

Systém řízení konvergované bezpečnosti

Bc. Dušan Janovský

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. Dušan Janovský
Osobní číslo:	A23591
Studijní program:	N1032A020003 Bezpečnostní technologie, systémy a management
Specializace:	Bezpečnostní management
Forma studia:	Kombinovaná
Téma práce:	Systém řízení konvergované bezpečnosti
Téma práce anglicky:	Converged Security Management System

Zásady pro vypracování

1. Vysvětlíte pojem konvergovaná bezpečnost.
2. Popíšete hlavní oblasti konvergované bezpečnosti.
3. Provedte návrh systému řízení konvergované bezpečnosti ve firmě se začleněním do organizační struktury.
4. Zajistěte, že navržený systém bude v souladu s legislativními a normativními předpisy.
5. Demonstrujte na modelovém příkladu.

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

Seznam doporučené literatury:

1. LUKÁŠ, Luděk a kol. *Konvergovaná bezpečnost*. 1.vydání. Zlín: VeRBuM, 2019, 206 s. ISBN 978-80-87500-99-6.
2. DUŠKOVÁ, Radka. *Bezpečnostní a krizový management v praxi*. České Budějovice: Vysoká škola evropských a regionálních studií, z.ú., 2016, 83 s. Studia. ISBN 978-80-7556-010-0.
3. SARGA, Libor. *Organizational security processes and crisis management in the knowledge society: doctoral thesis = Krizový management a bezpečnostní procesy organizace ve znalostní společnosti*. 2014, 279 s.
4. KHARCHENKO, Vyacheslav, DOTSENKO, Sergiy, ILLIASHENKO, Oleg a Sergiy KAMENSKYI. "Integrated Cyber Safety & Security Management System: Industry 4.0 Issue," *2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 2019, strana. 197-201, doi: 10.1109/DESSERT.2019.8770010.
5. DRASTICH, Martin. *Systém managementu bezpečnosti informací*. Praha: Grada, 2011. Průvodce (Grada). ISBN 978-80-247-4251-9.
6. SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. Expert (Grada). ISBN 978-80-247-3051-6.

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 zabývá problematikou konvergované bezpečnosti v kontextu podnikové praxe. V teoretické části je vysvětlen pojem konvergovaná bezpečnost a popsány její hlavní oblasti. Dále se tato část věnuje legislativním a normativním předpisům relevantním pro řízení bezpečnosti a v neposlední řadě poskytuje přehled nejtypičtějších forem organizačních struktur uplatňovaných v praxi. Praktická část se zaměřuje na analýzu současného stavu řízení bezpečnosti v organizacích z hlediska rozděleného či konvergovaného řízení jednotlivých oblastí bezpečnosti a dále se věnuje návrhu systému řízení konvergované bezpečnosti v organizaci. Navržené řešení je demonstrováno na modelovém příkladu.

Klíčová slova: konvergovaná bezpečnost, řízení bezpečnosti, řízení rizik

ABSTRACT

This thesis addresses the issue of converged security in the context of corporate practice. The theoretical part explains the concept of converged security and describes its main areas. It also deals with legislative and normative requirements relevant to security management and provides an overview of the most typical forms of organizational structures applied in practice. The practical part focuses on the analysis of the current state of security management in organizations in terms of separated or converged management of individual security domains and further presents a proposal for a converged security management system within an organization. The proposed solution is demonstrated using a model example.

Keywords: converged security, security management, risk management

Tímto bych chtěl poděkovat vedoucímu své diplomové práce panu Ing. Lukáši Králíkovi, Ph.D. za odborné rady a cenné připomínky, které mi poskytoval při její tvorbě. Také bych rád poděkoval svým blízkým, kteří mě během studia podporovali.

Prohlašuji, že při tvorbě této práce jsem použil nástroj generativního modelu AI ChatGPT, dostupného z: <https://chatgpt.com/>, za účelem pomoci parafrázování. Po použití tohoto nástroje jsem provedl kontrolu obsahu a přebírám za něj plnou zodpovědnost.

OBSAH

ÚVOD.....	12
I TEORETICKÁ ČÁST	13
1 KONVERGOVANÁ BEZPEČNOST.....	14
1.1 FYZICKÁ BEZPEČNOST	14
1.1.1 Základní dělení systému fyzické bezpečnosti	15
1.1.2 Prostorové dělení systému fyzické bezpečnosti	15
1.1.3 Vybrané hrozby v oblasti fyzické bezpečnosti.....	16
1.2 INFORMAČNÍ BEZPEČNOST	17
1.2.1 Vybrané hrozby v oblasti informační bezpečnosti.....	17
1.3 KYBERNETICKÁ BEZPEČNOST	18
1.3.1 Životní cyklus kybernetické bezpečnosti	19
1.3.2 Vybrané hrozby v oblasti kybernetické bezpečnosti.....	20
1.4 PROVOZNÍ BEZPEČNOST.....	20
1.4.1 Vybrané hrozby v oblasti provozní bezpečnosti	21
1.5 SHRUTÍ KAPITOLY	22
2 LEGISLATIVNÍ A NORMATIVNÍ RÁMEC KONVERGOVANÉ BEZPEČNOSTI.....	23
2.1 EVROPSKÁ LEGISLATIVA	23
2.1.1 Směrnice o opatřeních pro vysokou společnou úroveň kybernetické bezpečnosti v Unii.....	23
2.1.2 Směrnice o odolnosti kritických subjektů	24
2.1.3 Nařízení o digitální provozní odolnosti finančního sektoru.....	24
2.1.4 Obecné nařízení o ochraně osobních údajů.....	24
2.2 ČESKÁ LEGISLATIVA	25
2.2.1 Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti.....	25
2.2.2 Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků	25
2.2.3 Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů	26
2.2.4 Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)	26
2.2.5 Vyhláška č. 479/2024 Sb., o informační bezpečnosti	26
2.2.6 Zákon č. 110/2019 Sb., o zpracování osobních údajů.....	27
2.2.7 Zákon č. 262/2006 Sb., zákoník práce	27
2.2.8 Zákon č. 133/1985 Sb., o požární ochraně.....	27
2.3 PŘEHLED NOREM KONVERGOVANÉ BEZPEČNOSTI.....	28
2.3.1 ČSN EN 50131: Poplachové zabezpečovací a tísňové systémy	28

2.3.2	ČSN EN 60839: Elektronické systémy kontroly vstupu	28
2.3.3	ČSN EN 62676: Dohledové videosystémy pro použití v bezpečnostních aplikacích	28
2.3.4	ČSN EN 1143: Bezpečnostní úschovné objekty	29
2.3.5	ISO/IEC 27000: Normy pro řízení bezpečnosti informací	29
2.3.6	ISO 22300: Normy pro řízení kontinuity činností	30
2.3.7	ČSN ISO 31000: Řízení rizik – Směrnice	30
2.4	SHRNUTÍ KAPITOLY	30
3	PŘEHLED ORGANIZAČNÍCH STRUKTUR A SYSTÉMŮ ŘÍZENÍ BEZPEČNOSTI	32
3.1	TYPY ORGANIZAČNÍCH STRUKTUR	32
3.1.1	Liniová struktura	32
3.1.2	Funkcionální struktura	33
3.1.3	Liniově-štabní struktura	34
3.1.4	Divizní struktura	34
3.1.5	Maticová struktura	35
3.2	DRUHY PŘÍSTUPŮ K ŘÍZENÍ BEZPEČNOSTI V ORGANIZACÍCH	36
3.2.1	Centralizovaný přístup k řízení bezpečnosti	36
3.2.2	Decentralizovaný přístup k řízení bezpečnosti	36
3.2.3	Hybridní přístup k řízení bezpečnosti	37
3.3	SHRNUTÍ KAPITOLY	37
II	PRAKTICKÁ ČÁST	39
4	SOUČASNÝ STAV ŘÍZENÍ BEZPEČNOSTI V ORGANIZACÍCH	40
4.1	ANALÝZA PŘEVLÁDAJÍCÍCH PŘÍSTUPŮ K ŘÍZENÍ BEZPEČNOSTI	40
4.2	RIZIKA ODDĚLENÉHO ŘÍZENÍ BEZPEČNOSTI	42
4.3	SHRNUTÍ KAPITOLY	43
5	NÁVRH SYSTÉMU ŘÍZENÍ KONVERGOVANÉ BEZPEČNOSTI	45
5.1	ZÁKLADNÍ CHARAKTERISTIKA ORGANIZACE	46
5.2	STANOVENÍ CÍLŮ KONVERGOVANÉHO ŘÍZENÍ BEZPEČNOSTI	46
5.3	ORGANIZAČNÍ ZAJIŠTĚNÍ BEZPEČNOSTI	47
5.4	ŘÍZENÍ RIZIK	47
5.5	ZAJIŠTĚNÍ SOULADU S LEGISLATIVNÍMI A NORMATIVNÍMI POŽADAVKY	48
5.6	PLÁNOVÁNÍ A IMPLEMENTACE BEZPEČNOSTNÍCH OPATŘENÍ	48
5.7	REAKCE NA INCIDENTY	49
5.8	MONITOROVÁNÍ, AUDIT A ZLEPŠOVÁNÍ	49
5.9	SHRNUTÍ KAPITOLY	50
6	APLIKACE SYSTÉMU ŘÍZENÍ KONVERGOVANÉ BEZPEČNOSTI NA MODELOVÉ ORGANIZACI	51
6.1	ZÁKLADNÍ CHARAKTERISTIKA ORGANIZACE	51

6.2	STANOVENÍ CÍLŮ KONVERGOVANÉHO ŘÍZENÍ BEZPEČNOSTI	52
6.3	ORGANIZAČNÍ ZAJIŠTĚNÍ BEZPEČNOSTI	52
6.4	ŘÍZENÍ RIZIK.....	53
6.5	ZAJIŠTĚNÍ SOULADU S LEGISLATIVNÍMI A NORMATIVNÍMI POŽADAVKY	55
6.6	PLÁNOVÁNÍ A IMPLEMENTACE BEZPEČNOSTNÍCH OPATŘENÍ	56
6.7	REAKCE NA INCIDENTY	57
6.8	MONITOROVÁNÍ, AUDIT A ZLEPŠOVÁNÍ	58
6.9	SHRNUTÍ KAPITOLY	60
ZÁVĚR		61
SEZNAM POUŽITÉ LITERATURY.....		62
SEZNAM OBRÁZKŮ		71
SEZNAM TABULEK.....		72
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....		73
SEZNAM PŘÍLOH.....		75

ÚVOD

Bezpečnost je zásadním předpokladem pro stabilní a efektivní fungování moderních organizací. V dnešním dynamickém světě čelí tyto organizace neustále se vyvíjejícím bezpečnostním hrozbám, které již nespádají pouze do kategorie tradiční fyzické bezpečnosti, ale zahrnují také bezpečnost informační, kybernetickou a provozní. Tyto hrozby se navíc často prolínají a mohou mít synergický efekt, kdy například kybernetický útok může vést k narušení fyzické bezpečnosti objektu nebo provozu organizace. Je proto nezbytné, aby organizace k bezpečnosti přistupovaly komplexně jako k jednomu vzájemně propojenému celku integrujícímu jednotlivé oblasti bezpečnosti. Právě takovým komplexním pojetím bezpečnosti se zabývá koncept konvergované bezpečnosti.

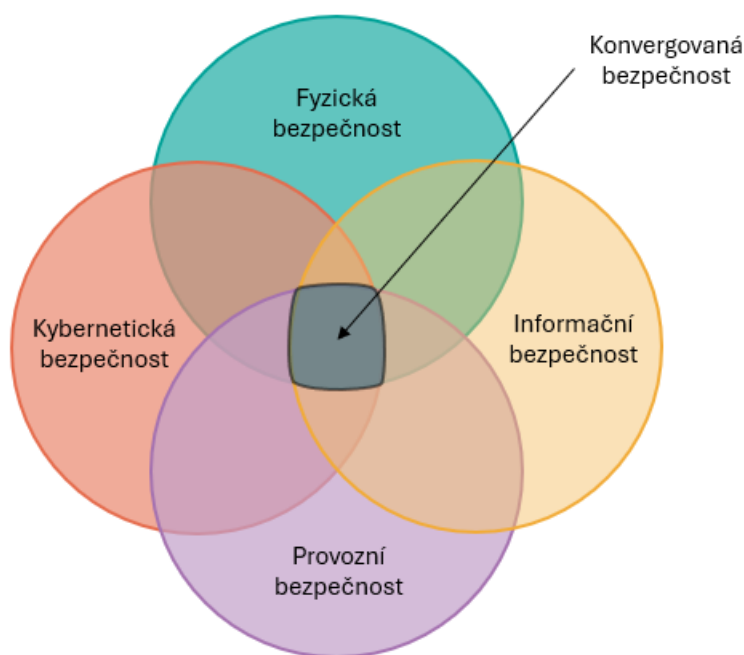
Konvergovaná bezpečnost představuje přístup, který propojuje různé oblasti bezpečnosti do jednoho uceleného systému. Zatímco tradiční modely pojetí bezpečnosti často oddělovaly fyzickou, kybernetickou a provozní bezpečnost, konvergovaný přístup naopak zdůrazňuje jejich vzájemnou provázanost. Cílem je vytvořit integrovaný systém, v jehož rámci bezpečnostní opatření z různých oblastí spolupracují jako jeden celek, což umožňuje komplexní a koordinovanou reakci na hrozby a minimalizaci potenciálních škod.

Teoretická část práce se zaměřuje na vymezení pojmu konvergovaná bezpečnost, charakteristiku jejích hlavních oblastí a přehled souvisejících legislativních a normativních požadavků i běžně uplatňovaných forem organizačních struktur. Praktická část se věnuje analýze současného stavu řízení bezpečnosti v organizacích z pohledu míry oddělenosti či propojení jednotlivých bezpečnostních oblastí a dále obsahuje návrh systému řízení konvergované bezpečnosti vhodný pro podnikové prostředí. Tento návrh je následně aplikován na modelové organizaci, kde je demonstrována jeho možná praktická využitelnost.

I TEORETICKÁ ČÁST

1 KONVERGOVANÁ BEZPEČNOST

Konvergovaná bezpečnost je specifickým druhem bezpečnosti, která spočívá v integraci kompatibilních druhů bezpečnosti do jednoho celku. Tento koncept umožňuje prostřednictvím analýzy souvislostí mezi projevy narušení bezpečnosti efektivně identifikovat vznikající hrozby a cíleně na ně reagovat. Konvergovaná bezpečnost v praxi zahrnuje nejčastěji bezpečnost fyzickou, kybernetickou, informační a provozní, její struktura se však může lišit v závislosti na specifických potřebách a charakteru chráněného objektu a na míře slučitelnosti jednotlivých bezpečnostních oblastí. Konvergovaná bezpečnost se využívá v oblastech, kde je nezbytná koordinace různých druhů bezpečnosti, například v energetice, dopravě, veřejné správě nebo zdravotnictví. [1]



Obrázek 1 Základní model konvergované bezpečnosti

(zdroj: [1])

V následujících částech kapitoly jsou popsány jednotlivé druhy bezpečnosti, které jsou součástí základního modelu konvergované bezpečnosti.

1.1 Fyzická bezpečnost

Fyzická bezpečnost je jedním z nejstarších druhů bezpečnosti. Jedním z prvních vyžívaných prostředků v rámci fyzické bezpečnosti byly mechanické zábranné systémy a fyzická ostraha, s technologickým rozvojem se však tyto prvky rozšířily o bezpečnostní technologie

na bázi elektronických systémů, které zahrnují například kamerové systémy, elektronické systémy kontroly vstupu nebo detektory kovů. Fyzická bezpečnost je základním kamenem konvergované bezpečnosti a její efektivní fungování je klíčové pro komplexní ochranu organizací. [1]

1.1.1 Základní dělení systému fyzické bezpečnosti

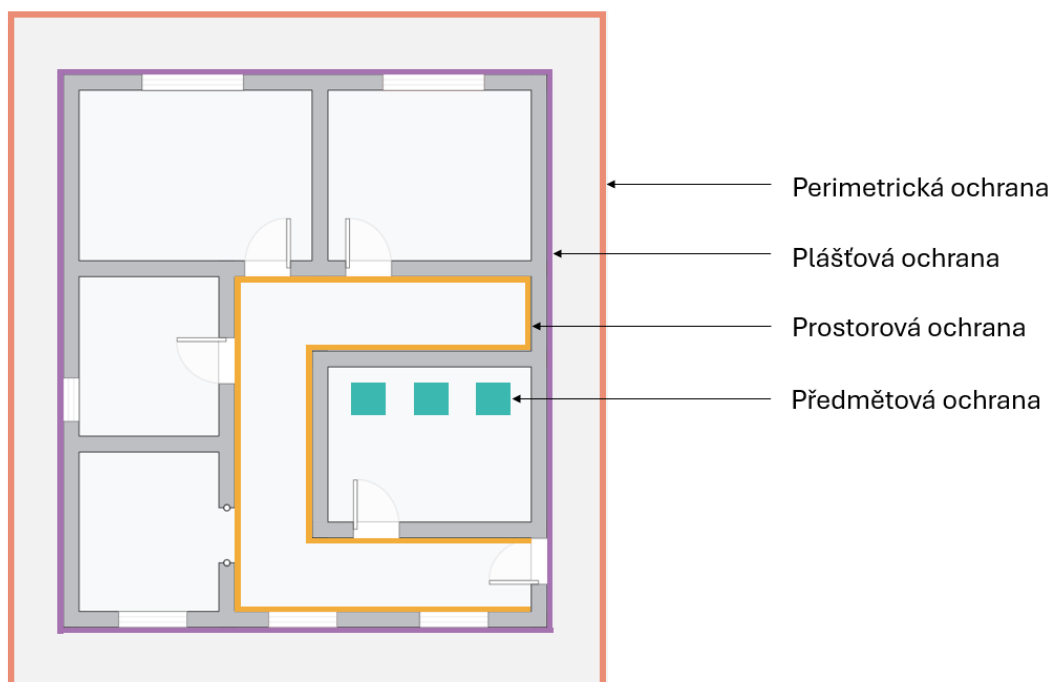
Systém fyzické bezpečnosti lze rozdělit na tři základní oblasti následovně:

- **fyzická ochrana:** chrání aktiva prostřednictvím fyzické přítomnosti ostrahy v objektech; zajišťována zpravidla hlídači, strážnými nebo bezpečnostní službou,
- **technická ochrana:** slouží k ochraně objektů a detekci neoprávněného přístupu pomocí technických prostředků; zahrnuje mechanické zábranné systémy (např. zámky, ploty) a elektronické systémy, jako jsou poplachové zabezpečovací a tísňové systémy, požární signalizace nebo systémy kontroly vstupu,
- **režimová opatření:** stanovují pravidla pro pohyb osob a materiálu, manipulaci s klíči a bezpečnostními systémy a řešení mimořádných událostí; rozlišují se na vnější (vstupy, vjezdy) a vnitřní (pohyb uvnitř objektu). [1, 2]

1.1.2 Prostorové dělení systému fyzické bezpečnosti

Systém fyzické bezpečnosti lze také rozdělit z hlediska prostoru, a to následovně:

- **perimetrická ochrana:** zabezpečuje vnější obvod chráněného objektu; slouží k včasné detekci neoprávněného vstupu a zpomalení narušitele,
- **plášťová ochrana:** slouží k ochraně vnějšího pláště budovy; jejím cílem je zabránit průchodu narušitele a signalizovat pokus o vniknutí,
- **prostorová ochrana:** slouží k detekci a zpomalení pohybu narušitele uvnitř budovy v případě, že překonal perimetrickou a plášťovou ochranu,
- **předmětová ochrana:** zajišťuje zabezpečení konkrétních aktiv, jako jsou hotovost, cennosti nebo citlivé dokumenty; jejím cílem je zabránit jejich odcizení nebo neoprávněné manipulaci. [1, 3]



Obrázek 2 Prostorové dělení systému fyzické bezpečnosti znázorněné na půdorysu domu

(zdroj: [1])

1.1.3 Vybrané hrozby v oblasti fyzické bezpečnosti

Fyzická bezpečnost se primárně vymezuje vůči záměrným hrozbám způsobeným lidskou činností, zahrnuje však také ochranu před hrozbami přírodního charakteru. Mezi významné příklady hrozeb patří:

- neoprávněný vstup do objektu,
- krádež,
- vandalismus,
- požár,
- sabotáž,
- fyzické napadení,
- teroristický útok.

Detailní popis hrozeb včetně odpovídajících opatření je uveden v příloze P I: Vybrané hrozby a protiopatření v oblasti fyzické bezpečnosti. [1, 4, 5]

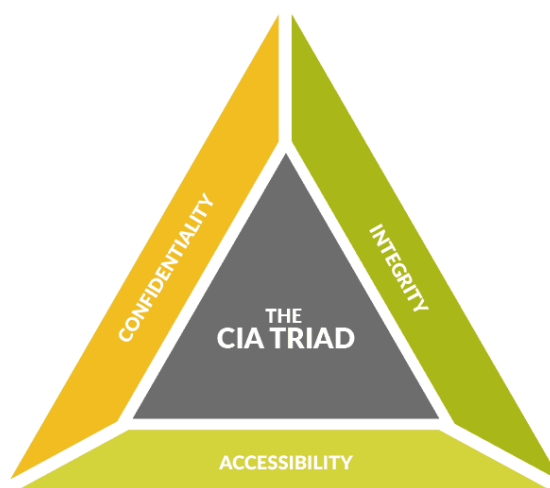
1.2

1.2 Informační bezpečnost

Informační bezpečnost je oblast, která se zabývá problematikou ochrany informací ve fyzické nebo elektronické formě před narušením jejich důvěrnosti, integrity a dostupnosti během celého životního cyklu, což zahrnuje jejich vznik, zpracování, ukládání, přenos a likvidaci. [1]

Pojmy důvěrnost, integrita a dostupnost tvoří tzv. CIA triádu (Confidentiality, Integrity, Availability) a označují klíčové aspekty ochrany informací:

- **Důvěrnost:** Informace musí být přístupná pouze oprávněným osobám.
- **Integrita:** Informace musí zůstat přesná a úplná a nesmí být neoprávněně změněna.
- **Dostupnost:** Informace i související systémy musí být k dispozici oprávněným uživatelům v požadovaném čase. [6, 7]



Obrázek 3 CIA triáda informační bezpečnosti

(zdroj: [8])

Mezi klíčové normy a legislativní předpisy v oblasti informační bezpečnosti se řadí norma ISO/IEC 27001, která stanovuje požadavky na systém řízení informační bezpečnosti (ISMS), zahrnující řízení rizik a implementaci bezpečnostních opatření, a Obecné nařízení o ochraně osobní údajů (General Data Protection Regulation – GDPR). [1]

1.2.1 Vybrané hrozby v oblasti informační bezpečnosti

Organizace z hlediska informační bezpečnosti čelí různým hrozbám, které mohou ohrozit důvěrnost, integritu a dostupnost informací. Zdrojem těchto hrozeb mohou být jak vnější,

tak vnitřní faktory, přičemž jejich dopady mohou mít pro organizaci vážné důsledky, pokud nebudou včas rozpoznány a minimalizovány vhodnými opatřeními.

Mezi významné příklady hrozeb v oblasti informační bezpečnosti patří zejména:

- neoprávněný přístup k informacím,
- únik informací,
- ztráta dat,
- neoprávněná manipulace s informacemi,
- průmyslová špionáž,
- sociální inženýrství.

Popis těchto hrozeb a přehled jim odpovídacích opatření je uveden v příloze P II: Vybrané hrozby a protiopatření v oblasti informační bezpečnosti. [9–16]

1.3 Kybernetická bezpečnost

Kybernetická bezpečnost je oblast informačních technologií zaměřená na ochranu sítí, zařízení a dat před neoprávněným přístupem a zneužitím. Jejím cílem je také zajištění důvěrnosti, integrity a dostupnosti informací. [18]

Ačkoliv se kybernetická bezpečnost často zaměřuje s informační bezpečností, nejde o totožné pojmy. Obě disciplíny spolu úzce souvisejí, ale každá se zaměřuje na jiný aspekt ochrany dat. Zatímco kybernetická bezpečnost se zaměřuje na ochranu digitálních dat, IT systémů, sítí a související infrastruktury, informační bezpečnost zahrnuje širší oblast ochrany všech informačních aktiv bez ohledu na jejich formu. Informační bezpečnost lze tedy chápat jako širší oblast, do níž spadá i kybernetická bezpečnost. [19]

Kybernetická bezpečnost se řídí řadou norem a legislativních předpisů, jejichž účelem je ochrana organizací a jednotlivců před kybernetickými hrozbami. Mezi klíčové legislativní předpisy patří směrnice NIS 2, zaměřená na zvýšení odolnosti organizací proti kybernetickým útokům v rámci EU. Významným mezinárodním standardem je například norma ISO/IEC 27001 pro systémy řízení informační bezpečnosti a rámec NIST Cybersecurity Framework zaměřený na řízení rizik v kybernetickém prostoru. V České republice oblast kybernetické bezpečnosti upravuje Zákon o kybernetické bezpečnosti, který stanovuje práva a povinnosti osob i pravomoc a působnost orgánů veřejné moci v této

oblasti. V neposlední řadě je důležitým nařízením také GDPR, které stanovuje povinnosti v oblasti ochrany osobních údajů a tím přispívá k celkové kybernetické bezpečnosti organizací. [1, 20, 21]

1.3.1 Životní cyklus kybernetické bezpečnosti

Účinná kybernetická bezpečnost vyžaduje systematický přístup k identifikaci rizik, zavádění ochranných opatření a reakci na bezpečnostní incidenty. NIST Cybersecurity Framework rozděluje tento proces do pěti základních fází:

1. **Identifikace** (Identify),
2. **Ochrana** (Protect),
3. **Detekce** (Detect),
4. **Reakce** (Respond),
5. **Obnova** (Recover). [21]

Identifikace

Cílem této fáze je porozumět kybernetickým rizikům a vytvořit přehled o klíčových aktivech, procesech a informačních tocích, které je nezbytné chránit. Zahrnuje mimo jiné identifikaci hrozeb, zranitelností a nastavení bezpečnostní politiky. [21]

Ochrana

Tato fáze se zaměřuje na zavedení opatření, která minimalizují riziko kybernetických útoků a zajišťují bezpečný provoz organizace. Mezi klíčové aktivity patří řízení přístupu k informacím, ochrana citlivých dat, pravidelné zálohování a školení zaměstnanců v oblasti kybernetické bezpečnosti. [21]

Detekce

Fáze detekce se zaměřuje na včasné rozpoznání bezpečnostních událostí prostřednictvím monitorování sítí, logů a podezřelých aktivit. Cílem této fáze je identifikovat bezpečnostní incidenty co nejdříve, aby na ně bylo možné rychle reagovat a minimalizovat škody. [21]

Reakce

Fáze reakce se zaměřuje na efektivní reakci na detekované bezpečnostní incidenty s cílem minimalizovat jejich dopady a obnovit běžný provoz organizace. Klíčovou součástí této fáze

je nejen samotné provedení reakčních opatření, ale také jejich pravidelné testování a zlepšování na základě získaných zkušeností. [21]

Obnova

Tato fáze se zaměřuje na co nejrychlejší obnovení narušeného provozu a služeb organizace po kybernetickém incidentu. Kromě samotného procesu obnovy zahrnuje i průběžné zlepšování plánů obnovy na základě zkušeností z předchozích incidentů, jejich pravidelnou aktualizaci a řízení komunikace s veřejností v průběhu obnovy. [21]

Uvedené fáze představují strukturovaný rámec, který lze přizpůsobit konkrétním podmínkám organizace a slouží jako základ pro systematické řízení kybernetické bezpečnosti.

1.3.2 Vybrané hrozby v oblasti kybernetické bezpečnosti

Kybernetické hrozby představují významné riziko pro organizace i jednotlivce, protože mohou vést k úniku citlivých dat, narušení provozu nebo finančním ztrátám. Útočníci neustále zdokonalují své metody, a proto je klíčové tyto hrozby nejen identifikovat, ale také zavádět účinná opatření k jejich prevenci a zmírnění dopadů.

Mezi významné kybernetické hrozby patří zejména:

- malware,
- phishing,
- denial-of-service útoky,
- útoky pomocí injekce kódu,
- man-in-the-middle útoky.

Popis těchto hrozeb a přehled odpovídajících protiopatření je uveden v příloze P III: Vybrané hrozby a protiopatření v oblasti kybernetické bezpečnosti. [22–24]

1.4 Provozní bezpečnost

Provozní bezpečnost představuje soubor opatření, procesů a strategií zaměřených na zajištění nepřerušného a bezpečného provozu organizace, podniku nebo systému za předvídatelných provozních podmínek. Jejím hlavním cílem je prevence výpadků, poruch a dalších incidentů, které by mohly narušit nebo zcela zastavit provoz organizace. [1]

Klíčovým prvkem je identifikace a ochrana kritických aktiv, procesů a systémů nezbytných pro plynulý chod organizace. To zahrnuje řízení rizik, detekci potenciálních hrozeb, včasnou reakci na incidenty a implementaci opatření pro minimalizaci jejich dopadů.

[1]

Provozní bezpečnost může být implementována různými přístupy v závislosti na zaměření organizace. Mezi klíčové přístupy patří **systém řízení kontinuity činností organizace** (Business Continuity Management Systém, BCMS) a **systém řízení bezpečnosti práce** (Safety Management System, SMS). [1]

Provozní bezpečnost ve smyslu BCMS se zaměřuje na zajištění kontinuity činností organizace nejen v rámci běžného provozu, ale i v případě jeho narušení. Tento typ bezpečnosti se opírá o zásady systému managementu kontinuity podnikání BCMS, což zahrnuje definování zásad pro prevenci výpadků, stanovení kritických procesů a implementaci opatření pro minimalizaci dopadů krizových situací. Klíčovou součástí je pochopení potřeb organizace, sledování výkonnostních indikátorů a přijímání opatření pro udržení funkčnosti organizace i za nepříznivých podmínek. [1]

Provozní bezpečnost ve smyslu SMS se zaměřuje na minimalizaci rizik spojených s lidskými chybami, nedostatky v provozních postupech, selháním technologií nebo vlivem vyšší moci. SMS představuje systematický a aktivní přístup k identifikaci a řízení rizik, přičemž jeho cílem je neustálé zvyšování úrovně bezpečnosti organizace, zejména z hlediska prevence zranění osob nebo poškození majetku. [1]

1.4.1 Vybrané hrozby v oblasti provozní bezpečnosti

Hrozby v oblasti provozní bezpečnosti se mohou u jednotlivých organizací lišit v závislosti na jejich zaměření, infrastruktuře a provozních procesech.

Typické hrozby v oblasti provozní bezpečností zahrnují například:

- výpadek elektrické energie,
- selhání kritických provozních systémů,
- narušení kontinuity provozu v důsledku lidské chyby,
- ztráta kvalifikované pracovní síly,
- přírodní katastrofa.

Popis těchto hrozeb a přehled odpovídajících protiopatření je uveden v příloze P IV: Vybrané hrozby a protiopatření v oblasti provozní bezpečnosti. [1, 25, 26, 27]

1.5 Shrnutí kapitoly

Konvergovaná bezpečnost je specifickým druhem bezpečnosti, který spočívá v propojení různých oblastí bezpečnosti do jednoho celku. Struktura konvergované bezpečnosti závisí na specifických potřebách a charakteru chráněného objektu a míře slučitelnosti jednotlivých bezpečnostních oblastí, nejčastěji však zahrnuje fyzickou, kybernetickou, informační a provozní bezpečnost.

Fyzická bezpečnost se zaměřuje na ochranu osob, majetku a informací prostřednictvím fyzické ochrany, technické ochrany a režimových opatření. Tyto oblasti zahrnují například fyzickou ostrahu, mechanické zábranné systémy, poplachové systémy a pravidla pro pohyb osob a materiálu v prostorách organizace. Mezi klíčové hrozby fyzické bezpečnosti patří krádež, vandalismus, požár, napadení nebo teroristický útok.

Informační bezpečnost se zaměřuje na ochranu informací ve fyzické i digitální podobě. Jejím cílem je zajištění důvěrnosti, integrity a dostupnosti informací, což jsou klíčové principy tzv. CIA triády. S těmito principy souvisí i řada hrozeb, kterým organizace v této oblasti čelí – například neoprávněný přístup k informacím, jejich únik nebo ztráta.

Kybernetická bezpečnost se zaměřuje na ochranu zařízení, sítí a dat před digitálními hrozbami, jako jsou malware, útoky typu denial of service nebo man-in-the-middle. Významnou roli v této oblasti hrají mezinárodní standardy a legislativní předpisy (např. NIS2, ISO/IEC 27001, NIST Framework), které stanovují požadavky na řízení rizik a ochranu digitální infrastruktury.

Provozní bezpečnost se zaměřuje na zajištění kontinuity činností organizace a jejího bezpečného provozu. Mezi hrozby v této oblasti patří výpadky elektrické energie, narušení provozu v důsledku lidské chyby nebo přírodní katastrofy.

Vzájemná propojenost výše zmíněných oblastí v rámci konvergované bezpečnosti umožňuje organizacím lépe identifikovat hrozby, efektivněji řídit rizika a optimalizovat bezpečnostní opatření. Díky integraci jednotlivých bezpečnostních oblastí lze dosáhnout vyšší úrovně ochrany a zajistit rychlejší a účinnější reakce na potenciální ohrožení.

2 LEGISLATIVNÍ A NORMATIVNÍ RÁMEC KONVERGOVANÉ BEZPEČNOSTI

Účinná aplikace principů konvergované bezpečnosti vyžaduje nejen odborné znalosti, ale také orientaci v legislativních předpisech a technických normách, které tuto oblast vymezují. Zajištění souladu s těmito předpisy a normami je klíčové nejen pro efektivní řízení bezpečnostních rizik, ale také pro splnění právních a regulatorních požadavků a ochranu organizace před případnými právními důsledky. Tato kapitola proto přináší přehled relevantní české a evropské legislativy a klíčových technických norem, které tvoří nezbytný rámec pro úspěšnou implementaci systému konvergované bezpečnosti.

2.1 Evropská legislativa

Mezi klíčové evropské předpisy relevantní pro oblast konvergované bezpečnosti patří směrnice NIS 2, směrnice CER, směrnice DORA a nařízení GDPR. Tyto předpisy vytvářejí právní rámec pro řízení rizik, zajištění kybernetické, informační i fyzické bezpečnosti, ochranu osobních údajů a posilování odolnosti kritické infrastruktury. Společně určují povinnosti organizací, stanovují základní bezpečnostní opatření a pravidla pro kontrolu jejich dodržování včetně možných sankcí.

2.1.1 Směrnice o opatřeních pro vysokou společnou úroveň kybernetické bezpečnosti v Unii

Směrnice (EU) 2022/2555 (tzv. NIS 2) nahrazuje předchozí směrnici NIS 1 a jejím cílem je posílit kybernetickou bezpečnost v EU prostřednictvím přísnějších požadavků na organizace v oblastech, jako je energetika, doprava, bankovníctví, poštovní služby nebo digitální infrastruktura. [28]

Mezi hlavní požadavky směrnice patří zavedení opatření pro řízení kybernetických rizik, vícefaktorová autentizace, pravidelné školení zaměstnanců a povinnost hlásit závažné bezpečnostní incidenty. Za nesplnění povinností stanovených směrnicí hrozí základním subjektům pokuty až do výše 10 milionů eur nebo 2 % celkového ročního obrátu; v případě důležitých subjektů se jedná až o 7 milionů eur nebo 1,4 % obrátu. [28, 29]

2.1.2 Směrnice o odolnosti kritických subjektů

Směrnice (EU) 2022/2557 (tzv. směrnice CER) ukládá členským státům povinnost zvýšit odolnost organizací působících v klíčových odvětvích, mezi které patří energetika, doprava, bankovníctví, veřejná správa či digitální infrastruktura. Cílem směrnice je snížit dopady hrozeb, jako jsou havárie, přírodní katastrofy, sabotáže nebo teroristické útoky. [30, 31]

CER a NIS2 se vzájemně doplňují a tvoří jednotný rámec pro posílení odolnosti vůči fyzickým i kybernetickým hrozbám. Směrnice požaduje, aby kritické subjekty přijímaly technická, organizační a bezpečnostní opatření v oblastech prevence incidentů, fyzické ochrany, krizového řízení, obnovy provozu, řízení bezpečnosti zaměstnanců a zvyšování jejich povědomí o opatřeních ke zvýšení odolnosti. [30, 31]

Dozor nad plněním požadavků a stanovení sankcí za jejich porušení spadá do pravomoci jednotlivých členských států. [30]

2.1.3 Nařízení o digitální provozní odolnosti finančního sektoru

Nařízení (EU) 2022/2554 (tzv. nařízení DORA) zavádí jednotný právní rámec pro řízení kybernetických rizik a rizik v oblasti informačních a komunikačních technologií (IKT) ve finančních institucích napříč Evropskou unií. Vztahuje se nejen na banky a pojišťovny, ale také na burzy, investiční podniky, fintech společnosti a další subjekty kritické pro stabilitu finančního trhu. [32, 33]

Nařízení má za cíl zajistit, aby tyto instituce byly schopné odolat kybernetickým útokům, technickým výpadkům a jiným digitálním hrozbám. Nařízení stanovuje povinnosti v oblasti prevence, detekce, zvládání incidentů, testování odolnosti a rovněž dohledu nad dodavateli IKT. [32, 33]

2.1.4 Obecné nařízení o ochraně osobních údajů

Nařízení (EU) 2016/679 (tzv. nařízení GDPR) stanovuje pravidla pro ochranu osobních údajů občanů Evropské unie. Tento předpis se vztahuje na všechny subjekty, které zpracovávají osobní údaje občanů EU bez ohledu na to, kde tyto subjekty sídlí. [34, 35]

Mezi povinnosti uložené nařízením patří například zajištění odpovídající úrovně zabezpečení osobních údajů, uplatnění principu minimalizace dat, omezení doby jejich uchovávání nebo zavedení opatření proti neoprávněnému přístupu a úniku údajů. V případě

porušení nařízení mohou být organizacím uloženy sankce až do výše 20 milionů eur nebo 4 % celosvětového ročního obratu, podle toho, která hodnota je vyšší. [34, 36]

2.2 Česká legislativa

Právní rámec konvergované bezpečnosti v České republice je tvořen souborem zákonů a vyhlášek, které upravují jednotlivé oblasti bezpečnosti, mezi které patří fyzická, kybernetická a informační bezpečnost, ochrana utajovaných informací, zpracování osobních údajů, požární ochrana nebo bezpečnost a ochrana zdraví při práci. Následující část textu přináší přehled vybraných právních předpisů, které výše uvedené oblasti upravují.

2.2.1 Zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti

Zákon o ochraně utajovaných informací a bezpečnostní způsobilosti upravuje pravidla pro ochranu utajovaných informací a podmínky přístupu k nim. Stanovuje čtyři stupně utajení (Přísně tajné, Tajné, Důvěrné a Vyhrazené), přičemž každý z nich vyžaduje odpovídající úroveň bezpečnostních opatření. [37]

Ochrana je zajišťována souborem opatření zahrnujících personální, administrativní a fyzickou bezpečnost, bezpečnost IKT systémů a kryptografickou ochranu. Zákon také určuje, jaké technické prostředky lze použít – například mechanické zábrany, poplachové a tísňové systémy, kamerové systémy nebo zařízení elektronické požární signalizace. [37]

Informační a komunikační systémy zpracovávající utajované informace musí být schváleny Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB). [37]

2.2.2 Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků

Vyhláška č. 528/2005 Sb. je prováděcím předpisem k zákonu o ochraně utajovaných informací a specifikuje požadavky na fyzickou bezpečnost a certifikaci technických prostředků. Stanovuje například bodové ohodnocení jednotlivých opatření fyzické bezpečnosti, minimální požadavky na zabezpečení objektů nebo metodiku hodnocení rizik. [38]

Vyhláška dále určuje náležitosti certifikace technických prostředků určených k ochraně utajovaných informací. Míra požadovaného zabezpečení se zvyšuje úměrně stupni utajení

a zahrnuje využití prostředků, jako jsou mechanické zábranné prostředky, poplachové zabezpečovací systémy nebo systémy kontroly vstupu. [38]

2.2.3 Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů

Zákon č. 181/2014 Sb. představuje klíčový právní předpis pro ochranu informačních a komunikačních systémů v České republice. Vztahuje se na poskytovatele základních služeb (např. v dopravě, energetice, zdravotnictví, bankovníctví) a na poskytovatele digitálních služeb, jako jsou online tržiště, vyhledávače nebo cloudové platformy. [39]

Zákon stanovuje povinnost zavést organizační a technická opatření pro zajištění bezpečnosti informačních a komunikačních systémů, mezi která patří například řízení bezpečnosti informací, bezpečnostní politika, autentizace uživatelů nebo použití kryptografických prostředků. [39]

2.2.4 Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

Vyhláška č. 82/2018 Sb. je prováděcím předpisem k zákonu o kybernetické bezpečnosti a konkretizuje požadavky na bezpečnostní opatření regulovaných subjektů. Upravuje například strukturu bezpečnostní dokumentace, rozsah bezpečnostních opatření, kategorizaci incidentů nebo pravidla jejich hlášení. [40]

Incidenty dělí podle závažnosti do tří kategorií a dále podle dopadu na důvěrnost, integritu či dostupnost aktiv. [40]

Součástí vyhlášky jsou mimo jiné také metodiky pro analýzu rizik, hodnocení aktiv, zpracování bezpečnostní politiky a pravidla pro likvidaci dat. [40]

2.2.5 Vyhláška č. 479/2024 Sb., o informační bezpečnosti

Vyhláška č. 479/2024 Sb. je prováděcím předpisem k zákonu č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Stanovuje požadavky na zajištění bezpečnosti informačních a komunikačních systémů a samostatných elektronických zařízení, která nakládají s utajovanými informacemi. [41]

Vyhláška dále stanovuje požadavky na bezpečné provozování informačních systémů podle stupně utajení a provozního módu, specifikuje náležitosti bezpečnostní dokumentace, pravidla certifikace a akreditace a v neposlední řadě podmínky schvalování projektů bezpečnosti komunikačních systémů. Zahrnuje také požadavky na samostatná elektronická zařízení zpracovávající utajované informace, jako jsou fotoaparáty, kamery nebo záznamníky. [41]

2.2.6 Zákon č. 110/2019 Sb., o zpracování osobních údajů

Zákon č. 110/2019 Sb. navazuje na nařízení GDPR a stanovuje práva a povinnosti při zpracování osobních údajů s cílem chránit soukromí fyzických osob v České republice. [42]

Na dodržování ochrany osobních údajů v České republice dohlíží dle zákona Úřad pro ochranu osobních údajů, který mimo jiné přijímá podněty a stížnosti na porušení povinností stanovených zákonem, poskytuje konzultace v oblasti ochrany osobních údajů, projednává přestupky a ukládá pokuty. [42]

2.2.7 Zákon č. 262/2006 Sb., zákoník práce

Zákoník práce je základním právním předpisem upravujícím vztahy mezi zaměstnavateli a zaměstnanci. Obsahuje mimo jiné pravidla pro vznik a zánik pracovního poměru, pracovní dobu, odměňování i dovolenou. Nedílnou součástí zákoníku práce jsou také ustanovení o bezpečnosti a ochraně zdraví při práci (BOZP), která ukládají povinnosti zaměstnavatelům i zaměstnancům s cílem zajistit bezpečné pracovní prostředí a minimalizovat rizika spojená s výkonem práce. [43]

2.2.8 Zákon č. 133/1985 Sb., o požární ochraně

Zákon č. 133/1985 Sb. stanovuje povinnosti a opatření k předcházení vzniku požárů a ochraně života, zdraví a majetku. Dále mimo jiné upravuje organizaci a činnost jednotek požární ochrany a vymezuje povinnosti fyzických, podnikajících fyzických a právnických osob v oblasti požární ochrany. [44]

Činnosti provozované podnikatelskými subjekty se dle zákona člení podle požárního nebezpečí na činnosti bez zvýšeného, se zvýšeným a s vysokým požárním nebezpečím. Bez ohledu na konkrétní zařazení mají však všechny podnikatelské subjekty povinnost například zajistit požární techniku, vytvářet podmínky pro hašení a záchranu, kontrolovat dodržování předpisů nebo hlásit vzniklé požáry příslušnému operačnímu středisku. [44]

2.3 Přehled norem konvergované bezpečnosti

Vedle závazných legislativních předpisů se v oblasti konvergované bezpečnosti uplatňují také technické normy a standardy, které organizacím poskytují doporučení pro řízení fyzické, informační, kybernetické i provozní bezpečnosti. Tato část kapitoly přináší přehled vybraných norem, které jsou z hlediska konvergované bezpečnosti relevantní.

2.3.1 ČSN EN 50131: Poplachové zabezpečovací a tísňové systémy

Soubor norem ČSN EN 50131 patří k nejvýznamnějším evropským standardům v oblasti fyzické bezpečnosti a upravuje problematiku poplachových zabezpečovacích a tísňových systémů (PZTS). Stanovuje například technické požadavky na bezpečnostní zařízení, napájecí zdroje nebo ústředny a zahrnuje také pokyny pro aplikaci PZTS. [45]

Výchozí částí je norma **ČSN EN 50131-1 – Systémové požadavky**, která definuje stupně zabezpečení objektů podle úrovně rizika a schopností potenciálního narušitele a slouží jako podklad pro volbu vhodných technických opatření. Tato norma zahrnuje také klasifikaci prostředí, ve kterých mohou být komponenty PZTS provozovány, specifikuje funkční požadavky a stanovuje zásady hlášení poplachových stavů v závislosti na stupni zabezpečení. [46]

2.3.2 ČSN EN 60839: Elektronické systémy kontroly vstupu

Soubor norem ČSN EN 60839 se zabývá problematikou elektronických systémů kontroly vstupu. Jeho jednotlivé části stanovují technické a funkční požadavky jak na jednotlivé komponenty, tak na celý systém, a to včetně požadavků na interoperabilitu, zabezpečení přenosu dat nebo řízení přístupu na základě definovaných oprávnění.

Mezi klíčové části souboru patří norma **ČSN EN 60839-11-1**, která klasifikuje systémy kontroly vstupu na základě hodnoty chráněného majetku a schopností potenciálních narušitelů. Významná je rovněž norma **ČSN EN 60839-11-2**, která stanovuje obecné požadavky na plánování, instalaci, provoz, údržbu a dokumentaci pro aplikaci těchto systémů. [46, 47]

2.3.3 ČSN EN 62676: Dohledové videosystémy pro použití v bezpečnostních aplikacích

Soubor norem ČSN EN 62676 se zaměřuje na bezpečnostní kamerové systémy používané pro dohled a ochranu majetku, osob či veřejných prostor. Jednotlivé části souboru stanovují

například systémové požadavky, požadavky na videopřenos, požadavky na přenosové protokoly nebo specifikace pro provoz kamerových systémů využívajících webové služby.

Mezi výchozí části souboru patří norma **ČSN 62676-1-1: Systémové požadavky – obecně**, která definuje stupně zabezpečení v oblasti kamerových systémů. Další významnou částí je také norma **ČSN EN 62676-4**, která obsahuje doporučení a požadavky pro výběr, plánování, instalaci, údržbu a zkoušení kamerových systémů včetně jejich vzájemného propojení. Věnuje se také zařízením pro zpracování obrazu určeným k použití v bezpečnostních aplikacích. [48, 49]

2.3.4 ČSN EN 1143: Bezpečnostní úschovné objekty

Soubor norem ČSN EN 1143 upravuje bezpečnostní požadavky, klasifikaci a zkušební metody pro úschovné objekty, mezi které patří skříňové trezory, ATM trezory, komorové trezory, trezorové dveře a depozitní systémy.

Klíčovou částí je norma **ČSN EN 1143-1**, která rozděluje úschovné objekty do bezpečnostních tříd I až XIII podle jejich odolnosti vůči násilnému překonání. Tato klasifikace je mimo jiné využívána pojišťovnami, které pojistné krytí cenností často podmiňují jejich uložením do trezoru odpovídající minimální bezpečnostní třídy. [49]

Normy rovněž stanovují zkušební postupy pro ověřování odolnosti úschovných objektů s využitím různých nástrojů a prostředků, jako jsou nářadí pro páčení nebo řezání, vrtáky, trhaviny a výbušniny. [50]

2.3.5 ISO/IEC 27000: Normy pro řízení bezpečnosti informací

ISO/IEC 27000 představuje soubor mezinárodních norem zaměřených na řízení bezpečnosti informací. Jednotlivé normy této řady se věnují různým oblastem informační a kybernetické bezpečnosti – od zavádění systému řízení bezpečnosti informací (ISMS), přes řízení rizik, až po implementaci konkrétních bezpečnostních opatření. [51]

Úvodní dokument této skupiny, **ISO/IEC 27000**, poskytuje přehled ostatních norem v rámci souboru, definuje základní pojmy a vysvětluje klíčové principy systémového přístupu k ochraně informací. Stěžejní normou řady je **ISO/IEC 27001**, která stanovuje požadavky na zavedení, provoz a zlepšování ISMS. Norma **ISO/IEC 27002** pak doplňuje tento rámec podrobným rozpracováním konkrétních bezpečnostních opatření a doporučení pro jejich implementaci s ohledem na důvěrnost, integritu a dostupnost informací. [51–53]

2.3.6 ISO 22300: Normy pro řízení kontinuity činností

Soubor norem ISO 22300 se zaměřuje na oblast odolnosti organizací a zajištění kontinuity jejich činností v případě mimořádných událostí. Tato skupina poskytuje metodický rámec pro prevenci, přípravu, reakci i obnovu provozu po incidentech, které mohou narušit běžné fungování organizace. [54]

Úvodní dokument **ISO 22300** slouží jako terminologický základ celé skupiny a zajišťuje jednotné porozumění klíčovým pojmům. Stěžejní normou této řady je **ISO 22301**, která definuje požadavky na zavádění, provoz, udržování a zlepšování systému řízení kontinuity činností (BCMS). Tento rámec dále doplňuje norma **ISO 22313**, která obsahuje metodická doporučení pro implementaci požadavků stanovených v ISO 22301. [54–56]

2.3.7 ČSN ISO 31000: Řízení rizik – Směrnice

Norma **ISO 31000** je ústředním dokumentem stejnojmenné skupiny norem zaměřených na řízení rizik. Poskytuje obecný rámec pro řízení rizik v organizacích napříč různými obory a sektory. Tato norma je založena na několika klíčových zásadách, jako jsou integrování řízení rizik do všech aktivit organizace, přizpůsobení řízení rizik kontextu organizace nebo trvalém zlepšování systému řízení rizik prostřednictvím učení se ze zkušeností. [57]

Stěžejní část normy tvoří proces řízení rizik, který zahrnuje kroky od stanovení rozsahu a kritérií, přes identifikaci, analýzu a hodnocení rizik až po jejich ošetřování, komunikaci se zainteresovanými stranami a vyhodnocování přijatých opatření. [57]

Doplňkovou normou k ISO 31000 je **IEC 31010**, která poskytuje přehled nástrojů a technik používaných pro posuzování rizik. [58]

2.4 Shrnutí kapitoly

Bezpečnostní opatření v rámci konvergované bezpečnosti vycházejí z právních předpisů a technických norem, které určují pravidla, povinnosti a doporučené postupy pro ochranu osob, informací, majetku a zajištění kontinuity činností organizací.

Z hlediska evropské legislativy patří mezi klíčové předpisy směrnice NIS 2 a CER, které se zaměřují na posílení kybernetické bezpečnosti a odolnosti kritických subjektů, a nařízení GDPR, které upravuje ochranu osobních údajů. V českém právním prostředí jsou bezpečnostní požadavky upraveny souborem zákonů a vyhlášek, které se vztahují například

k ochraně utajovaných informací, informační a kybernetické bezpečnosti, bezpečnosti a ochraně zdraví při práci nebo požární ochraně.

Normativní rámec konvergované bezpečnosti tvoří řada mezinárodních a evropských norem, které organizacím poskytují postupy a doporučení pro řízení fyzické, informační, kybernetické i provozní bezpečnosti. Mezi klíčové mezinárodní standardy patří ISO/IEC 27000 pro řízení informační bezpečnosti, ISO 22301 pro zajištění kontinuity činnosti a ISO 31000 pro řízení rizik. Evropské normy, jako jsou EN 50131 pro poplachové systémy, EN 62676 pro dohledové videosystémy nebo EN 1143 pro úschovné objekty, se zaměřují na oblast fyzické bezpečnosti.

Přehled předpisů a norem uvedených v této kapitole představuje základní rámec, nikoliv vyčerpávající výčet, neboť volba konkrétních dokumentů, jimiž by se organizace měla řídit, závisí na charakteru její činnosti, míře identifikovaných rizik, regulatorních požadavcích a dalších specifikách prostředí, v němž organizace působí.

3 PŘEHLED ORGANIZAČNÍCH STRUKTUR A SYSTÉMŮ ŘÍZENÍ BEZPEČNOSTI

Efektivní řízení konvergované bezpečnosti v rámci organizace vyžaduje především vhodně zvolenou organizační strukturu a na ni navazující přístup k řízení bezpečnosti. Způsob rozdělení kompetencí, odpovědností a vztahů mezi jednotlivými útvary zásadně ovlivňuje schopnost organizace reagovat na bezpečnostní hrozby a koordinovat jednotlivé oblasti bezpečnosti. Tato kapitola se proto nejprve věnuje základním typům organizačních struktur, jako je liniová, funkční nebo maticová, a následně představuje různé přístupy k řízení bezpečnosti, například přístup centralizovaný nebo hybridní.

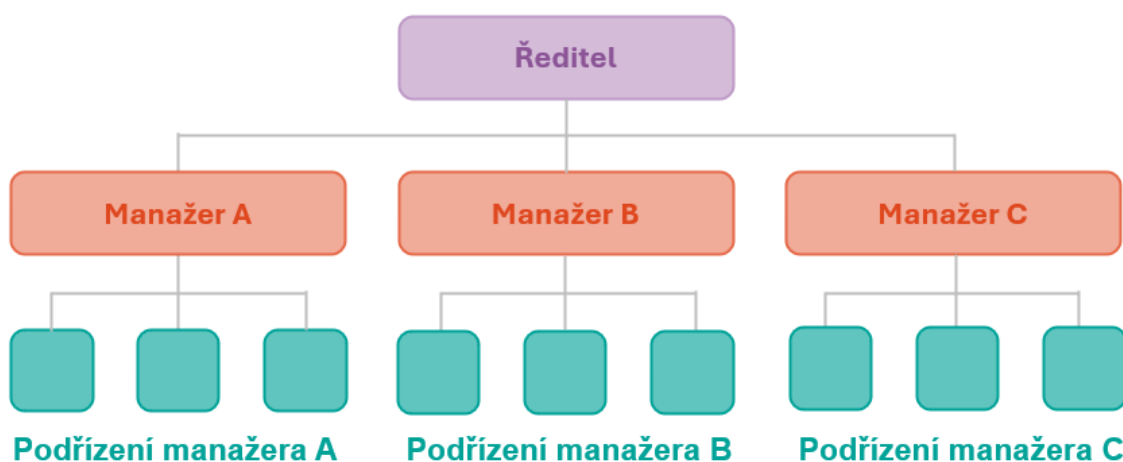
3.1 Typy organizačních struktur

Organizační struktura určuje, jak jsou v rámci organizace rozděleny úkoly, kompetence, pravomoci a komunikační vazby mezi jednotlivými útvary a pracovníky tak, aby celek fungoval efektivně a koordinovaně. Zvolený typ organizační struktury ovlivňuje fungování celé organizace, včetně způsobu řízení její bezpečnosti. Následující část práce přibližuje základní typy organizačních struktur, se kterými se lze v praxi setkat. [59]

3.1.1 Liniová struktura

Liniová organizační struktura je jedním z nejjednodušších a nejtradičnějších typů používaných v praxi. Je založena na principu jednotného řízení, kdy každý podřízený útvar spadá výhradně pod jeden nadřízený útvar. Výsledkem je jednoznačné rozdělení pravomocí, odpovědností i informačních toků. [59, 60]

K hlavním výhodám této struktury patří jasně vymezená nadřízenost a podřízenost, přehledně rozdělené kompetence a také přímá a rychlá komunikace. Nevýhodou jsou pak vyšší nároky na vedoucí pracovníky, kteří musí často disponovat znalostmi z různých oblastí činnosti organizace. [59, 60]

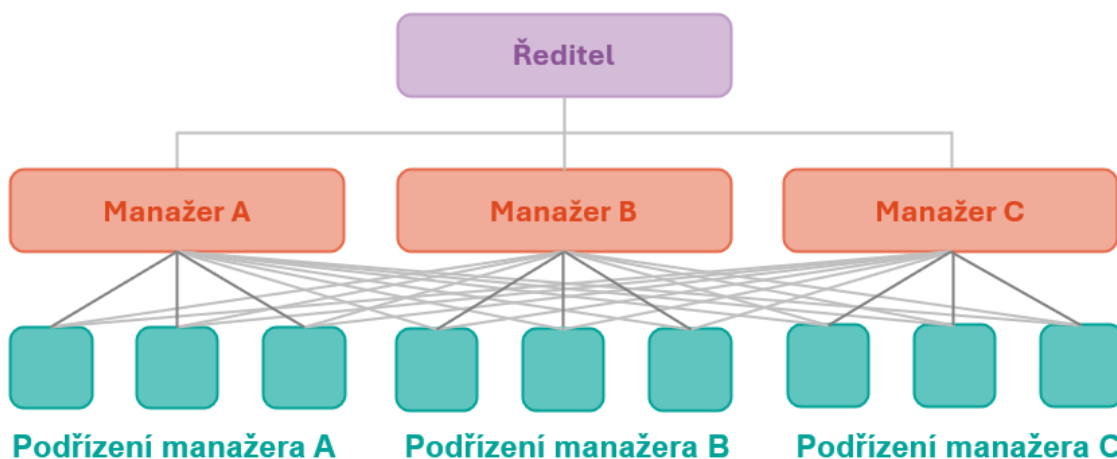


Obrázek 4 Schéma liniové organizační struktury
(zdroj: [61])

3.1.2 Funkcionální struktura

Funkcionální struktura je založena na specializaci řídicích funkcí, kdy je jeden vedoucí nahrazen několika specializovanými vedoucími. Každý z nich odpovídá pouze za svou oblast, zaměstnanci však mohou současně spadat pod více nadřízených v závislosti na povaze řešených úkolů. [59]

Mezi výhody funkcionální struktury patří vysoká míra specializace jednotlivých vedoucích pracovníků, jasné vymezení rolí a odpovědností zaměstnanců a efektivní využití zdrojů v rámci jednotlivých oddělení. Nevýhodou je naopak složitější koordinace mezi útvary, překrývání kompetencí nebo riziko protichůdných pokynů v důsledku vícenásobné podřízenosti. [59, 60]

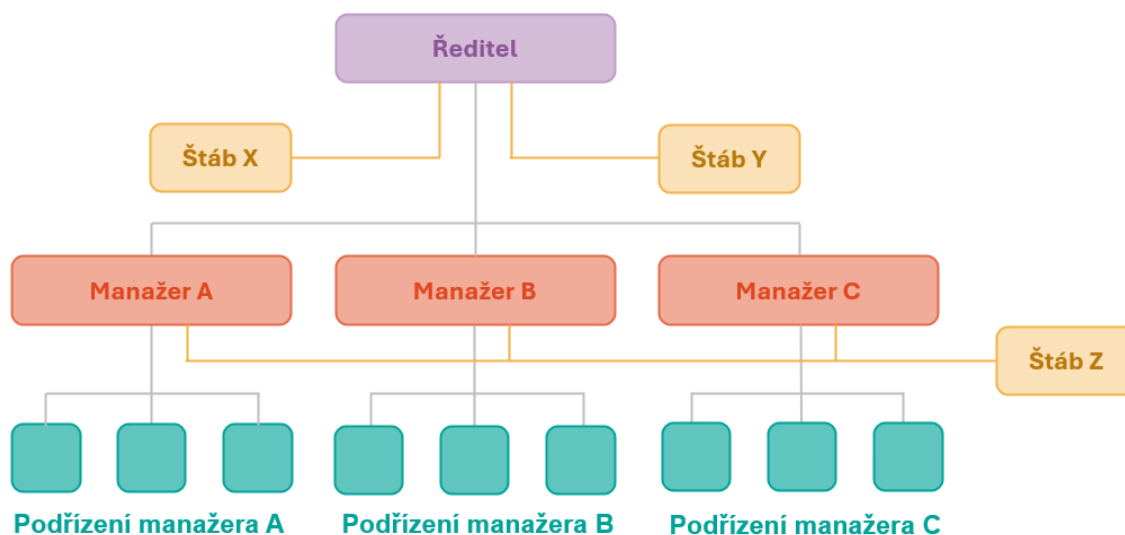


Obrázek 5 Schéma funkcionální organizační struktury
(zdroj: [62])

3.1.3 Liniově-štabní struktura

Liniově-štabní struktura kombinuje prvky liniové a funkcionální struktury. Zachovává jednotné vedení, které je typické pro liniovou strukturu, a zároveň umožňuje využití specializace prostřednictvím štabních útvarů, které poskytují odborné rady a podpůrné služby vedoucím liniových útvarů. [59]

Mezi výhody této struktury patří jednoduchost řízení, jasná odpovědnost, rychlost rozhodování a odborná podpora štabních útvarů. Nevýhodou je naopak složitější koordinace, riziko nárůstu byrokracie a tlak na rozšiřování štabních kapacit, což může zvyšovat náklady a snižovat pružnost organizace. [59, 60]



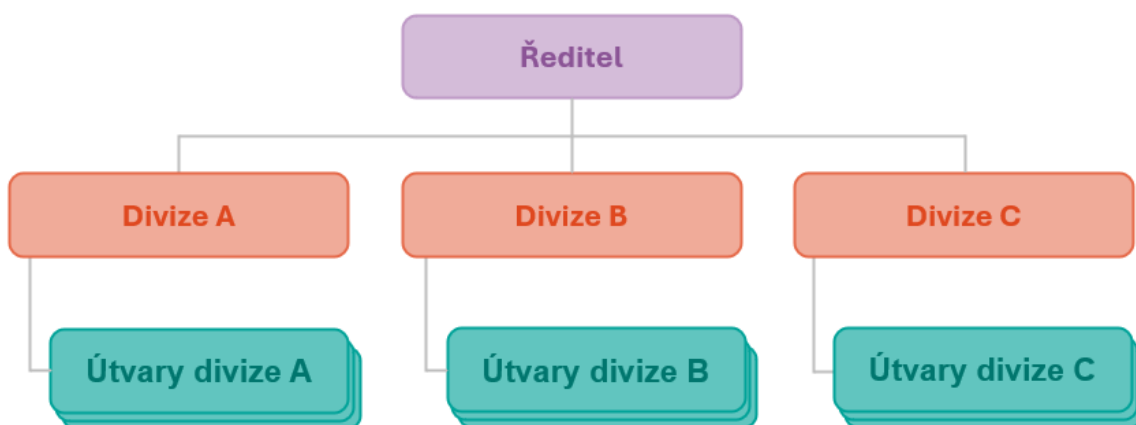
Obrázek 6 Schéma liniově-štabní organizační struktury

(zdroj: [60])

3.1.4 Divizní struktura

Divizní struktura je založena na vytvoření relativně samostatných celků (divizí), které jsou obvykle rozděleny podle určitého kritéria, například druhu poskytovaných produktů nebo služeb, geografického umístění nebo skupin zákazníků. [59]

Divizní struktura přináší organizaci vyšší míru autonomie jednotlivých celků, což umožňuje flexibilně reagovat na požadavky trhu, zefektivnit řízení a jasně vymezit odpovědnost za výsledky. Nevýhodou této struktury mohou být vyšší provozní náklady spojené s chodem více samostatných celků, obtížnější koordinace mezi divizemi, riziko vzájemné izolace a vznik rivality, která může oslabovat spolupráci v rámci celé organizace. [59, 63]



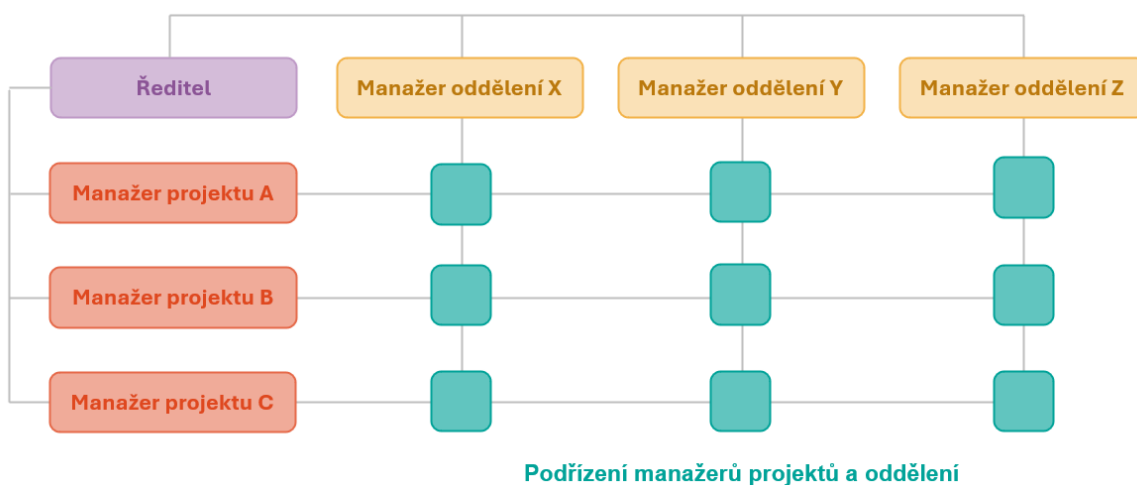
Obrázek 7 Schéma divizní organizační struktury

(zdroj: [64])

3.1.5 Maticová struktura

Maticová struktura kombinuje prvky funkcionální a divizní struktury. Obvykle vzniká v situaci, kdy je potřeba vytvořit projektově orientované týmy nad rámec standardní organizační struktury. Typickým rysem maticové struktury je tzv. dvojí podřízenost, kdy zaměstnanci bývají současně podřízeni jak vedoucímu funkčního útvaru, tak vedoucímu konkrétního projektu. [59]

Mezi hlavní výhody maticové struktury patří vysoká flexibilita, možnost rychle vytvářet specializované projektové týmy, důraz na týmovou spolupráci a vyšší zapojení manažerů do strategických rozhodnutí. Nevýhodou této struktury může být riziko konfliktů mezi vedoucími v horizontální a vertikální linii řízení, nejasné vymezení odpovědností a obtíže při určování priorit vyplývající z dvojí podřízenosti zaměstnanců. [59, 60]



Podřízení manažerů projektů a oddělení

Obrázek 8 Schéma maticové organizační struktury

(zdroj: [60])

3.2 Druhy přístupů k řízení bezpečnosti v organizacích

Zvolený přístup k řízení bezpečnosti určuje, jak jsou v organizaci nastaveny kompetence, odpovědnosti a rozhodovací pravomoci v oblasti bezpečnostního managementu. Výběr konkrétního přístupu ovlivňuje, jak je organizace schopna předcházet bezpečnostním hrozbám, včas na ně reagovat a minimalizovat jejich dopady. Tato část práce představuje tři základní přístupy k řízení bezpečnosti, a to centralizovaný, decentralizovaný a hybridní.

3.2.1 Centralizovaný přístup k řízení bezpečnosti

Centralizovaný přístup k řízení bezpečnosti je charakteristický tím, že veškeré řízení bezpečnosti je koncentrováno do jednoho centrálního útvaru. Tento přístup je typický zejména pro velké organizace s více pobočkami v rámci jedné země, případně na mezinárodní úrovni. Centrální tým pro řízení bezpečnosti zajišťuje nepřetržitý dohled nad provozem a klíčovými aktivy organizace. V případě výskytu hrozby tento tým shromáždí informace od manažerů dotčených lokalit, provede jejich analýzu, informuje vrcholový management a následně zpracuje doporučení, která předá zpět na lokální úroveň. Na základě těchto doporučení pak místní vedení rozhoduje o dalším postupu. [65]

Výhodou tohoto přístupu je lepší koordinace napříč organizací a efektivnější zvládání bezpečnostních incidentů, zejména díky centralizovanému toku informací a jednotnému řízení. Nevýhodou může být závislost na jednom centrálním místě, neboť v případě jeho selhání může být ohrožen chod celé organizace. [65]

3.2.2 Decentralizovaný přístup k řízení bezpečnosti

Decentralizovaný přístup k řízení bezpečnosti je založen na principu rozdělení odpovědnosti za bezpečnost do jednotlivých částí organizace, obvykle na lokální nebo regionální úroveň. Týmy zodpovědné za bezpečnost působí samostatně v rámci konkrétních provozů, přičemž rozhodovací pravomoci zůstávají na místní úrovni. V rámci tohoto přístupu není přítomen centrální bezpečnostní útvar, který by měl výhradní odpovědnost za rozhodování. Klíčová rozhodnutí se proto zpravidla přijímají a realizují přímo na úrovni jednotlivých lokalit. [65]

Výhodou decentralizovaného přístupu je vysoká míra nezávislosti jednotlivých lokalit, která umožňuje vedoucím pracovníkům v oblasti bezpečnosti přijímat opatření s ohledem na místní podmínky a specifické potřeby jednotlivých poboček či regionů. Mezi nevýhody tohoto přístupu patří například riziko vzniku nekonzistencí v bezpečnostních opatřeních

napříč organizací, což může vést ke slabinám v celkové bezpečnostní úrovni organizace, nebo vyšší provozní náklady z důvodu, že každá oblast vyžaduje vlastní bezpečnostní personál a infrastrukturu. [65, 66]

3.2.3 Hybridní přístup k řízení bezpečnosti

Hybridní přístup k řízení bezpečnosti kombinuje centralizované řízení bezpečnosti s realizací bezpečnostních opatření na lokální úrovni. V rámci tohoto přístupu organizace využívá ústřední bezpečnostní centrum, které zajišťuje informační podporu a nastavuje bezpečnostní politiku na centrální úrovni, zatímco regionální a místní týmy realizují konkrétní opatření a ohlašují veškeré hrozby tomuto centru. Některé organizace provozují více bezpečnostních center v různých regionech, aby se vyhnuly závislosti na jednom bodu a minimalizovaly dopady případného selhání centrální infrastruktury. [66]

Výhodou hybridního přístupu je, že umožňuje jednotné řízení bezpečnosti v organizaci, přičemž zároveň ponechává prostor pro flexibilní reakce na lokální hrozby. Tento přístup je navíc dobře škálovatelný, což z něj činí vhodné řešení pro organizace s mezinárodní působností. Nevýhodou tohoto modelu může být vyšší náročnost na koordinaci mezi centrální a lokální úrovní řízení. [66]

3.3 Shrnutí kapitoly

Organizační struktura a zvolený přístup k řízení bezpečnosti ovlivňují celkové fungování organizace, včetně rozdělení odpovědnosti, koordinace jednotlivých činností a schopnosti reagovat na bezpečnostní hrozby.

V první části této kapitoly byly popsány základní typy organizačních struktur, konkrétně liniová, funkcionální, liniově-štábní, divizní a maticová. Tyto struktury se odlišují především způsobem rozdělení pravomocí a odpovědností, uspořádáním komunikačních a řídicích vazeb, mírou specializace jednotlivých útvarů a nastavením vztahů nadřízenosti a podřízenosti mezi pracovníky či útvary.

Ve druhé části kapitoly byly představeny tři základní druhy přístupů k řízení bezpečnosti – centralizovaný, decentralizovaný a hybridní. Každý z těchto přístupů se liší rozdělením odpovědností, rozhodovacích pravomocí a mírou koordinace bezpečnostních aktivit mezi centrální a lokální úrovní. Zatímco centralizovaný přístup klade důraz na jednotné řízení a kontrolu, decentralizovaný přístup umožňuje vyšší míru autonomie jednotlivých lokalit. Hybridní přístup pak představuje kompromis, kdy je na centrální úrovni

nastavována bezpečnostní politika a poskytována informační podpora, zatímco realizace konkrétních bezpečnostních opatření je ponechána na jednotlivých lokalitách s ohledem na jejich specifické podmínky.

PRAKTICKÁ ČÁST

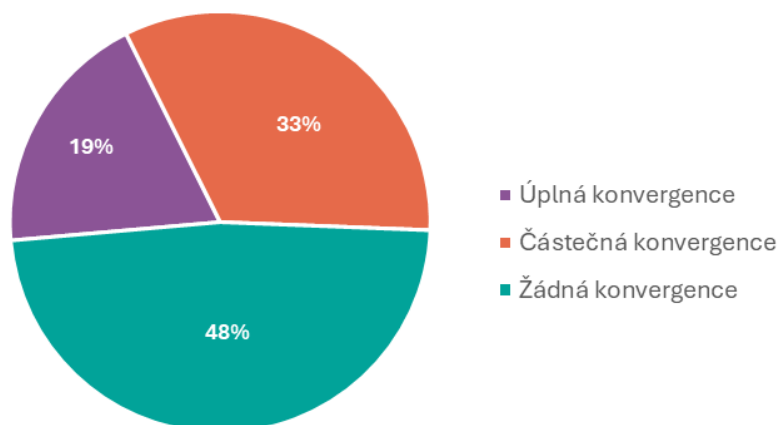
4 SOUČASNÝ STAV ŘÍZENÍ BEZPEČNOSTI V ORGANIZACÍCH

Bezpečnostní hrozby, kterým organizace v současnosti čelí, stále častěji překračují hranice jednotlivých druhů bezpečnosti a vyžadují koordinovaný přístup napříč celou strukturou firmy. Přesto v mnoha organizacích přetrvává oddělené řízení fyzické, kybernetické a provozní bezpečnosti. Tato kapitola analyzuje současné přístupy organizací k řízení bezpečnosti a prostřednictvím praktických příkladů ukazuje rizika spojená s odděleným fungováním fyzické, kybernetické a provozní bezpečnosti.

4.1 Analýza převládajících přístupů k řízení bezpečnosti

Jedním z významných témat současného řízení bezpečnosti v organizacích je způsob, jakým jsou spravovány jednotlivé oblasti bezpečnosti. Ačkoli odborná literatura i praxe stále častěji zdůrazňují potřebu konvergovaného řízení, tedy integrovaného a komplexního přístupu napříč všemi oblastmi, dostupné výzkumy naznačují, že v mnoha organizacích nadále převažuje oddělené uspořádání bez systematické koordinace.

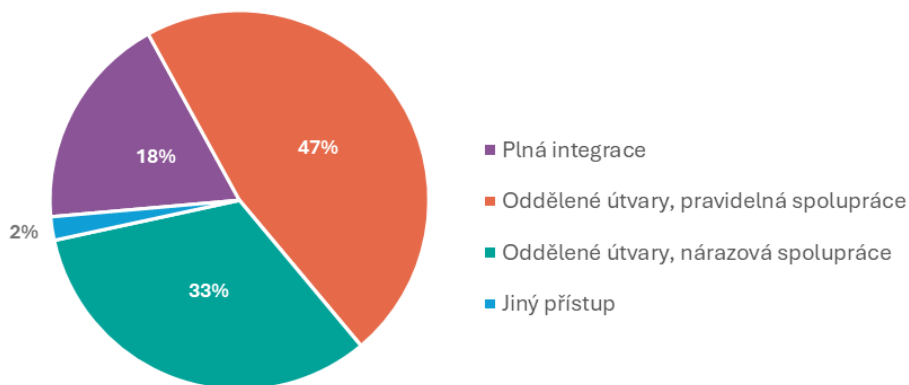
Touto problematikou se zabýval například výzkum organizace ASIS Foundation z roku 2019, který analyzoval odpovědi více než 1000 seniorních pracovníků z USA, Evropy a Indie působících v oblasti fyzické bezpečnosti, kybernetické bezpečnosti, provozní bezpečnosti a příbuzných oblastí. Výsledky tohoto šetření ukázaly, že pouze 19 % organizací mělo plně konvergované řízení bezpečnosti, které spojovalo fyzickou bezpečnost, kybernetickou bezpečnost a bezpečnost provozní. Dalších 5 % organizací mělo propojeno alespoň fyzickou a kybernetickou bezpečnost, 7 % alespoň kybernetickou a provozní bezpečnost a 21 % alespoň fyzickou a provozní bezpečnost. Souhrnně lze tedy říct, že alespoň částečnou formu konvergence vykazovalo 33 % respondentů. Naproti tomu 48 % organizací uvedlo, že mezi těmito oblastmi nemají zavedenou žádnou formu konvergence. Zároveň však 55 % z těchto organizací konstatovalo, že i přesto mezi jednotlivými oblastmi dochází alespoň k určité míře spolupráce či koordinace v otázkách bezpečnosti. [67]



Obrázek 9 Konvergence bezpečnosti
v organizacích - ASIS Foundation (2019)

(zdroj: [67])

Tématem konvergence bezpečnosti se zabýval také výzkum z roku 2022, publikovaný v roce 2024 v odborném časopise Information and Computer Security. Tento výzkum analyzoval přístupy 99 organizací ke konvergenci fyzické a kybernetické bezpečnosti. Studie ukázala, že pouze 18,4 % organizací mělo tyto oblasti integrovány v rámci jednoho organizačního útvaru (např. oddělení nebo divize). Největší část respondentů (46,9 %) uvedla, že oblasti fyzické a kybernetické bezpečnosti jsou sice organizačně oddělené, ale dochází mezi nimi k pravidelné spolupráci při řešení běžných operativních úkolů. Dalších 32,7 % organizací uvedlo, že tyto oblasti spolu standardně nespolupracují a k jejich koordinaci dochází pouze v případě potřeby. Zbylá 2 % respondentů uvedla jiný způsob řešení této problematiky. [68]



Obrázek 10 Konvergence fyzické a kybernetické bezpečnosti v organizacích - ICS (2024)

(zdroj: [68])

Ačkoli se oba výzkumy zaměřovaly na různé aspekty konvergence bezpečnosti, jejich výsledky se shodují v tom, že plná integrace fyzické, kybernetické a provozní bezpečnosti zatím nepředstavuje běžnou praxi v organizacích. Zatímco studie z roku 2019 zkoumala konvergenci všech tří oblastí, novější výzkum z roku 2022 se soustředil pouze na propojení fyzické a kybernetické bezpečnosti. Přestože tedy nelze jejich závěry plně srovnávat, v obou případech lze pozorovat určitou tendenci ke zvyšující se míře spolupráce mezi jednotlivými odděleními zodpovědnými za konkrétní oblasti bezpečnosti alespoň na operativní úrovni, což může svědčit o postupném posunu směrem ke konvergovanému modelu.

Za zmínku stojí rovněž skutečnost, že podle průzkumu z roku 2022 přechod k modelům řízení bezpečnosti v organizacích, založeným na plné integraci nebo užší spolupráci mezi jednotlivými oblastmi, zpravidla nevychází ze strategického rozhodnutí, ale má spíše reaktivní charakter. Podnětem k těmto změnám bývají nejčastěji bezpečnostní incidenty, změny ve vedení organizace nebo regulatorní požadavky. [68]

4.2 Rizika odděleného řízení bezpečnosti

Oddělené řízení fyzické, kybernetické a provozní bezpečnosti v organizaci může vytvářet slabiny, které zvyšují riziko vzniku bezpečnostních incidentů. Rizika spojená s nedostatečnou koordinací mezi těmito oblastmi ukazují následující příklady z praxe.

Kybernetický útok na společnost Maersk Line v roce 2017

V roce 2017 zasáhl logistickou společnost Maersk Line rozsáhlý ransomware útok známý jako NotPetya. Ransomware se rychle rozšířil napříč celou infrastrukturou společnosti, čímž ochromil přibližně 45 000 počítačů a 4 000 serverů. V důsledku útoku bylo uzavřeno 76 přístavních terminálů, přerušena činnost více než 800 lodí a došlo k narušení klíčových rezervačních systémů, což dočasně znemožnilo přijímat nové objednávky. Finanční škody společnosti přesáhly 300 milionů dolarů. [69]

Kybernetický útok na nemocnici v Benešově v roce 2019

V prosinci 2019 zasáhl IT systémy Nemocnice Rudolfa a Stefanie v Benešově rozsáhlý ransomware útok. Útočníci zašifrovali data na serverech, nemocničním vybavení a koncových stanicích, což znemožnilo poskytování standardní lékařské péče, vedlo ke zrušení plánovaných operací a vynutilo transport hospitalizovaných pacientů do jiných zařízení. Nemocnice byla nucena téměř na měsíc výrazně omezit provoz, přičemž celkové škody byly později vyčísleny na přibližně 59 milionů korun. [70, 71]

Zastavení vlakové dopravy v Dánsku v roce 2022

V roce 2022 došlo v Dánsku k incidentu, kdy byla na několik hodin zastavena veškerá doprava vlaků státního dopravce DSB. Příčinou výpadku nebyl přímý útok na DSB, ale hackerský útok na testovací prostředí platformy poskytující strojvedoucím klíčové provozní informace, například o rychlostních omezeních nebo stavebních pracích na trati. Po zjištění kompromitace subdodavatel odstavil své servery, což znemožnilo strojvedoucím bezpečně řídit vlaky a vedlo k úplnému zastavení železniční dopravy na několik hodin. [72, 73]

Případové studie ukazují, že nedostatečné propojení jednotlivých oblastí bezpečnosti a absence komplexních plánů pro zachování kontinuity provozu mohou vést k rozsáhlým škodám a vážnému narušení klíčových procesů organizací.

4.3 Shrnutí kapitoly

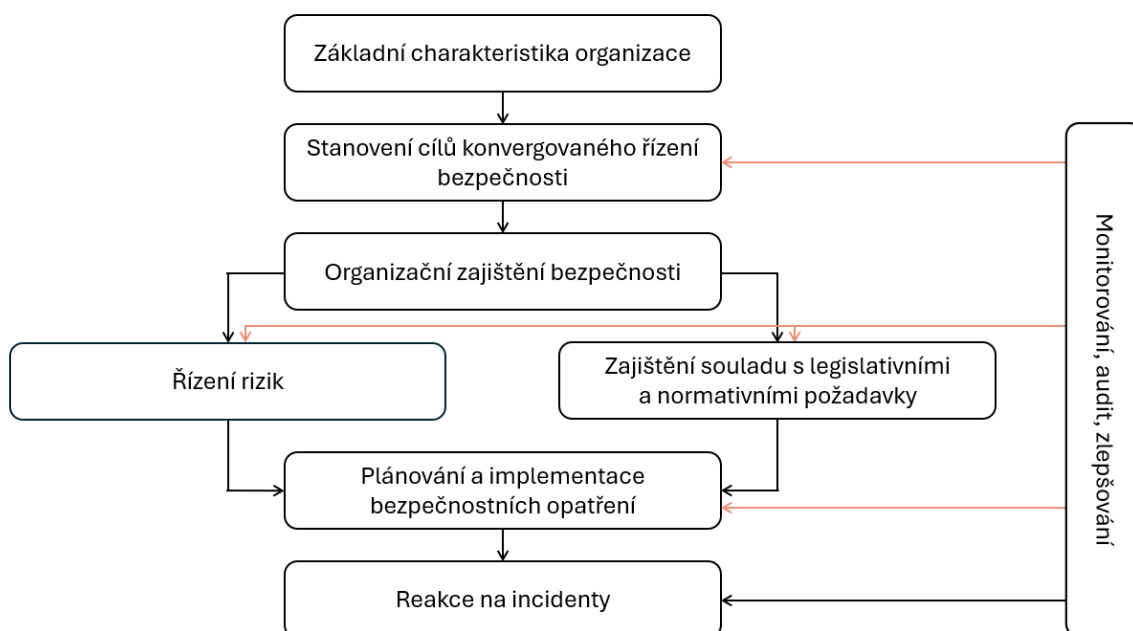
Ačkoli bezpečnostní praxe ukazuje, že efektivní řízení bezpečnosti vyžaduje komplexní a integrovaný přístup ke všem jejím oblastem, mnoho organizací nadále spravuje fyzickou, kybernetickou a provozní bezpečnost odděleně.

V první části kapitoly byly analyzovány dostupné výzkumy, které naznačují, že plně konvergované modely řízení bezpečnosti zatím nejsou běžnou praxí a oddělené řízení jednotlivých oblastí stále převažuje.

Druhá část kapitoly prostřednictvím příkladů z praxe ukázala, jak absence koordinace mezi jednotlivými oblastmi zvyšuje zranitelnost organizace a jaké dopady může mít na kontinuitu provozu. Uvedené příklady potvrzují, že pro posílení odolnosti organizace je nezbytné zajistit jednotné a koordinované řízení bezpečnosti napříč jejími jednotlivými oblastmi.

5 NÁVRH SYSTÉMU ŘÍZENÍ KONVERGOVANÉ BEZPEČNOSTI

Na základě analýzy současných přístupů k řízení bezpečnosti a příkladů demonstrujících důsledky odděleného řízení fyzické, kybernetické a provozní bezpečnosti je zřejmé, že efektivní konvergence těchto oblastí představuje zásadní předpoklad snižování bezpečnostních rizik, zajištění schopnosti organizace reagovat na mimořádné situace nebo udržení plynulosti provozu. Cílem této kapitoly proto bylo navrhnout metodicky členěný a prakticky využitelný systém řízení konvergované bezpečnosti, který bude použitelný napříč různými typy organizací a přizpůsobitelný jejich specifickým potřebám. Systém se skládá z osmi částí a princip jeho fungování je znázorněn na následujícím schématu (obr. 11).



Obrázek 11 Schéma systému řízení konvergované bezpečnosti

(zdroj: vlastní)

Výchozí částí systému je stanovení základních charakteristik organizace, mezi které patří například její velikost, oblast působnosti, organizační struktura nebo aktuální způsob zajištění bezpečnosti. Na základě těchto charakteristik jsou rozpracovány další části systému konvergovaného řízení bezpečnosti zahrnující stanovení bezpečnostních cílů, organizační zajištění bezpečnosti, řízení rizik, zohlednění legislativních a normativních požadavků a plánování a realizaci konkrétních bezpečnostních opatření. Tyto části zároveň slouží jako základ pro nastavení efektivního systému monitorování, auditu a zlepšování, který umožňuje průběžně vyhodnocovat stav systému a reagovat na změny v bezpečnostním prostředí.

Důležitou součástí systému je také schopnost organizace reagovat na incidenty, a to jak na základě předem nastavených postupů, tak s využitím informací získaných prostřednictvím monitoringu a auditu, které přispívají k jejich včasné detekci a efektivnímu řešení.

Následující kapitoly se věnují popisu jednotlivých částí systému.

5.1 Základní charakteristika organizace

Návrh systému řízení konvergované bezpečnosti by měl vždy vycházet z konkrétního prostředí organizace, v němž má být tento model uplatněn. Identifikace základních charakteristik organizace je nezbytným předpokladem pro navržení systému, který bude adekvátní jejím reálným potřebám i možnostem. Mezi tyto charakteristiky patří:

- oblast působnosti organizace,
- velikost organizace,
- počet a rozmístění provozoven,
- organizační struktura,
- stávající model řízení bezpečnosti,
- identifikace klíčových procesů,
- spolupráce s externími subjekty.

Uvedené informace tvoří výchozí rámec pro navržení konkrétní struktury řízení bezpečnosti zahrnující například určení odpovědností, analýzu a prioritizaci rizik, návrh vazeb mezi jednotlivými oblastmi bezpečnosti a identifikaci procesů vhodných k integraci či užší koordinaci.

5.2 Stanovení cílů konvergovaného řízení bezpečnosti

Systém řízení bezpečnosti v organizaci by měl být postaven na jasně definovaných cílech, které odráží její potřeby a specifika. V rámci konvergovaného přístupu je cílem vytvořit integrovaný, koordinovaný a efektivní systém, který:

- zajistí ochranu lidí, majetku, informací a dalších aktiv organizace,
- zajistí kontinuitu provozu v případě bezpečnostních incidentů různého rozsahu,
- propojí řízení rizik napříč fyzickou, kybernetickou a provozní bezpečností tak, aby mezi nimi existovala funkční provázanost,

- bude v souladu s legislativními a normativními požadavky vztahujícími se k činnosti organizace,
- umožní průběžné přizpůsobování bezpečnostních opatření v reakci na nové hrozby.

Tyto cíle, ve spojení s charakteristikami organizace definovanými v předchozí části, tvoří základ pro návrh konkrétních opatření, hodnocení účinnosti systému a jeho další rozvoj. Tyto cíle by měly být přijaty vedením organizace a promítnuty do všech úrovní jejího řízení.

5.3 Organizační zajištění bezpečnosti

Dalším klíčovým krokem při budování konvergovaného systému řízení bezpečnosti je jasné vymezení rolí, odpovědností a komunikačních vazeb mezi jednotlivými oblastmi. Vzhledem k tomu, že fyzická, kybernetická a provozní bezpečnost často spadají pod různá oddělení nebo úrovně řízení, je nezbytné vytvořit sjednocující rámec, který zajistí jejich koordinaci a provázanost.

Nezbytnou součástí tohoto rámce je určení odpovědné osoby nebo útvaru, který bude zajišťovat dohled nad řízením bezpečnosti jako celku. V menších organizacích může tuto roli plnit například bezpečnostní manažer, zatímco u větších firem může být vhodné vytvořit bezpečnostní štáb nebo pracovní skupinu složenou ze zástupců jednotlivých oblastí. I v případě kolektivního uspořádání je však vhodné určit jednoho koordinátora, který bude odpovědný za řízení činností skupiny a komunikaci s vrcholovým vedením.

Mezi pověřenými osobami nebo útvary by měly být formálně vymezeny odpovědnosti a kompetence. Zároveň je vhodné nastavit pravidelné komunikační kanály a mechanismy reportování, které umožní sdílení informací a koordinaci v případech, kdy incident v jedné oblasti může ovlivnit nebo narušit bezpečnost v oblasti jiné.

5.4 Řízení rizik

Efektivní řízení konvergované bezpečnosti v organizaci musí vycházet z komplexního a systematického řízení rizik napříč všemi bezpečnostními oblastmi. Tento přístup umožňuje odhalit nejen specifické hrozby v jednotlivých oblastech, ale také jejich vzájemné vazby a dopady na další oblasti bezpečnosti v rámci organizace.

Cílem fáze řízení rizik je vytvořit jednotný rámec, který zahrnuje:

- identifikaci aktiv (hmotných i nehmotných),

- hrozby a zranitelnosti v jednotlivých oblastech,
- dopady v primární i sekundární oblasti (např. kybernetické → provozní),
- vyhodnocení pravděpodobnosti a závažnosti dopadu,
- stanovení priorit k ošetření.

Organizace si mohou zvolit konkrétní metodiku posuzování rizik podle svých potřeb, (např. brainstorming, SWOT nebo FMEA), přičemž klíčové je, aby analýza zahrnovala všechny oblasti bezpečnosti a zohledňovala jejich vzájemné souvislosti.

Výstupem procesu řízení rizik by měl být katalog rizik, který nezahrnuje pouze jednotlivé hrozby, ale i jejich vzájemné vztahy mezi různými oblastmi bezpečnosti. Díky tomu lze navrhnout taková opatření, která účinně reagují na více typů rizik zároveň a umožňují koordinovaný přístup k jejich řešení.

5.5 Zajištění souladu s legislativními a normativními požadavky

Každý systém řízení bezpečnosti musí zohledňovat platné legislativní požadavky a zároveň by měl reflektovat i doporučené normativní standardy vztahující se k činnosti organizace. Ačkoli dodržování těchto standardů není právně závazné, v praxi bývá nezbytné – například jako podmínka pro získání pojistného plnění nebo při prokazování odpovídající úrovně zabezpečení vůči partnerům či zákazníkům.

Zajištění souladu by mělo být zohledněno jak při návrhu systému, tak i v průběhu jeho běžného fungování. Součástí bezpečnostního rámce by měl být proces pro sledování změn v legislativě a normách, jejich vyhodnocení a následná revize interních opatření včetně provádění pravidelných auditů souladu s aktuálními požadavky.

5.6 Plánování a implementace bezpečnostních opatření

Na základě výstupů z analýzy rizik je potřeba navrhnout a implementovat bezpečnostní opatření, která adresují identifikované hrozby a jejich možné dopady na ostatní oblasti bezpečnosti organizace. Tato opatření by zároveň měla být v souladu s příslušnými legislativními a normativními požadavky. Mohou mít technický, organizační nebo personální charakter.

Implementace opatření by měla probíhat jako strukturovaný proces s jasně stanovenými odpovědnostmi, harmonogramem, přidělenými zdroji a definovaným způsobem kontroly a vyhodnocení účinnosti přijatých opatření.

V rámci konvergovaného přístupu je důležité, aby byly jednotlivé oblasti bezpečnosti při plánování i realizaci opatření vzájemně koordinovány. Taková koordinace zajišťuje, že se opatření nebudou vzájemně rušit, ale budou fungovat jako jeden integrovaný celek.

5.7 Reakce na incidenty

Součástí efektivního systému řízení bezpečnosti musí být jasně definovaný proces pro detekci, hlášení a řešení bezpečnostních incidentů. V rámci konvergovaného přístupu je klíčové zajistit součinnost mezi jednotlivými oblastmi bezpečnosti, protože incident v jedné z nich může ovlivnit i ostatní.

Plán reakce na incidenty by měl zahrnovat:

- mechanismy pro včasné rozpoznání, hlášení a evidenci incidentů,
- rozdělení odpovědností mezi jednotlivé role při řešení incidentů,
- základní scénáře a postupy pro různé typy událostí,
- komunikační postupy pro interní i externí účely,
- způsob sdílení informací mezi útvary v případě incidentů s dopadem na více oblastí.

V některých typech organizací může být v návaznosti na vybrané typy incidentů žádoucí rovněž vypracovat plány kontinuity provozu, které definují postupy pro zajištění nebo obnovení klíčových procesů organizace v případě jejich narušení.

5.8 Monitorování, audit a zlepšování

Pro zajištění dlouhodobé funkčnosti celého systému je nezbytné jeho průběžné vyhodnocování a přizpůsobování aktuálním podmínkám a požadavkům. Monitorování, audit a zlepšování tak představují nedílnou součást konvergovaného přístupu k řízení bezpečnosti.

Součástí monitorování by mělo být sledování klíčových ukazatelů výkonnosti (KPI) a klíčových ukazatelů rizik (KRI). KPI slouží k hodnocení efektivity přijatých opatření a fungování systému řízení bezpečnosti, mezi které patří například průměrná doba reakce na incident, počet absolvovaných školení nebo četnost provádění interních auditů. Naopak KRI se zaměřují na indikaci vývoje rizik a potenciálních hrozeb zahrnujících například nárůst počtu zjištěných zranitelností, četnost pokusů o neautorizovaný přístup nebo opakovaný výskyt incidentů ve specifické oblasti. Správně nastavené ukazatele poskytují organizaci

zpětnou vazbu jak o účinnosti systému, tak o měnícím se bezpečnostním prostředí a napomáhají včas odhalit nedostatky v systému či vznikající rizika.

Pravidelnou součástí systému by měly být také bezpečnostní audity, ať už vykonávané interními nebo externími subjekty. Ty by měly pokrývat všechny oblasti bezpečnosti i jejich vzájemné vazby. Zjištěné nedostatky by měly vést k návrhům nápravných opatření.

Na základě výstupů z monitorování, auditů, analýz incidentů, legislativních změn nebo aktuálních potřeb organizace by měl být celý systém řízení bezpečnosti průběžně aktualizován a zlepšován.

5.9 Shrnutí kapitoly

V rámci této kapitoly byl představen modelový systém řízení konvergované bezpečnosti, jehož cílem je poskytnout strukturovaný rámec pro koordinovaný a integrovaný přístup k řízení fyzické, kybernetické a provozní bezpečnosti v organizaci.

Systém je tvořen několika vzájemně propojenými částmi – od vymezení základních charakteristik organizace a stanovení bezpečnostních cílů, přes organizační zajištění, řízení rizik a zajištění souladu s legislativními a normativními požadavky, až po plánování a implementaci bezpečnostních opatření, reakci na incidenty a procesy monitorování, auditu a zlepšování systému.

Navržený model slouží jako obecný rámec, který může být přizpůsoben různým typům organizací a využit jako základ pro zavádění systému řízení konvergované bezpečnosti a jeho následný provoz.

6 APLIKACE SYSTÉMU ŘÍZENÍ KONVERGOVANÉ BEZPEČNOSTI NA MODELOVÉ ORGANIZACI

V této kapitole je návrh systému řízení konvergované bezpečnosti uvedený v předchozí části aplikován na modelovou logistickou organizaci. Jednotlivé prvky systému jsou přizpůsobeny jejím specifickým podmínkám, struktuře a provoznímu prostředí.

6.1 Základní charakteristika organizace

Modelová organizace, na kterou je v této části aplikován návrh systému řízení konvergované bezpečnosti, je středně velká logistická firma zaměřující se na vnitrostátní i mezinárodní přepravu a skladování zboží. Společnost sídlí na okraji většího města, kde provozuje vlastní areál zahrnující administrativní budovu, skladové prostory a menší servisní zázemí.

Organizace zaměstnává přibližně 200 osob, přičemž značná část zaměstnanců pracuje jako řidiči, skladníci nebo dispečeri. Kromě toho firma zahrnuje administrativní, obchodní a technické oddělení, které zajišťují například řízení zakázek, komunikaci se zákazníky a správu informačních systémů. Ostatní útvary pracují v denním režimu s pevně stanovenou pracovní dobou.

Organizace má funkcionální organizační strukturu, která zahrnuje čtyři hlavní oblasti: provoz (sklad, doprava a dispečink), administrativu, obchod a IT. Řízení firmy zajišťuje úzký management v čele s jednatelem společnosti. Jednotlivé útvary jsou vedeny odpovědnými vedoucími a klíčová rozhodnutí jsou centralizována na úrovni vedení firmy.

Klíčové procesy organizace zahrnují:

- příjem, skladování a expedici zásilek,
- plánování přepravy a komunikace se řidiči,
- komunikaci se zákazníky,
- správu vozového parku a monitoring zásilek v reálném čase.

Organizace má vlastní IT infrastrukturu zahrnující interní síť, uživatelská zařízení, přístupové systémy a základní IT podporu. Pro řízení provozu využívá softwarové nástroje, jako je skladový systém, dispečerská platforma a zákaznický portál, které jsou provozovány formou cloudových služeb nebo spravovány externími dodavateli. Z hlediska fyzické bezpečnosti spravuje zabezpečený areál s kontrolou vstupu, kamerovým systémem

a ostrahou. Organizace zároveň spolupracuje s dalšími partnery, například se smluvními dopravci nebo dodavateli technologií.

V současné době je řízení bezpečnosti v organizaci řešeno odděleně v jednotlivých oblastech. Fyzická bezpečnost spadá pod správu areálu, kybernetická bezpečnost je v kompetenci IT správce a provozní bezpečnost spadá do odpovědnosti vedoucích provozních pracovníků. Neexistuje centrální role ani jednotný systém, který by zajišťoval koordinaci bezpečnostních opatření napříč těmito oblastmi.

6.2 Stanovení cílů konvergovaného řízení bezpečnosti

Cílem konvergovaného systému řízení bezpečnosti v modelové organizaci je vytvoření jednotného a koordinovaného přístupu k zajištění ochrany klíčových aktiv, plynulého provozu a schopnosti organizace reagovat na incidenty napříč různými oblastmi bezpečnosti. Vzhledem k provoznímu charakteru firmy, jejímu technologickému zázemí a zapojení externích subjektů je nezbytné, aby byly bezpečnostní mechanismy mezi jednotlivými oblastmi vzájemně provázané.

Hlavními cíli konvergovaného systému řízení bezpečnosti jsou:

- ochránit zaměstnance, zboží, vozidla, IT systémy i data zákazníků,
- sjednotit odpovědnosti a zjednodušit řízení bezpečnosti ve firmě,
- rychleji a efektivněji řešit krizové situace,
- získat lepší přehled o rizicích a tím nad nimi dosáhnout větší kontroly,
- plnit požadavky norem, zákonů i smluvních partnerů.

6.3 Organizační zajištění bezpečnosti

Aby bylo možné řídit bezpečnost v organizaci jako jeden celek, je nutné jasně rozdělit odpovědnosti a nastavit systém spolupráce mezi jednotlivými oblastmi. V rámci navrženého modelu bude za řízení konvergované bezpečnosti odpovědný bezpečnostní koordinátor, který bude přímo podřízen vedení firmy.

Tento koordinátor bude mít na starost celkový dohled nad bezpečností, koordinaci mezi oblastmi (fyzická, kybernetická a provozní bezpečnost), zajištění spolupráce s externími partnery a přípravu pravidelných zpráv pro vedení firmy. V rámci středně velké firmy může

tuto roli zastávat stávající zaměstnanec s odpovídajícími znalostmi a zkušenostmi, aniž by bylo nutné zřizovat novou pracovní pozici.

Primární odpovědnost za jednotlivé oblasti bezpečnosti bude ponechána v kompetenci pracovníků, kteří je doposud zajišťovali:

- fyzickou bezpečnost bude nadále řešit správce areálu ve spolupráci s ostrahou,
- kybernetickou bezpečnost bude mít na starosti IT správce,
- provozní bezpečnost zůstane v kompetenci vedoucích provozů (sklad, dispečink).

Mezi těmito osobami bude zřízena bezpečnostní pracovní skupina, která se bude pravidelně scházet, řešit aktuální hrozby, navrhopat opatření a hodnotit účinnost systému. Koordinátor bude zodpovědný za to, aby informace mezi jednotlivými oblastmi byly předávány efektivně a včas.

6.4 Řízení rizik

Modelová organizace disponuje řadou aktiv, jejichž ohrožení může ovlivnit plynulost provozu, bezpečnost zaměstnanců, zboží i informačních systémů. Rizika se mohou týkat jednotlivých oblastí bezpečnosti samostatně, ale často mají i vzájemné přesahy.

Řízení rizik proto tvoří jednu ze základních součástí systému konvergované bezpečnosti a zahrnuje jak samostatná rizika v jednotlivých oblastech, tak i rizika, která mohou zasahovat napříč více oblastmi současně.

Pro jejich identifikaci a hodnocení organizace využívá jednoduchý rámec založený na expertním posouzení a slovním škálování. Každé riziko je posuzováno z hlediska pravděpodobnosti výskytu a závažnosti dopadu. Obě hodnoty jsou klasifikovány na škále nízká – střední – vysoká, přičemž výsledná míra rizika je určena jejich kombinací dle následující matice (tab. 1).

Tabulka 1 Matice pro hodnocení míry rizika

	Nízký dopad	Střední dopad	Vysoký dopad
Nízká pravděpodobnost	Nízké	Nízké	Střední
Střední pravděpodobnost	Nízké	Střední	Vysoké
Vysoká pravděpodobnost	Střední	Vysoké	Vysoké

(zdroj: vlastní)

Na základě uvedeného přístupu byla pro účely návrhu vybrána tři klíčová aktiva stěžejní pro provoz organizace, jejichž ohrožení má potenciál zasahovat více oblastí bezpečnosti. Přehled těchto aktiv, včetně výběru souvisejících hrozeb, zranitelností, pravděpodobnosti výskytu, závažnosti dopadu, výsledné míry rizika a přesahů mezi oblastmi bezpečnosti, ilustruje následující tabulka.

Tabulka 2 Přehled vybraných aktiv, souvisejících hrozeb a hodnocení rizik pro modelovou organizaci

Aktivum	Hrozba	Zranitelnost	Pravděpodobnost	Dopad	Riziko	Mezioblastní přesah
Přepravní vozidla	Dopravní nehoda	Nevyhovující technický stav vozidla, únava řidiče	Nízká	Vysoký	Střední	Provozní → fyzická
	Krádež nákladu z vozidla	Parkování mimo zabezpečené prostory, nedostatečné fyzické zabezpečení ložného prostoru	Nízká	Vysoký	Střední	Fyzická → provozní
Dispečerský systém	Kybernetický útok	Slabé zabezpečení, neaktuální software	Střední	Vysoký	Vysoké	Kybernetická → provozní
	Výpadek systému	Nedostatečné zálohování, poruchy infrastruktury	Střední	Vysoký	Vysoké	Kybernetická → provozní
Skladové prostory	Požár	Chybějící nebo nefunkční detektory kouře, neoznačené únikové cesty a absence pravidelné kontroly evakuačních postupů	Nízká	Vysoký	Střední	Fyzická → provozní
	Vloupání	Nedostatečně zabezpečený obvod areálu, nedostatečné pokrytí areálu zabezpečovacími systémy	Střední	Střední	Střední	Fyzická → provozní

(zdroj: vlastní)

Uvedená tabulka představuje zjednodušený přehled vybraných aktiv modelové organizace, u nichž byly analyzovány konkrétní bezpečnostní hrozby a z nich vyplývající rizika. Výběr slouží k ilustraci principu konvergovaného řízení rizik – tedy situací, kdy ohrožení jednoho aktiva může mít dopad ve více oblastech bezpečnosti. I v tomto omezeném vzorku je patrné, že narušení aktiva v jedné oblasti může významně ovlivnit i oblast jinou. Tabulka zároveň plní funkci zjednodušeného katalogu rizik, který shrnuje vybraná aktiva, jejich hrozby, zranitelnosti, hodnocení rizik a mezioblastní přesahy v rámci konvergovaného přístupu.

6.5 Zajištění souladu s legislativními a normativními požadavky

Před návrhem konkrétních bezpečnostních opatření je důležité zohlednit také legislativní požadavky a normativní standardy, které mohou ovlivnit podobu a rozsah navrhovaných řešení. Tyto předpisy v některých oblastech organizace stanovují závazné povinnosti, jinde nabízejí doporučený rámec pro nastavení bezpečnostních procesů. Následující tabulky uvádějí vybrané legislativní předpisy a normativní standardy rozdělené podle oblastí bezpečnosti, kterých se v rámci organizace týkají.

Tabulka 3 Přehled vybraných legislativních předpisů pro modelovou organizaci

Oblast bezpečnosti	Legislativní předpis
Fyzická bezpečnost	Zákon č. 133/1985 Sb. o požární ochraně
	Vyhláška č. 23/2008 Sb. o technických podmínkách požární ochrany staveb
Kybernetická bezpečnost	Nařízení (EU) 2016/679 (GDPR)
	Zákon č. 110/2019 Sb. o zpracování osobních údajů
Provozní bezpečnost	Zákon č. 361/2000 Sb. o silničním provozu
	Zákon č. 262/2006 Sb. (zákoník práce)

(zdroj: vlastní)

Tabulka 4 Přehled vybraných normativních standardů pro modelovou organizaci

Oblast bezpečnosti	Norma
Fyzická bezpečnost	EN 50131: Elektronické zabezpečovací systémy
	EN 60839: Elektronické systémy kontroly vstupu
	EN 62676: Dohledové videosystémy pro použití v bezpečnostních aplikacích
Kybernetická bezpečnost	ISO 27001: Systémy managementu informační bezpečnosti
Provozní bezpečnost	ISO 45001: Systémy managementu bezpečnosti a ochrany zdraví při práci
	ISO 22301: Systémy managementu kontinuity podnikání

(zdroj: vlastní)

Zajištění souladu s legislativními a normativními předpisy by však nemělo být jednorázovou aktivitou – organizace by měla průběžně sledovat změny v relevantních právních předpisech a normách, vyhodnocovat jejich dopad a podle potřeby na ně reagovat. Tuto činnost by měla v rámci modelové organizace koordinovat bezpečnostní pracovní skupina, případně přímo pověřený bezpečnostní koordinátor.

6.6 Plánování a implementace bezpečnostních opatření

Na základě identifikovaných rizik a přehledu legislativních požadavků a norem byla navržena vybraná bezpečnostní opatření reagující na hrozby uvedené v kapitole 6.4. Jejich cílem je snížit pravděpodobnost výskytu těchto hrozeb, zmírnit jejich dopady nebo posílit celkovou odolnost organizace. Přehled navržených opatření je uveden v následující tabulce, přičemž pro každou z vybraných hrozeb je uvedeno odpovídající opatření, jeho typ a případná vazba na konkrétní legislativní nebo normativní dokument.

Tabulka 5 Přehled vybraných bezpečnostních opatření pro modelovou organizaci

Aktivum	Hrozba	Opatření	Typ	Vazba na předpis / normu
Přepavní vozidla	Dopravní nehoda	Zavedení pravidelného školení řidičů a vedení evidence o jeho absolvování	Personální	Zákon č. 262/2006 Sb.
	Krádež nákladu z vozidla	Používání bezpečnostních plomb, vytipování rizikových tras, školení řidičů o postupu v terénu	Organizační	Interní směrnice
Dispečerský systém	Kybernetický útok	Zavedení dvoufaktorové autentizace, pravidelná aktualizace systému	Technické	Nařízení (EU) 2016/679, Zákon č. 110/2019 Sb.
	Výpadek systému	Zavedení pravidelného zálohování a testování obnovitelnosti dat	Organizační	ISO 27001
Skladové prostory	Požár	Instalace detektorů kouře, kontrola únikových cest a revize požárních směrnic	Technické / organizační	Zákon č. 133/1985 Sb., Vyhláška č. 23/2008 Sb.
	Vloupání	Posílení fyzického zabezpečení perimetru (ploty, brány), rozšíření kamerového systému	Technické	EN 50131, EN 62676

(zdroj: vlastní)

Implementace opatření by měla probíhat v rámci strukturovaného procesu, který zahrnuje určení odpovědných osob, stanovení časového harmonogramu, přidělení zdrojů a nastavení kontrolních mechanismů pro vyhodnocování účinnosti. V rámci konvergovaného přístupu je důraz kladen na vzájemnou koordinaci jednotlivých oblastí, aby opatření nepůsobila izolovaně, ale přispívala ke zvýšení celkové bezpečnostní úrovně organizace.

6.7 Reakce na incidenty

V rámci modelové organizace mohou nastat incidenty různé povahy. V oblasti kybernetické bezpečnosti může jít například o výpadek dispečerského systému nebo pokus o neoprávněný přístup, v oblasti fyzické bezpečnosti o vloupání do areálu nebo požár a v oblasti provozní bezpečnosti například o dopravní nehodu nebo nehodu ve skladu. Vzhledem k tomu, že některé z těchto událostí mohou mít dopad na více oblastí současně, je vhodné stanovit jednotný rámec pro jejich detekci, řešení a zpětné vyhodnocení.

Navržený rámec pro reakci na incidenty v této organizaci by měl zahrnovat zavedení jednotného mechanismu evidence incidentů, například prostřednictvím interního elektronického formuláře dostupného odpovědným osobám. Odpovědnost za řešení incidentů by měla být rozdělena podle oblasti – za incidenty fyzické bezpečnosti by měl odpovídat správce areálu ve spolupráci s ostrahou, za incidenty kybernetické bezpečnosti IT správce a za incidenty provozní bezpečnosti vedoucí příslušného provozu (např. dispečinku nebo skladu).

V případě incidentů s přesahem do více oblastí by měly být odpovědné osoby povinny informovat bezpečnostního koordinátora, který bude zajišťovat součinnost mezi oblastmi a připravovat souhrnné přehledy o incidentech pro vedení organizace.

Pro vybrané typy incidentů, jako je výpadek systému nebo pokus o neoprávněný přístup, by měly být zpracovány stručné postupy, které stanoví jednotlivé kroky od zachycení události až po informování příslušných útvarů a případné zahájení eskalace. Součástí těchto postupů by měly být také nouzové kontakty pro případy, kdy některý z odpovědných pracovníků nebude aktuálně dostupný, například mimo běžnou pracovní dobu.

Incidenty by měly být pravidelně vyhodnocovány bezpečnostní pracovní skupinou, která zároveň navrhuje úpravy v opatřeních i postupech.

6.8 Monitorování, audit a zlepšování

Aby byl systém konvergované bezpečnosti dlouhodobě funkční, je nezbytné, aby byl průběžně monitorován, vyhodnocován a aktualizován. Tento přístup umožňuje včas identifikovat slabá místa, reagovat na měnící se bezpečnostní rizika a zajistit, že přijatá opatření zůstávají účinná a přiměřená aktuálním podmínkám.

Součástí monitorování v rámci modelové organizace je sledování klíčových ukazatelů výkonnosti systému (KPI) a klíčových ukazatelů rizik (KRI). Tyto metriky poskytují vedení i odpovědným pracovníkům důležitou zpětnou vazbu o tom, jak bezpečnostní systém funguje v praxi. Příklad konkrétních ukazatelů je uveden v následující tabulce.

Tabulka 6 Přehled vybraných KPI a KRI pro modelovou organizaci

Typ ukazatele	Ukazatel	Význam
KPI	Průměrná doba vyřešení incidentu	Sleduje efektivitu reakce na incidenty a schopnost organizace je vyřešit přiměřeném čase.
KPI	Frekvence testování schopnosti obnovy dispečerského systému včetně vyhodnocení výsledků	Odráží úroveň připravenosti na výpadky klíčového IT systému a schopnost obnovit provoz.
KPI	Počet absolvovaných školení BOZP za určité období	Sleduje úroveň proškolení zaměstnanců a naplnění požadavků v oblasti bezpečnosti práce.
KRI	Počet opakovaných výpadků dispečerského systému za určité období	Signalizuje technickou zranitelnost a potenciální selhání klíčového systému s dopadem na provoz.
KRI	Počet pracovních úrazů za určité období	Indikuje možné nedostatky v oblasti bezpečnosti a ochrany zdraví při práci.
KRI	Počet incidentů s dopadem do více oblastí bezpečnosti za určité období	Upozorňuje na slabiny v koordinaci mezi oblastmi bezpečnosti.

(zdroj: vlastní)

Organizace by měla pravidelně provádět bezpečnostní audity, které mohou být realizovány jak interně bezpečnostní pracovní skupinou, tak externími subjekty. Audity by měly zahrnovat nejen jednotlivé oblasti bezpečnosti, ale i jejich vzájemné vazby a úroveň celkové koordinace. Výsledky auditů slouží jako podklad pro návrh nápravných a preventivních opatření.

Na základě výsledků z monitorování, auditů, vyhodnocení incidentů, změn v legislativě a změn v provozním prostředí by měl být systém bezpečnosti průběžně aktualizován a zlepšován. Tuto činnost by měla provádět bezpečnostní pracovní skupina pod vedením

koordinátora, který zároveň připravuje souhrnné zprávy o stavu bezpečnosti a návrhy změn pro vedení firmy.

6.9 Shrnutí kapitoly

Tato kapitola se zabývala aplikací obecného návrhu systému řízení konvergované bezpečnosti na konkrétní modelovou organizaci – středně velkou logistickou firmu se zaměřením na přepravu a skladování zboží.

V rámci této aplikace byly stanoveny bezpečnostní cíle, zavedena role bezpečnostního koordinátora, vytvořena pracovní skupina složená ze zástupců jednotlivých oblastí bezpečnosti, vymezeny odpovědnosti a nastaven způsob spolupráce mezi útvary. Součástí řešení bylo také vyhodnocení rizik na základě vybraných aktiv, identifikace souvisejících hrozeb a posouzení pravděpodobnosti jejich výskytu i závažnosti dopadu. Na základě výsledků této analýzy byla navržena bezpečnostní opatření, která reagují na identifikované hrozby a jsou rámcově navázána na příslušné právní a normativní požadavky.

V neposlední řadě bylo v kapitole demonstrováno, jak může organizace prostřednictvím jednotného rámce reagovat na incidenty a jak lze nastavit procesy monitorování, auditů a zlepšování, včetně stanovení klíčových ukazatelů a rizik.

ZÁVĚR

Cílem této diplomové práce bylo vysvětlit pojem konvergovaná bezpečnost, popsat její klíčové oblasti a navrhnout systém řízení konvergované bezpečnosti včetně jeho aplikace na modelovou organizaci.

Teoretická část práce se věnovala vymezení pojmu konvergovaná bezpečnost, charakteristice jednotlivých oblastí bezpečnosti (fyzické, kybernetické, informační a provozní), přehledu legislativních a normativních požadavků, typům organizačních struktur a přístupům k řízení bezpečnosti v organizacích, zejména z hlediska míry centralizace.

Praktická část práce navázala analýzou převládajících přístupů k řízení bezpečnosti a jejich limitů v reálném prostředí. Následně byl zpracován návrh systému řízení konvergované bezpečnosti, který byl dále aplikován na fiktivní logistickou organizaci. Součástí tohoto návrhu bylo nastavení odpovědností v rámci systému řízení konvergované bezpečnosti, návrh bezpečnostních opatření pro vybrané hrozby, definování rámce reakce na incidenty, návrh postupu řízení rizik a nastavení procesů monitorování a zlepšování systému včetně stanovení klíčových ukazatelů výkonnosti a rizik.

Výstupem práce je ucelený návrh systému, který může sloužit jako základ pro zavedení konvergovaného přístupu k řízení bezpečnosti v menších až středně velkých organizacích. Přestože některé části modelu byly zpracovány pouze rámcově, jeho struktura poskytuje dostatečný základ pro další rozpracování podle specifických potřeb konkrétní organizace.

SEZNAM POUŽITÉ LITERATURY

- [1] LUDĚK, Lukáš a kolektiv. *Konvergovaná bezpečnost*. Zlín: VeRBuM, 2019. ISBN 978-80-87500-99-6.
- [2] KOTKOVÁ, Dora. *Režimová opatření*. Zlín: Univerzita Tomáše Bati ve Zlíně. 2020
- [3] LUKÁŠ, Luděk a kolektiv. *Bezpečnostní technologie, systémy a management I*. Zlín: VeRBuM, 2011. ISBN 978-80-87500-05-7.
- [4] *Vandalismus*. Online. Ministerstvo školství, mládeže a tělovýchovy České republiky. 2017. Dostupné z: https://msmt.gov.cz/uploads/Priloha_c._10_Vandalismus.docx. [cit. 2025-02-15].
- [5] ČESKO. Vyhláška Ministerstva vnitra č. 21 ze dne 11. ledna 1996, kterou se provádějí některá ustanovení zákona České národní rady o požární ochraně. Online. In: *Zákony pro lidi*. 2010–2025. Dostupné z: <https://www.zakonyprolidi.cz/cs/1996-21>. [cit. 2025-02-15].
- [6] GOGELA, Robert. *Standardy a definice pojmů bezpečnosti informací*. Online. CyberSecurity.CZ. [2025]. Dostupné z: <https://www.cybersecurity.cz/data/gogela.pdf>. [cit. 2025-02-16].
- [7] *Co je CIA triáda informační bezpečnosti*. Online. Aptien: Usnadněte si řízení provozu a administrativy firmy. 2025. Dostupné z: <https://aptien.com/cs/kb/articles/what-is-cia-triad#article-title>. [cit. 2025-02-16].
- [8] *What is the CIA Triad in Cyber Security?* Online. Threatscape: Cyber Security That Performs at Scale. C2024. Dostupné z: <https://www.threatscape.com/cyber-security-blog/understanding-the-cia-triad-in-cyber-security/>. [cit. 2025-02-16].
- [9] SALHI, Hatem. *Catalogue of threats & vulnerabilities*. Online. LinkedIn. 2016. Dostupné z: <https://www.linkedin.com/pulse/catalogue-threats-vulnerabilities-hatem-salhi/>. [cit. 2025-02-17].
- [10] *Unauthorized access*. Online. National Institute of Standards and Technology. [2025]. Dostupné z: https://csrc.nist.gov/glossary/term/unauthorized_access. [cit. 2025-02-17].
- [11] *Information leakage*. Online. National Institute of Standards and Technology. [2025]. Dostupné z: https://csrc.nist.gov/glossary/term/information_leakage. [cit. 2025-02-17].

- [12] *Data Loss: Overview, Causes and Implications, How To Prevent*. Online. Corporate Finance Institute. C2015-2025. Dostupné z: <https://corporatefinanceinstitute.com/resources/data-science/data-loss/>. [cit. 2025-02-18].
- [13] DHAKE, Tejas. *What is Data Tampering? Meaning, Types, Countermeasures*. Online. Business Louder. C2025. Dostupné z: <https://businesslouder.com/what-is-data-tampering/>. [cit. 2025-02-18].
- [14] KENTON, Will. *Industrial Espionage: Definition, Examples, Types, Legality*. Online. Investopedia. 2022. Dostupné z: <https://www.investopedia.com/terms/i/industrial-espionage.asp>. [cit. 2025-02-18].
- [15] KENTON, Will. *Confidentiality Agreement: Definition, Purpose, and Elements*. Online. Investopedia. 2024. Dostupné z: https://www.investopedia.com/terms/c/confidentiality_agreement.asp. [cit. 2025-02-18].
- [16] *What is Information Security*. Online. Aptien: Work management software for small and medium businesses. 2025. Dostupné z: <https://aptien.com/en/kb/articles/what-is-information-security>. [cit. 2025-02-18].
- [17] *What Is Social Engineering? Definition, Types & More*. Online. Proofpoint US: Enterprise Cybersecurity Solutions, Services & Training. C2025. Dostupné z: <https://www.proofpoint.com/us/threat-reference/social-engineering>. [cit. 2025-02-18].
- [18] *What is Cybersecurity?*. Online. Cybersecurity and Infrastructure Security Agency. 2021. Dostupné z: <https://www.cisa.gov/news-events/news/what-cybersecurity>. [cit. 2025-02-18].
- [19] *Kybernetická a informační bezpečnost. Legislativa, povinnosti, útoky*. Online. Bezpečnostprace.info: Portál o bezpečnosti práce (BOZP) a požární ochraně (PO). 2021. Dostupné z: <https://www.bezpecnostprace.info/kybernetika-informace/kyberneticka-bezpecnost-legislativa-povinnost>. [cit. 2025-02-18].
- [20] *Prováděcí nařízení k NIS2 je tady*. Online. Národní úřad pro kybernetickou a informační bezpečnost. 2024. Dostupné z:

<https://nukib.gov.cz/cs/infoservis/aktuality/2181-provadeci-narizeni-k-nis2-je-tady/>.
[cit. 2025-03-01].

- [21] MAHN, Amy; MARRON, Jeffrey a QUINN, Stephen. Getting Started with the NIST Cybersecurity Framework: A Quick Start Guide. *NIST Special Publication*. 2021, č. 1271. Dostupné z: <https://doi.org/https://doi.org/10.6028/NIST.SP.1271>. [cit. 2025-03-01].
- [22] BAKER, Kurt. *12 Most Common Types of Cyberattacks*. Online. CrowdStrike: We Stop Breaches with AI-native Cybersecurity. 2024. Dostupné z: <https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/common-cyberattacks/>. [cit. 2025-03-06].
- [23] JOBOY, Joyson. *Cyber Attacks and Countermeasures*. Online. LinkedIn. 2024. Dostupné z: <https://www.linkedin.com/pulse/cyber-attacks-countermeasures-joyson-joboy-pxtve/>. [cit. 2025-03-06].
- [24] LENAERTS-BERGMANS, Bart. *What Is an Injection Attack?*. Online. CrowdStrike: We Stop Breaches with AI-native Cybersecurity. 2024. Dostupné z: <https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/injection-attack/>. [cit. 2025-03-06].
- [25] *Business Continuity Incident Examples*. Online. Continuity2: Business Continuity Management Software. 2023. Dostupné z: <https://continuity2.com/blog/business-continuity-incident-examples>. [cit. 2025-03-08].
- [26] *Business Continuity: How to Mitigate the Risk of Human Error*. Online. Crises Control. 2023. Dostupné z: <https://www.crises-control.com/blogs/business-continuity-human-error/>. [cit. 2025-03-08].
- [27] DRUCKER, Phyllis. *What is a Business Continuity Management System?*. Online. ITChronicles. 2024. Dostupné z: <https://itchronicles.com/business-continuity/business-continuity-management-system/>. [cit. 2025-03-08].
- [28] 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 zrušení směrnice (EU) 2016/1148 (směrnice NIS2). *Úřední věstník Evropské unie*, L 333, 27. 12. 2022, s. 80–152. Dostupné z: <https://eur->

- lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32022L2555. [cit. 2025-03-09].
- [29] KUDEĚLKA, Tomáš a KÜHNEROVÁ, Eliška. *NIS 2: Na koho dopadá a jaké povinnosti ukládá?*. Online. KPMG Česká republika: Služby v oblasti auditu, daní, poradenství a práva. C2025. Dostupné také z: <https://kpmg.com/cz/cs/home/clanky-a-analyzy/2023/04/nis-2-na-koho-dopada-povinnosti.html>. [cit. 2025-03-09]
- [30] SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2022/2557 ze dne 14. prosince 2022 o odolnosti kritických subjektů a o zrušení směrnice Rady 2008/114/ES. *Úřední věstník Evropské unie*, L 333, 27. 12. 2022, s. 164–198. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32022L2557>. [cit. 2025-03-09].
- [31] PŘIBYLOVÁ SAXLOVÁ, Jaroslava. *Směrnice CER přináší novou regulaci pro oblast kritické infrastruktury*. Online. Advokátní kancelář Chreněk, Toman, Kotrba. 2023. Dostupné z: <https://www.chrenektomankotrba.cz/clanky/smernice-cer-prinasi-novou-regulaci-pro-oblast-kriticke-infrastruktury>. [cit. 2025-03-09].
- [32] 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 (nařízení o digitální provozní odolnosti – DORA). *Úřední věstník Evropské unie*, L 333, 27. 12. 2022, s. 1–84. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32022R2554>. [cit. 2025-03-09].
- [33] *DORA: Digitální provozní odolnost finančního trhu*. Online. Česká národní banka. C2025. Dostupné z: <https://www.cnb.cz/cs/dohled-financni-trh/dora-digitalni-provozni-odolnost-financniho-trhu/>. [cit. 2025-03-09].
- [34] SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (obecné nařízení o ochraně osobních údajů, GDPR). *Úřední věstník Evropské unie*, L 119, 4. 5. 2016, s. 1–88. Dostupné z: <https://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016R0679>. [cit. 2025-03-09].

- [35] *GDPR v kostce*. Online. Ministerstvo průmyslu a obchodu. [2018]. Dostupné z: https://mpo.gov.cz/assets/cz/podnikani/ochrana-osobnich-udaju-gdpr/2018/10/GDPR-v-kostce_strucna-metodika.pdf. [cit. 2025-03-09].
- [36] *Co je GDPR? Nařízení o ochraně osobních údajů*. Online. Blue Partners: Specialisté na informační systémy a bezpečnost IT. 2024. Dostupné z: <https://www.bluepartners.cz/slovník-it-pojmu/gdpr>. [cit. 2025-03-09].
- [37] ČESKO. Zákon č. 412 ze dne 21. září 2005, o ochraně utajovaných informací a o bezpečnostní způsobilosti. Online. In: *Zákony pro lidi*. 2010–2025. Dostupné z: <https://www.zakonyprolidi.cz/cs/2005-412>. [cit. 2025-03-11].
- [38] ČESKO. Vyhláška č. 528 ze dne 14. prosince 2005, o fyzické bezpečnosti a certifikaci technických prostředků. Online. In: *Zákony pro lidi*. 2010–2025. Dostupné z: <https://www.zakonyprolidi.cz/cs/2005-528>. [cit. 2025-03-11].
- [39] ČESKO. Zákon č. 181 ze dne 23. července 2014, o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Online. In: *Zákony pro lidi*. 2010–2025. Dostupné z: <https://www.zakonyprolidi.cz/cs/2014-181>. [cit. 2025-03-12].
- [40] ČESKO. Vyhláška č. 82 ze dne 21. května 2018, o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). Online. In: *Zákony pro lidi*. 2010–2025. Dostupné z: <https://www.zakonyprolidi.cz/cs/2018-82>. [cit. 2025-03-12].
- [41] ČESKO. Vyhláška č. 479 ze dne 19. prosince 2024, o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o některých náležitostech žádosti o uzavření smlouvy o zajištění činnosti (vyhláška o informační bezpečnosti). Online. In: *Zákony pro lidi*. 2010–2025. Dostupné z: <https://www.zakonyprolidi.cz/cs/2024-479>. [cit. 2025-03-13].
- [42] ČESKO. Zákon č. 110 ze dne 12. března 2019, o zpracování osobních údajů. Online. In: *Zákony pro lidi*. 2010–2025. Dostupné z: <https://www.zakonyprolidi.cz/cs/2019-110>. [cit. 2025-03-13].

- [43] ČESKO. Zákon č. 262 ze dne 21. dubna 2006, zákoník práce. Online. In: *Zákony pro lidi*. 2010–2025. Dostupné z: <https://www.zakonyprolidi.cz/cs/2006-262>. [cit. 2025-03-14].
- [44] ČESKO. Zákon České národní rady č. 133 ze dne 17. prosince 1985, o požární ochraně. Online. In: *Zákony pro lidi*. 2010–2025. Dostupné z: <https://www.zakonyprolidi.cz/cs/1985-133>. [cit. 2025-03-14].
- [45] ČSN EN 50131-1 ed. 2. *Poplachové systémy - Poplachové zabezpečovací a tísňové systémy - Část 1. Systémové požadavky*. 2007. Dostupné z: ČAS, <https://sponzorpristup.agentura-cas.cz/>. [cit. 2025-03-25].
- [46] ČSN EN 60839-11-1. *Poplachové a elektronické bezpečnostní systémy - Část 11-1: Elektronické systémy kontroly vstupu - Požadavky na systém a komponenty*. 2014. Dostupné z: ČAS, <https://sponzorpristup.agentura-cas.cz/>. [cit. 2025-03-25].
- [47] ČSN EN 60839-11-2. *Poplachové a elektronické bezpečnostní systémy - Část 11-2: Elektronické systémy kontroly vstupu - Pokyny pro aplikace*. 2016. Dostupné z: ČAS, <https://sponzorpristup.agentura-cas.cz/>. [cit. 2025-03-25].
- [48] ČSN EN 62676-1-1. *Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 1-1: Systémové požadavky - Obecně*. 2014. Dostupné z: ČAS, <https://sponzorpristup.agentura-cas.cz/>. [cit. 2025-03-25].
- [49] ČSN EN 62676-4. *Dohledové videosystémy pro použití v bezpečnostních aplikacích - Část 4: Pokyny pro aplikace*. 2016. Dostupné z: ČAS, <https://sponzorpristup.agentura-cas.cz/>. [cit. 2025-03-25].
- [50] ČSN EN 1143-1. *Bezpečnostní úschovné objekty - Požadavky, klasifikace a metody zkoušení odolnosti proti vloupání - Část 1: Skříňové trezory, ATM trezory, trezorové dveře a komorové trezory*. 2020. Dostupné z: ČAS, <https://sponzorpristup.agentura-cas.cz/>. [cit. 2025-03-27].
- [51] ČSN EN ISO/IEC 27000. *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník*. 2020. Dostupné z: ČAS, <https://sponzorpristup.agentura-cas.cz/>. [cit. 2025-03-28].
- [52] ČSN EN ISO/IEC 27001. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Systémy managementu informační bezpečnosti - Požadavky*. 2023. Dostupné z: ČAS, <https://sponzorpristup.agentura-cas.cz/>. [cit. 2025-03-28].

- [53] ČSN EN ISO/IEC 27002. *Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí - Opatření informační bezpečnosti*. 2023. Dostupné z: ČAS, <https://sponzorpristup.agentura-cas.cz/>. [cit. 2025-03-28].
- [54] ČSN EN ISO 22300. *Bezpečnost a odolnost - Slovník*. 2023. Dostupné z: ČAS, <https://sponzorpristup.agentura-cas.cz/>. [cit. 2025-03-29].
- [55] ČSN EN ISO 22301. *Bezpečnost a odolnost - Systémy managementu kontinuity podnikání - Požadavky*. 2020. Dostupné z: ČAS, <https://sponzorpristup.agentura-cas.cz/>. [cit. 2025-03-29].
- [56] ČSN EN ISO 22313. *Bezpečnost a odolnost - Systémy managementu kontinuity podnikání - Pokyny pro používání ISO 22301*. 2020. Dostupné z: ČAS, <https://sponzorpristup.agentura-cas.cz/>. [cit. 2025-03-29].
- [57] ČSN ISO 31000. *Management rizik - Směrnice*. 2018. Dostupné z: ČAS, <https://sponzorpristup.agentura-cas.cz/>. [cit. 2025-03-29].
- [58] ČSN EN IEC 31010 ed. 2. *Management rizik - Techniky posuzování rizik*. 2020. Dostupné z: ČAS, <https://sponzorpristup.agentura-cas.cz/>. [cit. 2025-03-29].
- [59] SMEJKAL, Vladimír a RAIS, Karel. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, c2010. ISBN 978-80-247-3051-6.
- [60] *Types of organizational structure in a company and its importance for HR department*. Online. Pinya HR: HR system from Czech creators. 2022. Dostupné z: <https://en.pinya.hr/blog/types-of-organizational-structure-in-an-organization-and-its-importance-for-the-department>. [cit. 2025-04-07].
- [61] *Difference Between Line Organization and Functional Organization*. Online, obrázek. Difference Between: Compare the Difference Between Similar Terms. 2017. Dostupné z: <https://www.differencebetween.com/difference-between-line-organization-and-vs-functional-organization/>. [cit. 2025-04-16].
- [62] *Functional structure*. Online, obrázek. CEOpedia: Management online. 2023. Dostupné z: https://ceopedia.org/index.php/Functional_structure. [cit. 2025-04-16].
- [63] *Pros and Cons of Implementing a Divisional Structure*. Online. Indeed: Job Search. 2025. Dostupné z: <https://www.indeed.com/career-advice/career-development/divisional-structure>. [cit. 2025-04-16].

- [64] *Divisional Structure: Examples, Advantages & Disadvantages*. Online, obrázek. Advergize: Empowering Marketers. [2025]. Dostupné z: <https://www.advergize.com/business/divisional-structure/>. [cit. 2025-04-17].
- [65] LEVY, Joe. *Centralized vs Decentralized Security Operations*. Online. Dataminr: Real-Time Event and Risk Detection. 2022. Dostupné z: <https://www.dataminr.com/resources/blog/centralized-vs-decentralized-security-operations-know-the-difference-and-which-to-adopt/>. [cit. 2025-04-17].
- [66] NASSER EDDIN, Hussein. *Centralized vs. Decentralized Security Operations: Striking the Right Balance*. Online. LinkedIn. 2025. Dostupné z: <https://www.linkedin.com/pulse/centralized-vs-decentralized-security-operations-hussein-nasser-eddin-njaoe/>. [cit. 2025-04-18].
- [67] BECK, David et al. *The State of Security Convergence in the United States, Europe, and India*. Online. ASIS Foundation. 2019. Dostupné z: https://www.asisonline.org/globalassets/publications-and-resources/convergence.pdf?client_md=. [cit. 2025-04-25].
- [68] MATTORD, Herbert; KOTWICA, Kathleen; WHITMAN, Michael a BATTAGLIA, Evan. Organizational perspectives on converged security operations. Online. *Information and Computer Security*. 2024, vol. 32, s. 218–235. ISSN 2056-4961. Dostupné z: <https://doi.org/10.1108/ICS-03-2023-0029>. [cit. 2025-04-25].
- [69] *Notpetya ransomware attack on Maersk - key learnings*. Online. LRQA: Assurance, Certification, Inspection, Training. [2025]. Dostupné z: <https://www.lrqa.com/en/insights/articles/notpetya-ransomware-attack-on-maersk-key-learnings/>. [cit. 2025-04-26].
- [70] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST. *Report on the State of Cyber Security in the Czech Republic in 2019*. Online. 2019. Dostupné z: https://nukib.gov.cz/download/publikace/zpravy_o_stavu/report-czech-cyber-security-2019-en.pdf. [cit. 2025-04-27].
- [71] *Kyberútok na nemocnici v Benešově způsobil škodu přes 59 milionů. Pachatele se vypátrat nepodařilo*. Online. Český rozhlas Střední Čechy. 2020. Dostupné z: <https://strednicechy.rozhlas.cz/kyberutok-na-nemocnici-v-benesove-zpusobil-skodu-pres-59-milionu-pachatele-se-8275194>. [cit. 2025-04-27].

- [72] *Danish train standstill on Saturday caused by cyber attack*. Online. Reuters: Breaking International News & Views. 2022. Dostupné z: <https://www.reuters.com/technology/danish-train-standstill-saturday-caused-by-cyber-attack-2022-11-03/#:~:text=COPENHAGEN%2C%20Nov%20%28Reuters%29%20,DSB%20said%20on%20on%20Thursday>. [cit. 2025-04-27].
- [73] *TROLLE, Jakob Slyngborg. Leverandør lukkede it-system efter sikkerhedsbrist, og pludselig stod alle tog i Danmark stille*. Online. Danmarks Radio. 2022. Dostupné z: <https://www.dr.dk/nyheder/indland/leverandoer-lukkede-it-system-efter-sikkerhedsbrist-og-pludselig-stod-alle-tog-i>. [cit. 2025-04-27].

SEZNAM OBRÁZKŮ

Obrázek 1 Základní model konvergované bezpečnosti	14
Obrázek 2 Prostorové dělení systému fyzické bezpečnosti znázorněné na půdorysu domu	16
Obrázek 3 CIA triáda informační bezpečnosti	17
Obrázek 4 Schéma liniové organizační struktury	33
Obrázek 5 Schéma funkcionální organizační struktury	33
Obrázek 6 Schéma liniově-štabní organizační struktury	34
Obrázek 7 Schéma divizní organizační struktury	35
Obrázek 8 Schéma maticové organizační struktury	35
Obrázek 9 Konvergence bezpečnosti v organizacích - ASIS Foundation (2019)	41
Obrázek 10 Konvergence fyzické a kybernetické bezpečnosti v organizacích - ICS (2024)	42
Obrázek 11 Schéma systému řízení konvergované bezpečnosti	45

SEZNAM TABULEK

Tabulka 1 Matice pro hodnocení míry rizika.....	54
Tabulka 2 Přehled vybraných aktiv, souvisejících hrozeb a hodnocení rizik pro modelovou organizaci	54
Tabulka 3 Přehled vybraných legislativních předpisů pro modelovou organizaci	55
Tabulka 4 Přehled vybraných normativních standardů pro modelovou organizaci.....	56
Tabulka 5 Přehled vybraných bezpečnostních opatření pro modelovou organizaci.....	57
Tabulka 6 Přehled vybraných KPI a KRI pro modelovou organizaci	59

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ASIS	American Society for Industrial Security (Americká společnost pro průmyslovou bezpečnost)
BCMS	Business Continuity Management System (Systém řízení kontinuity činností)
CER	Critical Entities Resilience (Odolnost kritických subjektů)
CIA	Confidentiality, Integrity, Availability (Důvěrnost, integrita, dostupnost)
ČSN	Česká technická norma
DDoS	Distributed Denial of Service (Distribuované odepření služby)
DLP	Data Loss Prevention (Prevence ztráty dat)
DNS	Domain Name System (Systém doménových jmen)
DORA	Digital Operational Resilience Act (Nařízení o digitální provozní odolnosti)
DoS	Denial of Service (Odepření služby)
DSB	Danske Statsbaner (Dánské státní dráhy)
EN	European Norm (Evropská norma)
FMEA	Failure Mode and Effects Analysis (Analýza způsobů a důsledků poruch)
GDPR	General Data Protection Regulation (Obecné nařízení o ochraně osobních údajů)
ICS	Information and Computer Security (Informační a počítačová bezpečnost)
IEC	International Electrotechnical Commission (Mezinárodní elektrotechnická komise)
IKT	Informační a komunikační technologie
ISMS	Information Security Management System (Systém řízení bezpečnosti informací)
ISO	International Organization for Standardization (Mezinárodní organizace pro normalizaci)
IT	Informační technologie
KPI	Key Performance Indicators (Klíčové ukazatele výkonnosti)
KRI	Key Risk Indicators (Klíčové ukazatele rizik)
NIS	Network and Information Systems (Sítě a informační systémy)

NIST	National Institute of Standards and Technology (Národní institut standardů a technologie)
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PZTS	Poplachový zabezpečovací a tísňový systém
RAID	Redundant Array of Independent Disks (Redundantní pole nezávislých disků)
SMS	Safety Management System (Systém řízení bezpečnosti práce)
SMS	Short Message Service (Služba krátkých textových zpráv)
SQL	Structured Query Language (Strukturovaný dotazovací jazyk)
SWOT	Strengths, Weaknesses, Opportunities, Threats (Silné stránky, slabiny, příležitosti, hrozby)
VPN	Virtual Private Network (Virtuální privátní síť)

SEZNAM PŘÍLOH

Příloha P I: Vybrané hrozby a protipatření v oblasti fyzické bezpečnosti

Příloha P II: Vybrané hrozby a protipatření v oblasti informační bezpečnosti

Příloha P III: Vybrané hrozby a protipatření v oblasti kybernetické bezpečnosti

Příloha P IV: Vybrané hrozby a protipatření v oblasti provozní bezpečnosti

PŘÍLOHA P I: VYBRANÉ HROZBY A PROTIOPATŘENÍ V OBLASTI FYZICKÉ BEZPEČNOSTI

Hrozba	Popis	Protiopatření
Neoprávněný vstup do objektu	Vstup narušitele do chráněného objektu bez povolení.	Dveřní zámky, elektronické systémy kontroly vstupu, fyzická ostraha, oplocení, režimová opatření.
Krádež	Odcizení aktiva pachatelem překonáním ochranných opatření nebo zaměstnancem zneužitím oprávnění k přístupu.	Kamerové systémy, poplachové systémy, osobní prohlídka.
Vandalismus	Svévolné poškozování a ničení majetku, které nepřináší pachateli žádné materiální obohacení a pro které pachatel zpravidla nemá žádný motiv.	Oplocení, kamerové systémy, osvětlení objektu, fyzická ostraha, poplachové systémy.
Požár	Nežádoucí hoření, které způsobilo usmrcení nebo zranění osob či zvířat, škody na materiálních hodnotách, nebo bezprostředně ohrozilo osoby, zvířata, majetek či životní prostředí.	Automatické hasicí systémy, ruční hasicí prostředky, požární signalizace, evakuační plány, školení zaměstnanců.
Sabotáž	Úmyslné poškozování nebo ničení majetku s cílem znemožnit jeho obvyklé využití.	Prověrky zaměstnanců a dodavatelů, kamerové systémy, elektronická kontrola vstupu, režimová opatření.

Hrozba	Popis	Protiopatření
Fyzické napadení	Záměrné použití fyzické síly vůči jiné osobě, které má potenciál způsobit újmu, zranění nebo smrt. Může jít o náhodné incidenty i cílené útoky na zaměstnance, návštěvníky nebo chráněné osoby.	Osobní strážce, nouzové tlačítko, kamerové systémy, režimová opatření, školení personálu, fyzická ostraha.
Teroristický útok	Úmyslné použití násilí ohrožujícího život nebo zdraví lidí, případně poškozujícího majetek či infrastrukturu, s cílem prosadit politické nebo politicko-náboženské zájmy.	Dle charakteru – například v případě hrozby útoku na veřejnou akci: fyzická kontrola osob, prověrka zaměstnanců a účinkujících, kontrolní stanoviště, spolupráce s bezpečnostními sbory.

PŘÍLOHA P II: VYBRANÉ HROZBY A PROTIOPATŘENÍ V OBLASTI INFORMAČNÍ BEZPEČNOSTI

Hrozba	Popis	Protiopatření
Neoprávněný přístup k informacím	Získání přístupu k citlivým informacím neoprávněnou osobou.	Silná hesla, vícefaktorová autentizace, řízení přístupových práv, šifrování dat, auditní záznamy.
Únik informací	Úmyslné nebo neúmyslné zpřístupnění citlivých informací neoprávněným osobám.	DLP (data loss prevention) strategie, šifrování dat, školení zaměstnanců o bezpečném zacházení s informacemi, utajení smluv a dohod.
Ztráta dat	Nenávratné poškození nebo smazání dat v důsledku selhání hardwaru, softwaru, lidské chyby nebo kybernetického útoku.	DLP (data loss prevention) strategie, zálohování dat, RAID pole, cloudové úložiště, plán obnovy po havárii, fyzická ochrana nosičů dat.
Neoprávněná manipulace s informacemi	Změna, smazání nebo jiné znehodnocení informací neoprávněnou osobou.	Řízení přístupových práv, kontrola integrity dat, auditní záznamy, fyzická ochrana nosičů dat.
Průmyslová špionáž	Nezákonné a neetické získání informací o jiné organizaci s cílem získání konkurenční výhody.	Utajení smluv a dohod, školení zaměstnanců o ochraně informací, bezpečnostní prověrky, fyzická ochrana objektu a dokumentů.

Hrozba	Popis	Protiopatření
Sociální inženýrství	Technika, jejímž cílem je zmanipulovat jedince k provedení určité akce nebo získání určité informace. Tento termín taktéž označuje podvodné jednání za účelem získání důvěrných informací organizace nebo přístupu do jejího informačního systému.	Školení zaměstnanců o zásadách bezpečnosti, ověřování identity volajících, ověřování emailových požadavků, fyzická ochrana objektu a dokumentů.

PŘÍLOHA P III: VYBRANÉ HROZBY A PROTIOPATŘENÍ V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

Hrozba	Popis	Protiopatření
Malware	Program nebo kód určený k poškození počítače, sítě nebo serveru. Zahrnuje různé typy hrozeb, jako jsou viry, trojské koně, ransomware nebo spyware.	Antimalwarový software, ochrana proti spamu, pravidelné aktualizace, školení uživatelů o škodlivých e-mailech a webových stránkách.
Phishing	Typ kybernetického útoku, při kterém útočník pomocí e-mailu, SMS, telefonátu nebo sociálních sítí manipuluje oběť k poskytnutí citlivých údajů, jako jsou hesla nebo čísla účtů. Často také láká oběť ke stažení škodlivého souboru, který může infikovat její zařízení.	Školení zaměstnanců, testovací phishingové kampaně, ověřování emailových adres a odkazů.
Denial of Service	Denial-of-Service (DoS) a Distributed Denial-of-Service (DDoS) útoky jsou kybernetické útoky zaměřené na narušení dostupnosti služby nebo systému. Při DoS útoku útočník zahlcuje síť nebo server velkým množstvím požadavků z jednoho zdroje, čímž znemožňuje uživatelům přístup ke službám. DDoS útok je prováděn z více zařízení, čímž je škodlivější, obtížněji odhalitelný a jeho odvrácení je náročnější.	Robustní síťová architektura, monitoring síťového provozu, plány reakce na DoS útoky, využití anti-DDoS softwaru.

Hrozba	Popis	Protiopatření
Útoky pomocí injeke kódu	Kybernetické útoky, při kterých útočník zneužije zranitelnosti aplikace k vložení škodlivého kódu do systému. Tyto útoky mohou umožnit spuštění neautorizovaných příkazů, neoprávněný přístup k datům nebo manipulaci s chodem systému. Mezi tyto útoky patří například SQL injection, cross-site scripting a command injection.	Validace vstupních dat, zabezpečené programování (např. připravené dotazy a parametrizované SQL dotazy), pravidelné bezpečnostní audity, aplikace bezpečnostních záplat.
Man-in-the-middle útok	Typ kybernetického útoku, při kterém útočník tajně zachytává nebo manipuluje s komunikací mezi dvěma stranami. Cílem tohoto útoku může být krádež přístupových údajů, bankovních údajů, ale také změna nebo podvržení přenášených dat. Tento útok může být proveden různými způsoby, například prostřednictvím podvržených Wi-Fi sítí, manipulací s DNS servery nebo kompromitací síťové infrastruktury.	Používání VPN při připojení k veřejným sítím, vyhýbání se neznámým Wi-Fi sítím a vypnutí automatického připojování, pravidelné aktualizace softwaru, používání bezpečnostních záplat.

PŘÍLOHA P IV: VYBRANÉ HROZBY A PROTIOPATŘENÍ V OBLASTI PROVOZNÍ BEZPEČNOSTI

Hrozba	Popis	Protiopatření
Výpadek elektrické energie	Neočekávaná ztráta elektrické energie, která může způsobit přerušení provozu kritických systémů a technologií.	Použití záložních zdrojů energie a jejich pravidelná údržba, plány obnovy po výpadku.
Selhání kritických provozních systémů	Výpadek nebo porucha klíčových systémů a zařízení nutných pro plynulý chod organizace.	Použití záložních systémů a jejich pravidelná údržba, vypracování postupů pro obnovu po havárii.
Narušení kontinuity provozu v důsledku lidské chyby	Narušení kontinuity provozu způsobené neúmyslnými chybami nebo nesprávnými rozhodnutími osob.	Školení zaměstnanců, používání kontrolních seznamů, implementace mechanismů zabraňujících chybám.
Ztráta kvalifikované pracovní síly	Ztráta klíčových zaměstnanců, jejichž znalosti, schopnosti a zkušenosti jsou nezbytné pro provoz organizace.	Školení zaměstnanců, plánování nástupnictví, systematické předávání znalostí mezi zaměstnanci.
Přírodní katastrofa	Neočekávaná přírodní událost, jako je povodeň, požáry, zemětřesení, nebo jiné extrémní počasí, která může přerušit nebo ohrozit plynulý chod organizace.	Tvorba evakuačních plánů, pravidelná cvičení a školení zaměstnanců, využívání alternativních pracovišť, zálohování dat.