

Analýza kybernetických hrozeb vybrané infrastruktury

Jan Navrátil

Bakalářská práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav bezpečnostního inženýrství

Akademický rok: 2024/2025

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: Jan Navrátil
Osobní číslo: A22744
Studijní program: B1032A020001 Bezpečnostní technologie, systémy a management
Forma studia: Kombinovaná
Téma práce: Analýza kybernetických hrozeb vybrané infrastruktury
Téma práce anglicky: Analysis of Cyber Threats to Selected Infrastructure

Zásady pro vypracování

- Identifikujte aktiva a relevantní kybernetické hrozby k danému subjektu.
- Zhodnotte zranitelnosti v zabezpečení subjektu.
- Proveďte analýzu rizik na základě hrozeb, zranitelností a jejich dopadů.
- Zohledněte legislativní požadavky při řízení rizik.
- Navrhněte opatření pro snížení identifikovaných rizik.

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. KOLOUCH, Jan a BAŠTA, Pavel. CyberSecurity. CZ.NIC. Praha: CZ.NIC, z.s.p.o., 2019. ISBN 9788088168317. Dostupné také z: <https://knihy.nic.cz/files/edice/cybersecurity.pdf>.
2. SMEJKAL, Vladimír; SOKOL, Tomáš a KODL, Jindřich. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.
3. DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. Řízení kybernetické bezpečnosti a bezpečnosti informací. Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.
4. SEDLÁK, Petr a KONEČNÝ, Martin. Přeměna ISMS v manažerské informatice. Vydání: první. Brno: CERM, akademické nakladatelství, 2023. ISBN 978-80-7623-110-8.
5. RAMEŠOVÁ, Kristina. Právní regulace kybernetické bezpečnosti a její meze. Právní instituty. V Praze: C.H. Beck, 2023. ISBN 978-80-7400-931-0.

Vedoucí bakalářské práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **13. prosince 2024**

Termín odevzdání bakalářské práce: **2. června 2025**

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan



Ing. Jan Valouch, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 13. prosince 2024

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

Beru na vědomí, že

- odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení bakalářské práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – bakalářskou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na bakalářské práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne

.....

podpis autora

ABSTRAKT

Tato bakalářská práce se zabývá analýzou kybernetických rizik u vybrané organizace v kontextu evropské směrnice NIS2 a českého legislativního rámce. Teoretická část definuje klíčové pojmy, kategorizuje kybernetické hrozby a představuje vybrané metody hodnocení rizik. V praktické části jsou identifikována klíčová aktiva organizace a analyzovány relevantní hrozby a zranitelnosti s využitím metod SWOT, What-If a FMEA. Výsledkem práce je návrh konkrétních bezpečnostních opatření, která respektují doporučení směrnice NIS2 a jejichž implementace přispěje ke zvýšení kybernetické odolnosti organizace.

Klíčová slova: kybernetická bezpečnost, analýza rizik, NIS2, SWOT, What-If, FMEA

ABSTRACT

This bachelor's thesis deals with cybersecurity risk analysis in a selected organization within the context of the European NIS2 Directive and the Czech legislative framework. The theoretical part defines key concepts, categorizes cyber threats, and introduces selected risk assessment methods. In the practical part, the organization's critical assets are identified, and relevant threats and vulnerabilities are analyzed using SWOT, What-If, and FMEA methods. The outcome of this thesis is a proposal of specific security measures that align with the recommendations of the NIS2 Directive, and whose implementation will contribute to enhancing the organization's cyber resilience.

Keywords: cybersecurity, risk analysis, NIS2, SWOT, What-If, FMEA

Rád bych poděkoval vedoucímu mé bakalářské práce panu doktorovi Ing. Davidu Malaníkovi, Ph.D., za jeho čas, cenné rady, odborné vedení, vstřícný přístup a trpělivost během celého procesu tvorby práce. Dále děkuji vedení vybrané organizace a pracovníkům odboru informatiky za ochotu, poskytnutí nezbytných informací a umožnění realizace analýzy. V neposlední řadě patří mé poděkování mé partnerce a rodině za jejich trvalou podporu, motivaci a pochopení v průběhu celého studia.

OBSAH

ÚVOD.....	11
I TEORETICKÁ ČÁST	12
1 SOUČASNÝ STAV KYBERNETICKÉ BEZPEČNOSTI V ČESKÉ REPUBLICE.....	13
1.1 VÝZNAM KYBERNETICKÉ BEZPEČNOSTI V PODMÍNKÁCH ČESKÉ REPUBLIKY	13
1.2 VÝZNAMNÉ KYBERNETICKÉ INCIDENTY	16
1.3 DOPADY KYBERNETICKÝCH INCIDENTŮ NA ORGANIZACE A SPOLEČNOST.....	17
1.4 VÝZNAM ANALÝZY RIZIK V OBLASTI KYBERNETICKÉ BEZPEČNOSTI.....	18
2 KYBERNETICKÁ BEZPEČNOST A SOUVISEJÍCÍ POJMY.....	19
2.1 DEFINICE KYBERNETICKÉ BEZPEČNOSTI	19
2.2 PRINCIPY OCHRANY INFORMACÍ (CIA TRIÁDA).....	20
2.3 TYPOLOGIE KYBERNETICKÝCH HROZEB A ZRANITELNOSTÍ.....	22
2.3.1 Klasifikace hrozeb podle původu.....	22
2.3.2 Typy útoků a hrozeb v praxi	23
2.3.3 Typologie zranitelností.....	24
3 ANALÝZA RIZIK V KYBERNETICKÉ BEZPEČNOSTI	27
3.1 ÚLOHA A VÝZNAM ANALÝZY RIZIK	27
3.2 VYMEZENÍ ROZSAHU ANALÝZY	28
3.3 IDENTIFIKACE A OCENĚNÍ AKTIV	29
3.4 IDENTIFIKACE HROZEB A ZRANITELNOSTÍ	31
3.5 PARAMETRY HODNOCENÍ RIZIK	32
3.6 PŘÍSTUPY A METODY ANALÝZY RIZIK.....	34
3.7 NÁVRH OPATŘENÍ PRO ŘÍZENÍ IDENTIFIKOVANÝCH RIZIK	35
4 LEGISLATIVA V OBLASTI KYBERNETICKÉ BEZPEČNOSTI	37
4.1 SMĚRNICE NIS2 A JEJÍ POŽADAVKY	37
4.2 ZÁKON Č. 181/2014 SB., O KYBERNETICKÉ BEZPEČNOSTI (ZoKB).....	38
4.3 NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST	39
4.4 NORMY ISO/IEC ŘADY 27000	41
4.5 NÁRODNÍ STRATEGIE KYBERNETICKÉ BEZPEČNOSTI ČR 2021–2025.....	42
II PRAKTICKÁ ČÁST.....	44
5 CHARAKTERISTIKA VYBRANÉHO SUBJEKTU	45
5.1 ORGANIZAČNÍ STRUKTURA	45
5.2 FYZICKÁ INFRASTRUKTURA A LOKALITA SUBJEKTU	45
5.3 INFORMAČNÍ A KOMUNIKAČNÍ INFRASTRUKTURA	46

6	IDENTIFIKACE AKTIV, HROZEB A ZRANITELNOSTÍ.....	48
6.1	DATOVÁ A APLIKAČNÍ AKTIVA	48
6.2	PROVOZ SÍŤOVÉ INFRASTRUKTURY	49
6.3	KONCOVÁ ZAŘÍZENÍ	50
6.4	LIDSKÉ ZDROJE.....	51
7	ANALÝZA RIZIK.....	53
7.1	DÍLČÍ ZÁVĚR ANALÝZ SWOT A WHAT-IF	53
7.2	POROVNÁNÍ VÝSLEDKŮ ANALÝZ A PRIORITIZACE RIZIK.....	54
8	NÁVRH BEZPEČNOSTNÍCH OPATŘENÍ	56
	ZÁVĚR.....	58
	SEZNAM POUŽITÉ LITERATURY	59
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	63
	SEZNAM PŘÍLOH.....	65

ÚVOD

Kybernetická bezpečnost v posledních letech získává stále větší význam v souvislosti s rostoucí digitalizací procesů, intenzivnějším využíváním cloudových služeb a širším zaváděním vzdáleného přístupu k citlivým datům. Tyto trendy však přinášejí také zvýšené riziko kybernetických incidentů, jejichž důsledky mohou ovlivnit nejen technickou infrastrukturu organizací, ale i kontinuitu poskytovaných služeb, důvěru klientů či uživatelů a právní odpovědnost subjektů. Rostoucí četnost a závažnost incidentů kladou důraz na nutnost systematického a důsledného přístupu k identifikaci, hodnocení a řízení kybernetických rizik.

Evropská unie na tyto výzvy reaguje přijetím směrnice NIS2, která stanovuje jednotné standardy zabezpečení informačních systémů a určuje nové povinnosti pro organizace působící v klíčových sektorech. V České republice je tato směrnice implementována zejména prostřednictvím novelizace zákona č. 181/2014 Sb., o kybernetické bezpečnosti, který zavádí požadavky na proaktivní řízení rizik, jasnou odpovědnost vedení organizací a důraz na prevenci, detekci i reakci na kybernetické hrozby. Zavedení tohoto legislativního rámce znamená, že organizace musí pečlivě analyzovat a přehodnotit svá bezpečnostní opatření, aby zajistily soulad s novými požadavky.

Cílem této bakalářské práce je na základě uvedeného kontextu provést analýzu kybernetických rizik u konkrétní organizace, identifikovat její klíčová informační aktiva a vyhodnotit potenciální hrozby a zranitelnosti. S využitím vybraných analytických metod navrhu technická a organizační opatření, jejichž implementace povede ke zvýšení celkové kybernetické odolnosti organizace v souladu se směrnicí NIS2. Práce je rozdělena na teoretickou část, ve které vymezují klíčové pojmy a metodologii analýzy rizik, a část praktickou, kde aplikují teoretické poznatky na vybranou organizaci a její specifické potřeby v oblasti kybernetické bezpečnosti.

Při tvorbě této práce byl použit velký jazykový model GPT-4.5 od společnosti OpenAI, dostupný prostřednictvím aplikace ChatGPT (<https://chat.openai.com/>). Nástroj byl použit jako podpůrný prostředek pro optimalizaci formální struktury textu, zajištění jazykové správnosti a parafrázování některých odborných informací. Veškeré výstupy byly následně mnou zkontrolovány a plně přebírám odpovědnost za jejich obsah.

I TEORETICKÁ ČÁST

1 SOUČASNÝ STAV KYBERNETICKÉ BEZPEČNOSTI V ČESKÉ REPUBLICE

Problematika kybernetické bezpečnosti je v současném digitálně propojeném světě zásadním tématem, které má dopad na všechny úrovně společnosti, včetně jednotlivců, organizací i státních institucí. Tato kapitola uvádí klíčové souvislosti, v nichž se kybernetická bezpečnost v podmínkách České republiky rozvíjí, představuje reálné incidenty, na jejichž základě lze pochopit závažnost problému, a analyzuje jejich dopady na organizace i společnost jako celek.

1.1 Význam kybernetické bezpečnosti v podmínkách České republiky

Kybernetická bezpečnost představuje v kontextu současné České republiky významný faktor ochrany státní správy, kritické infrastruktury a celospolečenské stability. Význam tohoto oboru vzrostl úměrně s postupující digitalizací veřejného i soukromého sektoru, kdy informační a komunikační technologie začaly plnit základní roli v zajišťování chodu institucí, provozu podniků, ale i každodenních činností občanů. Tento technologický vývoj je provázen rostoucím počtem potenciálních hrozeb, které mohou narušit důvěrnost, dostupnost či integritu informací. Česká republika čelí nejen technickým výzvám, ale i geopolitickému tlaku, zintenzivněnému zejména po roce 2022 v souvislosti s válkou na Ukrajině. Kybernetické útoky se tak stávají častým prostředkem v rámci mocenských strategií i prostředkem pro dosažení kriminálních cílů, přičemž jejich sofistikovanost i četnost podle zpráv Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) v posledních letech trvale narůstá [1].

Tento vývoj je doložen statistickými údaji uvedenými v každoročních zprávách NÚKIB. Zatímco v roce 2020 bylo evidováno 99 kybernetických bezpečnostních incidentů, v roce 2021 jejich počet vzrostl na 157 a o rok později, v roce 2022, činil 146 případů. Přestože se tehdy jednalo o mírný meziroční pokles, již následující rok 2023 přinesl výrazné zvýšení na celkových 262 incidentů, což představuje téměř osmdesátiprocentní meziroční zvýšení. Tento skok je zčásti vysvětlitelný rostoucím počtem nahlášených incidentů neregulovanými subjekty a zároveň vyšší aktivitou organizovaných kyberkriminálních i státem podporovaných aktérů. Pozornost si zaslouží i skutečnost, že se zvýšil počet incidentů směřujících na instituce veřejného sektoru, zejména samosprávy, zdravotnická zařízení či úřady státní správy, které často čelí útokům typu ransomware, DDoS či sofistikovanému phishingu [1; 2; 3; 4].

Nejčastěji se mezi formami útoků vyskytují DDoS kampaně, phishing a ransomwarové útoky. Právě ransomware představuje trvalou hrozbu, neboť cílí na znepřístupnění klíčových systémů prostřednictvím zašifrování dat a následného vydírání. Významné incidenty, jako útok na Fakultní nemocnici Brno v roce 2020 či Psychiatrickou nemocnici Kosmonosy, ukazují, že dopady těchto incidentů mohou být závažné jak po technické, tak po finanční stránce. DDoS útoky, hojně zaznamenávané v letech 2022 a 2023, často souvisely s působením ruských hacktivistických skupin a mířily na české státní instituce, média nebo finanční sektor, přičemž jejich primárním cílem bylo zahlcení služeb a dočasné vyřazení jejich webových rozhraní z provozu. Phishing a jeho sofistikované varianty, jako spear-phishing nebo quishing, se mezitím staly jedním z nejrozšířenějších vektorů útoku, neboť útočníci dokážou zneužít lidskou chybu pro získání přístupových údajů nebo zavedení škodlivého kódu do systémů [1; 2; 4; 5].

Vývoj v České republice odpovídá obecným trendům kybernetických hrozeb, které v širším evropském kontextu shrnuje zpráva Evropské agentury pro kybernetickou bezpečnost (ENISA) za období 2023–2024. Podle této zprávy patří mezi nejzávažnější hrozby v Evropské unii ransomware, malware, DDoS útoky a různé formy sociálního inženýrství, což odpovídá i zkušenostem z České republiky. Zpráva také upozorňuje na nový fenomén, kdy útočníci stále častěji využívají legitimní cloudové služby (Living Off Trusted Sites – LOTS), čímž komplikují efektivní detekci a prevenci hrozeb. Významnou roli přitom hraje geopolitický kontext, zejména rostoucí aktivita hacktivistických skupin, které svou intenzivní činností reagují na významné politické a společenské události, jako jsou například evropské volby nebo konflikt na Ukrajině. Tyto poznatky potvrzují, že výzvy v oblasti kybernetické bezpečnosti, kterým čelí Česká republika, jsou součástí širšího evropského rámce, který je reflektován v aktuálních evropských strategických dokumentech a doporučeních [6].

Na vzrůstající význam kybernetické bezpečnosti ukazuje také rostoucí legislativní a institucionální rámec. Česká republika přijala v roce 2014 zákon č. 181/2014 Sb., o kybernetické bezpečnosti, který stanovil základní povinnosti pro tzv. regulované subjekty. Významný posun v právním rámci představovalo přijetí evropské směrnice NIS2, jejíž implementace v ČR vyústila v přípravu nového zákona o kybernetické bezpečnosti. Tento legislativní posun významně rozšiřuje okruh povinných osob a zpřísňuje požadavky na zabezpečení informačních systémů, zejména v oblasti zdravotnictví, energetiky, digitálních

služeb nebo samospráv. NÚKIB v rámci tohoto procesu spolupracuje s odbornou veřejností, poskytuje metodickou podporu a připravuje také prováděcí předpisy [7].

Významným faktorem, který posiluje potřebu kybernetické bezpečnosti, je stále zjevnější souvislost mezi geopolitickými událostmi a nárůstem kybernetických útoků. Po vypuknutí ozbrojeného konfliktu na Ukrajině v roce 2022 zaznamenal NÚKIB zvýšený počet útoků na české subjekty, které byly motivovány českou podporou Ukrajiny. Útočící skupiny otevřeně deklarovaly svou aktivitu jako odvetu za politické postoje nebo kroky České republiky. V roce 2023 tak byly zaznamenány opakované vlny útoků vedených hacktivistickými skupinami, přičemž nejčastějšími cíli byly vládní instituce, letiště, banky nebo média. Tyto útoky většinou nevedly ke kompromitaci interních systémů, ale způsobily výpadky webových služeb a zvýšily nároky na obranyschopnost dotčených organizací [1; 2].

Neméně důležitou roli v zajištění kybernetické bezpečnosti hraje připravenost organizací, a to jak z hlediska technického zabezpečení, tak i personální a procesní kapacity. Podle zjištění NÚKIB však české instituce stále čelí závažným výzvám. Mezi ně patří zejména nedostatek kvalifikovaných odborníků, nedostatečné mzdové ohodnocení pracovníků ve veřejném sektoru a stagnující rozpočty vyčleňované na oblast bezpečnosti. V roce 2023 deklarovalo téměř 60 % organizací, že jejich finanční prostředky na kybernetickou bezpečnost nejsou dostatečné, a přibližně tři čtvrtiny subjektů vydávají na zabezpečení svých systémů méně než 5 % z celkového rozpočtu. S tím souvisí i zvýšená poptávka po outsourcingu, nábor absolventů či zájem o školení uživatelů, jelikož se tyto oblasti stávají klíčovými pro zvyšování odolnosti vůči útokům [1].

Z uvedeného je patrné, že kybernetická bezpečnost není pouze doménou IT specialistů, ale stává se strukturálním prvkem moderního řízení rizik na všech úrovních společnosti. Vývoj posledních let jednoznačně ukazuje, že efektivní ochrana kyberprostoru je nezbytná nejen pro stabilitu fungování jednotlivých institucí, ale i pro udržení důvěry veřejnosti ve stát a jeho schopnost chránit své digitální prostředí. Vzhledem k tomu, že intenzita kybernetických hrozeb bude pravděpodobně dále narůstat, je nutné považovat kybernetickou bezpečnost za trvalou prioritu a zároveň za výzvu, která přesahuje rámec technických opatření a vyžaduje strategickou koordinaci, adekvátní financování a posílení odborného zázemí napříč institucemi.

1.2 Významné kybernetické incidenty

Významné případy kybernetických incidentů, které v posledních letech zasáhly veřejné instituce v České republice, představují konkrétní ilustraci trendů uvedených v předchozí kapitole. Analýza těchto incidentů umožňuje nejen pochopení jejich praktických dopadů, ale také identifikaci slabých míst v oblasti technologického zabezpečení a krizového řízení institucí veřejné správy. Níže uvedené příklady zahrnují různé typy útoků, jejichž společným důsledkem bylo narušení dostupnosti veřejných služeb, ztráta datové integrity a významné provozní či ekonomické dopady na postižené organizace.

Jedním z velkých incidentů byl ransomwarový útok na Nemocnici Rudolfa a Stefanie v Benešově v prosinci 2019. V důsledku útoku došlo k rozsáhlému výpadku informačních systémů nemocnice, což vedlo k dvoutýdennímu omezení poskytování zdravotní péče. Incident poukázal na nedostatky v oblasti krizového plánování, zálohování a síťové segmentace, což vyvolalo intenzivní debatu o potřebě posílení bezpečnostních standardů zdravotnických zařízení v ČR [4].

Obdobně závažný ransomwarový útok zasáhl v březnu 2020 Fakultní nemocnici Brno. Tento incident způsobil rozsáhlý výpadek a významné omezení provozu ve všech třech lokalitách nemocnice, čímž došlo k zásadnímu narušení poskytování zdravotní péče. V reakci na tento útok nemocnice zahájila okamžitou spolupráci s Národním úřadem pro kybernetickou a informační bezpečnost a dalšími odbornými institucemi, které pomáhaly při řešení krizové situace a obnově klíčových systémů. Celkové finanční škody byly odhadnuty na stovky milionů korun. Tento incident zdůraznil potřebu systematického zajištění kybernetické bezpečnosti, zejména v oblasti zdravotnictví, a ukázal důležitost efektivního krizového managementu a spolupráce mezi institucemi při zvládání kybernetických incidentů [4].

Dalším typem incidentu, který se výrazně projevil v důsledku geopolitického napětí, byly koordinované DDoS útoky na české subjekty v roce 2022. Útoky prováděné proruskými hacktivistickými skupinami byly reakcí na politickou podporu České republiky vůči Ukrajině. Cílem těchto útoků byly především webové portály veřejné správy, médií a finančních institucí s cílem narušit jejich dostupnost a vyvolat psychologický tlak. Nejvíce útoků bylo zaznamenáno v říjnu 2022, kdy během jediného měsíce došlo k výraznému nárůstu incidentů. Důsledkem těchto útoků byla dočasná nedostupnost některých webových služeb, což zvýraznilo potřebu implementace efektivních opatření [2; 5].

Pro ilustraci problematiky ransomwarových útoků v širším regionálním kontextu lze uvést také incident na slovenském katastru nemovitostí v roce 2025. Tento útok, provedený formou ransomwarové kampaně, ochromil klíčové informační systémy slovenského katastru. Útok způsobil problémy v poskytování veřejných služeb, které byly nuceně přerušeny na několik dní. Přestože se jednalo o zahraniční incident, důsledky útoku a použítá metodika představují varování i pro českou veřejnou správu [8; 9].

1.3 Dopady kybernetických incidentů na organizace a společnost

Kybernetické incidenty, jak bylo popsáno v předchozích kapitolách, mají široké dopady jak na jednotlivé organizace, tak na společnost jako celek. Konkrétními příklady těchto dopadů mohou být ekonomické ztráty, narušení provozu organizací a společenské důsledky ve formě ztráty důvěry veřejnosti.

Ekonomické ztráty spočívají zejména v nákladech na obnovu systémů a infrastruktury po incidentu a v delších finančních dopadech, jako je přerušení provozu a náklady na krizový management. Typickým příkladem je ransomwarový útok na Fakultní nemocnici Brno, který v roce 2020 způsobil škody v řádu stovek milionů korun [4].

Narušení provozu organizací zahrnuje především omezení nebo úplné přerušení běžných činností, které vede k dočasné nedostupnosti poskytovaných služeb. Patří sem například omezení lékařské péče, kdy dochází k odkladu plánovaných výkonů a operačních zákroků, nebo přerušení administrativních služeb úřadů, což může výrazně komplikovat komunikaci a vyřizování běžných záležitostí občanů. Provozní omezení také často vyžadují nasazení mimořádných opatření a krizových plánů, což vede k dalším provozním komplikacím a zvýšeným nárokům na personál organizací [2; 4].

Společenské a politické důsledky incidentů se projevují snížením důvěry veřejnosti vůči institucím, zejména v oblasti ochrany citlivých dat a zajištění kontinuity služeb. V sektorech zdravotnictví a veřejné správy tyto incidenty ovlivňují vztah občanů k institucím. Politické dopady souvisí zejména s útoky, které jsou reakcí na geopolitické události, jako byly například koordinované DDoS útoky proruských hacktivistických skupin na české subjekty v roce 2022 [1; 2].

Uvedené příklady dopadů kybernetických incidentů jsou v souladu se zjištěními ENISA. Podle agentury jsou nejčastějšími důsledky kybernetických útoků narušení dostupnosti služeb ve veřejné správě, zdravotnictví a finančním sektoru, ekonomické škody

zahrnující bezprostřední náklady na obnovu a dlouhodobější finanční dopady v podobě ztráty důvěry zákazníků. Agentura rovněž upozorňuje na rostoucí obavy veřejnosti ohledně bezpečnosti osobních údajů a rizik spojených s manipulací s informacemi (Foreign Information Manipulation and Interference – FIMI) [6].

Z uvedených skutečností vyplývá, že dopady kybernetických incidentů přesahují rámec jednotlivých organizací a dotýkají se celé společnosti. Důsledky těchto incidentů proto vyžadují systematickou analýzu kybernetických rizik, která je krokem k zajištění prevence a připravenosti organizací na podobné scénáře. Tato problematika bude rozvíjena v následujících teoretických a praktických částech této bakalářské práce.

1.4 Význam analýzy rizik v oblasti kybernetické bezpečnosti

Počet kybernetických incidentů v posledních letech roste, a spolu s tím se zvyšují i jejich dopady. Jak ukazují předchozí kapitoly, útoky mohou vážně narušit chod organizací, způsobit finanční škody, vyvolat nejistotu u veřejnosti a narušit důvěru ve státní instituce. Častým problémem je, že řada organizací řeší bezpečnost až v okamžiku, kdy dojde k incidentu. Takový přístup je ale z dlouhodobého hlediska neudržitelný [1].

Smyslem analýzy rizik je pokusit se těmito situacím předejít. Organizace by měly znát svá klíčová aktiva, vědět, jaké hrozby jim reálně hrozí, kde mají zranitelná místa a jaké následky by případný útok mohl mít. Teprve na základě těchto informací je možné promyšleně rozhodnout, jaká opatření zavést a kde je naopak možné rozumně šetřit [10].

K analýze rizik však dnes organizace nepřistupují jen dobrovolně, významnou roli hraje i legislativa. Zákon o kybernetické bezpečnosti a nově také evropská směrnice NIS2 stanovují pro určité subjekty povinnost provádět analýzu rizik a přijímat odpovídající opatření. Nejde tedy jen o otázku vlastní bezpečnosti, ale i o dodržení právních povinností [11].

Z těchto důvodů má analýza rizik své pevné místo v řízení organizací, které pracují s informačními technologiemi. Její důležitost bude s postupující digitalizací dále růst. V této práci se proto dále zaměřím na to, co vše analýza rizik v kybernetické oblasti obnáší, jaké existují metody a jaké výhody může jejich použití přinést v praxi.

2 KYBERNETICKÁ BEZPEČNOST A SOUVISEJÍCÍ POJMY

Před tím, než je možné přistoupit k samotné analýze rizik v oblasti kybernetické bezpečnosti, je nutné vymezit základní pojmy, se kterými bude práce dále operovat. Tato kapitola proto postupně objasňuje, co se rozumí kybernetickou bezpečností, jaké principy ochrany informací jsou pro tuto oblast klíčové a jaké typy hrozeb a zranitelností se v digitálním prostředí běžně vyskytují. Všechny tyto pojmy tvoří výchozí rámec nejen pro pochopení metod analýzy rizik, ale také pro správné zařazení konkrétních bezpečnostních opatření, kterým se bude práce věnovat v dalších částech.

2.1 Definice kybernetické bezpečnosti

Kybernetická bezpečnost se jako samostatné odborné téma začala formovat s nástupem digitalizace a rozšiřováním informačních technologií do všech oblastí společenského i hospodářského života. Zatímco v počátcích šlo především o zabezpečení jednotlivých počítačových systémů, dnes se jedná o mnohohrstevnatou oblast pokrývající ochranu digitální infrastruktury, zajištění kontinuity služeb a prevenci před technologickými i lidskými hrozbami. Samotný pojem kybernetická bezpečnost není jednotně definován, ale ve většině odborných i legislativních pramenů se shodně vztahuje k ochraně informačních systémů a sítí, dat a služeb před narušením, zneužitím, poškozením nebo ztrátou jejich funkčnosti [12].

V prostředí České republiky je základní definice ukotvena v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti, kde je tento pojem vymezen jako „zajištění odolnosti informačních systémů, služeb a sítí elektronických komunikací proti kybernetickým bezpečnostním událostem“. Zákon dále rozvádí oblasti, které mají být předmětem ochrany, a zároveň definuje rámcové povinnosti provozovatelů informačních systémů ve veřejném i soukromém sektoru. Tento právní předpis tvoří základní rámec národní politiky kybernetické bezpečnosti a byl dále rozvinut novelami navazujícími na evropskou legislativu, zejména na směrnici NIS2, které se budu podrobně věnovat v další části této práce [11; 13].

Z hlediska systematického přístupu je vhodné rozlišit kybernetickou bezpečnost od širšího pojmu informační bezpečnost. Zatímco informační bezpečnost se vztahuje ke všem formám informací bez ohledu na jejich podobu včetně papírových záznamů nebo ústní komunikace, kybernetická bezpečnost se soustřeďuje specificky na digitální prostředí. Jinými slovy, kybernetická bezpečnost tvoří podmnožinu informační bezpečnosti, přičemž

její hlavní těžiště spočívá v technických, procesních a právních opatřeních na ochranu dat zpracovávaných, přenášovaných či ukládaných pomocí elektronických zařízení a sítí [10].

Přesahy mezi těmito dvěma oblastmi jsou přirozené, nicméně pro účely této práce se bude dále uplatňovat pojetí odpovídající právě definici kybernetické bezpečnosti ve smyslu zákona č. 181/2014 Sb., které bude věnována samostatná kapitola. Z hlediska aplikační praxe je podstatné, že kybernetická bezpečnost není pouze otázkou technologických nástrojů, ale zahrnuje rovněž lidské a organizační faktory, jako je školení zaměstnanců, nastavení přístupových práv či definování bezpečnostních politik [12].

S rostoucí digitalizací služeb veřejné správy, průmyslu, zdravotnictví nebo školství se kybernetická bezpečnost stává strategickým prvkem národní bezpečnosti. Incidents, jako jsou útoky ransomware na nemocnice, phishingové kampaně zaměřené na státní úřady nebo distribuované útoky DDoS, již nejsou výjimkou, ale běžnou součástí bezpečnostního prostředí. Je proto nezbytné chápat kybernetickou bezpečnost jako průřezové téma, jehož dopady přesahují hranice IT oddělení a týkají se celého organizačního rámce subjektu [1].

Na evropské úrovni hraje důležitou roli při tvorbě politik kybernetické bezpečnosti Agentura Evropské unie pro kybernetickou bezpečnost, která vydává doporučení, metodiky a přehledy hrozeb. V českém kontextu má klíčovou roli Národní úřad pro kybernetickou a informační bezpečnost, který koordinuje národní strategii, spravuje systém hlášení incidentů a vydává metodickou podporu subjektům podle zákona o kybernetické bezpečnosti. Dále fungují odborné složky jako CERT.CZ, které zajišťují provozní podporu při řešení bezpečnostních incidentů [10].

Lze tedy shrnout, že ačkoli pojem kybernetické bezpečnosti není mezinárodně definován jednotně, jeho jádro tvoří schopnost organizací a států odolávat, detekovat a reagovat na incidents, které ohrožují funkčnost a důvěryhodnost digitálních systémů.

2.2 Principy ochrany informací (CIA triáda)

Ochrana informací a informačních systémů v digitálním prostředí se v odborné literatuře i v praxi standardně opírá o tzv. CIA triádu, která představuje tři základní bezpečnostní cíle: důvěrnost (Confidentiality), integritu (Integrity) a dostupnost (Availability). Tyto principy tvoří základní rámec pro navrhování bezpečnostních opatření, hodnocení rizik i reakci na incidents. Jejich uplatnění je univerzální bez ohledu na typ organizace nebo technologické

prostředí a je běžně obsaženo v národních i mezinárodních bezpečnostních standardech, například v normách ISO/IEC 27000 [12; 10].

Důvěrnost znamená ochranu informací před neoprávněným přístupem, zveřejněním či prozračením. Cílem je zajistit, aby se k datům dostaly pouze oprávněné osoby a subjekty, a to jak na úrovni čtení, tak zpracování. Porušení důvěrnosti může mít vážné následky, například v oblasti zdravotnictví by neoprávněné zveřejnění zdravotní dokumentace mohlo vést nejen ke ztrátě důvěry pacientů, ale i k právním důsledkům. Mezi běžná opatření na ochranu důvěrnosti patří šifrování dat, řízení přístupových práv, autentizace uživatelů či použití tzv. klasifikace informací. V kontextu organizací se důvěrnost týká nejen citlivých dokumentů, ale i např. interních komunikačních kanálů, databází zákazníků nebo smluvních informací. Nedostatečné zabezpečení těchto oblastí je jedním z častých bodů zneužití v rámci útoků typu phishing nebo insider threat [12].

Integrita označuje zachování přesnosti, správnosti a úplnosti informací a systémů. Znamená, že data nebyla neautorizovaně změněna, poškozena nebo ztracena, ať už úmyslně, nebo omylem. Například u elektronické fakturace nebo účetnictví je zajištění integrity klíčové, jelikož jakákoli neautorizovaná změna v údajích může vést k chybám ve vykazování nebo k právní odpovědnosti. Z hlediska opatření se integrita zajišťuje pomocí kontrolních mechanismů, verzování dokumentů, digitálních podpisů, kontrolních součtů a auditních záznamů. Důležitým aspektem je schopnost detekovat změny v reálném čase a provádět pravidelnou kontrolu konzistence databází a systémů. Integrita bývá často narušována útoky typu malware, SQL injection nebo neautorizovaným přepisem souborů [12; 14].

Dostupnost znamená zajištění toho, že autorizovaní uživatelé mají k informacím a službám přístup v okamžiku, kdy je potřebují. Jedná se o klíčový aspekt zejména v oblastech, kde je kontinuální provoz nezbytný, například v energetice, zdravotnictví nebo dopravě. Nedostupnost může být způsobena nejen útokem, ale i technickou poruchou, výpadkem elektrické energie, softwarovou chybou nebo chybným lidským zásahem. Zajištění dostupnosti obvykle zahrnuje redundanci systémů, pravidelné zálohování, havarijní plány, nepřetržitý monitoring infrastruktury a používání nepřerušitelných zdrojů napájení (UPS). Mezi typické útoky cílené na dostupnost patří DDoS, kdy útočník zahlučuje server požadavky, čímž ho vyřadí z provozu. Význam dostupnosti výrazně vzrostl s přechodem organizací do cloudových prostředí a s rozvojem online služeb [12; 14].

Model CIA slouží nejen jako teoretické východisko, ale i jako praktický nástroj pro návrh bezpečnostních opatření a hodnocení stavu kybernetické ochrany v organizacích.

V rámci následující analýzy rizik se s těmito třemi aspekty pracuje při klasifikaci aktiv a identifikaci hrozeb. Jejich porušení je typickým cílem útočníků a jejich zachování je cílem bezpečnostních opatření [12].

2.3 Typologie kybernetických hrozeb a zranitelností

Kybernetické hrozby a zranitelnosti představují vzájemně propojené prvky, jejichž pochopení je důležité pro efektivní řízení rizik v digitálním prostředí. Znalost jejich povahy a vzájemných souvislostí umožňuje lépe posoudit potenciální rizika, kterým informační systémy organizace mohou čelit [12].

2.3.1 Klasifikace hrozeb podle původu

V kontextu kybernetické bezpečnosti se hrozba zpravidla definuje jako potenciální událost nebo situace, která může nepříznivě ovlivnit důvěrnost, integritu nebo dostupnost informačních aktiv. Správná identifikace a kategorizace hrozeb je zásadním předpokladem pro následnou analýzu rizik, návrh bezpečnostních opatření a vytvoření odpovídajících krizových scénářů. Jedním z běžně používaných přístupů k jejich systematickému třídění je členění podle původu nebo charakteru, což umožňuje identifikovat i skryté vazby mezi hrozbou, zranitelností a potenciálním dopadem [12].

Lidské hrozby zahrnují jak neúmyslné chyby, tak cílené škodlivé jednání jednotlivců nebo skupin. V oblasti kybernetické bezpečnosti se zvláštní pozornost věnuje tzv. vnitřním hrozbám, které pocházejí od osob s oprávněným přístupem k systémům, jako například zaměstnanců, dodavatelů nebo smluvních partnerů. Typickým příkladem může být administrátor, který zneužije přístupová práva k manipulaci s daty nebo je úmyslně poskytne třetí straně. Vedle záměrného jednání je třeba počítat i s lidskými omyly, jako jsou nechtěné změny v konfiguraci, kliknutí na phishingový odkaz nebo zaslání citlivého dokumentu na nesprávnou adresu [12; 14].

Technogenní hrozby vznikají v důsledku selhání technologií, na nichž jsou informační systémy závislé. Jedná se například o hardwarové poruchy (selhání diskových polí, přehřátí serveru, výpadek napájení) nebo softwarové chyby (bugy v operačních systémech, zranitelnosti v aplikacích, nekompatibilita systémů). Velmi rizikovým faktorem je také využívání zastaralého nebo neaktualizovaného softwaru, u nějž již výrobce neposkytuje bezpečnostní záplaty, tzv. end-of-life software. Z technologického hlediska jsou

zranitelnosti často vstupním bodem pro exploity a útoky typu zero-day, které využívají neznámé nebo neopravené chyby v systému [12; 14].

Do kategorie přírodních hrozeb spadají události, které nejsou způsobeny lidskou činností, ale přesto mohou mít zásadní dopad na provoz ICT infrastruktury. Typickými příklady jsou povodně, požáry, zemětřesení, bouře, extrémní teploty nebo výkyvy v dodávkách elektrické energie. Zatímco některé z těchto jevů lze předvídat a před nimi se chránit, např. záložní zdroje UPS, klimatizace serveroven, umístění infrastruktury mimo povodňové zóny, jiné mohou být natolik náhlé a rozsáhlé, že způsobí nenahraditelné škody. I přesto se přírodní hrozby v analýze rizik často podceňují, zejména v prostředí menších organizací [12; 14].

V tomto členění je zřejmé, že původ hrozby významně ovlivňuje nejen pravděpodobnost jejího výskytu, ale také možnosti reakce a míru připravenosti organizace. Například proti přírodní katastrofě je třeba plánovat dopředu a vytvořit záložní systémy, zatímco proti lidské hrozbě je účinnější bezpečnostní kultura a řízení přístupových práv. V následující části bude podrobněji rozebrána typologie kybernetických útoků podle jejich cíle a způsobu provedení, v návaznosti na principy CIA modelu.

2.3.2 Typy útoků a hrozeb v praxi

Kybernetické útoky se v praxi realizují různými způsoby, přičemž cílem útočníků bývá narušit některý z pilířů informační bezpečnosti – důvěrnost, integritu nebo dostupnost. Klasifikace útoků podle jejich cílové složky CIA modelu přináší přehledný rámec, který umožňuje pochopit základní motivace útočníků, používané prostředky i potenciální dopady. V následujícím textu jsou uvedeny typické formy útoků, rozdělené podle toho, kterou bezpečnostní vlastnost nejčastěji ohrožují [12; 14].

Útoky zaměřené na důvěrnost usilují o získání citlivých informací bez vědomí vlastníka. Typickým příkladem jsou phishingové kampaně, při nichž útočník pod falešnou identitou získává přihlašovací údaje, čísla platebních karet nebo osobní data. Zvlášť nebezpečný je tzv. spear-phishing, cílený na konkrétní osoby, či jeho moderní varianta quishing, využívající podvržené QR kódy. Jiným druhem útoku na důvěrnost je tzv. sniffing, tedy odposlech síťového provozu, který útočníkovi umožňuje zachytit nešifrované přenosy dat mezi zařízeními. Do této kategorie patří také tzv. data leakage, tedy neúmyslný únik dat z organizace, často zapříčiněný lidskou chybou, například zasláním e-mailu s citlivou

přílohou na nesprávného adresáta. Všechny tyto formy útoků mohou vést k porušení zákonů na ochranu osobních údajů a výrazně poškodit reputaci organizace [12; 14].

Útoky na integritu cílí na nepozorovanou nebo neoprávněnou změnu obsahu dat, čímž dochází ke zkreslení, poškození nebo falšování informací. Jednou z nejčastějších forem je tzv. SQL injection, útok využívající nedostatečného ošetření vstupu v databázových dotazech. Útočník tímto způsobem může manipulovat s databází, měnit záznamy nebo dokonce vymazat její obsah. Obdobně nebezpečné jsou i tzv. man-in-the-middle útoky, kdy útočník zachytává a mění komunikaci mezi dvěma stranami bez jejich vědomí. Do této skupiny patří i ransomware, pokud jeho cílem není pouze zablokovat přístup, ale i znehodnotit nebo zašifrovat data. V některých případech dochází ke kombinaci více typů porušení, například útočník nejen poškodí soubory, ale zároveň hrozí zveřejněním zcizených dat, čímž zasáhne i důvěrnost [12; 14; 15].

Útoky na nedostupnost se snaží znemožnit oprávněným uživatelům přístup k informacím nebo službám. Nejznámější formou je tzv. Distributed Denial of Service, kdy je cílový server zahlcen obrovským množstvím požadavků z různých IP adres, což vede k jeho výpadku. Tyto útoky jsou často prováděny pomocí botnetů, sítí kompromitovaných zařízení, které útočník ovládá na dálku. Dostupnost může být také ohrožena útoky typu logic bomb, při nichž je do systému vložen škodlivý kód, jenž se aktivuje při splnění určitých podmínek (např. datum, akce uživatele). Velmi častou příčinou ztráty dostupnosti jsou rovněž špatně provedené aktualizace, chybějící zálohování nebo chyby v konfiguraci síťových prvků. I proto se dostupnost netýká pouze útoků, ale obecně i provozní spolehlivosti ICT infrastruktury [12; 14].

2.3.3 Typologie zranitelností

Zranitelnost představuje slabé místo v systému, infrastruktuře, procesech nebo lidském faktoru, které může být zneužito k realizaci bezpečnostní hrozby. Zatímco hrozba označuje potenciál pro vznik nežádoucí události, zranitelnost je podmínkou, která její realizaci umožňuje. V rámci analýzy rizik proto hraje identifikace zranitelností klíčovou roli, neboť určuje míru pravděpodobnosti, s jakou může být aktivum ohroženo. Zranitelnosti se vyskytují napříč technologickými, organizačními i lidskými strukturami organizace [12].

Technické zranitelnosti se vztahují ke konkrétnímu hardwarovému nebo softwarovému prvku ICT infrastruktury. Patří sem zejména neaktualizovaný operační systém, chybějící bezpečnostní záplaty, špatně nastavené konfigurace firewallů, slabé šifrování dat nebo

veřejně dostupné služby bez odpovídajícího zabezpečení. V oblasti webových aplikací jde často o zranitelnosti typu XSS (Cross-Site Scripting) nebo právě zmíněné SQL injection, které mohou být zneužity k narušení integrity a důvěrnosti dat. Riziková je rovněž absence síťové segmentace, přítomnost starých, tzv. end-of-life zařízení bez výrobní podpory nebo například využívání výchozích přihlašovacích údajů na síťových prvcích. Technické zranitelnosti lze do značné míry omezit pravidelným monitoringem, penetračním testováním a automatickým nasazováním aktualizací [12; 14].

Organizační zranitelnosti vznikají v důsledku chybějících nebo nedostatečně definovaných pravidel, postupů a odpovědností v rámci řízení bezpečnosti. Typickým příkladem je neexistence bezpečnostní politiky, chybějící školení zaměstnanců, nevhodně nastavené procesy pro změnové řízení nebo nejasná pravidla pro správu uživatelských účtů. Závažným nedostatkem bývá také absence interních auditů nebo pravidelného testování připravenosti na krizové situace. Tento typ zranitelností často souvisí s organizační kulturou a prioritami vedení. Pokud kybernetická bezpečnost není vnímána jako systémový prvek řízení rizik, dochází k jejímu podceňování, které může v krizové situaci vést k nedostatečné reakci a vysokým škodám [12; 14].

Fyzické zranitelnosti představují slabiny v ochraně prostor, zařízení a materiálních aktiv. Sem patří nedostatečně zabezpečený přístup do serverovny, absence kamerového systému, nechráněné rozvodné skříně nebo chybějící záložní napájení. V extrémních případech může jít o umístění serverů v prostorách bez protipožárních opatření nebo o sdílení prostor s nepovolanými osobami. Tyto slabiny se neprojevují tak často jako technické nebo organizační, ale jejich dopad bývá vážný. Ztráta fyzického zařízení může znamenat nejen ztrátu dat, ale i ohrožení důvěrnosti, pokud nejsou data na discích šifrována [12; 14].

Lidský faktor představuje jednu z nejvýznamnějších a zároveň nejhůře kontrolovatelných oblastí zranitelnosti. Neúmyslné chyby, špatné návyky, nedostatek školení nebo únavu nelze zcela eliminovat. Nejčastěji se projevují ve formě kliknutí na škodlivý odkaz, opakovaného používání stejných hesel, ignorování bezpečnostních hlášení nebo sdílení přístupových údajů. Obávaným scénářem je také sociální inženýrství, kdy útočník manipuluje zaměstnance k provedení nechtěné akce. Z hlediska prevence je klíčová osvěta, pravidelná školení a budování bezpečnostního povědomí. Řízení lidských zranitelností zahrnuje nejen technická opatření, ale také systematickou práci s firemní kulturou a jasně nastavené procesy [12; 14].

Tato čtyři základní typová členění zranitelností tvoří rámec pro posouzení připravenosti organizace čelit kybernetickým hrozbám. Jejich existence sama o sobě nepředstavuje riziko, ale ve spojení s konkrétní hrozbou a hodnotným aktivem vzniká scénář, který již musí být vyhodnocen. Tímto propojením se zabývá analýza rizik, která bude rozebrána v další části práce.

3 ANALÝZA RIZIK V KYBERNETICKÉ BEZPEČNOSTI

Analýza rizik představuje v rámci kybernetické bezpečnosti klíčový proces, který umožňuje systematicky pochopit a vyhodnotit hrozby působící na informační aktiva organizace. V kontextu systému řízení bezpečnosti informací (ISMS) se jedná o nezbytný krok, jehož prostřednictvím lze určit potenciální zranitelnosti a posoudit závažnost možných dopadů bezpečnostních incidentů. Efektivní analýza rizik přitom vyžaduje jasné vymezení rozsahu hodnocení, přesnou identifikaci aktiv a hrozeb, a také aplikaci vhodných analytických metod, jejichž cílem je objektivně stanovit míru rizika a doporučit odpovídající opatření pro jeho řízení. Z provedené analýzy lze následně odvodit konkrétní bezpečnostní opatření odpovídající specifickým potřebám organizace, čímž analýza rizik tvoří nezbytnou součást celkového systému řízení bezpečnosti informací [10; 16].

3.1 Úloha a význam analýzy rizik

Analýza rizik představuje klíčový nástroj řízení kybernetické bezpečnosti, jehož cílem je systematicky identifikovat a hodnotit potenciální hrozby, zranitelnosti a možné dopady na informační aktiva organizace. V kontextu kybernetické bezpečnosti je analýza rizik nezbytným předpokladem k pochopení míry ohrožení, kterému může být subjekt vystaven, a zároveň umožňuje efektivní plánování ochranných opatření. Riziko bývá v tomto rámci definováno jako kombinace pravděpodobnosti výskytu hrozby a závažnosti jejího dopadu na konkrétní aktivum, například informační systém, databázi nebo infrastrukturu [10; 16].

Význam analýzy rizik spočívá především v tom, že umožňuje identifikovat slabá místa v zabezpečení a přidělit ochranným opatřením odpovídající prioritu. Tím napomáhá k racionálnímu využití dostupných zdrojů, technických, personálních i finančních. Umožňuje organizacím lépe porozumět tomu, jaké typy hrozeb se na jejich provoz vztahují, a v jaké míře jsou na ně jednotlivá aktiva citlivá. Pravidelné vyhodnocování rizik dále přispívá ke schopnosti organizace reagovat na nové scénáře, vyvíjející se hrozby a změny v technologickém nebo legislativním prostředí [10; 16].

Analýza rizik není izolovaným jednorázovým procesem, ale součástí širšího rámce řízení bezpečnosti informací. Jejím výstupem nejsou jen seznamy hrozeb, ale také podklady pro rozhodování, plánování a zavádění konkrétních technických a organizačních opatření. V tomto smyslu tvoří základní stavební prvek systémového řízení informační bezpečnosti podle modelu PDCA (Plan–Do–Check–Act), kde představuje vstupní krok plánovací fáze.

Na základě výsledků analýzy jsou stanovena bezpečnostní opatření, jejichž účinnost je následně sledována, kontrolována a vyhodnocována [10; 16].

Praktické využití analýzy rizik v oblasti kybernetické bezpečnosti zahrnuje široké spektrum činností. Typickými analyzovanými scénáři jsou například možnosti zneužití přístupových údajů, zavedení škodlivého softwaru do systému, ztráta nebo poškození dat, nefunkčnost záloh, selhání hardwaru, výpadek napájení nebo manipulace s citlivými informacemi ze strany uživatelů. V případě, že by takové události nastaly, mohou vést k částečné nebo úplné ztrátě dostupnosti služeb, ohrožení důvěrnosti údajů nebo narušení integrity procesů. Pro každý z těchto scénářů je třeba samostatně zhodnotit pravděpodobnost výskytu, závažnost dopadu i zranitelnost aktiva [16].

Analýza rizik je v prostředí kybernetické bezpečnosti vnímána jako proces, který se musí opakovat a pravidelně aktualizovat. Vzhledem k dynamickému vývoji kybernetických hrozeb, proměnlivosti útočných technik i rostoucím závislostem organizací na digitální infrastruktuře není možné spoléhat na statický nebo jednorázový přístup. Rizika, která byla dříve považována za okrajová, mohou během krátké doby přerůst v reálné hrozby. Pravidelná revize analýzy rizik proto zajišťuje, že bezpečnostní opatření zůstávají přiměřená aktuálním podmínkám [10; 16].

Analýza rizik je v současnosti považována za jeden ze základních nástrojů, které umožňují systematické posouzení úrovně kybernetické ochrany v organizaci. Její využití se stalo běžnou součástí přístupů k řízení bezpečnosti informačních systémů a digitálních aktiv v různých typech institucí. Pravidelné hodnocení rizik přispívá k udržení přiměřené úrovně ochrany a k pružné reakci na proměnlivé podmínky v oblasti technologií, provozu i hrozeb. Tento proces zároveň poskytuje podklad pro volbu metod, které se uplatňují při praktickém vyhodnocování bezpečnostní situace v konkrétním prostředí [16].

3.2 Vymezení rozsahu analýzy

Stanovení jasného rozsahu analýzy rizik je nezbytným krokem v procesu řízení bezpečnosti informací v rámci organizace. Účelem tohoto kroku je přesně určit hranice, ve kterých budou identifikována a následně vyhodnocena potenciální bezpečnostní rizika. Vymezení rozsahu zahrnuje stanovení technických, organizačních a geografických hranic, které určují konkrétní oblasti, technologie a odpovědnosti vstupující do hodnocení. Správně definovaný rozsah přispívá k relevantnosti výsledků analýzy a umožňuje formulovat odpovídající bezpečnostní opatření odpovídající skutečným potřebám organizace [10].

V rámci technického vymezení jsou určeny všechny významné systémy a zařízení, které organizace používá. Do analýzy jsou zahrnuty prvky jako servery, pracovní stanice, mobilní zařízení, firewallová řešení či síťové přepínače. Kromě těchto fyzických zařízení je nutné vymezit i softwarová aktiva, mezi něž patří operační systémy, databázové aplikace, interní komunikační nástroje a aplikace pro správu přístupových práv uživatelů. Specifikace těchto aktiv umožňuje podrobnější posouzení potenciálních zranitelností a jejich dopadů na provoz organizace [10; 14].

Geografické vymezení analýzy stanovuje konkrétní fyzické lokality, jejichž bezpečnost je klíčová pro chod organizace a zachování integrity a dostupnosti informačních aktiv. Zahrnují se především prostory s největší koncentrací citlivých informačních systémů, jako jsou serverovny, datová centra či administrativní prostory s klíčovými zařízeními a datovými úložišti. Geografické ohraničení je nutné nejen kvůli identifikaci rizik spojených s fyzickou bezpečností, ale také pro přístup k řízení bezpečnosti informací [10; 16].

Organizační vymezení rozsahu zahrnuje definování relevantních organizačních jednotek a rolí uživatelů, kteří mají významný vliv na správu, zabezpečení a provoz informačních aktiv. Důležitými součástmi tohoto vymezení jsou zejména útvary odpovědné za IT, management, ale také další oddělení, která pracují s citlivými informacemi, například oddělení finanční či personální. Identifikace těchto organizačních útvarů umožňuje zohlednit skutečné odpovědnosti a kompetence v procesu řízení rizik a cílit bezpečnostní opatření na konkrétní potřeby jednotlivých organizačních jednotek [10; 16].

V praktické části této práce přímo využiji uvedené vymezení rozsahu analýzy. Konkrétně identifikuji klíčová datová a aplikační aktiva, prvky síťové infrastruktury, koncová zařízení i lidské zdroje. U každé z těchto oblastí následně určím relevantní zranitelnosti a související hrozby, jejichž vzájemným propojením stanovím rizikové scénáře. Na základě těchto scénářů pak navrhnu konkrétní bezpečnostní opatření odpovídající reálným potřebám analyzované organizace.

3.3 Identifikace a ocenění aktiv

Identifikace a ocenění aktiv je jedním z klíčových kroků analýzy rizik v oblasti kybernetické bezpečnosti. Aktiva představují všechny důležité zdroje organizace, které vyžadují ochranu před hrozbami kvůli jejich významu pro její činnost. V kontextu analýzy rizik se aktiva dělí na primární a podpurná. Toto rozdělení umožňuje jasně určit prioritu ochrany jednotlivých

typů aktiv podle jejich důležitosti a potenciálních dopadů, které by nastaly v případě jejich narušení [12].

Primární aktiva představují klíčové zdroje, jejichž narušení, ztráta či nedostupnost by měly přímý a závažný dopad na hlavní činnost organizace. Mezi primární aktiva patří především informační aktiva, jako jsou aplikační databáze, personální záznamy, finanční informace, strategické plány či obchodní tajemství. Tato data jsou důležitá zejména kvůli své citlivosti a vlivu na chod organizace. Kromě informačních aktiv se mezi primární aktiva řadí i klíčové softwarové systémy a aplikace, bez nichž by organizace nebyla schopna efektivně provozovat svou činnost. Ty zahrnují například interní informační systémy, účetní programy, databázové aplikace nebo specializované softwarové nástroje pro řízení procesů organizace [12; 16].

V rámci oceňování primárních aktiv je důležité zohlednit nejen jejich finanční hodnotu, ale také jejich provozní důležitost a případné negativní dopady v případě jejich ohrožení či narušení. Ocenění může být založeno na kvalitativním hodnocení citlivosti dat a kvantitativním hodnocení případných finančních škod, které by vznikly v případě jejich ztráty nebo kompromitace [12; 16].

Podpůrná aktiva představují veškeré zdroje, jejichž ohrožení by nepřímou, ale významně ovlivnilo schopnost organizace provozovat svoji hlavní činnost. Patří sem zejména fyzická infrastruktura, hardwarová zařízení, lidské zdroje a podpůrné procesy. Mezi fyzická a hardwarová aktiva řadíme servery, pracovní stanice, síťová zařízení, zařízení pro zálohování dat, mobilní technologie či další technická zařízení nutná k chodu organizace. Oceňování těchto aktiv se provádí podle pořizovacích nákladů, hodnoty jejich obnovy, ale také podle významu pro udržení provozuschopnosti celé organizace [12; 16].

Zvláštní důležitost mezi podpůrnými aktivy mají lidská aktiva, která zahrnují pracovníky organizace. Tito pracovníci svými znalostmi, kompetencemi a přístupovými právy ovlivňují úroveň zabezpečení organizace a mohou se přímo či nepřímou podílet na vzniku bezpečnostních incidentů. Mezi klíčové role, které jsou z hlediska analýzy rizik důležité, patří bezpečnostní manažer, administrátor IT systémů, pracovníci odpovědní za správu dat, manažeři a další zaměstnanci s přístupem k citlivým informacím [12; 16].

Důležitou kategorií podpůrných aktiv je také fyzická infrastruktura, která zahrnuje prostory organizace, datová centra, serverovny, kanceláře, prostory s přístupovými systémy a další místa, jejichž narušení by mohlo způsobit nedostupnost primárních aktiv či jejich

ohrožení z důvodu fyzického přístupu neoprávněných osob. Při oceňování těchto aktiv se bere v potaz význam fyzické ochrany aktiv, ale také jejich dostupnost pro zajištění kontinuity provozu [12; 16].

3.4 Identifikace hrozeb a zranitelností

Identifikace hrozeb a zranitelností představuje další logický krok analýzy rizik v kybernetické bezpečnosti, který navazuje na již vymezený rozsah analýzy a definovaná aktiva. Hlavním cílem této fáze je určit, jakým potenciálním hrozbám může organizace čelit a jaké slabiny či nedostatky v jejích systémech a procesech mohou být zneužity k jejich realizaci. Jasně stanovení těchto prvků umožňuje provést následné objektivní hodnocení rizik a navrhnout vhodná preventivní a ochranná opatření odpovídající reálné situaci v organizaci [12].

Hrozby lze obecně definovat jako potenciální události nebo aktivity, které mohou negativně ovlivnit důvěrnost, integritu nebo dostupnost informačních aktiv. Mezi typické kybernetické hrozby patří například malware, ransomware, phishingové útoky, neoprávněný přístup, únik dat nebo DDoS útoky. Hrozby mohou být kategorizovány podle jejich původu na interní, způsobené zaměstnanci nebo interními procesy, a externí, způsobené vnějšími útočníky nebo třetími stranami. V této části analýzy jsou identifikovány konkrétní typy hrozeb relevantní pro danou organizaci, a to na základě jejího technologického prostředí, charakteru uchovávaných informací a způsobu provozu informačních systémů [12; 14].

Vedle samotných hrozeb je nutné identifikovat také zranitelnosti, tedy slabá místa, která mohou být využita k realizaci těchto hrozeb. Zranitelnosti mohou mít různý charakter. Technické zranitelnosti zahrnují například neaktualizovaný software, špatně zabezpečené sítě, nedostatečné zabezpečení přístupových údajů nebo nevyhovující konfigurace hardwarových zařízení. Organizační zranitelnosti se mohou týkat chybějících či nedostatečných bezpečnostních politik a procedur, nedostatečného školení zaměstnanců nebo neefektivního systému řízení bezpečnosti. Lidské zranitelnosti obvykle souvisí s chybami či nedbalostí zaměstnanců, které mohou vést k neoprávněnému přístupu či úniku informací [12].

K identifikaci hrozeb a zranitelností lze využít různé metodické přístupy, například SWOT analýzu, What-If analýzu nebo metody založené na odborném posouzení. V rámci této práce budou následně v praktické části využity vybrané metody, odpovídající specifickým podmínkám analyzované organizace. Cílem jejich použití bude sestavit

přehlednou strukturu relevantních hrozeb a zranitelností, které se týkají konkrétních aktiv a jejich bezpečnosti [17; 18].

3.5 Parametry hodnocení rizik

Hodnocení rizik v oblasti kybernetické bezpečnosti vyžaduje použití jasně definovaných parametrů, které umožňují objektivní a systematické vyhodnocení jednotlivých rizikových scénářů. Tyto parametry slouží jako vstupní proměnné zejména pro analytické metody, jakou je metoda FMEA (Failure Mode and Effects Analysis), a poskytují společný rámec pro jejich vzájemné porovnávání. Mezi často používané parametry patří pravděpodobnost výskytu hrozby, dopad hrozby na aktivum a pravděpodobnost odhalení rizika. Správně definované parametry pomáhají zajistit konzistentní, opakovatelné a transparentní hodnocení rizik, jehož výsledkem je jasná prioritizace navrhovaných bezpečnostních opatření [19; 20].

Prvním parametrem je pravděpodobnost výskytu hrozby, která označuje odhadovanou četnost realizace určitého rizikového scénáře. Stanovení pravděpodobnosti vychází ze zkušeností organizace, historických statistik bezpečnostních incidentů nebo z odborných odhadů. Pravděpodobnost se zpravidla určuje na kvalitativní škále s několika stupni, typicky nízká, střední a vysoká. Nízká pravděpodobnost odpovídá výjimečnému výskytu, vysoká pravděpodobnost naopak označuje často nebo opakovaně realizované scénáře. Mezi faktory ovlivňující tento parametr patří motivace útočníků, dostupnost prostředků pro provedení útoku, povědomí o známých zranitelnostech nebo exponovanost organizace vůči určitým typům hrozeb [20].

Pro potřeby analýzy rizik metodou FMEA v této práci jsou definovány následující kategorie pravděpodobnosti výskytu hrozeb s příslušnými číselnými ohodnoceními. Kategorie „Velmi nízká“ (ohodnocení 1) označuje situace, kdy je výskyt hrozby prakticky vyloučen. Kategorie „Nízká“ (ohodnocení 2 až 5) charakterizuje hrozby, jejichž výskyt je velmi málo pravděpodobný, jde o ojedinělé incidenty v mimořádných případech. Kategorie „Střední“ (ohodnocení 6) označuje občasný, avšak nepravidelný výskyt hrozeb, odpovídající náhodným incidentům v běžném provozu organizace. Kategorie „Vysoká“ (ohodnocení 7 až 8) zahrnuje pravidelný výskyt hrozeb v prostředí s nižší úrovní zabezpečení, kde jsou incidenty častější. Poslední kategorie „Velmi vysoká“ (ohodnocení 9 až 10) označuje téměř jistý výskyt hrozby, kdy incidenty nastávají s velmi vysokou pravděpodobností [20].

Druhým významným parametrem je dopad hrozby na aktivum, který označuje míru následků v případě, že se hrozba skutečně naplní. Dopad je určován na základě několika

kritérií, mezi něž patří provozní, finanční, právní nebo reputační následky. Při vyhodnocování dopadu se sledují zejména parametry, jako jsou doba výpadku služeb, rozsah kompromitovaných nebo ztracených dat, finanční škody či možné právní následky. Dopad bývá hodnocen pomocí kvalitativní stupnice, přičemž nejvyšší úroveň dopadu označuje situace vedoucí k dlouhodobému narušení činnosti organizace nebo k významné finanční či právní škodě [20].

Pro účely analýzy rizik metodou FMEA v této práci se používá následující klasifikace významu dopadů incidentů s příslušnými číselnými ohodnoceními. „Zanedbatelný význam“ (ohodnocení 1) představuje situaci, kdy incident nemá žádný měřitelný dopad na provoz nebo bezpečnost organizace a jeho výskyt pravděpodobně nebude zaznamenán. „Nízký význam“ (ohodnocení 2 až 3) zahrnuje incidenty, jejichž dopad způsobuje pouze drobné komplikace bez výraznějšího negativního vlivu na celkový chod organizace. „Střední význam“ (ohodnocení 4 až 6) označuje incidenty, které již mají znatelný vliv na běžné činnosti, vedou k omezení efektivity procesů nebo k dílčímu snížení kvality poskytovaných služeb. „Vysoký význam“ (ohodnocení 7 až 8) charakterizuje závažné incidenty způsobující významné narušení provozu, výrazné zhoršení kvality služeb nebo hmotné škody. Nejzávažnější kategorie „Velmi vysoký význam“ (ohodnocení 9 až 10) pokrývá incidenty, které ohrožují bezpečnost klíčových aktiv organizace, případně zásadně omezují provoz organizace [20].

Specifickým parametrem používaným v metodě FMEA je pravděpodobnost odhalení rizika. Tento parametr odráží schopnost organizace včas identifikovat riziko a reagovat na něj předtím, než se plně projeví. Pravděpodobnost odhalení závisí na efektivitě zavedených kontrolních mechanismů, dostupnosti a kvalitě monitorovacích nástrojů a úrovni povědomí zaměstnanců o rizikových faktorech. Hodnotí se opět kvalitativně, přičemž nízká pravděpodobnost odhalení znamená, že riziko je pravděpodobně odhaleno včas a lze podniknout účinná opatření k jeho eliminaci nebo minimalizaci. Naopak vysoká pravděpodobnost odhalení znamená, že existující kontrolní mechanismy jsou nedostatečné a riziko pravděpodobně nebude včas identifikováno [20].

Pro účely analýzy rizik metodou FMEA v této práci se používá následující klasifikace odhalitelnosti incidentů s příslušnými číselnými ohodnoceními. „Velmi vysoká odhalitelnost“ (ohodnocení 1) znamená, že incident je téměř vždy včas rozpoznán ještě předtím, než může způsobit jakékoli negativní dopady. „Vysoká odhalitelnost“ (ohodnocení 2 až 3) označuje situaci, kdy incidenty bývají běžně detekovány dostupnými kontrolními

mechanismy, avšak výjimečně mohou uniknout pozornosti. „Střední odhalitelnost“ (ohodnocení 4 až 6) představuje případy, kdy incidenty jsou detekovány pouze občas a kontrolní mechanismy jsou částečně účinné, což umožňuje, že některé incidenty projdou bez odhalení. „Nízká odhalitelnost“ (ohodnocení 7 až 8) zahrnuje incidenty, které jsou jen zřídka zachyceny dostupnými kontrolními prostředky, jejichž efektivita je omezená, a většina těchto incidentů není včas odhalena. Nejzávažnější kategorie „Velmi nízká odhalitelnost“ (ohodnocení 9 až 10) označuje incidenty, které jsou téměř neodhalitelné pomocí kontrolních mechanismů, což vede k tomu, že většina incidentů zůstává skryta a projeví se až při vzniku závažných důsledků [20].

Pro výpočet celkové míry rizika je v metodě FMEA využíváno číslo RPN (Risk Priority Number), které je výsledkem násobení pravděpodobnosti výskytu, závažnosti dopadu a pravděpodobnosti odhalení rizika [20]:

$$\text{RPN} = \text{Výskyt} \times \text{Závažnost} \times \text{Odhalitelnost} \quad (1)$$

Pro hranici zanedbatelného rizika byla použita hodnota odpovídající 50% úrovni každého ze zmíněných parametrů, což při výpočtu odpovídá hodnotě rizikového čísla $5^3 = 125$. Naopak hranice pro závažné riziko vychází z hodnoty odpovídající 85% úrovni těchto parametrů, což vede k hodnotě rizikového čísla přibližně $8,5^3 \approx 614$. V návaznosti na tento výpočet jsou v práci navrhována bezpečnostní opatření pouze pro rizika s významnou či závažnou klasifikací, tedy ta, jejichž rizikové číslo dosahuje hodnot od 126 do 1000.

3.6 Přístupy a metody analýzy rizik

Pro provedení analýzy rizik v kybernetické bezpečnosti existuje široká škála metod a analytických přístupů. Tyto metody se liší svým charakterem, stupněm formalizace, nároky na vstupní informace a možnostmi interpretace výsledků. V praxi bývá volba konkrétních metod přizpůsobena potřebám organizace, dostupným zdrojům a typu analyzovaných aktiv. Ačkoli lze nalézt různé další přístupy a techniky pro analýzu rizik, v rámci této práce jsem se rozhodl zaměřit na metody, které svými vlastnostmi vhodně odpovídají konkrétním podmínkám analyzovaného subjektu.

SWOT analýza patří mezi kvalitativní metody, jejichž cílem je systematicky identifikovat a vyhodnotit vnitřní a vnější faktory ovlivňující bezpečnost organizace. Mezi

interní faktory se řadí silné a slabé stránky, například technická úroveň systémů, organizační zabezpečení či schopnosti personálu. Externí faktory zahrnují příležitosti a hrozby plynoucí z vnějšího prostředí, například vývoj v oblasti kybernetických útoků, legislativní změny nebo dostupnost moderních bezpečnostních řešení. Hlavní výhodou SWOT analýzy je její přehlednost a srozumitelnost, díky níž lze jednoduše identifikovat klíčové oblasti, které vyžadují bližší pozornost. Nevýhodou je její subjektivní charakter, který omezuje možnosti přesné kvantifikace výsledků [18].

Dalším kvalitativním přístupem je What-If analýza, která umožňuje identifikovat potenciální rizika pomocí formulace hypotetických otázek typu „Co by se stalo, kdyby...“. Tato metoda je založena na předpokladu, že detailní posouzení různých scénářů pomůže odhalit méně zřejmé nebo méně pravděpodobné situace, které by přesto mohly vést k závažným následkům. What-If analýza je vysoce flexibilní a lze ji aplikovat v různých kontextech analýzy rizik. Její předností je schopnost odhalovat rizika, která mohou být jinými přístupy přehlédnuta. Nevýhodou metody je obtížnější kvantifikace rizik a větší míra subjektivity, což vyžaduje doplnění dalšími analytickými metodami [17; 21].

Metoda FMEA je rovněž metodou, která se původně používala v oblasti výrobního inženýrství, ale její aplikace se v posledních letech rozšířila také do oblasti kybernetické bezpečnosti. Metoda se zaměřuje na systematickou identifikaci možných selhání, posouzení pravděpodobnosti jejich výskytu, závažnosti jejich dopadů a pravděpodobnosti jejich včasného odhalení. Výsledkem je tzv. rizikové číslo RPN, které umožňuje detailní porovnání jednotlivých rizikových scénářů a jasnou definici priorit. Metoda FMEA je velmi podrobná a umožňuje odhalit slabá místa systému, nicméně vyžaduje vyšší časovou náročnost a poměrně hlubokou odbornou znalost analyzovaných systémů a procesů [20].

3.7 Návrh opatření pro řízení identifikovaných rizik

Cílem této části analýzy rizik je navrhnout konkrétní opatření, jejichž zavedení přispěje k minimalizaci identifikovaných kybernetických rizik na přijatelnou úroveň. Návrh bezpečnostních opatření vychází z výsledků předchozích kroků analýzy. Opatření jsou navrhována tak, aby byla účelná, odpovídající a realizovatelná v podmínkách organizace.

Technická opatření zahrnují zavedení nebo zlepšení bezpečnostních technologií a kontrol, jejichž účelem je omezit technické zranitelnosti systémů a minimalizovat dopady kybernetických hrozeb. Mezi nejčastěji používaná technická opatření patří například pravidelná aktualizace a správa softwaru, nasazení antivirových a antimalwarových

systemů, aplikace firewallů a systémů detekce průniků. Mezi další opatření patří implementace řízení přístupových práv na principu minimálních oprávnění, šifrování citlivých dat při přenosu i jejich uchovávání, pravidelné zálohování důležitých dat a technická redundance klíčových prvků infrastruktury. Zavádění těchto opatření vyžaduje důsledné plánování, odborné znalosti a dostatečnou technickou infrastrukturu, aby byla zajištěna jejich správná implementace a účinnost v praxi [12; 14].

Organizační opatření směřují k vytvoření efektivního rámce pro řízení kybernetické bezpečnosti uvnitř organizace. Tato opatření zahrnují zavedení a aktualizaci bezpečnostních politik, metodik a směrnic, které stanovují pravidla, odpovědnosti a postupy v oblasti informační bezpečnosti. Součástí organizačních opatření je rovněž pravidelné provádění auditů, kontrol a hodnocení bezpečnostního stavu organizace. Mezi doporučená organizační opatření patří také definování krizového plánu a postupu při řešení kybernetických incidentů, včetně jasně stanovených rolí a odpovědností při jejich zvládnutí. Organizace by měla rovněž zavést pravidla pro bezpečné nakládání s informacemi a řízení přístupu uživatelů do informačních systémů, včetně pravidelné revize těchto pravidel [12; 14].

Další významnou kategorií jsou personální opatření, která se zaměřují na lidský faktor v kybernetické bezpečnosti. Uživatelé systémů často představují jednu z největších zranitelností, protože mohou neúmyslně nebo vlivem lidské chyby způsobit bezpečnostní incidenty. Hlavním cílem personálních opatření je proto vzdělávání a pravidelné zvyšování povědomí zaměstnanců v oblasti kybernetické bezpečnosti. Organizace by měla zajistit pravidelná školení zaměřená na správné postupy při práci s informačními systémy, rozpoznávání hrozeb typu phishing nebo sociální inženýrství a reakce na bezpečnostní incidenty. Vhodné je také zavedení systému pravidelného ověřování znalostí zaměstnanců a poskytování zpětné vazby, která podporuje správné postupy v oblasti bezpečnosti informací [12; 14].

Při navrhování jednotlivých opatření je třeba postupovat systematicky a podle priorit definovaných výsledky analýzy rizik. Každé opatření by mělo mít stanovenou odpovědnou osobu nebo útvar, potřebné zdroje a jasně definované cíle. Návrh opatření by měl být také přiměřený závažnosti identifikovaných rizik a možnostem organizace, aby bylo zajištěno efektivní využití dostupných zdrojů [12].

4 LEGISLATIVA V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

V této kapitole se zaměřuji na legislativní a normativní rámec, který stanovuje podmínky pro zajištění kybernetické bezpečnosti a tvoří základní východisko pro realizaci analýzy rizik. Nejprve předkládám přehled směrnice Evropského parlamentu a Rady EU 2022/2555 (tzv. NIS2), jejímž cílem je harmonizace požadavků na řízení bezpečnosti sítí a informačních systémů napříč členskými státy Evropské unie a rozšíření působnosti na další subjekty a odvětví. Následně se věnuji zákonu č. 181/2014 Sb., o kybernetické bezpečnosti, který upravuje povinnosti subjektů v oblasti ochrany informací, včetně zavedení bezpečnostních opatření, hlášení incidentů a vedení dokumentace. V další části se zabývám prováděcími vyhláškami a metodickými dokumenty Národního úřadu pro kybernetickou a informační bezpečnost, které konkretizují požadavky stanovené zákonem. Současně uvádím normy ISO/IEC řady 27000, jež tvoří mezinárodně uznávaný rámec pro zavedení a řízení bezpečnosti informací. Závěrem se opírám o Národní strategii kybernetické bezpečnosti České republiky, která formuluje strategické cíle státu v této oblasti a podporuje uplatňování systematického přístupu k řízení rizik [22].

4.1 Směrnice NIS2 a její požadavky

Směrnice Evropského parlamentu a Rady EU 2022/2555, známá jako NIS2, představuje aktualizovaný právní rámec v oblasti kybernetické bezpečnosti, který nahrazuje původní směrnicí EU 2016/1148. Jejím cílem je posílit úroveň kybernetické odolnosti napříč členskými státy a odstranit rozdíly, které vznikly v důsledku rozdílného provádění původní úpravy. Směrnice NIS2 stanovuje jednotná pravidla pro řízení kybernetických bezpečnostních rizik, oznamování incidentů a dohled nad jejich plněním, přičemž zdůrazňuje potřebu koordinovaného postupu napříč celou Evropskou unií [11; 23].

Významnou změnou oproti předchozí právní úpravě je rozšíření oblasti působnosti směrnice. Zatímco dřívější směrnice rozlišovala mezi provozovateli základních služeb a poskytovateli digitálních služeb, NIS2 zavádí novou kategorizaci na základní a důležité subjekty. Tyto kategorie jsou definovány na základě velikostního kritéria a kritické důležitosti dané organizace v rámci konkrétního odvětví. Směrnice se vztahuje nejen na subjekty z oblasti energetiky, dopravy nebo zdravotnictví, ale nově také na některé úřady veřejné správy, výzkumné organizace, poštovní služby nebo poskytovatele řízených služeb [11; 24].

Součástí požadavků směrnice je zavedení opatření pro řízení rizik v oblasti kybernetické bezpečnosti. Subjekty spadající do působnosti směrnice jsou povinny zavést technická a organizační opatření, která odpovídají úrovni hrozeb, typu činností a velikosti organizace. Mezi tyto povinnosti patří například zajištění bezpečnosti dodavatelského řetězce, řízení přístupových práv, školení zaměstnanců, monitorování incidentů nebo vytváření bezpečnostní dokumentace. Důraz je kladen na přiměřenost přijatých opatření a na systematické posuzování rizik, které tvoří základ pro výběr konkrétních prostředků ochrany [11; 25].

Dalším klíčovým prvkem směrnice je oznamování bezpečnostních incidentů. Tato povinnost je strukturována do tří fází: včasné varování do 24 hodin, první hlášení do 72 hodin a závěrečná zpráva nejpozději do jednoho měsíce. Cílem je zajistit rychlou výměnu informací mezi organizacemi a příslušnými národními orgány, čímž se zvyšuje celková úroveň připravenosti a reakceschopnosti. Směrnice rovněž stanovuje, že subjekty musí informovat příjemce svých služeb, pokud incident může mít dopad na jejich bezpečnost [11; 24].

Směrnice NIS2 také posiluje dozorové a vynucovací pravomoci národních orgánů. Ty mohou ukládat sankce za neplnění povinností, provádět kontroly a vydávat závazná opatření. Členské státy jsou povinny zřídit nebo určit příslušné orgány dohledu, týmy CSIRT a jednotná kontaktní místa, která budou plnit koordinační úlohu při přeshraničních incidentech [24; 25].

4.2 Zákon č. 181/2014 Sb., o kybernetické bezpečnosti (ZoKB)

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, představuje základní právní předpis České republiky v oblasti ochrany sítí a informačních systémů. Jeho účelem je stanovit povinnosti subjektům, které provozují nebo spravují informační a komunikační infrastrukturu, a vymezit působnost Národního úřadu pro kybernetickou a informační bezpečnost. Zákon současně přejímá požadavky evropské legislativy a reaguje na potřebu jednotného a systematického přístupu k řízení bezpečnosti informací na národní úrovni [22].

V rámci vymezeného působení upravuje zákon povinnosti správců a provozovatelů významných informačních systémů, systémů základní služby, komunikačních systémů a prvků kritické informační infrastruktury. Těmto subjektům zákon ukládá povinnost zavést a udržovat tzv. bezpečnostní opatření. Tato opatření zahrnují jak technické, tak organizační

prvky a jejich cílem je zajištění důvěrnosti, integrity a dostupnosti informací zpracovávaných v rámci těchto systémů [7; 13].

Jedním ze stěžejních organizačních opatření, které zákon výslovně vyžaduje, je řízení rizik. Podle zákona je každá regulovaná osoba povinna provádět identifikaci, hodnocení a řízení rizik, která by mohla ohrozit bezpečnost jejích informačních aktiv. Tento proces musí být dokumentován a pravidelně aktualizován tak, aby odpovídal aktuálním hrozbám, technologiím a provozním podmínkám. Zákon rovněž stanovuje povinnost vést bezpečnostní dokumentaci, v níž musí být analýza rizik řádně popsána a doložena. Výstupy analýzy slouží jako podklad pro návrh dalších opatření, například zavedení kontrolních mechanismů, změny v organizační struktuře nebo posílení technického zabezpečení. Z pohledu kybernetické bezpečnosti se tedy jedná o základní předpoklad pro smysluplné řízení ochrany informačních systémů [13; 26].

Zákon č. 181/2014 Sb. také zavádí povinnost hlásit kybernetické bezpečnostní incidenty a přijímat opatření k jejich řešení. Hlásicí povinnost se vztahuje na subjekty veřejného i soukromého sektoru, přičemž úřad plní koordinační a dohledovou funkci. Povinnosti v oblasti hlášení i obsahu bezpečnostních opatření dále konkretizují prováděcí právní předpisy, které jsou zmíněny v následující části práce [13].

Význam tohoto zákona pro praktickou realizaci analýzy rizik spočívá především v tom, že z ní činí závazný a opakovaně prováděný proces. Subjekty, na které se zákon vztahuje, nejsou oprávněny provádět analýzu rizik pouze formálně, ale jsou povinny průběžně vyhodnocovat stav zabezpečení svých systémů a na základě toho činit konkrétní kroky k posílení své odolnosti vůči hrozbám [13; 26].

4.3 Národní úřad pro kybernetickou a informační bezpečnost

Národní úřad pro kybernetickou a informační bezpečnost je ústředním správním úřadem pro oblast kybernetické bezpečnosti v České republice. Zřízen byl zákonem č. 205/2017 Sb., kterým došlo k oddělení agendy kybernetické bezpečnosti od Národního bezpečnostního úřadu. Jeho právní postavení je vymezeno v § 21a zákona č. 181/2014 Sb., o kybernetické bezpečnosti. Podle tohoto ustanovení vykonává NÚKIB působnost státu v oblasti kybernetické bezpečnosti a pro vybrané oblasti ochrany utajovaných informací, přičemž sídlem úřadu je město Brno [22].

Úřad vykonává řadu činností v rámci státní správy, přičemž jeho hlavním úkolem je zajištění bezpečnosti sítí a informačních systémů, které jsou významné z hlediska fungování státu, veřejné správy nebo dalších kritických činností. NÚKIB zpracovává návrhy bezpečnostních opatření, vydává závazné předpisy ve formě opatření obecné povahy, kontroluje plnění zákonných povinností, vede správní řízení a v případě zjištění porušení zákona je oprávněn ukládat sankce. Je rovněž odpovědný za určování provozovatelů základních služeb a informačních systémů základní služby a za jejich kontrolu [13].

Součástí činností NÚKIB je také zajištění provozu vládního týmu CERT (GovCERT.CZ), který se specializuje na sběr, analýzu a řešení kybernetických bezpečnostních incidentů v systémech státní správy. Tým zajišťuje koordinaci při řešení incidentů, spolupráci s ostatními národními i mezinárodními CSIRT týmy a podílí se na prevenci a ochraně před hrozbami. NÚKIB má v rámci zákona oprávnění vystupovat jako koordinační orgán také v případě vyhlášení stavu kybernetického nebezpečí, jehož vyhlášení umožňuje zákon v situaci rozsáhlého ohrožení důvěrnosti, integrity nebo dostupnosti informací v sítích elektronických komunikací nebo informačních systémech [27; 28].

Vedle výkonu správních a kontrolních činností plní NÚKIB i úlohu odbornou a metodickou. Vydává doporučení, návody a metodiky, které slouží jako podpůrný rámec pro subjekty, na které se vztahují povinnosti stanovené zákonem o kybernetické bezpečnosti. Tato metodická podpora se týká především tvorby bezpečnostní dokumentace, zavádění bezpečnostních opatření a zejména vedení analýzy rizik [2].

NÚKIB zároveň působí jako hlavní aktér v oblasti osvěty, vzdělávání a zvyšování povědomí o problematice kybernetické bezpečnosti. Realizuje veřejné vzdělávací kampaně a školení zaměřené na různé cílové skupiny. Mezi nejznámější aktivity patří e-learningové kurzy „Dávej kyber!“, „Šéfuj kyber!“ a specializovaný program „Kyber nemocnice!“ pro zdravotnický sektor. Kromě vzdělávání se NÚKIB pravidelně účastní a organizuje národní i mezinárodní cvičení, například Locked Shields nebo sektorové simulace Health Czech, které umožňují testovat připravenost organizací na krizové situace [1].

Z pohledu analýzy rizik představuje NÚKIB zásadní instituci. Určuje rámec, podle kterého musí subjekty řízení rizik realizovat, a poskytuje metodickou podporu pro to, jak správně postupovat. Zároveň kontroluje, zda subjekty provádějí analýzu rizik v souladu s platnými právními předpisy a metodickými požadavky, a zda na základě výsledků této analýzy přijaly odpovídající bezpečnostní opatření. Výsledky analýzy rizik jsou proto

kontrolovatelným výstupem, který může být ze strany NÚKIB ověřován v rámci výkonu jeho kontrolních pravomocí [13].

4.4 Normy ISO/IEC řady 27000

Normy ISO/IEC řady 27000 představují mezinárodně uznávaný rámec pro řízení bezpečnosti informací. Tato skupina norem poskytuje jednotnou metodiku, terminologii a strukturu pro implementaci systému řízení bezpečnosti informací, který je založen na cyklu plánování, realizace, kontroly a zlepšování. V kontextu kybernetické bezpečnosti jsou tyto normy doporučovány jako nástroj pro systematické a opakovatelné posuzování, řízení a zmírňování rizik, zejména v prostředí veřejných institucí a regulovaných subjektů [22].

Klíčovou normou celé řady je ISO/IEC 27001, která specifikuje požadavky na zavedení, udržování a zlepšování systému řízení bezpečnosti informací. Umožňuje organizacím vymezit bezpečnostní cíle, identifikovat a hodnotit rizika, definovat opatření a pravidelně přezkoumávat jejich účinnost. ISO/IEC 27001 je zároveň základem pro certifikaci ISMS a bývá využívána jako referenční rámec při interním i externím hodnocení bezpečnostní zralosti organizací [22; 29].

Norma ISO/IEC 27002 doplňuje ISO/IEC 27001 a slouží jako soubor doporučených bezpečnostních opatření. Poskytuje konkrétní směrnice pro oblast řízení aktiv, lidských zdrojů, fyzické bezpečnosti, řízení přístupů, šifrování, incident managementu nebo řízení dodavatelů. Je využívána při plánování bezpečnostních politik a tvorbě konkrétních bezpečnostních pravidel na úrovni organizace. Z pohledu řízení rizik napomáhá správnému přiřazení opatření k identifikovaným hrozbám a zranitelnostem [22].

Z pohledu této práce má zásadní význam norma ISO/IEC 27005, která je zaměřena výhradně na řízení rizik v oblasti bezpečnosti informací. Poskytuje metodický rámec pro identifikaci aktiv, hrozeb, zranitelností, pravděpodobností a dopadů. Umožňuje organizacím stanovit míru rizika, provést její interpretaci a rozhodnout o vhodných způsobech ošetření rizik, například přijetím, zmírněním, přenesením nebo vyloučením. Norma zároveň zdůrazňuje nutnost průběžného přehodnocování rizik a zohlednění změn ve vnějším i vnitřním prostředí organizace [22; 30].

Vzhledem k zaměření této práce je norma ISO/IEC 27005 využívána jako podpůrný rámec pro systematické vedení analýzy rizik. Poskytuje logickou návaznost jednotlivých kroků hodnocení rizik, podporuje kvalifikované rozhodování o prioritizaci opatření a

umožňuje srovnatelnost výsledků mezi různými scénáři. Její použití napomáhá zajištění souladu s doporučeními NÚKIB i se směrnicí NIS2.

4.5 Národní strategie kybernetické bezpečnosti ČR 2021–2025

Národní strategie kybernetické bezpečnosti České republiky pro období let 2021–2025 představuje základní koncepční dokument, který formuluje cíle státu v oblasti ochrany kybernetického prostoru. Strategie je zpracována Národním úřadem pro kybernetickou a informační bezpečnost. Jedná se o strategický rámec, který usiluje o zajištění odolnosti státních institucí, kritické infrastruktury i celé společnosti vůči kybernetickým hrozbám [31].

Strategie je členěna do několika hlavních strategických cílů, které vycházejí z aktuálních výzev v oblasti informační bezpečnosti. Mezi tyto cíle patří například posilování schopnosti státu předcházet kybernetickým incidentům a reagovat na ně, rozvoj odborných kapacit, posílení spolupráce mezi veřejným a soukromým sektorem nebo podpora výzkumu a inovací. Významná pozornost je věnována také vzdělávání, zvyšování povědomí o kybernetické bezpečnosti a budování důvěry veřejnosti v digitální služby [31].

Z pohledu této práce je podstatné, že strategie vyzdvihuje důležitost řízení kybernetických bezpečnostních rizik jako jednoho z klíčových prvků systému ochrany informačních aktiv. Dokument stanovuje cíl rozšířit využívání analýzy rizik ve veřejné správě, zvýšit kvalitu výstupů tohoto procesu a zajistit, aby na jejich základě byla přijímána efektivní opatření. Strategie rovněž podporuje harmonizaci postupu při hodnocení rizik napříč sektory, včetně využívání jednotných rámců a metodických doporučení vytvořených NÚKIB [31].

Součástí strategie je i závazek státu podporovat implementaci směrnice NIS2, která posiluje požadavky na řízení rizik a bezpečnostní opatření v celé Evropské unii. V návaznosti na tuto směrnici klade strategie důraz na rozvoj standardizovaného přístupu k analýze hrozeb, zranitelností a dopadů na činnost institucí a služeb. Přijetí takového postupu umožňuje srovnatelnost výsledků napříč organizacemi a napomáhá efektivnímu rozhodování o prioritách v oblasti kybernetické ochrany [31].

Strategie rovněž zdůrazňuje význam pravidelného testování připravenosti institucí prostřednictvím cvičení, například ve spolupráci s NÚKIB, a podporuje zavádění preventivních opatření, která vycházejí z výsledků hodnocení rizik. V oblasti osvěty a vzdělávání se strategie opírá o podporu národních kampaní a vzdělávacích projektů, které

přispívají ke zvýšení úrovně bezpečnostního povědomí napříč veřejnou správou i mezi občany [31].

Z hlediska systematického řízení bezpečnosti informací představuje Národní strategie kybernetické bezpečnosti významný prvek, který propojuje politickou rovinu s odbornou praxí. Podporuje využívání mezinárodních norem, sdílení informací mezi subjekty a aktivní účast České republiky na formování evropské politiky kybernetické bezpečnosti. Jejím prostřednictvím stát deklaruje dlouhodobý závazek chránit informační aktiva veřejného sektoru a vytvářet podmínky pro bezpečné digitální prostředí [31].

II PRAKTICKÁ ČÁST

5 CHARAKTERISTIKA VYBRANÉHO SUBJEKTU

Analyzovaný subjekt působí ve veřejném sektoru v oblasti vzdělávání. Hlavním zaměřením činnosti je příprava a realizace vzdělávacích programů, které zahrnují odborné kurzy, semináře a specializační školení. Tyto vzdělávací aktivity jsou poskytovány formou prezenční i distanční výuky. Subjekt přitom zabezpečuje nejen samotnou výuku, ale rovněž organizační, technickou a administrativní podporu všech souvisejících procesů.

5.1 Organizační struktura

Organizační struktura subjektu je rozdělena do tří základních odborů, které se dále interně člení. První z nich je vzdělávací odbor, jehož odpovědností je vše, co přímo souvisí s přípravou a realizací vzdělávacích aktivit. Tento odbor má na starosti obsahovou náplň vzdělávání, komunikaci s externími lektory a účastníky kurzů, přípravu studijních materiálů a koordinaci samotné výuky.

Druhým je administrativní odbor, který zabezpečuje interní provozní procesy organizace. Mezi hlavní oblasti jeho působnosti patří organizační řízení subjektu, vedení mzdové a účetní agendy, personální správa zaměstnanců a správa vnitřních dokumentů. Tento odbor rovněž řídí interní komunikaci, koordinuje provozní záležitosti a zajišťuje administrativní podporu nezbytnou pro efektivní řízení a chod celé organizace.

Třetím odborem je odbor informatiky, který má na starosti správu a provoz informačních a komunikačních technologií organizace. Jeho činnost je nezbytná pro zajištění technické podpory všech částí organizace. Odbor informatiky zabezpečuje správu výpočetní techniky, audiovizuální techniky a infrastruktury informačních systémů. Mezi jeho hlavní odpovědnosti patří konfigurace a údržba systémů, aktualizace softwaru, správa databázových a aplikačních serverů, zabezpečení síťové infrastruktury a řízení přístupových práv. Důležitou součástí práce tohoto odboru je také pravidelná kontrola funkčnosti a zabezpečení provozovaných technologií, což z něj činí významnou technickou oporu pro bezproblémový chod celé organizace.

5.2 Fyzická infrastruktura a lokalita subjektu

Organizace realizuje svou činnost ve třech samostatných budovách, které se nacházejí na různých místech. Tyto budovy jsou přizpůsobeny potřebám vzdělávacích a podpůrných činností a jsou vzájemně propojeny sdílenou informační a komunikační infrastrukturou.

Výukové prostory zahrnují běžné učebny určené pro prezenční výuku a specializované učebny s počítačovým a audiovizuálním vybavením, umožňujícím realizaci specifických vzdělávacích programů. Některé učebny umožňují také hybridní výuku, kdy část účastníků absolvuje školení distanční formou.

Nezbytnou součástí infrastruktury organizace jsou tři serverovny. Jedna z těchto serveroven slouží jako centrální místo pro provoz klíčových informačních systémů a úložišť dat, zatímco zbývající dvě plní podpůrnou funkci. V serverovnách je instalováno vybavení pro zajištění nepřetržitého provozu systémů, včetně záložních napájecích zdrojů (UPS) a přepěťové ochrany.

Prostory serveroven jsou zabezpečeny poplachovým zabezpečovacím a tísňovým systémem (PZTS). Dohled nad těmito prostory je zajištěn kamerovým systémem. Pro monitorování podmínek uvnitř serveroven jsou používány senzory detekující teplotu, vlhkost, kouř či únik vody. Přístup do těchto místností je vyhrazen pouze pověřeným osobám.

5.3 Informační a komunikační infrastruktura

Informační a komunikační infrastruktura subjektu tvoří nezbytné technické zázemí pro realizaci všech činností organizace. Základním prvkem infrastruktury je lokální síť, která je rozdělena do několika logických segmentů podle účelu a způsobu využití. Síť je segmentována na část určenou zaměstnancům, část pro veřejnost (veřejně přístupná Wi-Fi síť), dále na síť učeben, oddělenou část pro vnitřní servery a vyhrazenou demilitarizovanou zónu (DMZ), která slouží pro provoz veřejně dostupných služeb. K řízení síťového provozování organizace využívá aktivní síťové prvky, které umožňují rozdělení provozu, zabezpečení sítě pomocí firewallu a monitoring síťové komunikace.

Serverová infrastruktura je založena převážně na virtualizačním řešení provozovaném v režimu on-premise, tedy přímo na infrastruktuře subjektu. V rámci této virtualizační platformy běží hlavní produkční aplikační a databázové servery, které jsou klíčové pro chod organizace a její informační systémy. Vedle této platformy je provozováno samostatné řešení pro zálohování dat a systémů, které zajišťuje pravidelné ukládání a obnovu dat v případě potřeby. Správa serverových systémů zahrnuje pravidelné aktualizace, správu konfigurací a kontrolu dostupnosti provozovaných služeb.

V organizaci jsou zaměstnanci vybaveni pracovními stanicemi, jejichž provoz a bezpečnost jsou spravovány centrálně pomocí nástrojů Microsoft Active Directory (AD). Tyto nástroje zajišťují řízení přístupových oprávnění, distribuci softwarových aktualizací a nastavení pracovních prostředí uživatelů. Pracovní stanice zaměstnanců jsou zabezpečeny pomocí pokročilého řešení typu EDR (Endpoint Detection and Response), zatímco počítače v učebnách využívají standardní řešení antimalwarové ochrany.

Z hlediska bezpečnosti a ochrany informačních aktiv organizace jsou implementována opatření, která mají obecně zajistit důvěrnost, integritu a dostupnost informací. V této souvislosti je kladen důraz na segmentaci sítě, kontrolu přístupových oprávnění k informačním systémům, ochranu před nežádoucími aktivitami prostřednictvím firewallu a monitoring provozu sítí a koncových zařízení.

6 IDENTIFIKACE AKTIV, HROZEB A ZRANITELNOSTÍ

V rámci analýzy kybernetické bezpečnosti je nezbytné přesně vymezit aktiva, jejichž narušení by mohlo negativně ovlivnit provozní kontinuitu nebo vést ke ztrátě či kompromitaci citlivých dat. Toto vymezení se zaměřuje na datová a aplikační aktiva, síťovou infrastrukturu, koncová zařízení a rovněž lidský faktor, přičemž u každé z těchto oblastí jsou následně popsány typické zranitelnosti a relevantní hrozby, které mohou vést k bezpečnostním incidentům.

6.1 Datová a aplikační aktiva

Datová a aplikační aktiva zahrnují fyzické servery, na kterých jsou provozovány virtualizační platformy umožňující běh virtuálních strojů a kontejnerů. Virtualizační technologie efektivně využívají technické zdroje a umožňují konsolidovat různé aplikace na menší počet fyzických zařízení. Pomocí virtualizace je možné pružněji reagovat na měnící se provozní požadavky, efektivněji řídit dostupné kapacity a snadněji spravovat informační systémy organizace. Provoz virtualizačních nástrojů však s sebou přináší také některé bezpečnostní zranitelnosti, jako jsou nedostatečně pravidelné aktualizace hypervisorů a nástrojů správy, slabá kontrola administrátorských účtů nebo nedostatečné oddělení a zabezpečení jednotlivých virtuálních sítí. Relevantní hrozby, které mohou uvedené zranitelnosti využít, zahrnují zejména neoprávněný přístup k administračním rozhraním virtualizačních platform, cílené zneužití známých bezpečnostních chyb hypervisorů či únik informací mezi jednotlivými virtuálními prostředím v důsledku nedostatečné izolace. Uvedené události mohou vést k narušení provozu kritických systémů organizace, úniku citlivých dat nebo k získání kontroly nad virtuálními prostředím neoprávněnou osobou.

K významným aktivům dále patří podnikové informační systémy, které zajišťují chod a podporu procesů organizace. Sem patří například aplikace určené pro ekonomickou agendu, systémy řízení lidských zdrojů, mzdové a personální aplikace, ale také vzdělávací platformy nebo e-learningová řešení. Nedílnou součástí těchto aktiv jsou rovněž databázové systémy, ve kterých jsou uložena a spravována data organizace, včetně dat zaměstnanců, obchodních partnerů nebo dalších interních údajů. K této skupině rovněž patří systémy pro centralizovanou správu identit a přístupových práv, typicky realizované prostřednictvím adresářových služeb, v tomto případě Active Directory. Organizace dále provozuje systémy vzdáleného přístupu, které umožňují zaměstnancům bezpečný přístup k pracovním aplikacím i mimo prostory organizace. Další významnou součástí jsou monitorovací a

dohledové systémy, které zajišťují kontrolu provozního stavu aplikací, sítí a hardwaru. Typickými zranitelnostmi těchto aktiv jsou zastaralý software bez aktuálních bezpečnostních záplat, slabé zabezpečení uživatelských účtů a chybné konfigurace aplikací či databázových systémů. Z těchto zranitelností vyplývají relevantní hrozby, například kybernetické útoky založené na škodlivém softwaru (malware, ransomware), phishingové útoky cílící na uživatele, útoky na webové aplikace typu SQL injection či neoprávněné ovládnutí administrátorských nebo uživatelských účtů.

Součástí informační infrastruktury organizace jsou rovněž systémy určené pro pravidelné zálohování dat, aplikací a konfigurací, které zajišťují jejich obnovitelnost v případě incidentu nebo technického selhání. Tyto systémy pravidelně vytvářejí kopie kritických dat z virtuálních prostředí, databází, aplikačních serverů a klíčových konfigurací. Vytvořené zálohy jsou ukládány na oddělená zabezpečená úložiště. Mezi obvyklé zranitelnosti zálohovacích systémů patří nedostatečné zabezpečení úložišť záloh, nepravidelné či neověřené zálohování a slabá kontrola přístupových práv k zálohovacím procesům a médiím. Relevantními hrozbami pro oblast zálohování jsou především cílené ransomware útoky, které mohou zašifrovat, poškodit nebo zcela znepřístupnit záložní data, interní chyby administrátorů vedoucí ke ztrátě důležitých informací nebo neoprávněné manipulace se zálohovanými daty. Tyto incidenty mohou významně ovlivnit schopnost organizace rychle obnovit provoz v případě kybernetického útoku nebo havárie.

6.2 Provoz síťové infrastruktury

Provoz síťové infrastruktury zahrnuje síťové prvky a zařízení, která zabezpečují interní i externí komunikační spojení organizace. K těmto aktivům patří přepínače (switche), směrovače (routery) a bezpečnostní zařízení typu firewall, jejichž funkcí je regulace přístupu mezi různými částmi sítě a ochrana před potenciálními kybernetickými hrozbami. Důležitou součástí infrastruktury jsou rovněž zařízení bezdrátové sítě (Wi-Fi), jako jsou přístupové body a jejich řídicí systémy. Pro zvýšení bezpečnosti a přehlednosti komunikačních toků jsou využívány síťové segmenty, často realizované prostřednictvím virtuálních sítí (VLAN), které umožňují izolaci jednotlivých síťových částí podle jejich bezpečnostních či provozních požadavků. Nedílnou součástí provozu sítě jsou také technologie pro vzdálený přístup uživatelů, typicky realizované pomocí VPN (Virtual Private Network), které poskytují uživatelům bezpečný přístup k vnitřním systémům z vnějšího prostředí.

Typické zranitelnosti síťové infrastruktury se týkají především nedostatečné aktualizace a konfigurace používaných síťových prvků. Mezi nejčastější patří zastaralý firmware síťových zařízení, slabě nastavená pravidla firewallu a neadekvátní zabezpečení síťových segmentů, které mohou umožnit neoprávněné přístupy a nežádoucí datové toky uvnitř organizace. V oblasti bezdrátového připojení bývá častou slabinou nedostatečné zabezpečení přístupových bodů či absence dostatečného šifrování přenášených dat. U vzdálených přístupů jsou problematické zejména slabé autentizační mechanismy a nedostatečná ochrana komunikačních kanálů. Nedostatky se také mohou projevit v nedostatečném monitorování síťového provozu, což snižuje schopnost detekovat a reagovat na bezpečnostní události včas.

Mezi relevantní hrozby, které mohou uvedené zranitelnosti zneužít, patří především neoprávněný přístup do interních částí infrastruktury, vedoucí k potenciálním únikům citlivých dat nebo kompromitaci systémů. Závažnou hrozbou jsou také distribuované DDoS útoky, které mohou omezit dostupnost služeb či narušit běžný provoz síťových zařízení organizace. U vzdálených přístupů představují významnou hrozbu pokusy o prolomení přihlašovacích údajů, například pomocí brute-force nebo credential stuffing útoků. Další vážnou bezpečnostní hrozbou je šíření škodlivého softwaru, například malware nebo ransomware, prostřednictvím slabě zabezpečených segmentů sítě. Nedostatečně zabezpečená bezdrátová infrastruktura může být rovněž vystavena riziku odposlechu přenášených informací nebo získání neoprávněného přístupu do sítě. Riziko interních incidentů navíc zvyšuje i nedostatečné sledování síťového provozu, které může vést k opožděnému odhalení nebo nedostatečné reakci na bezpečnostní incidenty.

6.3 Koncová zařízení

Koncová zařízení představují důležitou součást informační infrastruktury organizace. Jedná se především o pracovní stanice a notebooky, které zaměstnanci využívají při plnění každodenních pracovních úkolů, a dále o výpočetní techniku, která je umístěna v prostorách určených pro výuku či společná jednání. Mezi koncová zařízení patří také mobilní technologie, například chytré telefony nebo tablety, umožňující zaměstnancům bezpečný přístup k interním systémům a službám organizace, a to i mimo standardní pracovní prostory. Součástí těchto zařízení je rovněž instalovaný software, zejména operační systémy, kancelářské aplikace a bezpečnostní nástroje určené k ochraně dat a systémů.

Mezi nejčastější zranitelnosti koncových zařízení patří zastaralý či neaktualizovaný software, zejména operační systémy a aplikace, což výrazně zvyšuje riziko zneužití známých bezpečnostních chyb útočníky. Významnou slabinou bývá rovněž absence nebo nedostatečná úroveň antivirové a antimalwarové ochrany, která může vést k proniknutí škodlivého softwaru do zařízení. K dalším běžným nedostatkům patří slabé zabezpečení uživatelských účtů, jako jsou nevhodná hesla nebo absence silnější autentizace, což umožňuje potenciálním útočníkům získat neoprávněný přístup k zařízení a datům. Významnou zranitelností mobilních zařízení pak může být nedostatečné šifrování uložených dat nebo slabá kontrola jejich používání a správy ze strany organizace.

Relevantní hrozby, které se ke koncovým zařízením vztahují, zahrnují zejména phishingové útoky a další techniky sociálního inženýrství, které se snaží od uživatelů vylákat citlivé údaje či přístupové informace. K významným hrozbám patří rovněž infekce zařízení škodlivým softwarem, například typu ransomware nebo spyware, což může vést k úniku citlivých dat, zašifrování dat a následnému vydírání, případně k úplnému znepřístupnění zařízení. Další rizika zahrnují kompromitaci uživatelských účtů prostřednictvím slabých přihlašovacích údajů nebo jejich úniku, což umožňuje útočníkům neoprávněný přístup do interních systémů organizace. Nedostatečně zabezpečená mobilní zařízení dále představují zvýšené riziko ztráty nebo úniku informací mimo kontrolované prostředí. Tato koncová zařízení mohou být také zneužita jako vstupní bod k dalším cíleným útokům na kritickou infrastrukturu organizace, což klade důraz na nezbytnost jejich důsledného zabezpečení, pravidelného monitorování a vzdělávání uživatelů.

6.4 Lidské zdroje

Lidské zdroje představují zaměstnanci organizace, kteří při své každodenní činnosti využívají informační systémy a technologie. Z pohledu kybernetické bezpečnosti jsou významnou součástí také administrátoři a IT specialisté odpovědní za správu, konfiguraci a zabezpečení informačních systémů a technologií. S lidskými zdroji souvisejí rovněž interní procesy správy uživatelských účtů, nastavení přístupových práv a definice rolí jednotlivých zaměstnanců, které určují, jakým způsobem a v jakém rozsahu mohou zaměstnanci využívat interní systémy a data organizace.

Mezi typické zranitelnosti související s lidským faktorem patří zejména nedostatečné bezpečnostní povědomí zaměstnanců a nízká informovanost o kybernetických hrozbách. Zásadní slabinou bývá také slabá nebo nevhodně implementovaná pravidla správy

uživatelských účtů, hesel a přístupových oprávnění, což může vést k neoprávněným přístupům do systémů. Dalšími častými zranitelnostmi jsou absence pravidelného vzdělávání zaměstnanců v oblasti informační bezpečnosti a nedostatečná kontrola toho, zda zaměstnanci stanovená bezpečnostní pravidla skutečně dodržují. V neposlední řadě může organizaci ohrožovat také nejasné rozdělení odpovědnosti za dodržování bezpečnostních opatření a pravidel.

Relevantní hrozby v této oblasti jsou spojeny především s phishingovými útoky a metodami sociálního inženýrství, jejichž cílem je získat od zaměstnanců citlivé informace nebo přístupové údaje. Významnou hrozbou je také neúmyslný únik informací způsobený lidskou chybou nebo neopatrností při manipulaci s citlivými daty. Další riziko představuje neoprávněné použití přístupových oprávnění zaměstnanci v důsledku jejich kompromitace nebo nedostatečné správy těchto oprávnění. Nelze vyloučit ani možnost interních útoků či záměrného poškození dat ze strany zaměstnanců. Závažnou hrozbou je rovněž opožděná identifikace nebo nedostatečná reakce zaměstnanců na bezpečnostní incidenty, což může zhoršit jejich dopady na chod organizace a integritu interních systémů. Uvedené skutečnosti kladou důraz na potřebu systematického a kontinuálního vzdělávání zaměstnanců a zajištění kvalitního bezpečnostního řízení v celé organizaci.

7 ANALÝZA RIZIK

Analýza rizik je rozdělena dvou částí. Nejprve provedu analýzy SWOT a What-if, jejichž účelem je identifikovat silné a slabé stránky, příležitosti a hrozby v oblasti kybernetické bezpečnosti, a rovněž ověřit připravenost organizace na specifické scénáře hrozeb. Na základě těchto výsledků následně stanovím oblasti, které vyžadují podrobnější hodnocení metodou FMEA. Tento přístup umožní přesnější určení priorit v oblasti řízení rizik a efektivní návrh opatření pro zvýšení odolnosti organizace vůči identifikovaným hrozbám.

7.1 Dílčí závěr analýz SWOT a What-If

Dílčí závěr provedených analýz SWOT a What-if poukazuje na klíčové aspekty v oblasti řízení rizik kybernetické bezpečnosti vybrané organizace. Výsledky analýz ukazují, že organizace disponuje několika pozitivními předpoklady, které přispívají ke zvýšení její odolnosti vůči kybernetickým incidentům. Mezi tyto předpoklady lze zařadit především centralizované řešení virtualizační infrastruktury umožňující efektivní bezpečnostní správu, existenci redundantních řešení klíčových systémů, pravidelné zálohování kritických dat a využívání moderních technologií ochrany koncových zařízení a přístupů.

Nicméně analýzy zároveň identifikovaly několik oblastí, které vyžadují zvýšenou pozornost a efektivnější řízení rizik. Z hlediska technologických a organizačních zranitelností byly za nejvýznamnější označeny zejména nižší úroveň zabezpečení a testování zálohovacích systémů, absence pravidelné a centralizované správy bezpečnostních aktualizací a nedostatečný monitoring kybernetických incidentů v reálném čase. Významnou zranitelností se rovněž ukázala neúplná dokumentace infrastruktury a krizových scénářů obnovy dat a služeb.

V oblasti lidského faktoru analýzy potvrdily existenci rizik spojených s nízkou úrovní pravidelného vzdělávání zaměstnanců v otázkách kybernetické bezpečnosti a jejich nedostatečným zapojením do preventivních bezpečnostních opatření. Tyto nedostatky zvyšují pravděpodobnost úspěšných kybernetických útoků založených na sociálním inženýrství a zvyšují riziko úniku citlivých informací.

Na základě výsledků analýz SWOT a What-if byly pro podrobnější hodnocení metodou FMEA vybrány oblasti datových a aplikačních aktiv a oblast lidských zdrojů. Tyto oblasti byly zvoleny z důvodu jejich kritického významu pro zajištění provozní kontinuity organizace, vysoké míry závislosti ostatních systémů a procesů na jejich správném

fungování a zranitelnosti vůči identifikovaným hrozbám. Podrobná analýza těchto oblastí metodou FMEA umožní podrobnější identifikaci rizik, posouzení jejich závažnosti a následný návrh efektivních nápravných opatření.

7.2 Porovnání výsledků analýz a prioritizace rizik

Výsledky analýz potvrdily existenci silných stránek, které pozitivně ovlivňují úroveň kybernetické bezpečnosti organizace, zejména v oblasti technického stavu infrastruktury a používaných technologií. Mezi ně patří centralizovaná virtualizační infrastruktura, která umožňuje jednotnou správu bezpečnosti, redundantní řešení klíčových systémů, pravidelné zálohování dat na samostatná úložiště a implementace moderních technologií na ochranu koncových zařízení a uživatelských přístupů.

Analýzy zároveň upozornily na několik oblastí s potenciálními nedostatky, které vyžadují zvýšenou pozornost. První důležitou oblastí je správa a zabezpečení zálohovacích systémů. Byly identifikovány možné nedostatky týkající se geografického oddělení zálohovacích úložišť od primární infrastruktury, což by mohlo v případě vážného incidentu ohrozit obě umístění současně. Dále se ukázala nepravidelnost ověřování funkčnosti záloh, což zvyšuje riziko jejich selhání v kritických situacích. Slabší zabezpečení přístupů k zálohovacím systémům rovněž představuje možné riziko neoprávněného přístupu a manipulace s daty.

Další významnou oblastí je řízení přístupů a aktualizací, kde byly odhaleny potenciální problémy, jež mohou negativně ovlivnit celkovou bezpečnost organizace. Mezi identifikovaná rizika patří provozování zastaralých verzí softwaru, což může vést ke zranitelnostem a vyššímu riziku kybernetických útoků. Nedostatečná kontrola přístupových oprávnění může rovněž umožnit neoprávněný přístup k citlivým informacím. Dalším problémem je možná zranitelnost fyzické infrastruktury při výpadcích napájení, což by mohlo způsobit závažné provozní problémy a ohrozit dostupnost klíčových systémů.

V oblasti lidských zdrojů analýzy upozornily na možné nedostatky ovlivňující bezpečnostní povědomí a chování zaměstnanců. Mezi hlavní rizika patří potenciální náchylnost k phishingovým útokům, nedostatečná kontrola přístupových práv, neopatrné zacházení s citlivými daty a rizikové sdílení přístupových údajů mezi zaměstnanci. Další problémy zahrnují možnou nedostatečnost ve frekvenci a obsahu bezpečnostních školení, nedodržování interních bezpečnostních politik, absenci specializovaných školení pro administrátory a IT pracovníky, nedostatečné rušení přístupových práv po odchodu

zaměstnanců, nejasnosti ohledně zaměření testování znalostí a nízkou frekvenci těchto testů, což může snížit efektivitu celkových bezpečnostních opatření.

Poslední oblastí s potenciálními problémy je dokumentace procesů, infrastruktury a krizových scénářů. Analýzy odhalily nedostatky v úplnosti, aktuálnosti a dostupnosti dokumentace klíčových procesů, což komplikuje bezpečnostní správu a schopnost efektivně reagovat na incidenty. Nedostatečně aktualizovaná dokumentace infrastruktury vytváří nejistotu ohledně jejího skutečného stavu a omezuje možnosti rychlé identifikace a řešení problémů. Byly také zjištěny mezery v dokumentaci krizových scénářů a postupů, jejichž absence nebo nedostatečnost může významně zvýšit riziko chybného nebo opožděného rozhodování při řízení krizových situací.

Realizace navržených opatření v uvedených oblastech přispěje ke zvýšení celkové úrovně kybernetické bezpečnosti organizace. Systematické řešení identifikovaných nedostatků posílí schopnost organizace efektivně reagovat na aktuální kybernetické hrozby a zároveň zvýší její odolnost vůči potenciálním rizikům v budoucnu.

8 NÁVRH BEZPEČNOSTNÍCH OPATŘENÍ

Na základě provedených analýz byla identifikována doporučení pro vybrané oblasti kybernetické bezpečnosti. Organizace disponuje omezenými zdroji, které je nutné alokovat efektivně a s ohledem na priority, jež byly stanoveny výsledky těchto analýz. Bezpečnost je však kontinuální proces, a proto by měla organizace pravidelně přehodnocovat svá opatření a přizpůsobovat je aktuálním hrozbám a možnostem. Z těchto důvodů byla doporučení rozčleněna do následujících klíčových oblastí, jejichž cílem je optimální využití dostupných kapacit a zvýšení celkové úrovně zabezpečení organizace.

V oblasti zálohování dat a aplikací se doporučuje zavést systematický proces pravidelného ověřování obnovitelnosti záloh, což zajistí, že v případě potřeby bude možné data skutečně obnovit, a tím minimalizovat riziko nedostupnosti kritických systémů a služeb. Rovněž je vhodné implementovat geografické oddělení zálohovacích systémů od primární infrastruktury v souladu s pravidlem zálohování 3-2-1, které doporučuje uchovávat alespoň tři kopie dat, na dvou různých typech úložišť, přičemž alespoň jedna kopie by měla být umístěna mimo primární lokalitu. Tím se výrazně sníží riziko ztráty dat v případě fyzického poškození nebo jiné události ohrožující hlavní úložiště. Dále je doporučeno zvážit posílení zabezpečení přístupů k zálohovaným datům, například implementací šifrování nebo jiných mechanismů přístupových oprávnění, které odpovídají aktuálním bezpečnostním standardům.

V oblasti vzdělávání zaměstnanců se doporučuje zavedení pravidelného, systematického a kontinuálního vzdělávacího programu zaměřeného na zvýšení bezpečnostního povědomí. Za tímto účelem je vhodné navázat spolupráci s odborem vzdělávání, který může pomoci s vytvořením a realizací efektivního vzdělávacího programu. Obsah školení by měl být přizpůsoben aktuálním hrozbám s ohledem na doporučení Národního úřadu pro kybernetickou a informační bezpečnost, jehož vzdělávací programy mohou sloužit jako inspirace. Program by měl rovněž reflektovat aktuální trendy a poznatky uvedené v pravidelných zprávách a doporučeních NÚKIB, a zaměřit se obecně na zvýšení povědomí zaměstnanců o aktuálních formách kybernetických útoků a na jejich motivaci aktivně se zapojovat do preventivních bezpečnostních opatření. Dále je důležité pravidelně zdůrazňovat rizika spojená se sdílením přístupových údajů mezi zaměstnanci a zařadit do programu specifické pokyny a pravidla, jak těmto situacím předcházet. Součástí vzdělávacího programu by mělo být rovněž pravidelné ověřování znalostí zaměstnanců, jehož četnost a obsah by měly být přesněji definovány a pravidelně aktualizovány podle

vývoje kybernetických hrozeb a doporučení odborných institucí. Kromě toho je doporučeno zaměřit se také na pravidelné a specializované vzdělávání IT pracovníků, které jim umožní získávat a udržovat odborné znalosti potřebné pro správnou správu a ochranu informačních systémů a technologií.

V oblasti využití technických nástrojů pro podporu kybernetické bezpečnosti je doporučeno implementovat centralizovanou správu bezpečnostních aktualizací operačních systémů a uživatelských aplikací. Dále je vhodné nasadit nástroje pro monitoring bezpečnostních incidentů v reálném čase napříč celou infrastrukturou, které umožní včasnou detekci a rychlou reakci na případné incidenty. Tyto nástroje mohou efektivně automatizovat časově náročné procesy, zajistit pravidelnost a jednotnost aktualizací napříč celou organizací a tím významně zvýšit úroveň jejího zabezpečení. Dalším doporučeným opatřením je automatizace deaktivace uživatelských účtů po odchodu zaměstnanců. Tato automatizace zajistí okamžité odebrání přístupových práv, čímž se minimalizuje riziko neoprávněného přístupu k citlivým datům a systémům.. Dalším doporučeným opatřením je implementace záložních generátorů nebo bateriových systémů, které zajistí kontinuitu provozu infrastruktury při výpadcích elektrické energie, a tím významně sníží zranitelnost organizace vůči provozním problémům způsobeným výpadky napájení.

Poslední oblastí doporučení je dokumentace a zavedení jasně definovaných procesů a krizových scénářů. Součástí těchto procesů by měly být rovněž pravidelné audity a revize přístupových oprávnění, které zajistí, že oprávnění zaměstnanců odpovídají jejich aktuálním pracovním rolím. To minimalizuje riziko neoprávněného přístupu k citlivým informacím a zvyšuje celkovou bezpečnost organizace. Výše zmíněné procesy a krizové scénáře vyžadují kompletní, aktuální a srozumitelnou dokumentaci, která poskytuje pevný základ pro efektivní řízení kybernetické bezpečnosti a úspěšné řešení případných bezpečnostních incidentů. Význam kvalitní dokumentace je rovněž zdůrazněn evropskou směrnicí NIS2 a standardy pro řízení informační bezpečnosti, které kladou důraz na jasně definované procesy, řízení dokumentů a opatření, jejichž účinnost by měla být pravidelně ověřována. Z tohoto důvodu se doporučuje zajistit pravidelnou aktualizaci dokumentace, její dostupnost všem relevantním zaměstnancům a pravidelné ověřování funkčnosti v rámci cvičení nebo simulací krizových scénářů. Tento přístup umožní organizaci efektivněji zvládat krizové situace a minimalizovat jejich dopady v souladu s legislativními požadavky.

ZÁVĚR

Tato bakalářská práce se zabývala analýzou kybernetických rizik u vybraného subjektu a návrhem opatření pro jejich řízení. V teoretické části jsem se nejprve zaměřil na současný stav kybernetické bezpečnosti v České republice, kde jsem analyzoval zprávy vydané institucemi NÚKIB a ENISA, uvedl příklady významných kybernetických incidentů, jejich dopady na organizace i širší společnost a zdůraznil potřebu systematického přístupu k řízení kybernetických rizik. Dále jsem definoval klíčové pojmy jako CIA triáda, typy kybernetických hrozeb a zranitelností a popsal metody používané k analýze rizik. Dále jsem představil legislativní rámec a relevantní normy, abych poskytl ucelený kontext potřebný pro správné pochopení a efektivní aplikaci bezpečnostních opatření v praxi.

V praktické části práce jsem nejprve obecně charakterizoval vybraný subjekt, jeho organizační strukturu, fyzickou infrastrukturu a informační systémy. Poté jsem vymezil rozsah analýzy, identifikoval klíčová aktiva organizace a provedl analýzu relevantních hrozeb a zranitelností. Provedl jsem podrobnou analýzu rizik s využitím SWOT analýzy a metod What-If a FMEA, což mi umožnilo identifikovat a seřadit prioritní oblasti podle závažnosti identifikovaných rizik a významu jednotlivých aktiv pro organizaci. Výsledkem tohoto hodnocení byl návrh konkrétních bezpečnostních opatření, která respektují doporučení směrnice NIS2 a jejichž implementace přispěje ke zvýšení kybernetické odolnosti dané organizace a zajištění kontinuity provozu jejích informačních systémů.

Vypracování této bakalářské práce pro mě bylo přínosnou zkušeností. Zpočátku se téma jevilo jako značně rozsáhlé a náročné, avšak díky postupnému a systematickému přístupu se mi podařilo téma úspěšně zvládnout. Během zpracování práce jsem se seznámil s různými metodami analýzy kybernetických rizik, osvojil si jejich praktickou aplikaci a pochopil důležitost systematického a důsledného přístupu k bezpečnosti informací. Získané poznatky a zkušenosti plánuji využít nejen ve svém profesním životě, ale věřím, že tato práce může být užitečná i pro ostatní organizace či jednotlivce, kteří se chtějí seznámit s problematikou kybernetické bezpečnosti.

SEZNAM POUŽITÉ LITERATURY

- [1] NÚKIB. Zpráva o stavu kybernetické bezpečnosti ČR za rok 2023. Online. 2024. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2023.pdf. [cit. 2025-05-20].
- [2] NÚKIB. Zpráva o stavu kybernetické bezpečnosti ČR za rok 2022. Online. 2023. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kyberneticke_bezpecnosti_CR_za_rok_2022.pdf. [cit. 2025-05-20].
- [3] NÚKIB. Zpráva o stavu kybernetické bezpečnosti ČR za rok 2021. Online. 2022. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kybernetick_bezpenosti_2021.pdf. [cit. 2025-05-20].
- [4] NÚKIB. Zpráva o stavu kybernetické bezpečnosti ČR za rok 2020. Online. 2021. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_KB_2020.pdf. [cit. 2025-05-20].
- [5] NÚKIB. Upozornění na zvýšené riziko DDoS útoků. Online. 2022. Dostupné z: https://nukib.gov.cz/download/aktuality/221101_upozornn%20na%20riziko%20DDoS%20tok.pdf. [cit. 2025-05-20].
- [6] ENISA. ENISA THREAT LANDSCAPE 2024. Online. 2024. Dostupné z: https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf. [cit. 2025-05-20].
- [7] NÚKIB. Legislativita kybernetické bezpečnosti. Online. 2025. Dostupné z: <https://nukib.gov.cz/cs/kyberneticka-bezpecnost/regulace-a-kontrola/legislativa/>. [cit. 2025-05-20].
- [8] ÚGKK SR. Aktuálne informácie k situácii v rezorte ÚGKK SR. Online. 2025. Dostupné z: <https://www.skgeodesy.sk/sk/ugkk/aktualne-informacie-k-situacii-rezorte-ugkk-sr/>. [cit. 2025-05-20].
- [9] NBÚ SR. Aktuálne informácie v prípade kybernetického útoku na ÚGKK SR. Online. 2025. Dostupné z: <https://www.nbu.gov.sk/aktualne-informacie-v-pripade-kybernetickeho-utoku-na-urad-geodezie-kartografie-a-katastra-sr/>. [cit. 2025-05-20].

- [10] DOUCEK, Petr; KONEČNÝ, Martin a NOVÁK, Luděk. Řízení kybernetické bezpečnosti a bezpečnosti informací. Professional Publishing, 2019. ISBN 978-80-88260-39-4.
- [11] EVROPSKÁ UNIE. 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 NIS 2). Online. In: Úřední věstník Evropské unie. 2022. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32022L2555>. [cit. 2025-05-20].
- [12] KOLOUCH, Jan a BAŠTA, Pavel. CyberSecurity. CZ.NIC, 2019. ISBN 9788088168317.
- [13] ČESKO. Zákon č. 181/2014 Sb. ze dne 23. července 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Online. In: . Dostupné z: <https://www.e-sbirka.cz/sb/2014/181?zalozka=text>. [cit. 2025-05-20].
- [14] JIRÁSEK, Petr; NOVÁK, Luděk a POŽÁR, Josef. Výkladový slovník Kybernetické bezpečnosti. Online. 2015. Dostupné z: https://www.cybersecurity.cz/data/slovník_v310.pdf. [cit. 2025-05-20].
- [15] NÚKIB. Analýza hrozby ransomware. Online. 2020. Dostupné z: https://nukib.gov.cz/download/publikace/analyzy/Analyza_hrozby_ransomware.pdf. [cit. 2025-05-20].
- [16] SEDLÁK, Petr a NOVÁK, Luděk. Přeměna ISMS v manažerské informatice. CERM, akademické nakladatelství, 2023. ISBN 978-80-88260-39-4.
- [17] NEXT GENERATION SECURITY SOLUTIONS. Techniky identifikace a analýzy rizik. Online. 2022. Dostupné z: <https://www.ngss.cz/clanek/techniky-identifikace-a-analyzy-rizik-2022-01-28>. [cit. 2025-05-20].
- [18] ATLASSIAN. What is a SWOT analysis. Online. 2025. Dostupné z: <https://www.atlassian.com/work-management/strategic-planning/swot-analysis>. [cit. 2025-05-20].

- [19] WOELKE, Karolina; GRUBER, Harald a VLKOVÁ, Šárka. Příručka pro hodnocení rizik v malých a středních podnicích. ISSA, 2012. ISBN 978-80-86973-71-5.
- [20] ČESKÁ SPOLEČNOST PRO JAKOST. Úloha a aplikační možnosti metody FMEA při zabezpečování spolehlivosti. 2001. Online. Dostupné z: https://www.csq.cz/fileadmin/user_upload/Clenstvi/Centra/Sborniky_spolehlivost/05_FMEA.pdf. [cit. 2025-05-20].
- [21] CRDR Metody a způsoby hodnocení rizik na pracovišti. Online. 2018. Dostupné z: <https://www.dokumentacebozp.cz/aktuality/metody-hodnoceni-rizik-bozp>. [cit. 2025-05-20].
- [22] SMEJKAL, Vladimír; SOKOL, Tomáš a KODL, Jindřich. Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti. Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.
- [23] EVROPSKÁ UNIE. 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. In: Úřední věstník Evropské unie. 2016. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN>. [cit. 2025-05-20].
- [24] NÚKIB. Průvodce směrnicí NIS2. Online. 2025. Dostupné z: <https://portal.nukib.gov.cz/pruvodce-smernici-nis2>. [cit. 2025-05-20].
- [25] NÚKIB. New EU Directive on Cyber Security „NIS2“ and proposal of the NEW ACT ON CYBER SECURITY. Online. 2023. Dostupné z: <https://osveta.nukib.gov.cz/course/view.php?id=168#section-14>. [cit. 2025-05-20].
- [26] NÚKIB. Průvodce novým zákonem o kybernetické bezpečnosti. Online. 2025. Dostupné z: <https://portal.nukib.gov.cz/pruvodce-novym-zakonom-o-kyberneticke-bezpecnosti>. [cit. 2025-05-20].
- [27] RAMEŠOVÁ, Kristina. Právní regulace kybernetické bezpečnosti a její meze. C. H. Beck, 2023. ISBN 978-80-7400-931-0.

- [28] NCKB. Kybernetická bezpečnost. Online. 2025. Dostupné z: <https://nukib.gov.cz/cs/kyberneticka-bezpecnost/>. [cit. 2025-05-20].
- [29] IBM. What is ISO 27001. Online. 2022. Dostupné z: <https://www.ibm.com/cloud/compliance/iso-27001>. [cit. 2025-05-20].
- [30] FORÊT, Christophe. ISO 27005: summary, requirements, pros and cons. Online. In: C-RISK. 2023. Dostupné z: <https://www.c-risk.com/blog/iso-27005>. [cit. 2025-05-20].
- [31] NÚKIB. Národní strategie kybernetické bezpečnosti 2020-2025. Online. 2020. Dostupné z: https://nukib.gov.cz/download/publikace/strategie_akcni_plany/narodni_strategie_kb_2020-2025_%20cr.pdf. [cit. 2025-05-20].

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CIA	Confidentiality, Integrity, Availability (důvěrnost, integrita, dostupnost)
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial of Service (distribuované odepření služby)
DMZ	Demilitarized Zone (demilitarizovaná zóna)
EDR	Endpoint Detection and Response
ENISA	European Union Agency for Cybersecurity (Evropská agentura pro kybernetickou bezpečnost)
EU	Evropská unie
FIMI	Foreign Information Manipulation and Interference (zahraniční informační manipulace a interference)
FMEA	Failure Mode and Effects Analysis (analýza možných vad a jejich následků)
ICT	Information and Communication Technologies (informační a komunikační technologie)
IDS/IPS	Intrusion Detection System / Intrusion Prevention System (systém detekce/průniku)
ISMS	Information Security Management System (systém řízení bezpečnosti informací)
IT	Information Technology (informační technologie)
LOTS	Living Off Trusted Sites (využívání legitimních důvěryhodných stránek pro kybernetické útoky)
NATO	North Atlantic Treaty Organization (Severoatlantická aliance)
NIS2	Network and Information Security Directive 2 (směrnice EU o bezpečnosti sítí a informačních systémů)
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PDCA	Plan–Do–Check–Act (plánuj–dělej–ověřuj–jednej)
PZTS	Poplachový zabezpečovací a tísňový systém

RPN	Risk Priority Number (číselné vyjádření priority rizika)
SQL	Structured Query Language (strukturovaný dotazovací jazyk)
SWOT	Strengths, Weaknesses, Opportunities, Threats (silné stránky, slabé stránky, příležitosti, hrozby)
UPS	Uninterruptible Power Supply (nepřerušitelný zdroj napájení)
VLAN	Virtual Local Area Network (virtuální lokální síť)
VPN	Virtual Private Network (virtuální privátní síť)
Wi-Fi	Wireless Fidelity (bezdrátová síťová technologie)

SEZNAM PŘÍLOH

Příloha P I: Výsledky SWOT analýz

Příloha P II: What-if analýzy

Příloha P III: FMEA analýzy

PŘÍLOHA P I: VÝSLEDKY SWOT ANALÝZ

SWOT analýza datových a aplikačních aktiv

Silné stránky – současné bezpečnostní výhody	Slabé stránky – současné bezpečnostní nedostatky
- Centralizovaná virtualizační infrastruktura umožňující jednotnou bezpečnostní správu a kontrolu. - Pravidelné zálohování dat a aplikací na oddělené NAS uložení mimo hlavní infrastrukturu. - Většina klíčových systémů integrována do jednotné centrální správy přístupů. - Existující dohledový systém umožňující průběžný monitoring bezpečnostních incidentů.	- Nedostatečná aplikace bezpečnostních aktualizací (riziko zastaralého softwaru). - Chybějící pravidelné testování záloh (riziko ztráty nebo nedostupnosti dat). - Neúplná integrace aplikací do centrální správy oprávnění (vyšší riziko neoprávněného přístupu). - Nedostatečný monitoring v reálném čase (omezená schopnost včasné detekce hrozeb). - Nízká kontrola bezpečnosti externě spravovaných aplikací (riziko nekontrolovaných zranitelností).
Příležitosti – možnosti zlepšení bezpečnosti	Hrozby – potenciální bezpečnostní rizika
- Rostoucí nabídka automatizovaných nástrojů pro správu bezpečnostních aktualizací aplikací a operačních systémů na trhu. - Legislativní a regulační požadavky (např. NIS2, ISO 27001) podporující lepší integraci systémů do centrální správy přístupů a ověřování bezpečnosti dat. - Rostoucí dostupnost pokročilých monitorovacích řešení s využitím behaviorální analýzy a AI pro včasnou detekci incidentů na aplikační vrstvě. - Dostupnost nezávislých externích auditorů a bezpečnostních konzultantů umožňujících objektivní posouzení bezpečnostního stavu dat a aplikací.	- Zneužití zranitelností neaktualizovaných systémů. - Neoprávněný přístup k citlivým datům kvůli nedostatečné správě oprávnění. - Nedostupnost klíčových dat a aplikací způsobená netestovanými procesy obnovy. - Únik citlivých dat vlivem kompromitace aplikací spravovaných externími dodavateli. - Závažné incidenty neodhalené včas kvůli omezenému monitoringu aplikační infrastruktury.

SWOT analýza provozu síťové infrastruktury

Silné stránky – současné bezpečnostní výhody	Slabé stránky – současné bezpečnostní nedostatky
• Oddělení síťových segmentů (VLAN) omezující šíření incidentů. • Centrální správa firewallů umožňující efektivní řízení přístupů. • Vzdálený přístup (VPN) zajišťující chráněnou externí komunikaci. • Redundantní síťová spojení zvyšující dostupnost kritických systémů. • Monitoring síťových prvků pro rychlou detekci výpadků. • Centralizované ukládání logů umožňující retrospektivní analýzu incidentů.	• Omezený monitoring síťových bezpečnostních incidentů v reálném čase. • Neúplná dokumentace síťové infrastruktury komplikující řešení incidentů. • Vystavené webové služby do internetu představující potenciální cíl útoků. • Základní zabezpečení veřejné Wi-Fi se zvýšeným rizikem zneužití. • Nedostatečné zálohování konfigurací síťových zařízení pro případ obnovy.
Příležitosti – možnosti zlepšení bezpečnosti	Hrozby – potenciální bezpečnostní rizika
• Zvyšující se dostupnost pokročilých řešení IDS/IPS na trhu, umožňující lepší detekci a prevenci útoků cílených na síťovou infrastrukturu. • Rozšířená nabídka specializovaných externích firem provádějících penetrační testy a audity síťové bezpečnosti, umožňující včasnou detekci slabých míst a návrh zlepšení. • Legislativní tlak motivující organizace k pravidelnému ověřování bezpečnostního stavu a dokumentaci síťové infrastruktury. • Rostoucí dostupnost a cenová přístupnost moderních nástrojů pro automatizované zálohování konfigurací síťových zařízení, zajišťující rychlejší obnovu po incidentu	• Cílené DDoS útoky s narůstající intenzitou, schopné způsobit nedostupnost kritických služeb organizace. • Zneužívání kritických zranitelností v síťových zařízeních a protokolech, které organizace nedokáže dostatečně rychle detekovat a odstranit. • Externí snahy o neoprávněný přístup a narušení služeb prostřednictvím vystavených veřejných síťových rozhraní a webových služeb organizace. • Zvyšující se komplexnost a sofistikovanost útoků na veřejné Wi-Fi sítě, vedoucí k riziku odposlechu či kompromitace uživatelských dat.

SWOT analýza koncových zařízení

Silné stránky – současné bezpečnostní výhody	Slabé stránky – současné bezpečnostní nedostatky
- Nasazení EDR řešení na koncových stanicích zajišťující pokročilou detekci incidentů. - Antivirová a antimalware ochrana koncových zařízení v učebnách. - Používání VPN pro zabezpečený vzdálený přístup do interních služeb. - Centrální správa bezpečnostních politik na koncových zařízeních. - Využití šifrování úložišť koncových zařízení.	- Chybějící centralizovaná správa aktualizací OS a firmware na zařízeních mimo vnitřní síť. - Absence centrální správy aktualizací uživatelských aplikací (Office, prohlížeče, PDF). - Absence MDM systému pro správu a zabezpečení mobilních zařízení. - Využívání firemních zařízení pro soukromé účely zvyšující bezpečnostní rizika. - Zvýšené riziko bezpečnostních incidentů na PC v učebnách z důvodu jejich používání externími uživateli.
Příležitosti – možnosti zlepšení bezpečnosti	Hrozby – potenciální bezpečnostní rizika
- Dostupnost moderních cloudových platform pro centralizovanou správu aktualizací OS, firmware a uživatelských aplikací. - Rostoucí nabídka Mobile Device Management (MDM) řešení na trhu pro správu a zabezpečení mobilních zařízení. - Zvýšená podpora výrobců zařízení a softwaru v oblasti pravidelných bezpečnostních aktualizací a automatizace jejich nasazování. - Rostoucí legislativní a regulatorní důraz na posilování zabezpečení koncových zařízení a jejich centralizovanou správu.	- Zneužití známých zranitelností neaktualizovaných OS a aplikací na koncových zařízeních. - Nárůst kybernetických útoků cílených specificky na mobilní zařízení, využívajících jejich slabší zabezpečení a absenci centrální správy. - Riziko fyzické krádeže či ztráty přenosných zařízení vedoucí k potenciálnímu úniku citlivých dat organizace. - Riziko zneužití PC v učebnách v důsledku jejich častého využívání externími uživateli, zvyšující pravděpodobnost kompromitace.

SWOT analýza lidských zdrojů

Silné stránky – současné bezpečnostní výhody	Slabé stránky – současné bezpečnostní nedostatky
• Roční testování uživatelů v oblasti kybernetické bezpečnosti. • Zapojení vedení organizace do prosazování kybernetické bezpečnosti. • Interní komunikace bezpečnostních rizik a incidentů zaměstnancům. • Využívání vícefaktorové autentizace (2FA) uživatelských účtů.	• Absence pravidelných interních školení zaměstnanců v oblasti kybernetické bezpečnosti. • Chybějící interní dokumentace a návody pro bezpečné chování zaměstnanců. • Slabá podpora zaměstnanců v oblasti identifikace a hlášení podezřelých aktivit. • Nízká míra zapojení zaměstnanců do prevence kybernetických hrozeb. • Nízká motivace zaměstnanců k aktivnímu dodržování pravidel kybernetické bezpečnosti.
Příležitosti – možnosti zlepšení bezpečnosti	Hrozby – potenciální bezpečnostní rizika
• Dostupné vzdělávací programy NÚKIB • Možnost čerpat dotační podporu na kybernetickou bezpečnost • Dostupnost externích odborníků a konzultačních služeb • Technologický pokrok v bezpečnostních řešeních (AI, cloud).	• Úspěšné phishingové útoky cílené na zaměstnance. • Riziko úniku informací v důsledku cílených externích útoků • Zneužití sociálního inženýrství vůči zaměstnancům. • Rostoucí sofistikovanost útoků ztěžující jejich identifikaci • Nárůst práce na dálku zvyšující riziko nedodržování pravidel.

PŘÍLOHA P II: WHAT-IF ANALÝZY

What-if analýza datových a aplikačních aktiv

Co když ransomware cílí přímo na záložní data? Má organizace nasazenou dostatečnou ochranu těchto záloh, která zajistí jejich odolnost vůči poškození nebo zašifrování?

Organizace provádí zálohování na několika úrovních, a to na úrovni aplikací, databází, virtualizace a síťového úložiště NAS. V případě, že by došlo k poškození jednoho druhu záloh, měly by zbývající typy záloh zajistit dostupnost potřebných dat.

Co když dojde k výpadku nebo poškození virtuálních strojů? Má organizace definované a ověřené postupy, které umožní jejich rychlou obnovu ze záloh?

Ano, organizace má stanovené postupy pro rychlou obnovu VM.

Co když nastane situace vyžadující rychlou obnovu ze záloh? Má organizace jistotu, že zálohy půjde bez problémů obnovit?

Organizace v současnosti pravidelné testování obnovitelnosti záloh neprovádí.

Co když bude nutné obnovit konkrétní data nebo konfigurace z určitého časového bodu v minulosti, dokáže organizace obnovit data ze starší verze záloh?

Ano, zálohy jsou pravidelně uchovávány ve více verzích, což umožňuje obnovu starších dat nebo konfigurací dle potřeby.

Co když dojde k fyzickému poškození nebo nedostupnosti primární lokality, kde jsou uloženy zálohy? Uchovává organizace zálohy aplikací a dat také na jiném místě, aby bylo možné data obnovit i při ztrátě hlavního úložiště?

Zálohy aplikací a databází organizace ukládá pouze na úložiště NAS ve stejné lokalitě jako primární infrastruktura. Žádné další zálohy na jiné fyzické lokalitě v současnosti neexistují.

Co když nastane situace vyžadující rychlou obnovu konkrétních aplikací a dat? Má organizace detailně zdokumentované postupy obnovy pro všechny důležité aplikace?

Organizace má obecně zdokumentovány základní postupy obnovy dat, avšak pro některé aplikace detailní postupy obnovy chybí.

Co když dojde k výpadku serveru adresářové služby? Má organizace zajištěnu redundanci pro zachování dostupnosti správy přístupových oprávnění?

Ano, adresářová služba je provozována redundantně na dvou serverech, takže v případě výpadku jednoho serveru zůstává dostupná.

Co když výrobce aplikace nebo operačního systému vydá kritickou bezpečnostní aktualizaci opravující závažnou zranitelnost? Je organizace schopna tuto aktualizaci aplikovat dostatečně rychle?

Pokud aplikaci dodává nebo spravuje externí dodavatel, aktualizaci provedeme ve spolupráci s ním v nejkratším možném termínu. Obecné aktualizace operačních systémů spravovaných interně provádíme ručně v pravidelných intervalech.

Co když dojde k bezpečnostnímu incidentu v aplikační infrastruktuře? Je dohledový systém organizace schopen včas zachytit jak základní, tak pokročilé bezpečnostní události jako malware nebo cílené útoky?

Současný dohledový systém dokáže zachytit základní pokusy o neoprávněný přístup, avšak jeho možnosti pro včasnou detekci sofistikovanějších bezpečnostních hrozeb jsou omezené. Organizace nedisponuje pokročilejším bezpečnostním nástrojem pro monitoring.

What-if analýza provozu síťové infrastruktury

Co když dojde k objevení kritické bezpečnostní chyby v prvcích síťového provozu? Má organizace zavedený systém pravidelné kontroly a aktualizace těchto prvků?

Organizace provádí kontroly a aktualizace prvků síťového provozu pravidelně manuálně. Nicméně mezi vznikem zranitelnosti a její aktualizací může být prostor pro zvýšené riziko.

Co když se útočník dostane do vnitřní sítě organizace? Jsou vnitřní části infrastruktury dostatečně chráněny, aby se zabránilo jeho dalšímu pohybu?

Firewall je spravován centrálně a sítě jsou segmentovány tak, aby zařízení byla izolována. Tudíž by se útočník neměl dostat dále do dalších segmentů.

Co když je síťová infrastruktura organizace vystavena kybernetickému útoku z externího prostředí, například typu DDoS? Je organizace schopna takové události včas detekovat a adekvátně na ně reagovat?

Organizace je schopna detekovat základní výpadky služeb. Není však vybavena pokročilejším systémem pro detekci DDoS útoků. V případě takového útoku může dojít k přerušení některých služeb.

Co když dojde k pokusu o prolomení zabezpečení veřejně vystavených webových služeb nebo síťových rozhraní organizace? Jsou tyto služby dostatečně chráněny proti takovým útokům?

Veřejné služby se snažíme držet co nejvíce aktuální. Pravidla firewallu a přístupová oprávnění jsou omezena do maximální nutné výše, aby se minimalizovalo riziko těchto útoků.

Co když dojde k pokusu o neoprávněné připojení nebo odposlech přenášených dat ve firemní Wi-Fi síti? Je bezdrátová síť organizace dostatečně zabezpečená proti těmto rizikům?

Wi-Fi síť je zabezpečena standardním šifrováním, avšak její zabezpečení je základní, bez dodatečných mechanismů pro monitoring nebo pokročilou ochranu proti odposlechům či neoprávněnému přístupu.

Co když dojde k pokusu o prolomení autentizace vzdáleného přístupu? Má organizace implementované dostatečně silné autentizační mechanismy?

Organizace pro vzdálené přístupy využívá VPN s vícefaktorovou autentizací, což zajišťuje dostatečně silnou ochranu proti pokusům o prolomení přístupových údajů.

Co když nastane technický výpadek nebo poškození páteřních síťových prvků organizace? Má organizace redundantní řešení, která zajistí dostupnost klíčových služeb?

Organizace používá protokoly pro redundanci síťového provozu a udržuje v záloze hardwarové prvky, aby zajistila dostupnost kritických služeb.

Co když dojde k poškození nebo chybě v prvcích síťového provozu? Provádí organizace pravidelné zálohy konfigurací, které umožní jejich rychlou obnovu?

Organizace udržuje některé zálohy konfigurací síťových prvků, ale neprovádí je automatizovaně ani pravidelně, což může způsobit prodlevy při jejich obnově.

Co když dojde k incidentu v síťové infrastruktuře vyžadujícímu rychlou analýzu a reakci? Má organizace dostupnou aktuální a kompletní dokumentaci síťové infrastruktury včetně krizových scénářů?

Dokumentace síťové infrastruktury existuje, ale není kompletní ani pravidelně aktualizovaná. Organizace rovněž nedisponuje detailními krizovými scénáři pro řešení všech možných incidentů.

What-if analýza koncových zařízení

Co když dojde k odhalení kritické bezpečnostní zranitelnosti v operačních systémech koncových zařízení? Má organizace zavedenou centrální správu, která umožní rychlou aktualizaci všech zařízení?

Organizace provádí aktualizace OS na koncových zařízeních automatizovaně prostřednictvím nastavených pravidel přímo na jednotlivých zařízeních. Aktualizace však nejsou spravovány centrálně.

Co když dojde k objevení zranitelností v aplikacích na koncových zařízeních? Je organizace schopna rychle zajistit jejich aktualizaci?

Organizace aktuálně neprovádí centrální správu aktualizací uživatelských aplikací (Office, PDF, prohlížeče). Podle typu aplikace se aktualizace provádí buď automaticky, nebo manuálně jednotlivými uživateli.

Co když se koncová zařízení stanou terčem kybernetického útoku malwarem nebo ransomwarem? Jsou tato zařízení dostatečně chráněna a vybavena pokročilými nástroji pro včasnou detekci a reakci?

Organizace využívá antivirovou a antimalwarovou ochranu na všech koncových zařízeních a disponuje EDR řešením, které umožňuje pokročilou detekci a rychlou reakci na incidenty. Zároveň mají uživatelé povinnost ukládat svá důležitá data do vyhrazených prostor spravovaných a zálohovaných organizací pro případnou potřebu obnovy dat.

Co když dojde ke kompromitaci nebo ztrátě mobilního zařízení? Disponuje organizace nástroji, které umožní vzdáleně zabezpečit nebo smazat uložená data?

Organizace v současnosti nedisponuje centrálním systémem MDM pro správu mobilních zařízení, což omezuje možnosti vzdáleného zabezpečení nebo smazání dat v případě ztráty či krádeže zařízení.

Co když dojde ke ztrátě nebo krádeži přenosného zařízení? Jsou data na těchto zařízeních dostatečně chráněna před neoprávněným přístupem?

Ano, úložiště dat na většině koncových zařízení jsou šifrována, což významně omezuje riziko neoprávněného přístupu k datům v případě jejich ztráty nebo odcizení.

Co když dojde k bezpečnostnímu incidentu na zařízeních dostupných externím uživatelům (například v učebnách)? Má organizace tato zařízení dostatečně zabezpečena?

Zařízení používaná externími uživateli jsou vybavena základní antivirovou ochranou, avšak vzhledem k častému a různorodému využití může být jejich zabezpečení omezené

Co když zaměstnanci využívají firemní zařízení k soukromým účelům? Existují dostatečná opatření nebo kontroly, aby se minimalizovala bezpečnostní rizika?

Zaměstnanci jsou obeznámeni s pravidly používání firemních zařízení pro soukromé účely, nicméně technicky není možné tomuto využívání zcela zabránit.

Co když dojde k fyzické ztrátě nebo krádeži koncových zařízení? Má organizace připravena efektivní opatření pro minimalizaci dopadů?

Organizace uplatňuje základní opatření v podobě šifrování dat a zároveň je schopna pomocí bezpečnostního softwaru provést vzdálené zamknutí zařízení. V případě zařízení využívajících VPN může organizace rovněž zakázat přístup konkrétního uživatele.

What-if analýza lidských zdrojů

Co když se zaměstnanci stanou cílem phishingového útoku nebo sociálního inženýrství? Jsou dostatečně připraveni tyto hrozby rozpoznat a správně na ně reagovat?

Zaměstnanci absolvují jednou ročně testování v oblasti kybernetické bezpečnosti, nicméně organizace neprovádí pravidelná školení zaměřená na průběžné zvyšování bezpečnostního povědomí.

Co když dojde k neoprávněnému použití uživatelského účtu v důsledku kompromitace hesla? Jsou uživatelské účty a přístupy dostatečně zabezpečené?

Organizace využívá vícefaktorovou autentizaci (2FA) pro klíčové systémy a uživatelské účty, což výrazně omezuje riziko neoprávněného přístupu.

Co když zaměstnanec zaznamená podezřelou aktivitu nebo bezpečnostní incident? Existují jasné postupy pro hlášení takových situací?

Zaměstnanci jsou obeznámeni s tím, že jakoukoli podezřelou aktivitu nebo bezpečnostní incident mají neprodleně hlásit odboru informatiky. Vybrané aktuální bezpečnostní trendy jsou interně zmiňovány a probírány.

Co když zaměstnanci nedodržují stanovená bezpečnostní pravidla kvůli nejasnostem v jejich výkladu nebo uplatňování? Jsou zaměstnanci obeznámeni s pravidly bezpečného chování na svých zařízeních?

Zaměstnanci jsou obeznámeni s pravidly bezpečného chování na svých zařízeních a organizace má tato pravidla dokumentována.

Co když se zaměstnanci při práci na dálku nechovají dostatečně bezpečně? Jsou nastavena odpovídající opatření pro kontrolu a vynucení bezpečnostních pravidel?

Organizace má definovaná pravidla pro práci na dálku a zaměstnanci využívají VPN s vícefaktorovou autentizací.

Co když zaměstnanci obdrží phishingové e-maily? Má organizace implementovaná technická opatření pro minimalizaci doručování těchto zpráv zaměstnancům?

Organizace má nasazené filtrování e-mailů na úrovni serveru, což omezuje doručení phishingových zpráv zaměstnancům.

Co když zaměstnanci mají přidělena širší oprávnění, než skutečně potřebují? Jsou přístupová oprávnění pravidelně revidována a upravována dle reálných potřeb?

Organizace provádí pravidelné revize oprávnění zaměstnanců a při jejich nastavování se snaží minimalizovat rozsah oprávnění pouze na nutnou úroveň pro snížení bezpečnostních rizik.

PŘÍLOHA P III: FMEA ANALÝZY

FMEA analýza datových a aplikačních aktiv

ANALÝZA SOUČASNÉHO STAVU										NÁVRH OPATŘENÍ		ANALÝZA PO REALIZACI			
Prvek	Chyba	Následky	Závažnost	Příčina	Výskyt	Opatření	Řízení procesu	Odhalení	RPN	Doporučená opatření	Odpovědnost	Závažnost	Výskyt	Odhalení	RPN
Fyzické servery a virtualizační prostředí	Selhání hardware	Nedostupnost kritických aplikací	9	Porucha diskového pole	3	RAID pole	Monitoring hardware, pravidelné reporty	3	81	Neřešeno	Odbor informatiky	9	3	3	81
		Ztráta dat	10			Pravidelné zálohy			90			10	3	3	90
		Nedostupnost virtualizačního prostředí	9	Výpadek fyzického serveru	2	Clusterizace	Monitoring hardware	3	54	Neřešeno		9	2	3	54
		Výpadek fyzické infrastruktury	9	Výpadek napájení	5	UPS, přepínače sítí			135	Instalace generátorů, bateriového úložiště		9	2	2	36

ANALÝZA SOUČASNÉHO STAVU										NÁVRH OPATŘENÍ		ANALÝZA PO REALIZACI			
Prvek	Chyba	Následky	Závažnost	Příčina	Výskyt	Opatření	Řízení procesu	Odhalení	RPN	Doporučená opatření	Odpovědnost	Závažnost	Výskyt	Odhalení	RPN
	Porucha chladicího systému	Výpadek a poškození hardware	10	Technická závada klimatizace	4	Redundantní chlazení, pravidelný servis	Monitoring prostředí	2	80	Neřešeno		10	4	2	80
	Neoprávněný přístup ke správě	Kompromitace serverů a dat	10	Slabé zabezpečení admin. rozhraní	3	Politika hesel, oddělení administrace	Monitoring a logování přístupů	4	120			10	3	4	120
podnikové informační aplikace a databáze	Výpadek podnikových aplikací	Přerušení provozu, nedostupnost služeb	9	Selhání fyzického serveru	2	Redundantní virtualizační prostředí	Monitoring dostupnosti aplikací	3	54	Neřešeno		9	2	3	54

ANALÝZA SOUČASNÉHO STAVU										NÁVRH OPATŘENÍ		ANALÝZA PO REALIZACI			
Prvek	Chyba	Následky	Závažnost	Příčina	Výskyt	Opatření	Řízení procesu	Odhalení	RPN	Doporučená opatření	Odpovědnost	Závažnost	Výskyt	Odhalení	RPN
	Chybná konfigurace aplikací	Narušení funkcí, omezení provozu	9	Lidská chyba při konfiguraci	4	Konfigurační dokumentace, zálohy systémů	Žádné	3	108	Neřešeno		9	4	3	108
	Neaktuální verze software	Zranitelnost aplikace a operačních systémů	7	Nedostatečné aktualizace	6	Žádné	Pravidelná ruční kontrola	8	336	Zavedení systému patch management		7	2	2	28
	Chyby databázového systému	Ztráta či nedostupnost dat	10	Technická závada databáze	4	Zálohování systémů	Monitoring dostupnosti systémů	3	120	Neřešeno		10	4	3	120
	Neoprávněný přístup k datům	Únik citlivých informací	7	Nedostatečné řízení oprávnění	5	Politika přístupů	Žádné	7	245	zavedení pravidelných auditů a revizí oprávnění		7	2	2	28

ANALÝZA SOUČASNÉHO STAVU										NÁVRH OPATŘENÍ		ANALÝZA PO REALIZACI			
Prvek	Chyba	Následky	Závažnost	Příčina	Výskyt	Opatření	Řízení procesu	Odhalení	RPN	Doporučená opatření	Odpovědnost	Závažnost	Výskyt	Odhalení	RPN
	Ztráta nebo poškození dat	Nedostupnost informací, narušení provozu	10	Lidská chyba, selhání úložiště	6	Pravidelné zálohování	Pravidelné reporty zálohování	5	300	Zřízení off-site záloh, testování obnovy dat		10	2	2	40
Systémy zálohování	Selhání plánovaného zálohování	Nemožnost obnovy aktuálních dat	10	Technická chyba, chybné nastavení	4	Automatizace záloh	Pravidelné reporty	3	120	Neřešeno		10	4	3	120
	Chyba při obnově dat ze záloh	Ztráta dat, nemožnost obnovy	10	Poškozené zálohy, lidská chyba	5	Žádné	Žádné	8	400	Testování obnovy dat, tvorba dokumentace		10	3	3	90
	Neoprávněný přístup k zálohám	Únik citlivých dat	7	Nedostatečné zabezpečení záloh	3	Omezený přístup k zálohám	Logování přístupů	6	126	Šifrování zálohovaných dat		7	3	2	42

ANALÝZA SOUČASNÉHO STAVU										NÁVRH OPATŘENÍ		ANALÝZA PO REALIZACI			
Prvek	Chyba	Následky	Závažnost	Příčina	Výskyt	Opatření	Řízení procesu	Odhalení	RPN	Doporučená opatření	Odpovědnost	Závažnost	Výskyt	Odhalení	RPN
	Nedostatečná frekvence zálohování	Ztráta aktuálních dat	8	Nevhodně nastavená politika záloh	2	Žádné	Pravidelné zálohování	3	48	Neřešeno		8	2	3	48
	Chybějící ověření integrity záloh	Nemožnost obnovy, poškození dat	10	Nedostatečný proces kontroly	2	Automatické ověřování integrity	Žádné	3	60	Neřešeno		10	2	3	60
	Nevhodné umístění záloh	Ztráta záloh při poškození primární lokality	10	Umístění záloh v blízkosti produkce	7	Žádné	Žádné	8	560	Umístění záloh na oddělených lokalitách		10	2	5	100

FMEA analýza lidských zdrojů

ANALÝZA SOUČASNÉHO STAVU										NÁVRH OPATŘENÍ		ANALÝZA PO REALIZACI			
Prvek	Chyba	Následky	Závažnost	Příčina	Výskyt	Opatření	Řízení procesu	Odhalení	RPN	Doporučená opatření	Odpovědnost	Závažnost	Výskyt	Odhalení	RPN
Povědomí a chování zaměstnanců	Podlehnutí phishingovému útoku	Únik přihlašovacích údajů, kompromitace systémů	8	Nedostatečné povědomí zaměstnanců	7	Obeznamení zaměstnanců	Filtrace pošty	6	336	Pravidelná školení a testy	Odbory informatiky a vzdělávání	8	3	2	48
	Neopatrné zacházení s citlivými daty	Únik citlivých dat	7	Neznalost nebo ignorace bezpečnostních pravidel	5	Stanovení pravidel	Žádné	6	210	Pravidelná školení, audity		7	2	2	28
	Nedodržení bezpečnostních politik a pravidel	Zvýšené riziko incidentů	7	Nízké povědomí, nedostatečné vymáhání pravidel	4	Stanovení pravidel	Žádné	5	140	Školení, kontrola pravidel	Vedoucí pracovníci	7	2	3	42

ANALÝZA SOUČASNÉHO STAVU										NÁVRH OPATŘENÍ		ANALÝZA PO REALIZACI			
Prvek	Chyba	Následky	Závažnost	Příčina	Výskyt	Opatření	Řízení procesu	Odhalení	RPN	Doporučená opatření	Odpovědnost	Závažnost	Výskyt	Odhalení	RPN
	Používání slabých nebo opakovaných hesel	Neoprávněný přístup, kompromitace účtů	8	Nízká informovanost, pohodlnost uživatelů	4	Politika hesel, vícefaktorová autentizace	Žádné	3	96	Neřešeno	Odbor informatiky	8	4	3	96
	Neoznámení podezřelého chování nebo incidentu	Eskalace incidentu, větší škody	5	Nízké povědomí o oznamovacích postupech	5	Obeznamení zaměstnanců	Žádné	5	125	Školení hlášení incidentů		5	2	2	20
Vzdělávání a testování zaměstnanců	Nedostatečná frekvence vzdělávání	Nízké povědomí, zvýšené riziko incidentů	5	Nedostatečná priorita vzdělávání	6	Žádné	Žádné	5	150	Roční plán školení	Odbory informatiky a vzdělávání	5	3	2	30

ANALÝZA SOUČASNÉHO STAVU										NÁVRH OPATŘENÍ		ANALÝZA PO REALIZACI			
Prvek	Chyba	Následky	Závažnost	Příčina	Výskyt	Opatření	Řízení procesu	Odhalení	RPN	Doporučená opatření	Odpovědnost	Závažnost	Výskyt	Odhalení	RPN
	Chybějící specializované školení pro administrátory a IT pracovníky	Nedostatečné znalosti specializovaného personálu	7	Nedostatečná priorita vzdělávání	5	Žádné	Příležitostné školení na vybrané oblasti	4	140	Specializovaná školení	Vedoucí odboru informatiky	7	3	3	63
	Nejasné nebo nedostatečné zaměření testování	Nízká relevance testů	6	Nesledování aktuálních trendů	6	Žádné	Roční testování zaměstnanců	5	180	Aktualizace testů podle dat z NÚKIB	Odbory informatiky a vzdělávání	6	2	2	24
	Absence testování znalostí zaměstnanců	Neověřené znalosti, zvýšená pravděpodobnost incidentů	6	Chybějící mechanismus ověřování znalostí	4	Pravidelné testování znalostí	Žádné	6	144	Zvýšení četnosti vzdělávacích aktivit		6	2	3	36

ANALÝZA SOUČASNÉHO STAVU										NÁVRH OPATŘENÍ		ANALÝZA PO REALIZACI			
Prvek	Chyba	Následky	Závažnost	Příčina	Výskyt	Opatření	Řízení procesu	Odhalení	RPN	Doporučená opatření	Odpovědnost	Závažnost	Výskyt	Odhalení	RPN
Řízení přístupových práv zaměstnanců	Neaktuální nebo nesprávně nastavená přístupová práva	Riziko neoprávněného přístupu, únik dat	7	Nedostatečná správa a aktualizace práv	4	Nastavení nutných přístupových práv	Žádné	4	112	Neřešeno	Odbor informatiky	7	4	4	112
	Příliš široká oprávnění zaměstnanců	Neoprávněný přístup, riziko zneužití dat	5	Nedostatečné řízení oprávnění uživatelů	4	Pravidlo minimálních oprávnění	Žádné	6	120	Neřešeno		5	4	6	120
	Absence pravidelného auditu přístupových práv	Nezjištěné neoprávněné přístupy, zvýšená rizika	4	Nezavedený proces kontroly	8	Žádné	Žádné	7	224	Pravidelný audit práv		4	2	2	16

ANALÝZA SOUČASNÉHO STAVU										NÁVRH OPATŘENÍ		ANALÝZA PO REALIZACI			
Prvek	Chyba	Následky	Závažnost	Příčina	Výskyt	Opatření	Řízení procesu	Odhalení	RPN	Doporučená opatření	Odpovědnost	Závažnost	Výskyt	Odhalení	RPN
	Nedostatečné odstranění práv po odchodu zaměstnance	Neoprávněný přístup, únik informací	7	Chybějící proces deaktivace přístupů	4	Ruční proces deaktivace přístupů	Žádné	5	140	Automatizace procesu deaktivace účtů		7	2	2	28
	Sdílení přístupových údajů mezi zaměstnanci	Kompromitace přístupů, obtížná identifikace incidentů	5	Nedostatečné povědomí, absence jasných pravidel	5	Zavedeny pravidla a politiky	Žádné	8	200	Školení, kontrola dodržování		5	3	5	75
	Absence nebo slabá vícefaktorová autentizace (MFA)	Zvýšené riziko kompromitace účtů	8	Chybějící implementace MFA	2	Povinná vícefaktorová autentizace pro kritické systémy	Žádné	3	48	Neřešeno		8	2	3	48