotnické dokumentace ručně.[330]

Po kybernetickém útoku na Fakultní nemocnici Brno byla implementována řada opatření na posílení kybernetické bezpečnosti nemocnic spadajících pod zákon o kybernetické bezpečnosti.[331] Tato opatření měla za cíl snížit riziko opakování takových incidentů.[332] Okamžitá

---

[326] NÚKIB. *Doporučená bezpečnostní opatření k varování ze dne 16. dubna 2020*. NÚKIB, 2020.

[327] MUNI. *Výroční zpráva o činnosti 2020*. Masarykova univerzita, 2021, s. 56.

[328] ČT24. Základní provoz nemocnice v Brně i po kybernetickém útoku funguje, řekl ředitel [online]. *ct24.ceskatelevize.cz.* [cit. 12.05.2024]. https://ct24.ceskatelevize.cz/clanek/domaci/zakladni-provoz-nemocnice-v-brne-i-po-kybernetickem-utoku-funguje-rekl-reditel-52024

[329] FN Brno. Ing. Antonín Koukal: Krizové řízení musí fungovat, bez ohledu na to, jaká je hodina nebo den [online]. *fnbrno.cz.* [cit. 14.05.2024]. https://www.fnbrno.cz/ing-antonin-koukal-krizove-rizeni-musi-fungovat-bez-ohledu-na-to-jaka-je-hodina-nebo-den/t6927

[330] ČT24. Základní provoz nemocnice v Brně i po kybernetickém útoku funguje, řekl ředitel [online]. *ct24.ceskatelevize.cz.* [cit. 12.05.2024]. https://ct24.ceskatelevize.cz/clanek/domaci/zakladni-provoz-nemocnice-v-brne-i-po-kybernetickem-utoku-funguje-rekl-reditel-52024

[331] NÚKIB. NÚKIB vydal reaktivní opatření pro vybrané subjekty ve zdravotnictví [online]. *nukib.gov.cz.* [cit. 16.05.2024]. https://nukib.gov.cz/cs/infoservis/aktuality/1418-nukib-vydal-reaktivni-opatreni-pro-vybrane-subjekty-ve-zdravotnictvi/

[332] ibidem

opatření zahrnovala rychlé změny hesel a omezení neesenciální internetové komunikace, což bylo většinou nemocnic splněno.[333] Kroky plánované na několik dní zahrnovaly zabezpečení záloh a zvýšenou informovanost zaměstnanců o phishingu, kde některé nemocnice měly problémy s plným dodržením.[334] Dlouhodobější opatření na týden a dva týdny zahrnovala skenování systémů na zranitelnosti, zákaz neautorizovaných aplikací a instalaci antivirového softwaru, což bylo rovněž částečně nebo plně splněno.[335]

Na základě zkušeností z tohoto útoku byla zavedena dlouhodobá opatření na zlepšení kybernetické bezpečnosti v českém zdravotnictví. Patří sem pravidelná školení personálu, zlepšení zabezpečení IT systémů, implementace pokročilých bezpečnostních technologií a vytvoření plánů pro rychlou reakci na budoucí incidenty.

Tyto kroky a spolupráce mezi různými institucemi ilustrují významnou snahu o zlepšení kybernetické bezpečnosti a ochrany kritické infrastruktury, zejména v době zvýšeného tlaku na zdravotnická zařízení kvůli pandemii COVID-19.

Okolnosti případu

Kybernetický útok na Fakultní nemocnici v Brně se odehrál v době, kdy nemocnice hrála klíčovou roli v boji proti pandemii COVID-19. To znamenalo, že jakýkoliv narušení provozu mělo potenciálně závažné důsledky pro veřejné zdraví.[336] Útok také upozornil na potřebu silnějších opatření kybernetické bezpečnosti v sektoru zdravotnictví, který byl během pandemie obzvláště zranitelný.

V tomto období se zvýšil počet kybernetických útoků na zdravotnické systémy po celém světě, včetně České republiky. Útoky na nemocnice a zdravotnické instituce byly časté i v jiných evropských zemích,

[333] Kotoučová, H. *Kybernetické útoky na nemocnice a zdravotnické prostředky*. 2021, diplomová práce, Masarykova univerzita, Fakulta sociálních studií, s. 53.

[334] ibidem

[335] ibidem

[336] NÚKIB. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020*. NÚKIB, 2021, s. 3.

jako je Německo[337] a Francie[338]. Tyto útoky často využívaly obdobné techniky, jako jsou phishingové e-maily a ransomware, a měly za cíl paralyzovat zdravotnické systémy a požadovat výkupné. Nemocnice se staly častým cílem hackerů z několika důvodů, které je činí zvláště zranitelnými. Především uchovávají obrovské množství citlivých osobních a zdravotních informací o pacientech.[339] Tyto údaje zahrnují rodná čísla, finanční informace a zdravotní záznamy, které mohou být zneužity k podvodům, vydírání nebo prodeji na černém trhu, což činí nemocnice atraktivním cílem pro kybernetické zločince. Dalším důvodem je to, že nemocnice jsou často více nakloněny rychle zaplatit výkupné, aby obnovily své systémy a minimalizovaly narušení péče o pacienty. Hackeři vědí, že výpadky v nemocnicích mohou ohrozit lidské životy, což zvyšuje pravděpodobnost zaplacení výkupného.[340] To je důležité, protože rychlé obnovení přístupu k datům je pro nemocnice klíčové pro zachování bezpečnosti pacientů. Nemocnice také spravují rozsáhlé sítě propojených lékařských zařízení, což ztěžuje udržování bezpečnosti.[341] Každé zařízení může představovat potenciální vstupní bod pro útočníky.[342] Složitost těchto sítí, a často zastaralé technologie využívané v nemocnicích, zvyšují riziko kybernetických útoků. Navíc mnoho nemocnic trpí nedostatkem financí a odborníků na kybernetickou bezpečnost. To znamená, že

[337] Viz nemocnice v Düsseldorfu

[338] Vitard, A. En pleine pandémie de Covid-19, les Hôpitaux de Paris victimes d'une cyberattaque [online]. *usine-digitale.fr.* [cit. 15.05.2024]. https://www.usine-digitale.fr/article/en-pleine-pandemie-de-covid-19-l-ap-hp-est-victime-d-une-attaque-par-deni-de-service.N944741

[339] Swivel Secure. 9 reasons why healthcare is the biggest target for cyberattacks [online]. *swivelsecure.com.* [cit. 20.06.2024]. https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/

[340] Arcserve. Hackers Have Made Healthcare Their Number One Target: How You Can Protect Your Organization's Data [online]. *arcserve.com.* [cit. 19.06.2024]. https://www.arcserve.com/blog/hackers-have-made-healthcare-their-number-one-target-how-you-can-protect-your-organizations

[341] Swivel Secure. 9 reasons why healthcare is the biggest target for cyberattacks [online]. *swivelsecure.com.* [cit. 20.06.2024]. https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/

[342] ibidem

nemají dostatečné zdroje na implementaci nejnovějších bezpečnostních opatření a na pravidelná školení zaměstnanců, což z nich činí snadnější cíl. Dalším faktorem je potřeba zdravotnického personálu mít rychlý přístup k informacím na různých zařízeních, což vytváří riziko, že bezpečnostní opatření budou obcházena nebo oslabena kvůli potřebě okamžitého sdílení dat.[343] Tento urgentní charakter zdravotnické práce může vést k nižší opatrnosti při používání technologií, což dále zvyšuje zranitelnost nemocnic vůči útokům.

Další okolností bylo, že kybernetické útoky na zdravotnická zařízení se staly častějšími v důsledku zvýšeného používání digitálních technologií ve zdravotnictví.[344] To zahrnovalo elektronické zdravotní záznamy, telemedicínu a další digitální služby, které zvýšily zranitelnost zdravotnických systémů vůči kybernetickým hrozbám.[345] Nemocnice v Brně nebyla výjimkou a její zvýšená závislost na digitálních technologiích znamenala, že byla zranitelnější vůči kybernetickým útokům.

Nedostatky a úspěchy

Nemocnice neměla včasně záplatovaný software, což umožnilo útočníkům využít známé zranitelnosti. Nedostatek povědomí o hrozbách mezi zaměstnanci přispěl k úspěchu útoku, protože phishingové e-maily často slouží jako brána pro malware. Prvotní reakce na kybernetický útok nebyla dostatečně efektivní, přestože nemocnice kontaktovala NÚKIB, tak plná obnova systémů trvala velmi dlouho.[346] Některé klíčové systémy nebyly funkční ani několik týdnů po útoku, což výrazně ovlivnilo schopnost

[343] Swivel Secure. 9 reasons why healthcare is the biggest target for cyberattacks [online]. *swivelsecure.com.* [cit. 20.06.2024]. https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/

[344] He, Y., et al. Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. *J Med Internet Res*. 2021, roč. 23, č. 4, s. 14-15.

[345] Williams, Ch. M., Chaturvedi, R., Chakravarthy, K. Cybersecurity Risks in a Pandemic. *J Med Internet Res*. 2020, roč. 22, č. 9, s. 1-2.

[346] Novotná, H. Před třemi roky zasáhl Fakultní nemocnici Brno kybernetický útok. Systém dodnes není plně obnovený [online]. *irozhlas.cz.* [cit. 15.05.2024]. https://www.irozhlas.cz/zpravy-domov/kyberneticky-utok-nemocnice-brno-obnova-dat_2303132201_gen

nemocnice poskytovat péči.[347] Systémy, jako nemocniční informační systém, byly obnovovány postupně, což vedlo k dlouhodobým omezením provozu.[348]

Úspěchem bylo rychlé kontaktování NÚKIB po identifikaci útoku nemocnice, což zajistilo koordinovanou reakci na zmírnění dopadů útoku. IT tým nemocnice efektivně izoloval infikované systémy a minimalizoval šíření ransomwaru, což umožnilo rychlé obnovení kritických operací. Nemocnice následně posílila své interní bezpečnostní politiky a zvýšila povědomí o kybernetických hrozbách mezi zaměstnanci.[349]

Další úspěch spočíval v rychlé komunikaci s veřejností a pacienty, což pomohlo minimalizovat paniku a zajistit, že pacienti byli rychle přesměrováni do jiných zdravotnických zařízení. Nemocnice také využila externí odborníky na kybernetickou bezpečnost, aby pomohli s obnovou systémů a posílením jejich zabezpečení.[350] Nemocnice obdržela pomoc od odborníky z NÚKIB a specialistu ze Všeobecné fakultní nemocnice v Praze.[351] Tito experti pomohli s analýzou útoku, identifikací zranitelností a implementací bezpečnostních opatření.

5.2 Závěr případové studie

Tato případová studie poskytla vhled do kybernetických útoků na kritickou infrastrukturu v různých sektorech a zemích EU. Analýza čtyř konkrétních incidentů – útok na Deutsche Bahn v Německu, útok na nemocnici v Düsseldorfu, ransomware útok na Enel v Itálii a kybernetický útok na Fakultní nemocnici v Brně – odhalila různé aspekty kybernetické

[347] ibidem

[348] ibidem

[349] NÚKIB. NÚKIB a CZ.NIC nabízí pomoc nemocnicím v oblasti kyber bezpečnosti [online]. *nukib.gov.cz*. [cit. 15.05.2024]. https://nukib.gov.cz/cs/infoservis/aktuality/1420-nukib-a-cz-nic-nabizi-pomoc-nemocnicim-v-oblasti-kyber-bezpecnosti/

[350] Horák, J. Na nemocnici v Brně zaútočil vyděračský virus, špitál povolal krizového IT manažera [online]. *zpravy.akutalne.cz*. [cit. 15.05.2024]. https://zpravy.aktualne.cz/domaci/na-nemocnici-v-brne-zautocil-vyderacsky-virus-spital-povolal/r~ff91a02c6aa011eab1110cc47ab5f122/

[351] ibidem

bezpečnosti a zranitelnosti, které jsou klíčové pro zajištění kontinuity služeb v těchto klíčových sektorech.

Studie ukázala, že zranitelnosti ve starších systémech a opožděné aktualizace bezpečnostních záplat jsou častými příčinami úspěšných kybernetických útoků. Příkladem je útok na Deutsche Bahn, kde zpožděná implementace bezpečnostních záplat vedla k rozsáhlému narušení provozu. Útoky na nemocnice v Düsseldorfu a Brně poukázaly na kritickou důležitost efektivního krizového řízení a komunikačních strategií. Rychlá reakce a koordinace s jinými zdravotnickými zařízeními pomohly minimalizovat škody a zajistit péči pro pacienty. Incidenty v energetickém sektoru, jako útok na Enel, zdůrazňují nutnost pravidelných bezpečnostních auditů a školení zaměstnanců. Organizace musí neustále zvyšovat povědomí o kybernetických hrozbách a zlepšovat své schopnosti reagovat na incidenty.

Analýza ukázala, že reakce na kybernetické útoky se liší napříč různými sektory a zeměmi. Německo, navzdory snahám o silný právní rámec, čelí významným výzvám spojeným s financováním a implementací bezpečnostních opatření, podobně jako Itálie. Nejen tyto země mají potíže se zabezpečením adekvátních finančních prostředků na modernizaci svých systémů a na zajištění účinných preventivních opatření. Česká republika, díky NÚKIB a jeho aktivitám, dosáhla určitého pokroku, ale stále čelí výzvám v oblasti implementace pokročilých bezpečnostních technologií a zajištění dostatečného financování. Zásadní je zavedení dlouhodobých preventivních opatření, jako jsou modernizace IT systémů, implementace pokročilých bezpečnostních technologií a zavedení robustních plánů obnovy po havárii a kontinuity podnikání.

Pro zlepšení kybernetické bezpečnosti je nezbytné zajistit pravidelné aktualizace a záplaty všech IT systémů a zařízení, aby se minimalizovalo riziko zneužití zranitelností. Organizace musí mít dobře připravené krizové plány a pravidelně provádět cvičení, která simulují kybernetické útoky, aby byli zaměstnanci připraveni na reálné incidenty. Investice do kybernetické bezpečnosti, včetně modernizace infrastruktury a školení zaměstnanců, by měly být zvýšeny. Zlepšení mezinárodní spolupráce a sdílení informací o kybernetických hrozbách může pomoci lépe reagovat na globální kybernetické útoky.

Případová studie ukázala, že kybernetická bezpečnost je dynamickým a komplexním polem, které vyžaduje neustálou pozornost, investice a spolupráci mezi veřejným a soukromým sektorem. Implementace

nových právních rámců, jako jsou nařízení CRA, směrnice NIS 2 a směrnice CER, může významně přispět k posílení kybernetické bezpečnosti kritické infrastruktury v Evropě.

Dle povinností nařízení CRA, které bylo rozebráno v podkapitole 4.3 teoretické části, se požaduje provádění bezpečnostních hodnocení a poskytování aktualizací, což by zajistilo, že nové produkty a systémy zůstanou zabezpečené proti novým hrozbám. V případě Deutsche Bahn by to znamenalo, že nové komponenty a systémy zavedené do jejich infrastruktury by měly vyšší úroveň zabezpečení již od výroby, což by snížilo riziko podobných útoků v budoucnu. Výrobci také budou muset provádět důkladné bezpečnostní hodnocení svých produktů, aby identifikovali a opravili potenciální zranitelnosti předtím, než se produkty dostanou na trh. To zajistí, že nové produkty nebudou obsahovat známé zranitelnosti, které by mohly být zneužity. Tento krok by tedy významně přispěl k bezpečnosti digitálních prvků v železniční infrastruktuře, jako je Deutsche Bahn, a minimalizoval by riziko, že produkty s nezajištěnými zranitelnostmi budou nasazeny do provozu. Dále budou muset výrobci poskytovat pravidelné bezpečnostní aktualizace a podporu po celou dobu životního cyklu produktů. To pomůže udržovat produkty zabezpečené i proti nově objeveným hrozbám a zranitelnostem. Tento požadavek by napomohl v tom, že i po nasazení nových systémů by Deutsche Bahn a další společnosti mohly pravidelně aktualizovat své systémy, čímž by se předešlo situacím, kdy jsou zneužívány zranitelnosti starších systémů. Ovšem zde je nutné, aby samy společnosti dbaly na nutnost aktualizací pro udržení dostatečné kybernetické bezpečnosti ve svém podniku.

Nařízení CRA zavádí povinnost pro výrobce informovat uživatele o úrovni kybernetické ochrany, kterou jejich produkty poskytují, a o postupech pro bezpečné nastavení produktů po jejich zakoupení. To zvyšuje informovanost uživatelů a jejich schopnost chránit se před kybernetickými hrozbami. Pro Deutsche Bahn a další uživatele by to znamenalo lepší přehled o bezpečnostních funkcích jejich systémů a možnost implementovat doporučená bezpečnostní opatření, čímž by se zvýšila celková úroveň ochrany.

Směrnice NIS 2 rozšiřuje rozsah působnosti na více sektorů a typů kritických entit, což znamená, že více organizací bude muset dodržovat přísné kybernetické standardy. Tento krok by zajistil, že i organizace, které nebyly dosud zahrnuty v původní směrnici NIS, budou muset

implementovat pokročilá bezpečnostní opatření a pravidelně provádět bezpečnostní audity. Směrnice NIS 2 zavádí přísnější požadavky na řízení kybernetických rizik. Organizace budou muset provádět pravidelná hodnocení rizik, identifikovat a chránit svá kritická aktiva a mít připravené plány na reakci a obnovu po incidentech. Tento požadavek by vedl k celkové lepší připravenosti organizací na kybernetické útoky a snížil by jejich dopad na provoz. Jednou z významných změn je zlepšení požadavků na hlášení kybernetických incidentů. Organizace budou muset rychle a efektivně informovat příslušné orgány o kybernetických incidentech, což umožní lepší koordinaci a reakci na úrovni celé EU. To by vedlo k rychlejší a efektivnější reakci na kybernetické hrozby a minimalizaci škod. Ovšem implementace těchto opatření by v praxi znamenala zvýšené nároky na finanční a lidské zdroje organizací. Zatímco větší organizace mohou mít dostatečné prostředky na zavedení a udržování těchto opatření, menší a střední podniky mohou čelit značným finančním výzvám. Náklady na pravidelné bezpečnostní audity, školení zaměstnanců a modernizaci IT systémů mohou být pro mnoho organizací obtížně zvládnutelné. Navíc, administrativní zátěž spojená s dodržováním těchto předpisů může vést k zmatkům a obtížím při jejich implementaci.

Směrnice CER by mohla pomoci zlepšit odolnost kritických infrastruktur tím, že by členské státy musely vypracovat národní strategie a pravidelně provádět hodnocení rizik. To by umožnilo lépe identifikovat a řešit rizika v sektorech jako je energetika, což by mohlo pomoci firmám jako Enel lépe chránit svou infrastrukturu před kybernetickými hrozbami. Energetické společnosti by musely zavést systémy pro monitorování a řízení kybernetických hrozeb a pravidelně školit zaměstnance, což by snížilo riziko úspěšných kybernetických útoků.

Implementace těchto nových právních předpisů může v praxi přinést několik konkrétních přínosů. Organizace budou muset zavést komplexní bezpečnostní opatření, pravidelně provádět bezpečnostní audity a školit své zaměstnance, což povede k celkovému zvýšení úrovně kybernetické bezpečnosti. Nicméně, náklady na implementaci těchto opatření mohou být značné, zejména pro menší organizace. Tyto finanční výzvy mohou vést k nerovnoměrné úrovni zabezpečení napříč sektory a mohou zhoršit situaci pro organizace, které již nyní bojují s nedostatkem zdrojů.

Finanční podpora pro implementaci pokročilých bezpečnostních opatření by mohla pomoci menším společnostem a organizacím, které

nemají dostatek zdrojů na investice do kybernetické bezpečnosti. EU by mohla lépe propagovat stávající fondy a programy, popřípadě vytvořit nové na podporu těchto investic, což by zvýšilo celkovou úroveň bezpečnosti v Evropě.[352] [353]

EU by mohla hrát klíčovou roli v podpoře těchto organizací prostřednictvím efektivnější propagace stávajících fondů a programů zaměřených na kybernetickou bezpečnost. V současné době existují různé iniciativy, které však nemusí být dostatečně známé nebo dostupné pro všechny potenciální příjemce. Lepší informovanost a snadnější přístup k těmto prostředkům by mohly umožnit širší využití těchto programů a tím posílit bezpečnostní infrastrukturu napříč celou Evropou.

Komplexnost a administrativní zátěž spojená s dodržováním nových předpisů může také vést k zmatkům a obtížím při jejich implementaci. Navíc různé přístupy k transpozici a implementaci na národní úrovni mohou způsobit nesoulad a problémy při harmonizaci těchto pravidel napříč členskými státy EU, což může komplikovat situaci pro mezinárodní firmy.

Kybernetická bezpečnost kritické infrastruktury je zásadní pro zajištění stability a bezpečnosti evropských států. Analyzované případy ukazují, že současné bezpečnostní opatření a postupy nebyly dostatečně efektivní. Nová legislativa EU představuje krok správným směrem, avšak její úspěch bude záviset na důsledné implementaci a dodržování. Především kontrola dodržování daných povinností bude hrát klíčovou roli. Kromě technologických opatření je podstatné i vzdělávání a informovanost zaměstnanců, což může výrazně přispět k prevenci úspěšných kybernetických útoků.

I přes tyto výzvy, nové právní rámce představují důležitý krok k vyšší odolnosti a bezpečnosti kritické infrastruktury v Evropě, což může významně přispět k lepší ochraně proti kybernetickým hrozbám v budoucnu. Implementace těchto předpisů v České republice by měla přinést zlepšení v oblasti kybernetické bezpečnosti, zvýšení investic do

[352] European Commission. Digital Europe Programme [online]. *commission.europa.eu.* [cit. 06.06.2024]. https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/digital-europe-programme_en

[353] European Commission. Internal Security Fund [online]. *commission.europa.eu.* [cit. 06.06.2024]. https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/internal-security-fund_en

bezpečnostních technologií a větší důraz na vzdělávání a informovanost zaměstnanců o aktuálních hrozbách. Tyto kroky jsou klíčové pro posílení obranyschopnosti proti kybernetickým útokům a zajištění kontinuity provozu kritické infrastruktury.

Zvýšení školení zaměstnanců v oblasti kybernetické bezpečnosti je klíčovým opatřením, které může významně přispět k ochraně organizací před kybernetickými hrozbami. Školení zaměstnanců je důležité, protože lidský faktor je často nejslabším článkem v bezpečnostním řetězci. Zaměstnanci, kteří nejsou dostatečně informováni o kybernetických hrozbách, mohou neúmyslně otevřít škodlivé přílohy v e-mailech, navštívit nebezpečné webové stránky nebo sdílet citlivé informace s neoprávněnými osobami. Školení zaměstnanců je účinný nástroj, jak prokazatelně seznámit zaměstnance s jejich povinnostmi a zvýšit jejich povědomí o bezpečnostních politikách a postupech organizace. Nicméně v praxi naráží tento proces na několik významných problémů.

Jedním z hlavních problémů je formální přístup k školení. Běžná praxe zahrnuje školení pouze jednou za rok.[354] Ty navíc často probíhají formou videí nebo prezentací. Takový přístup však neumožňuje dostatečně efektivní osvojení znalostí a dovedností potřebných k reálnému zajištění bezpečnosti. Výsledky experimentu z článku „Bezpečnost ICT ve vnitřních předpisech a školení zaměstnanců“ ukázaly, že videa mají výrazně nižší účinnost ve srovnání s osobními prezentacemi, které umožňují interaktivní formu výuky a okamžité odpovědi na otázky zaměstnanců.[355]

Dalším problémem je nedostatečná frekvence a kontinuita školení. Školení často neodráží aktuální změny v bezpečnostních politikách a technologiích. Zaměstnanci tedy nejsou průběžně informováni o nových hrozbách a způsobech jejich mitigace, což vede ke snižování úrovně jejich připravenosti na bezpečnostní incidenty.

Organizace také čelí výzvám při implementaci praktických simulací a testů, které jsou klíčové pro hlubší pochopení a osvojení bezpečnostních zásad. Experimenty s řízenými phishingovými kampaněmi nebo

[354] Loutocký, P., Malinka, K. Bezpečnost ICT ve vnitřních předpisech a školení zaměstnanců. *Revue pro právo a technologie*. 2016, roč. 14, č. 4, s. 59.

[355] Loutocký, P., Malinka, K. Bezpečnost ICT ve vnitřních předpisech a školení zaměstnanců. *Revue pro právo a technologie*. 2016, roč. 14, č. 4, s. 61.

simulacemi neohlášené instalace softwaru ukázaly, že zaměstnanci často nereagují správně na tyto situace, což poukazuje na potřebu častějších a realističtějších tréninků.[356]

Mezi problémy v oblasti školení zaměstnanců v kybernetické bezpečnosti patří nejen nezájem zaměstnanců, ale také finanční zajištění všech povinností kybernetické bezpečnosti. Následují některé návrhy řešení, která mohou organizacím pomoci efektivněji a nákladově úsporněji školit své zaměstnance. Vzdělávání několika zaměstnanců, kteří se pak stanou interními školiteli a budou moci školit ostatní kolegy, může být nákladově efektivní.[357] Tento model "train-the-trainer" minimalizuje potřebu externích školitelů a umožňuje organizacím lépe využít své interní zdroje. Implementace nízkonákladových simulací a praktických cvičení, jako jsou řízené phishingové kampaně, může být efektivní metodou výcviku.[358] Tato cvičení mohou být prováděna interně s minimálními náklady, ale s vysokým dopadem na zlepšení bezpečnostního povědomí zaměstnanců. Namísto velkých ročních školení mohou organizace zavést pravidelné krátké aktualizace a mikroškolení, které jsou zaměřeny na konkrétní bezpečnostní problémy. Tato forma školení je časově méně náročná a může být lépe integrovatelná do běžné pracovní rutiny, čímž zvyšuje efektivitu a udržitelnost vzdělávání. Menší organizace mohou spolupracovat a sdílet zdroje na školení s jinými organizacemi nebo se zapojit do komunitních programů. Tímto způsobem mohou sdílet náklady a přístup k vyšší kvalitě školení, což jim umožňuje dosáhnout lepších výsledků i při omezeném rozpočtu.

Celkově tedy, i když je školení zaměstnanců v oblasti kybernetické bezpečnosti nezbytné, je jeho efektivní provedení v praxi velmi problematické. Organizace musí investovat nejen do obsahu školení, ale také do

---

[356] Loutocký, P., Malinka, K. Bezpečnost ICT ve vnitřních předpisech a školení zaměstnanců. *Revue pro právo a technologie*. 2016, roč. 14, č. 4, s. 59–61.

[357] Association for Talent Development. What Is Train the Trainer? [online]. *td.org*. [cit. 20.06.2024]. https://www.td.org/talent-development-glossary-terms/what-is-train-the-trainer

[358] TheinSecurity. Vzdělávejte své zaměstnance pomocí simulace phishingu [online]. *thein.eu*. [cit. 20.06.2024]. https://www.thein.eu/media/filer_public/76/33/763378bf-1e7c-4697-8c83-bff85c8fa39c/theinsecurity_phishingove_kampane.pdf

metod a frekvence jeho provádění, aby bylo možné dosáhnout požadované úrovně bezpečnosti.

Celkově lze říci, že k dosažení vysoké úrovně kybernetické bezpečnosti je nutná kombinace technických a lidských opatření. Implementace nové legislativy a zvýšené investice do kybernetické bezpečnosti jsou nezbytné k ochraně kritické infrastruktury v EU před rostoucími hrozbami kybernetických útoků. V průběhu roku 2020 proběhlo více útoků na zdravotnické instituce a v roce 2023 na bankovní sektor, což zdůrazňuje zranitelnost těchto sektorů vůči kybernetickým hrozbám. Tato vlna útoků poukazuje na potřebu komplexního přístupu k zabezpečení zdravotnických zařízení a bank, které často uchovávají citlivá data.

Tato studie byla omezena několika faktory, které ovlivnily její rozsah a hloubku. Za prvé, nové právní předpisy týkající se kybernetické bezpečnosti nebyly dosud plně implementovány, což znemožňuje posouzení jejich účinnosti v praxi. Bez možnosti sledovat reálné aplikace těchto předpisů není možné jednoznačně hodnotit jejich dopady na kybernetickou situaci v zemi.

Za druhé, nebylo možné získat přístup k některým interním dokumentům nemocnic a společností a jednotlivých úřadů, které by mohly poskytnout podrobnější pohled na průběh vyšetřování kybernetických útoků a reakční postupy těchto institucí. Tento nedostatek omezených dat komplikuje přesné zhodnocení reakční rychlosti a efektivity opatření přijatých v konkrétních případech.

Pro budoucí výzkum je zásadní monitorovat implementaci nových právních předpisů a sledovat, jak jsou aplikovány v praxi. Důležité je hodnotit jejich dopady na reakční dobu a efektivitu kybernetických opatření. Další klíčovou oblastí je průběžná analýza nových kybernetických útoků na kritickou infrastrukturu. Tento přístup umožní identifikovat nové trendy a zranitelnosti, které by mohly být zneužity. Dalším doporučením je hodnocení spolupráce mezi státními institucemi a soukromým sektorem v oblasti kybernetické bezpečnosti. Toto hodnocení pomůže pochopit, jak nové právní předpisy ovlivňují koordinaci a společné úsilí v boji proti kybernetickým hrozbám.

6 Závěr

Tato diplomová práce se zaměřila na analýzu právních nástrojů určených k zajištění kybernetické bezpečnosti kritické infrastruktury. Práce byla strukturována do několika kapitol, které postupně rozvíjely teoretické základy, historický vývoj, současný stav a praktické aplikace právních předpisů v oblasti kybernetické bezpečnosti.

První kapitola poskytla detailní definici základních pojmů a konceptů souvisejících s kybernetickou bezpečností a kritickou infrastrukturou. Byly zde definovány termíny jako kybernetická bezpečnost, kybernetický bezpečnostní incident a kritická infrastruktura. Tato kapitola zdůraznila důležitost těchto pojmů pro pochopení problematiky a jejich aplikaci v praktických situacích. Rovněž byly popsány rozdíly mezi národní a evropskou kritickou infrastrukturou, což pomohlo vytvořit základní rámec pro další analýzu. V této kapitole byly uvedeny praktické příklady kritické infrastruktury, jako je například distribuční společnost ČEZ a evropská přenosová síť ENTSO-E. Byly zde diskutovány konkrétní případy, kdy selhání nebo útok na tyto infrastruktury může mít závažné důsledky pro společnost. Také se věnovala procesem identifikace a určení prvků kritické infrastruktury a evropské kritické infrastruktury. Byly zde popsány jednotlivé fáze tohoto procesu a kritéria, podle kterých jsou prvky hodnoceny a určovány. Kapitola také rozebírala nové přístupy k identifikaci subjektů kritické infrastruktury podle navrhovaného zákona.

Druhá kapitola se zaměřila na historický vývoj kyberbezpečnosti kritické infrastruktury, včetně klíčových legislativních a strategických iniciativ v Evropské unii. Byly zde představeny hlavní milníky, jako je založení agentury ENISA, přijetí směrnice NIS a Cybersecurity Act. Kapitola také diskutovala budoucí výzvy a návrhy na zlepšení kyberbezpečnosti. Historická analýza poskytla kontext pro pochopení, jak se právní rámec vyvíjel a jaké faktory ovlivňovaly jeho formování.

Třetí kapitola se věnovala analýze jednotlivých předpisů týkajících se kybernetické bezpečnosti kritické infrastruktury v rámci Evropské unie. Byly zde rozebrány klíčové legislativní a strategické iniciativy, jako je směrnice NIS 2, Cybersecurity Act a další relevantní předpisy. Kapitola se zaměřila na jejich dopady na národní legislativu a praxi, diskutovala

jejich silné a slabé stránky a poskytla doporučení pro jejich implementaci a další rozvoj.

Čtvrtá kapitola poskytla analýzu kybernetických útoků na kritickou infrastrukturu prostřednictvím vícepřípadové explanatorní studie, která se zaměřila na čtyři významné incidenty: útok na Deutsche Bahn, nemocnici v Düsseldorfu, společnost Enel a Fakultní nemocnici v Brně. Výsledky této analýzy odhalily různé reakce organizací na kybernetické hrozby, identifikovaly zranitelnosti a nabídly doporučení pro zlepšení kybernetické bezpečnosti. Bylo zjištěno, že klíčovými faktory pro úspěšnou obranu proti kybernetickým útokům jsou efektivní krizové řízení, rychlá implementace bezpečnostních opatření a kontinuální aktualizace systémů. Kapitola také zdůraznila význam legislativních opatření, zejména směrnice NIS a dalších relevantních evropských nařízení, a jejich vliv na efektivitu reakcí na kybernetické incidenty. Bylo zřejmé, že legislativní rámec hraje klíčovou roli při formování bezpečnostních strategií a postupů v různých zemích. Srovnání mezi Českou republikou, Itálií a Německem ukázalo na různé přístupy a úrovně připravenosti, což podtrhlo potřebu harmonizace a zlepšení kybernetické bezpečnosti napříč Evropou. Tato analýza poskytla cenné poznatky o slabinách a silných stránkách současných bezpečnostních opatření a nabídla doporučení pro zlepšení kybernetické bezpečnosti kritické infrastruktury.

Na základě provedené analýzy a případových studií bylo zjištěno několik klíčových bodů. Moderní společnost je stále více závislá na digitálních technologiích, což zvyšuje riziko a komplexnost kybernetických útoků. Právní rámec musí být flexibilní a schopný reagovat na nové hrozby. Současná právní úprava je však často nepřehledná a vyžaduje lepší koordinaci a harmonizaci, aby se zamezilo právní nejistotě a zvýšila se efektivita ochrany kritické infrastruktury.

Dalším významným zjištěním byl nedostatek finančních prostředků na zajištění odpovídající úrovně kybernetické bezpečnosti. Mnoho společností čelí výzvám spojeným s omezenými rozpočty na bezpečnostní opatření, což může ohrozit jejich schopnost efektivně reagovat na kybernetické hrozby. To podtrhuje nutnost nejen právní, ale i finanční podpory, aby byla kritická infrastruktura adekvátně chráněna. Nedostatečné finanční zdroje mohou vést k nedostatečnému zabezpečení, což ohrožuje celkovou bezpečnost a stabilitu infrastruktury.

Práce také zdůraznila význam spolupráce mezi vládními a soukromými subjekty, stejně jako investice do nových technologií a postupů.

Sdílení informací a osvědčených postupů může významně přispět k lepší ochraně kritických systémů. Na základě těchto zjištění byla formulována doporučení, která zahrnují zlepšení školení zaměstnanců v oblasti kybernetické bezpečnosti, harmonizaci právních předpisů na národní i unijní úrovni a podporu inovací a výzkumu nových bezpečnostních technologií a metod.

Zvýšení povědomí a pravidelné školení zaměstnanců je zásadní pro posílení obrany proti kybernetickým útokům. Harmonizace právních předpisů zajistí jednotné a efektivní právní prostředí pro ochranu kritické infrastruktury. Podpora výzkumu a vývoje nových technologií a metod pomůže udržet krok s rychle se měnícími kybernetickými hrozbami a podpoří spolupráci mezi akademickou sférou, průmyslem a vládními institucemi.

Dosažení vysoké úrovně kybernetické bezpečnosti kritické infrastruktury je komplexní a neustále se vyvíjející úkol, který vyžaduje koordinované úsilí na všech úrovních společnosti. Právní rámec musí být neustále aktualizován a přizpůsobován novým výzvám, aby byla zajištěna stabilita a bezpečnost v digitálním věku. Tato práce poskytla komplexní přehled o současném stavu právního rámce pro kybernetickou bezpečnost kritické infrastruktury a přispěla k lepšímu porozumění této problematiky v akademickém i praktickém kontextu.

Použité zdroje

1. Adami. M., et al. Summary of First Interim Study Report (D1). In: Adami. M., et al. *Study to support the review of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) - No. 2020- 665*. CEPS, 2021, s. 9-27.
2. AlAnsary, S. A., Latif, R., Saba, T. Multi Factor Authentication as a Service (MFAaaS) for Federated Cloud Environments. In: Daimi, K., Sadoon, A. A. (eds). *Proceedings of the Second International Conference on Innovations in Computing Research (ICR'23).* Springer, 2023, s. 227.
3. Alhazmi, O., Malaiya, Y. *Evaluating Disaster Recovery Plans Using the Cloud*. IEEE, 2013, s. 3-6.
4. Amler, P., Lupač, T. Evropa brání svou digitální budoucnost: Akt o kybernetické odolnosti [online]. *havelpartners.blog.* [cit. 14.05.2024]. https://www.havelpartners.blog/evropa-brani-svou-digitalni-budoucnost-akt-o-kyberneticke-odolnosti
5. Ananda, S., Putranti, I., Dir, A. Analysis Of The EU Cybersecurity Act Under The Theory Of Neoliberal Institutionalism. *Arena Hukum*. 2022, roč. 15, č. 1, s. 189-192.
6. Arcserve. Hackers Have Made Healthcare Their Number One Target: How You Can Protect Your Organization's Data [online]. *arcserve.com.* [cit. 19.06.2024]. https://www.arcserve.com/blog/hackers-have-made-healthcare-their-number-one-target-how-you-can-protect-your-organizations
7. Association for Talent Development. What Is Train the Trainer? [online]. *td.org.* [cit. 20.06.2024]. https://www.td.org/talent-development-glossary-terms/what-is-train-the-trainer
8. Asure. Cybersecurity: Is the Office Safer than Remote? [online]. *asuresoftware.com.* [cit. 20.06.2024]. https://www.asuresoftware.com/blog/cybersecurity-is-the-office-safer-than-remote/
9. Baezner, M., Robin, P. *Cyber and Information warfare in the Ukrainian conflict.* Zürich, 2018, s.15.

10. Baig, Z., Mekala, S. H., Zeadally, S. Ransomware Attacks of the COVID-19 Pandemic: Novel Strains, Victims, and Threat Actors. *IT Professiona*. 2023, roč. 25, č. 5, s. 37-40.
11. Barrat, J., Dupont, H. NIS 2: Developing Cyber Maturity and Compliance through Cyber Risk Quantification (CRQ) [online]. *citalid.com*. [cit. 03.05.2024]. https://citalid.com/resources/nis-2-cyber-directive/
12. Bogoslov, A., Stoica, E. A. Europe's Struggle and Transformation in an Almost Fully Digitized World. *Revista Economică*. 2019, č. 71(4), s. 31-34.
13. Božić, V. *Strengthening Cybersecurity Resilience: Collaborative Efforts in the NIS2 Framework*. 2024, s. 8-9.
14. Božić, V. *The Network and Information Systems (NIS) Directive 2: A Comprehensive Analysis*. 2024, s. 8-14.
15. Brookson, Ch., et al. *Definition of Cybersecurity - Gaps and overlaps in standardisation*. ENISA, 2015, s. 30.
16. Bundeskriminalamt. *Cybercrime: Bundeslagebild 2017*. BKA, 2017, s. 29.
17. Burdova, C. What Is EternalBlue and Why Is the MS17-010 Exploit Still Relevant? [online]. *avast.com.* [cit. 16.06.2024]. https://www.avast.com/c-eternalblue
18. Coker, J. EU Agrees 'Cyber Solidarity Act' to Bolster Incident Response and Recovery [online]. *infosecurity-magazine.com.* [cit. 29.04.2024]. https://www.infosecurity-magazine.com/news/eu-cyber-solidarity-incident/
19. Cyber Risk GmbH. Healthcare - Critical Entities Resilience Directive (CER) [online]. *european-health-data-space.com*. [cit. 20.11.2023]. https://www.european-health-data-space.com/CER_Training.html
20. Cyber Risk GmbH. The Critical Entities Resilience Directive (CER) [online]. *critical-entities-resilience-directive.com*. [cit. 12.04.2024]. https://www.critical-entities-resilience-directive.com/
21. CISA. Cyber-Attack Against Ukrainian Critical Infrastructure [online]. *cisa.gov*. [cit. 15.06.2024]. https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01

22. Cybersecurity and Infrastructure Security Agency. *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-byDesign and -Default*. CISA, 2023, s. 8-9.
23. Cybersecurity and Infrastructure Security Agency. *Shifting the balance of cybersecurity risk: Principles and approaches for secure by design software*. CISA, 2023, s. 4-15.
24. ČEZ. O společnosti [online]. *cezdistribuce.cz*. [cit. 14.05.2024]. https://www.cezdistribuce.cz/cs/o-spolecnosti
25. ČT24. Policie odložila případ kybernetického útoku na FN Brno. Nejsou důkazy k obvinění konkrétního pachatele [online]. *ct24.ceskatelevize.cz.* [cit. 15.05.2024]. https://ct24.ceskatelevize.cz/clanek/regiony/policie-odlozila-pripad-kybernetickeho-utoku-na-fn-brno-nejsou-dukazy-k-obvineni-konkretniho-pachate-18896
26. ČT24. Základní provoz nemocnice v Brně i po kybernetickém útoku funguje, řekl ředitel [online]. *ct24.ceskatelevize.cz.* [cit. 12.05.2024]. https://ct24.ceskatelevize.cz/clanek/domaci/zakladni-provoz-nemocnice-v-brne-i-po-kybernetickem-utoku-funguje-rekl-reditel-52024
27. Deutsche Bahn AG. The foundation of Deutsche Bahn AG [online]. *deutschebahn.com.* [cit. 19.06.2024]. https://www.deutschebahn.com/en/group/history/topics/foundation-6929102#
28. Deutsche Bahn Engineering and Consulting. Sustainable mobility: DB to achieve climate neutrality ten years early [online]. *db-engineering-consulting.com.* [cit. 19.06.2024]. https://db-engineering-consulting.com/en/news/sustainable-mobility-db-to-achieve-climate-neutrality-ten-years-early/
29. Deutsche Bahn. *2017 Integrated Report: Departure into a new era!* Deutsche Bahn AG, 2017, s. 154 a 200.
30. Deutsche Bahn. Business Units [online]. *deutschebahn.com.* [cit. 19.06.2024]. https://www.deutschebahn.com/en/group/business_units
31. Deutsche Bahn. Deutsche Bahn invests a record EUR 7.6 bn in Strong Rail in Germany in 2023 [online]. *deutschebahn.com.* [cit. 19.06.2024]. https://www.deutschebahn.com/en/presse/press_releases/Deutsche-Bahn-invests-a-

record-EUR-7-6-bn-in-Strong-Rail-in-Germany-in-2023-12760244

32. DFMG. Kybernetické útoky v energetice [online]. *ceskovdatech.cz.* [cit. 14.05.2024]. https://www.ceskovdatech.cz/clanek/46-kyberneticke-utoky-v-energetice/#article-content
33. Dionysopoulos, C., et al. Open Letter on the Significance of Free and Open Source Software in the EU's Proposed Cyber Resilience Act [online]. *typo3.org*. [cit. 15.05.2024]. https://typo3.org/fileadmin/t3o_common_storage/documents/press_releases/2023-07_Open_Letter_to_EU_Legislators/Open_Letter_on_the_Significance_of_Free_and_Open_Source_Software_in_the_EU_s_Proposed_Cyber_Resilience_Act.pdf
34. Dunkelberger, D. Understanding the EU Cybersecurity Act and Its Effect on Businesses [online]. *ispartnersllc.com.* [cit. 15.05.2024]. https://www.ispartnersllc.com/blog/eu-cybersecurity-act-effects-businesses/
35. Düsseldorf. Office for Statistics and Elections [online]. *duesseldorf.de.* [cit. 10.06.2024]. https://www.duesseldorf.de/statistik-und-wahlen/statistik-und-stadtforschung/statistics
36. Důvodová zpráva k návrhu zákonu o kritické infrastruktuře [online]. *odok.cz*. [cit. 20.05.2024]. https://odok.cz/portal/veklep/material/ALBSD2AH4CXO/
37. Eckhardt, P., Kotovskaia, A. The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive. *International Cybersecurity Law Review*. 2023, roč. 4, s. 148-158.
38. Enel Communications. *Integrated annual report 2020*. Enel SpA, 2021, s. 100 a 176.
39. Enel. Enel Group [online]. *enel.com.co.* [cit. 12.06.2024]. https://www.enel.com.co/en/the-companies/enel-group.html
40. Enel. Our story [online]. *enel.com.* [cit. 12.06.2024]. https://www.enel.com/company/about-us/our-story
41. Enel. Sustainability plan 2024-2026 and results 2023 [online]. *beyondreporting.enel.com.* [cit. 20.06.2024]. https://beyondreporting.enel.com/content/dam/enel-beyondreporting/2023/bds/en/performance-2023/digitalization/pdf/digitalization.pdf

42. ENISA. Cybersecurity Certification Framework [online]. *enisa.europa.eu.* [cit. 18.05.2024]. https://www.enisa.europa.eu/topics/certification/cybersecurity-certification-framework
43. ENISA. National Cyber Security Strategies - Interactive Map [online]. *enisa.europa.eu.* [cit. 20.06.2024]. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map
44. ENISA. O agentuře ENISA – Agentuře Evropské unie pro kybernetickou bezpečnost [online]. *enisa.europa.eu*. [cit. 16.05.2024]. https://www.enisa.europa.eu/about-enisa/about/cs
45. ENTSO-E. ENTSO-E Mission Statement [online]. *entsoe.eu*. [cit. 20.05.2024]. https://www.entsoe.eu/about/inside-entsoe/objectives/
46. European Commission. Critical infrastructure resilience [online]. *home-affairs.ec.europa.eu*. [cit. 16.04.2024]. https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/protection/critical-infrastructure-resilience_en
47. European Commission. Digital Europe Programme [online]. *commission.europa.eu.* [cit. 06.06.2024]. https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/digital-europe-programme_en
48. European Commission. Internal Security Fund [online]. *commission.europa.eu.* [cit. 06.06.2024]. https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/internal-security-fund_en
49. European Commission. The EU Cyber Solidarity Act [online]. *digital-strategy.ec.europa.eu.* [cit. 24.05.2024]. https://digital-strategy.ec.europa.eu/en/policies/cyber-solidarity
50. European Commission. The EU Cybersecurity Act [online]. *digital-strategy.ec.europa.eu.* [cit. 18.05.2024]. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act
51. European Commission. Tisková zpráva: EU Cybersecurity plan to protect open internet and online freedom and opportunity ze dne 07. února 2013 [online]. *ec.europa.eu.* [cit. 19.05.2024]. https://ec.europa.eu/commission/presscorner/detail/en/IP_13_94

52. European Cyber Security Organisation. *Challenges of the industry to implement the CRA*. ECSO, 2024, s. 7 a 10.

53. European Cyber Security Organisation. *Position paper: Cyber Resilience Act*. ECSO, 2022, s. 2.

54. European Parliamentary Research Service. *Cyber solidarity act*. European Union, 2024, s. 4-7.

55. European Parliamentary Research Service. *ENISA and a new cybersecurity act*. European Union, 2019, s. 11 a 15.

56. Fakultní nemocnice Brno. Areál Bohunice, Jihlavská 20 [online]. *fnbrno.cz.* [cit. 06.06.2024]. https://www.fnbrno.cz/areal-bohunice-jihlavska-20/k274

57. Fakultní nemocnice Brno. Historie FN Brno [online]. *fnbrno.cz.* [cit. 06.06.2024]. https://www.fnbrno.cz/historie-fn-brno/t5760

58. Fakultní nemocnice Brno. Prezentační publikace o FN Brno [online]. *fnbrno.cz.* [cit. 06.06.2024]. https://www.fnbrno.cz/prezentacni-publikace-o-fn-brno/f3642

59. Fakultní nemocnice Brno. Spuštění Centra inovací FN Brno s Prusa Research a.s. jako strategickým partnerem – Memorandum o spolupráci [online]. *fnbrno.cz*. [cit. 06.06.2024]. https://www.fnbrno.cz/areal-bohunice/interni-gastroenterologicka-klinika/spusteni-centra-inovaci-fn-brno-s-prusa-research-a-s-jako-strategickym-partnerem-memorandum-o-spolupraci/t7764

60. Farkač, M. Jednotný digitální trh – atraktivní, leč problematický návrh [online]. *tvorimevropu.cz.* [cit. 25.05.2024]. https://tvorimevropu.cz/2015/04/08/jednotny-digitalni-trh-atraktivni-lec-problematicky-navrh/

61. Federal Office for Information Security. Cyber attack on Düsseldorf University Hospital: BSI warns of acute exploitation of known vulnerability [online]. *bsi.bund.de.* [cit. 28.05.2024]. https://www.bsi.bund.de/DE/Service-Navi/Presse/Pressemitteilungen/Presse2020/UKDuesseldorf_170920.html

62. Federal Office for Information Security. Cyber Security in Healthcare. *BSI Magazine.* 2020, č. 2, s. 13.

63. Federal Office for Information Security. Second Act to Increase the Security of Information Technology Systems [online]. *bsi.bund.de.*

[cit. 28.05.2024]. https://www.bsi.bund.de/DE/Das-BSI/Auftrag/Gesetze-und-Verordnungen/IT-SiG/2-0/it_sig-2-0_node.html

64. Federal Office for Information Security. *The State of IT Security in Germany 2017*. BSI, 2017, s. 26.
65. Fernandez, J. M. Navigating the EU Critical Entities Resilience Directive [online]. *deloitte.com.* [cit. 12.06.2024]. https://www.deloitte.com/lk/en/services/risk-advisory/perspectives/navigating-the-eu-critical-entities-resilience-directive.html
66. Flek, L. *Právní problémy české kybernetické bezpečnosti*. 2018, diplomová práce, Masarykova univerzita, Právnická fakulta.
67. FN Brno. Ing. Antonín Koukal: Krizové řízení musí fungovat, bez ohledu na to, jaká je hodina nebo den [online]. *fnbrno.cz*. [cit. 14.05.2024]. https://www.fnbrno.cz/ing-antonin-koukal-krizove-rizeni-musi-fungovat-bez-ohledu-na-to-jaka-je-hodina-nebo-den/t6927
68. Fordoński, R., Kasprzak, W. WannaCry ransomware cyberattack as violation of international law. *Studia Prawnoustrojowe*. 2019, č. 44, s. 47-48.
69. GFI Software. Enel hit by ransomware [online]. *techgenix.com.* [cit. 15.05.2024]. https://techgenix.com/enel-hit-by-ransomware/
70. Goodin, D. A patient dies after a ransomware attack hits a hospital [online]. *wired.com. [*cit. 16.05.2024]. https://www.wired.com/story/a-patient-dies-after-a-ransomware-attack-hits-a-hospital/
71. Hassan, S., et al. Real-Time Investigation of Cross-Technology Interference in Heterogeneous IoT Networks. *IEEE Access.* 2017, s. 5-9.
72. He, Y., et al. Health Care Cybersecurity Challenges and Solutions Under the Climate of COVID-19: Scoping Review. *J Med Internet Res*. 2021, roč. 23, č. 4, s. 14-15.
73. Headmind Partners. The Cyber Solidarity Act [online]. *headmind.com.* [cit. 16.05.2024]. https://www.headmind.com/en/cyber-solidarity-act/

74. Horák, J. Na nemocnici v Brně zaútočil vyděračský virus, špitál povolal krizového IT manažera [online]. *zpravy.akutalne.cz.* [cit. 15.05.2024]. https://zpravy.aktualne.cz/domaci/na-nemocnici-v-brne-zautocil-vyderacsky-virus-spital-povolal/r~ff91a02c6aa011eab1110cc47ab5f122/

75. Horák, J. Obecné ohrožení, vydírání a škoda 150 milionů. Vyšetřování kyberútoku míří do ciziny [online]. *zpravy.akutalne.cz.* [cit. 15.05.2024]. https://zpravy.aktualne.cz/domaci/obecne-ohrozeni-vydirani-a-skoda-150-milionu-vysetrovani-kyb/r~6e02e8a881ad11eb89ccac1f6b220ee8/

76. Cherepanov, A., Lipovsky, R. BlackEnergy – What We Really Know About the Notorious Cyber Attacks. *Virus Bulletin*. 2016, s. 1-6.

77. Chiara, P. G. The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements. *International Cybersecurity Law Review*. 2022, roč. 3, s. 259 a 270.

78. Chin, K. The EU Cyber Resilience Act: Securing Digital Products [online]. *upguard.com.* [cit. 12.05.2024]. https://www.upguard.com/blog/eu-cyber-resilience-act-cra

79. Ikeda, S. Ransomware Attack at German Hospital Responsible for First Documented Death [online]. *cpomagazine.com.* [cit. 14.05.2024]. https://www.cpomagazine.com/cyber-security/ransomware-attack-at-german-hospital-responsible-for-first-documented-death/

80. Ilascu, I. Power company Enel Group suffers Snake Ransomware attack [online]. *bleepingcomputer.com.* [cit. 15.05.2024]. https://www.bleepingcomputer.com/news/security/power-company-enel-group-suffers-snake-ransomware-attack/

81. IT Governance Ltd. The EU Cybersecurity Act [online]. *itgovernance.co.uk*. [cit. 12.05.2024]. https://www.itgovernance.co.uk/eu-cybersecurity-act

82. Jara, A. J., Martinez, I. C., Sanchez, J. *CyberSecurity Resilience Act (CRA) in practice for IoT devices: Getting ready for the NIS2*. Conference: IEEE Smart Cities Futures Summit, Marrakech, Morocco, 2024, s. 2.

83. Kaspersky. BlackEnergy APT Attacks in Ukraine [online]. *kaspersky.com*. [cit. 15.06.2024]. https://www.kaspersky.com/resource-center/threats/blackenergy

84. Kaspersky. What is WannaCry ransomware? [online]. *kaspersky.com.* [cit. 20.05.2024]. https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

85. Kastrati, B., Pavleski, A., Spasov, N. Cyber-security as an issue of the contemporary security agenda. In: Dujovski, N. (eds). *The strategic and security concept for the countries of southest europe.* International scientific conference, Skopje, 2023, roč. 8, č. 1, s. 303-304.

86. Khomami, N., Solon, O. 'Accidental hero' halts ransomware attack and warns: this is not over [online]. *theguardian.com*. [cit. 17.05.2024]. https://www.theguardian.com/technology/2017/may/13/accidental-hero-finds-kill-switch-to-stop-spread-of-ransomware-cyber-attack

87. Khurshid, A., et al. EU Cybersecurity Act and IoT Certification: Landscape, Perspective and a Proposed Template Scheme. *IEEE Access*. 2022, roč. 10, s. 129934.

88. Kiteworks. Introduction to the EU's Proposed Cyber Resilience Act [online]. *kiteworks.com.* [cit. 15.06.2024]. https://www.kiteworks.com/risk-compliance-glossary/eu-cyber-resiliency-act/

89. Klick, J., Brandstetter, T., Koch, R. Epidemic? The Attack Surface of German Hospitals during the COVID-19 Pandemic. In: Jančárková, T., et al. (eds). *2021 13th International Conference on Cyber Conflict: Going viral.* Tallinn, Estonia, NATO CCDCOE Publications, 2021, s. 74 a 89.

90. Knight, B. How to save Germany's hospitals [online]. *dw.com.* [cit. 15.05.2024]. https://www.dw.com/en/how-to-save-germanys-hospitals/a-63634230

91. Kohler, C. The EU Cybersecurity Act and European standards: an introduction to the role of European standardization. *International Cybersecurity Law Review*. 2020, roč. 1, s. 7-11.

92. Kotoučová, H. *Kybernetické útoky na nemocnice a zdravotnické prostředky*. 2021, diplomová práce, Masarykova univerzita, Fakulta sociálních studií.

93. Kowalski, B., Intemann, M., Mühlenbruch, T. Bedeutung des Cybersecurity Acts für die IT-Sicherheitszertifizierung in Deutschland und Europa. *Schwerpunkt*. 2021, roč. 45, s. 247-248.

94. Kritická infrastruktura v ČR: Přehled klíčových odvětví a jejich význam pro stát [online]. *arpki.cz*. [cit. 16.04.2024]. https://www.arpki.cz/kriticka-infrastruktura/kriticka-infrastruktura/

95. Kumar, A., Prasad, P. Business continuity plan. *South Asian Journal of Engineering and Technology*. 2020, č. 102, s. 1-2.

96. Lété, B. The Relevance of Multistakeholder Input for the EU Cybersecurity Strategy. In: Lété, B. *Implementing the EU Cybersecurity Strategy.* The European Cyber Agora, 2021, s. 9.

97. Limbergová, Z. Akt o kybernetické odolnosti. *Revue pro právo a technologie*. 2023, roč. 14, č. 27, s. 8.

98. Liu, Z., et al. Working Mechanism of Eternalblue and Its Application in Ransomworm. In: Chen, X., Shen, J., Susilo, W. (eds). *Cyberspace Safety and Security.* Xi'an, China, 2022, 14th International Symposium, s. 178-180.

99. Loutocký, P., Malinka, K. Bezpečnost ICT ve vnitřních předpisech a školení zaměstnanců. *Revue pro právo a technologie*. 2016, roč. 14, č. 4, s. 59–61.

100. Manjezi, Z., Botha, R. A. Preventing and Mitigating Ransomware. In: Venter, H., et al. (eds). *Information Security.* Pretoria, South Africa, 17th International Conference, ISSA 2018, s. 155-157.

101. MergeBase. EU Cybersecurity Act [online]. *mergebase.com*. [cit. 15.05.2024]. https://mergebase.com/compliance/eu-cybersecurity-act/

102. Mikac, R. Protection of the EU's Critical Infrastructures: Results and Challenges. *Applied Cybersecurity & Internet Governance*. 2023, roč. 2, č. 1, s. 13.

103. Miliard, M. Hospital ransomware attack leads to fatality after causing delay in care [online]. *healthcareitnews.com*. [cit. 24.05.2024]. https://www.healthcareitnews.com/news/hospital-ransomware-attack-leads-fatality-after-causing-delay-care

104. MITRE. 2015 Ukraine Electric Power Attack [online]. *MITRE ATT&CK.* [cit. 15.06.2024]. https://attack.mitre.org/campaigns/C0028/

105. MITRE. APT28 [online]. *MITRE ATT&CK.* [cit. 15.06.2024]. https://attack.mitre.org/groups/G0007/

106. Moroz, M. Stanovisko Asociace kritické infrastruktury ČR k Návrhu zákona o odolnosti subjektů kritické infrastruktury a o změně dalších zákonů [online]. *AKI ČR*. [cit. 15.05.2024]. https://www.akicr.cz/2024/03/01/zakon-o-kriticke-infrastrukture-pripominky-aki-cr-k-navrhu-zakona/

107. MUNI. *Výroční zpráva o činnosti 2020.* Masarykova univerzita, 2021, s. 56.

108. Nabto. Understanding the EU Cyber Resilience Act and What It Means for You [online]. *nabto.com*. [cit. 20.06.2024]. https://www.nabto.com/eu-cyber-resilience-act/

109. Nařízení Evropského parlamentu a Rady (EU) 2019/881 ze dne 17. dubna 2019 o agentuře ENISA („Agentuře Evropské unie pro kybernetickou bezpečnost"), o certifikaci kybernetické bezpečnosti informačních a komunikačních technologií a o zrušení nařízení (EU) č. 526/2013.

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

111. National Cyber Security Centre. Secure by Default [online]. *ncsc.gov.uk.* [cit. 15.05.2024]. https://www.ncsc.gov.uk/information/secure-default

112. National Cybersecurity Agency. About ACN [online]. *acn.gov.it.* [cit. 16.06.2024]. https://www.acn.gov.it/portale/en/chi-siamo

113. Návrh Nařízení Evropského parlamentu a Rady o horizontálních požadavcích na kybernetickou bezpečnost produktů s digitálními prvky a o změně nařízení (EU) 2019/1020.

114. Návrh zákona o kritické infrastruktuře.

115. Návrh zákona o kybernetické bezpečnosti.

116. Nonnemann, F. Před mikrofonem: Jak se připravuje nová legislativa o kritické infrastruktuře [online]. *gdpr.cz*. [cit. 27.04.2024]. https://www.gdpr.cz/pred-mikrofonem-jak-se-pripravuje-nova-legislativa-o-kriticke-infrastrukture

117. Nonnemann, F. Před mikrofonem: Nový zákon o kritické infrastruktuře se blíží! [online]. *gdpr.cz*. [cit. 05.06.2024]. https://www.gdpr.cz/pred-mikrofonem-novy-zakon-o-kriticke-infrastrukture-se-blizi

118. Norton Rose Fulbright. WannaCry Ransomware Attack Summary [online]. *dataprotectionreport.com.* [cit. 20.05.2024]. https://www.dataprotectionreport.com/2017/05/wannacry-ransomware-attack-summary/

119. Novotná, H. Před třemi roky zasáhl Fakultní nemocnici Brno kybernetický útok. Systém dodnes není plně obnovený [online]. *irozhlas.cz.* [cit. 15.05.2024]. https://www.irozhlas.cz/zpravy-domov/kyberneticky-utok-nemocnice-brno-obnova-dat_2303132201_gen

120. NÚKIB. *Doporučená bezpečnostní opatření k varování ze dne 16. dubna 2020.* NÚKIB, 2020.

121. NÚKIB. FN v Brně Bohunicích dnes nahlásila NÚKIBu kybernetický bezpečnostní incident [online]. *nukib.gov.cz.* [cit. 19.06.2024]. https://nukib.gov.cz/cs/infoservis/aktuality/1417-fn-v-brne-bohunicich-dnes-nahlasila-nukibu-kyberneticky-bezpecnostni-incident/

122. NÚKIB. Incident Reporting [online]. *nukib.gov.cz.* [cit. 14.06.2024]. https://nukib.gov.cz/en/cyber-security/government-cert/incident-reporting/

123. NÚKIB. Kybernetická bezpečnost [online]. *nukib.gov.cz.* [cit. 25.04.2024]. https://nukib.gov.cz/cs/kyberneticka-bezpecnost/

124. NÚKIB. Legislativa KB [online]. *nukib.gov.cz.* [cit. 16.06.2024]. https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/

125. NÚKIB. Legislativní rada vlády doporučila návrh zákona [online]. *nukib.gov.cz.* [cit. 20.06.2024]. https://nukib.gov.cz/cs/infoservis/aktuality/2125-legislativni-rada-vlady-doporucila-navrh-zakona/

126. NÚKIB. Návrh nového zákona o kybernetické bezpečnosti vstupuje do další fáze [online]. nukib.gov.cz. [cit. 20.06.2024]. https://nukib.gov.cz/cs/infoservis/aktuality/2125-legislativni-rada-vlady-doporucila-navrh-zakona/

127. NÚKIB. Nová vlna vyděračských e-mailů [online]. *nukib.gov.cz.* [cit. 16.06.2024]. https://nukib.gov.cz/cs/infoservis/hrozby/1521-nova-vlna-vyderacskych-e-mailu/

128. NÚKIB. NÚKIB a CZ.NIC nabízí pomoc nemocnicím v oblasti kyber bezpečnosti [online]. *nukib.gov.cz.* [cit. 15.05.2024].

https://nukib.gov.cz/cs/infoservis/aktuality/1420-nukib-a-cz-nic-nabizi-pomoc-nemocnicim-v-oblasti-kyber-bezpecnosti/

129. NÚKIB. NÚKIB vydal reaktivní opatření pro vybrané subjekty ve zdravotnictví [online]. *nukib.gov.cz.* [cit. 19.05.2024]. https://nukib.gov.cz/cs/infoservis/aktuality/1418-nukib-vydal-reaktivni-opatreni-pro-vybrane-subjekty-ve-zdravotnictvi/

130. NÚKIB. NÚKIB vydal Varování před hrozbou a doporučil opatření [online]. *nukib.gov.cz.* [cit. 16.06.2024]. https://nukib.gov.cz/cs/infoservis/hrozby/1491-nukib-vydal-varovani-pred-hrozbou-a-doporucil-opatreni/

131. NÚKIB. NXNSAttack - zranitelnost protokolu DNS [online]. *nukib.gov.cz.* [cit. 16.06.2024]. https://nukib.gov.cz/cs/infoservis/hrozby/1438-nxnsattack-zranitelnost-protokolu-dns/

132. NÚKIB. Upozornění na hrozbu ransomware útoků [online]. *nukib.gov.cz*. [cit. 16.06.2024]. https://nukib.gov.cz/cs/infoservis/hrozby/1428-upozorneni-na-hrozbu-ransomware-utoku/

133. NÚKIB. Upozornění na rizika softwaru firmy SolarWinds [online]. *nukib*.gov.cz. [cit. 16.06.2024]. https://nukib.gov.cz/cs/infoservis/hrozby/1665-upozorneni-na-rizika-softwaru-firmy-solarwinds/

134. NÚKIB. Upozornění na zranitelnost SAP NetWeaver [online]. *nukib.gov.cz.* [cit. 16.06.2024]. https://nukib.gov.cz/cs/infoservis/hrozby/1595-upozorneni-na-zranitelnost-sap-netweaver/

135. NÚKIB. Upozornění na zranitelnost Windows DNS server [online]. *nukib.gov.cz*. [cit. 16.06.2024]. https://nukib.gov.cz/cs/infoservis/hrozby/1596-upozorneni-na-zranitelnost-windows-dns-server/

136. NÚKIB. Upozornění na zranitelnost Zerologon [online]. *nukib.gov.cz.* [cit. 16.06.2024]. https://nukib.gov.cz/cs/infoservis/hrozby/1636-upozorneni-na-zranitelnost-zerologon/

137. NÚKIB. Upozornění na zvýšenou aktivitu malwaru Emotet [online]. *nukib.gov.cz.* [cit. 16.06.2024]. https://nukib.gov.cz/cs/infoservis/hrozby/1638-upozorneni-na-zvysenou-aktivitu-malwaru-emotet/

138. NÚKIB. *Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2020*. NÚKIB, 2021, s. 3.

139. Opinion of the European Economic and Social Committee on the 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: the Digital Agenda for Europe — Driving European growth digitally'. Dokument COM (2012) 784 – v konečném znění.

140. Oxfeldt, M. NIS2 Directive: A key to compliance is business continuity [online]. *keepit.com*. [cit. 16.04.2024]. https://www.keepit.com/blog/nis2-key-to-compliance/

141. Pollard, M. A Case Study of Russian Cyber-Attacks on the Ukrainian Power Grid: Implications and Best Practices for the United States. *Pepperdine Policy Review*. 2024, Vol. 16, článek 1, s. 12.

142. Porter, S. Cyberattack on Czech hospital forces tech shutdown during coronavirus outbreak [online]. *healthcareitnews.com.* [cit. 18.05.2024]. https://www.healthcareitnews.com/news/emea/cyberattack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak

143. Prasad, N., Jain, S. Intelligent Technologies in High-Speed Rail Transit Systems. In: Upadhyay, R. K., Sharma, S. K., Kumar, V. (eds). *Intelligent Transportation System and Advanced Technology*. Springer Singapore, 2024, s. 217.

144. Predescu, S. G., Savu, D., Badea, V. E. Cybersecurity in the Railway Sector. *Romanian Cyber Security Journal*. 2022, roč. 4, č. 2, s. 98.

145. Procházka, R. *Kontrolní závěr z kontrolní akce 19/26: Budování kybernetické bezpečnosti České republiky*. NKÚ, 2019, s. 4-5.

146. Proksch, J. Stanovisko Svazu průmyslu a dopravy ČR k Návrhu zákona o odolnosti subjektů kritické infrastruktury a o změně dalších zákonů (zákon o kritické infrastruktuře) [online]. *Svaz průmyslu a dopravy České republiky*. [cit. 15.05.2024]. https://www.spcr.cz/images/Stanovisko_SP_%C4%8CR_k_n%C3%A1vrhu_z%C3%A1kona_o_KI_final.pdf

147. ProLibertate. Vnitro chystá zásadní omezení lidských práv [online]. *prolibertate.cz*. [cit. 03.05.2024]. https://www.prolibertate.cz/2024/03/vnitro-chysta-zasadni-omezeni-lidskych-prav/

148. Prucková, M. German hospital ransomware attack (2020) [online]. *cyberlaw.ccdcoe.org.* [cit. 13.06.2024].

https://cyberlaw.ccdcoe.org/wiki/German_hospital_ransomware_attack_(2020)

149. Pursiainen, C., Kytömaa, E. From European critical infrastructure protection to the resilience of European critical entities: what does it mean? *Sustainable and Resilient Infrastructure*. 2023, č. 8, s. 89-90.

150. Pursiainen, Ch., Kytömaa, E. Sustainable and Resilient Infrastructure ISSN: (Print) From European critical infrastructure protection to the resilience of European critical entities: what does it mean? *Sustainable and Resilient Infrastructure*. 2022, roč. 8, č. 6, s. 93-94.

151. Ralston, W. The untold story of a cyberattack, a hospital and a dying woman [online]. *wired.com.* [cit. 14.06.2024]. https://www.wired.com/story/ransomware-hospital-death-germany/

152. Ramaswami, A., Boehm, M. Understanding the Cyber Resilience Act: What Everyone involved in Open Source Development Should Know [online]. *linuxfoundation.org*. [cit. 20.06.2024]. https://www.linuxfoundation.org/blog/understanding-the-cyber-resilience-act

153. Rosati, E. The DSM Directive 3 years on: have we found our digital single market yet? *Journal of Intellectual Property Law & Practice.* 2022, roč. 17, č. 5, s. 397-398.

154. Růžková, P. NIS2 a novinky pro české firmy: Co se mění v oblasti kybernetické bezpečnosti [online]. *master.cz.* [cit. 16.05.2024]. https://www.master.cz/blog/nis2-a-novinky-pro-ceske-firmy-co-se-meni-v-oblasti-kyberneticke-bezpecnosti/

155. Řehák, D., Hadáček, L. Metodika jednotného určování zařízení pro výrobu, přenos a distribuci elektřiny národní a evropskou kritickou infrastrukturou a zajišťování fyzické ochrany těchto zařízení. In: Řehák, D., Hadáček, L. *Objektivizace hrozeb a rizik zařízení pro výrobu a přenos elektřiny*. Praha, 2013, s. 8-12.

156. Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu Výboru a Výboru regionů. Strategie pro jednotný digitální trh v Evropě. Dokument COM(2015) 192 - v konečném znění.

157. Selvaraj, K., et al. WannaCrypt ransomware worm targets out-of-date systems [online]. *microsoft.com.* [cit. 18.06.2024]. https://www.microsoft.com/en-us/security/blog/2017/05/12/wannacrypt-ransomware-worm-targets-out-of-date-systems/

158. Schirrmacher, D. Workaround available: Critical vulnerability in Citrix ADC and Gateway [online]. *heise.de.* [cit. 17.05.2024]. https://www.heise.de/news/Workaround-verfuegbar-Kritische-Luecke-in-Citrix-ADC-und-Gateway-4627525.html

159. Schmitz-Berndt, S. Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive. *Journal of Cybersecurity*. 2023, roč. 9, č. 1, s. 9.

160. Schmitz-Berndt, S. Refining the Mandatory Cybersecurity Incident Reporting Under the NIS Directive 2.0: Event Types and Reporting Processes. In: Onwubiko, C., et al. (eds). *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media*. Springer Proceedings in Complexity, Singapore, 2023, s. 344-349.

161. Schmitz-Berndt, S., Chiara, P. G. One step ahead: mapping the Italian and German cybersecurity laws against the proposal for a NIS2 directive. *International Cybersecurity Law Review*. 2022, roč. 3, s. 298-299.

162. Sickinghe, F., Karniyevich, N. CER Directive [online]. *twobirds.com*. [cit. 26.05.2024]. https://www.twobirds.com/en/trending-topics/cybersecurity/rce-directive

163. Sievers, T. Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations. *International Cybersecurity Law Review*. 2021, roč. 2, s. 225-229.

164. Simola, J., et al. Impact of Cyber Security Operations on Hardware Requirements for Stable and Workable Industrial Environments. *International Conference on Cyber Warfare and Security.* 2024, roč. 19, č. 1, s. 350-351.

165. Simsek, A. German hospitals protest lack of funds, warn of looming crisis [online]. *aa.com.tr.* [cit. 14.06.2024]. https://www.aa.com.tr/en/europe/german-hospitals-protest-lack-of-funds-warn-of-looming-crisis/2996922

166. Sinner, F. IT-Sicherheitsgesetz [online]. *link11.com.* [cit. 25.05.2024]. https://www.link11.com/de/glossar/it-sicherheit-sgesetz/

167. Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

168. Směrnice Evropského parlamentu a rady (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES.

169. Sordyl, J. Meeting the Challenges of a Changing Threat Landscape with the CER Directive [online]. *insights.pecb.com*. [cit. 22.05.2024]. https://insights.pecb.com/meeting-the-challenges-of-a-changing-threat-landscape-with-the-cer-directive/

170. Spiegel. 450 railway computers affected by "WannaCry" virus [online]. *spiegel.de.* [cit. 12.05.2024]. https://www.spiegel.de/netzwelt/web/wannacry-450-bahn-computer-von-cyber-attacke-betroffen-a-1147921.html

171. Společná zpráva Evropskému parlamentu a Radě o provádění společného rámce pro boj proti hybridním hrozbám – reakce Evropské unie. Dokument JOIN(2017) 30 - v konečném znění.

172. Společné sdělení Evropskému parlamentu a Radě. Odolnost, odrazování a obrana: budování silné kybernetické bezpečnosti pro EU. Dokument JOIN(2017) 450 - v konečném znění.

173. Společné sdělení Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a výboru regionů. Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor. Dokument 52013JC0001 – v konečném znění.

174. Swivel Secure. 9 reasons why healthcare is the biggest target for cyberattacks [online]. *swivelsecure.com.* [cit. 20.06.2024]. https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/

175. Šilarová, J. Jak se připravit na NIS2: Nový zákon o kybernetické bezpečnosti pro střední a velké podniky [online]. *alvao.com.* [cit. 18.05.2024]. https://www.alvao.com/cs/blog/jak-se-pripravit-na-nis2

176. Šimsa, P., Michalcová, L., Ptáček, O. Směrnice NIS2 a nový Zákon o kybernetické bezpečnosti [online]. *pwc.com.* [cit. 03.06.2024]. https://www.pwc.com/cz/cs/temata/smernice-nis2.html

177. Šlekytė, I. What is Netwalker ransomware? [online]. *nordvpn.com.* [cit. 16.05.2024]. https://nordvpn.com/blog/netwalker-ransomware/

178. Štorek, D. Pracoviště typu CSIRT a CERT v Evropě. *Ochrana & Bezpečnost.* 2018, roč. 7, č. 1, s. 51.

179. The University Hospital of Düsseldorf. About us [online]. *uniklinik-duesseldorf.de.* [cit. 10.06.2024]. https://www.uniklinik-duesseldorf.de/international-patients/english/about-us

180. The University Hospital of Düsseldorf. History of the University Hospital Düsseldorf [online]. *uniklinik-duesseldorf.de.* [cit. 12.05.2024]. https://www.uniklinik-duesseldorf.de/ueber-das-ukd/geschichte-des-ukd

181. The University Hospital of Düsseldorf. Innovation and transparency [online]. *uniklinik-duesseldorf.de*. [cit. 10.06.2024]. https://www.uniklinik-duesseldorf.de/ueber-das-ukd/unternehmen

182. TheinSecurity. Vzdělávejte své zaměstnance pomocí simulace phishingu [online]. *thein.eu.* [cit. 20.06.2024]. https://www.thein.eu/media/filer_public/76/33/763378bf-1e7c-4697-8c83-bff85c8fa39c/theinsecurity_phishingove_kampane.pdf

183. Thouvenin, F., Tamò-Larrieux, A. Data Ownership and Data Access Rights: Meaningful Tools for Promoting the European Digital Single Market? In: Burri, M. (eds). *Big Data and Global Trade Law*. Cambridge University Press, 2021, s. 319.

184. Tugnoli, F., et al. At a glance: cybersecurity best practices in Italy [online]. *lexology.com.* [cit. 14.05.2024]. https://www.lexology.com/library/detail.aspx?g=d3975429-3d0d-4b24-b9c0-9102f2cc9f5e

185. Two Birds. Cyber Solidarity Act [online]. *twobirds.com.* [cit. 15.05.2024]. https://www.twobirds.com/en/capabilities/practices/digital-rights-and-assets/european-digital-strategy-developments/cybersecurity/cybersecurity/cyber-solidarity-act

186. Two Birds. The EU Cybersecurity Act [online]. *twobirds.com*. [cit. 15.05.2024]. https://www.twobirds.com/en/capabilities/practices/digital-rights-and-assets/european-digital-strategy-developments/cybersecurity/cybersecurity/the-eu-cybersecurity-act

187. Uniqkey. What Is The NIS2 Directive? [online]. *nis2directive.eu.* [cit. 12. 02.2024]. https://nis2directive.eu/what-is-nis2/

188. Victor, K. Reflective Loading Runs Netwalker Fileless Ransomware [online]. *trendmicro.com.* [cit. 16.06.2024]. https://www.trendmicro.com/en_us/research/20/e/netwalker-fileless-ransomware-injected-via-reflective-loading.html

189. Vitard, A. En pleine pandémie de Covid-19, les Hôpitaux de Paris victimes d'une cyberattaque [online]. *usine-digitale.fr.* [cit. 15.05.2024]. https://www.usine-digitale.fr/article/en-pleine-pandemie-de-covid-19-l-ap-hp-est-victime-d-une-attaque-par-deni-de-service.N944741

190. Vostoupal, J. *Certifikace kyberbezpečnostních technologií*. 2018/2019, diplomová práce, Masarykova univerzita, Právnická fakulta.

191. Williams, Ch. M., Chaturvedi, R., Chakravarthy, K. Cybersecurity Risks in a Pandemic. *J Med Internet Res*. 2020, roč. 22, č. 9, s. 1-2.

192. Young, T. Security by Design and by Decree [online]. *securitycompass.com.* [cit. 19.06.2024]. https://www.securitycompass.com/blog/security-by-design-and-by-decree/

193. Zákon č. 181/2014 Sb., zákon o kybernetické bezpečnosti, ve znění pozdějších předpisů.

194. Zákon č. 240/2000 Sb. o krizovém řízení, ve znění pozdějších předpisů.

195. Zákon č. 240/2000 Sb., krizový zákon, ve znění pozdějších předpisů.

196. Zpráva Komise Evropskému parlamentu a Radě hodnotící konzistentnost přístupů členských států při určování provozovatelů základních služeb v souladu s čl. 23 odst. 1 směrnice 2016/1148/EU o bezpečnosti sítí a informačních systémů. Dokument COM(2019) 546 - v konečném znění.