Návrh dynamických penalizačních faktorů konvergované bezpečnosti v rámci vybraného subjektu

Bc. Marian Mikulka

Diplomová práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektroniky a měření

Akademický rok: 2022/2023

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Marian Mikulka**
Osobní číslo:	**A20216**
Studijní program:	**N1032A020003 Bezpečnostní technologie, systémy a management**
Specializace:	**Bezpečnostní technologie**
Forma studia:	**Kombinovaná**
Téma práce:	**Návrh dynamických penalizačních faktorů konvergované bezpečnosti v rámci vybraného subjektu**
Téma práce anglicky:	**Design of Dynamic Converged Security Penalty Factors within the Selected Entity**

Zásady pro vypracování

1. Vypracujte literární rešerši na téma konvergovaná bezpečnost.
2. Formulujte základní zásady konvergované bezpečnosti na právní podmínky ČR.
3. Vypracujte literární rešerši na téma. penalizační faktory.
4. Analyzujte současný stav ochrany ve vybraném objektu.
5. Navrhněte penalizační faktory konvergované bezpečnosti ve vybraném objektu.

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

Seznam doporučené literatury:

1. LUKÁŠ, Luděk. Teorie bezpečnosti a typologie druhů bezpečnosti. In: *Sborník 21. vědecké konference s mezinárodní účastí Riešenie krízových situácií v špecifickom prostredí*, 25. – 26. května 2016, Žilina: EDIS. ISBN 978-80-554-1213-9.
2. LUKÁŠ, Luděk. *Teorie bezpečnosti I*. Zlín: Radim Bačuvčík – VeRBuM, 2017. ISBN 978-80-87500-89-7.
3. ŠENK, Zdeněk. *Bezpečnost a ochrana zdraví při práci: prakticky a přehledně podle normy OHSAS*. 2., aktualiz. vyd. Olomouc: ANAG, 2012. Práce, mzdy, pojištění. ISBN 978-80-7263-737-9.
4. VALOUCH, Jan, URBANČOKOVÁ, Hana. Katalog penalizačních kritérií fyzické bezpečnosti objektů. [Výzkumná zpráva]. Projekt: VI 20172019054 "Analytický programový modul pro hodnocení odolnosti v reálném čase z hlediska konvergované bezpečnosti". Praha: TTC TELEKOMUNIKACE, s.r.o., 2018.
5. VALOUCH, Jan, URBANČOKOVÁ, Hana. Obecný katalog penalizačních faktorů [Výzkumná zpráva]. Projekt: VI 20172019054 "Analytický programový modul pro hodnocení odolnosti v reálném čase z hlediska konvergované bezpečnosti". Praha: TTC TELEKOMUNIKACE, s.r.o., 2019.
6. LUKÁŠ, Luděk. Metodika hodnocení odolnosti z pohledu konvergované bezpečnosti. [Výzkumná zpráva]. Projekt: VI 20172019054 "Analytický programový modul pro hodnocení odolnosti v reálném čase z hlediska konvergované bezpečnosti". Praha: TTC TELEKOMUNIKACE, s.r.o., 2018.

Vedoucí diplomové práce: **doc. Ing. Martin Hromada, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **20. listopadu 2023**
Termín odevzdání diplomové práce: **28. května 2024**

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

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

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

Ve Zlíně dne 1. prosince 2023

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že 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;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že 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 samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne …….

podpis studenta

ABSTRAKT

V této diplomové práci byla shrnuta literární rešerše konvergované bezpečnosti, jednotlivé druhy bezpečností, které konvergovaná bezpečnost slučuje a její zásady na právní podmínky České republiky. Dále byla shrnuta literární rešerše analýzy rizik, hrozeb a penalizačních faktorů na jejichž základě byl v druhé kapitole praktické části diplomové práce vypracován katalog dynamických penalizačních faktorů pro vybranou společnost. Společnost byla představena v předchozí kapitole spolu i s analýzou současného stavu objektu a identifikací aktiv.

Klíčová slova: Konvergovaná bezpečnost, analýza rizik, dynamické penalizační faktory, návrh penalizačních faktorů.

ABSTRACT

In this diploma thesis has been summarized the literary research on converged security including its combined individual types as well as its principles on the legal conditions of the Czech Republic. Furthermore, is has been summed up a literary research of risk analysis, threats and penalty factors. Based on that the catalogue of dynamic penalty factors for the selected company has been drawn up in the practical part of the second chapter of this thesis. The company was introduced in the previous thesis chapter together with the analysis of the object current state of and the identification of assets.

Keywords: Converged security, risk analysis, dynamic penalty factors, design of penalty factors.

Tímto bych chtěl poděkovat svému vedoucímu práce panu doc. Ing. Martinu Hromadovi, Ph.D. za jeho odborné rady a připomínky při tvorbě diplomové práce. A dále také své partnerce za pevné nervy a plnou podporu.

OBSAH

ÚVOD **9**
I TEORETICKÁ ČÁST **10**
1 KONVERGOVANÁ BEZPEČNOST **11**
1.1 FYZICKÁ BEZPEČNOST (FB) 13
1.1.1 Hlavní oblasti 14
1.1.2 Hrozby ve fyzické bezpečnosti 16
1.2 INFORMAČNÍ BEZPEČNOST (IB) 16
1.3 KYBERNETICKÁ BEZPEČNOST (KB) 16
1.3.1 Klíčové aspekty 17
1.3.2 Hrozby v kybernetickém prostoru 19
1.4 PROVOZNÍ BEZPEČNOST (PB) 19
1.4.1 Hrozby v provozní bezpečnosti 21
2 ASPEKTY KONVERGOVANÉ BEZPEČNOSTI V PRÁVNÍCH PODMÍNKÁCH ČR **23**
2.1 ZÁKON O KYBERNETICKÉ BEZPEČNOSTI (Č. 181/2014 SB.) 23
2.2 ZÁKON O OCHRANĚ OSOBNÍCH ÚDAJŮ (Č. 110/2019 SB.) 23
2.3 ZÁKON O BEZPEČNOSTI PRÁCE (Č. 309/2006 SB.) 23
2.4 ZÁKON O KRIZOVÉM ŘÍZENÍ (Č. 240/2000 SB.) 24
3 PENALIZAČNÍ FAKTORY **25**
3.1 ODOLNOST A JEJÍ HODNOCENÍ 25
3.2 DĚLENÍ PENALIZAČNÍCH FAKTORŮ 26
3.3 KATALOG PENALIZAČNÍCH FAKTORŮ 26
3.4 VÝPOČET INDEXU ODOLNOSTI 28
3.5 KVANTIFIKACE PENALIZAČNÍCH FAKTORŮ A NĚKTERÉ METODY 30
3.5.1 Multikriteriální hodnocení velikosti penalizace 30
3.5.2 Metoda založená na expertním odhadu 31
3.5.3 Fullerova metoda 31
4 ANALÝZA RIZIK V KONVERGOVANÉ BEZPEČNOSTI **33**
4.1 KLÍČOVÉ ASPEKTY 33
4.2 VYBRANÉ METODY ANALÝZY RIZIK 35
4.2.1 Checklist 35
4.2.2 PNH 36
4.2.3 HRA 38
II PRAKTICKÁ ČÁST **39**
5 ANALÝZA SOUČASNÉHO STAVU OCHRANY VE VYBRANÉM OBJEKTU **40**
5.1 SPECIFIKACE VYBRANÉHO REFERENČNÍHO OBJEKTU 40
5.2 ANALÝZA RIZIK 41
5.2.1 Identifikace a hodnocení aktiva 42
5.2.2 Hodnocení a identifikace hrozeb 45
5.2.3 Analýza rizik pomocí metody PNH 47

6 NÁVRH DYNAMICKÝCH PENALIZAČNÍCH FAKTORŮ KONVERGOVANÉ BEZPEČNOSTI 50
ZÁVĚR 57
SEZNAM POUŽITÉ LITERATURY 59
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 62
SEZNAM OBRÁZKŮ 63
SEZNAM TABULEK 64

ÚVOD

V dnešní době, kdy vlivem rychlého technologického rozvoje dochází k velkému nárůstu nových nebezpečí a rizik, je žádoucí propojení vybraných druhů bezpečnosti do jedné a to do tzv. konvergované bezpečnosti.
Konvergovaná bezpečnost přináší několik výhod, a to zejména v kontextu integrovaného a komplexního přístupu k ochraně organizace, informací a prostředí. Díky konvergovanému zabezpečení tedy dochází také k lepší ochraně aktiva, zachování kontinuity provozu a snižovaní rizika škodlivých událostí a útoků.
Dnešní bezpečnostní iniciativy podporují začlenění fyzické, informační, kybernetické a provozní bezpečnosti do konvergovaného zabezpečení pro větší efektivitu a možnosti. Při zajišťování jednotlivých druhů bezpečností odděleně docházelo nejen k neefektivnosti řešení bezpečnosti a vyšším finančním nákladům, ale také například k neschopnosti propojení informací, a tudíž k pomalejším reakcím a zásahům.

V rámci této diplomové práce, byly v teoretické části rozepsány jednotlivé druhy bezpečnosti, jako i samotná konvergovaná bezpečnost, byly formulovány aspekty konvergované bezpečnosti na právní podmínky ČR, dále byla věnována kapitola problematice penalizačních faktorů a v poslední kapitole teoretické části byla popsána analýza rizik i s jejími výhodami pro konvergovanou bezpečnost. V rámci praktické části této diplomové práce byl zanalyzován současný stav ochrany ve vybraném referenčním objektu a následně byla provedena analýza rizik a poté navrhnuty penalizační faktory pro daný objekt.

I. TEORETICKÁ ČÁST

1 KONVERGOVANÁ BEZPEČNOST

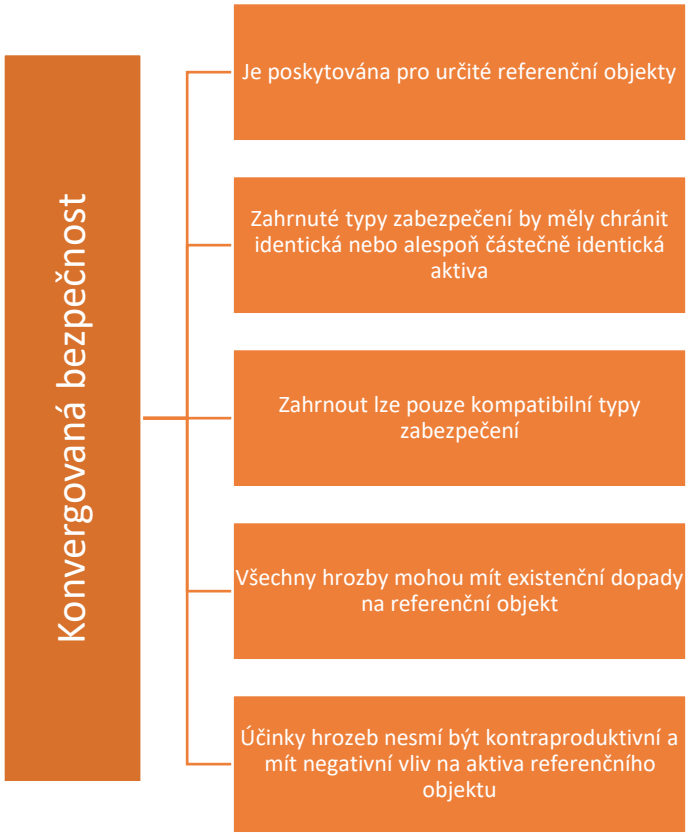
Bezpečnost je jedním ze základních pilířů moderního světa. Cílem bezpečnosti jako oboru je chránit referenční objekty (např. lidi, organizace, kritickou infrastrukturu) a jejich majetek před poškozením, případně minimalizovat dopady narušení bezpečnosti. Referenční objekt aktivně zajišťuje svou bezpečnost prostřednictvím souborů opatření určených k zajištění bezpečnosti v definované části bezpečnostního prostředí [1, 2].

V rámci své ochrany musí referenční objekty poskytovat narůstající počet těchto typů zabezpečení, a to primárně díky technologickému rozvoji. Například pro referenční objekt výrobního závodu tyto typy zabezpečení zahrnují fyzickou bezpečnost, kybernetickou bezpečnost, provozní zabezpečení, administrativní zabezpečení a bezpečnost a ochranu zdraví při práci. Nad rámec těchto základních zabezpečení lze k nim přidat personální zabezpečení, bezpečnost životního prostředí, radiační bezpečnost, bezpečnost technických zařízení atd. je-li to požadováno nebo je to nutné [3].

V současné době fungují jednotlivé typy zabezpečení nezávisle na ostatních typech zabezpečení, což s sebou nese řadu nevýhod. Jedním ze základních negativ této situace je nemožnost propojit příznaky vznikajícího narušení bezpečnosti, detekované v jednotlivých typech zabezpečení do jednoho celku. Dalším negativem jsou zvyšující se náklady na zajištění bezpečnosti, vyplývající ze samostatného zajišťování zabezpečení jednotlivých typů. Následky se projevují jak po stránce technologické, tak zejména po stránce personální či organizační. Každý typ zabezpečení je poté obvykle zajišťován samostatnou skupinou odborníků, která má vlastní finanční rozpočet, bezpečnostní technologie a také ochranné procesy [4].

V současné době je z praktických důvodů nezbytné hledat způsoby, jak jednotlivé typy zabezpečení spojit do jednoho celku a tento trend vyústil v koncept konvergovaného zabezpečení. Konvergovaná bezpečnost integruje a sjednocuje různé aspekty bezpečnosti do jednoho komplexního rámce. To může zahrnovat fúzi fyzické a kybernetické bezpečnosti, integrované sledování a reakce na hrozby nebo sjednocení různých bezpečnostních technologií a postupů, a tudíž i cíleněji zajistit jejich řešení [5].

V praxi konvergovanou bezpečnost tedy chápeme jako komplexní zabezpečení firem, objektů nebo organizací jako celku. Jedná se tedy o multifunkční obor, který spojuje využívání prostředků situační analýzy a zpracování hromadných dat, což zajišťují nové sofistikované systémy informačního managementu (CSIM, SIEM) [6].



Obr. 1: Základní principy konvergované bezpečnosti (upraveno z [7]).

V souvislosti s rozvojem moderních technologických konceptů, jako je IoT, Průmysl 4.0, Smart Cities, dochází k masivnímu nárůstu datového toku, což lze hodnotit pouze na základě algoritmů hromadného zpracování dat. Podmínkou kompatibility je potřeba chránit referenční objekt stejnými aktivy a také časové charakteristiky projevů narušení bezpečnosti, které by měly být přibližně stejné. Projevy konvergovaného zabezpečení jsou v časovém rozsahu sekund – minut – hodin. V případě, že jeden typ zabezpečení by se měnil kratším časovém horizontu (v minutách) než druhý (v letech), nemělo by sloučení do konvergovaného zabezpečení smysl. Dominantní roli by zde vždy hrál typ zabezpečení s krátkými časovými změnami [8].

Sloučením dříve samostatných bezpečnostních typů dosáhneme korelace jednotlivých projevů narušení bezpečnosti. S tím je svázána i rychlejší detekce narušení bezpečnosti, její způsob, rozsah a predikce možného budoucího průběhu narušení [7].

Z důvodu potřeby zajištění celkové bezpečnosti je vhodné přistoupit k výběru pouze dílčích bezpečností, které jsou pro daný referenční objekt podstatné a jejich sledování bude smysluplné [6].

Mezi základní zásady fungující konvergované bezpečnosti poté patří:

- centrální správa a monitorování bezpečnostních systémů,
- využívání analytických postupů a kybernetické inteligence pro identifikaci hrozeb,
- rizikový management,
- automatizace a technologické inovace,
- a především komunikace a spolupráce mezi týmy spravující jednotlivé druhy bezpečnosti [5].

Za základní druhy bezpečnosti, které se (většinou) sjednocují do konvergované bezpečnosti, považujeme fyzickou, informační, kybernetickou a provozní bezpečnost [6].

1.1 Fyzická bezpečnost (FB)

Jedná se o nejznámější druh bezpečnosti a ochranných opatření. Samotný pojem fyzická bezpečnost označuje soubor opatření vůči rizikům a narušením působících fyzickou cestou. Účelem FB je zabezpečení fyzických prostor, zařízení, osob a aktiv vůči záměrným hrozbám, jejichž původcem je člověk [6]. Je tedy zaměřena především proti neoprávněnému přístupu, poškození, krádeži nebo jiným nebezpečím. Mezi základní hrozby patří kriminalita, teroristický útok, vojenský zájem. FB podléhá množství mezinárodních a národních standardů včetně podzákonných norem a vyhlášek [4].

Fyzická bezpečnost využívá retenci, redukci, detekci, odstrašení a reakci jako bezpečnostní metody. Redukce aktivně zadržuje škodící účinek a tím může zamezit narušení, zatím co retence snižuje pravděpodobnost vzniku, anebo velikost škody způsobené narušením. K redukci je zapotřebí ochranných prvků typu vícevrstvé bariéry. Při překonání bariéry poskytují poté retenční prvky delší reakční dobu pro fyzickou ostrahu nebo zásah policie (reakci). Detekce je založena na technických systémech sloužících ke zjištění okolností narušení bezpečnosti. Odstrašení spočívá v přesvědčivém informačním a demonstračním účinku [6]. Je to klíčový aspekt celkového bezpečnostního programu a obvykle zahrnuje několik prvků a opatření.

1.1.1 Hlavní oblasti

I. Monitorování a reakce na potencionální hrozby:

Zabezpečení vstupů a výstupů budov prostřednictvím klíčových karet, biometrických prvků nebo jiných bezpečnostních systémů. Vytváření kontrolních bodů a omezení přístupu na základě oprávnění. Zavedení pravidel pohybu osob a jimi prováděných úkonů v daném prostoru. Moderní dohledová řešení jsou založena na integraci různých snímacích subsystémů. Každý subsystém obsahuje množství různorodých a distribuovaných senzorů, které mají na starosti detekce abnormálních podmínek nebo nežádoucích událostí ve sledovaném prostředí. Tyto prvky vedou k rychlé reakce na potenciální hrozby nebo incidenty [9].

II. Omezení přístupu:

Využívání bezpečnostních prvků jako jsou brány, ploty a bariéry pro zpomalení či odrazení narušitele. Důležitá je zde vícestupňová a průlomová odolnost, kde každá vrstva má své specifika, které vychází z pořadí a dispozic dané ochrany. Tyto bezpečností prvky jsou děleny na perimetrickou, plášťovou, prostorovou a předmětovou ochranu.

Perimetrické bezpečnostní opatření se nachází na obvodu pozemku a v prostoru mezi hranicí a chráněným objektem. Jejich cílem je primárně odstrašení, zpomalení a signalizace narušení obvodu referenčního objektu. Signalizaci zajišťují detektory, které musí splňovat vyšší požadavky ke klimatickým podmínkám a zpravidla musí mít delší dosah a užší detekční charakteristiku.

Plášťová bezpečnostní opatření jsou realizována na plášti referenčního objektu (zpravidla budovy). Jejich cílem je znemožnění nebo alespoň zpoždění průchodu narušitele do objektu. Mezi plášťové bezpečnostní prvky tvoří stěny, okna, dveře, zámkové systémy, mříže, detektory narušení plíště budovy a další. Na rozdíl od perimetrických detektorů mají plášťové detektory kratší dosah a širší detekční charakteristiku a jsou zpravidla umístěny uvnitř budovy.

Prostorová bezpečnostní opatření jsou realizována ve vnitřních prostorech referenčních objektů (na chodbách, schodištích, v místnostech). Jejich cílem je zpoždění a odhalení pohybu narušitele. Mezi prvky prostorových opatření patří dveře, zámkové systémy, mříže, kamerové systémy a detektory signalizující vniknutí do vnitřních prostor. Detektory by měly mít kratší dosah a širší kuželovou detekční charakteristiku.

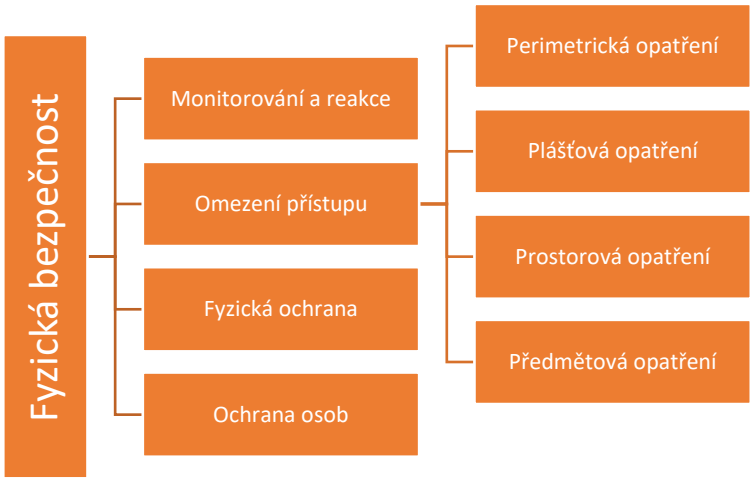
Předmětová bezpečnostní opatření jsou cílená na ochranu chráněných aktiv, jimiž jsou obvykle umělecké předměty, patentově chráněné vzory a další cenné fyzické předměty. Prvky předmětových opatření zamezují jejich odcizení a neoprávněné manipulaci. Mezi tyto prvky řadíme trezory, vitríny, kamerové systémy poplachové senzory a další. Detektory slouží k identifikaci bezprostřední přítomnosti narušitele nebo neoprávněné osoby a měly by tedy mít krátký dosah a širokoúhlou, plochou charakteristiku [6].

III. Fyzická ochrana:

Proškolený personál strážní služby, který zabezpečuje ochranu referenčních objektů, aktiv a osob. Ostraha je jediným pilířem fyzické bezpečnosti, která se může aktivně podílet a bezprostředně provést zákrok vedoucí ke zmaření záměrů narušitele, jeho dopadení a odvrácení nebezpečí [6]. Mnoho organizací má uzavřené televizní kamery (CCTV) a najímají si ostrahu, která vše monitoruje z velínu, což vyžaduje jejich plnou pozornost. Monitorovat stav zabezpečení s maximální úrovní pozornosti, není v lidských možnostech a jde tedy o významnou zranitelnost. Použití řešení řízených umělou inteligencí (AI) je potenciální způsob, jak tuto zranitelnost překonat [10].

IV. Ochrana osob:

Vypracování plánů pro ochranu osob, krizový management a evakuační plány včetně úkrytů a bezpečných zón. Je důležité, aby bezpečnostní opatření byla pravidelně aktualizována a revizována podle změn v rizikovém prostředí a nových technologiích [9].



Obr. 2: Přehled dělení některých oblastí fyzické bezpečnosti.

1.1.2 Hrozby ve fyzické bezpečnosti

U fyzické bezpečnosti za původce hrozeb považujeme primárně člověka, ale lze zařadit i hrozby přírodního charakteru. Mezi základní hrozby řadíme kriminální činnosti, teroristické útoky nebo vojenský zájem cizí moci. Tyto hroby poté mohou vést ke ztrátě, poškození či zničení majetku, ztrátu kontroly a ovládání, poškození zdraví nebo ztrátě života [6].

1.2 Informační bezpečnost (IB)

Jedná se o multidisciplinární obor, jehož účelem je ochrana dat a informací před neoprávněným přístupem, ztrátou, zneužitím nebo škodlivými útoky [11]. Jejich bezpečností se zabývá od vzniku, přes zpracování, ukládání, přenos až k likvidaci ať už ve fyzické nebo elektronické formě prostřednictvím logických, technických, fyzických a organizačních opatření [6].

Informační bezpečnost musí řešit veškerou ochranu informací organizace, tedy celého informačního systému. To zahrnuje ochranu informací v mluvené i psané formě a zejména jejich ochranu při zpracování a přenosu.

Je klíčovým prvkem pro organizace, které závisejí na informačních technologiích a zpracování dat. Zahrnuje mnoho aspektů a postupů, které mají za cíl zajistit bezpečnost informací a dat. Mezi klíčové prvky patří například ochrana přístupu, šifrování, ochrana proti malwaru a škodlivým útokům, ochrana sítí nebo plánování krizové situace [11].

1.3 Kybernetická bezpečnost (KB)

KB můžeme považovat za odvětví výpočetní techniky, informačních a komunikačních technologií. Kybernetickou bezpečnost je možno vnímat za součást informační bezpečnosti uplatňované u počítačů i sítích. Rozdílem mezi těmito dvěma odvětvími je ale cíl ochrany, přičemž ochrana informací v jakékoliv podobě je cílem informační bezpečnosti, zatímco cílem kybernetické bezpečnosti je ochrana informací pouze v digitální podobě [6].

Kybernetická bezpečnost se stala hlavním zájmem a důležitým tématem ve veřejných i soukromých společnostech, orgánech činných v trestním řízení a finančních institucích, kvůli stále rostoucím kybernetickým rizikům. Kybernetická bezpečnost se zaměřuje na ochranu počítačových systémů, sítí, dat a elektronických zařízení před kybernetickými hrozbami a útoky [12].

Dle Susskind [13] kybernetická bezpečnost je přímo spjata se systémovým řízením společnosti, řízením rizik a dodržováním předpisů. Má také vliv jak na interní zainteresované

strany – od ředitelů (jednatelů) až po stážisty, tak i externí zainteresované strany – dodavatele, zákazníci, spotřebitelé i pojišťovny.

Hlavním cílem je snížení rizika nedovolené manipulace a zajištění ochrany před vyvíjejícími bezpečnostními hrozbami [6].

1.3.1 Klíčové aspekty

I. Identifikace a ochrana:

Identifikace a ochrana zranitelností v počítačových systémech a softwaru prostřednictvím pravidelných aktualizací a záplat. Využívání antivirových programů, antimalwaru a bezpečnostních prvků k prevenci útoků.

II. Správa identit a přístupových práv:

Správa a zajištění bezpečného přístupu k systémům prostřednictvím efektivní správy identit a přístupových práv.

III. Šifrování dat:

Používání šifrování k zabezpečení komunikace a uložených dat, což znesnadňuje neoprávněným osobám přístup k citlivým informacím.

IV. Monitorování a detekce:

Sledování síťového provozu a aktivit v reálném čase za účelem detekce neobvyklých nebo podezřelých vzorů, což může signalizovat kybernetický útok.

V. Zálohování a obnova:

Pravidelné zálohování dat a vypracování plánů pro obnovu v případě, že dojde k úniku dat nebo jiným ztrátám.

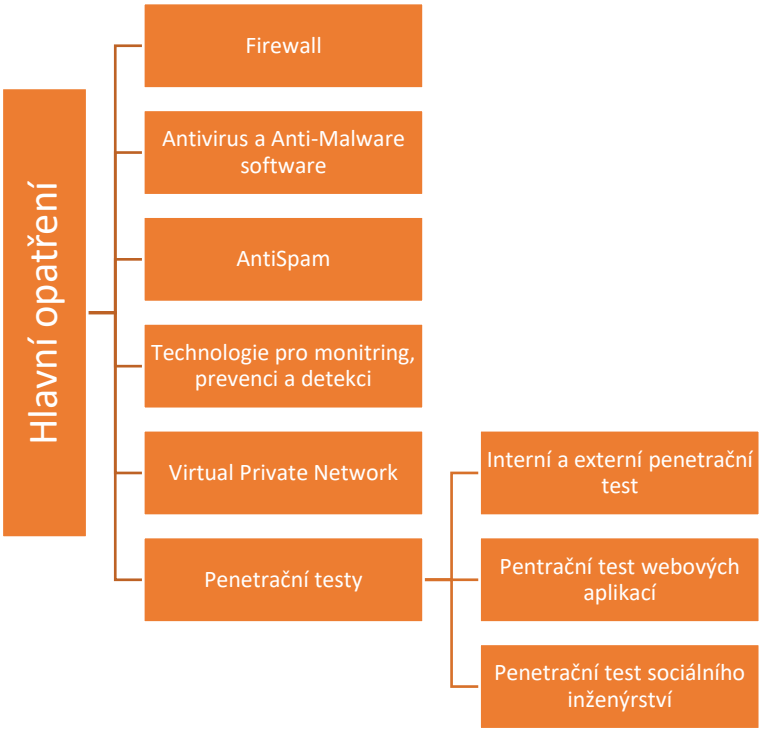
VI. Vědomostní a technické školení:

Poskytování školení zaměstnancům k povědomí o kybernetických hrozbách, ať už jde o phishing, sociální inženýrství nebo jiné útoky.

VII. Incidentní reakce:

Připravenost a plánování reakce na kybernetické incidenty, včetně izolace a eliminace hrozeb a následných kroků k obnovení bezpečnosti [12, 13].

Jak kybernetická bezpečnost, tak technologie informačního zabezpečení vyžaduje neustálé hodnocení a inovace, jelikož jde o značně rozvinuté oblasti. Díky rychlému nárůstu používání technologií, došlo také k rozvoji technologií, které poskytují uživateli některé výhody jako je úspora času a práce, ale které představují bezpečnostní riziko. Například Internet věcí (IoT), i s jeho aplikacemi, je považován za jednou z nejlepších technologií, které nám usnadňují práci poskytováním funkcí (tj. konektivita a aktivní zapojení), které nám pomáhají dosáhnout zlepšení, zvýšení efektivity a výměna znalostí. IoT je definován jako skupina vzájemně propojených lidí a zařízení a také umožňuje zařízením komunikovat mezi sebou bez účasti člověka. Zahrnuje propojené senzory reálného světa, elektronická zařízení a systémy k internetu. Jelikož je hlavní podporou IoT je internet, tak jakékoli bezpečnostní hrozby, které se zaměřují na internet, mohou ovlivnit IoT [14]. Podle důležitosti sítě a technologie v jakékoli aplikaci je třeba vzít v úvahu zabezpečenost sítě, kdy síť je zranitelná vůči útokům při přenosu dat do komunikačních kanálů. Nezbytné pro zabezpečení sítě IoT (stejně jako u jiných sítí) jsou, mimo jiné, následující obecné bezpečnostní požadavky: ověření, integrita, důvěryhodnost, dostupnost, neodmítatelnost, autorizace, aktuálnost.



Obr. 3: Hlavní opatření v kybernetickém prostoru proti hrozbám (upr. z [6]).

1.3.2 Hrozby v kybernetickém prostoru

Hrozby představují velký problém, protože kybernetické útoky mohou vést např. ke krádeži duševního vlastnictví, objemu citlivých údajů, osobních informací, know how a jiné. V dnešní době se neustále objevují nové kybernetické hrozby, kterým je třeba se vyhnout a stejně tak se bránit proti možným únikům a následným škodám. Aktuálně jsou útoky pokročilejší oproti minulosti v jejich komplexnosti a výskytu v nejrůznějších formách, které například mají v úmyslu získat přístup do počítačové sítě bez souhlasu vlastníka (malware - ransomware, adware, spyware, virus, počítačový červ, trojský kůň) [6]. Zabezpečení sítě je poté hlavním zájmem dnešní generace výpočetní techniky. Například ochrana softwarových zdrojů zahrnuje ochranu hardwarového softwaru, operačních systémů, prohlížeče, serverové protokoly atd. Mezi bezpečnostní protokoly a standardy, které se používají pro bezpečnost a soukromí s cílem minimalizace počtu útoků vedených na sítě počítačů patří například skupina nejpoužívanějších norem ISO/IEC 27000 (Řízení rizik v informační bezpečnosti – Information Security Management System – ISMS), nebo také Secure Socket Layer (SSL), protokoly TLS (Transport Layer Security) bezpečný internet, Protokol (IPsec), Secure Hypertext Transfer Protocol (SHTTP), bezpečný e-mail (Pretty Good Privacy (PGP) a Secure/Multipurpose Internet Mail Extensions (S/MIME) ,Secure Shell (SSH) a další [15].

Jelikož může počítačová kriminalita přesahovat i národní měřítko, tak představuje závažný problém, kterému musí každý stát, který má své systémy připojeny k internetu, být schopen odolat a bránit se. Díky tempu rozvoje nových informačních technologií a s nimi spojenými službami tedy musí kybernetická bezpečnost pružně reagovat na nové hrozby a udržovat své bezpečnostní postupy a technologie aktuální [6].

1.4 Provozní bezpečnost (PB)

Provozní bezpečnost lze chápat jako klíčový prvek celkového bezpečnostního programu a pomáhá podniku (firmě nebo systému) minimalizovat rizika spojená s jejich provozem a zajistit, že jsou schopny reagovat na neočekávané události s minimálními dopady na bezpečnost a kontinuitu provozu [16].

Z hlediska dostupnosti a kvality služeb je nutno zaručit požadovanou dobu jejich obnovy v případě výpadku a je tedy potřeba nejenom použití modernizovaných, udržovaných a zálohovaných technologií, ale také zabezpečení vhodné strategie řízení kontinuity činnosti organizace. Pro zajištění provozní bezpečnosti lze poté vycházet ze zásad systému managementu

kontinuity podnikání BCMS (Business Continuity Management System) nebo ze zásad SMS (Safety Management System).

I. BCMS

Z pohledu BCMS jsou pro organizace důležité zásady jako stanovení základní strategie, implementace kontroly úrovně, funkčnosti a stanovení potřebných opatření organizace, jakožto i objektivní měření a sledování klíčových indikátorů výkonnosti. Tyto zásady zvyšují účinnost opatření přijatých v rámci sledování a řešení konvergované bezpečnosti v reálném čase.

II. SMS

Účelem systému SMS je cíleně a systematicky zvyšovat provozní bezpečnost, tudíž aktivně vyhledávat a minimalizovat potenciální a identifikovaná rizika vedoucí ke zranění osob/ poškození majetku.

Organizace, které provozují složité a nebezpečné technologie mohou mít potenciál způsobit významné události (počet úmrtí a/nebo zranění) pokud se něco pokazí, tudíž potřebují fungovat konzervativně. Samozřejmě se ale také potýkají s běžným komerčním tlakem na snižování nákladů a/nebo maximalizaci výroby. Dosažení vhodné rovnováhy mezi těmito dvěma prioritami poté vyžaduje od vlastníků, provozních organizací a regulačních orgánů mnohostranný přístup, který se zabývá návrhem, konstrukcí, údržbou a provozem [16].

Provozní bezpečnost často také bývá vnímána jako měřítko kvality, která umožňuje fungování (za předem stanovených podmínek) s přijatelným minimálním poměrem nehod.

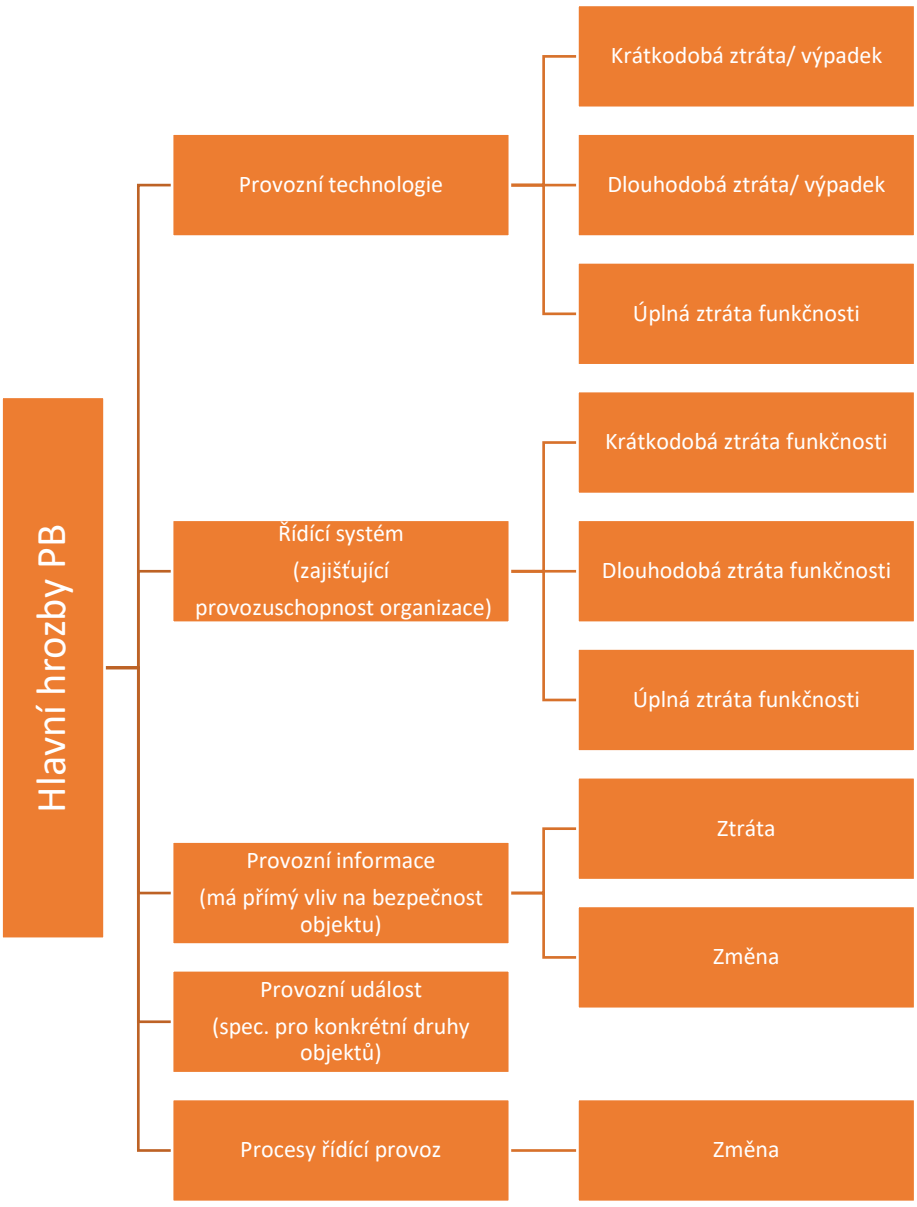
Chod podniku musí být neustále zajištěn, a proto musí dojít k identifikaci klíčových procesů a systémů, které jsou pro provoz nezbytné. První krok – stanovení kontextu, poznání prostředí podniku a definování klíčových fází provozu, je jedním z nejdůležitějších v PB. Zde je nutno připravit proces detekce chyb a výpadků, aby mohlo na ně mohlo být bezprostředně reagováno. Analýza rizik se poté soustředí na vyhledávání nekritičtějších rizik. Vyhodnocení rizik stanovuje prioritu rizik a jejich hranici. A finálním krokem je fáze zvládání rizik, při níž dochází k minimalizaci a eliminaci rizik, popřípadě přípravy na tyto rizika [6].

Pracovníci provozní bezpečnosti jsou často v nebezpečných průmyslových odvětvích vyzýváni, aby dokázali vyvážit výrobní a bezpečnostní cíle jejich provozu. Předpisy a průmyslové normy se poté zaměřují na definování a dodržování provozních limitů různého druhu jako primární způsob dosažení správné rovnováhy. Takové limity v mnoha případech odstraňují potřebu okamžitých úsudků, přičemž zaměření se pouze na dodržování předem

definovaného rámce podceňuje přímý příspěvek provozních manažerů k bezpečnosti na základě jejich odborného úsudku [16].

1.4.1 Hrozby v provozní bezpečnosti

Hrozby PB (obr. 4) mohou ohrozit provoz vybraného objektu, popřípadě jej úplně vyřadit z funkčnosti. Mezi faktory, které mají vliv na bezpečnost řadíme například řídící systémy, provozní technologie, informace, události a procesy organizace. Jednotlivé hrozby jsou u každého druhu referenčního objektu rozdílné, v závislosti na povaze zabezpečení, vnějších faktorech a druhem objektu. Jednotlivé objekty mohou být ohrožovány jinými hrozbami, které ohrožují jeho provoz [6].



Obr. 4: Hlavní hrozby PB, ovlivnitelné výše zmíněnými faktory (upr. z [6]).

Konvergovaná bezpečnost představuje integrovaný přístup k ochraně organizace, informací a prostředí, který spojuje fyzickou, kybernetickou a provozní bezpečnost do jednotného rámce. Tento komplexní přístup umožňuje organizacím lépe identifikovat, hodnotit a řídit různé druhy bezpečnostních hrozeb a rizik a poskytuje větší efektivitu, flexibilitu a reaktivitu při reakci na tyto hrozby. Tím pomáhá organizacím lépe chránit svá aktiva, zachovat kontinuitu provozu a minimalizovat dopad bezpečnostních incidentů a hrozeb. V konečném důsledku přispívá k posílení celkové bezpečnosti a odolnosti organizace vůči stále se měnícím bezpečnostním výzvám a hrozbám [5].

2 ASPEKTY KONVERGOVANÉ BEZPEČNOSTI V PRÁVNÍCH PODMÍNKÁCH ČR

Konvergovaná bezpečnost z pohledu práva České republiky představuje integrovaný přístup k bezpečnosti, který spojuje fyzickou a kybernetickou bezpečnost a soustředí se na ochranu lidí, zařízení, informací a prostředí před různými hrozbami a riziky. Zásady konvergované bezpečnosti se mohou lišit v závislosti na konkrétní právních předpisech a regulačním prostředí dané země.

I když v ČR není přímo definován právní termín "konvergovaná bezpečnost", některé zákony a předpisy poskytují rámec pro provádění integrovaných bezpečnostních opatření [6, 18].

2.1 Zákon o kybernetické bezpečnosti (č. 181/2014 Sb.)

Tento zákon stanovuje zásady pro ochranu kybernetické infrastruktury a kritických informačních systémů v České republice. Klíčovými cíli tohoto zákona je zvýšit bezpečnost infrastruktury státu a důležitých informačních systémů, kde jsou uchovávány osobní údaje velkého počtu lidí a také je zajistit bezpečnostní standardy a ochranu kybernetického prostoru, což je základní součástí konvergované bezpečnosti [19].

2.2 Zákon o ochraně osobních údajů (č. 110/2019 Sb.)

Tento zákon upravuje zpracování osobních údajů a zajišťuje jejich ochranu v souladu s právem Evropské unie, zejména s nařízením GDPR. Cílem zákona je zkvalitnění kontroly při manipulací s osobními daty osob, což pro podniky to znamená zavádění přísnějších pravidel při zpracování osobních údajů. Ochrana osobních údajů je důležitým aspektem konvergované bezpečnosti, zejména v kontextu kybernetické bezpečnosti a ochrany soukromí [20].

2.3 Zákon o bezpečnosti práce (č. 309/2006 Sb.)

Tento zákon stanovuje povinnosti zaměstnavatelů a pracovníků v oblasti bezpečnosti a ochrany zdraví při práci. Zahrnuje opatření k prevenci pracovních úrazů a ochranu zdraví zaměstnanců, což může zahrnovat i opatření týkající se fyzické a provozní bezpečnosti pracovních prostor [21].

2.4 Zákon o krizovém řízení (č. 240/2000 Sb.)

Tento zákon upravuje postupy a opatření pro řízení krizových situací a ochranu obyvatelstva v případě mimořádných událostí. Zahrnuje plánování a koordinaci opatření pro ochranu kritické infrastruktury a zajištění kontinuity provozu, což může být součástí konvergované bezpečnostní strategie [22].

Tyto právní předpisy poskytují základní rámec pro konvergovanou bezpečnost v České republice a definují povinnosti a zodpovědnosti subjektů v oblasti kybernetické bezpečnosti, ochrany osobních údajů, bezpečnosti práce a krizového řízení. Organizace a podniky by měly tyto právní předpisy dodržovat a přizpůsobit své bezpečnostní opatření a postupy v souladu s jejich požadavky.

3 PENALIZAČNÍ FAKTORY

Penalizační faktory slouží k vyhodnocení bezpečnosti na chráněném prostoru, jejichž cílem je vytvořit seznam pevných faktorů, která jsou obecně platná. K nim jsou přiřazeny hodnoty, které popisují, jak moc je daný faktor pro objekt (organizaci) důležitý a jak moc poklesne odolnost při jeho absenci, narušení, poškození, poplachovém stavu atd.

3.1 Odolnost a její hodnocení

Odolnost je jedním ze základních parametrů, které jsou sledovány v rámci individuální bezpečnosti.

Průběžná a aktuální znalost úrovně odolnosti systému ochrany umožňuje řešit jednotlivá narušení bezpečnosti a provádět účinná nápravná opatření. Pokud dojde ke zhoršení parametrů jednotlivých ochranných systémů v důsledku nedostatků v organizace a zabezpečení, z důvodu technických poruch nebo z důvodu klimatických podmínek, jeho snižuje se také odolnost [23].

Jako hodnocení odolnosti označujeme schopnost opatření referenčního objektu chránit aktiva a zvládat narušení bezpečnosti v aktuálním stavu. Tento stav odolnosti sledujeme snímáním projevů (nebo změn) vnějších a vnitřních činitelů. Obecně platí, že jakákoli změna v odolnosti se může kvalitativně nebo kvantitativně projevit, a lze tudíž posoudit účinky a dopady na odolnost referenčního objektu. Posouzení odolnosti je tedy většinou založeno na snímání těchto změn stavu činitelů (faktorů), které se podstatně promítají do změn odolnosti. Díky hodnocení odolnosti v reálném čase je poté možno identifikovat nebezpečnou situaci a umožnit přijetí adekvátních opatření k ochraně majetku, obnovení odolnosti a k nápravě [6, 23].

Odolnost referenčního objektu se stanovuje jako abstraktní hodnota, která se vyjadřuje ve stanoveném rozmezí od 100 do 0. Absolutní odolnost (ideální stav) je nastavena na hodnotu 100, a tudíž spodní hranice odolnosti referenčního objektu je vyjádřena hodnotou 0. K dosažení výchozí hodnoty odolnosti (100) musí mít systém ochrany implementován všechna požadovaná opatření, přičemž nedošlo k žádné penalizaci. Pokud byla všechna opatření překonána narušitelem, došlo k narušení všech aktiv nebo má systém ochrany nefungující opatření, dojde k dosažení nulové hodnoty.

Penalizace poté posuzuje, jak se úroveň odolnosti systému ochrany při změně stavu snížila. Ve vztahu k určitým aktivům jsou všechny klíčové faktory, které popsují změny v odolnosti systému ochrany označovány jako penalizační faktory [7].

3.2 Dělení penalizačních faktorů

Penalizační faktory jsou děleny na dvě skupiny, a to statické a dynamické.

Statické faktory působí určitý dlouhodobý stav v objektu až do okamžiku, kdy jsou odstraněny. Statické penalizační faktory jsou obvykle faktory, které zůstávají relativně konstantní nebo se mění jen pomalu v čase a jsou často spojeny s infrastrukturou, prostředím nebo zavedenými procesy [24]. Je důležité je identifikovat a řešit při plánování a provádění bezpečnostních opatření, protože mohou představovat trvalé riziko a ohrožovat bezpečnost objektu. Jejich minimalizace a řešení může vyžadovat strategické investice a systematický přístup k řízení bezpečnosti [25].

Dynamické faktory se velmi rychle mění v čase a popisují nám bezprostřední bezpečnostní situaci [6]. Identifikace a monitorování dynamických penalizačních faktorů je klíčovým aspektem efektivního řízení bezpečnosti, protože umožňuje organizaci reagovat na aktuální hrozby a rizika a přijímat relevantní opatření k minimalizaci jejich dopadu [24].

3.3 Katalog penalizačních faktorů

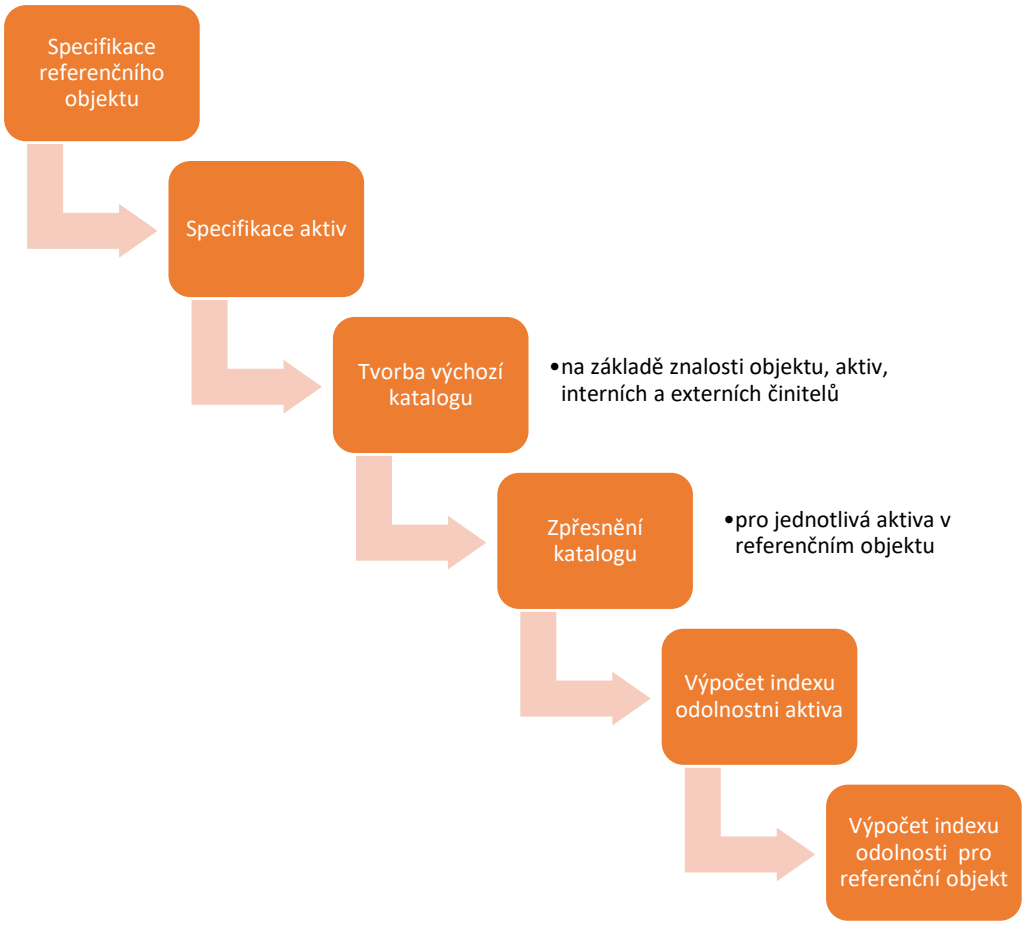
Obecný katalog penalizačních faktorů je přehledem všech možných interních a externích faktorů, jež můžou ovlivnit odolnost referenčního objektu z pohledu konvergované bezpečnosti. Je sestavován vzhledem k chráněným aktivům a potenciálním hrozbám (rizikům), a představuje v rámci hodnocení odolnosti objektů hlavní nástroj při využití metody penalizace. Nezávisle na typu referenčních objektů tedy obsahuje široký seznam všech penalizačních faktorů napříč druhy bezpečnosti (fyzická, informační, kybernetická, provozní), které konvergovaná bezpečnost zahrnuje [6,25].

Hodnoty penalizací jsou zde poté pro jednotlivé kvantifikace určeny na základě expertního odhadu. Bodové hodnoty penalizačních faktorů nabývají hodnot 1 až 10, přičemž hodnota 1 vyjadřuje minimální snížení odolnosti a hodnota 10 kritické narušení odolnosti objektu.

Při znalosti konkrétního referenčního objektu, upravujeme katalog dle daného aktiva a vybíráme před výpočtem odolnosti ty penalizační faktory které jsou pro podnik relevantní a vztahují se k chráněnému aktivu a rizikům, které na aktivum působí. U konkrétních příkladů poté v rámci aplikace katalogu můžeme také přiřazovat váhy (v rozmezí hodnot 1- 5), jejichž

cílem je určit důležitější aktiva. Hodnota 1 vyjadřuje menší vliv a dopad faktoru na aktivum, zatímco hodnota 5 dopad maximální [6, 24].

Postup tvorby katalogu penalizačních faktorů pro daný referenční objekt je znázorněn na obr.5.



Obr. 5: Etapy tvorby katalogu penalizačních faktorů pro vyhodnocení odolnosti konkrétního objektu (přepracováno z [6]).

Výsledný obecný katalog penalizačních faktorů obsahuje plný výčet relevantních statických a dynamických faktorů z pohledu konvergované bezpečnosti, tudíž faktory pro provozní bezpečnost, fyzickou bezpečnost a kybernetickou bezpečnost.

Tyto penalizační faktory z obecného katalogu se poté využívají při výpočtu indexů odolnosti referenčního objektu I_{ro} [6].

3.4 Výpočet indexu odolnosti

Ve výpočtu indexu odolnosti posuzujeme aktuální stav ochrany systému ze statického a dynamického hlediska. Statická část je primárně závislá na opatřeních přijatých k zajištění bezpečnosti (udává výchozí úroveň odolnosti). Dynamická část, která představuje dopady narušení bezpečnosti či poruchy atd. je poté od této hodnoty odečítána.

Index odolnosti aktiva se počítá pro každý druh bezpečnosti odděleně, zatímco index odolnosti referenčního objektu představuje agregaci (prostý průměr/ využití vah) všech indexů odolnosti pro jednotlivé druhy bezpečnosti.

Výpočet indexu statické odolnosti aktiva I_{ods} je poté definován jako:

$$I_{ods} = 100 - \frac{\sum_{i=1}^{n} P_{si} * V_i}{P_{smax}} * 100 \quad (1)$$

Přičemž

$$P_{smax} = \sum_{i=1}^{x} P_{si} * V_i \quad (2)$$

Tab. 1: Popis členů rovnice (1) a (2).

$\boldsymbol{n}$	celkový počet aktivních statických penalizačních faktorů v daném druhu bezpečnosti pro zvolené aktivum
$\boldsymbol{P_{si}}$	i-tý aktivní statický penalizační faktor v daném druhu bezpečnosti
$\boldsymbol{V_i}$	váha statického penalizačního faktoru vzhledem k danému aktivu (v rozmezí 1–5)
$\boldsymbol{P_{smax}}$	suma všech statických penalizačních faktorů v daném druhu bezpečnosti pro zvolené aktivum; výpočet dle rovnice 2
$\boldsymbol{x}$	celkový počet statických penalizačních faktorů pro zvolené aktivum v daném druhu bezpečnosti

Vzhledem k tomu, že referenční objekt zahrnuje zpravidla více aktiv, musí být tedy pro každý druh bezpečnosti nejprve stanoveny indexy odolnosti jednotlivých aktiv.

Výpočet indexu odolnosti aktiva z pohledu fyzické I_{fai}, kybernetické I_{kai} a provozní bezpečnosti I_{pai} je poté definován jako:

$$I_{f,k,p\ ai} = I_{ods} - \frac{\sum_{j=1}^{m} P_{dj} * V_j}{P_{dmax}} * I_{ods} \quad (3)$$

Přičemž

$$P_{dmax} = \sum_{j=1}^{y} P_{dj} * V_j \quad (4)$$

Tab. 2: Popis členů rovnice (3) a (4).

$\boldsymbol{I_{ods}}$	index statické odolnosti aktiva
$\boldsymbol{m}$	celkový počet aktivních dynamických penalizačních faktorů v daném druhu bezpečnosti pro zvolené aktivum
$\boldsymbol{P_{dj}}$	j-tý aktivní dynamický penalizační faktor v daném druhu bezpečnosti
$\boldsymbol{P_{dmax}}$	suma všech dynamických penalizačních faktorů v daném druhu bezpečnosti pro zvolené aktivum
$\boldsymbol{V_j}$	váha dynamického penalizačního faktoru vzhledem k danému aktivu (v rozmezí 1–5)
$\boldsymbol{y}$	celkový počet dynamických penalizačních faktorů pro zvolené aktivum v daném druhu bezpečnosti

Výsledné hodnoty jsou v rozmezí 0–100, přičemž hodnota 0 představuje nulovou odolnost, zatímco hodnota 100 vyjadřuje odolnost maximální.

Následně se z indexů odolnosti aktiv I_{fai}, I_{kai}, I_{pai} pro jednotlivé druhy bezpečnosti agregací vypočítá index odolnosti aktiva I_{ai} průměrem (5), nebo s přihlédnutím k váhám (6).

$$I_{ai} = \frac{I_{fai} + I_{kai} + I_{pai}}{u} \quad (5)$$

$$I_{ai} = \sum_{i=1}^{u} (I_{f,k,p\ ai} * V_i) \quad (6)$$

Tab. 3: Popis členů rovnice (5) a (6).

$I_{f,k,p\,ai}$	index odolnosti daného druhu bezpečnosti (f, k, p) i-tého aktiva
u	počet druhů bezpečnosti
V_i	váha druhu bezpečnosti pro i-té aktivum (součet vah musí být roven 1)

Posledním krokem je výpočet indexu odolnosti referenčního objektu I_{ro}, který vyjadřuje míru aktuální ochrany aktiva referenčního objektu proti rizikům, která spadají do jednotlivých druhů bezpečnosti. Je tvořen agregací dílčích indexů odolnosti aktiv I_{ai} do výsledného indexu odolnosti I_{ro} celého referenčního objektu. Opět můžeme vypočítat průměrem (7) nebo s váhováním (8).

$$I_{ro} = \frac{\sum_{i=1}^{u} I_{ai}}{u} \tag{7}$$

$$I_{ro} = \sum_{i=1}^{u} (I_{ai} * V_i) \tag{8}$$

Tab. 4: Popis členů rovnice (7) a (8).

I_{ai}	index odolnosti i-tého aktiva
u	počet aktiv
V_i	váha i-tého aktiva v referenčním objektu (součet vah musí být roven 1)

Důležité pro hodnocení odolnosti jsou primárně změny v čase. Tudíž dochází-li ke snižování hodnoty indexu odolnosti je snižována i odolnost systému ochrany, což by mělo by vést k aktivaci opatření, čímž se by měla hodnota indexu odolnosti opět navyšovat.

3.5 Kvantifikace penalizačních faktorů a některé metody

Výpočet indexů odolnosti referenčního objektu I_{ro} se odvíjí od správného nastavení penalizací identifikovaných penalizačních faktorů, přičemž existuje několik metod pro jejich kvantifikaci.

3.5.1 Multikriteriální hodnocení velikosti penalizace

Metoda je založena na stanovení hodnoty penalizace na základě kritérií, jež jsou ohodnoceny v závislosti na charakteru samotného penalizačního faktoru a jeho atributů. Index penalizace

P, je ukazatelem výše penalizace penalizačního faktoru. Index snížení odolnosti P_o vyjadřuje, do jaké míry má vliv penalizačního faktoru na snížení odolnosti systému ochrany. Hodnocení nabývá hodnot 4 (přímé snížení vlivu) nebo 1 (nepřímé snížení vlivu). Index rozsahu vlivu P_r sděluje z pohledu referenčního objektu rozsah působnosti faktoru, tzn. lokální (hodnota 1) nebo plošný (hodnota 2). A kritérium kritičnosti P_k ukazuje naléhavost vlivu na změny odolnosti, tudíž nenaléhavý (hodnota 1), naléhavý (hodnota 2). Výpočet pro daný referenční objekt je poté definován takto:

$$P = Po * Pr * Pk \tag{9}$$

3.5.2 Metoda založená na expertním odhadu

Specifika referenčního objektu jsou hodnocena na základě poznání a vypsání penalizačních faktorů z pohledu konvergované bezpečnosti. Faktorům jsou přiřazeny hodnoty, které vyjadřují míru důležitosti daného faktoru pro referenční objekt a pomocí vah jsou poté ještě faktory upraveny dle určení dopadu pro konkrétní aktivum.

Tab. 5: Dělení faktorů do skupin, jejich dopad a hodnocení.

Skupina	**V případě narušení**	**Hodnota**
Kritické faktory	Zničení objektu/ zastavení činnosti	100-80
Významné faktory	Výrazné omezení činnosti/ významné narušení procesů	79-50
Málo významné faktory	Narušení provozu/ činnosti, ale bez významné následky	49-20
Zanedbatelné faktory	Při opakujícím se výskytu mohou poškodit objekt/ omezit jeho činnost	19-1

3.5.3 Fullerova metoda

Fullerova metoda se zpravidla užívá v situacích, kdy je pro hodnotitele obtížné obodovat jednotlivá kritéria kvůli velkému počtu kritérií. Hodnotitel při použití této metody určuje, které z kritérií má větší vliv na odolnost aktiva, přičemž se rozhoduje vždy pouze mezi dvěma kritérii. Principem je předkládání dvojic kritérií, které se sestavují do tzv. Fullerova trojúhelníku. Důležitějšímu kritériu pro hodnocení odolnosti aktiva je poté přidělena 1 bod, pokud jsou obě kritéria stejně důležitá tak jen 0,5 bodu oběma kritériím. Po sečtení počtu bodů v řádku a sloupci určíme, která kritéria mají na odolnost aktiva větší vliv [6].

Penalizační faktory zahrnují různé nedostatky a slabiny, které snižují úroveň bezpečnosti organizace. Patří sem například nedostatečná fyzická ochrana, zranitelné kybernetické systémy, nedostatečné školení personálu, nedostatečné řízení rizik a nedbalost ve splnění právních a regulačních požadavků. Tyto faktory mohou vést k nebezpečným situacím, ztrátám dat, finančním ztrátám, poškození reputace organizace a dalším negativním následkům. Identifikace a řešení penalizačních faktorů jsou klíčové pro posílení bezpečnosti a ochrany organizace před riziky a hrozbami [23].

4 ANALÝZA RIZIK V KONVERGOVANÉ BEZPEČNOSTI

Analýza rizik je charakterizována jako proces, zahrnující vymezení rizik, určení míry jejich závažnosti a jejich dopad na aktiva, a také stanovení pravděpodobnosti jejich uskutečnění. Analýza rizik v konvergované bezpečnosti poté zahrnuje komplexní posouzení různých typů rizik, která mohou ohrozit fyzickou, kybernetickou a informační bezpečnost organizace. Tento integrovaný přístup umožňuje organizacím efektivněji identifikovat, hodnotit a řídit rizika napříč různými bezpečnostními doménami [26, 27].

4.1 Klíčové aspekty

Jelikož je analýza rizik komplexní proces, je třeba při jejich vypracovávání postupovat metodicky. Při vlastní analýze rizik je tedy aplikován obecný postup za sebou následujícími obecnými činnostmi v určité posloupnosti.

Obr. 6: Klíčové kroky analýzy rizik v konvergované bezpečnosti.

I. Identifikace rizik:

Fyzická rizika jsou spojena s fyzickými útoky, přírodními katastrofami, krádežemi, vandalismem a dalšími fyzickými hrozbami. Kybernetická rizika spojujeme s kybernetickými útoky, hackingem, malwarem, phishingem a dalšími hrozbami pro informační systémy. Zatímco informační rizika souvisí s únikem nebo krádeží citlivých informací, neautorizovaným přístupem a nedodržením ochrany osobních údajů.

II. Identifikace aktiv:

Spočívá ve vytvoření soupisu všech aktiv, spolu s názvem a umístěním daného aktiva.

III. Posouzení rizik:

Posuzujeme pravděpodobnost, s jakou může dojít k identifikovaným rizikům. Dopadem je poté myšleno hodnocení závažnosti dopadu jednotlivých rizik na organizaci, včetně finančních ztrát, poškození reputace, přerušení provozu a dalších důsledků. A následně je na místě použití kombinace hodnocení pravděpodobnosti a dopadu k vytvoření celkového hodnocení rizik, které pomůže určit jejich prioritizaci.

IV. Kategorizace a prioritizace rizik:

Rizika jsou kategorizována a prioritizována na základě jejich celkového hodnocení, přičemž nejvyšší prioritu mají rizika s vysokou pravděpodobností a vysokým dopadem.

V. Návrh opatření:

Preventivní opatření jsou zaměřena na prevenci vzniku rizik, jako je zlepšení fyzické bezpečnosti, posílení kybernetických ochranných mechanismů a implementace politik pro ochranu informací. Zmírňující opatření se zaměřují na zmírnění dopadu rizik, pokud k nim dojde, jako je zavedení záložních systémů, plány reakce na incidenty a krizový management. A detekční opatření zahrnují implementace systémů pro detekci bezpečnostních hrozeb a incidentů v reálném čase.

VI. Implementace a monitorování:

Za implementací opatření se skrývá realizace navržených opatření v praxi, včetně školení zaměstnanců, nasazení technologií a vytvoření procedur. A následně je nutno pravidelné monitorování účinnosti implementovaných opatření a přezkum analýzy rizik, aby se zajistilo, že rizika jsou řádně řízena a opatření jsou aktuální [26, 27].

Pro komplexní pojetí analýzy rizik je nutno také doplnit analýzu hrozeb. Hrozba je činitel, působící chráněné aktivum, nebo bezpečnostní opatření. Hrozby se zpravidla rozdělujme dle úmyslu (náhodné/ úmyslné) a dle zdroje (vnitřní/vnější). Náhodné hrozby jsou ty, ke kterým může dojít bez předchozího úmyslu. Často jsou to hrozby přírodního původu (povodeň, zemětřesení, požár atd-), nebo se jedná o technické selhání – (výpadek proudu, dopravní nehoda, kontaminace vod atd.), nebo o lidskou chybu. Úmyslná hrozba je promyšlena a připravena dopředu, přičemž je stvořena a spuštěna konkrétním jedincem (či více jedinci). Řadíme sem většinou trestnou činy jako je krádež, teroristický útok, ozbrojený konflikt ale také např. zneužití pravomocí nebo neoprávněný přístup. Vnitřní hrozby jsou ty, které pochází zevnitř uvažované společnosti (techn. závada, pochybení, úmysl). Vnější poté logicky ty, co pochází zvnějšku (útok, pohroma) [29].

Díky integrovanému přístupu konvergované bezpečnosti je umožněn komplexní a koherentní přístup k řízení rizik napříč fyzickou, kybernetickou a informační bezpečností. Díky aplikaci analýzy rizik je poté organizace lépe připravena na různé typy hrozeb a může rychleji a efektivněji reagovat a také dochází k optimalizaci využití zdrojů a investic do bezpečnosti tím, že se vyhýbá duplikaci úsilí a maximalizuje efektivitu bezpečnostních opatření. Analýza rizik také zvyšuje celkovou odolnost organizace vůči bezpečnostním incidentům a zlepšuje schopnost zotavit se z krizových situací.

4.2 Vybrané metody analýzy rizik

Pro přijetí opatření a zajištění připravenosti na řešení mimořádných událostí je analýza rizik a její následné hodnocení nezbytné. Metod analýzy rizik existuje několik, a právě proto je důležitým faktorem výběr správné metody v závislosti na účelu, pro který je konkrétní analýza rizik určena. Níže jsou popsány některé z metod, z nichž jedna byla využita v praktické části této diplomové práce.

4.2.1 Checklist

Metoda kontrolního seznam (neboli Checklist) je jednoduchý a účinný nástroj pro identifikaci a hodnocení rizik. Používá se k systematickému ověření, zda byly všechny potenciální rizikové faktory a nebezpečí zohledněny a adekvátně řízeny. Tato metoda je oblíbená díky své jednoduchosti, snadné použitelnosti a efektivitě při identifikaci rizik.

Mezi hlavní výhody této metody patří jednoduchost a efektivita, jelikož je metoda snadno použitelná a efektivní při identifikaci a řízení rizik, což ji činí vhodnou pro širokou škálu

aplikací. Poskytuje strukturovaný a systematický způsob kontroly a hodnocení rizik, což zajišťuje, že žádný aspekt bezpečnosti není opomenut. Pomáhá také vytvořit jasnou a transparentní dokumentaci identifikovaných rizik a přijatých opatření. Kontrolní seznamy lze snadno přizpůsobit specifickým potřebám organizace nebo projektu.

4.2.2 PNH

PNH je metoda analýzy rizik používaná k identifikaci a hodnocení potenciálních nebezpečí a hrozeb v raných fázích projektu nebo systému. Tato metoda je podobná PHA (Preliminary Hazard Analysis), ale specificky se zaměřuje na identifikaci a hodnocení hrozeb, které by mohly negativně ovlivnit bezpečnost a provozní integritu systému.

Výsledné riziko (R) je u této metody výsledkem násobku pravděpodobnosti vzniku (P); závažnosti potenciálních následků (N) a názoru hodnotitelů (H), ten zahrnuje všechna různá kritéria, včetně vlivu pracovního prostředí, úrovně údržby atd. Zmíněným parametrům se poté obvykle přiděluje hodnota vzestupně od 1-5 (viz *tab. 6. – 9*) [30, 31].

Tab. 6: Význam bodového hodnocení u parametru P [upraveno z 31].

Pravděpodobnost vzniku	**Hodnocení**
Zanedbatelná	1
Nepravděpodobná	2
Pravděpodobná	3
Velmi pravděpodobná	4
Téměř jistá	5

Tab. 7: Význam bodového hodnocení u parametru N [upraveno z 31].

Závažnost následků	**Hodnocení**
Bez následků	1
Mírné následky	2
Významné následky	3
Velmi významné následky	4
Katastrofické následky	5

Tab. 8: Význam bodového hodnocení u parametru H [upraveno z 31].

Názor hodnotitelů	**Hodnocení**
Zanedbatelný vliv na míru nebezpečí a ohrožení	1
Malý vliv na míru nebezpečí a ohrožení	2
Větší, nezanedbatelný vliv na míru nebezpečí a ohrožení	3
Velký a významný vliv na míru nebezpečí a ohrožení	4
Více významných a nepříznivých vlivů na závažnost a následky nebezpečí a ohrožení	5

Tab. 9: Výsledkové hodnocení míry rizika R [upraveno z 31].

Rizikový stupeň	**R**	**Míra rizika**
I.	> 100	Nepřijatelné riziko
II.	100 – 51	Nežádoucí riziko
III.	50 - 11	Mírné riziko
IV.	10 - 3	Akceptovatelné riziko
V	< 3	Bezvýznamné riziko

Celkové hodnocení míry rizika je poté následující: dle tabulky uvedené výše, je následující: Rizikový stupeň I. (Nepřijatelné riziko) – nutné okamžité zavedení bezpečnostních opatření. Může znamenat katastrofické důsledky (smrt, zastavení činnosti, krach společnosti atd).

Rizikový stupeň II. (Nežádoucí riziko) – nutné urychlené zavedení bezpečnostních opatření. Rizikový stupeň III. (Mírné riziko) – nutno zavést bezpečnostní opatření dle daného plánu ve stanoveném termínu.

Rizikový stupeň IV. (Akceptovatelné riziko) – přijatelné po informovaném souhlasu vedení společnosti.

Rizikový stupeň V. (Bezvýznamné riziko) – není vyžadováno zavedení opatření

Mezi hlavní výhody patří včasná identifikace rizik, tudíž identifikace potenciálního nebezpečí a hrozeb v rané fázi, což může zabránit vzniku problémů později. A také systematický přístup, jež poskytuje strukturovaný způsob, jak identifikovat a hodnotit rizika. A samozřejmě také zlepšení bezpečnosti tím, že identifikuje a minimalizuje potenciální nebezpečí a také poskytuje cenné informace pro informované rozhodování o bezpečnostních opatřeních a investicích [32].

4.2.3 HRA

Metoda HRA (Hazard and Risk Analysis, česky Analýza nebezpečí a rizik) je systematický přístup k identifikaci, hodnocení a řízení rizik spojených s nebezpečími v různých oblastech, jako jsou průmyslové procesy, stavebnictví, doprava a další. Tato metoda je navržena tak, aby poskytla detailní pochopení nebezpečí a jejich potenciálních dopadů, což umožňuje přijmout účinná opatření ke zmírnění rizik.

Hlavní výhodou této metody je komplexní přístup díky detailnímu a systematickému přístupu k identifikaci a hodnocení rizik, což zajišťuje, že žádný aspekt rizika není opomenut. Také poskytuje strukturované informace a analýzy, které podporují informované rozhodování o bezpečnostních opatřeních a investicích. Výhodou je také její flexibilita, jelikož ji lze přizpůsobit různým typům organizací a odvětví, což z ní činí univerzální nástroj pro řízení rizik [30, 31].

Analýza rizik pomáhá identifikovat a hodnotit kombinované hrozby, řídit rizika napříč fyzickými a kybernetickými doménami, zajišťovat kontinuitu provozu, plnit právní a regulační požadavky a zvyšovat povědomí a školení zaměstnanců. V konečném důsledku přispívá k vytvoření robustního a integrovaného systému ochrany. Analýza rizik v konvergované bezpečnosti je tedy klíčovým nástrojem pro moderní organizace, které čelí širokému spektru bezpečnostních hrozeb v propojeném světě.

Cílem teoretické části této diplomové práce bylo stručně shrnou důležitost konvergované bezpečnosti v moderním světě. Byla popsány jak její jednotlivé bezpečnosti, tak její aspekty na právo ČR. V souvislosti s reálným využitím konvergované bezpečnosti v praxi se další části diplomové práce zaobírají tématikou penalizačních faktorů a analýzy rizik , včetně jejich hodnocení a metod.

II. PRAKTICKÁ ČÁST

5 ANALÝZA SOUČASNÉHO STAVU OCHRANY VE VYBRANÉM OBJEKTU

Vybraným objektem je společnost, která byla založena v roce 2010 a byla zaměřena na výrobu a svařování malých železných dílců. Výroba byla nejdříve v malé dílně u rodinného domu zakladatele. V roce 2011 byli najati další tři zaměstnanci na svařování a výrobu dílů.

Společnost se pomalu rozrůstala až v roce 2020 přišlo stěhování do nových a větších prostor. Zakladatel společnosti zjistil, že je potřeba více zaměstnanců, kteří budou mít na starosti příjem objednávek, obsluhu a vývoj softwaru do automatických výrobních strojů, zajištění základního servisu, nákup materiálu a podobně.

K roku 2024 má společnost asi 40 zaměstnanců, kteří pracují na dvousměnný provoz a 10 zaměstnanců kteří pracují na jednosměnný provoz. Jejich 20 stabilních odběratelů jim vytěžuje výrobu asi na 85 % a zbylých 15 % výroby jsou malé zakázky, kde se snaží společnost inovovat ve výrobě. Společnost se pomalu rozrůstá a vedení společnosti zvažuje založení dceřiné výroby na Slovensku.

5.1 Specifikace vybraného referenčního objektu

Sídlo společnosti se nachází v uzavřeném objektu, ve kterém je více výrobních hal pro jiné společnosti. Do tohoto objektu je jen jedna příjezdová brána a celý objekt je hlídán ostrahou, která hlídá 24 hodin denně a vjezdová brána je monitorována kamerovým systémem se záznamem, který přenáší obraz na pracoviště ostrahy. Každé vozidlo se musí nahlásit ostraze a jednotlivci, kteří chtějí do areálu musí projít kolem ostrahy.

Vybraná společnost má ve vlastnictví dvě sousedící budovy. První má dvě nadzemní podlaží. V přízemí budovy je zázemí pro zaměstnance a v prvním nadzemním patře jsou administrativní prostory. V druhé budově se nachází výroba a sklad drobného materiálu. Rozměrnější materiál je skladován ve venkovních kryté hale, která je umístěna za budovami na pozemku oploceném drátěným plotem.

Zabezpečení oken je realizováno na všech oknech administrativní budovy, a to magnetickými kontakty. Vchod pro zaměstnance a návštěvníky je z přední strany administrativní budovy. Každý zaměstnanec má čipovou kartu na své jméno, přes kterou je řešen vstup a výstup z budovy a zároveň i monitorována docházka zaměstnanců. Pro návštěvníky je u dveří umístněný zvonek do kanceláře sekretariátu, odkud jsou puštěni dovnitř nebo návštěvu

někdo vyzvedne. Nákladová brána je uzavřena a otvírá se pouze pokud přijede nový materiál nebo se vyskladňují zhotovené výrobky.

Perimetrická ochrana je řešena kamerovým systémem, který snímá prostor venkovního oploceného areálu a prostor nákladní brány. Obrazové záznamy z kamer se přenášejí na monitor umístněný v kanceláři v administrativní budově v prvním nadzemním podlaží. Zde se zobrazují obrazové záznamy ze všech kamer v objektu, záznamy se také ukládají na uložiště, které se nachází v budově.

Vnitřní prostory jsou chráněny umístněným kamerovým systémem, který snímá vstupní dveře a dveře do prvního nadzemního podlaží. V prvním nadzemním podlaží jsou také instalovány pohybové detektory, které jsou deaktivovány po vstupu oprávněného zaměstnance, zadáním přístupového hesla. V obou budovách je nainstalován systém EPS (elektrické požární signalizace). Výstup z PZTS (poplachový zabezpečovací a tísňový systém) a EPS není nikam přenášen, informace se zobrazují notifikací na mobilním telefonu vybraným zaměstnancům a ti to dále řeší. Veškeré informace se ukládají na uložiště.

Kybernetická bezpečnost je řešena vlastní sítí, do které jsou připojeny všechny počítače, přístupové heslo každého zaměstnance se pravidelně mění. Každý zaměstnanec má přístup jen k datům, které potřebuje ke své práci. Přístup k datům každého zaměstnance určuje správce sítě. Na počítačích je nainstalován antivirový program. Zaměstnanci mají zakázáno instalovat jakékoliv programy, k počítači lze připojit jakékoliv další zařízení (přenosné disky a podobně). Veškerá zařízení májí připojení i internetu, webové stránky nepodléhají kontrole ani stahování příloh emailu není nijak kontrolováno. Upozornění na výskyt škodlivých kódů v stahovaných souborech provádí antivirový program.

Provozní bezpečnost je v objektu řešena pouze sledováním dodávky elektrické energie, kdy při výpadku elektrické energie se důležitá zařízení automaticky připojí k náhradnímu zdroji energie (baterii).

5.2 Analýza rizik

Pro zajištění bezpečnosti a bezpečného provozu vybrané společnosti byly na základě definovaných aktiv analyzována rizika a hrozby. Implementace analýzy rizik umožňuje firmě připravit se na možné nouzové situace tím, že identifikuje potenciální rizika a vypracuje plány reakce na mimořádné události. Na základě analýzy rizik byly také identifikovány

potenciální hrozby, které by mohly vést k poškození vybavení nebo materiálů, např. svařovacího zařízení a materiálů, které jsou velmi drahé.

5.2.1 Identifikace a hodnocení aktiva

Hmotná a nehmotná aktiva ve společnosti byla identifikována a ohodnocena, přičemž byla využita následující stupnice:

Tab. 10: Stupnice pro hodnocení aktiv [vlastní zpracování].

Hodnota	Popis důležitosti
0	Zanedbatelná
1	Velmi nízká
2	Nízká
3	Střední
4	Vysoká
5	Velmi vysoká

V následujících tabulkách jsou rozepsány jednotlivé skupiny aktiv a jejich hodnocení důležitosti pro společnost.

Tab. 11: Informační aktiva společnosti [vlastní zpracování].

Strategické informace (strategie, know -how...)	5
Osobní údaje (zaměstnanci)	4
Obchodní dokumentace (dodavatelé, odběratelé, smlouvy)	5
Systémová dokumentace a jiné informace	3

Tab. 12: Osoby ve společnosti [vlastní zpracování].

Vedoucí pracovníci	4
Externí správce IT	3
Administrativní pracovníci	4
Pracovník pro vývoj	3
Dělníci výroby	4

Tab. 13: Prostory a objekty společnosti [vlastní zpracování].

Hranice pozemku	2
Budovy společnosti	4

Venkovní sklad materiálu	4
Vnitřní sklad drobného materiálu a náhradních dílu	4

Tab. 14: Hardwarové zařízení společnosti [vlastní zpracování].

Server	3
Pevná koncová zařízení (PC)	3
Mobilní zařízení	3
Tiskárny, skenery, kopírky	2

Tab. 15:Technická zařízení společnosti [vlastní zpracování].

Klimatizace a topení	3
Výrobní stroje	5
Silová kabeláž	2
Kancelářská technika	1

Tab. 16: Software společnosti [vlastní zpracování].

Databáze	3
Kancelářský SW (MS Office)	2
CNC program	3
Poštovní a komunikační SW (e-mail)	3
Antivirový SW, antispam	3

Tab. 17: Datová uložiště společnosti [vlastní zpracování].

Záložní a archivační média	4
Zařízení pro přenášení dat (USB flash disk)	2

Tab. 18: Komunikační zařízení společnosti [vlastní zpracování].

Komunikační linky externí - síťové (Internet)	3
Komunikační linky externí - telefonní	3
LAN (jako celek)	4
Kabeláž datová	3
Telefony mobilní	3

Tab. 19: Prostředky pro vývoj společnosti [vlastní zpracování].

Databáze	3
Testovací data	2
Prototypy	3

Tab. 20: Výrobní a zásobní materiál společnosti [vlastní zpracování].

Materiál	4
Náhradní díly	3
Zbytkový materiál	1

Tab. 21: Bezpečnost a řízení společnosti [vlastní zpracování].

Kamerový systém, PZTS, EPS	4
Havarijní plány	3
Bezpečnostní školení	2
Dokumentace bezpečnostních systémů (schémata, postupy, nastavení)	2
Bezpečnostní směrnice pro uživatele	3

Tab. 22: Ostatní [vlastní zpracování].

Klíče od místností	3
Přístupová hesla a kódy	4
Autentizační předměty (čipové karty)	5
Papírová dokumentace (systémová, programátorská, provozní...)	2
Uživatelská dokumentace (návod k použití)	1

Na základě identifikovaných a ohodnocených aktiv společnosti byly dále identifikovány a hodnoceny hrozby a rizika, které by mohly pro společnost znamenat závažné problémy spojené s finanční zátěží.

5.2.2 Hodnocení a identifikace hrozeb

Hodnocení hrozeb je klíčový proces, který umožňuje identifikovat, hodnotit a řídit rizika spojená s různými aspekty v našem případě svařování. Hrozby, které ohrožují vybraný objekt byly identifikovány a ohodnoceny dle možnosti výskytu hrozby uvedené v *Tab. 23*.

Tab. 23: Možnost výskytu hrozby [vlastní zpracování].

Hodnota	Popis
0	Žádná
1	Zanedbatelná
2	Nízká
3	Střední
4	Vysoká
5	Velmi vysoká
6	Jistá

Prvním krokem je identifikace všech potenciálních hrozeb a nebezpečí, které mohou ovlivnit zdraví a bezpečnost pracovníků, majetek a životní prostředí. V následujících tabulkách jsou tyto identifikované hrozby, které ohrožují vybrané objekty a k nim přiřazené ohodnocení uvedeny.

Tab. 24: Technické a technologické [vlastní zpracování].

Přerušení dodávky elektrické energie	5
Poruchy interní sítě (výpadky, špatné napětí...)	4
Poškozené zařízení (mobilní i pevná)	3
Porucha na zařízení (mobilní i pevná)	5
Špatné zabezpečení SW (hesla...)	3
Chyba přenosu dat	3
Nevyhovující provozní prostředí	1
Nedostatečné zabezpečení	3

Tab. 25: Přírodní [vlastní zpracování].

Povodně	2
Bouře	1

Oheň	4
Prach, špína	3
Vlhkost	2
Špatná teplota	1

Tab. 26: Způsobené lidským faktorem – úmyslné z vnějšího prostředí [vlastní zpracování].

Odposlech	1
Krádež	5
Neoprávněný vstup	6
Útok, napadení SW, HW (viry, phising...)	6
Cizí osoby (uklízečka, vrátný...)	3

Tab. 27: Způsobené lidským faktorem – úmyslné z vnitřního prostředí [vlastní zpracování].

Vandalismus	3
Úmyslná manipulace s daty	2
Neoprávněné užití systému IT	4
Zneužití oprávnění	5

Tab. 28: Způsobené lidským faktorem – neúmyslné [vlastní zpracování].

Použití vlastního zařízení	6
Jednoduchá, lehce napadnutelná hesla	5
Nedostatečná kvalifikace zaměstnanců	5
Nedostatečný, chybějící bezpečnostní management	3
Neoprávněné stahování a užívání SW	4
Nepřizpůsobení IT modernizací	2
Malé zabezpečení pro vzdálený přístup	2
Neproduktivní surfování po internetu	4

Z tabulek hrozeb byly vybrány hrozby, které dosahují minimální hodnoty 4 (Vysoká) a vyšší.

V kategorii Technické a technologické to jsou tři hrozby:

1. Přerušení dodávky elektrické energie s hodnotou 5.
2. Porucha interní sítě s hodnotou 4.

3. Porucha na zařízení s hodnotou 5.

V kategorii Přírodní hrozby je to jedna hrozba:

1. Prach, špína.

V kategorii Způsobené lidským faktorem – Úmyslné z vnějšího prostředí to jsou tři hrozby:

1. Krádež.
2. Neoprávněný vstup.
3. Útok, napadení SW, HW.

V kategorii Způsobené lidským faktorem – Úmyslné z vnitřního prostředí to jsou dvě hrozby:

1. Neoprávněné užití systému s hodnotou 4.
2. Zneužití oprávnění s hodnotou 5.

A v poslední kategorii Neúmyslné to je pět hrozeb:

1. Použití vlastního zařízení s hodnotou 6.
2. Jednoduchá, lehce napadnutelná hesla s hodnotou 5.
3. Nedostatečná kvalifikace zaměstnanců s hodnotou 5.
4. Neoprávněná stahování a užívání SW s hodnotou 4.
5. Neproduktivní surfování po internetu s hodnotou 4.

Po identifikaci hrozeb následovalo jejich hodnocení dle pravděpodobnosti výskytu a závažnosti dopadů. Identifikované hrozby byly použity jako atributy pro hodnocení rizik pomocí metody PNH.

5.2.3 Analýza rizik pomocí metody PNH

Z vybraných metod popsaných v teoretické části byla vybrána metoda PNH pro hodno rizik vybrané společnosti. Tato metoda byla zvolena na základě požadavku na systematický a strukturovaný postup, bezpečnost a provozní integritu systému.

Tab. 29: Metoda PNH [vlastní zpracování]

Technické a technologické	**P**	**N**	**H**	**R**
Přerušení dodávky elektrické energie	3	4	3	36
Poruchy interní sítě (výpadky, špatné napětí...)	3	3	2	18
Porucha na zařízení (mobilní i pevná)	4	5	3	60
Přírodní				
Prach, špína	3	4	3	36
Způsobené lidským faktorem				
Úmyslné z vnějšího prostředí				
Krádež	4	4	3	48
Neoprávněný vstup	3	4	3	36
Útok, napadení SW, HW (viry, phising...)	3	3	4	36
Úmyslné z vnitřního prostředí				
Zneužití oprávnění	3	3	2	18
Neúmyslné				
Použití vlastního zařízení (BYOD...)	3	3	3	27
Jednoduchá, lehce napadnutelná hesla	4	4	4	64
Nedostatečná kvalifikace zaměstnanců	2	3	2	12
Neoprávněné stahování a užívání SW	3	2	3	18
Neproduktivní surfování po internetu	4	4	4	64

Dle tabulky *Tab. 9.* uvedená v teoretické části se dělí míra rizika na pět rizikových stupňů a podle hodnot z *Tab. 29*. vzniklo toto rozdělení:

I. Rizikový stupeň (Nepřijatelné riziko).
   Do I. Rizikového stupně podle zadaných kritérii nespadá žádné riziko.
II. Rizikový stupeň (Nežádoucí riziko).
   - Porucha na zařízení (mobilní i pevná).
   - Jednoduchá, lehce napadnutelná hesla.
   - Neproduktivní surfování po internetu.

III. Rizikový stupeň (Mírné riziko).
   - Poruchy interní sítě (výpadky, špatné napětí...).
   - Prach, špína.
   - Krádež.
   - Neoprávněný vstup.

- Útok, napadení SW, HW (viry, phising...).
- Zneužití oprávnění.
- Použití vlastního zařízení (BYOD...).
- Neoprávněné stahování a užívání SW.
- Nedostatečná kvalifikace zaměstnanců.

IV. Rizikový stupeň (Akceptovatelné riziko).
Do II. Rizikového stupně se podle zadaných kritérii nevlezlo žádné riziko.

V. Rizikový stupeň (Bezvýznamné riziko).
Ani do V. Rizikového stupně se podle zadaných kritérii nevlezlo žádné riziko.

Na začátku této kapitoly je představena společnost, areál, ve které se nachází i referenční objekty dané společnosti a bylo blíže popsáno jejich aktuální zabezpečení. Následně byla identifikována hmotná i nehmotná aktiva na jejichž základě byly dále identifikovány hrozby a rizika. Zjištěné hrozby byly expertním šetřením ohodnoceny a dále využity pro analýzu rizik metodou PNH. Na základě výsledných zjištění z analýzy rizik byly v následující kapitole hodnoceny penalizační faktory.

6 NÁVRH DYNAMICKÝCH PENALIZAČNÍCH FAKTORŮ KONVERGOVANÉ BEZPEČNOSTI

Pro návrh dynamických penalizačních faktorů pro vybranou společnost byl vypracován katalog penalizačních faktorů, s kvantifikovanými penalizačními faktory. Na hodnocení penalizace faktorů byla vybrána metoda založena na expertním odhadu, která je popsána v kapitole 3.5.2., přičemž penalizační faktory dělíme do 4 odstupňovaných skupin (Kritické, Významné, Málo významné a Zanedbatelné faktory) v závislosti na jejich dopadu na objekt nebo činnosti. Maximální hodnota penalizace nabývá hodnoty 100, tzn. kritické faktory. A nejnižší hodnota penalizace nabývá hodnoty 1, tzn. zanedbatelné faktory.

Katalogy penalizačních faktorů byly pro přehlednost rozděleny do třech tabulek pro každou bezpečnost odděleně. Jelikož náplní této práce jsou pouze dynamické faktory, nebyly do tabulek statické faktory zahrnuty. Výchozí penalizace je v tabulkách vedena pro konvergovanou bezpečnost, tudíž jsou penalizační faktory vztaženy na jednotlivé druhy bezpečnosti. Tzn. jaký je předpokládaný dopad daného činitele (faktoru) na fyzickou (FB), kybernetickou (KB) a provozní bezpečnost (PB).

Aktiva vybrané společnosti pro návrh katalogu penalizačních faktorů konvergované bezpečnosti jsou vypsána v předešlé kapitole (viz *tab. 7- 18)*.

Tab. 30: Dynamické penalizační faktory fyzické bezpečnosti [vlastní zpracování, 33].

Kategorie faktoru	Název faktoru	Charakteristika faktoru	Výchozí penalizace		
			FB	KB	PB
Technická ochrana	Poplachový stav PZTS	Narušení perimetru objektu	70	10	10
		Narušení pláště objektu – technické prostupy	70	10	10
		Narušení pláště objektu - okna	90	20	10
		Narušení pláště objektu - dveře	90	20	10
		Narušení vnitřního prostoru objektu	90	20	10
	Další stavy PZTS	Poruchový stav PZTS	70	20	10
		PZTS ve stavu sabotáže	90	30	10
		PZTS ve stavu odstřeženo	10	10	10
	Poplachový stav detekován DV (dohledový videosystém)	Narušení perimetru objektu	70	10	10
		Narušení pláště objektu – technické prostupy	70	10	10
		Narušení pláště objektu - okna	90	20	10
		Narušení pláště objektu - dveře	90	20	10

		Narušení vnitřního prostoru objektu	90	20	10
		Narušení předmětové ochrany	90	20	10
	Další stavy DV	Poruchový stav DV	70	10	10
		DV ve stavu sabotáže	90	10	10
		Odchod pracovníka sledujícího DV z pracoviště	60	10	10
		DV mimo provoz, vypnut	50	20	20
	Stav přístupového systému	Poplachová informace	60	20	10
		Evidence osoby v objektu v určité době	20	10	10
		Pokus o vstup do objektu v určité době	20	10	10
		Porucha	80	20	20
		Sabotáž	90	20	20
		Evidence odchodu určité osoby z objektu v určité době	50	10	10
	Stav EPS	Poplach	100	100	100
		Porucha	70	70	70
		Sabotáž	90	80	80
		Vypnuto	70	70	70
Režimová ochrana	Vstup/výstup osob	Nefunkční kontrolní mechanismus	60	10	20
	Vjezd/ výjezd vozidel	Nefunkční kontrolní mechanismus	40	10	20
	Klíčové hospodářství	Nefunkční systém	40	10	20
Administrativní bezpečnost	Incidenty administrativní bezpečnosti	Ztráta dokumentů důležitých pro ochranu objektu	70	30	10
Personální bezpečnost	Zahájení trestního stíhání zaměstnance	Oblast související s bezpečností	50	30	20
Vnější vlivy, lokalita	Riziková akce v okolí objektu	Sport, kultura, demonstrace	30	20	20
	Živelní pohroma	Živelní pohroma v okolí objektu	30	30	30
	Vliv počasí	Zhoršená viditelnost	30	20	20
	Nařízená evakuace objektu	např. nácvik	20	20	50
	Informace o hrozbě	např. pohyb nebezpečných osob	40	40	30
	Havárie Technické vlivy	Výskyt podezřelých vozidel	40	20	30
		Průmyslová havárie v okolí objektu	50	10	50
		Nárůst rušení EMC	40	20	10

Na základě expertního zjištění bylo identifikováno 42 faktorů z oblasti fyzické bezpečnosti, přičemž nejvyšší dosažené hodnoty (100) dosáhl poplachový stav EPS ve všech 3 oblastech konvergované bezpečnosti z důvodu ohrožení života i majetku. Vnější vlivy jsou jedním z faktorů, které mají menší dopady.

Tab. 31: Dynamické penalizační faktory kybernetické bezpečnosti [vlastní zpracování, 33].

Kategorie faktoru	Název faktoru	Charakteristika faktoru	Výchozí penalizace		
			FB	KB	PB
Narušení běhu infrastruktury	PC LAN	Neaktualizovaný OS	30	50	40
		Neaktualizovaný OS GDPR	70	100	70
	Neaktuální verze SW anti-virové ochrany	V LAN síti	40	60	50
		Ve WAN síti	50	70	50
		Technika s GDPR	50	80	60
	Neaktuální verze databáze antivirového SW	V LAN síti	50	70	60
		Ve WAN síti	60	80	60
		Technika s GDPR	60	100	70
	Aktivní malware v síti	V LAN síti	30	40	30
		Ve WAN síti	40	50	40
		Technika s GDPR	40	60	50
	Chybová hlášení	RootCheck – chyba	10	20	20
		Missing `httpOnly` Cookie Attribute	30	50	40
		Sensitive Information via HTTP	40	60	50
	Napájení	Výpadek napájení – UPS	30	40	30
		Výpadek napájení – vypnutí	40	60	40
Únik dat	Neznámý provoz LAN	Upload - Známý protokol	40	60	40
		Upload - neznámý protokol	50	70	60
		Upload - šifrovaná komunikace	60	90	70
	Neznámý provoz WAN	Upload - Známý protokol	50	70	50
		Upload - neznámý protokol	50	80	60
		Upload - šifrovaná komunikace	60	100	70
	Zneužití zranitelností	Detekce backdooru	50	80	60
		Detekce ransomware	50	80	60
		Detekce user/password leak	50	80	60
		Detekce neznámého USB zařízení	40	70	50
	Ztráta chytrého telefonu	Šifrovaný obsah metodou dle Bezpečnostní Politiky	30	50	40
		Šifrovaný obsah jinou metodou	40	60	40
		Nešifrovaný obsah	50	80	60
		GDPR obsah	70	100	70
	Reklamace chytrého telefonu bez možnosti bezpečného smazání	Šifrovaný obsah metodou dle Bezpečnostní Politiky	20	30	20
		Šifrovaný obsah jinou metodou	30	40	30
		Nešifrovaný obsah	40	60	50
		GDPR obsah	60	80	60
	Odchod zaměstnance s BYOD bez možnosti bezpečného smazání	Šifrovaný obsah metodou dle Bezpečnostní Politiky	50	70	50
		Šifrovaný obsah jinou metodou	50	80	60
		Nešifrovaný obsah	70	100	70
		GDPR obsah	70	100	70

V oblasti kybernetické bezpečnosti bylo identifikováno 37 faktorů, přičemž nejvyšší hodnoty (100) bylo dosaženo při ztrátě GDPR obsahu z důvodu možnosti trestně-právního stíhání ve smyslu zákona č.110/2019 Sb. Nejnižší hodnoty (10) byly přiřazeny při chybovém hlášení o chybě.

Tab. 32: Dynamické penalizační faktory provozní bezpečnosti [vlastní zpracování, 33].

Kategorie faktoru	Název faktoru	Charakteristika faktoru	Výchozí penalizace		
			FB	**KB**	**PB**
Provozní technologie	Klimatizace	Ztráta komunikace	10	20	20
		Porucha	10	30	20
		Selhání	10	30	20
	Ventilace	Ztráta komunikace	10	20	20
		Porucha	10	30	20
		Selhání	10	30	20
	Vytápění	Ztráta komunikace	10	20	20
		Porucha	10	20	20
		Selhání	10	20	20
	Voda	Ztráta komunikace	10	10	20
		Porucha	10	10	40
		Selhání	10	10	40
	Osvětlení	Ztráta komunikace	20	10	40
		Porucha	20	10	40
		Selhání	20	10	40
	Řízení elektrické energie	Ztráta komunikace	20	30	40
		Porucha	40	40	60
		Selhání	30	50	60
	Záložní zdroj	Porucha	10	30	10
		Selhání	10	30	10
		Neprováděné revize	10	10	10
	Počítače / notebooky zaměstnanců	Porucha	10	50	40
		Selhání	10	50	40
	Síť typu internet	Porucha	10	20	20
		Selhání	10	20	20
	Kamerový systém	Porucha	20	10	20
		Selhání	20	10	20
Provozní informace	Informace o počasí	Vysoká teplota	10	10	20
		Nízká teplota	10	10	20
		Vysoká bio zátěž	10	10	10
		Výskyt bouřkové aktivity	10	10	10
		Výskyt silného větru	10	10	10
	Informace o omezení provozu	Krátkodobě plánované omezení provozu	10	10	10

	Informace o teplotě technologií	Neplánované omezení provozu	10	20	20
		Vysoká teplota technologie	20	30	30
		Kriticky vysoká teplota technologie	30	40	40
		Vysoká teplota v pracovních prostorech	20	40	50
		Kriticky vysoká teplota v pracovních prostorech	40	60	60
Personál	Nedostupnost lidských zdrojů	Nemoc	10	20	30
		Výpověď	10	30	30
		Pracovní úraz	10	20	30
Provozní události – narušení kontinuity činnosti	Mráz	Silný mráz	10	10	10
		Velmi silný mráz	20	20	20
		Extrémní mráz	30	20	20
	Náledí, ledovka a námraza	Nízké nebezpečí	10	10	20
		Vysoké nebezpečí	10	10	20
		Extrémní nebezpečí	10	10	20
	Sněhové jevy	Silné sněžení	10	10	10
		Nová sněhová pokrývka	10	10	10
		Vysoká sněhová pokrývka	20	10	10
		Extrémní nová sněhová pokrývka	30	10	20
	Povodeň	1. SPA - bdělost	10	10	10
		2. SPA - pohotovost	10	10	20
		3. SPA – ohrožení	20	10	30
	Teplo	Vysoké teploty	10	10	10
		Velmi vysoké teploty	20	20	30
	Vítr	Silný vítr	10	10	10
		Velmi silný vítr	10	10	10
		Extrémně silný vítr	10	10	10
	Bouřky	Silné bouřky	20	20	10
		Velmi silné bouřky	30	20	20
		Extrémně silné bouřky	40	30	20
	Výpadek elektrické energie	Územní / Regionální výpadek elektrické energie	70	90	90
		Úplný výpadek elektrické energie v objektu	70	90	90
		Částečný výpadek elektrické energie v objektu	70	90	90
		Okolní výpadek elektrické energie	70	90	90
	Evakuace	Úplná evakuace	20	30	60
		Částečná evakuace	20	40	60
	Invakuace	Úplná invakuace	20	20	40
		Částečná invakuace	20	20	40
	Porucha IT služeb	Porucha klíčových IT služeb	20	70	30
		Porucha ostatních IT služeb	20	60	30

	Porucha zařízení	Porucha nezávažná	20	30	60
		Porucha závažná	30	40	70
	Selhání zařízení	Krátkodobé selhání	20	30	50
		Dlouhodobé selhání	30	40	60
	Krádež	Odcizení informací a dat s řízeným přístupem	10	50	50
		Odcizení interních informací	10	60	60
		Odcizení klíčových aktiv - komponentů	10	50	70
		Odcizení ostatních aktiv - komponentů	10	40	70
	Zranění	Malé závažnosti	10	10	10
		Střední závažnosti	10	10	20
		Vysoké závažnosti	10	10	30
		Smrtelná	10	10	50
	Nehoda	Zanedbatelná	10	10	10
		Menšího rozsahu	10	10	30
		Závažná	20	10	40
Provozní události – rutinní činnosti	Směna	Nedodržení povinnosti – základní stupeň závažnosti	10	10	30
	Reportování	Nedodržení povinnosti – základní stupeň závažnosti	10	20	30
	Evidence událostí	Nedodržení povinnosti – základní stupeň závažnosti	10	20	30
Provozní události – znalosti a dovednosti zaměstnanců	Řidičské oprávnění určité kategorie	Ukončení platnosti	10	10	10
	Školení o požární ochraně	Ukončení platnosti	10	10	20
	Školení BOZP	Ukončení platnosti	10	10	20
	Certifikace	Ukončení platnosti	10	10	30
	Jiná školení	Ukončení platnosti	10	10	30

V oblasti provozní bezpečnosti bylo identifikováno 95 faktorů, přičemž nejvyšší hodnoty (90) bylo dosaženo v případě výpadku elektrické energie, jelikož záložní zdroj není dimenzován na zátěž způsobenou připojením výrobních strojů. Nejnižších hodnot (10) bylo dosaženo například při větších povětrnostních podmínkách, či ukončení platnosti řidičského oprávnění zaměstnanců, jelikož rozvoz vyrobených produktů není zajišťován a v blízkosti areálu se nachází zastávka hromadné dopravy, tudíž se zaměstnanec bez řidičského oprávnění má stále jak dopravit do práce.

V této kapitole byly identifikovány a popsány penalizační faktory, k nimž byly přiřazeny hodnoty, které popisují, jak moc je daný faktor pro danou společnost důležitý a jak moc poklesne odolnost při jeho narušení, poškození, poplachovém stavu atd.

V katalogu penalizačních faktorů byly faktory pro lepší přehlednost rozděleny do kategorií faktorů, tedy u fyzické bezpečnosti na kategorie technická ochrana, režimová ochrana, administrativní bezpečnost, personální bezpečnost a vnější vlivy. U kybernetické bezpečnosti na kategorie narušení běhu infrastruktury a únik dat. U provozní bezpečnosti kategorie provozní technologie, provozní informace, personál, provozní události narušení kontinuity činnosti, provozní události rutinní činnosti a provozní události znalosti a dovednosti zaměstnanců. Jednotlivé penalizační faktory poté byly vydefinovány na základě expertních úvah, přičemž byly také blíže charakterizovány. Výskyt každého z očekávaných dynamických penalizačních faktorů znamená okamžité snížení odolnosti aktiva po celou dobu výskytu tohoto dynamického penalizačního faktoru.

Ze zjištěných dat analýzy rizik a penalizačních faktorů byla zjištěna potřeba pořízení výkonnějšího dieselového náhradní zdroje, pravidelné revizní kontroly zařízení, zvýšení IT ochrany externím zaměstnancem a školením zaměstnanců v kybernetické bezpečnosti.

Toto šetření analýzy rizik, hrozeb a navrhnutí penalizačních faktorů pro danou společnost je platné pouze aktuálním stavu (tzn. 40 zaměstnanců, 2 budovy a 2 sklady). Při očekávané budoucí expanzi společnosti (tzn. navýšení počtu zaměstnanců, pořízení většího skladu, popřípadě i další výrobní haly) bude zapotřebí důkladné proškolení zaměstnanců v kyberbezpečnosti a BOZP, rozšíření PZTS a EPS o aplikaci automatického hlášení narušení objektů Policii ČR nebo Hasiče, pořízení více požárních hlásičů a popřípadě i najmutí fyzické ostrahy.

ZÁVĚR

První část teoretické části této diplomová práce je zaměřena na konvergovanou bezpečnost, její popis, včetně popisu jednotlivých bezpečností, které zahrnuje. U jednotlivých bezpečností byly popsány hlavní oblasti a také nastíněny hrozby, kterým jednotlivé bezpečnosti čelí. V následující části byly formulovány základní zásady konvergované bezpečnosti na právní podmínky ČR. Tudíž Zákon o kybernetické bezpečnosti, Zákon o ochraně osobních údajů, Zákon o bezpečnosti práce a Zákon o krizovém řízení. V předposlední kapitole teoretické části byla vypracována literární rešerše na téma penalizační faktory, přičemž byla popsána i odolnost a její hodnocení, jakožto jeden ze základních parametrů, které jsou sledovány v rámci individuální bezpečnosti. Bylo popsáno dělení penalizačních faktorů a katalog penalizačních faktorů, včetně stanovení etap tvorby tohoto katalogu a výpočtu odolnosti referenčního objektu a aktiva. Ke konci kapitoly byly popsány některé metody pro kvantifikaci penalizačních faktorů. V poslední kapitole poté byla popsána problematika analýzy rizik, jakožto klíčové části pro úspěšné zavedení a udržení konvergované bezpečnosti.

V první kapitole praktické části byla představena zájmová společnost, jakožto i jednotlivé referenční objekty a jejich zabezpečení. Dále byla provedena analýza rizik, v níž byla identifikována a ohodnocena aktiva společnosti na základě jejich důležitosti pro společnost. Byla provedena identifikace a hodnocení hrozeb, jež byly následně využity při analýz rizik společnosti. Výsledkem analýzy rizik bylo zjištění, že dosáhnutého nejvyššího rizikového stupně (IV. Nežádoucí riziko) v rámci šetření bylo dosaženo u poruchy na zařízení, při použití lehce napadnutelných hesel zaměstnanců nebo při neproduktivním surfování na internetu. Ve stupni mírného rizika to poté byly např. poruchy interní sítě, prach a špína, krádež, útok, napadení SW, HW atd.

V následné části byly sestaveny tabulky katalogu dynamických penalizačních faktorů, k nimž byly dle metody expertního odhadu přiřazeny hodnoty, které udávají, jak moc se sníží úroveň odolnosti při působení daného faktoru. Na základě tohoto katalogu byly identifikovány jako nejdůležitější faktory udané společnosti v rámci konvergované bezpečnosti např. poplachové stavy EPS systému, což by mohlo vést ke zničení objektu, a tudíž i zastavení činnosti; dále výpadek elektrické energie jehož důsledkem by mohlo být zastavení nebo výrazné omezení činnosti; nebo například poplachový stav PZTS, což by také mohlo vést k zastavení činnosti.

Pro kompletní identifikaci penalizačních faktorů pro danou společnost by bylo zapotřebí ještě doplnění statických penalizačních faktorů, jimiž se tato práce nezabývá.

SEZNAM POUŽITÉ LITERATURY

[1] Lukáš, L.; Hromada, M.; Pavlik, L. The Key Theoretical Models for the Safety and Security Ensuring. In *Proceedings of the 2016 Third International Conference on Mathematics and Computers in Sciences and in Industry (MCSI)*, Chania, Greece, 27–29 August 2016; pp. 61–65.

[2] Lippert, R.K.; Walby, K.; Steckle, R. Multiplicities of corporate security: Identifying emerging types, trends and issues. *Secur. J.* 2013, *26*, 206–221.

[3] Leander, A. Commercial security practices. In *The Routledge Handbook of New Security Studies*; Burgess, J.P., Ed.; Routledge: London, UK, 2010; pp. 208–216.

[4] Chen, P.-Y.; Kataria, G.; Krishnan, R. Correlated Failures, Diversification, and Information Security Risk Management. *MIS Q*. 2011, 35, 397–422.

[5] Tyson, D. Security Convergence: Managing Enterprise Security Risk; *Butterworth-Heinemann: Oxford*, UK, 2011.

[6] Lukáš, L. Konvergovaná bezpečnost. Zlín: Radim Bačuvčík - VeRBuM, 2019. ISBN isbn978-80-87500-99-6.

[7] Hromada, M; Rehak, D; Lukáš, L Resilience Assessment in Electricity Critical Infrastruction from the Point of View of Converged Security. *Energies* **2021**, *14*(6), 1624.

[8] Contos, B.T.; Crowell, W.P.; De Rodeff, C.; Dunkel, D.; Cole, E.; McKenna, R. *Physical and Logical Security Convergence: Powered by Enterprise Security Management*; Syngress: Burlington, MA, USA, 2007.

[9] Flammini, F.; Mazzocca, N.; Pappalardo, A.; Pragliola, C.; a Vittorini, V. Improving the Dependability of Distributed Surveillance Systems Using Diverse Redundant Detectors. In: ZAMOJSKI, Wojciech a Jarosław SUGIER, ed. *Dependability Problems of Complex Information Systems*. Cham: Springer International Publishing, 2015, s. 35-53. Advances in Intelligent Systems and Computing. ISBN 978-3-319-08963-8.

[10] Achar, S.; Faruqui, N.; Whaiduzzaman, M.; Awaian, A.; a Alazab, M. Cyber-Physical System Security Based on Human Activity Recognition through IoT Cloud Computing. *Electronics*. 2023, 2023(4), 12.

[11] Alkhudhayr, F.; Alfarraj, S.; Aljameeli, B.; a Elkhdiri, S. Information Security:A review of information security issues and techniques. *INTERNATIONAL CONFERENCE ON*

COMPUTER APPLICATIONS & INFORMATION SECURITY (ICCAIS) [online]. 2019, **2019**(2), 1-6.

[12] Vinnakota, Tiramula. A Second Order Cybernetic Model for Governance of Cyber Security in Enterprises. *IEEE 6th International Conference on Advanced Computing (IACC)* [online]. 2016, **2016**(11), 706-710.

[13] Susskind, N. G. Cybersecurity Compliance and Risk Management Strategies: What Directors, Officers, and Managers Need to Know. NYUJL & Bus., 11, 573, 2014.

[14] Torten,R.; Reaiche, C.; and Boyle, S. "The impact of security awarness on information technology professionals' behavior", Computers & Security, vol. 79, pp. 68-79, 2018.

[15] Deogirikar, J.; and Vidhate, A. "Security attacks in IoT: A survey", in *International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*. IEEE, 2017, pp. 32-36.

[16] Hayes, J. Use of safety barriers in operational safety decision making. *Safety Science* [online]. 2012, **50**(3), 424-432.

[17] Solms, R.; and Niekerk, J.; "From information security to cyber security", *Computers & Security*, vol. 38, pp. 97-102, 2013.

[18] Lukáš, L. a kolektiv. Teorie bezpečnosti I. Zlín: Radim Bačuvčík – VerBuM, 2017, ISBN 978-80-87500-89-7.

[19] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) – *Sbírka zákonů České republiky*. Částka 75/2014.

[20] Zákon č. 110/2019 Sb., o zpracování osobních údajů – *Sbírka zákonů České republiky*. Částka 47/2019.

[21] Zákon č. 309/2006 Sb., kterým se upravují další požadavky bezpečnosti a ochrany zdraví při práci v pracovněprávních vztazích a o zajištění bezpečnosti a ochrany zdraví při činnosti nebo poskytování služeb mimo pracovněprávní vztahy (zákon o zajištění dalších podmínek bezpečnosti a ochrany zdraví při práci) – *Sbírka zákonů České republiky*. Částka 96/2016.

[22] Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) – *Sbírka zákonů České republiky*. Částka 73/2000.

[23] Argyroudis, S.A.; Mitoulis, S.A.; Hofer, L.; Zanini, M.A.; Tubaldi, E.; Frangopol, D.M. Resilience assessment framework for critical infrastructure in a multi-hazard environment: Case study on transport assets. *Sci*. 2020, 714, 136854.

[24] Lapková, D.; Mrázková, L. Penalizační faktory pro hodnocení bezpečnosti měkkého cíle. Univerzita Tomáše Bati, Zlín.

[25] Coaffee, J.; Fussey, P. Constructing resilience through security and surveillance: The politics, practices and tensions of securitydriven resilience. *Secur*. 2015, 46, 86–105.

[26] SMEJKAL, V. a RAIS, K. Řízení rizik ve firmách a jiných organizacích. 3., rozš. a aktualiz. vyd. Praha: Grada, 2010. *Expert.*

[27] Dvořáková, A. Analýza rizik ve vybraném podniku. Bakalářská práce. *Univerzita Pardubice.* Pardubice. 2020.

[28] Fenclová, N. Analýza rizik obce s rozšířenou působností Rakovník. Diplomová práce. *České vysoké učení technické v Praze*. Kladno. 2023.

[29] Janošec, J. Hrozba a riziko v bezpečnostní terminologii. *Univerzita Pardubice*. Pardubice, c2007-2015, 2010.

[30] Tichý, M. Ovládání rizika: analýza a management. *Praha*: C. H. Beck, 2006

[31] Šefčík, V. Analýza rizik. 2009. *Zlín*. ISBN 978-80-7318-696-8.

[32] Rizika a jejich analýza. VŠB [online]. Dostupné z: http://fei1.vsb.cz/kat420/vyuka/Magisterske%20nav/prednasky/web/RIZIKA.pdf

[33] Analytický programový modul pro hodnocení odolnosti v reálném čase z hlediska konvergované bezpečnosti: *Technická dokumentace*. 2019.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

FB	Fyzická bezpečnost.
IB	Informační bezpečnost.
KB	Kybernetická bezpečnost.
PB	Provozní bezpečnost.
IoT	Internet věcí.
EPS	Elektronická požární signalizace.
PZTS	Poplachový zabezpečovací a tísňový systém.
DV	Dohledový videosystém.
BYOD	Bring your own device.
SW	Software.
HW	Hardware.
PNH	Preliminary Hazard Analysis.
HRA	Hazard and Risk Analysis.

SEZNAM OBRÁZKŮ

Obr. 1: Základní principy konvergované bezpečnosti (upraveno z [7])......12
Obr. 2: Přehled dělení některých oblastí fyzické bezpečnosti. 15
Obr. 3: Hlavní opatření v kybernetickém prostoru proti hrozbám (upr. z [6])......18
Obr. 4: Hlavní hrozby PB, ovlivnitelné výše zmíněnými faktory (upr. z [6]). 21
Obr. 5: Etapy tvorby katalogu penalizačních faktorů pro vyhodnocení odolnosti konkrétního objektu (přepracováno z [6]). 27
Obr. 6: Klíčové kroky analýzy rizik v konvergované bezpečnosti. 33

SEZNAM TABULEK

Tab. 1: Popis členů rovnice (1) a (2). 28
Tab. 2: Popis členů rovnice (3) a (4). 29
Tab. 3: Popis členů rovnice (5) a (6). 30
Tab. 4: Popis členů rovnice (7) a (8). 30
Tab. 5: Dělení faktorů do skupin, jejich dopad a hodnocení. 31
Tab. 6: Význam bodového hodnocení u parametru P [upraveno z 31]. 36
Tab. 7: Význam bodového hodnocení u parametru N [upraveno z 31]. 36
Tab. 8: Význam bodového hodnocení u parametru H [upraveno z 31]. 37
Tab. 9: Výsledkové hodnocení míry rizika R [upraveno z 31]. 37
Tab. 10: Stupnice pro hodnocení aktiv [vlastní zpracování]. 42
Tab. 11: Informační aktiva společnosti [vlastní zpracování]. 42
Tab. 12: Osoby ve společnosti [vlastní zpracování]. 42
Tab. 13: Prostory a objekty společnosti [vlastní zpracování]. 42
Tab. 14: Hardwarové zařízení společnosti [vlastní zpracování]. 43
Tab. 15:Technická zařízení společnosti [vlastní zpracování]. 43
Tab. 16: Software společnosti [vlastní zpracování]. 43
Tab. 17: Datová uložiště společnosti [vlastní zpracování]. 43
Tab. 18: Komunikační zařízení společnosti [vlastní zpracování]. 43
Tab. 19: Prostředky pro vývoj společnosti [vlastní zpracování]. 44
Tab. 20: Výrobní a zásobní materiál společnosti [vlastní zpracování]. 44
Tab. 21: Bezpečnost a řízení společnosti [vlastní zpracování]. 44
Tab. 22: Ostatní [vlastní zpracování]. 44
Tab. 23: Možnost výskytu hrozby [vlastní zpracování]. 45
Tab. 24: Technické a technologické [vlastní zpracování]. 45
Tab. 25: Přírodní [vlastní zpracování]. 45
Tab. 26: Způsobené lidským faktorem – úmyslné z vnějšího prostředí [vlastní zpracování]. 46
Tab. 27: Způsobené lidským faktorem – úmyslné z vnitřního prostředí [vlastní zpracování]. 46
Tab. 28: Způsobené lidským faktorem – neúmyslné [vlastní zpracování]. 46
Tab. 29: Metoda PNH [vlastní zpracování] 48

Tab. 31: Dynamické penalizační faktory fyzické bezpečnosti [vlastní zpracování, 33]. 50
Tab. 32: Dynamické penalizační faktory kybernetické bezpečnosti [vlastní zpracování, 33]. 52
Tab. 33: Dynamické penalizační faktory provozní bezpečnosti [vlastní zpracování, 33]. 53