

Informační podpora manažera kybernetické bezpečnosti

Bc. Lubomír Langer

Diplomová práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav elektroniky a měření

Akademický rok: 2024/2025

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	Bc. Lubomír Langer
Osobní číslo:	A23607
Studijní program:	N1032A020003 Bezpečnostní technologie, systémy a management
Specializace:	Bezpečnostní technologie
Forma studia:	Kombinovaná
Téma práce:	Informační podpora manažera kybernetické bezpečnosti
Téma práce anglicky:	Information Support of the Cybersecurity Manager.

Zásady pro vypracování

- Provedte literární rešerši k tématu informační podpory manažera kybernetické bezpečnosti.
- Navrhněte rámec informační podpory s ohledem na klíčové nástroje a doporučené postupy.
- Vytvořte maturity model pro hodnocení vyspělosti systému informační podpory.
- Posudte navržený model na základě teoretické analýzy.
- Vyhodnotte výsledky a diskutujte slabé stránky modelu.

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

Seznam doporučené literatury:

1. RABII, Anass; ASSOUL, Saliha; QUAZZANI TOUHAM, Khadija a ROUDIES, Ounsa. Information and cyber security maturity models: a systematic literature review. Online. Information and cyber security. 2020, roč. 2020, č. Volume 28 4, s. 627-644. ISSN 2056-4961. Dostupné z: <https://doi.org/10.1108/ICS-03-2019-0039>
2. BANOTH, Rajkumar; GUGULOTHU, Narsimha a GODISHALA, Aruna Kranthi. A Comprehensive Guide to Information Security Management and Audit. 2023. Boca Raton, Florida, USA: CRC Press, 2023. ISBN 9781003322191.
3. PASCOE, Cherilyn; QUINN, Stephen a SCARFONE, Karen. The NIST Cybersecurity Framework (CSF) 2.0. Online. NIST Pubs. 2024, roč. 2024, č. NIST CSWP 29, s. 32. Dostupné z: <https://doi.org/10.6028/NIST.CSWP.29>
4. EVROPSKÝ PARLAMENT A RADA EVROPSKÉ 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). In: . Štrasburk, 2022. Dostupné také z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32022L2555&qid=1724329129730>
5. EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE. legislativní akt, NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011. Štrasburk, 2022. Dostupné také z: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32022R2554>
6. MINIMÁLNÍ BEZPEČNOSTNÍ STANDARD: podpůrný materiál pro subjekty, které nespádají pod zákon o kybernetické bezpečnosti. Online. Brno: NAKIT, Ministerstvo vnitra české republiky, NÚKIB, 2023. Dostupné také z: https://nukib.gov.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf

Vedoucí diplomové práce:

Ing. Lukáš Králík, Ph.D.

Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **29. listopadu 2024**

Termín odevzdání diplomové práce: **30. května 2025**

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



Ing. Milan Navrátil, Ph.D. v.r.
ředitel ústavu

Ve Zlíně dne 29. listopadu 2024

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že

- odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení diplomové práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji diplomovou 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 – diplomovou 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 diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové 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 diplomové práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne

.....
podpis autora

ABSTRAKT

Tato diplomová práce se zaměřuje na návrh komplexního modelu informační podpory pro manažera kybernetické bezpečnosti (ISO/CISO). Cílem je zajistit, aby měl bezpečnostní manažer přístup ke správným a včasným informacím potřebným pro rozhodování v oblasti řízení rizik, incidentů a souladu s legislativními požadavky. Práce zahrnuje přehled rámců kybernetické bezpečnosti (NIST CSF, ISO/IEC 27001, COBIT), návrh strukturovaného rámce podpory a vývoj maturity modelu, který umožňuje hodnotit úroveň vyspělosti systému informační podpory. Model je dále aplikován na případové studii fiktivní banky FinCore Bank a.s., kde jsou identifikovány oblasti pro zlepšení. Navržený model je validován vůči mezinárodním standardům a regulacím, jako jsou NIS2 a DORA. Výsledkem je prakticky využitelný nástroj pro systematické posuzování a rozvoj informační podpory v organizacích.

Klíčová slova: kybernetická bezpečnost, ISO, CISO, informační podpora, maturity model, NIST CSF, ISO/IEC 27001, COBIT, NIS2, DORA

ABSTRACT

This diploma thesis focuses on the design of a comprehensive information support model for the cybersecurity manager (ISO/CISO). The aim is to ensure that the security manager has access to accurate and timely information necessary for decision-making in risk management, incident handling and regulatory compliance. The thesis includes an overview of cybersecurity frameworks (NIST CSF, ISO/IEC 27001, COBIT), a structured information support framework, and the development of a maturity model used to assess the level of cybersecurity information support in an organization. The model is applied to a case study of the fictitious FinCore Bank a.s., identifying areas for improvement. The proposed model is validated against international standards and regulatory frameworks, such as NIS2 and DORA. The result is a practically applicable tool for systematic assessment and development of information support in organizations.

Keywords: cybersecurity, ISO, CISO, information support, maturity model, NIST CSF, ISO/IEC 27001, COBIT, NIS2, DORA

Tímto bych rád poděkoval vedoucímu mé diplomové práce, Ing. Lukáši Králíkovi, Ph.D., za jeho odborné vedení, cenné rady a podporu během zpracování této práce. Mé poděkování patří také mé rodině a přátelům za jejich trpělivost, pochopení a povzbuzení po celou dobu mého studia.

OBSAH

ÚVOD.....	13
I TEORETICKÁ ČÁST	14
1 SPECIFIKA KYBERNETICKÉ BEZPEČNOSTI	15
1.1 VÝVOJ A SOUČASNÝ STAV KYBERNETICKÉ BEZPEČNOSTI	15
1.1.1 Historie kybernetických hrozeb a obranných mechanismů	15
1.1.2 Vývoj bezpečnostních rolí ve firmách	16
1.1.3 Trendy v kybernetické bezpečnosti	17
1.2 ROLE MANAŽERA KYBERNETICKÉ BEZPEČNOSTI V ORGANIZACI.....	18
1.2.1 Porovnání hlavních bezpečnostních rolí ve firmách	18
1.2.2 Odpovědnosti a kompetence	18
1.2.3 Vztah k ostatním manažerským oddělením	19
1.3 NÁSTROJE A RÁMCE PRO PODPORU KYBERNETICKÉ BEZPEČNOSTI.....	21
1.3.1 NIST CSF 2.0 – jak pomáhá v praxi	21
1.3.2 ISO/IEC 27001 a další bezpečnostní normy	23
1.3.3 Maturity modely	24
1.3.4 Porovnání přístupů	25
1.4 PŘEHLED LEGISLATIVY A REGULACÍ.....	26
1.4.1 Směrnice NIS2 a její dopady na organizace	26
1.4.2 Nařízení DORA pro finanční sektor	27
1.4.3 GDPR a bezpečnost informací	28
1.4.4 Česká vyhláška o kybernetické bezpečnosti	28
2 NÁVRH RÁMCE INFORMAČNÍ PODPORY	30
2.1 POTŘEBY MANAŽERA KYBERNETICKÉ BEZPEČNOSTI	30
2.1.1 Jaké informace potřebuje ISO/CISO ke správnému rozhodování	30
2.1.2 Klíčové bezpečnostní ukazatele	31
2.1.3 Potřeby v oblasti monitoringu, reportingu, analytiky a eskalace bezpečnostních incidentů	32
2.2 ARCHITEKTURA INFORMAČNÍ PODPORY	33
2.2.1 Definování klíčových komponent systému informační podpory	33
2.2.2 Model informačního toku mezi manažery bezpečnosti, IT týmem a vedením	34
2.2.3 Technické nástroje (SIEM systémy, threat intelligence platformy, risk management nástroje)	36
2.3 DOPORUČENÉ NÁSTROJE A POSTUPY	36
2.3.1 Přehled nejpoužívanějších softwarových řešení	37
2.3.2 Automatizace kybernetické bezpečnosti	38
2.3.3 Role umělé inteligence v kybernetické bezpečnosti	38
II PRAKTICKÁ ČÁST	40
3 VYTVOŘENÍ MATURITY MODELU	41

3.1	ÚVOD DO NAVRŽENÉHO MATURITY MODELU	41
3.1.1	Definice a smysl maturity modelů v kybernetické bezpečnosti	42
3.1.2	Přínosy aplikace maturity modelu pro organizace	42
3.2	SPECIFIKACE NAVRŽENÉHO MATURITY MODELU	43
3.2.1	Klíčové oblasti (domény)	43
3.2.2	Úrovně vyspělosti navrženého maturity modelu	45
3.3	IMPLEMENTAČNÍ DOPORUČENÍ	47
3.3.1	Bezpečnostní monitoring a reporting	48
3.3.2	Řízení bezpečnostních incidentů a automatizace reakcí	49
3.3.3	Řízení rizik	50
3.3.4	Řízení aktiv.....	51
3.3.5	Organizační řízení a compliance	53
3.4	AUDITNÍ PROCES A HODNOCENÍ	54
3.4.1	Metodika a postup provádění auditů	55
3.4.2	Sběr důkazů a dokumentace	56
3.4.3	Vyhodnocení výsledků a doporučení	57
4	POSOUZENÍ MODELU NA PŘÍKLADU SPOLEČNOSTI FINCORE BANK A.S.....	59
4.1	CHARAKTERISTIKA SPOLEČNOSTI FINCORE BANK A.S.	59
4.2	MATURITY MODEL INFORMAČNÍ PODPORY – FINCORE BANK A.S.	60
4.2.1	Bezpečnostní monitoring a reporting	60
4.2.2	Řízení bezpečnostních incidentů a automatizace reakcí	61
4.2.3	Řízení rizik	61
4.2.4	Řízení aktiv.....	62
4.2.5	Governance a compliance	62
4.3	NÁVRH ZLEPŠENÍ PRO ZVÝŠENÍ VYSPĚLOSTI.....	63
4.3.1	oporučená opatření pro posun z Tier 2 na Tier 3 v oblastech s nižší úrovní.....	64
4.3.2	Specifická opatření pro případný posun do úrovně Tier 4 v klíčových oblastech.....	66
4.3.3	Prioritizace opatření s ohledem na významnost a efektivitu	67
4.4	PLÁN IMPLEMENTACE ZLEPŠENÍ	69
4.4.1	Časový harmonogram implementace opatření	69
4.4.2	Stanovení odpovědnosti za realizaci jednotlivých opatření	70
4.4.3	Potřebné zdroje (finanční, lidské, technické)	71
4.5	VALIDACE NAVRŽENÉHO MODELU.....	73
4.5.1	Teoretická validace vůči relevantním standardům	73
4.5.2	Zhodnocení vhodnosti modelu pro bankovní sektor (specifické regulační požadavky).....	75
4.6	IDENTIFIKACE SLABÝCH STRÁNEK A OMEZENÍ MODELU	77
4.6.1	Analýza možných problémů při aplikaci modelu v praxi	77

4.6.2	Diskuse omezení navrženého modelu (např. dostupnost zdrojů, organizační kultura)	78
4.7	NÁVRH METODIKY PRAKTICKÉ VALIDACE MODELU	79
4.7.1	Popis metodiky ověření modelu v reálných podmínkách	79
4.7.2	Navrhované scénáře a postupy testování	80
4.7.3	Způsob sběru důkazů a jejich analýza	83
5	DISKUZE A ZÁVĚR	85
5.1	SHRNUTÍ DOSAŽENÝCH VÝSLEDKŮ	85
5.1.1	Vyhodnocení přínosu vytvořeného modelu	86
5.2	KRITICKÉ ZHODNOCENÍ	86
	SEZNAM POUŽITÉ LITERATURY	89
	SEZNAM OBRÁZKŮ	92
	SEZNAM TABULEK	93
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	94
	SEZNAM PŘÍLOH	97

ÚVOD

Kybernetická bezpečnost představuje jednu z klíčových oblastí řízení moderních organizací. Rostoucí počet hrozeb, zvyšující se regulatorní tlak a závislost na informačních systémech vytvářejí potřebu efektivního řízení bezpečnostních opatření napříč celou organizací. V tomto kontextu hraje zásadní roli manažer kybernetické bezpečnosti, který je odpovědný za ochranu informačních aktiv, řízení rizik a dodržování souladu s legislativními požadavky.

Tato diplomová práce se zaměřuje na návrh komplexního modelu **informační podpory pro roli ISO/CISO**, jehož cílem je zajistit, aby manažer kybernetické bezpečnosti měl přístup ke správným informacím ve správný čas. Součástí návrhu je nejen identifikace potřebných nástrojů a ukazatelů, ale také vytvoření přehledné architektury informační podpory a procesního rámce pro její provoz a rozvoj.

V první části práce je zpracována literární rešerše zaměřená na vývoj kybernetických hrozeb, roli bezpečnostních manažerů a přehled existujících rámců a norem (např. NIST CSF, ISO/IEC 27001, COBIT). Následně je navržen strukturovaný rámec informační podpory zahrnující potřeby ISO/CISO, technickou architekturu, doporučené nástroje a ukazatele.

Druhá část práce je věnována návrhu **maturity modelu**, který umožňuje měřit vyspělost systému informační podpory v organizaci. Model je rozdělen do pěti domén a čtyř úrovní vyspělosti. Jeho použití je dále ilustrováno na případové studii **FinCore Bank a.s.**, kde jsou jednotlivé oblasti vyhodnoceny, identifikována slabá místa a navržena opatření pro další rozvoj.

Závěrečná část práce se věnuje zhodnocení přínosu navrženého modelu, jeho validaci vůči mezinárodním standardům (např. NIS2, ISO/IEC 27001, DORA) a diskuzi o možných omezeních a směrech budoucího rozvoje.

I TEORETICKÁ ČÁST

1 SPECIFIKA KYBERNETICKÉ BEZPEČNOSTI

Tato kapitola shrnuje hlavní oblasti kybernetické bezpečnosti důležité pro práci manažera kybernetické bezpečnosti. Popisuje vývoj hrozeb a obranných opatření, roli ISO/CISO, klíčové rámce (např. NIST CSF 2.0, ISO/IEC 27001, CIS Controls) i legislativní požadavky (NIS2, DORA, CER, GDPR), které ovlivňují bezpečnostní strategii organizací.

1.1 Vývoj a současný stav kybernetické bezpečnosti

Kybernetická bezpečnost se v posledních letech stala klíčovou součástí IT a strategického řízení. Digitalizace zvýšila efektivitu, ale zároveň přinesla nové hrozby a zranitelnosti. Ty vyžadují technologická, procesní i lidská opatření [1][2].

Z původního zaměření na státní a vojenské systémy se bezpečnostní normy rozšířily do komerční sféry. Mezi klíčové nástroje řízení bezpečnosti dnes patří ISO/IEC 27001, NIST CSF a CIS Controls [3][1].

Moderní hrozby, jako jsou ransomware¹, phishing², nebo útoky na dodavatelské řetězce, vedou k zavádění přístupů typu zero trust³, využívání umělé inteligence a automatizace bezpečnostních procesů [2].

Evropská legislativa, zejména směrnice NIS2 a nařízení DORA, ukládá organizacím povinnost zajistit vysokou úroveň ochrany informačních systémů a posiluje spolupráci mezi členskými státy [4].

Přesto mnohé organizace stále nedostatečně hodnotí svou bezpečnostní úroveň a neprovádějí systematická zlepšení [5]. Vzhledem k rychlému vývoji hrozeb je nezbytné investovat do strategií, technologií i vzdělávání [3][1].

1.1.1 Historie kybernetických hrozeb a obranných mechanismů

Kybernetické hrozby se od 80. let vyvinuly z izolovaných incidentů v globální problém ovlivňující veřejný i soukromý sektor. Prvním výrazným útokem byl Morrisův červ (1988), který infikoval tisíce počítačů a vedl ke vzniku prvního týmu CERT [2][6].

¹ Ransomware je škodlivý software, který zašifruje data a požaduje výkupné.

² Phishing je podvodné získávání citlivých údajů pomocí falešné komunikace.

³ Zero Trust je bezpečnostní přístup, který nedůvěřuje žádnému uživateli ani zařízení bez ověření.

V 90. letech a na počátku 21. století došlo k masivnímu šíření virů a červů, jako byly ILOVEYOU a Code Red. Tyto útoky zvýšily důraz na ochranu koncových zařízení a podnítily rozvoj antivirových řešení a firewallů [6].

Po roce 2010 se hrozby staly cílenějšími a sofistikovanějšími. Příkladem je Stuxnet (2010), který narušil fyzickou infrastrukturu v Íránu [2]. WannaCry (2017) pak infikoval statisíce zařízení po celém světě a ukázal dopady zanedbaných aktualizací [2].

Současné útoky často kombinují technické prostředky se sociálním inženýrstvím. Organizace proto přecházejí na proaktivní přístupy – zero trust, behaviorální analýzu, threat intelligence nebo SOC [3][2][6]. Jak upozorňuje Banoth, efektivní obrana vyžaduje pokročilou analytiku a predikci rizik [3].

Historický vývoj ukazuje, že kybernetické hrozby se mění s každým technologickým skokem. V reakci na ně se vyvíjí i role osob odpovědných za řízení bezpečnosti – právě této problematice se věnuje následující podkapitola.

1.1.2 Vývoj bezpečnostních rolí ve firmách

S rostoucí složitostí IT prostředí a počtem kybernetických hrozeb vznikla potřeba specializovaných bezpečnostních manažerů. Zpočátku byla bezpečnost v organizacích spravována neformálně různými IT pracovníky. Tento přístup se ukázal jako neudržitelný, a proto se začaly formovat samostatné role zaměřené výhradně na bezpečnost [2].

V 90. letech vznikla pozice **Information Security Officer (ISO)**, jejímž úkolem bylo zajistit dodržování interních bezpečnostních pravidel a externích předpisů [2]. Se zvyšující se komplexností hrozeb a potřebou strategického řízení bezpečnosti se postupně prosadila role **Chief Information Security Officer (CISO)**, která přebírá odpovědnost za bezpečnostní politiku na úrovni vrcholového managementu [7][8].

Zatímco ISO je primárně zodpovědný za každodenní bezpečnostní operace, CISO formuluje a prosazuje celkovou bezpečnostní strategii. Obě role jsou komplementární, přičemž CISO je dnes často členem vrcholového vedení a klíčovým aktérem při plnění regulačních požadavků [7].

Moderní organizace považují CISO za nedílnou součást rozhodovacích procesů. Jeho role se rozšiřuje z technického specialisty na strategického lídra odpovědného za ochranu informačních aktiv a reputace celé organizace [9].

1.1.3 Trendy v kybernetické bezpečnosti

Kybernetická bezpečnost se neustále vyvíjí v reakci na měnící se hrozby a technologie. Mezi klíčové trendy posledních let patří automatizace, umělá inteligence, útoky na dodavatelské řetězce, přechod k modelu Zero Trust a rostoucí regulační požadavky [3][1].

- **Umělá inteligence a automatizace**

AI umožňuje rychlou detekci anomálií a predikci útoků, ale může být zneužita i útočníky – např. při tvorbě phishingových kampaní nebo využití deepfake (imitace identity) technologií [1][10].

Ransomware a útoky na dodavatele

Ransomware zůstává jednou z největších hrozeb, často spojených s dvojitým vydíráním [2]. Útoky přes dodavatele, jak ukázal incident Target (útok přes dodavatele HVAC – únik dat z 40 mil. karet), zvyšují potřebu zabezpečení dodavatelského řetězce [11]. Nařízení DORA posiluje povinnosti v této oblasti [12].

- **Zero Trust a přechod od perimetrické bezpečnosti**

Model Zero Trust klade důraz na ověření identity všech přístupů, bez ohledu na jejich umístění. Je standardem v regulovaných sektorech, jako je finance či zdravotnictví [3].

- **SOC a behaviorální analýza**

Moderní bezpečnostní operační centra využívají strojové učení k detekci incidentů a prevenci útoků dříve, než k nim dojde. Zásadní roli hraje korelace dat a threat intelligence [3].

- **Regulace a standardizace**

Evropské předpisy jako NIS2 a DORA harmonizují požadavky na řízení rizik, auditovatelnost a odolnost. Organizace musejí zajistit shodu a schopnost reagovat na incidenty [3][12][2].

Aktuální trendy ukazují, že kybernetická bezpečnost je dynamickou disciplínou, která vyžaduje pružnou adaptaci a mezioborovou spolupráci. V následující kapitole se zaměříme na roli manažera kybernetické bezpečnosti, který tyto změny musí řídit napříč organizací.

1.2 Role manažera kybernetické bezpečnosti v organizaci

Manažer kybernetické bezpečnosti, označovaný jako **ISO (Information Security Officer)** nebo **CISO (Chief Information Security Officer)**, je klíčovou postavou odpovědnou za ochranu informačních aktiv, řízení bezpečnostních rizik a dodržování regulatorních požadavků [9][7].

Označení role se liší podle kontextu – česká vyhláška hovoří o „manažerovi kybernetické bezpečnosti“, zatímco mezinárodní rámce obvykle rozlišují ISO a CISO. Rozsah jejich odpovědností se odvíjí od velikosti organizace a míry regulace [13].

Zatímco ISO se soustředí na **operativní bezpečnost**, CISO odpovídá za **strategické řízení**, komunikaci s vedením a integraci bezpečnosti do firemní politiky [7]. Ve větších organizacích tvoří CISO součást vrcholového vedení, v menších firmách může být role ISO i CISO sloučena.

1.2.1 Porovnání hlavních bezpečnostních rolí ve firmách

Obě role cílí na ochranu informačních aktiv, liší se však v zaměření:

Information Security Officer (ISO) – operativa:

- Implementace bezpečnostních standardů (např. ISO/IEC 27001, NIST CSF) [3][1]
- Řízení kybernetických incidentů, aktualizace systémů [13]
- Školení zaměstnanců, komunikace s IT, HR [9][2]

Chief Information Security Officer (CISO) – strategie:

- Definice bezpečnostní strategie a architektury (např. ZTA) [4][12]
- Komunikace s vedením, schvalování rozpočtů, KPI/KRI [3][13]
- Integrace bezpečnosti do firemních procesů a strategických cílů [2]

Zatímco ISO operativně provádí bezpečnostní opatření, CISO určuje dlouhodobé směřování bezpečnostní politiky a hájí její důležitost na úrovni vedení [7].

1.2.2 Odpovědnosti a kompetence

Klíčové odpovědnosti ISO/CISO:

- Řízení bezpečnostní politiky a souladu s normami (NIS2, GDPR, DORA) [4][12]
- Řízení incidentů, forenzní analýza, dohled pomocí SIEM/IDS [9][6]
- Školení zaměstnanců, řízení bezpečnostních požadavků na dodavatele [13][11]

Nezbytné kompetence:

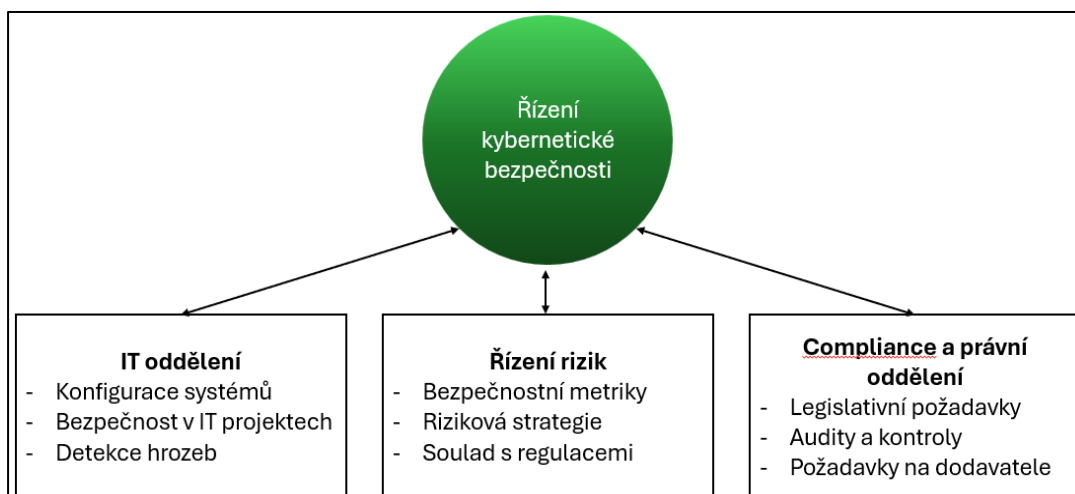
- **Technické:** řízení identit a přístupů (IAM), šifrování, detekce incidentů, audit [9]
- **Manažerské:** strategie, plánování rozpočtu, investice [7]
- **Komunikační:** reporting vedení, spolupráce s regulátory [13]

ISO i CISO musí rozumět nejen technologiím, ale i řízení změn, financím a komunikaci. S ohledem na rostoucí rizika a legislativní tlak je kladen důraz na jejich odborný růst.

Efektivní řízení bezpečnosti závisí na spolupráci těchto rolí s dalšími klíčovými pozicemi, jako jsou CIO, CRO či soulad (compliance). Právě této spolupráci se věnuje následující kapitola.

1.2.3 Vztah k ostatním manažerským oddělením

Účinné řízení kybernetické bezpečnosti vyžaduje úzkou spolupráci mezi bezpečnostním manažerem a dalšími klíčovými odděleními – především IT, řízením rizik a compliance. Každé z těchto oddělení přispívá k celkové odolnosti organizace jiným úhlem pohledu.



Obrázek 1: Schéma spolupráce manažera kybernetické bezpečnosti s klíčovými odděleními v organizaci
(zdroj: vlastní zpracování)

Spolupráce s IT oddělením

IT tým spravuje technologickou infrastrukturu, zatímco bezpečnostní tým dohlíží na její ochranu. Úzká spolupráce mezi těmito složkami je nezbytná pro:

- bezpečnou konfiguraci systémů, šifrování a síťové zabezpečení,

- integraci bezpečnosti do IT projektů (např. v rámci DevSecOps přístupů),
- detekci hrozeb pomocí nástrojů jako SIEM a IDS [14].

Podle COBIT 5 by měla být bezpečnost pevnou součástí IT governance a reflektovat nejen technologické, ale i obchodní cíle organizace [14]. Nedostatečná koordinace může vést k mezerám v ochraně a zpomalení projektů.

Spolupráce s oddělením řízení rizik

Oddělení řízení rizik definuje rámec pro identifikaci, hodnocení a mitigaci podnikových rizik, mezi nimiž kybernetická hrozba hraje stále větší roli. Spolupráce se zaměřuje na:

- začlenění kybernetických hrozeb do celkové rizikové strategie,
- definice bezpečnostních ukazatelů (KPI, KRI) pro sledování výkonnosti opatření,
- zajištění souladu s požadavky jako NIS2, DORA a GDPR [15].

ISO/IEC 27005:2018 zdůrazňuje, že řízení rizik v oblasti bezpečnosti informací musí být plně integrováno do obecného řízení rizik organizace [15]. Nedostatečné zapojení bezpečnostního manažera do tohoto procesu vede často k podcenění technologických rizik.

Spolupráce s compliance a právním oddělením

Compliance dohlíží na dodržování právních a interních předpisů. Je partnerem při interpretaci legislativních požadavků a přípravě bezpečnostních politik. ISO/CISO spolupracují na:

- přípravě podkladů pro audity a kontroly,
- nastavení procesů pro ochranu osobních údajů (např. dle GDPR),
- řízení smluvních rizik a bezpečnostních požadavků na dodavatele.

Efektivní řízení kybernetické bezpečnosti tedy vyžaduje nejen odborné schopnosti ISO a CISO, ale také jejich schopnost spolupracovat napříč organizací. Koordinace s IT, řízením rizik a compliance zajišťuje, že bezpečnostní opatření jsou nejen technicky správná, ale i strategicky sladěná a právně vymahatelná. Následující kapitola se proto zaměří na přehled nástrojů, rámců a metodik, které těmto rolím poskytují systematickou oporu při plnění jejich odpovědností.

1.3 Nástroje a rámce pro podporu kybernetické bezpečnosti

Efektivní řízení kybernetické bezpečnosti vyžaduje jasně definované rámce, nástroje a metodiky, které organizacím pomáhají systematicky identifikovat, řídit a snižovat bezpečnostní rizika. Standardizované přístupy zároveň umožňují vyhodnocovat úroveň vyspělosti, sladit strategii s regulacemi a zavádět osvědčené postupy [15].

Tato kapitola představuje klíčové rámce a normy, které tvoří základní oporu bezpečnostních strategií.

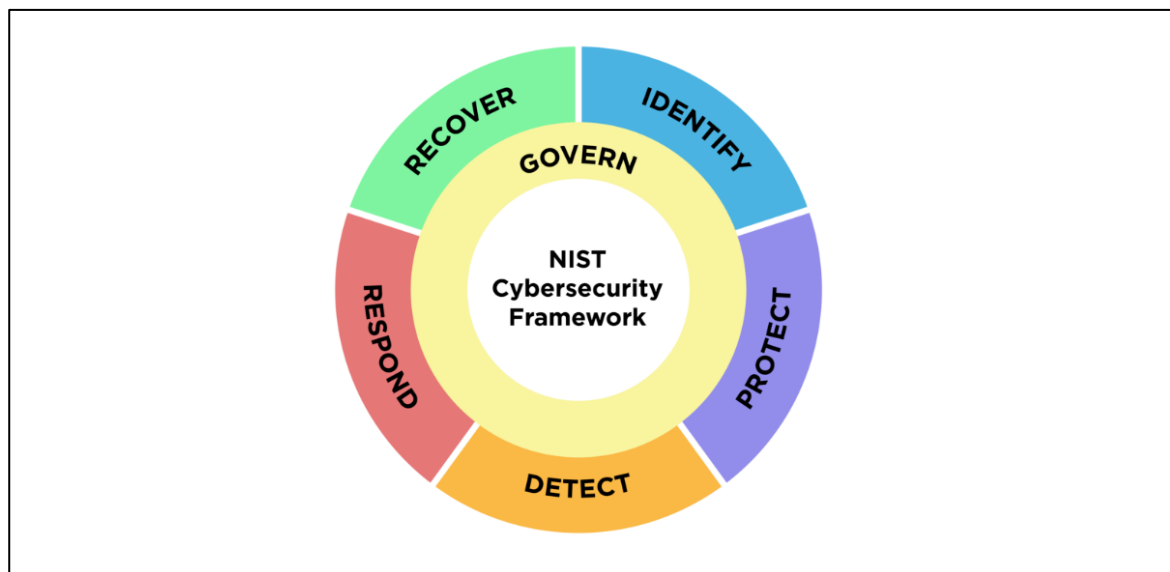
Přehled vybraných rámců:

- **ISO/IEC 27001** – Mezinárodní standard pro řízení bezpečnosti informací (ISMS), zaměřený na ochranu důvěrnosti, integrity a dostupnosti prostřednictvím řízeného systému [15].
- **ISO/IEC 27005** – Metodický rámec pro řízení bezpečnostních rizik, navazující na ISO/IEC 27001. Obsahuje procesy pro identifikaci, hodnocení a mitigaci hrozeb [15].
- **NIST CSF 2.0** – Americký rámec kybernetické bezpečnosti založený na pěti klíčových funkcích (Identify, Protect, Detect, Respond, Recover), rozšířený o novou funkci „Govern“ [14].
- **COBIT 5** – Rámec pro řízení a správu IT a bezpečnostních procesů, propojující IT governance s obchodními cíli [14].

Volba rámce závisí na povaze organizace, míře regulace a požadované úrovni vyspělosti. V následujících podkapitolách rozebereme jednotlivé rámce podrobněji.

1.3.1 NIST CSF 2.0 – jak pomáhá v praxi

NIST Cybersecurity Framework 2.0 (CSF 2.0) představuje modernizovanou verzi rámce od NIST, která reaguje na současné hrozby a klade důraz na integraci bezpečnosti do řízení celé organizace [1].



Obrázek 2: Klíčové funkce rámce NIST Cybersecurity Framework 2.0 (CSF 2.0)
(zdroj: vlastní úprava dle [1])

Rámec nyní obsahuje šest klíčových funkcí:

- **Identify** (Identifikace) – porozumění organizačnímu prostředí, aktivům, uživatelům a rizikům, které ohrožují cíle organizace. [1]
- **Protect** (Ochrana) – zavádění opatření, která pomáhají zabránit nebo zpomalit dopad kybernetických incidentů. [1]
- **Detect** (Detekce) – schopnost rychle rozpoznat bezpečnostní incidenty v reálném čase nebo na základě anomálií. [1]
- **Respond** (Reakce) – efektivní reakce na incidenty s cílem minimalizovat škody a obnovit provoz. [1]
- **Recover** (Obnova) – strategie a procesy pro návrat do normálního provozu po incidentu, včetně zlepšování připravenosti. [1]
- **Govern** (Řízení) – nově definovaná funkce, která klade důraz na odpovědnost vedení za kybernetickou bezpečnost, sladění s cíli organizace a plnění regulatorních požadavků. [1]

Funkce **Govern**, nově zavedená v rámci NIST CSF 2.0, posiluje odpovědnost vedení za kybernetickou bezpečnost, propojuje ji s řízením rizik, zvyšuje shodu s regulacemi (např. NIS2, DORA, ISO/IEC 27001) a zlepšuje meziodborovou komunikaci v organizaci [1].

NIST CSF 2.0 je kompatibilní s dalšími normami a dobře využitelný ve středních i velkých organizacích. Díky novým principům usnadňuje vedení firem orientaci v oblasti bezpečnosti a podporuje transparentní a odpovědný přístup ke kybernetickému riziku [1].

1.3.2 ISO/IEC 27001 a další bezpečnostní normy

Řada norem ISO/IEC 27000 představuje mezinárodně uznávaný rámec pro systematické řízení informační bezpečnosti. Poskytuje organizacím strukturovaný přístup k ochraně informačních aktiv, řízení rizik a splnění regulatorních požadavků.

ISO/IEC 27001 – systém řízení informační bezpečnosti (ISMS)

Norma ISO/IEC 27001 definuje požadavky na zavedení a provoz **systému řízení informační bezpečnosti (ISMS)**. Zaměřuje se na procesní řízení rizik spojených s ochranou informací a vyžaduje cyklický přístup zahrnující plánování, implementaci, monitorování a zlepšování. Její implementace umožňuje organizacím:

- systematicky řídit bezpečnostní rizika,
- získat certifikaci potvrzující shodu s mezinárodními požadavky,
- zvýšit důvěryhodnost vůči partnerům a zákazníkům [16].

ISO/IEC 27002 – doporučené bezpečnostní kontroly

ISO/IEC 27002 rozšiřuje ISO/IEC 27001 o praktická doporučení k jednotlivým **bezpečnostním kontrolám**. Nabízí flexibilní sadu opatření pro řízení přístupů, zabezpečení sítí, fyzickou bezpečnost, školení zaměstnanců a další oblasti. Organizace si mohou vybrat relevantní kontroly podle svých specifik a úrovně rizika [17].

ISO/IEC 27005 – řízení rizik informační bezpečnosti

Tato norma se specificky věnuje **identifikaci, analýze a řízení bezpečnostních rizik**. Slouží jako praktický doplněk k ISO/IEC 27001 a umožňuje:

- vyhodnotit pravděpodobnost a dopad hrozeb,
- prioritizovat bezpečnostní opatření,
- efektivně přidělit zdroje

ISO/IEC 27005 zdůrazňuje, že řízení rizik musí být kontinuálním procesem integrovaným do celkové bezpečnostní politiky [15].

Normy ISO 27000 poskytují komplexní a osvědčený rámec, který je vhodný pro organizace všech velikostí a sektorů. Jejich implementace usnadňuje dosažení regulační shody (např. s NIS2, GDPR, DORA) a zároveň podporuje důvěru klientů i partnerů.

1.3.3 Maturity modely

Pro systematické řízení kybernetické bezpečnosti je zásadní schopnost vyhodnotit úroveň vyspělosti organizace. K tomuto účelu slouží maturity modely, které organizacím umožňují:

- zhodnotit současný stav řízení bezpečnosti,
- určit cílovou úroveň zralosti,
- efektivně plánovat zlepšování.

Mezi nejpoužívanější modely patří **CMMI**, **COBIT 5** a **CIS Controls** [14], [15], [18].

CMMI – Capability Maturity Model Integration

CMMI je rámec pro zlepšování výkonnosti organizací prostřednictvím řízeného rozvoje procesů. Původně vznikl pro řízení softwarových projektů, ale je využitelný i v kybernetické bezpečnosti. Definiuje **pět úrovní vyspělosti**, které umožňují organizaci postupně rozvíjet své schopnosti [18].

COBIT 5 – Governance a řízení IT

COBIT 5 od ISACA je komplexní rámec pro **IT governance** a řízení bezpečnosti. Propojuje strategické cíle organizace s cíli IT, obsahuje kontrolní mechanismy, ukazatele a podporuje řízení rizik [14]. Široce se využívá v komerční i veřejné správě.

CIS Controls – praktická bezpečnostní opatření

CIS Controls je sada **18 konkrétních bezpečnostních kontrol**, rozdělených podle úrovně složitosti a velikosti organizace. Nabízí pragmatický přístup a je vhodný i pro menší firmy, které chtějí rychle zvýšit svou odolnost vůči hrozbám [15].

Každý z těchto modelů nabízí odlišný přístup – od strategického řízení po praktická opatření. Organizace si mohou vybrat model dle svých potřeb nebo je kombinovat pro maximální efekt.

1.3.4 Porovnání přístupů

Různé přístupy k řízení kybernetické bezpečnosti nabízejí odlišné výhody i omezení v závislosti na potřebách organizace. V této části jsou porovnány tři maturity modely – CMMI, COBIT 5 a CIS Controls – a normy ISO/IEC 27001 a ISO/IEC 27005. Cílem je poskytnout přehled jejich silných a slabých stránek a doporučit vhodné použití [14], [16], [19], [20].

Tabulka 1: Porovnání rámců a modelů řízení kybernetické bezpečnosti

Model / Norma	Výhody	Nevýhody	Vhodné pro
CMMI	- Strukturované zlepšování procesů - Použitelný napříč odvětvími - Jasně definované úrovně zralosti	- Nepokrývá bezpečnost do hloubky - Náročná implementace - Slabá vazba na regulační rámce	Organizace zaměřené na procesní řízení
COBIT 5	- Propojuje IT a byznys - Obsahuje hodnotící ukazatele a kontrolní mechanismy - Umožňuje auditovatelnost - Podpora řízení rizik	- Vyžaduje silnou podporu vedení - Komplexní implementace - Možnost překryvu s jinými normami	Střední a velké organizace
CIS Controls	- Rychlá a praktická implementace - Prioritizace rizik - Vhodné i pro malé týmy - Jasně definovaná opatření	- Omezená strategická hloubka - Menší flexibilita pro komplexní prostředí - Slabší návaznost na compliance	Menší a střední organizace
ISO/IEC 27001/27005	- Mezinárodní uznání - Možnost certifikace - Propojení s řízením rizik - Transparentní systém řízení bezpečnosti	- Vyšší nároky na zdroje - Administrativní zátěž - Fokus na procesy spíše než na konkrétní technologie	Organizace všech velikostí

(zdroj: vlastní zpracování dle [15], [14], [16], [19], [20])

Výše uvedené modely a rámce představují základní stavební kameny pro systematické řízení kybernetické bezpečnosti. Jejich vhodná kombinace umožňuje organizacím nejen efektivně řídit technické a organizační aspekty bezpečnosti, ale také plnit náročné regulační požadavky. Vzhledem k rostoucím legislativním nárokům je však klíčové zohlednit i právní rámec, který definuje povinnosti organizací v oblasti kybernetické bezpečnosti. Těmto aspektům se věnuje následující kapitola. [15], [14]

1.4 Přehled legislativy a regulací

Kybernetická bezpečnost je stále více ovlivňována právními a regulatorními požadavky na národní i mezinárodní úrovni. Na evropské úrovni vzniká komplexní rámec, který definuje minimální standardy ochrany informačních systémů, pravidla pro řízení rizik, ohlašování incidentů i odpovědnost managementu.

Tyto evropské předpisy – jako např. GDPR, NIS2, DORA či CER jsou postupně promítány do českého právního řádu prostřednictvím adaptačních zákonů. Příkladem je nařízení GDPR, jehož požadavky byly v České republice konkretizovány zákonem č.110/2019 Sb., o zpracování osobních údajů, nebo v případě NIS2 novým zákonem o kybernetické bezpečnosti, jehož návrh je momentálně ve fázi schvalování [4], [12], [16], [26], [27].

Tato kapitola stručně představuje klíčové regulace v oblasti kybernetické bezpečnosti:

- **Směrnici NIS2**, která rozšiřuje povinnosti v oblasti kybernetické bezpečnosti v rámci EU [4].
- **Nařízení DORA**, které stanovuje pravidla digitální odolnosti pro finanční sektor [12].
- **Obecné nařízení o ochraně osobních údajů (GDPR)** a český **adaptační zákon č. 110/2019 Sb.**, které upravují nakládání s osobními daty, [27]
- **Zákon č. 181/2014 Sb. o kybernetické bezpečnosti (ZKB)**, který představuje základní rámec české legislativy. [23].

1.4.1 Směrnice NIS2 a její dopady na organizace

Směrnice NIS2 (EU 2022/2555) nahrazuje původní směrnici NIS1 a výrazně rozšiřuje požadavky na kybernetickou bezpečnost v EU. Cílem je zajistit jednotnou úroveň ochrany kritické a důležité infrastruktury ve všech členských státech [4].

Hlavní změny a požadavky NIS2:

- **Rozšíření působnosti** – dopadá nejen na poskytovatele kritických služeb, ale i na firmy v nových odvětvích (např. výroba, pojišťovnictví, digitální infrastruktura) [4].
- **Povinnosti řízení rizik** – organizace musí zavést technická a organizační opatření pro prevenci, detekci a reakci na incidenty [4].
- **Hlášení incidentů** – povinnost nahlásit incident do 24 hodin od zjištění [4].

- **Odpovědnost vedení** – statutární orgány nesou přímou odpovědnost za plnění povinností [4].
- **Sankce** – až do výše 2 % ročního obratu nebo 10 milionů EUR [4].

Dopad na organizace:

Organizace spadající pod působnost NIS2 musí:

- přizpůsobit své řízení bezpečnosti legislativním požadavkům,
- aktualizovat analýzy rizik,
- připravit plány reakce na incidenty a interní procesy pro reportování,
- zajistit školení managementu a bezpečnostní kulturu [4].

1.4.2 Nařízení DORA pro finanční sektor

Nařízení DORA (EU 2022/2554) představuje jednotný rámec pro **digitální provozní odolnost** subjektů ve finančním sektoru. Na rozdíl od směrnice NIS2 je přímo **závazné a použitelné** bez nutnosti transpozice do národního práva [12].

Hlavní cíle a oblasti DORA:

- **Kybernetická odolnost** – zajištění kontinuity a bezpečnosti ICT systémů finančních institucí. [12]
- **Řízení rizik ICT** – povinnost zavést rámec řízení rizik zahrnující identifikaci, ochranu, detekci, reakci a obnovu. [12]
- **Testování odolnosti** – pravidelné testování, včetně penetračních testů. [12]
- **Oznamování incidentů** – jednotná pravidla pro hlášení závažných incidentů dozorovým orgánům. [12]
- **Řízení třetích stran (outsourcing)** – přísná pravidla pro smlouvy s ICT poskytovateli a monitoring jejich výkonnosti. [12]

Dopad na organizace:

Finanční instituce a jejich ICT dodavatelé musí:

- zmapovat a dokumentovat své ICT prostředí a závislosti,
- vytvořit plány obnovy a reakce na incidenty (BCP/DRP),
- aktualizovat smluvní vztahy s poskytovateli ICT služeb,
- zajistit testování odolnosti systémů včetně tzv. pokročilých testů (TLPT).

1.4.3 GDPR a bezpečnost informací

Obecné nařízení o ochraně osobních údajů (GDPR – General Data Protection Regulation, EU 2016/679) je klíčovým právním rámcem pro zpracování osobních údajů v EU. V České republice je doplněno a upřesněno zákonem č. 110/2019 Sb., o zpracování osobních údajů, který stanoví výjimky, pravidla dohledu a specifika aplikace [16].

Bezpečnostní požadavky podle GDPR:

- **Článek 32 – Zabezpečení zpracování**

Organizace musí zavést technická a organizační opatření, která zajistí odpovídající úroveň bezpečnosti vzhledem k rizikům (např. pseudonymizace, šifrování, řízení přístupů) [16].

- **Řízení rizik**

Úroveň zabezpečení musí odpovídat pravděpodobnosti a závažnosti dopadu na práva a svobody fyzických osob. Tento přístup odpovídá zásadám řízení bezpečnostních rizik [16].

- **Povinnost oznamovat porušení ochrany osobních údajů**

Incidenty, které mohou ohrozit osobní údaje, musí být nahlášeny dozorovému úřadu do 72 hodin. V určitých případech také samotným subjektům údajů [16].

- **Odpovědnost správce a záznamy o činnostech zpracování**

Organizace musí být schopna prokázat, že dodržuje pravidla GDPR (tzv. princip odpovědnosti – *accountability*) [16].

Dopad na kybernetickou bezpečnost:

GDPR klade důraz na bezpečnost zpracování údajů jako součást ochrany soukromí. Mnohá opatření v oblasti kybernetické bezpečnosti – např. řízení přístupů, detekce incidentů či šifrování – jsou zároveň klíčová pro splnění požadavků GDPR. Neplnění může vést k **pokutám až do výše 20 milionů EUR nebo 4 % celosvětového obrátu organizace** [16].

1.4.4 Česká vyhláška o kybernetické bezpečnosti

Český právní rámec kybernetické bezpečnosti je definován zejména zákonem č. 181/2014 Sb. o kybernetické bezpečnosti a **vyhláškou č. 82/2018 Sb.**, která stanovuje konkrétní požadavky na zajištění kybernetické bezpečnosti u povinných subjektů. Vyhlášku vydal Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) [9][2].

Hlavní oblasti úpravy podle vyhlášky:

- **Bezpečnostní opatření** – povinnosti v oblasti řízení rizik, bezpečnostních politik, řízení přístupů, kryptografických prostředků [9].
- **Detekce bezpečnostních událostí** – požadavky na monitorování, vyhodnocování logů a hlášení incidentů [9].
- **Reakce na incidenty** – zavedení interních procesů pro zvládání incidentů a povinnosti vůči NÚKIB [9].
- **Fyzická a personální bezpečnost** – omezení fyzického přístupu a ověření důvěryhodnosti pracovníků [9].
- **Dokumentace a kontrola** – vedení přehledné bezpečnostní dokumentace, umožnění kontrol [9].

Dopad na organizace:

Povinné subjekty – zejména provozovatelé kritické infrastruktury, významných informačních systémů a základních služeb – musí:

- implementovat opatření dle vyhlášky v plném rozsahu,
- provádět pravidelné testování a přezkoumání bezpečnosti,
- hlásit kybernetické bezpečnostní incidenty NÚKIB ve stanovených lhůtách [9][2].

Přehled legislativních a metodických rámců ukazuje, že role ISO/CISO je pevně ukotvena nejen v organizační praxi, ale i v právních a normativních požadavcích. Pro její efektivní výkon je nezbytná systematická a funkční informační podpora.

Shrnutí:

Na základě poznatků uvedených v této kapitole se následující část práce zaměřuje na návrh strukturovaného rámce informační podpory, který reflektuje potřeby manažera kybernetické bezpečnosti v kontextu moderních hrozeb, technologií a organizačních požadavků.

2 NÁVRH RÁMCE INFORMAČNÍ PODPORY

Úspěšné řízení kybernetické bezpečnosti vyžaduje, aby měl manažer bezpečnosti k dispozici správné informace ve správný čas. Tato kapitola se zaměřuje na návrh komplexního rámce informační podpory pro roli ISO/CISO. Cílem je definovat klíčové potřeby, strukturu podpůrného systému, používané nástroje a rozdíly v přístupu podle typu organizace. Rámec reflektuje nejen technické požadavky, ale i provozní realitu organizací různé velikosti a regulace.

2.1 Potřeby manažera kybernetické bezpečnosti

Manažer kybernetické bezpečnosti (ISO/CISO) musí činit rozhodnutí na základě informací, které pokrývají technickou, organizační i strategickou rovinu. Informační podpora proto nesmí být jen otázkou dat, ale musí zahrnovat i jejich interpretaci v kontextu rizik a obchodních cílů organizace [15].

Podle Koloucha a Bašty má ISO/CISO čelit nejen kybernetickým hrozbám, ale také tlaku na reportování vedení, dodržování regulatorních rámců a zajištění kontinuity služeb [2]. Informační podpora mu proto musí umožnit:

- monitorovat bezpečnostní stav a incidenty,
- hodnotit rizika a navrhnout opatření,
- komunikovat s vedením i technickými týmy,
- plánovat rozvoj bezpečnostních kapacit v souladu s prioritami organizace.

2.1.1 Jaké informace potřebuje ISO/CISO ke správnému rozhodování

ISO/IEC 27005 definuje rámec řízení bezpečnostních rizik, který je úzce spojen s informační podporou bezpečnostních manažerů. Pro efektivní rozhodování potřebuje ISO/CISO přístup k těmto oblastem informací [15]:

- **Bezpečnostní stav systémů** – přehled o zranitelnostech, aktualizacích, konfiguracích a provozních odchylkách. Tyto informace často poskytují nástroje pro skenování zranitelností, konfiguraci systémů a síťový monitoring.
- **Incidenty a události** – klasifikace, rozsah dopadu a stav řešení. Manažer musí mít k dispozici informace o aktuálním stavu detekce, reakce i související dokumentaci.

- **Audit a compliance** – výstupy z interních auditů a kontroly souladu s normami (např. ISO/IEC 27001, NIS2, GDPR). Tyto informace jsou klíčové pro rozhodování o nápravných opatřeních a komunikaci s vedením.
- **Hodnocení rizik** – identifikovaná rizika, jejich pravděpodobnost, dopad a navrhované mitigace. Tyto informace vycházejí z pravidelných risk assessmentů podle definovaných metodik.
- **Business kontext** – návaznosti bezpečnostních problémů na klíčové služby, SLA, provozní limity a obchodní priority. Umožňuje rozhodování podle dopadu na organizaci.
- **Odpovědnosti a procesy** – kdo je za co zodpovědný, jak vypadá schvalovací proces a jak probíhá eskalace incidentů.

Informace musí být nejen dostupné, ale i správně strukturované, včasné a srozumitelné pro konkrétní rozhodovací situaci. Manažer bezpečnosti je mostem mezi technikou, rizikem a vedením – a tomu musí odpovídat i podpora, kterou dostává [2][15].

2.1.2 Klíčové bezpečnostní ukazatele

Pro správné řízení bezpečnosti potřebuje ISO/CISO nejen kvalitní data, ale také schopnost jejich vyhodnocení pomocí vhodných ukazatelů. Klíčové výkonnostní ukazatele (KPI – Key Performance Indicators) a ukazatele rizik (KRI – Key Risk Indicators) umožňují sledovat efektivitu bezpečnostních opatření, včas rozpoznat potenciální slabiny a argumentovat při rozhodování o prioritách a investicích [2].

Kolouch a Bašta zdůrazňují, že metriky (míry) musí být srozumitelné nejen pro bezpečnostní odborníky, ale i pro vedení organizace. Mají sloužit jako most mezi technickým stavem a strategickým pohledem [2].

Příklady klíčových ukazatelů pro ISO/CISO:

KPI – Výkonnostní ukazatele:

- Počet aplikovaných bezpečnostních záplat v čase (patch compliance rate)
- Průměrná doba detekce a reakce na incident (MTTD/MTTR)
- Podíl školených zaměstnanců v oblasti kybernetické hygieny
- Počet zjištěných nesouladů při interním auditu

KRI – Ukazatele rizik:

- Počet otevřených kritických zranitelností v systémech

- Míra úspěšnosti phishingových testů
- Počet výjimek ze standardů bezpečnosti (např. výjimky z MFA)
- Výskyt opakujících se incidentů ve stejných systémech

Dobře nastavené ukazatele pomáhají nejen řídit běžný provoz bezpečnosti, ale také podporují komunikaci s vedením a regulačními orgány. Při výběru konkrétních ukazatelů je důležité, aby odpovídaly cíli měření, byly realisticky měřitelné a umožňovaly srovnání v čase.

Bezpečnostní ukazatele by neměly být jen „čísla pro reporting“, ale nástrojem pro prioritizaci a zlepšování bezpečnostního stavu. Bez nich není možné řídit bezpečnost na základě dat.

2.1.3 Potřeby v oblasti monitoringu, reportingu, analytiky a eskalace bezpečnostních incidentů

Schopnost včas identifikovat a zvládat bezpečnostní incidenty je jedním z pilířů efektivní kybernetické bezpečnosti. NIST CSF 2.0 definuje detekci, reakci a obnovu jako klíčové funkce rámce, přičemž monitoring a reporting incidentů tvoří základní předpoklad pro jejich naplnění [1].

ISO/CISO potřebuje přístup k relevantním a aktuálním informacím o událostech, které mohou ohrozit bezpečnost systémů a dat. Tyto informace mu umožňují:

- včas rozpoznat anomálie,
- zahájit efektivní eskalaci,
- sledovat trend výskytu incidentů,
- reagovat podle předem definovaných scénářů.

Podle Koloucha a Bašty by systém podpory měl zahrnovat nejen detekční technologie, ale i procesní stránku reakce – tedy reporting, analytiku a rozhodovací podporu [2].

Klíčové požadavky informační podpory:

- **Monitoring**

Průběžné sledování síťového provozu, systémových událostí a chování uživatelů. Využívají se nástroje jako SIEM, IDS/IPS, endpoint monitoring [1].

- **Reporting**

Automatizované i ruční výstupy o zjištěných událostech. Důraz je kladen na

přehlednost, kategorizaci a vazbu na SLA. Reporty by měly být přizpůsobené adresátům – jiné pro technický tým, jiné pro vedení.

- **Analytika**

Korelace událostí, rozpoznání vzorců útoků a predikce chování. Pokročilé analytické nástroje často využívají umělou inteligenci a strojové učení pro detekci anomálií [1].

- **Eskalace**

Definované procesy, kdy a komu se událost předává k řešení. Musí být napojeny na klasifikaci incidentů, priority, rozhodovací kompetence a krizové řízení.

Efektivní zvládnání incidentů je závislé nejen na technických nástrojích, ale i na tom, jak rychle a přesně informace dorazí k osobám s odpovědností za rozhodování. Informační podpora proto musí reflektovat různé úrovně a kanály komunikace.

2.2 Architektura informační podpory

Architektura informační podpory představuje strukturu systémů, nástrojů a procesů, které zajišťují přísun relevantních informací pro rozhodování ISO/CISO. Cílem je vytvořit propojený ekosystém, který podporuje každodenní operativu i strategické řízení bezpečnosti.

Podle rámce COBIT 5 by měla být informační architektura řízena podle obchodních potřeb organizace, být dostatečně flexibilní a umožňovat efektivní komunikaci mezi bezpečnostními rolemi, IT týmem a vrcholovým vedením [14].

V následujících podkapitolách je popsán návrh hlavních komponent, model toku informací a typické nástroje, které tuto architekturu podporují.

2.2.1 Definování klíčových komponent systému informační podpory

Systém informační podpory pro ISO/CISO by měl být tvořen souborem technologických, procesních a komunikačních prvků, které společně zajišťují sběr, vyhodnocení a distribuci informací důležitých pro bezpečnostní řízení. Podle COBIT 5 by tato architektura měla odpovídat principům **integrace, konzistence, odpovědnosti a udržitelnosti** [14].

Mezi klíčové komponenty patří:

- **Datové vstupy**

Informace ze systémů pro monitoring (např. SIEM), nástrojů pro správu zranitelností, asset managementu, logů, auditu a uživatelských aktivit.

- **Analytické a rozhodovací prvky**

Nástroje pro korelaci událostí, hodnocení rizik, reporting, vizualizaci a tvorbu ukazatelů. Důležitá je schopnost transformovat surová data do podoby využitelné pro rozhodování [14].

- **Komunikační rozhraní a dashboardy**

Prostředí pro přístup k informacím – ať už ve formě centralizovaného dashboardu, automatizovaného reportingu, alertingového systému nebo pravidelných analytických výstupů. Výstupy musí odpovídat cílovým skupinám – IT, vedení, compliance.

- **Eskalace a řízení odpovědnosti**

Jasně definovaná pravidla, kdo dostává jaké informace, kdy a na základě jakých událostí. Architektura musí podporovat rychlou eskalaci i pravidelné řízení.

Podle Koloucha a Bašty je důležité, aby systém nebyl tvořen pouze technickými prvky, ale také definovanými procesy a odpovědnostmi – bez toho nebude informační podpora skutečně funkční [2].

Klíčem k úspěšné architektuře není množství nástrojů, ale jejich propojenost, interpretace dat a schopnost doručit správnou informaci správnému člověku ve správný čas.

2.2.2 Model informačního toku mezi manažery bezpečnosti, IT týmem a vedením

Efektivní informační podpora v oblasti kybernetické bezpečnosti vyžaduje nejen dostupnost dat, ale také jasně definovaný tok informací mezi jednotlivými rolemi. ISO/CISO funguje jako spojovací článek mezi technickou a strategickou úrovní řízení. Informace musí proudit ve dvou směrech – **zdola nahoru (od IT směrem k vedení) a shora dolů (od vedení k technickým týmům)** [3][2].

Podle rámce COBIT 5 je zásadní, aby informační architektura podporovala **role, odpovědnosti a požadavky jednotlivých úrovní řízení**. Tím se snižuje riziko chybné interpretace a zpoždění informací [14].

Hlavní směry informačního toku:

- **IT → ISO/CISO**

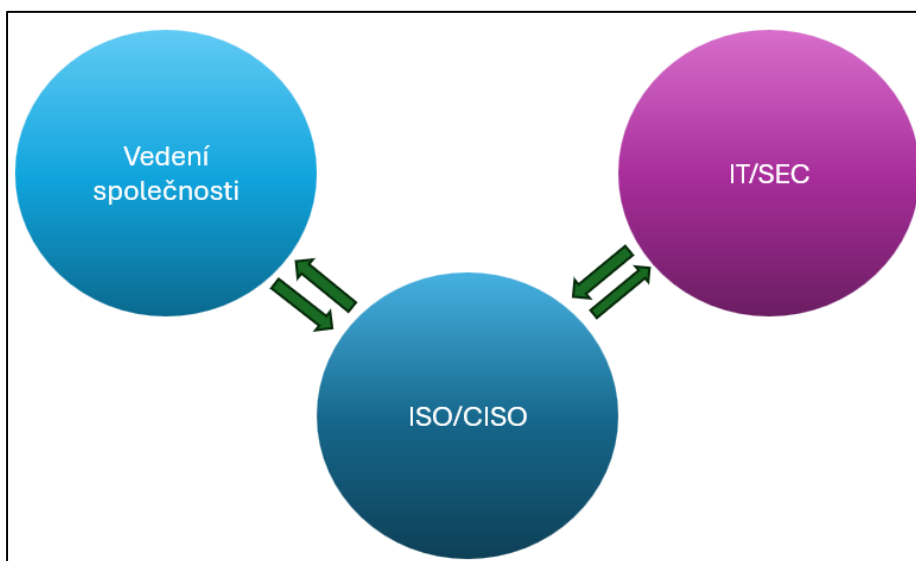
Technická data o incidentech, zranitelnostech, změnách v prostředí, provozních výpadcích, konfiguracích. Tato data jsou často získávána z nástrojů jako SIEM, vulnerability management nebo monitoring sítě [3].

- **ISO/CISO → Vedení**

Překlad technických informací do jazyka rizik, dopadů a priorit. Typickými výstupy jsou přehledy souladu s regulacemi, reporty o incidentech, návrhy na rozpočty a opatření [2][14].

- **Vedení → ISO/CISO → IT**

Vedení organizace definuje strategická rozhodnutí, obchodní cíle a regulační priority. ISO/CISO na základě těchto zadání navrhuje bezpečnostní projekty, interní politiky a překládá požadavky vedení do konkrétních technických opatření, která realizuje IT oddělení [3].



Obrázek 3: Vztahy a tok informací mezi vedením společnosti, ISO/CISO a IT/SEC týmem
(zdroj: vlastní zpracování)

Typická informační rozhraní v organizaci:

- Dashboardy a reporty pro vedení
- Alerting pro IT týmy a SOC
- Interní wiki nebo GRC nástroje pro řízení procesů
- Pravidelné bezpečnostní porady

Správně nastavený informační tok zajišťuje, že se informace dostanou ke správným lidem včas, v přehledné formě a s jasnou vazbou na rozhodovací pravomoci [3][2][14].

2.2.3 Technické nástroje (SIEM systémy, threat intelligence platformy, risk management nástroje)

Technické nástroje tvoří páteř systému informační podpory. Pomáhají detekovat hrozby, vyhodnocovat incidenty, řídit rizika a vytvářet výstupy pro rozhodování. ISO/CISO musí mít přístup k datům nejen v reálném čase, ale také k analytickým a historickým výstupům [3].

Mezi klíčové nástroje patří:

- **SIEM systémy (Security Information and Event Management)**
Slouží ke sběru, korelaci a analýze logů ze síťových zařízení, serverů, aplikací a bezpečnostních komponent. Umožňují identifikaci vzorců útoků, anomálií a incidentů. Zástupci: Splunk, IBM QRadar, ArcSight [2].
- **Threat Intelligence platformy**
Umožňují shromažďovat, validovat a využívat informace o aktuálních hrozbách (indikátory kompromitace, TTP útočníků). Integrují se do SIEM a slouží k predikci a prevenci útoků. Příklady: MISP, Recorded Future, ThreatConnect [2][3].
- **Risk management nástroje**
Podporují identifikaci, hodnocení a mitigaci rizik. Zajišťují sledování změn v rizikovém profilu organizace a přehled o plánovaných a implementovaných opatřeních. Často součástí GRC platform. Příklady: RSA Archer, ServiceNow Risk, LogicManager [3].
- **CMDB a asset management**
Databáze aktiv a jejich konfigurací tvoří základ pro řízení zranitelností, přístupů a provozních závislostí. Vede k lepšímu pochopení dopadu hrozeb a zajištění kontinuity služeb [2].

Důležitá není jen samotná technologie, ale také její správná integrace, přehlednost výstupů a schopnost poskytovat informace v takové podobě, která odpovídá potřebám ISO/CISO i ostatních uživatelů systému.

2.3 Doporučené nástroje a postupy

Technologická řešení hrají klíčovou roli v každodenní práci manažera kybernetické bezpečnosti. Kromě základních systémů, jako jsou SIEM nebo nástroje pro správu rizik, existují specializovaná softwarová řešení, která zvyšují efektivitu detekce, reakce a řízení

bezpečnostních procesů. Tato kapitola představuje výběr doporučených nástrojů a moderních přístupů, které mají přímý dopad na úroveň informační podpory v organizaci.

2.3.1 Přehled nejpoužívanějších softwarových řešení

V oblasti informační podpory patří mezi nejčastěji používané nástroje platformy pro korelaci dat, automatizaci incidentů a zpracování hrozeb. ISO/CISO se na jejich výstupy spoléhá při každodenním rozhodování, plánování opatření i komunikaci s vedením a auditory.

Vybraná řešení:

- **Splunk**

Výkonný SIEM systém s možností vizualizace dat a tvorby vlastních měř. Vhodný pro velké organizace s požadavky na pokročilou analytiku a flexibilitu [3].

- **IBM QRadar**

Komplexní platforma pro bezpečnostní monitoring, korelaci logů a správu incidentů. Využíván ve středních i velkých firmách pro centralizovaný dohled [2].

- **Elastic Security**

Otevřená platforma vycházející z Elasticsearch. Poskytuje funkce pro detekci hrozeb, korelaci událostí a analýzu dat v reálném čase. Je vhodná pro organizace s požadavky na flexibilitu, otevřenost a vlastní správu prostředí [21].

- **Palo Alto Cortex XSOAR**

Pokročilá SOAR platforma (Security Orchestration, Automation and Response), která umožňuje automatizaci reakcí na incidenty pomocí tzv. playbooků. Usnadňuje standardizaci bezpečnostních procesů a zrychluje reakční časy [22].

Výběr konkrétního řešení závisí na velikosti organizace, dostupných zdrojích a požadavcích na škálovatelnost. Pro ISO/CISO je důležité, aby nástroj poskytoval přehledné výstupy, podporoval integraci se stávajícími systémy a umožňoval nastavení měř a alertů dle potřeb organizace.

2.3.2 Automatizace kybernetické bezpečnosti

S rostoucím počtem bezpečnostních událostí a nedostatkem kvalifikovaných odborníků se organizace stále častěji spoléhají na automatizaci bezpečnostních operací. Platformy typu SOAR umožňují standardizovat, zrychlit a zefektivnit reakce na incidenty a snižují riziko lidské chyby v krizových situacích.

Podle Koloucha a Bašty je automatizace klíčovým prvkem při budování odolnosti organizace – zvláště v prostředí, kde není možné ručně vyhodnocovat všechny události [2]. SOAR systémy propojují nástroje jako SIEM, threat intelligence a workflow nástroje do jednoho automatizovaného celku.

Hlavní funkce SOAR systémů:

- **Orchestrace**

Integrace různých bezpečnostních nástrojů do jednoho prostředí. Systém sbírá a propojuje informace z logovacích, analytických a detekčních nástrojů [22].

- **Automatizace reakcí**

Na základě předdefinovaných scénářů (playbooků) lze provádět automatické akce, jako je blokáce IP adresy, deaktivace účtu nebo odeslání upozornění. To zvyšuje rychlost reakce a zajišťuje konzistenci postupu [22].

- **Záznam a audit**

Každý krok automatizovaného procesu je zaznamenán, což podporuje auditní dohled a sledování souladu s politikami organizace [22].

- **Redukce zátěže SOC**

Automatizace pomáhá filtrovat nerelevantní události a umožňuje bezpečnostním analytikům soustředit se na skutečně kritické incidenty [22].

SOAR platformy jsou vhodné zejména pro střední a velké organizace, které již provozují vlastní SOC nebo plánují jeho rozvoj. Pomáhají budovat procesní vyspělost a snižují závislost na lidské operativě.

2.3.3 Role umělé inteligence v kybernetické bezpečnosti

Umělá inteligence (AI) se stává klíčovým prvkem v kybernetické bezpečnosti. Umožňuje automatizaci detekce hrozeb, analýzu anomálií i rychlejší rozhodování. Zároveň ale představuje nová rizika, například zneužití pro cílené phishingové útoky či deepfake [10].

AI se dnes běžně integruje do nástrojů typu SIEM, EDR či SOAR. Umožňuje:

- **Rychlejší detekci** neobvyklého chování na síti a koncových zařízeních,
- **Korekci falešně pozitivních alertů** pomocí strojového učení,
- **Predikci vývoje incidentů** a doporučení dalších kroků,
- **Zefektivnění práce SOC týmů** díky automatizaci rutinních úloh.

Podle NGSS je však nutné, aby AI nebyla vnímána jako náhrada lidské analýzy, ale jako **podpůrný nástroj**, který zvyšuje kapacitu lidského týmu a posiluje odolnost organizace [10].

Rizika spojená s AI v bezpečnosti:

- **Zneužití útočníky** – např. generování realistických podvodných e-mailů pomocí LLM modelů,
- **Závislost na „black-box“ algoritmech** – snížená transparentnost rozhodování,
- **Etické a regulatorní otázky** – AI v bezpečnostních procesech může být obtížné auditovat.

Umělá inteligence nabízí nové možnosti efektivního řízení bezpečnosti, ale její nasazení musí být vyvážené, auditovatelné a podpořené odbornou kontrolou [10].

II PRAKTICKÁ ČÁST

3 VYTVOŘENÍ MATURITY MODELU

Tato kapitola je praktickou částí diplomové práce a je zaměřena na tvorbu vlastního maturity modelu, který má za cíl systematicky posoudit a hodnotit vyspělost informační podpory manažera kybernetické bezpečnosti v bankovním sektoru. Vytvořený model je přizpůsoben potřebám středně velké organizace (cca 200 zaměstnanců), která působí jako dceřiná společnost větší korporace s více než 10 000 zaměstnanci v České republice. Tento specifický kontext přináší jak výhody v podobě možnosti využití zkušeností a infrastruktury mateřské organizace, tak i výzvy související s limitovanými lokálními zdroji, potřebou dodržování regulačních požadavků a koordinací bezpečnostních aktivit napříč celou skupinou [4], [12].

Navržený maturity model vychází z osvědčených mezinárodních standardů a rámců (ISO/IEC 27005, NIST Cybersecurity Framework 2.0, COBIT 5) a zohledňuje regulační požadavky Evropské unie stanovené směrnicí NIS2 a nařízením DORA [5], [1], [14].

Pro vytvoření tohoto modelu byly definovány jasné úrovně vyspělosti, relevantní domény (oblasti) a kritéria pro jejich hodnocení. Cílem modelu je poskytnout manažerům kybernetické bezpečnosti jasnou strukturu pro vyhodnocení současného stavu bezpečnosti v oblasti informační podpory, identifikaci klíčových oblastí pro zlepšení a stanovení jasných kroků k dosažení vyšší úrovně zralosti a kybernetické odolnosti.

Kapitola je rozdělena na několik částí. Nejdříve bude uveden podrobný popis a vysvětlení samotného konceptu maturity modelu (kapitola 3.1). Následně bude představen vlastní návrh struktury modelu, definovány oblasti (domény) a stanoveny úrovně vyspělosti (kapitola 3.2). V dalších podkapitolách budou detailně popsána kritéria a metodika hodnocení, návrh auditního procesu, implementační doporučení a postupy kontinuálního zlepšování.

3.1 Úvod do navrženého maturity modelu

V kontextu kybernetické bezpečnosti a informační podpory manažera kybernetické bezpečnosti představují maturity modely účinný nástroj, který umožňuje organizacím objektivně vyhodnotit svůj současný stav bezpečnostních opatření a stanovit cíle dalšího rozvoje a zlepšování. Maturity model, který je předmětem této kapitoly, se zaměřuje na specifické potřeby středně velké organizace působící v bankovním sektoru. Jeho primárním cílem je vytvořit strukturovaný rámec, jenž manažerům kybernetické bezpečnosti

(ISO/CISO) pomůže identifikovat silné a slabé stránky stávající informační podpory a poskytnout jasná vodítka pro zvyšování kybernetické odolnosti organizace.

3.1.1 Definice a smysl maturity modelů v kybernetické bezpečnosti

Maturity modely obecně představují strukturované nástroje, jejichž cílem je hodnocení úrovně vyspělosti procesů a postupů v konkrétních oblastech řízení, a to za použití definovaných úrovní vyspělosti (tiers) a kritérií. V oblasti kybernetické bezpečnosti slouží především k tomu, aby organizace získaly ucelený a konzistentní pohled na úroveň řízení kybernetických rizik, procesů a technologických opatření [5].

Organizace, zejména v bankovním sektoru, kde jsou informace vysoce citlivým a cenným aktivem, jsou stále více vystaveny rostoucím a sofistikovaným kybernetickým hrozbám. Z tohoto důvodu je zavedení efektivního systému řízení informační bezpečnosti (ISMS) klíčovým aspektem provozní odolnosti, která má zásadní dopad nejen na bezpečnost organizace samotné, ale i na její klienty a celkovou stabilitu finančního trhu [12].

V návaznosti na normy a standardy, jako jsou ISO/IEC 27001, ISO/IEC 27005 a NIST Cybersecurity Framework 2.0, lze pomocí maturity modelu lépe stanovit priority a konkrétní kroky vedoucí k cílovému bezpečnostnímu stavu [1].

3.1.2 Přínosy aplikace maturity modelu pro organizace

Použití navrženého maturity modelu přináší organizaci několik klíčových výhod, a to zejména v prostředí, kde je kladen důraz na vysokou úroveň regulace a compliance, jako je tomu právě v bankovním sektoru.

- **Systematické hodnocení:** Model umožňuje průběžně hodnotit účinnost nastavených procesů informační podpory a identifikovat oblasti, které vyžadují cílenou pozornost.
- **Strategické plánování a řízení:** Pomocí maturity modelu mohou manažeři kybernetické bezpečnosti efektivně definovat strategické cíle a priority a zaměřit zdroje organizace tam, kde budou mít největší dopad na zvýšení kybernetické odolnosti [1].
- **Transparentnost vůči managementu a regulátorům:** Model umožňuje jasně a srozumitelně prezentovat stav kybernetické bezpečnosti a její rozvoj vůči vyššímu vedení i regulatorním orgánům, což usnadňuje prokázání souladu s regulatorními požadavky podle směrnice NIS2 nebo nařízení DORA [4], [12].

- **Podpora rozhodování:** Manažerům poskytuje objektivní data o současném stavu a doporučeních pro další kroky, což jim umožňuje přijímat informovaná rozhodnutí o investicích do bezpečnostních technologií a opatření [3].
- **Zvýšení efektivity řízení bezpečnosti:** Díky jasně definovaným kritériím jednotlivých úrovní zralosti organizace snižují čas a náklady spojené s řízením kybernetické bezpečnosti, protože mohou cíleně implementovat opatření s největším efektem na snížení rizik [18].

3.2 Specifikace navrženého maturity modelu

Cílem této části práce je detailně představit navržený maturity model informační podpory manažera kybernetické bezpečnosti, který reflektuje praktické potřeby středně velké organizace působící v bankovním sektoru v České republice. Model byl vytvořen na základě osvědčených mezinárodních standardů a rámců, zejména ISO/IEC 27005, COBIT 5 a NIST Cybersecurity Framework 2.0. Současně bere v úvahu i regulatorní požadavky stanovené směrnicí NIS2 a nařízením DORA [5], [1], [4], [12], [14].

Termín „úroveň vyspělosti“ je v této práci používán konzistentně pro označení jednotlivých etap nebo stavů v rámci maturity modelu. Nicméně v souladu s rámcem NIST Cybersecurity Framework je běžně používaným a mezinárodně uznávaným termínem také „Tier“ (doslova „stupeň“), proto v textu vedle sebe uvádíme oba termíny pro zachování souladu s odbornou literaturou a terminologií používanou v praxi [1].

3.2.1 Klíčové oblasti (domény)

V rámci navrženého maturity modelu byly definovány klíčové oblasti (domény), které odpovídají specifickým potřebám řízení informační podpory manažera kybernetické bezpečnosti v prostředí středně velké bankovní organizace působící v České republice. Při výběru těchto domén byl kladen důraz na pokrytí všech relevantních aspektů kybernetické bezpečnosti s ohledem na regulatorní rámce EU (zejména NIS2 a DORA) [4], [12] a osvědčené mezinárodní standardy a rámce, jako jsou ISO/IEC 27001 a NIST Cybersecurity Framework 2.0 [1], [16].

Každá doména byla zvolena tak, aby reflektovala kritické oblasti bezpečnostních procesů, které musí organizace systematicky řídit, monitorovat a kontinuálně zlepšovat:

1. Bezpečnostní monitoring a reporting (Monitoring a reporting bezpečnostních událostí)

Tato doména zahrnuje procesy shromažďování, analýzy a reportingu bezpečnostních informací, které jsou nezbytné pro operativní a strategické řízení bezpečnosti v organizaci. Jedná se například o sledování bezpečnostních událostí a incidentů, využívání bezpečnostních dashboardů a pravidelný reporting vůči managementu a regulatorním orgánům [1].

2. Řízení bezpečnostních incidentů a automatizace reakcí (Incident management a SOAR)

Tato doména zahrnuje jak procesní řízení bezpečnostních incidentů, tak i využití automatizace pro zefektivnění reakcí na tyto incidenty. Zahrnuty jsou všechny kroky životního cyklu incidentu – od identifikace, klasifikace a analýzy, přes samotnou reakci, až po implementaci preventivních opatření. Součástí domény je rovněž využití pokročilých technologických nástrojů, zejména Security Orchestration, Automation, and Response (SOAR), které umožňují automatizovanou a koordinovanou reakci na incidenty. Efektivní propojení procesních a technologických prvků řízení bezpečnostních incidentů je klíčové pro rychlou, přesnou a efektivní mitigaci kybernetických hrozeb a zároveň přispívá k souladu s platnou legislativou a regulatorními požadavky [1], [4], [14].

3. Řízení rizik (Risk Management)

Tato doména zahrnuje procesy identifikace, analýzy, vyhodnocení a řízení kybernetických rizik, která ovlivňují provozní stabilitu organizace. Efektivní řízení rizik vyžaduje použití systematického přístupu v souladu s ISO/IEC 27005, který umožňuje identifikovat a prioritizovat rizika a určit odpovídající opatření pro jejich minimalizaci nebo eliminaci [3].

4. Řízení aktiv (Asset Management)

Správa aktiv zahrnuje identifikaci a evidenci informačních aktiv, stanovení jejich hodnoty, určení vlastníků a zajištění jejich odpovídající ochrany. Správně nastavené řízení aktiv je předpokladem efektivní ochrany informací a zároveň napomáhá organizaci splnit regulatorní požadavky a audity podle standardu ISO/IEC 27001 [16].

5. Organizační governance a compliance (Governance a soulad s regulatorními požadavky)

Tato oblast se zaměřuje na dodržování regulatorních požadavků, legislativy a interních pravidel v oblasti kybernetické bezpečnosti. Zahrnuje také odpovědnosti managementu, jasné definování rolí a pravomocí (ISO/CISO), jakož i pravidelné vyhodnocování

compliance vůči směrnici NIS2 a nařízení DORA, které jsou v bankovním sektoru klíčové [4], [12].

3.2.2 Úrovně vyspělosti navrženého maturity modelu

Pro objektivní hodnocení informační podpory kybernetické bezpečnosti je nezbytné definovat jasné strukturované **úrovně vyspělosti**, které organizacím umožňují nejen přesně identifikovat svůj aktuální stav, ale také cíleně definovat další kroky vedoucí k optimalizaci bezpečnostních procesů a opatření. Navržený maturity model pracuje se čtyřmi úrovněmi vyspělosti (Tier 1–4), přičemž tento koncept úrovní vychází z mezinárodně uznávaných rámců, zejména NIST Cybersecurity Framework 2.0 [1] a COBIT 5 [14].

Níže jsou detailně popsány jednotlivé úrovně vyspělosti včetně akademických a praktických referencí:

❖ Tier 1: Počáteční (Ad-hoc)

První úroveň vyspělosti reprezentuje organizace, které nemají formálně definované procesy informační podpory kybernetické bezpečnosti. Bezpečnostní opatření jsou prováděna reaktivně, zpravidla až jako reakce na incidenty nebo bezpečnostní události. Procesy řízení bezpečnosti jsou neformalizované, nekonzistentní a závisí převážně na znalostech a schopnostech jednotlivých pracovníků [5], [14].

Příklad:

Organizace reaguje na incidenty individuálně, nemá formalizovaný reporting incidentů ani jednotný způsob evidence kybernetických událostí.

❖ Tier 2: Informovaný přístup (Risk-informed)

Druhá úroveň je charakterizována základní znalostí kybernetických rizik a implementací základních bezpečnostních opatření. Organizace již identifikovala klíčová rizika, ale řízení těchto rizik je pouze částečné a procesy nejsou plně standardizované. Organizace využívá základní nástroje, například základní SIEM systém, avšak zatím bez pokročilé analytiky či automatizovaných reakcí [3], [1].

Dle ISO/IEC 27005 organizace na této úrovni začíná formalizovat procesy řízení rizik, ale implementace opatření ještě není systematická ani plně integrovaná do celkové struktury řízení bezpečnosti [3].

Příklad:

Organizace používá základní monitoring SIEM, ale incidenty jsou řešeny převážně manuálně bez automatizace.

❖ Tier 3: Formalizovaný a opakovatelný (Repeatable)

Na této úrovni organizace dosahují již formalizovaných, pravidelně opakovaných a auditovaných procesů. Bezpečnostní opatření jsou systematicky aplikována napříč celou organizací, existují jasně definované role a odpovědnosti, pravidelné vyhodnocování rizik a audity podle ISO/IEC 27001 [16]. Reporting incidentů je centralizovaný a pravidelný, což umožňuje kvalitní řízení kybernetické bezpečnosti a snadné plnění regulatorních požadavků (např. NIS2, DORA) [4], [12].

Dle COBIT 5 se organizace na této úrovni vyznačují zavedenými procesy řízení, které jsou pravidelně hodnoceny, což umožňuje kontinuální zlepšování a zajištění efektivity řízení bezpečnosti [14].

Příklad:

Organizace má plně funkční SIEM řešení a definovaný proces incident response, který je pravidelně testován a auditován.

❖ Tier 4: Adaptivní (Optimized)

Nejvyšší úroveň vyspělosti (Optimized) je typická pro organizace, které efektivně integrují pokročilé technologie (SIEM, SOAR, AI) a využívají je k automatizaci, predikci a efektivnímu řízení kybernetické bezpečnosti. Procesy jsou dynamicky upravovány na základě aktuálních potřeb, nové hrozby jsou identifikovány prediktivně a organizace je schopná jim předcházet díky pokročilé analytice [1], [14].

Organizace je na této úrovni schopná pružně reagovat na regulatorní změny, má proaktivní přístup k řízení rizik a kontinuálně optimalizuje své bezpečnostní procesy [1].

Příklad:

Organizace využívá pokročilé analytické nástroje (AI, ML) integrované do SOAR systému pro automatické detekování a řešení incidentů v reálném čase.

3.3 Implementační doporučení

Pro zajištění objektivního a konzistentního hodnocení úrovně vyspělosti v jednotlivých doménách navrženého maturity modelu je klíčové jasné definovat konkrétní kritéria a indikátory. Tato kritéria budou umožňovat detailní a praktické vyhodnocení aktuálního stavu informační podpory manažera kybernetické bezpečnosti v organizaci.

Kritéria vychází z mezinárodních standardů a rámců, zejména **ISO/IEC 27001**, **ISO/IEC 27005**, rámce **NIST Cybersecurity Framework 2.0** a **COBIT 5** [3], [1], [14], [16]. Současně reflektují požadavky evropské legislativy (zejména směrnice NIS2 a nařízení DORA) na informační podporu kybernetické bezpečnosti [4], [12].

Každé kritérium je formulováno tak, aby bylo měřitelné, relevantní a aplikovatelné v praxi. Kritéria jsou rozdělena podle definovaných domén a úrovní vyspělosti (Tierů), přičemž každá úroveň má svá specifická kritéria odrážející odpovídající úroveň řízení a implementace bezpečnostních procesů.

Hodnocení podle těchto kritérií umožňuje:

- Přesně identifikovat současnou úroveň vyspělosti organizace v jednotlivých doménách.
- Určit slabé a silné stránky informační podpory.
- Definovat konkrétní kroky, které organizace potřebuje učinit, aby se posunula do vyšší úrovně vyspělosti.
- Transparentně prokázat soulad s regulačními požadavky v oblasti kybernetické bezpečnosti (NIS2, DORA).

Každá doména z kapitoly bude nyní detailně rozpracována s definicí konkrétních kritérií pro každou z úrovní vyspělosti definovaných v kapitole.

Pro každou doménu a úroveň budou vytvořeny:

- **Kvalitativní indikátory:** jasný popis očekávaného stavu procesů a opatření.
- **Kvantitativní indikátory:** pokud možno měřitelné ukazatele umožňující objektivní posouzení stavu bezpečnosti (např. míra automatizace reakcí na incidenty, procento pokrytí aktiv v evidenci apod.).
- **Praktické příklady:** konkrétní scénáře, které ilustrují naplnění daného kritéria v praxi.

Metodika hodnocení zahrnuje kombinaci:

- Analýzy dokumentace a interních politik organizace.
- Rozhovorů s relevantními pracovníky (ISO/CISO, IT, Risk Management).
- Přezkumu konfigurace a využití technologických nástrojů (např. SIEM, SOAR, Asset Management systémů).

3.3.1 Bezpečnostní monitoring a reporting

Doména „Bezpečnostní monitoring a reporting“ představuje jednu z klíčových oblastí pro efektivní řízení kybernetické bezpečnosti. Tato doména zahrnuje procesy sběru, analýzy a reportingu bezpečnostních událostí a incidentů, využití monitorovacích nástrojů (např. SIEM systémů), a poskytování relevantních dat pro manažerské rozhodování [1], [16].

Tabulka níže shrnuje jasně definovaná kritéria, kvantitativní a kvalitativní indikátory a praktické příklady pro každou úroveň vyspělosti této domény:

Tabulka 2: Kritéria, indikátory a příklady implementace jednotlivých úrovní vyspělosti (Tierů) pro doménu „Řízení bezpečnostních informací (Monitoring, Reporting a Analytika)“

Úroveň vyspělosti	Kritéria	Indikátory	Praktický příklad
Tier 1: Počáteční (Ad-hoc)	Neexistují formální pravidla pro monitoring a reporting. Analýza dat probíhá pouze ad-hoc.	Organizace nevyužívá centralizovaný monitoring ani reporting incidentů.	Incidenty se řeší neformálně, např. telefonicky nebo e-mailem, bez systematické evidence.
Tier 2: Informovaný (Risk-informed)	Zaveden základní monitoring a reporting incidentů. Základní ruční analytika dat.	Využíván základní monitoring (např. open-source SIEM). Reporting je pravidelný, ale neúplný.	Organizace používá jednoduchý nástroj typu Graylog pro sledování bezpečnostních událostí, ale reakce na incidenty je manuální a pomalá.
Tier 3: Formalizovaný a opakovatelný (Repeatable)	Formalizovaný proces monitoringu a reportingu pomocí pokročilých nástrojů (SIEM). Pravidelné audity a kontroly efektivity procesu.	Pokročilý SIEM s pravidelnými analýzami trendů. Formalizovaný reporting s detailními bezpečnostními statistikami.	SIEM (např. Splunk nebo QRadar) automaticky sbírá data, která se pravidelně analyzují a reportují vedení dle požadavků regulatorních předpisů (např. NIS2).

Úroveň vyspělosti	Kritéria	Indikátory	Praktický příklad
Tier 4: Adaptivní (Optimized)	Pokročilá automatizace monitoringu a analýzy s využitím SIEM, SOAR a AI. Automatická reakce na incidenty v reálném čase.	Plná integrace SIEM, SOAR a AI. Automatické reporty a reakce na incidenty bez manuálních zásahů.	SIEM a SOAR systémy automaticky analyzují a řeší incidenty za podpory AI, což minimalizuje lidský faktor a výrazně zkracuje dobu odezvy.

(zdroj: vlastní zpracování dle [1], [14], [16])

Tato struktura jasně definuje kritéria a indikátory pro každou úroveň vyspělosti domény „Řízení bezpečnostních informací“. Na základě těchto kritérií lze efektivně posoudit, v jaké úrovni se organizace nachází, a stanovit jasné kroky pro dosažení vyšší úrovně vyspělosti a celkového zlepšení informační podpory kybernetické bezpečnosti.

3.3.2 Řízení bezpečnostních incidentů a automatizace reakcí

Doména „Řízení bezpečnostních incidentů“ zahrnuje procesy identifikace, analýzy, reakce a prevence kybernetických incidentů společně s využitím technologií pro automatizaci těchto procesů, zejména nástrojů typu Security Orchestration, Automation and Response (SOAR). Díky integraci procesů řízení incidentů s automatizačními technologiemi organizace významně zkracuje dobu odezvy, snižuje riziko negativních dopadů bezpečnostních incidentů a současně splňuje požadavky platné legislativy a regulatorních standardů [1], [14].

Tabulka 3: Kritéria, indikátory a příklady implementace jednotlivých úrovní vyspělosti (Tierů) pro doménu „Řízení bezpečnostních incidentů a automatizace reakcí“

Úroveň vyspělosti	Kritéria	Indikátory	Praktický příklad
Tier 1: Počáteční (Ad-hoc)	Incidenty jsou řešeny ad-hoc, bez formálního procesu. Automatizace reakcí na incidenty není implementována.	Neexistuje systém evidence a analýzy incidentů. Reakce probíhá ručně a nekoordinovaně.	Incidenty řeší jednotlivci bez jasných pravidel, typicky telefonicky či e-mailem, bez evidence či zpětného vyhodnocování.
Tier 2: Informovaný (Risk-informed)	Zaveden základní proces řízení incidentů.	Evidence incidentů existuje, ale není systematická. Reakce	Incidenty se evidují v tabulce (např. Excel), ale reakce je ruční a

Úroveň vyspělosti	Kritéria	Indikátory	Praktický příklad
	Automatizace reakcí je minimální nebo žádná.	jsou manuální, bez pokročilých technologických nástrojů.	pomalá. Organizace používá základní monitoring, ale bez integrace se SOAR.
Tier 3: Formalizovaný a opakovatelný (Repeatable)	Organizace má formální proces řízení incidentů, pravidelně jej vyhodnocuje a zlepšuje. Zavedeny pokročilé nástroje pro monitoring (SIEM) a částečná automatizace reakcí (SOAR).	Existují formalizované procedury a nástroje (např. Splunk s Phantom nebo ServiceNow Security Incident Response). Zavedená částečná automatizace, základní workflow řešení incidentů.	Incidenty jsou automaticky detekovány SIEM nástrojem a základní reakce jsou částečně automatizované pomocí SOAR, což zkracuje dobu řešení incidentů a umožňuje efektivní reporting managementu.
Tier 4: Adaptivní (Optimized)	Pokročilý proces řízení incidentů plně integrovaný s automatizací (SOAR) a umělou inteligencí (AI). Incidenty jsou detekovány, analyzovány a řešeny automaticky v reálném čase.	Plná integrace pokročilých nástrojů (SIEM, SOAR, AI) s automatizovaným workflow. Incidenty jsou detekovány prediktivně, reakce je okamžitá, automatická a bez nutnosti manuálních zásahů.	Systémy (např. Cortex XSOAR) automaticky identifikují bezpečnostní incidenty pomocí AI a okamžitě reagují automatizovanou mitigací, což minimalizuje dopady incidentů a umožňuje kontinuální optimalizaci procesu řízení incidentů.

(zdroj: vlastní zpracování dle [1], [14])

Závěrem této domény lze konstatovat, že zvyšování úrovně vyspělosti v oblasti řízení bezpečnostních incidentů významně přispívá k celkové kybernetické odolnosti organizace a její schopnosti efektivně plnit regulační požadavky dle evropské legislativy, zejména NIS2 a DORA [4], [12].

3.3.3 Řízení rizik

Doména „Řízení rizik“ zahrnuje systematické procesy identifikace, analýzy, hodnocení a řízení kybernetických rizik. Efektivní řízení rizik je nezbytné pro správné nastavení priorit bezpečnostních opatření a cílenou ochranu organizace před kybernetickými hrozbami. Správné řízení rizik také umožňuje splnit požadavky regulačních norem, zejména ISO/IEC 27005, směrnice NIS2 a nařízení DORA.

Tabulka 4: Kritéria, indikátory a příklady implementace jednotlivých úrovní vyspělosti (Tierů) pro doménu „Řízení rizik“

Úroveň vyspělosti	Kritéria	Indikátory	Praktický příklad
Tier 1: Počáteční (Ad-hoc)	Rizika nejsou systematicky identifikována ani řízena, hodnocení rizik probíhá ad-hoc nebo vůbec neprobíhá.	Organizace nevede formální evidenci rizik, ani neprovádí jejich analýzu nebo hodnocení.	Rizika jsou řešena pouze reaktivně v případě incidentů, bez dokumentace nebo pravidelného přezkoumávání.
Tier 2: Informovaný (Risk-informed)	Organizace provádí základní identifikaci a analýzu rizik, avšak proces není zcela formalizován ani systematický.	Existuje jednoduchá evidence rizik (např. tabulkový dokument), ale chybí pravidelná aktualizace a analýza dopadů.	Organizace má vytvořen základní seznam kybernetických rizik, ale hodnocení se provádí pouze příležitostně nebo povrchně.
Tier 3: Formalizovaný a opakovatelný (Repeatable)	Proces řízení rizik je formalizovaný dle standardu ISO/IEC 27005, pravidelně se provádí identifikace, analýza, vyhodnocení a řízení rizik.	Zavedeny jsou pravidelné revize rizik a aktualizace opatření; dokumentace je systematická a strukturovaná.	Organizace využívá pravidelně aktualizovaný registr rizik, provádí systematickou analýzu a stanovuje konkrétní opatření pro řízení rizik.
Tier 4: Adaptivní (Optimized)	Pokročilý a proaktivní přístup k řízení rizik, využití automatizace a pokročilé analytiky (AI, strojové učení) pro identifikaci a predikci rizik.	Automatizovaná analýza rizik v reálném čase, integrace výsledků analýzy rizik do strategického plánování bezpečnosti organizace.	Rizika jsou kontinuálně monitorována pomocí pokročilé analytiky; potenciální hrozby jsou identifikovány prediktivně, což umožňuje proaktivní reakci.

(zdroj: vlastní zpracování dle [8], [14])

Závěrem lze konstatovat, že jasně strukturované a formalizované řízení rizik je pro organizace v bankovním sektoru zásadní pro zajištění efektivní ochrany, prokázání souladu s regulatorními požadavky a posílení celkové odolnosti vůči kybernetickým hrozbám.

3.3.4 Řízení aktiv

Doména „Řízení aktiv“ zahrnuje systematickou správu, evidenci a ochranu informačních a technologických aktiv organizace. Správné řízení aktiv je předpokladem efektivního řízení kybernetické bezpečnosti, neboť umožňuje přesnou identifikaci kritických aktiv, určení

jejich vlastníků, definování hodnoty aktiv, a následně vhodné nastavení ochranných opatření podle požadavků ISO/IEC 27001.

Tabulka 5: Kritéria, indikátory a příklady implementace jednotlivých úrovní vyspělosti (Tierů) pro doménu „Řízení aktiv“

Úroveň vyspělosti	Kritéria	Indikátory	Praktický příklad
Tier 1: Počáteční (Ad-hoc)	Neexistuje formální evidence aktiv organizace. Aktiva nejsou systematicky řízena ani chráněna.	Organizace nemá žádný seznam aktiv nebo má jen částečné neformální seznamy. Není definován vlastník aktiv.	Evidence aktiv je udržována pouze individuálně jednotlivými zaměstnanci, bez centrální koordinace.
Tier 2: Informovaný (Risk-informed)	Základní evidence aktiv existuje, ale není plně formalizovaná ani pravidelně aktualizovaná. Aktiva mají alespoň základně definované vlastníky.	Organizace má jednoduchý registr aktiv (např. Excel tabulka). Aktiva jsou nepravidelně aktualizována.	Seznam aktiv je dostupný, ale ne vždy aktuální; některá aktiva jsou uvedena bez přesných detailů (např. chybí hodnoty, klasifikace či vlastníci).
Tier 3: Formalizovaný a opakovatelný (Repeatable)	Organizace vede formalizovaný registr aktiv dle ISO/IEC 27001. Aktiva mají definované vlastníky, pravidelně se aktualizují a jejich ochrana je systematicky řízena podle hodnoty a rizik.	Zaveden je centralizovaný systém řízení aktiv, který umožňuje pravidelnou aktualizaci, klasifikaci aktiv a přidělení vlastníků. Jsou stanoveny odpovědnosti a postupy kontroly správnosti evidence.	Registr aktiv je pravidelně revidován a aktualizován, každé aktivum má jasně určeného vlastníka, který odpovídá za jeho ochranu a pravidelnou kontrolu.
Tier 4: Adaptivní (Optimized)	Pokročilý systém automatické evidence a správy aktiv s integrací do systémů monitoringu a řízení rizik. Využití pokročilé analytiky pro automatickou klasifikaci a prioritizaci ochrany aktiv.	Automatizované procesy pro identifikaci a klasifikaci aktiv v reálném čase. Integrace systému správy aktiv se systémy monitoringu, řízení rizik a incident management (SIEM, SOAR).	Aktiva jsou automaticky identifikována a klasifikována pomocí integrovaných systémů; při jakékoli změně v evidenci aktiv je automaticky aktualizován registr a přizpůsobena ochranná opatření.

(zdroj: vlastní zpracování dle [14], [16]).

Závěrem lze uvést, že formalizované a systematické řízení aktiv významně přispívá k účinnému řízení kybernetické bezpečnosti, protože organizace získává přehled o svých aktivech, jejich hodnotě a může efektivně nastavovat bezpečnostní opatření v souladu s regulatorními a normativními požadavky (např. ISO/IEC 27001).

3.3.5 Organizační řízení a compliance

Doména „Organizační řízení a compliance“ zahrnuje systematické řízení kybernetické bezpečnosti napříč celou organizací, včetně dodržování interních bezpečnostních politik, mezinárodních standardů (zejména ISO/IEC 27001) a regulatorních požadavků (směrnice NIS2 a nařízení DORA). Klíčovou součástí této domény je stanovení jasných odpovědností manažerských rolí v oblasti kybernetické bezpečnosti (zejména ISO a CISO), efektivní komunikace směrem k vedení organizace a pravidelné vyhodnocování souladu s legislativními a regulatorními požadavky.

Tabulka 6: Kritéria, indikátory a příklady implementace jednotlivých úrovní vyspělosti (Tier) pro doménu „Organizační řízení a compliance“

Úroveň vyspělosti	Kritéria	Indikátory	Praktický příklad
Tier 1: Počáteční (Ad-hoc)	Organizační řízení kybernetické bezpečnosti není formálně stanoveno, odpovědnosti jsou nejasné. Compliance není systematicky řešena.	Chybí formalizované bezpečnostní politiky nebo jsou neúplné a zastaralé. Odpovědnosti ISO/CISO nejsou stanoveny.	Řízení bezpečnosti probíhá nesystematicky, bez jasné odpovědnosti a struktury řízení.
Tier 2: Informovaný (Risk-informed)	Organizační řízení a compliance jsou částečně zavedeny. Existují základní bezpečnostní politiky, ale nejsou pravidelně aktualizovány ani kontrolovány.	ISO/CISO má částečně definovanou roli, ale její zapojení do strategických rozhodnutí organizace je minimální.	Politiky bezpečnosti existují, ale nejsou pravidelně aktualizovány; role ISO/CISO je formálně stanovena jen obecně.
Tier 3: Formalizovaný a opakovatelný (Repeatable)	Organizační řízení bezpečnosti je formalizováno podle standardu ISO/IEC 27001. Compliance se systematicky vyhodnocuje podle platné legislativy.	Pravidelné revize a aktualizace bezpečnostních politik. Jasně definované a pravidelně aktualizované odpovědnosti ISO/CISO.	Probíhají pravidelné interní audity a vyhodnocování compliance, ISO/CISO pravidelně komunikuje s vedením organizace.

Úroveň vypělosti	Kritéria	Indikátory	Praktický příklad
Tier 4: Adaptivní (Optimized)	Organizační řízení je pokročilé a flexibilní, compliance se průběžně automaticky vyhodnocuje pomocí specializovaných nástrojů. ISO/CISO je klíčovým strategickým partnerem vedení.	Automatizované nástroje (např. platformy typu GRC) se využívají pro kontinuální monitoring compliance vůči platné legislativě. ISO/CISO je plně integrován do strategického řízení organizace.	Compliance je automaticky sledována, ISO/CISO aktivně předkládá strategické návrhy vedení, účastní se rozhodování o rozvoji bezpečnostních opatření.

(zdroj: vlastní zpracování dle [1], [14])

Závěrem lze uvést, že systematické organizační řízení a efektivní compliance významně zvyšují schopnost organizace předcházet kybernetickým incidentům, efektivně na ně reagovat a transparentně prokazovat soulad s regulačními požadavky.

3.4 Auditní proces a hodnocení

Tato kapitola popisuje metodiku a doporučené postupy auditu a hodnocení vypělosti systému informační podpory manažera kybernetické bezpečnosti na základě navrženého maturity modelu. Jasně definovaný auditní proces je nezbytný pro objektivní a transparentní vyhodnocení aktuálního stavu organizace v jednotlivých doménách a úrovních vypělosti. Součástí kapitoly bude definice auditních technik, způsobu sběru důkazů, pravidelného vyhodnocování, interpretace výsledků a následného stanovení doporučení pro další rozvoj informační podpory kybernetické bezpečnosti.

Kapitola bude členěna do následujících částí:

Metodika a postup provádění auditů

Sběr důkazů a dokumentace

Vyhodnocení výsledků a doporučení

Auditní proces vychází ze standardních postupů uvedených v ISO/IEC 27001 a COBIT 5, s cílem zajistit jak soulad s platnou legislativou, tak i dosažení žádoucí úrovně kybernetické bezpečnosti a efektivní podpory role manažera kybernetické bezpečnosti [14], [16].

3.4.1 Metodika a postup provádění auditů

Aby mohl maturity model účinně plnit svoji roli nástroje pro objektivní vyhodnocování vyspělosti informační podpory kybernetické bezpečnosti, je klíčové zavést jasnou a systematickou metodiku auditu. Auditní proces popsáný v této kapitole definuje postupy, techniky a odpovědnosti při provádění pravidelných hodnocení vyspělosti systému informační podpory kybernetické bezpečnosti v organizaci. Cílem této metodiky je zajistit objektivitu, transparentnost a opakovatelnost výsledků auditu, což je předpokladem účinného řízení kybernetických rizik a compliance s platnou legislativou a regulačními standardy [14], [16].

Auditní proces je složen z následujících hlavních fází:

1. Plánování auditu

- Stanovení rozsahu auditu (vymezení hodnocených domén, úrovní vyspělosti a metodiky sběru důkazů).
- Určení odpovědných osob a vytvoření auditního týmu.
- Sestavení harmonogramu auditu a koordinace s vedením organizace a manažerem kybernetické bezpečnosti (ISO/CISO).

2. Sběr důkazů

- Dokumentační analýza – přezkum interních politik, směrnic, evidence incidentů, registrů rizik a dalších relevantních dokumentů
- technická analýza – kontrola konfigurace bezpečnostních technologií a systémů (SIEM, SOAR)
- rozhovory s odpovědnými pracovníky (zejména ISO/CISO, IT manažer, Risk manažer) pro ověření implementace procesů.

3. Vyhodnocení získaných důkazů

- Objektivní posouzení sesbíraných důkazů vzhledem k definovaným kritériím a indikátorům vyspělosti
- klasifikace aktuální úrovně vyspělosti v jednotlivých doménách
- identifikace nesouladů a slabých míst.

4. Reporting a prezentace výsledků

- Zpracování závěrečné auditní zprávy, shrnující výsledky, zjištění, slabá místa a doporučení.

- Prezentace výsledků vedení organizace s návrhem konkrétních opatření pro přechod na vyšší úroveň vyspělosti.
- Transparentní komunikace výsledků vůči regulačním orgánům (pokud to vyžaduje platná legislativa).

Auditní postup vychází z mezinárodních doporučení a metodik dle ISO/IEC 27001 a COBIT 5, které zajišťují objektivní hodnocení stavu kybernetické bezpečnosti a efektivní podporu řízení informační bezpečnosti [3], [14], [16].

Tabulka 7: Přehled fází auditního procesu a hlavních aktivit při hodnocení vyspělosti informační podpory kybernetické bezpečnosti

Fáze auditu	Hlavní aktivity a kroky
Plánování auditu	Určení rozsahu auditu, sestavení auditního týmu, příprava harmonogramu, definice metodiky sběru důkazů.
Realizace auditu (sběr důkazů)	Dokumentační analýza, rozhovory s pracovníky, kontrola technologických systémů (SIEM, SOAR), sběr relevantních technických a procesních důkazů.
Vyhodnocení výsledků	Analýza nasbíraných důkazů, stanovení úrovně vyspělosti v jednotlivých doménách, identifikace slabých míst a rizik.
Reporting a prezentace	Zpracování závěrečné zprávy, prezentace výsledků vedení, doporučení opatření pro zlepšení úrovně vyspělosti a souladu s platnou legislativou.

(zdroj: vlastní zpracování dle [14], [16])

Závěrem této části lze konstatovat, že systematicky prováděný auditní proces výrazně zvyšuje transparentnost řízení kybernetické bezpečnosti, umožňuje cílenou optimalizaci bezpečnostních opatření a poskytuje manažerům kybernetické bezpečnosti důležitý nástroj pro strategické řízení bezpečnosti.

3.4.2 Sběr důkazů a dokumentace

Sběr důkazů představuje klíčovou fází auditního procesu, která zajišťuje objektivitu a opakovatelnost výsledků auditu. Pro kvalitní posouzení vyspělosti informační podpory kybernetické bezpečnosti musí být sběr důkazů proveden systematicky, transparentně a v souladu s ověřenými standardy a metodikami. Dle doporučení COBIT 5 a ISO/IEC 27001 zahrnuje auditní proces kombinaci více metod získávání důkazů, které zajišťují komplexní pohled na stav řízení kybernetické bezpečnosti v organizaci [3], [14], [16]:

- analýza dokumentace (interní bezpečnostní politiky, procedury, výsledky auditů, reporty incidentů);
- rozhovory s odpovědnými pracovníky (ISO/CISO, manažeři IT a rizik);
- přezkum konfigurace používaných bezpečnostních technologií (např. SIEM, SOAR);
- pozorování implementace bezpečnostních procesů přímo v praxi;
- dotazníkové šetření (ověření vnímání úrovně bezpečnosti mezi zaměstnanci).

Získané důkazy je nutné dokumentovat jasným a transparentním způsobem. Doporučuje se vytvoření centrálního repozitáře dokumentace (např. SharePoint nebo Confluence), který umožní snadnou dostupnost dokumentů pro opakované audity, transparentní prezentaci výsledků a jejich průběžnou aktualizaci [14], [16].

Při sběru a dokumentaci důkazů je klíčové zajistit jejich platnost, relevanci a spolehlivost, aby auditní závěry byly objektivní a využitelné pro další rozhodování a zlepšování systému informační podpory kybernetické bezpečnosti [16].

3.4.3 Vyhodnocení výsledků a doporučení

Vyhodnocení výsledků auditu představuje závěrečnou fázi auditního procesu, během které dochází k analýze získaných důkazů a interpretaci zjištění s ohledem na kritéria definovaná v navrženém maturity modelu. Vyhodnocení musí být objektivní, jasné a zaměřené na identifikaci jak silných stránek, tak oblastí, které vyžadují další zlepšení. Výsledkem vyhodnocení je stanovení konkrétní úrovně vyspělosti organizace v každé posuzované doméně a formulace doporučení, která umožní dosažení vyšších úrovní vyspělosti [1], [14], [16].

Při vyhodnocování výsledků je doporučeno provést následující kroky:

- shrnutí zjištěných výsledků a důkazů podle jednotlivých domén a kritérií;
- objektivní přiřazení dosažených úrovní vyspělosti (Tierů) pro každou doménu maturity modelu;
- identifikace slabých míst a oblastí s nízkou úrovní zralosti, které vyžadují prioritní pozornost;
- návrh konkrétních doporučení a opatření ke zlepšení stavu bezpečnosti a zvýšení úrovně zralosti v jednotlivých doménách;
- formulace krátkodobých i dlouhodobých cílů, včetně realistického časového rámce pro jejich dosažení.

Stanovení výsledného skóre zralosti

Kvantifikace úrovně vyspělosti organizace je klíčovým prvkem vyhodnocení výsledků auditu. Výsledné skóre zralosti se stanovuje na základě dosažené úrovně vyspělosti (Tier) v jednotlivých doménách maturity modelu. Existuje několik přístupů ke stanovení celkového skóre:

- **Metoda průměru** – Výsledné skóre je vypočítáno jako průměr úrovní vyspělosti napříč všemi doménami.
- **Metoda nejnižší úrovně** – Celková úroveň vyspělosti odpovídá doméně s nejnižším dosaženým Tierem.
- **Metoda váženého skóre** – Každá doména je ohodnocena váhou podle její důležitosti pro organizaci, výsledné skóre se pak vypočítává váženým průměrem.

Výběr konkrétní metody závisí na strategii organizace a na jejím přístupu k řízení bezpečnosti. Doporučuje se metoda váženého skóre, která umožňuje zohlednit rozdílnou důležitost jednotlivých oblastí pro organizaci [3], [14].

Výsledné skóre zralosti slouží jako klíčový ukazatel pro plánování dalšího rozvoje kybernetické bezpečnosti v organizaci. Zajišťuje systematické sledování pokroku a umožňuje efektivní měření účinnosti zavedených opatření v čase [16].

Shrnutí:

Navržený maturity model umožňuje strukturovaně hodnotit úroveň informační podpory ISO/CISO v pěti klíčových doménách. Díky čtyřem úrovním vyspělosti a metodice hodnocení představuje praktický nástroj pro plánování rozvoje bezpečnostních procesů. V další kapitole bude model aplikován na případové studii banky FinCore a.s., kde bude ověřena jeho použitelnost v praxi.

4 POSOUZENÍ MODELU NA PŘÍKLADU SPOLEČNOSTI FINCORE BANK A.S.

Tato kapitola se zaměřuje na praktické ověření navrženého modelu informační podpory na příkladu fiktivní bankovní instituce FinCore Bank a.s.

4.1 Charakteristika společnosti FinCore Bank a.s.

Tabulka 8: Základní charakteristika společnosti FinCore Bank a.s.

Oblast	Popis
Název organizace	FinCore Bank a.s.
Typ	Středně velká komerční banka s orientací na retail a SME sektor
Počet zaměstnanců	Přibližně 200, z toho cca 20 v IT a kyberbezpečnosti
Pobočková síť	Centrála v Praze, 10 regionálních poboček
IT infrastruktura	Hybridní prostředí: on-premise datové centrum (Praha) a cloud (Microsoft Azure + SaaS služby pro HR a reporting)
Bezpečnostní struktura	ISO/CISO v jedné osobě, podporován 2 interními specialisty a externím SOC pro L1 detekci a DLP monitoring
Regulační rámce	Společnost je subjektem pod dohledem ČNB a musí plnit požadavky dle NIS2, DORA, ZKB, GDPR a PCI DSS
Certifikace	Certifikace ISO/IEC 27001 (auditována ročně), řízení rizik dle ISO/IEC 27005
Governance	ISO/CISO reportuje měsíčně CIO a je členem risk governance boardu. Bezpečnostní politika je schvalována vedením a pravidelně revidována.
Monitoring a reporting	SIEM (Splunk) pokrývá hlavní systémy a je napojen na ticketing a dashboardy. Reporting je formalizovaný a probíhá pravidelně vůči vedení i regulátorům.
Incident management	Existuje formální proces řízení incidentů, ale reakční doby a SLA nejsou měřeny. Automatizace probíhá částečně – SOAR je ve fázi testování.
Řízení rizik	Organizace má formalizovaný rámec, rizika jsou hodnocena kvartálně a prezentována vedení. Existují akční plány a klasifikace dopadů.
Řízení aktiv	Evidence v CMDB pokrývá fyzická a většinu logických aktiv. Klasifikace je dostupná jen pro vybrané typy, opatření nejsou systematicky navázána na klasifikaci.
Compliance a kultura bezpečnosti	Soulad s NIS2 a DORA je řízen projektově. Probíhá interní audit a vzdělávací kampaně (např. phishing simulace). Bezpečnostní kultura je podporována vedením a zahrnuta do strategického rozhodování.

(zdroj: vlastní zpracování)

4.2 Maturity model informační podpory – FinCore Bank a.s.

Na základě navrženého maturity modelu byla provedena podrobná analýza úrovně informační podpory kybernetické bezpečnosti ve společnosti FinCore Bank a.s. Hodnocení pokrývá pět klíčových domén, které jsou zásadní pro efektivní řízení bezpečnosti v roli ISO/CISO. Každá doména byla rozdělena do pěti hodnocených oblastí, jejichž vyspělost byla posuzována podle čtyřstupňové škály Tier (1–4), přičemž celkové hodnocení domény odpovídá nejnižší hodnotě v rámci dané oblasti.

Cílem hodnocení bude ověřit, nakolik je informační podpora ve FinCore Bank a.s. schopna naplňovat potřeby bezpečnostního managementu v kontextu řízení rizik, incidentů, souladu s regulacemi a technické bezpečnosti. Hodnocení bylo prováděno s využitím rámce COBIT 5 a v návaznosti na požadavky standardů ISO/IEC 27001, ISO/IEC 27005, směrnice NIS2 a nařízení DORA.

4.2.1 Bezpečnostní monitoring a reporting

Tabulka 9: Hodnocení domény Bezpečnostní monitoring a reporting

Hodnocená oblast	Tier	Hodnocení
Monitoring bezpečnostních událostí	3	Monitoring je pokročilý, SIEM je napojen na všechna kritická aktiva včetně poboček. Chybí však behaviorální detekce a pokrytí SaaS služeb.
Využití SIEM a dashboardů	3	Existují oddělené dashboardy pro bezpečnostní tým a management, napojené na ticketing. Chybí však plná automatizace mezi nimi.
Reporting vedení	3	ISO pravidelně předkládá měsíční reporty s přehledy incidentů a trendů. Vedení má možnost doplňujících analýz na vyžádání.
Reporting regulatorům	3	Hlášení incidentů probíhá podle ZKB a NIS2. Postupy jsou dokumentované, ale validace procesu v zátěži dosud neproběhla.
Kvalita zaznamenaných dat	3	Většina systémů loguje a NTP synchronizace je nastavena centrálně. Existuje pravidelná kontrola integrity logů.

(zdroj: vlastní zpracování dle [14])

Výsledný **Tier: 3**

4.2.2 Řízení bezpečnostních incidentů a automatizace reakcí

Tabulka 10: Hodnocení domény Řízení bezpečnostních incidentů a automatizace reakcí

Hodnocená oblast	Tier	Hodnocení
Incident response proces	3	Proces řízení incidentů je formalizovaný, zahrnuje klasifikaci, evidenci i eskalaci.
Automatizace detekce a reakce (SOAR)	2	Nasazení SOAR probíhá, ale reálná integrace do provozu je zatím jen částečná.
Evidence a klasifikace incidentů	3	Incidenty jsou evidovány v centralizovaném systému, klasifikace je standardizovaná.
Reakční časy a eskalace	2	SLA jsou interně stanoveny, ale nejsou vždy měřeny. Eskalace je závislá na ručním zásahu.
Lessons learned	3	Probíhají pravidelné retrospektivy po vážnějších incidentech, výstupy se ukládají a sdílejí.

(zdroj: vlastní zpracování dle [14])

Výsledný **Tier: 2**

4.2.3 Řízení rizik

Tabulka 11: Hodnocení domény Řízení rizik

Hodnocená oblast	Tier	Hodnocení
Rámec řízení rizik	3	Banka používá rámec dle ISO/IEC 27005. Rizika se hodnotí čtvrtletně, zapojení stakeholderů je standardní.
Identifikace rizik	3	Proces zahrnuje workshopy s vlastníky aktiv a využití zkušeností z auditů a incidentů.
Dopad a pravděpodobnost	3	Používá se validovaná riziková matice. Dopady jsou kvantifikovány dle business dopadu a reputace.
Akční plány	3	Každé významné riziko má přiřazený plán opatření s termíny a vlastníkem.
Integrace do řízení	3	Rizika jsou prezentována na risk committee. Výsledky ovlivňují strategické plánování i rozpočet.

(zdroj: vlastní zpracování dle [14])

Výsledný **Tier: 3**

4.2.4 Řízení aktiv

Tabulka 12: Hodnocení domény Řízení aktiv

Hodnocená oblast	Tier	Hodnocení
Evidence aktiv	3	CMDB je pravidelně aktualizována a propojena s HR, onboardingem i bezpečnostními politikami.
Klasifikace a hodnota aktiv	2	Klasifikace existuje jen pro vybrané typy aktiv, ne pro všechna data. Hodnota aktiv není kvantifikována.
Vlastnictví aktiv	3	Každé aktivum má vlastníka uvedeného v CMDB. Dochází k přezkumu při personálních změnách.
Ochranná opatření dle klasifikace	2	Opatření nejsou přímo navázána na klasifikaci. Dochází k přístupům „one size fits all“.
Revize evidence	3	Pololetní revize probíhá na základě výstupů z auditu a projektových změn.

(zdroj: vlastní zpracování dle [14])

Výsledný **Tier: 2**

4.2.5 Governance a compliance

Tabulka 13: Hodnocení domény Governance a compliance

Hodnocená oblast	Tier	Hodnocení
Role a odpovědnosti ISO/CISO	3	Role je vymezena, ISO má mandát, ale nemá dedikovaný tým ani zástup.
Politiky a směrnice	3	Politiky jsou udržovány, schvalovány vedením a přezkoumávány minimálně jednou ročně.
Interní audit a kontrola	3	Každoročně probíhá audit kybernetické bezpečnosti, jeho výstupy jsou použity pro revizi procesů.
Compliance s NIS2/DORA	3	Organizace má projektový plán souladu, jednotlivé úkoly jsou přiřazeny a termínované.
Kultura a řízení bezpečnosti	4	Bezpečnostní kultura je podporována vedením. Probíhají phishing testy, gamifikované školení a aktivní komunikace. ISO má přímý přístup na strategické poradní orgány banky.

(zdroj: vlastní zpracování dle [14])

Výsledný **Tier: 3**

Shrnutí:

Tabulka 14: Souhrn vyspělosti jednotlivých domén maturity modelu

Doména	Tier	Poznámka
Bezpečnostní monitoring a reporting	3	Formalizované procesy, standardní pokrytí, solidní reporting
Řízení incidentů a automatizace	2	SOAR a reakční časy zatím neplní standard Tier 3
Řízení rizik	3	Všechny procesy formalizované, integrovány do řízení
Řízení aktiv	2	Klasifikace a kontrolní vazby nejsou systematické
Governance a compliance	3	Silná bezpečnostní kultura (obsahuje oblast Tier 4)

(zdroj: vlastní zpracování dle [14])

Z výsledků maturity modelu vyplývá, že domény „Řízení incidentů“ a „Řízení aktiv“ dosahují úrovně Tier 2, což ukazuje na dílčí slabiny. Mezi hlavní nedostatky patří částečně zavedená automatizace reakcí (SOAR), nedefinované míry reakčních dob a slabá provázanost klasifikace aktiv s jejich ochranou. Přesto i v těchto oblastech existují procesy na vyšší úrovni, které tvoří základ pro další zlepšení.

Pozornost si zaslouží i oblast bezpečnostní kultury, která dosahuje úrovně Tier 4. Tato vyspělost reflektuje silnou podporu ze strany vedení, aktivní vzdělávání uživatelů a integraci bezpečnostního povědomí do řízení. Jde o výraznou přednost, která může sloužit jako vzor pro další oblasti.

Celkově lze konstatovat, že společnost FinCore Bank a.s. má pevně nastavené procesy informační podpory kybernetické bezpečnosti, zejména v doménách na úrovni Tier 3. Iniciativy zaměřené na posílení slabších míst mohou významně přispět ke zvýšení celkové odolnosti a efektivity bezpečnostního řízení.

4.3 Návrh zlepšení pro zvýšení vyspělosti

Z provedeného hodnocení vyspělosti systému informační podpory kybernetické bezpečnosti ve FinCore Bank a.s. vyplynulo, že některé oblasti dosahují pouze úrovně Tier 2, zatímco většina ostatních je hodnocena jako Tier 3. Cílem této kapitoly je navrhnout konkrétní opatření, která povedou ke zvýšení zralosti v oblastech s nižším hodnocením, a dále identifikovat vysoce rozvinuté oblasti, kde je možné uvažovat o přechodu na úroveň Tier 4. Návrhy zohledňují nejen požadavky na procesní řízení a technickou infrastrukturu, ale také

standards jako ISO/IEC 27001, NIST CSF 2.0 a rámce COBIT 5, které sloužily jako základ pro návrh maturity modelu.

4.3.1 doporučená opatření pro posun z Tier 2 na Tier 3 v oblastech s nižší úrovní

Cílem této podkapitoly je navrhnout konkrétní kroky vedoucí ke zvýšení vyspělosti informační podpory kybernetické bezpečnosti ve FinCore Bank a.s. v těch oblastech, které byly v rámci maturity modelu hodnoceny jako Tier 2. Posun na úroveň Tier 3 podle logiky modelu COBIT 5 znamená přechod od základní schopnosti řídit procesy k jejich standardizaci, formalizaci, vyhodnocování a částečné automatizaci [14].

1) Řízení bezpečnostních incidentů a automatizace reakcí

Na úrovni Tier 2 bývají procesy incident response založeny na základních postupech, často bez formalizovaných playbooků a měr. Pro dosažení úrovně Tier 3 je nezbytné zlepšit koordinaci, dokumentaci i automatizaci činností:

- **Zavedení nástroje typu SOAR (Security Orchestration, Automation and Response):** Integrace SOAR umožňuje provázat detekci incidentů, eskalační postupy a automatické reakce (např. izolaci koncových bodů, blokaci IP adres). Implementace tohoto typu řešení je doporučována i v rámci moderních rámců jako NIST CSF 2.0 a ISO/IEC 27035 [1][16].
- **Standardizace pomocí incident response playbooků:** Každý typ incidentu (phishing, malware, insider threat) by měl mít formálně popsany reakční scénář. Tyto tzv. "runbooks" zvyšují konzistenci reakcí a snižují závislost na konkrétních pracovnících [3].
- **Zavedení ukazatelů pro řízení výkonu:** Doporučuje se sledovat bezpečnostní ukazatele jako Mean Time To Detect (MTTD), Mean Time To Respond (MTTR) a počet uzavřených incidentů v definovaném SLA. Tyto ukazatele slouží jako Key Risk Indicators (KRIs) [5].
- **Systém lessons learned:** Každý vážnější incident by měl být vyhodnocen z pohledu příčin a preventivních opatření. Závěry by měly být promítnuty do aktualizace dokumentace i školení týmu [18].

- **Provádění simulačních cvičení ("tabletop exercises"):** Pravidelné testování reakce týmu na modelové scénáře napomáhá připravenosti. NIST i ISO doporučují tuto praxi jako součást kontinuálního zlepšování schopnosti reakce [1][21].

2) Řízení aktiv

Efektivní řízení aktiv je klíčové pro ochranu citlivých informací a infrastruktury. Posun z Tier 2 na Tier 3 zahrnuje zejména systematickou evidenci, klasifikaci a přiřazení odpovědností:

- **Rozšíření centrální evidence aktiv (CMDB):** Všechna relevantní aktiva, včetně dat, systémů, zařízení i cloudových služeb, musí být evidována a pravidelně aktualizována. Správa aktiv v CMDB je považována za základní stavební kámen ISMS podle ISO/IEC 27001 a 27005 [16][21].
- **Klasifikace aktiv podle CIA triády (důvěrnost, integrita, dostupnost):** ISO/IEC 27005 zdůrazňuje, že klasifikace aktiv podle dopadů na tyto atributy umožňuje efektivní řízení rizik [21].
- **Zavedení odpovědnosti vlastníků aktiv:** Každé aktivum musí mít určeného vlastníka, který nese odpovědnost za jeho ochranu, změnové řízení a rozhodování o přístupu. Tato odpovědnost je výslovně uvedena i ve směrnici NIS2 [4].
- **Provázání klasifikace s kontrolními opatřeními:** Klasifikace musí být propojena s konkrétními bezpečnostními opatřeními (např. šifrováním, DLP, SIEM korelací). Tento přístup je doporučen v rámci ISO/IEC 27002 [17].
- **Provádění pravidelných revizí a interních auditů:** Organizace by měla alespoň jednou ročně revidovat evidenci aktiv a vyhodnotit, zda jsou ochranná opatření adekvátní jejich klasifikaci. Tato praxe je běžnou součástí řízení bezpečnostních opatření dle COBIT 5 i ISO/IEC 27001 [14][16].

Přechod z Tier 2 na Tier 3 tedy vyžaduje nejen technologické nástroje, ale především rozvoj formalizovaných procesů, přehledných odpovědností, jasně definovaných měř a systémových vazeb mezi identifikovanými riziky a realizovanými opatřeními. Cílem není pouze zlepšit dokumentaci, ale především zvýšit předvídatelnost, efektivitu a robustnost informační podpory kybernetické bezpečnosti.

4.3.2 Specifická opatření pro případný posun do úrovně Tier 4 v klíčových oblastech

Přestože cílovým stavem maturity modelu ve FinCore Bank a.s. je dosažení úrovně Tier 3 jako standardní úrovně vyspělosti, v několika vybraných oblastech lze uvažovat o postupném přechodu na úroveň Tier 4. Tato nejvyšší úroveň vyžaduje nejen formalizaci a měřitelnost procesů, ale i jejich **proaktivní optimalizaci**, využití pokročilých nástrojů a **evidence-based přístup** k řízení bezpečnosti. V této podkapitole jsou navržena specifická opatření pro ty oblasti, kde existuje organizační připravenost, kapacitní zázemí a technologické předpoklady pro tento další vývoj.

Bezpečnostní monitoring a reporting

- **Zavedení behaviorální analýzy pomocí AI/ML:** Moderní systémy detekce anomálií využívající strojové učení umožňují včasné odhalení neobvyklého chování v síti či na koncových bodech bez nutnosti pevně definovaných signatur. Tento přístup doporučuje i NIST CSF 2.0 v rámci domény *Detect (DE)* jako způsob zvyšování kybernetické odolnosti [1].
- **Korelace logů napříč hybridní infrastrukturou:** Pro dosažení vyšší úrovně Tier je nutné mít schopnost integrované analýzy dat z on-premise systémů, cloudových služeb i mobilních zařízení. Pokročilé SIEM platformy by měly být rozšířeny o konektory a korelační pravidla pokrývající celou infrastrukturu [3][19].
- **Automatizace reportingu směrem k vrcholovému vedení:** V Tier 4 se očekává, že reporting je nejen přesný a pravidelný, ale také přizpůsobený cílové skupině (např. představenstvu) včetně trendových analýz, predikcí a rizikových scénářů [5].

Řízení rizik

- **Pokročilé kvantitativní hodnocení rizik (např. metody FAIR, Monte Carlo simulace):** V prostředí s vysokou mírou nejistoty je vhodné uvažovat o rozšíření klasických kvalitativních metod o kvantitativní přístup. NIST SP 800-30 tento přístup výslovně doporučuje jako prostředek k lepší prioritizaci investic do bezpečnosti [18].
- **Automatizace sběru a aktualizace vstupních dat o rizicích:** Systém řízení rizik by měl být propojen s dalšími systémy organizace – např. s

helpdeskovým systémem, CMDB nebo SIEM – a automaticky aktualizovat pravděpodobnosti výskytu hrozeb na základě reálných dat [21].

- **Zavedení rizikových ukazatelů (Key Risk Indicators, KRIs):** Organizace by měla pracovat s dynamickými ukazateli, které upozorňují na vznikající rizika (např. počet neaktualizovaných systémů, změny v topologii sítě, chybné konfigurace) [5][17].

Governance a compliance

- **Integrace cyber risk managementu do celopodnikového řízení rizik (ERM):** Namísto izolovaného řízení IT rizik je nutné, aby byla kybernetická rizika součástí jednotné ERM struktury. ISO/IEC 27005 i COBIT 5 doporučují tento přístup k zajištění sladění s obchodními cíli organizace [21][14].
- **Proaktivní compliance assurance (tzv. continuous compliance monitoring):** V oblasti finančního sektoru je klíčové, aby byla zajištěna trvalá shoda s požadavky nařízení DORA, NIS2 a GDPR. Pro aktivní dohled je možné využít nástroje typu GRC (Governance, Risk and Compliance), které umožňují průběžnou validaci souladu a reporting odchylek [12][4].
- **Zavedení ukazatelů pro měření efektivity compliance programů:** Ukazatele jako "compliance coverage", "policy violation rate" nebo "time to remediation" umožňují objektivní hodnocení vyspělosti řízení souladu s legislativou [3][14].

Dosažení úrovně Tier 4 vyžaduje nejen pokročilé technologie, ale především **zralé procesy, efektivní leadership a kulturu kontinuálního zlepšování**. Tato úroveň je určena pro organizace, které bezpečnost vnímají jako strategický nástroj k ochraně důvěry, konkurenceschopnosti a obchodní kontinuity.

4.3.3 Prioritizace opatření s ohledem na významnost a efektivitu

Vzhledem k omezeným zdrojům – lidským, finančním i technologickým – je nezbytné u každého z navržených opatření zvážit, **v jakém pořadí a s jakou důležitostí** má být implementováno. V této části je proto provedeno doporučení prioritizace opatření s ohledem na jejich **vliv na kybernetickou odolnost** organizace a **nákladovou efektivitu** jejich zavedení. Tato prioritizace zároveň zohledňuje logiku samotného maturity modelu – tzn. že **hlavním cílem je dosažení cílové úrovně Tier 3**, přičemž posun na Tier 4 je vnímán jako rozvojový, nikoli kritický.

Přechod mezi jednotlivými úrovněmi Tier v maturity modelu je založen na principu postupného rozvoje vyspělosti procesů a schopností organizace. Nižší úroveň (např. Tier 2) zpravidla představuje částečně definované nebo ad-hoc přístupy, zatímco vyšší úroveň (např. Tier 3) odpovídá standardizovanému, měřenému a řízenému způsobu řízení bezpečnosti. Tento přístup vychází z osvědčených metodik jako je CMMI a COBIT 5 a je široce aplikován v oblasti řízení kybernetické bezpečnosti. [14], [20].

A) Metodika stanovení priorit

Při návrhu priorit je důležité rozlišovat:

- **Kritická opatření (vysoká priorita):** Jedná se o opatření ve všech oblastech, které dosud nedosahují cílové úrovně Tier 3 (tedy nyní jsou na Tier 2). Tato opatření mají přímý vliv na základní zralost procesů a často i na regulační shodu (např. incident response, řízení aktiv). Jejich neimplementace může představovat riziko pro celou organizaci.
- **Pokročilá opatření (střední priorita):** Opatření směřující z Tier 3 na Tier 4 jsou považována za rozvojová. Mívají vyšší nároky na zdroje, změnu kultury či technologií. Priorita těchto kroků je podmíněna dostupností kapacit a měnícími se hrozbami, případně regulačními požadavky.
- **Nízká priorita:** Opatření, která mají malý dopad, nízkou efektivitu nebo řeší oblasti mimo klíčové procesy, nejsou v této fázi doporučena k realizaci.

B) Doporučená matice priorit

Oblast	Opatření	Výchozí Tier	Cílový Tier	Doporučená priorita
Řízení incidentů	Zavedení SOAR nástroje a standardizovaných playbooků	Tier 2	Tier 3	Vysoká
Řízení aktiv	Zavedení odpovědnosti vlastníků a klasifikace	Tier 2	Tier 3	Vysoká
Governance a compliance	Continuous compliance monitoring	Tier 3	Tier 4	Střední
Monitoring a reporting	Korelace logů, behaviorální analýza	Tier 3	Tier 4	Střední
Řízení rizik	Automatizace vstupních dat, kvantitativní modely	Tier 3	Tier 4	Střední

Tabulka 15: Prioritizace doporučených opatření dle výchozí a cílové úrovně vyspělosti (Tier) (zdroj: vlastní zpracování).

C) Shrnutí a doporučení pro FinCore Bank a.s.

Z výše uvedeného přehledu vyplývá, že prioritně by se organizace měla zaměřit na:

- **Řízení bezpečnostních incidentů** – absence automatizace a měřitelných SLA představuje významné riziko. Zavedení nástroje typu SOAR spolu se standardizovanými playbooky přinese výrazné zlepšení reakční schopnosti.
- **Řízení aktiv** – neexistující plná klasifikace a nejasně definovaná odpovědnost vlastníků aktiv ztěžují zavádění efektivních ochranných opatření. Přechod na Tier 3 zde představuje klíčový předpoklad pro řízení bezpečnostních rizik.

Naopak opatření směřující k úrovni Tier 4 (např. pokročilý monitoring, kvantitativní řízení rizik) mohou být realizována postupně, až po stabilizaci základních procesů a posílení kapacit.

4.4 Plán implementace zlepšení

Zvýšení úrovně vyspělosti systému informační podpory kybernetické bezpečnosti ve FinCore Bank a.s. vyžaduje nejen návrh konkrétních opatření, ale také jejich **systematickou implementaci** v čase. Tato kapitola navrhuje **realistický harmonogram, určení odpovědností a potřebné zdroje** pro postupné zavádění doporučených zlepšení, včetně návaznosti na priority stanovené v předchozí části. Cílem je zajistit dosažení cílové úrovně maturity modelu (min. Tier 3 ve všech oblastech) v časově zvládnutelném a organizačně udržitelném rámci.

4.4.1 Časový harmonogram implementace opatření

Implementace navržených opatření bude ve FinCore Bank a.s. probíhat ve čtyřech fázích během dvou let. Plán reflektuje reálné časové možnosti a logické návaznosti mezi jednotlivými aktivitami. Klíčová pozornost je věnována oblastem hodnoceným jako Tier 2, jejichž zlepšení má nejvyšší prioritu.

V první fázi (měsíce 1–6) se organizace zaměří na zavedení klasifikace aktiv a určení jejich vlastníků. Současně proběhne školení týmu a mapování procesů řízení incidentů jako příprava pro budoucí nasazení SOAR.

Ve druhé fázi (měsíce 7–12) dojde k výběru a návrhu architektury SOAR systému, včetně tvorby prvních reakčních scénářů (playbooků). CMDB bude rozšířena a propojena s dalšími nástroji.

Třetí fáze (měsíce 13–18) zahrnuje testovací nasazení SOAR a zahájení korelace logů napříč infrastrukturou. V oblasti compliance bude zavedeno centralizované sledování souladu s politikami a regulacemi.

Ve čtvrté fázi (měsíce 19–24) bude SOAR systém nasazen do ostrého provozu. Zároveň bude zavedena automatizace sběru dat pro řízení rizik a příprava hodnotících ukazatelů pro pokročilé hodnocení vyspělosti v oblastech mířících k Tier 4.

Tabulka 16: Časový harmonogram implementace opatření ve FinCore Bank a.s.

Fáze	Období	Hlavní činnosti
I	Měsíce 1–6	Zavedení klasifikace aktiv a vlastnické odpovědnosti. Mapování procesů řízení incidentů. Školení týmu.
II	Měsíce 7–12	Výběr a návrh architektury SOAR. Tvorba pilotních playbooků. Rozšíření CMDB a integrace s nástroji.
III	Měsíce 13–18	Testování SOAR. Korelace logů napříč hybridní infrastrukturou. Zavedení compliance dashboardu.
IV	Měsíce 19–24	Nasazení SOAR do ostrého provozu. Automatizace sběru dat pro řízení rizik. Příprava hodnotících ukazatelů pro Tier 4.

(zdroj: vlastní zpracování)

Harmonogram je navržen tak, aby byl realistický a podporoval udržitelný rozvoj informační podpory kybernetické bezpečnosti

4.4.2 Stanovení odpovědnosti za realizaci jednotlivých opatření

Pro jasné rozdělení odpovědností mezi zapojené role v rámci implementace opatření byla zvolena metoda **RACI matice**, doporučovaná v rámci rámce **COBIT 5** [14]. Tento přístup umožňuje přehledně určit, kdo za daný krok nese odpovědnost, kdo rozhoduje, kdo spolupracuje a kdo má být informován. Použití RACI modelu je zároveň v souladu s požadavky normy **ISO/IEC 27001** na jednoznačné určení bezpečnostních rolí a odpovědností [16].

RACI matice odpovědností za realizaci opatření

V následující tabulce jsou uvedeny klíčové oblasti implementace zlepšení a přiřazeny odpovědnosti jednotlivým aktérům v souladu s RACI modelem podle COBIT 5 [14]. RACI označuje čtyři typy rolí:

R – Responsible (zodpovědný za provedení úkolu)

A – Accountable (celkově odpovědný za výsledek)

C – Consulted (konzultovaný, spolupracující)

I – Informed (informovaný)

Tabulka 17: RACI matice odpovědností za realizaci bezpečnostních opatření

Oblast	ISO/CISO	IT tým	Externí SOC	Risk Management	Interní audit	Top management
Klasifikace a správa aktiv	A	R	I	C	I	I
Návrh a výběr SOAR řešení	A	C	R	I	I	I
Tvorba incident response playbooků	A	C	R	I	I	I
Monitoring a korelace událostí	A	R	R	I	I	I
Compliance reporting a hodnotící ukazatele	A	R	C	C	I	I
Automatizace řízení rizik	A	R	C	R	I	I
Dohled nad implementací a reporting	A	I	I	I	C	R
Schválení rozpočtu a strategie bezpečnosti	I	I	I	I	I	A

(zdroj: vlastní zpracování dle [14])

Tato matice umožňuje jasné přiřazení odpovědností a podporuje transparentní řízení projektu v souladu s osvědčenými rámci řízení bezpečnosti informací. Zároveň zdůrazňuje **aktivní roli vedení organizace**, které podle ISO/IEC 27001 odpovídá za stanovení politiky, zajištění zdrojů a podporu kontinuálního zlepšování ISMS [16].

4.4.3 Potřebné zdroje (finanční, lidské, technické)

Úspěšná realizace navržených opatření vyžaduje nejen správně nastavené procesy a odpovědnosti, ale také odpovídající **personální, technické a finanční zajištění**. V této kapitole jsou identifikovány klíčové typy zdrojů potřebné pro dosažení cílové úrovně vyspělosti systému informační podpory ve FinCore Bank a.s.

Lidské zdroje

V oblasti lidských zdrojů je nezbytné zajistit především:

- dedikovanou kapacitu ISO/CISO, který bude řídit a koordinovat celý projekt implementace,

- součinnost interního IT týmu při správě aktiv, konfiguraci nástrojů a integraci systémů,
- spolupráci externího SOC poskytovatele, zejména pro tvorbu a testování playbooků, korelaci událostí a provoz SOAR systému,
- zapojení risk managementu při návrhu hodnotících ukazatelů a propojení řízení rizik s bezpečnostními opatřeními,
- a interní audit pro nezávislé ověřování průběhu implementace.

Dále je nutné počítat s časovými alokacemi pro školení zaměstnanců a zvyšování jejich bezpečnostního povědomí, především v souvislosti s novými procesy a nástroji.

Technické zdroje

Mezi hlavní technické požadavky patří:

- nástroj pro správu aktiv a konfiguraci CMDB (např. ServiceNow, GLPI, Jira Assets),
- SIEM řešení pro centralizovaný sběr a korelaci logů (již provozováno externím SOC),
- SOAR systém pro orchestraci incidentů (např. IBM QRadar SOAR, Splunk SOAR, Palo Alto Cortex XSOAR),
- nástroje pro správu rizik a compliance (např. GRC platforma nebo vlastní řešení integrované s ISMS),
- dostatečné výpočetní a úložné kapacity pro logování, analýzu a zálohování.

Implementace nových nástrojů vyžaduje také podporu ze strany infrastruktury, například možnost bezpečné integrace s Active Directory, VPN a cloudovými službami.

Finanční zdroje

Finanční náročnost projektu bude záviset především na:

- licencování a provozních nákladech zvoleného SOAR řešení a případných rozšíření SIEM,
- implementačních službách a integraci, která bude zajišťována částečně dodavatelsky,
- školení a rozvoji personálu, zejména u technických i netechnických uživatelů,
- a případné akvizici GRC nebo risk management nástroje, pokud nebude využito stávajícího řešení.

Vzhledem k rozsahu změn se doporučuje vytvořit samostatný rozpočet pro řízení informační podpory bezpečnosti, ideálně s víceroletým výhledem a možností průběžného vyhodnocování návratnosti a dopadů investic.

Všechny uvedené požadavky a návrhy vycházejí z rámce COBIT 5, který definuje řízení bezpečnosti IT včetně odpovědností, hodnotících ukazatelů a kapacitních potřeb [14], a dále z normy ISO/IEC 27001, která stanovuje povinnosti v oblasti vedení, zdrojů a plánování v rámci systému řízení bezpečnosti informací (ISMS) [16]. Doporučení týkající se externí spolupráce, školení a nástrojové podpory jsou formulována rovněž na základě odborné literatury v oblasti bezpečnostního managementu a auditu [3].

4.5 Validace navrženého modelu

Cílem této kapitoly je ověřit vhodnost a použitelnost navrženého modelu informační podpory kybernetické bezpečnosti. Validace probíhá jednak teoreticky – porovnáním s mezinárodními standardy a rámci, jednak prakticky – na příkladu modelové organizace FinCore Bank a.s.. V této části práce je hodnoceno, zda navržený rámec a maturity model odpovídají požadavkům klíčových norem a zda je jejich struktura uplatnitelná v praxi, zejména v prostředí regulované organizace ve finančním sektoru.

4.5.1 Teoretická validace vůči relevantním standardům

Pro ověření vhodnosti navrženého modelu informační podpory byla provedena srovnávací analýza s vybranými standardy a rámci, které jsou široce uznávány v oblasti kybernetické bezpečnosti a řízení informačních systémů. Cílem je zjistit, zda model pokrývá klíčové domény, procesy a principy doporučované těmito normami a zda je v souladu s osvědčenými postupy.

ISO/IEC 27001:2022

Norma ISO/IEC 27001 definuje požadavky na systém řízení bezpečnosti informací (ISMS) a klade důraz na řízené přístupy k identifikaci rizik, aplikaci bezpečnostních opatření a průběžné zlepšování. Navržený model reflektuje základní strukturu této normy, zejména:

- řízení aktiv a klasifikaci informací (kapitoly 5, 6 a příloha A normy),
- řízení bezpečnostních incidentů, včetně přípravy na reakce a sběru důkazů,
- systémové řízení rizik v souladu s požadavky na plánování a podpůrné procesy,

- odpovědnosti vedení a interního auditu, jak je popsáno v části Leadership a Operation.

Model dále vychází z návazných norem ISO/IEC 27002 (kontroly) a ISO/IEC 27005 (řízení rizik), čímž podporuje ucelený přístup k bezpečnostnímu managementu [16].

NIST Cybersecurity Framework (CSF) 2.0

Rámec NIST CSF 2.0 strukturuje kybernetickou bezpečnost do pěti hlavních domén: Identify, Protect, Detect, Respond, Recover. Nově je rámec rozšířen o funkci **Govern**, která zdůrazňuje potřebu strategického řízení kybernetické bezpečnosti na úrovni vedení organizace.

Navržený model informační podpory tuto logiku respektuje – jednotlivé domény maturity modelu lze jednoznačně přiřadit k těmto funkcím:

- **Identify** → řízení aktiv, klasifikace a řízení rizik,
- **Protect** → governance, compliance a kontrolní opatření,
- **Detect** → monitoring, logování, threat intelligence,
- **Respond** → řízení incidentů a SOAR integrace,
- **Recover** je částečně pokryt plánováním zlepšení a zpětnou vazbou v incident managementu.
- **Govern** → governance, compliance, role ISO/CISO, odpovědnost vedení, napojení na řízení rizik a plnění regulatorních požadavků, včetně sledování KPI a KRI.

Struktura modelu odpovídá organizačním i procesním požadavkům NIST CSF a umožňuje auditovatelné zhodnocení vyspělosti v každé oblasti [1].

COBIT 5

COBIT 5 je rámec pro řízení a správu IT procesů, který klade důraz na vazbu mezi IT a byznysem, přiřazení odpovědností (např. pomocí RACI), řízení výkonnosti a měření přidané hodnoty. Navržený model informační podpory ve FinCore Bank a.s. odpovídá těmto principům:

- jasně definuje procesní oblasti a jejich vyspělost (maturity model),
- přiděluje role a odpovědnosti napříč strukturou (viz RACI matice v kapitole 4.4.2),

- podporuje řízení na základě hodnotících ukazatelů, včetně KPI a KRI,
- a je v souladu s cílem dosažení efektivního řízení IT bezpečnosti jako součásti celkové hodnoty organizace [14].

CIS Controls v8

Kontrolní seznam CIS Controls (Center for Internet Security) poskytuje konkrétní bezpečnostní opatření (v současnosti 18), která organizacím pomáhají dosahovat odolnosti vůči hrozbám. Model informační podpory adresuje většinu z těchto oblastí, zejména:

- kontrola a správa aktiv (Control 1, 2),
- monitorování a detekci (Control 8, 17),
- řízení přístupů a identit (Control 5, 6),
- řízení bezpečnostních incidentů (Control 17),
- bezpečnostní školení a governance (Control 14, 16).

Přestože model neimplementuje CIS Controls přímo, jeho struktura je s nimi plně kompatibilní a může být dále rozšířena o konkrétní kontrolní mechanismy uvedené v CIS Controls [19].

Na základě uvedené srovnávací analýzy lze konstatovat, že navržený model informační podpory je v souladu s klíčovými mezinárodními standardy a rámci, reflektuje jejich základní principy a je schopen podporovat dosažení požadované úrovně kybernetické bezpečnosti ve středně velké regulované organizaci.

4.5.2 Zhodnocení vhodnosti modelu pro bankovní sektor (specifické regulační požadavky)

Bankovní sektor představuje vysoce regulované prostředí s přísnými požadavky na bezpečnost, kontinuitu služeb a prokazatelnost dodržování pravidel. Informační podpora kybernetické bezpečnosti v tomto sektoru musí reflektovat nejen obecně uznávané rámce, ale i specifické regulační požadavky na finanční instituce. Cílem této kapitoly je posoudit, zda navržený model informační podpory odpovídá těmto požadavkům a je vhodně použitelný v prostředí středně velké banky, jakou je FinCore Bank a.s.

Soulad s evropskou a českou legislativou

Navržený model podporuje naplnění klíčových požadavků vybraných regulačních rámců:

- **Směrnice NIS2 (EU 2022/2555):** model je v souladu s požadavky na řízení rizik, odpovědnost vedení, schopnost reakce na incidenty a pravidelný reporting. Domény modelu jako řízení aktiv, incident response, governance a auditovatelnost opatření pokrývají požadavky uvedené v člancích 21–23 směrnice [4].
- **Nařízení DORA (EU 2022/2554):** v oblasti digitální odolnosti finančních institucí DORA vyžaduje technické i organizační zabezpečení, testování, dohled nad třetími stranami a řízení provozních rizik. Model informační podpory zahrnuje procesy, které odpovídají oblastem řízení rizik, monitoringu, governance a řízení aktiv, čímž podporuje naplnění požadavků nařízení [12].
- **Zákon o kybernetické bezpečnosti (č. 181/2014 Sb.):** model odpovídá zejména části týkající se organizačních opatření, bezpečnostní dokumentace, kontroly přístupů, detekce událostí a řízení bezpečnostních incidentů, jak je definováno v § 4–8 zákona a příslušných prováděcích vyhláškách [23].
- **Nařízení GDPR (EU 2016/679), zákon č.110/2019 Sb.:** prostřednictvím domén řízení aktiv, klasifikace informací a přidělení odpovědností umožňuje model plnění požadavků na zabezpečení zpracování osobních údajů dle článků 24 a 32 [16].

Soulad s PSD2 a PCI DSS

Specifikem bankovního sektoru je nutnost plnit i požadavky standardů souvisejících s platebními službami a zpracováním karetních údajů:

- **Směrnice PSD2 (EU 2015/2366)** ukládá poskytovatelům platebních služeb povinnost zajistit důvěrnost, integritu a dostupnost dat, implementaci silného ověřování klienta (SCA) a kontrolu přístupů třetích stran. Navržený model zahrnuje tyto aspekty zejména v doménách governance, řízení incidentů a přístupových práv, čímž umožňuje plnění článků 94–98 směrnice [24].
- **Standard PCI DSS v4.0 (Payment Card Industry Data Security Standard)** stanovuje konkrétní bezpečnostní požadavky pro organizace, které zpracovávají karetní údaje. Model informační podpory tyto požadavky adresuje především v oblastech logování, správy aktiv, řízení přístupů, segmentace sítí a monitoringu událostí, čímž přispívá k naplnění požadavků jednotlivých kapitol standardu [25].

Specifické potřeby finanční instituce

Model informační podpory zohledňuje rovněž charakteristické znaky finančních institucí, jako je:

- důraz na **auditovatelnost procesů a zpětnou dohledatelnost rozhodnutí**, což je klíčové z pohledu regulatorních kontrol a reputace,
- schopnost **přizpůsobení hybridní infrastruktury**, tedy kombinaci on-premise systémů, cloudových služeb a služeb třetích stran,
- **postupné zavádění** dle vyspělosti jednotlivých oblastí, což je praktické z hlediska řízení změn ve středně velké organizaci,
- a **přímá role vedení** při řízení bezpečnosti, včetně odpovědnosti za strategické rozhodování a dostupnost zdrojů, jak požadují jak NIS2, tak DORA.

Celkové zhodnocení

Na základě výše uvedených skutečností lze konstatovat, že navržený model informační podpory kybernetické bezpečnosti je vhodně navržen pro prostředí bankovního sektoru. Umožňuje řízené a auditovatelné zavádění bezpečnostních opatření v souladu s požadavky evropské i národní legislativy a reflektuje jak technické, tak organizační potřeby regulovaných subjektů.

4.6 Identifikace slabých stránek a omezení modelu

Ačkoli navržený model informační podpory nabízí komplexní a strukturovaný přístup ke zvýšení kybernetické odolnosti organizace, je nezbytné reflektovat i jeho možné slabiny a omezení. Tato kapitola se věnuje potenciálním problémům, které mohou nastat při jeho aplikaci v praxi, a kriticky hodnotí vlastnosti modelu z hlediska jeho obecné použitelnosti.

4.6.1 Analýza možných problémů při aplikaci modelu v praxi

Při nasazení modelu informační podpory do reálného provozu mohou organizace čelit následujícím výzvám:

- **Nedostatečné personální kapacity** – úspěšná realizace modelu vyžaduje aktivní zapojení interních rolí (ISO/CISO, IT, audit) a spolupráci s externími partnery. V organizacích s omezenými kapacitami nebo chybějícími zkušenostmi může být realizace výrazně zpomalena.

- **Odpor ke změnám a organizační kultura** – některá opatření (např. důsledná klasifikace aktiv, řízení přístupů, eskalace incidentů) mohou narážet na neformální zvyklosti a odpor zaměstnanců, zejména pokud nebyly dříve vyžadovány nebo měřeny.
- **Závislost na externích dodavatelích** – využití služeb externího SOC nebo cloudových nástrojů (SOAR, GRC) může být limitováno kvalitou služeb, SLA, dostupností integrací nebo bezpečností samotného poskytovatele.
- **Omezené finanční zdroje** – i při dobře navrženém plánu a dostupných technických řešeních může být realizace modelu zpomalena nebo pozastavena z důvodu nedostatečného rozpočtu. Nákup nástrojů, jejich integrace, školení zaměstnanců či externí konzultace představují významné výdaje. Zejména v menších organizacích nebo v prostředí s konzervativním přístupem k rozpočtování bezpečnosti může být finanční omezení zásadním faktorem ovlivňujícím úspěšnost implementace.
- **Nároky na řízení a koordinaci** – bez silné role bezpečnostního manažera a podpory top managementu může dojít ke ztrátě kontroly nad prioritami, termíny nebo kvalitou realizovaných opatření.
- **Fragmentace bezpečnostních systémů** – pokud organizace nemá jednotnou IT architekturu, může být složité zajistit centrální monitoring, správu přístupů nebo jednotnou evidenci aktiv.

4.6.2 Diskuse omezení navrženého modelu (např. dostupnost zdrojů, organizační kultura)

Kromě praktických obtíží je vhodné zvážit i obecná omezení samotného návrhu modelu:

- **Model není univerzální** – byl navržen pro prostředí středně velké banky s konkrétními technologickými a organizačními předpoklady. Jeho přímá aplikace v jiných typech organizací (např. průmysl, zdravotnictví, veřejná správa) by vyžadovala přizpůsobení domén, hodnotících ukazatelů a nástrojového vybavení.
- **Maturity model je zjednodušený** – navržený model pracuje se čtyřmi úrovněmi vyspělosti, což přináší přehlednost, ale zároveň může limitovat jemnější vyhodnocení některých aspektů (např. rozdíl mezi formalizovaným a optimalizovaným procesem).

- **Není zaměřen na technické detaily implementace** – cílem modelu je poskytnout rámec pro řízení informační podpory, nikoli definovat konkrétní bezpečnostní architekturu, síťové konfigurace nebo kryptografické standardy. Tyto aspekty by musely být řešeny samostatně.
- **Závislost na existenci kultury řízení bezpečnosti** – model předpokládá, že organizace již disponuje alespoň základním vědomím o významu bezpečnosti a má zavedené minimální procesy (např. ISMS, řízení přístupů). V prostředích, kde taková kultura není přítomna, může být zavádění modelu obtížné nebo neúčinné.

4.7 Návrh metodiky praktické validace modelu

K ověření skutečné použitelnosti navrženého modelu informační podpory je nezbytné provést jeho **praktickou validaci v reálném prostředí organizace**. Tato kapitola představuje návrh metodiky, která umožní systematicky ověřit funkčnost a přínosy jednotlivých částí modelu v běžném provozu. Cílem je získat objektivní zpětnou vazbu o účinnosti, efektivitě a aplikovatelnosti navrženého rámce a maturity modelu.

4.7.1 Popis metodiky ověření modelu v reálných podmínkách

Validace bude založena na kombinaci pozorování, strukturovaných rozhovorů, sběru dokumentace a analýzy praktických případů (use cases). Základní principy metodiky:

- Validace proběhne v rámci běžného provozu organizace (v tomto případě FinCore Bank a.s.), bez umělého zasahování do procesů.
- Hodnoceny budou jak procesní aspekty (např. existují formální odpovědnosti? jsou procesy dodržovány?), tak technické nástroje (např. je možné vyhodnotit KRI? probíhá korelace logů?).
- Validace bude mít kvalitativní i kvantitativní složku – posoudí se nejen funkčnost jednotlivých prvků, ale také jejich dopad na zlepšení bezpečnostního řízení.
- Hodnocení bude řízeno pomocí předem definovaného kontrolního seznamu (checklistu), odvozeného z jednotlivých domén maturity modelu.

Interní checklist pro validaci ve FinCore Bank a.s.:

Tabulka 18: Ukázkový interní checklist pro validaci informační podpory ve FinCore Bank a.s.

Doména	Ověřovací otázka	Výsledek (ano / ne / částečně)
Řízení aktiv	Jsou všechna kritická aktiva evidována v CMDB včetně klasifikace a vlastníka?	
	Je klasifikace aktiv provázána s technickými a organizačními opatřeními?	
Incident management	Existují aktuální a schválené playbooky pro nejběžnější typy incidentů?	
	Byly v posledních 6 měsících zaznamenány a vyhodnoceny reálné incidenty?	
Monitoring	Probíhá korelace bezpečnostních událostí mezi cloudem a on-premise infrastrukturou?	
	Jsou pravidelně vyhodnocována bezpečnostní KPI/KRI a předkládána vedení?	
Řízení rizik	Je k dispozici aktuální registr kybernetických rizik propojený s konkrétními aktivy a opatřeními?	
Governance & compliance	Existuje RACI matice nebo podobné formální přiřazení odpovědností?	
	Je zaveden mechanismus pravidelné interní revize vyspělosti v jednotlivých oblastech modelu?	

(zdroj: vlastní zpracování dle [1], [9], [2], [8], [14])

Vyplněním checklistu získá organizace přehled o tom, ve kterých oblastech dosahuje cílové úrovně vyspělosti, a kde je naopak nutné doplnit procesy, nástroje nebo odpovědnosti. Tento výstup může sloužit jako podklad pro gap analýzu, plán nápravných opatření a přehled pro vedení.

4.7.2 Navrhované scénáře a postupy testování

V rámci praktické validace navrženého modelu informační podpory se doporučuje ověření jeho funkčnosti pomocí předem definovaných **testovacích scénářů**, které simulují běžné provozní situace. Cílem těchto scénářů je **ověřit funkčnost procesů, připravenost nástrojů a reakci odpovědných osob**.

Každý scénář je strukturován tak, aby odpovídal jedné z domén modelu. Výstupem testování by měl být záznam o průběhu, zjištěné nedostatky a doporučení ke zlepšení.

Scénář 1 – Ověření klasifikace a správy aktiv

Doména: Řízení aktiv

Popis: Auditor vybere náhodné kritické aktivum (např. databázi klientských údajů) a ověří, zda:

- je evidováno v CMDB,
- má přiřazeného vlastníka,
- má klasifikaci (např. vysoká důvěrnost),
- jsou k němu navázána odpovídající ochranná opatření (např. šifrování, přístupová práva).

Cíl: Ověřit konzistenci evidence a provázanost klasifikace s bezpečnostními opatřeními.

Scénář 2 – Reakce na bezpečnostní incident

Doména: Incident management

Popis: Simulace bezpečnostního incidentu – např. detekce podezřelého e-mailu s phishingovým obsahem. SOC tým incident zachytí v SIEM a aktivuje příslušný playbook v SOAR. Cílem je sledovat:

- dobu detekce, eskalace a uzavření,
- zapojení odpovědných rolí dle playbooku,
- zdokumentování incidentu a závěrů (lessons learned).

Cíl: Ověřit připravenost na incident, kvalitu reakce a efektivitu koordinace.

Scénář 3 – Vyhodnocení bezpečnostních ukazatelů

Doména: Monitoring a reporting

Popis: Analytik vyhledá poslední měsíční přehled bezpečnostních ukazatelů (např. MTTR, počet zablokovaných pokusů o přístup, KRI změny v konfiguraci) a ověří, zda:

- jsou data aktuální a úplná,
- byly předány vedení (např. skrze dashboard nebo zprávu),
- byly na základě bezpečnostních ukazatelů přijaty konkrétní kroky.

Cíl: Ověřit efektivitu monitoringu a schopnost přetavit data do rozhodování.

Scénář 4 – Kontrola řízení rizik

Doména: Řízení rizik

Popis: Vybrané aktivum (např. internetová bankovní aplikace) je porovnáno s registrem rizik. Ověřuje se:

- zda je k aktivu přiřazeno relevantní riziko,
- jaká opatření byla definována a kdo je zodpovědný za jejich realizaci,
- kdy naposledy byla rizika aktualizována a kdo je přezkoumával.

Cíl: Ověřit provázanost aktiv a rizik, aktuálnost řízení a existenci odpovědností.

Scénář 5 – Ověření odpovědnosti a dohledatelnosti

Doména: Governance a compliance

Popis: Auditor vybere oblast (např. řízení přístupů) a ověří:

- zda jsou formálně definovány role a odpovědnosti (např. pomocí RACI),
- zda existují záznamy o rozhodnutích a schváleních v této oblasti,
- zda vedení má k dispozici aktuální přehled o stavu domény a případných slabinách.

Cíl: Ověřit funkčnost governance struktury a schopnost řídit model na strategické úrovni.

Každý scénář by měl být doplněn formulářem záznamu obsahujícím:

- identifikátor scénáře,
- doménu a testovaný proces,
- krokový popis testu,
- pozorování, výsledek (splněno / částečně / nesplněno),
- a doporučení pro zlepšení.

Výsledky testování tvoří podklad pro analytickou zprávu validace a následné rozhodování o úpravách, prioritách nebo plánu rozvoje modelu.

Navržené scénáře a metodika testování vycházejí z principů doporučených v rámci standardů ISO/IEC 27001 [16], NIST Cybersecurity Framework [1] a rámce COBIT 5 [14], avšak byly autorsky upraveny pro potřeby maturity modelu informační podpory.

4.7.3 Způsob sběru důkazů a jejich analýza

Na základě ověřovacích scénářů uvedených v předchozí části probíhá sběr důkazů, které slouží jako podklad pro objektivní vyhodnocení funkčnosti a vyspělosti jednotlivých oblastí modelu. Každý scénář (např. simulace incidentu, kontrola klasifikace aktiv nebo přezkum ukazatelů) generuje informace, které je nutné systematicky zaznamenat, vyhodnotit a propojit s cílovými úrovněmi maturity.

Cílem této fáze je **zhodnotit, nakolik byl navržený model informační podpory úspěšně aplikován v reálném provozu**, a identifikovat oblasti, které vyžadují úpravu, doplnění nebo zvýšenou pozornost.

Typy důkazů získané během testování

Při testování jsou shromažďovány různé typy důkazních materiálů:

- **Procesní dokumenty:** směrnice, playbooky, rozhodnutí, RACI matice, zápisy z jednání,
- **Technické výstupy:** záznamy z CMDB, SIEM, SOAR, logy, reporty, exporty z GRC nástrojů,
- **Formuláře a checklisty:** výstupy z validace scénářů a checklistových otázek,
- **Záznamy z pozorování a interview:** např. s vlastníky aktiv, analytiky SOC nebo vedením,
- **Hodnotící ukazatele a statistiky:** KPI (např. průměrná doba reakce), KRI, počet incidentů, zjištěná rizika.

Důležité je, aby všechny důkazy byly dohledatelné, auditovatelné a konzistentní s procesní dokumentací.

Vyhodnocení pomocí gap analýzy

Pro každou ověřovanou položku z checklistu nebo scénáře je následně provedeno hodnocení pomocí jednoduché gap analýzy, tedy porovnání:

- **očekávaného stavu** (např. plná klasifikace aktiv, existující incident playbook, sledování KRI),
- **s reálně pozorovaným stavem.**

Hodnocení probíhá pomocí tří kategorií:

- **Splněno** – požadavek je naplněn v plném rozsahu,

- **Částečně splněno** – některé prvky nebo procesy chybí, nejsou úplné nebo nejsou pravidelně vykonávány,
- **Nesplněno** – oblast není zavedena nebo není možné doložit její funkčnost.

Výsledky jsou zaznamenány do validačního formuláře a následně agregovány do přehledu, který umožní určit celkovou úroveň vyspělosti každé domény (např. řízení aktiv = Tier 2, incident response = Tier 3). Tento přehled slouží jako podklad pro rozhodování o zlepšení, investicích a prioritách dalšího rozvoje systému informační podpory.

Shrnutí:

Aplikace maturity modelu ve FinCore Bank a.s. ukázala jeho použitelnost v praxi a schopnost odhalit konkrétní slabiny v systému informační podpory. Na základě hodnocení byly navrženy cílené kroky vedoucí ke zvýšení úrovně vyspělosti, které respektují reálné možnosti organizace i regulatorní požadavky bankovního sektoru.

5 DISKUZE A ZÁVĚR

Závěrečná kapitola práce shrnuje hlavní přínosy navrženého modelu informační podpory kybernetické bezpečnosti, hodnotí jeho praktickou použitelnost a představuje prostor pro jeho další rozvoj. Zároveň nabízí kritické zhodnocení samotného přístupu, použitých metod i případných omezení, která se objevila v průběhu návrhu a validace modelu.

5.1 Shrnutí dosažených výsledků

Hlavním cílem diplomové práce bylo navrhnout komplexní model informační podpory pro manažera kybernetické bezpečnosti v organizaci, který by zahrnoval nástroje, procesy, odpovědnosti a metody hodnocení vyspělosti systému.

Tento cíl byl naplněn prostřednictvím následujících kroků:

1. V teoretické části byla provedena literární rešerše klíčových norem, rámců a legislativních požadavků (např. ISO/IEC 27001, NIST CSF 2.0, COBIT 5, NIS2, DORA, PCI DSS, PSD2), které tvoří základ pro navržený rámec informační podpory.
2. Na základě těchto vstupů byl sestaven strukturovaný rámec informační podpory, členěný do pěti hlavních domén: řízení aktiv, řízení incidentů, bezpečnostní monitoring, řízení rizik a governance & compliance.
3. Byl vytvořen maturity model, který rozlišuje čtyři úrovně vyspělosti (Tier 1–4) a umožňuje organizaci hodnotit aktuální stav, plánovat zlepšení a porovnávat se s cílovým stavem.
4. V praktické části byl model aplikován na fiktivní organizaci FinCore Bank a.s., čímž byla demonstrována použitelnost rámce v reálném kontextu středně velké regulované banky.
5. Proběhla teoretická i praktická validace modelu, včetně návrhu ověřovací metodiky, checklistu, testovacích scénářů a gap analýzy, která umožňuje řízené ověřování vyspělosti.

Výsledkem je ucelený návrh, který je v souladu s mezinárodními standardy, zohledňuje specifika bankovního sektoru a poskytuje praktické nástroje pro řízení, měření i zlepšování informační podpory v oblasti kybernetické bezpečnosti.

5.1.1 Vyhodnocení přínosu vytvořeného modelu

Navržený model přináší následující konkrétní přínosy:

- **Systémové uchopení informační podpory** – model nabízí strukturovaný rámec, který jasně vymezuje domény, odpovědnosti, nástroje a postupy potřebné pro roli ISO/CISO.
- **Možnost měření vyspělosti** – pomocí maturity modelu lze hodnotit aktuální stav a plánovat rozvoj bezpečnostních procesů v čase.
- **Soulad s regulacemi a normami** – rámec odpovídá požadavkům NIS2, DORA, PSD2, PCI DSS i ISO/IEC 27001, čímž usnadňuje řízení shody a přípravu na audit.
- **Podpora řízení a rozhodování** – Hodnotící ukazatele, KRI a KPI umožňují přenést výstupy modelu na úroveň vedení organizace a podpořit informované řízení rizik.
- **Uplatnitelnost v různých prostředích** – ačkoliv je model navržen pro bankovní sektor, jeho základní struktura je adaptovatelná i na jiné typy organizací.

Z těchto důvodů lze model považovat za **praktický nástroj**, který má přidanou hodnotu nejen pro bezpečnostního manažera, ale i pro vedení firmy a další zainteresované role.

5.2 Kritické zhodnocení

Přestože navržený model přináší systematický přístup k informační podpoře bezpečnostního řízení, je nutné reflektovat i jeho limity:

- **Model je navržen primárně pro prostředí středně velké banky** – jeho použití v jiném kontextu vyžaduje úpravy, např. v rozsahu domén, hloubce hodnotících ukazatelů nebo použitých nástrojích.
- **Maturity model je záměrně zjednodušený** – což podporuje srozumitelnost, ale omezuje granularitu vyhodnocení.
- **Praktická validace proběhla na fiktivní organizaci** – zatím bez nasazení v reálném prostředí, což znamená, že přínosy i překážky zavedení mohou být odlišné.

- Některé části modelu předpokládají existenci určitých nástrojů nebo procesů, např. CMDB, SOAR nebo GRC – což v některých organizacích nemusí být dostupné bez investic.

I přes uvedená omezení představuje navržený model **prakticky využitelný rámec**, který může sloužit jako vodítko pro ISO, CISO i vedení organizace při systematickém řízení kybernetické bezpečnosti a budování bezpečnostní kultury.

SEZNAM POUŽITÉ LITERATURY

- [1] PASCOE, Cherilyn; QUINN, Stephen a SCARFONE, Karen. The NIST Cybersecurity Framework (CSF) 2.0. Online. NIST Pubs. 2024, roč. 2024, č. NIST CSWP 29, s. 32. Dostupné z: <https://doi.org/10.6028/NIST.CSWP.29>.
- [2] KOLOUCH, Martin a BAŠTA, Martin. Kybernetická bezpečnost. Online. Praha: Univerzita obrany, 2021. ISBN 978-80-7582-079-2. Dostupné z: <https://www.unob.cz/cybersecurity.pdf>
- [3] BANOTH, Rajkumar; GUGULOTHU, Narsimha a GODISHALA, Aruna Kranthi. A Comprehensive Guide to Information Security Management and Audit. 2023. Boca Raton, Florida, USA: CRC Press, 2023. ISBN 9781003322191.
- [4] EVROPSKÝ PARLAMENT A RADA EVROPSKÉ 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). In: . Štrasburk, 2022. Dostupné také z: <https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32022L2555&qid=1724329129730>.
- [5] RABII, Anass; ASSOUL, Saliha; QUAZZANI TOUHAMI, Khadija a ROUDIES, Ounsa. Information and cyber security maturity models: a systematic literature review. Online. Information and cyber security. 2020, roč. 2020, č. Volume 28 4, s. 627-644. ISSN 2056-4961. Dostupné z: <https://doi.org/10.1108/ICS-03-2019-0039>.
- [6] YESHIVA UNIVERSITY. The Evolution of Cyber Threats. Katz School of Science and Health, 2024. Dostupné z: <https://online.yu.edu/katz/blog/the-evolution-of-cyber-threats>.
- [7] DATAGUARD. Information Security Officer vs. Chief Information Security Officer: Understanding the Differences. Online. DataGuard, 2024. Dostupné z: <https://www.dataguard.com/blog/information-security-officer-ciso>.
- [8] RADA EVROPSKÉ UNIE. Vývoj kybernetické bezpečnosti v EU: časová osa klíčových milníků. Online. Consilium.europa.eu, 2024. Dostupné z: <https://www.consilium.europa.eu/cs/policies/cybersecurity/timeline-cybersecurity/>.

- [9] MINIMÁLNÍ BEZPEČNOSTNÍ STANDARD: podpůrný materiál pro subjekty, které nespadají pod zákon o kybernetické bezpečnosti. Online. Brno: NAKIT, Ministerstvo vnitra české republiky, NÚKIB, 2023. Dostupné také z: https://nukib.gov.cz/download/publikace/podpurne_materialy/minimalni-bezpecnostni-standard_v1.2.pdf.
- [10] NGSS.cz. Umělá inteligence a kybernetická bezpečnost. Online. NGSS.cz, 2023. Dostupné z: <https://www.ngss.cz/clanek/umela-inteligence-a-kyberneticka-bezpecnost-2023-02-24>.
- [11] CDR.cz. Proč jsou dodavatelské řetězce nejslabším článkem? Online. CDR.cz, 2024. Dostupné z: <https://cdr.cz/clanek/kyberkoutek-proc-jsou-dodavatejske-retezce-nejslabsim-clankem>.
- [12] EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE. legislativní akt, NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2022/2554 ze dne 14. prosince 2022 o digitální provozní odolnosti finančního sektoru a o změně nařízení (ES) č. 1060/2009, (EU) č. 648/2012, (EU) č. 600/2014, (EU) č. 909/2014 a (EU) 2016/1011. Štrasburk, 2022. Dostupné také z: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32022R2554>.
- [13] NÁRODNÍ SOUSTAVA POVOLÁNÍ. Manažer kybernetické bezpečnosti. Online. NSP, 2024. Dostupné z: <https://nsp.cz/jednotka-prace/manazer-kyberneticke-bezp>.
- [14] ISACA. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. ISACA, 2012. Dostupné z: <https://www.isaca.org>.
- [15] ISO/IEC. ISO/IEC 27005:2018. Information Security Risk Management. ISO/IEC, 2018. Dostupné z: <https://www.karlancer.com/api/file/1683114859-CH6u.pdf>.
- [16] ISO/IEC. ISO/IEC 27001:2022. Information Security Management Systems – Requirements. ISO/IEC, 2022. Dostupné z: <https://itref.ir/uploads/editor/2ef522.pdf>.
- [17] ISO/IEC. ISO/IEC 27002:2022. Information Security Controls. ISO/IEC, 2022. Dostupné z: <https://itref.ir/uploads/editor/d3d149.pdf>.
- [18] PUTRA, A. P. a SOEWITO, B. Integrated Methodology for Information Security Risk Management using ISO 27005:2018 and NIST SP 800-30 for Insurance Sector. International Journal of Advanced Computer Science and Applications, 2023, roč. 14, č. 4. Dostupné z: <http://www.ijacsa.thesai.org>.

- [19] SPLUNK. CIS Critical Security Controls. Online. Splunk, 2024. Dostupné z: https://www.splunk.com/en_us/blog/learn/cis-critical-security-controls.html.
- [20] CIO. CMMI Explained. Online. CIO, 2024. Dostupné z: <https://www.cio.com/article/274530/cmmi-explained.html>.
- [21] ELASTIC. Elastic Security. Online. Elastic, 2024. Dostupné z: <https://www.elastic.co/what-is/elastic-security>.
- [22] PALO ALTO NETWORKS. Cortex XSOAR. Online. Palo Alto Networks, 2024. Dostupné z: <https://www.paloaltonetworks.com/cortex/xsoar>.
- [23] ČESKÁ REPUBLIKA. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. In: Sbírka zákonů České republiky. Dostupné z: <https://www.zakonyprolidi.cz/cs/2014-181>.
- [24] EVROPSKÁ UNIE. Směrnice Evropského parlamentu a Rady (EU) 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu (PSD2). Úřední věstník Evropské unie, L 337, 23. 12. 2015. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32015L2366>.
- [25] PCI SECURITY STANDARDS COUNCIL. Payment Card Industry Data Security Standard – Requirements and Security Assessment Procedures. Version 4.0. Wakefield, MA: PCI SSC, 2022. Dostupné z: <https://www.pcisecuritystandards.org/>.
- [26] EVROPSKÝ PARLAMENT A RADA EVROPSKÉ UNIE. Nařízení (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES (CER). Úřední věstník Evropské unie, L 333, 27.12.2022, s. 164–198. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CELEX:32022L2557>
- [27] ČESKÁ REPUBLIKA. Zákon č. 110/2019 Sb., o zpracování osobních údajů. In: Sbírka zákonů České republiky, částka 47, 30. 4. 2019. Dostupné z: <https://www.zakonyprolidi.cz/cs/2019-110>

SEZNAM OBRÁZKŮ

Obrázek 1: Schéma spolupráce manažera kybernetické bezpečnosti s klíčovými odděleními v organizaci	19
Obrázek 2: Klíčové funkce rámce NIST Cybersecurity Framework 2.0 (CSF 2.0)	22
Obrázek 3: Vztahy a tok informací mezi vedením společnosti, ISO/CISO a IT/SEC týmem	35

SEZNAM TABULEK

Tabulka 1: Porovnání rámců a modelů řízení kybernetické bezpečnosti	25
Tabulka 2: Kritéria, indikátory a příklady implementace jednotlivých úrovní vyspělosti (Tierů) pro doménu „Řízení bezpečnostních informací (Monitoring, Reporting a Analytika)“	48
Tabulka 3: Kritéria, indikátory a příklady implementace jednotlivých úrovní vyspělosti (Tierů) pro doménu „Řízení bezpečnostních incidentů a automatizace reakcí“	49
Tabulka 4: Kritéria, indikátory a příklady implementace jednotlivých úrovní vyspělosti (Tierů) pro doménu „Řízení rizik“	51
Tabulka 5: Kritéria, indikátory a příklady implementace jednotlivých úrovní vyspělosti (Tierů) pro doménu „Řízení aktiv“	52
Tabulka 6: Kritéria, indikátory a příklady implementace jednotlivých úrovní vyspělosti (Tier) pro doménu „Organizační řízení a compliance“	53
Tabulka 7: Přehled fází auditního procesu a hlavních aktivit při hodnocení vyspělosti informační podpory kybernetické bezpečnosti	56
Tabulka 8: Základní charakteristika společnosti FinCore Bank a.s.....	59
Tabulka 9: Hodnocení domény Bezpečnostní monitoring a reporting	60
Tabulka 10: Hodnocení domény Řízení bezpečnostních incidentů a automatizace reakcí .	61
Tabulka 11: Hodnocení domény Řízení rizik	61
Tabulka 12: Hodnocení domény Řízení aktiv	62
Tabulka 13: Hodnocení domény Governance a compliance	62
Tabulka 14: Souhrn vyspělosti jednotlivých domén maturity modelu	63
Tabulka 15: Prioritizace doporučených opatření dle výchozí a cílové úrovně vyspělosti (Tier) (zdroj: vlastní zpracování).....	68
Tabulka 16: Časový harmonogram implementace opatření ve FinCore Bank a.s.....	70
Tabulka 17: RACI matice odpovědností za realizaci bezpečnostních opatření.....	71
Tabulka 18: Ukázkový interní checklist pro validaci informační podpory ve FinCore Bank a.s.	80

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

Zkratka	Význam
AI	Artificial Intelligence (Umělá inteligence)
A	Accountable – zodpovědný za výsledek (v rámci RACI matice)
C	Consulted – konzultovaný (v rámci RACI matice)
CER	Critical Entities Resilience
CM	Configuration Management
CISO	Chief Information Security Officer
CMDB	Configuration Management Database
COBIT	Control Objectives for Information and Related Technology
CSF	Cybersecurity Framework
DLP	Data Loss Prevention
DORA	Digital Operational Resilience Act
EDR	Endpoint Detection and Response
GRC	Governance, Risk and Compliance
GDPR	General Data Protection Regulation
HVAC	Heating, Ventilation and Air Conditioning
IAM	Identity and Access Management
ICS	Information and Cyber Security
IDS	Intrusion Detection System
ISO	Information Security Officer
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ISMS	Information Security Management System

Zkratka	Význam
IT	Information Technology
I	Informed – informovaný (v rámci RACI matice)
KPI	Key Performance Indicator
KRI	Key Risk Indicator
MFA	Multi-Factor Authentication
MTTD	Mean Time to Detect
MTTR	Mean Time to Respond
NIS2	Network and Information Security Directive 2
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PCI DSS	Payment Card Industry Data Security Standard
R	Responsible – ten, kdo úkol vykoná (v rámci RACI matice)
RACI	Responsible, Accountable, Consulted, Informed
SaaS	Software as a Service
SCA	Strong Customer Authentication
SIEM	Security Information and Event Management
SLA	Service-Level Agreement
SOC	Security Operations Center
SOAR	Security Orchestration, Automation and Response
SP	Special Publication (NIST)
SSO	Single Sign-On
Tier	Úroveň vyspělosti v rámci maturity modelu
TTP	Tactics, Techniques, and Procedures (v threat intelligence)

Zkratka	Význam
VPN	Virtual Private Network
ZKB	Zákon o kybernetické bezpečnosti
ZTA	Zero Trust Architecture

SEZNAM PŘÍLOH

Příloha P I: Řízení rizik Maturity model.pdf

PŘÍLOHA P I: ŘÍZENÍ RIZIK MATURITY MODEL

Tato příloha znázorňuje procesní schéma maturity modelu informační podpory manažera kybernetické bezpečnosti. Diagram ukazuje tok informací od vstupních zdrojů (logy, audity, rozhovory) přes jejich zpracování a rozdělení do klíčových domén, až po vyhodnocení úrovně vyspělosti (Tier 1–4) s doporučenými opatřeními pro každý stupeň. Model slouží jako nástroj pro hodnocení a plánování rozvoje informační podpory, konkrétně v oblasti řízení rizik.