Analýza rizik pro vybranou prodejnu a návrh opatření pro zodolnění zabezpečení

Pavel Hoffmann

Bakalářská práce
2024

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav bezpečnostního inženýrství

Akademický rok: 2023/2024

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Pavel Hoffmann**
Osobní číslo:	**A21776**
Studijní program:	**B1032A020001 Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Analýza rizik pro vybranou prodejnu a návrh opatření pro zodolnění zabezpečení**
Téma práce anglicky:	**Risk analysis of a selected store and proposal of measures to enhance security**

Zásady pro vypracování

1. Uveďte základní terminologii.
2. Popište postup pro zpracování analýzy rizik.
3. Charakterizujte objekt pro provedení analýzy rizik.
4. Proveďte analýzu současného stavu vybraného objektu.
5. Navrhněte bezpečnostní opatření.

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

Seznam doporučené literatury:

1. ČASTORÁL, Zdeněk, 2017. Management rizik v současných podmínkách. Vydání I. Praha: Univerzita Jana Amose Komenského. ISBN 9788074521324.
2. KYNCL, Jaromír, 2014. Bezpečnost objektu ve světle moderních technologií. Praha: Komora podniků komerční bezpečnosti České republiky. ISBN 9788026071150.
3. PROCHÁZKOVÁ, Dana, 2011. Analýza a řízení rizik. V Praze: České vysoké učení technické. ISBN 9788001048412.
4. ŠEFČÍK, Vladimír, 2009. Analýza rizik. Zlín: Univerzita Tomáše Bati ve Zlíně. ISBN 9788073186968.
5. SMEJKAL, Vladimír a RAIS, Karel, 2013. Řízení rizik ve firmách a jiných organizacích. 4., aktualiz. a rozš. vyd. Expert (Grada). Praha: Grada. ISBN 9788024746449.

Vedoucí bakalářské práce: **Ing. Bc. Krystyna Ljubymenko**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **8. prosince 2023**
Termín odevzdání bakalářské práce: **28. května 2024**

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

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

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

Ve Zlíně dne 8. prosince 2023

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské 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 bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- 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 – bakalářskou 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 bakalářské 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 bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne …….

Pavel Hoffmann, v. r.

ABSTRAKT

Tato bakalářská práce se zaměřuje na analýzu rizik vybraného objektu prodejny a návrh bezpečnostních opatření. Cílem je identifikovat potenciální rizika a navrhnout účinná opatření k jejich minimalizaci. Práce kombinuje teoretický přehled s praktickým přístupem, aby poskytla komplexní pohled na problematiku bezpečnosti aktiv.

V teoretické části je uvedena základní terminologie a popsán obecný postup pro provedení analýzy rizik. Dále jsou uvedeny některé používané metody a v závěru popsána metodika zvolená pro realizaci této bakalářské práce.

Praktická část se zaměřuje na charakteristiku hodnoceného objektu. Dále je provedena analýza současného stavu dle zvolené metodiky, její vyhodnocení a návrh bezpečnostních opatření.

Klíčová slova: analýza rizik, zabezpečení, opatření, prodejna, bezpečnost.

ABSTRACT

This bachelor's thesis focuses on the risk analysis of a selected retail store and the proposal of security measures. The aim is to identify potential risks and suggest effective measures to minimize them. The thesis combines a theoretical overview with a practical approach to provide a comprehensive view of asset security issues.

The theoretical part introduces the basic terminology and describes the general procedure for conducting a risk analysis. It also presents some commonly used methods and concludes with the methodology chosen for the implementation of this bachelor's thesis.

The practical part focuses on the characterization of the evaluated object. It includes an analysis of the current state according to the chosen methodology, its evaluation, and the proposal of security measures.

Keywords: risk analysis, security, measures, retail store, safety.

Rád bych poděkoval vedoucí mé práce paní Ing. Bc. Krystyně Ljubymenko za cenné rady, připomínky a celkové vedení v průběhu tvorby bakalářské práce.

Dále bych rád poděkoval své manželce, rodině a přátelům za trpělivost a podporu během celého studia.

V neposlední řadě bych také rád poděkoval vedení společnosti, která mi umožnila tuto práci realizovat na jednom z jejich objektů.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Bezpečnost si v obecném pohledu pravděpodobně představuje každý člověk trochu jinak. Pro jednotlivce, žijícího například ve městě, může být pojem bezpečnost spojen třeba s tím, že se po setmění lze volně procházet po ulici, aniž by se musel obávat přepadení. Obecně lze říci, že očekáváme, že se o tuto oblast primárně postará stát a jeho silové složky.

Pro organizace a instituce se již stává problematika bezpečnosti více vrstvenou disciplínou, kdy do hry vstupují například legislativní požadavky, případně další speciální regulatorní požadavky, a to nejen v oblasti fyzické, ale i kybernetické bezpečnosti. Vzhledem k tomu, že se závislost lidstva na IT technologiích neustále zvyšuje a z kybernetického zločinu se stal velice výnosný obchod, je potřeba více než dříve zahrnout i tuto oblast do návrhů zabezpečení aktiv společností. Zajištěním bezpečnostních opatření se ve firmách v dnešní době zabývají i celé týmy odborníků.

Každému většímu projektu, a to nejen v oblasti bezpečnosti, by měla předcházet důkladná analýza stavu posuzovaného prostředí, aby bylo možno správně a zodpovědně připravit vhodná řešení a k jednotlivým fázím namapovat odpovídající finanční, lidské a další potřebné zdroje.

Cílem této práce je analýza rizik pro vybranou prodejnu nábytku, kterou ročně navštíví tisíce zákazníků, o které se stará několik desítek zaměstnanců, a následně návrh opatření pro zodolnění zabezpečení. Pro zpracování této analýzy byl se souhlasem provozovatele vybrán existující objekt, aby se vstupní informace co nejvíce přiblížily realitě a zároveň bylo možno výsledky této práce použít jako odrazový můstek k detailnější analýze, kterou posuzovaná společnost do budoucna zvažuje.

V teoretické části jsou definovány základní pojmy z oblasti zpracování analýzy rizik, které jsou důležité pro následné pochopení vztahů mezi nimi a jednotlivých dílčích kroků při zpracování analýzy, popsaných v druhé části práce. Dále jsou stručně zmíněny některé z používaných metod analýzy rizik a v závěru teoretické části je podrobně popsána metodika, podle které bylo postupováno v praktické části této práce a která vychází z požadavků Zákona o kybernetické bezpečnosti a související Vyhlášky o kybernetické bezpečnosti.

Praktická část se věnuje charakteristice vybraného objektu z pohledu lokality, popisu samotného objektu a jeho zabezpečení. Údaje v této části musely být na žádost vedení provozovatele anonymizovány, takže jednotlivé popisy i fotografie mají spíše obecnější charakter.

V další kapitole byla provedena samotná analýza současného stavu zabezpečení objektu a aktiv společnosti. Bylo postupováno podle metodiky popsané v teoretické části a výsledkem je návrh na zlepšení vybraných bezpečnostních opatření.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ TERMINOLOGIE

V této úvodní části bych rád vysvětlil základní pojmy, které se v souvislosti s analýzou rizik používají, a jsou důležité k pochopení tématu a pro správné provedení analýzy. Veškeré lidské činnosti jsou z podstaty věci spojeny s určitým stupněm nejistoty a nebezpečí. Míru rizika, spojeného s naším snažením, buď akceptujeme, nebo vymýšlíme různá opatření, která nám mohou pomoci riziko snížit, omezit jeho následky, případně se mu úplně vyhnout.

Akademický slovník současné češtiny definuje slovo analýza jako zkoumání určitého jevu, předmětu nebo činnosti spočívající v myšlenkovém nebo faktickém rozčleňování celku na jednotlivé prvky, v zjišťování jejich vlastností, funkcí, souvislostí a vztahů mezi nimi. [1]

V terminologickém slovníku Výzkumného ústavu bezpečnosti práce je pak možno nalézt definici pro analýzu rizik jako proces analýzy nebezpečí (zdroje rizika) při určité činnosti, v určitém systému a odhad (ocenění) úrovní rizika pro lidi, životní prostředí (včetně hospodářských zvířat) a majetek, které toto nebezpečí (zdroj rizika) představuje. Výsledky analýzy rizika pak lze použít pro hodnocení rizika. [2]

Původ slova riziko můžeme najít již ve staré řečtině, kde se slovem „riza“ označoval kořen, tedy určitou překážku, později se toto slovo začalo používat i v jiných jazycích ve smyslu nebezpečí, se kterým se setkávali obchodníci na cestách po moři. Slovo „risk“ je v dnešní době možno chápat jako jakékoliv nebezpečí. Podle Petra Marka lze říci, že riziko „představuje nebezpečí, že se skutečné výsledky budou lišit od očekávaných“. [3]

1.1 Aktivum

Aktivum představuje cokoliv, co má pro společnost nebo organizaci hodnotu, která může být ohrožena hrozbou. Hodnotu aktiva je možno určit buď objektivně na základě jeho pořizovací ceny nebo subjektivně, kdy osoba, zodpovědná za dané aktivum, ocení jeho důležitost, případně kombinací obou těchto způsobů.

Aktiva můžeme dělit na hmotná a na nehmotná. Mezi hmotná aktiva se řádí například lidé, nemovitosti, různé ceniny a další. Nehmotnými aktivy mohou být například informace, autorské právo, pověst firmy, patenty, loajalita zaměstnanců apod. Aktivem také může být i samotná hodnocená společnost, protože hrozba může ovlivnit její budoucnost a mít i likvidační následky.

[4]

Zákon o kybernetické bezpečnosti na dělení aktiv pohlíží ještě z jiného úhlu a charakterizuje aktiva jako primární a podpůrná.

1.1.1 Primární aktiva

Jedná se o informační systémy a služby nutné pro zajištění chodu organizace. Obvykle bývají spojena s výkonem nebo poskytováním určité služby. Dle NÚKIB jsou to takové služby a informace, jejichž ztráta nebo narušení by mělo dopad na chod, funkčnost, účel a bezpečnost celé organizace, případně systému nebo služby s ohledem na vymezený rozsah ISMS z hlediska důvěrnosti, integrity a dostupnosti. Za primární aktivum můžeme označit takové aktivum, která má zásadní hodnotu pro provoz organizace. V případě obchodní společnosti to může být například e-shop nebo samotný proces prodeje, jehož narušení může ohrozit samotnou existenci obchodní společnosti. [5]

1.1.2 Podpůrná aktiva

NÚKIB definuje podpůrná aktiva jako aktiva nutná pro správnou funkčnost, zpracování, uchování a zajištění bezpečnosti primárních aktiv. Sama o sobě podpůrná aktiva netvoří hodnotu pro organizaci. Podpůrná aktiva jsou technická aktiva, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačních systémů. Podpůrnými aktivy mohou být například technické vybavení, komunikační prostředky, programové vybavení, objekty, lidské zdroje, dodavatelé, externí systémy nebo služby. Podpůrná aktiva mohou patřit do více kategorií a je tedy nutné posuzovat hrozby a rizika ve všech odpovídajících kategoriích. [5]

1.2 Hrozba

Podle terminologického slovníku Ministerstva vnitra je hrozbou označován přírodní nebo člověkem podmíněný proces představující potenciál, tj. schopnost zdroje hrozby být aktivován a způsobit škodu. Tento potenciál může být záměrně spuštěn nebo náhodně využit pro atakování specifických zranitelností aktiva. Hrozba bývá zdrojem rizika. [6]
Hrozby mohou být vnějšího charakteru jako například různé přírodní katastrofy (povodeň, tornádo, sníh…), požár, krádeže, kontrola finančního úřadu, politické změny a další. Mohou také pocházet zevnitř organizace a typicky se jedná o různé chyby zaměstnanců, ať už úmyslné či nikoliv. [4]

Hrozbou způsobená škoda je definována jako její dopad, který lze posuzovat podle celkové hodnoty nákladů na obnovení činnosti postiženého subjektu nebo odstranění následků vzniklých škod. Hrozby mohou působit i opakovaně a na více aktiv najednou.
Při posuzování úrovně hrozby zohledňujeme její nebezpečnost, tedy schopnost působit škodu, dále pravděpodobnost, s jakou hrozba může aktivum ohrozit, frekvenci výskytu a také motivaci útočníka (hrozby) realizovat tuto hrozbu. Při identifikaci hrozeb je důležité si uvědomit, že všechny výše uvedené faktory se v čase mohou měnit, a to v závislosti například na politické situaci, technologickém vývoji nebo v souvislosti se změnou klimatu. [4]

1.3 Zranitelnost

Můžeme ji charakterizovat jako slabinu posuzovaného aktiva, jeho nedostatky nebo špatný stav, který hrozba může využít k ohrožení hodnoty aktiva uplatněním nežádoucího vlivu. Jedná se o vlastnost aktiva, která vyjadřuje jeho citlivost na působení dané hrozby, ale sama o sobě škodu nepůsobí. Lze říci, že zranitelnost bez odpovídající hrozby nemusí vyžadovat opatření, ale je dobré ji monitorovat a zároveň hrozba bez odpovídající zranitelnosti, kterou by mohla zneužít, nemusí představovat riziko. Obecně lze tedy zranitelnost charakterizovat jako náchylnost aktiva ke vzniku škody. Úroveň zranitelnosti posuzujeme podle důležitosti aktiva pro analyzovanou společnost a jeho náchylnosti k poškození hrozbou. [4]

1.4 Protiopatření

Primárním cílem protiopatření (opatření) je předejít vzniku škody, případně zmenšit následky, které v rámci škody vzniknou. Může se jednat o proces, technický prostředek, nebo cokoliv dalšího, co je na základě analýzy navrženo buď pro zmenšení působení hrozby, snížení jejího dopadu nebo redukci zranitelnosti aktiva. Z pohledu analýzy rizik jsou protiopatření posuzována na základě jejich efektivity (míra snížení zranitelnosti nebo účinků hrozby a detekce) a vynaložených nákladů. Obecně platí pravidlo, že náklady vynaložené na zavedení protiopatření musí být přiměřené hodnotě chráněných aktiv, případně hodnotě škod způsobených hrozbou. Při návrhu protiopatření je důležité posoudit již přijatá opatření, aby nevznikaly duplikace nebo nežádoucí interakce. [4]

1.5 Riziko

Vyjadřuje míru ohrožení aktiva uplatněním hrozby a tím vzniku škody. Vzniká vzájemným působením hrozby a aktiva. Velikost rizika je vyjádřena jeho úrovní. Hrozba, která nepůsobí na žádné aktivum, nemusí být při analýze rizik brána v úvahu. Míru rizika, tedy pravděpodobnost škodlivých následků vyplývajících z hrozby a ze zranitelnosti zájmu, je možno posoudit na základě analýzy rizik. [4]

Další možnou definici přináší oficiální terminologický slovník Ministerstva vnitra: Riziko je možnost, že s určitou pravděpodobností vznikne událost, kterou považujeme z bezpečnostního hlediska za nežádoucí. Riziko je vždy odvoditelné a odvozené z konkrétní hrozby. Míru rizika, tedy pravděpodobnost škodlivých následků vyplývajících z hrozby a ze zranitelnosti zájmu, je možno posoudit na základě analýzy rizik, která vychází i z posouzení naší připravenosti hrozbám čelit. Riziko také představuje účinek nejistoty na dosažení cílů nebo pravděpodobnost výskytu nežádoucí události s nežádoucími následky. [6]

Velikost rizika posuzujeme podle jeho úrovně, která je dána jak hodnotou a zranitelností aktiva, tak úrovní hrozby. Riziko je tedy kombinací naplnění scénáře incidentu a jeho následků.

Dle NÚKIB lze však říci, že účelem identifikace rizik není vytvoření všech dostupných kombinací. Například u aktiv typu lidských zdrojů nemá smysl vytvářet kombinace obsahující zranitelnosti typu nedostatečné údržby a hrozby typu poškození nebo selhání technického nebo programového vybavení. Vždy je ale potřeba zvažovat všechny možné logické varianty kombinace aktivum-zranitelnost-hrozba. [5]

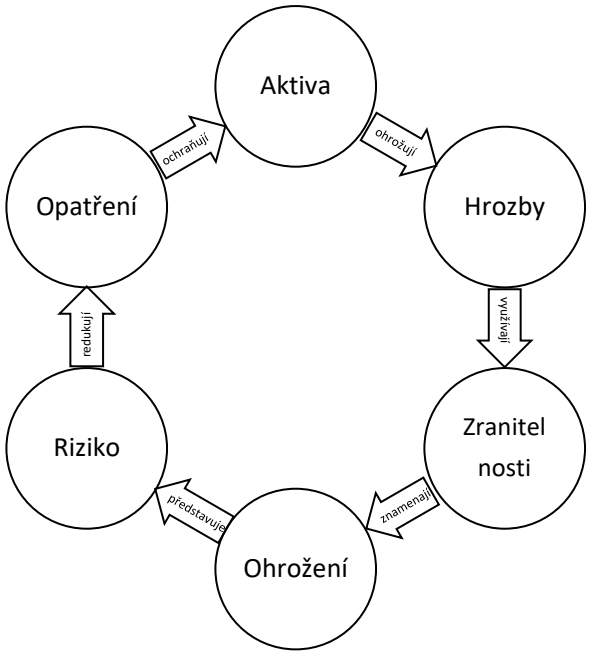
Při posuzování úrovně rizika je vhodné nastavit si její tzv. referenční hodnotu. Riziko s hodnotou vyšší, než je referenční, je potřeba ošetřit pomocí protiopatření a opačně, riziko s hodnotou nižší, než je referenční, je považováno za tzv. zbytkové, u něhož jsou následky případného incidentu pro subjekt akceptovatelné. Referenční hodnotu bychom si tedy měli nastavit tak, aby pro nás byl dopad stále ještě zanedbatelný. [4]

1.6 Vztahy v analýze rizik

Jednotlivé pojmy, které byly popsány výše, spolu navzájem souvisí a vztahy mezi nimi lze popsat následovně:

- Hrozba využívá zranitelnosti a po překonání protiopatření způsobí škodu na aktivu (dopad).
- Hodnota aktiva motivuje útočníka k realizaci hrozby. Aktivum se vyznačuje určitou zranitelností vůči působení hrozby a zároveň je nebo může být chráněno před hrozbami protiopatřeními.
- Protiopatření chrání aktivum, detekuje hrozby a zmírňuje nebo zcela zabraňuje jejich působení na aktiva. Protiopatření zároveň odrazují útočníky od aktivování hrozeb.
- Hrozba působí přímo na aktivum nebo na protiopatření s cílem získat k aktivu přístup.
- Hrozba vyžaduje zdroje (podmínky) k tomu, aby mohla být aktivována a působit na aktivum. [4]

Graficky je možno tyto vztahy jednoduše znázornit takto:



Obrázek 1_Vztahy v analýze rizik [vlastní]

1.7 CIA triáda

V oblasti kybernetické bezpečnosti, jejíž posuzování je v dnešní době stále aktuálnější a mělo by být součástí analýzy rizik, se používá zkratka CIA (C-Confidentiality, I-Integrity, A-Availability).

Obrázek 2_CIA triáda [7]

1.7.1 Confidentiality (Důvěrnost)

- Znamená, že k informaci mají přístup pouze oprávněné osoby.
- Narušená důvěrnost znamená, že informace má nepovolaná osoba.
- Zajištěná důvěrnost vylučuje zneužití informace.
- Pod pojmem informace je obecně chápán vlastní datový obsah zprávy, její velikost, doba existence, typ komunikace atd.

[1] [8]

1.7.2 Integrity (Integrita, Neporušenost)

- Znamená, že informace je uživateli doručena bez nežádoucích změn či úprav.
- Narušená integrita znamená, že informace jsou poškozené, jiné, než mají být.
- Zajištěná integrita znamená zajištění správnosti a úplnosti informací v informačních systémech.

[1] [8]

1.7.3 Availability (Dostupnost)

- Znamená, že oprávněný uživatel může získat ze systému data kdykoliv v případě potřeby.
- Narušená dostupnost znamená, že informace nejsou dostupné, mohou být ztracené.
- Zajištěná dostupnost znamená, že data jsou k dispozici, že nedošlo k jejich ztrátě.

[1] [8]

V závěru této kapitoly lze říci, že se v rámci zpracování analýzy rizik můžeme setkat s velkým množstvím používaných termínů. Zde byly popsány a vysvětleny ty nejpoužívanější z nich a vztahy mezi nimi. Pochopení těchto souvislostí je důležité pro správné zpracování analýzy rizik. Dále byla představena CIA triáda, která zdůrazňuje důležitost zachování důvěrnosti, integrity a dostupnosti, což jsou klíčové aspekty bezpečnosti informací a dalších aktiv.

2 ANALÝZA RIZIK – POSTUP A METODY

2.1 Obecný postup

Aktiva většinou nejsou ohrožena pouze jedním rizikem, ale obvykle kombinací více rizik, která v součtu mohou představovat hrozbu. Tato rizika je potřebné posoudit podle jejich relevance pro posuzovaný objekt a zaměřit se primárně na ně.

Obecné činnosti prováděné při analýze rizik:

- stanovení hranice analýzy rizik,
- identifikace aktiv,
- stanovení hodnoty aktiv,
- identifikace hrozeb,
- analýza hrozeb a zranitelností,
- odhad pravděpodobnosti jevu,
- měření stupně rizika,
- vyhodnocení výsledků a návrh protiopatření,

[4]

Nejprve je tedy potřeba na základě diskuse s managementem určit hranici (referenční úroveň), která rozdělí aktiva zahrnutá do analýzy a ostatní, kterých se analýza nebude týkat. V dalším kroku dochází k vytvoření seznamu všech aktiv, která budou posuzována. Pro stanovení hodnoty aktiv je potřeba vycházet z kombinace nákladových (pořizovací cena) a výnosových (aktivum generuje zisk) charakteristik. Dále je podstatné rozlišit význam aktiva, tedy jedná-li se o tzv. jedinečné nebo nahraditelné aktivum. Větší množství aktiv je možno seskupovat, mají-li podobné vlastnosti. NÚKIB doporučuje při posuzování hodnoty aktiv uvažovat o nejhorším možném scénáři a nebrat v úvahu zavedená bezpečnostní opatření. Při identifikování hrozeb, které mohou alespoň na jednom analyzovaném aktivu způsobit škodu, můžeme vycházet z různých seznamů dle dostupné literatury, vlastních zkušeností, dříve provedených průzkumů a analýz, případně formou diskuse s managementem a garanty aktiv doplnit hrozby specifické pro zkoumaný subjekt. V další fázi určujeme, s jakou pravděpodobností může hrozba zneužít zranitelnosti aktiva a posuzujeme každou dříve identifikovanou hrozbu vůči každému aktivu zahrnutému do analýzy. Zároveň bereme v úvahu již přijatá protiopatření. Dále se snažíme určit, zda je zkoumaný jev náhodný nebo není, případně ho můžeme úplně vyloučit jako nepravděpodobný. Ke každému posuzovanému jevu doplníme údaj o pravděpodobnosti jeho vzniku. Výši rizika určujeme

na základě výpočtu nebo kvalifikovaného odhadu. V závěrečné fázi shrneme výsledky analýzy rizik a současně navrhneme protiopatření vedoucí ke snížení zranitelnosti aktiv nebo ke zmírnění dopadů realizovaných hrozeb, případně k jejich eliminaci.[4] [5]
V etapě zvládání rizik jsou pro rizika, která nejsou akceptována z důvodu nízké úrovně nebo z jiných důvodů, navržena vhodná opatření, jejichž cílem je snížit jejich hodnotu na akceptovatelnou úroveň. Podle výše úrovně rizika jsou určovány priority řešení a jsou navrhována adekvátní bezpečnostní opatření a zvoleny přístupy pro zvládání (ošetření) rizik.

2.2 Možné varianty ošetření rizik

2.2.1 Modifikace rizika

Jedná se o zavedení nových bezpečnostních opatření, případně posílení těch stávajících, s cílem snížení pravděpodobnosti nebo závažnosti dopadu hrozby. Modifikace rizika se doporučuje u rizik, která mají vysokou pravděpodobnost výskytu se závažnými následky.

2.2.2 Přenesení rizik

Varianta ošetření rizik přesunem nebo sdílením rizik na jiné organizace. Může se jednat např. o pojištění, uzavírání dlouhodobých smluv, outsourcing, celkovou změnu smluvních podmínek, aj. Přenesení rizik bývá doporučováno u rizik s nízkou pravděpodobností výskytu a závažnými následky.

2.2.3 Vyhnutí se rizikům

Varianta, kdy je na základě vyloučení rizikového prvku zabráněno riziku vůbec vzniknout. Vyhnutí se činnosti nebo podmínce, která riziko generuje. Může se například jednat o rozvázání smlouvy se stávajícím dodavatelem, náhradu/obnovu informačního systému apod. Vyhnutí se rizikům se doporučuje u rizik s vysokou pravděpodobností výskytu a závažnými následky.

2.2.4 Akceptování rizik

Tato varianta znamená souhlas s vyhodnoceným rizikem s tím, že nebude prováděna žádná činnost vedoucí ke snížení rizika. Předpokladem k podstoupení rizika je v tomto případě dosažení úrovně rizika splňujícího kritéria akceptace rizik a není tedy potřeba přijímat protiopatření. Riziko lze podstoupit i v případě, že případná opatření by byla obtížně realizovatelná nebo neúměrně nákladná.

Vzhledem k tomu, že se dopad rizik i pravděpodobnost výskytu mohou v průběhu času měnit a vyvíjet, je doporučené identifikovaná rizika monitorovat. Monitoring umožňuje flexibilně reagovat na změny a v souladu s tím případně upravit metody zvládání monitorovaných rizik. To samé se týká samotné organizace a její schopnosti rizika zvládat. Některá rizika mohou být v souladu s metodikou akceptovatelnosti rizik akceptována, ale i přesto se doporučuje monitorovat, jestli se jejich závažnost v průběhu času nemění. Akceptace může být pasivní – nezavádíme žádná opatření a riziko pouze evidujeme v registru rizik kromě záznamu daného rizika. Pro aktivní opatření vytváříme v plánování lidských a finančních zdrojů určitou rezervu, kterou je možno případný výskyt rizika pokrýt. [5]

2.3 Používané metody

2.3.1 Kvantitativní metody

Jedná se o metody založené na matematickém výpočtu rizika v souvislosti s frekvencí výskytu hrozby a jejího dopadu. Používá se číselné hodnocení při ocenění vzniku i dopadu dané události. Kvantitativní metody se používají hlavně v oblasti finančních rizik a technické bezpečnosti. Jejich hlavní výhodou je transparentnost, lepší kontrola nákladů a poměrně velká přesnost. Nevýhodou je naopak větší náročnost na výpočet, čas i lidské zdroje a s tím spojené finanční náklady při jejich realizaci. [4] [9] [10]
Příklady:

- Simulace Monte Carlo (Monte Carlo Simulation) – dokáže převést jednotlivá rizika a jejich nejistoty do jediné veličiny popisující riziko celého projektu.
- Analýza stromu událostí (ETA – Event Tree Analysis) – používá k modelování různých scénářů a k vypočítání pravděpodobnosti výskytu každého scénáře.

[4] [9] [10]

2.3.2 Kvalitativní metody

Metoda postavená na popisu pravděpodobnosti, s jakou daná událost nastane, a na závažnosti potenciálního dopadu. Riziko je vyjádřeno v určitém rozsahu. Úroveň rizika je obvykle určována jen kvalifikovaným odhadem. Často se používá jako úvodní přehled vedoucí k identifikaci rizik nebo tam, kde její výsledek postačuje k rozhodování, případně nejsou k dispozici dostatečné údaje pro provedení kvantitativní analýzy. Je méně náročná a nevyžaduje tolik zdrojů a času, ale za zápor může být považováno např. hledisko subjektivity pohledu hodnotitele.

Příklady:

- Metoda PHA (předběžné posouzení ohrožení) – postup, při kterém jsou vyhledávány nebezpečné stavy nebo nouzové situace, jejich příčiny a dopady. Tento koncept zahrnuje soubor různých druhů technik posouzení a hodnocení rizik, například What-if, What-if/checklists, HAZOP, FMEA, FTA nebo jejich kombinace
- Metoda Delphi (Delphi Technique) – využívá společného názoru na analýzu a řešení rizika projektů získaného od odborníků.
- Analýza příčin a důsledků (Cause-and-Effect Analysis) – metoda kombinující ETA (strom událostí) a FTA (strom poruch) analýzy.
- Metoda PNH – bodová polo-kvantitativní metoda vhodná k rychlému vyhodnocení konkrétních rizik.

[9] [10]

2.4 Metodika zpracování analýzy v praktické části

Po dohodě s vedením společnosti bylo při této analýze postupováno v souladu s požadavky Zákona o kybernetické bezpečnosti (Zákon č. 181/2014 Sb. – „Zákon o kybernetické bezpečnosti…“, dále ZoKB) a prováděcí vyhlášky (Vyhláška č. 82/2018 Sb. – „Vyhláška o kybernetické bezpečnosti, dále VoKB). [11] [12]

S přihlédnutím k faktu, že většina systémů je řízena centrálně, tedy nejsou fyzicky přístupné v posuzovaném objektu, byla po dohodě se zodpovědnými zástupci společnosti v rámci této analýzy posuzována pouze vybraná opatření, spojená se zabezpečením primárních a podpůrných aktiv hodnoceného objektu.

S ohledem na charakter tohoto dokumentu a cíle analýzy byl zvolen méně formální přístup sběru informací a podkladů k vyhodnocení. Sběr informací probíhal formou rozhovorů s kompetentními pracovníky společnosti, prověřováním a ověřováním formou osobních návštěv v objektu.

2.4.1 Identifikace aktiv a jejich zhodnocení

V rámci tohoto kroku byla aktiva rozdělena následovně:

Třída aktiva: a) Primární aktivum; b) Podpůrné aktivum

Typ aktiva: a) Primární aktivum – Informace, Služby

b) Podpůrné aktivum – Technická aktiva, Zabezpečovací technika, Uživatelé, Dodavatelé, Zboží, Budova, Místnosti

Dále byly identifikovány vazby mezi primárními a podpůrnými aktivy. Tyto vazby je možno použít k seskupení aktiv pro následnou analýzu rizik.

Následně proběhlo ohodnocení důležitosti aktiv s uplatněním kvalitativní stupnice, která vyjadřuje míru důležitosti aktiva pro Společnost a je v souladu s požadavky VoKB.

Stupnice pro hodnocení aktiv je čtyřbodová. Nejméně závažný dopad je hodnocen 1 bodem a nejzávažnější dopad je hodnocen 4 body. Aktivum je hodnoceno pro každý bezpečnostní atribut.

Primární aktiva se hodnotí podle níže uvedených stupnic důvěrnosti, dostupnosti a integrity (CIA).

Tabulka 1_ Stupnice pro hodnocení aktiva důvěrnosti v souladu s VoKB [5] [11]

Úroveň		**Popis**
1	Nízká	Aktiva jsou **veřejně přístupná nebo byla určena ke zveřejnění** (např. na základě zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle tzv. traffic light protokolu (dále jen „TLP“) je využíváno označení TLP: WHITE.
2	Střední	Aktiva **nejsou veřejně přístupná** a tvoří je např. interní informace SPOLEČNOSTI. Ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním. V případě sdílení takového aktiva omezené na komunitu s třetími stranami, pokud jsou informace užitečné pro informovanost všech zúčastněných organizací a také u kolegů v rámci širší komunity nebo sektoru, ale ne prostřednictvím veřejně přístupných kanálů. Použití klasifikace podle TLP je využíváno zejména označení TLP: GREEN nebo TLP: AMBER.
3	Vysoká	Aktiva nejsou veřejně přístupná a jejich **ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními** (např. obchodní tajemství podle zákona č. 89/2012 Sb., občanský zákoník, osobní údaje podle zákona č. 110/2019 Sb., o zpracování osobních údajů. V případě sdílení takového aktiva omezené na organizaci účastníků a s klienty nebo zákazníky, kteří potřebují znát informace, aby se ochránili nebo zabránili dalším škodám. Použití klasifikace podle TLP je využíváno zejména označení TLP: AMBER.
4	Kritická	Aktiva nejsou veřejně přístupná a **vyžadují** nadstandardní **ochranu nad rámec předchozí kategorie** (např. strategické obchodní tajemství, citlivé osobní údaje, šifrovací materiál, autentizační údaje). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP: RED. Příjemci informací nesmí sdílet informace TLP: RED s žádnými stranami mimo konkrétní výměnu, schůzku nebo konverzaci, ve které byly původně zveřejněny. V kontextu schůzky jsou například informace TLP: RED omezeny na ty, kteří jsou na schůzce přítomni. Ve většině případů by informace TLP: RED měly být vyměňovány ústně nebo osobně.

Tabulka 2_Stupnice pro hodnocení integrity aktiva v souladu s VoKB [5] [11]

Úroveň		**Popis**
0	Nehodnoceno	Aktivum nebylo hodnoceno z hlediska integrity, resp. hodnocení integrity není relevantní.
1	Nízká	Aktivum **nevyžaduje ochranu** z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy společnosti.
2	Střední	Aktivum může vyžadovat ochranu z hlediska integrity. **Narušení** integrity aktiva může vést k poškození oprávněných zájmů Společnosti a může se projevit **méně závažnými dopady** na primární aktiva /ostatní aktiva.
3	Vysoká	Aktivum vyžaduje ochranu z hlediska integrity. **Narušení** integrity aktiva vede k poškození oprávněných zájmů Společnosti **s podstatnými dopady** na primární aktiva /ostatní aktiva.
4	Kritická	Aktivum vyžaduje ochranu z hlediska integrity. **Narušení** integrity vede k velmi vážnému poškození oprávněných zájmů Společnosti **s přímými a velmi vážnými dopady** na primární aktiva /ostatní aktiva.

Tabulka 3_Stupnice pro hodnocení dostupnosti aktiva v souladu s VoKB [5] [11]

Úroveň		**Popis**
1	Nízká	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca **do 1 týdne**).
2	Střední	Narušení dostupnosti aktiva by nemělo překročit **dobu pracovního dne (8hod.)**, dlouhodobější výpadek vede k možnému ohrožení zájmů Společnosti.
3	Vysoká	Narušení dostupnosti aktiva by **nemělo překročit dobu několika hodin (4hod.)**. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení zájmů Společnosti. Aktiva jsou považována za velmi důležitá.
4	Kritická	Narušení dostupnosti aktiva **není přípustné, a i krátkodobá nedostupnost (v řádu několika minut)** vede k vážnému ohrožení zájmů Společnosti.

2.4.2 Identifikace hrozeb a jejich zhodnocení

V rámci identifikace hrozeb a jejich zdrojů bylo postupováno tak, že byl sepsán seznam hrozeb a jejich zdrojů, které mohou svým působením ohrozit minimálně jedno z aktiv Společnosti. V rámci identifikace hrozeb a jejich zdrojů bylo vycházeno ze seznamu hrozeb, sestaveného z hrozeb VoKB, který byl dále doplněn o hrozby ze směrnice ISO 27005, další dostupné literatury či vlastních zkušeností.

Vybrané hrozby jsou ohodnoceny dle stupnice hodnocení hrozeb níže.

Tabulka 4_Stupnice hodnocení úrovní hrozeb [5] [11]

Úroveň		**Popis**
1	Nízká	Hrozba je zanedbatelná nebo je málo pravděpodobná. Předpokládaná **realizace** hrozby **není častější než jednou za 5 let**.
2	Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná **realizace** hrozby je v rozpětí **od 1 roku do 5 let**.
3	Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná **realizace** hrozby je **v rozpětí od 1 měsíce do 1 roku**.
4	Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná **realizace** hrozby je **častější než jednou za měsíc**.

2.4.3 Identifikace zranitelností a jejich zhodnocení

Pro identifikaci zranitelností se vycházelo ze seznamu hrozeb a zranitelností, který byl vytvořen ze zranitelností popsaných ve VoKB (viz příloha č. 3, VoKB) a dále byl doplněn o zranitelnosti ze směrnice ISO 27005, další dostupné literatury a informace o známých vadách a slabinách aktiv.

Zranitelnost byla hodnocena dle stupnice hodnocení úrovní zranitelností – viz uvedená stupnice. Při hodnocení zranitelností byla uvažována jednak opatření chránící aktivum proti působení hrozby, ale také přirozená odolnost aktiva proti působení hrozby.

Tabulka 5_Stupnice hodnocení úrovní zranitelností [5] [11]

Úroveň		**Popis**
1	Nízká	Zranitelnost neexistuje nebo je **zneužití** zranitelnosti **málo pravděpodobné**. Jsou zavedena **kvalitní bezpečnostní opatření**, která jsou schopna včas detekovat možné slabiny (zranitelnosti) nebo případné pokusy o jejich zneužití.
2	Střední	Zneužití zranitelnosti je **málo pravděpodobné** až pravděpodobné. Jsou zavedena **kvalitní bezpečnostní opatření**, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné slabiny nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.
3	Vysoká	Zneužití zranitelnosti je **pravděpodobné až velmi pravděpodobné**. Bezpečnostní **opatření jsou zavedena**, ale jejich **účinnost nepokrývá všechny** potřebné **aspekty** a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
4	Kritická	Zneužití zranitelnosti je **velmi pravděpodobné až víceméně jisté**. Bezpečnostní opatření nejsou realizována anebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření

2.4.4 Identifikace a hodnocení rizik

Pro určení úrovně rizika (tzn. jak je pravděpodobné, že hrozba nastane a jak vysoký bude mít dopad pro Společnost) byla použita funkce, která bere v úvahu význam aktiva, hrozbu a zranitelnost u aktiva. Úroveň jednotlivého dílčího rizika byla vypočítána dle následujícího vzorce:

R = V × H × Z

Legenda:

- R úroveň (hodnota) rizika
- V význam aktiva
- H hrozba
- Z zranitelnost

V rámci analýzy byl tento postup výpočtu použit stejným způsobem na všechna identifikovaná aktiva, hrozby a zranitelnosti.

2.4.5 Vyhodnocení úrovně rizika

V rámci vyhodnocení úrovně rizika bylo určeno, jestli dané riziko lze akceptovat nebo je nutné použít některou z možných variant k jeho ošetření.

Výsledné riziko způsobené hrozbou je považováno za maximální hodnotu složenou z dílčích rizik způsobených stejnojmennou hrozbou.

Při určování rizika u skupiny aktiv je brán nejvyšší význam rizika v této skupině. Pro vyhodnocení úrovně rizika je výsledná hodnota z výpočtu rizika pro každou skupinu aktiv porovnána s tabulkou níže.

Tabulka 6_Stupnice pro vyhodnocení úrovně rizika [5] [11]

Úroveň		**Popis rizika**
1–16	**Nízké**	Riziko je považováno za akceptovatelné.
17–32	**Střední**	Riziko může být řízeno méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko akceptovatelné.
33–48	**Vysoké**	Riziko je dlouhodobě neakceptovatelné a musí být zahájeny systematické kroky k jeho odstranění.
49–64	**Kritické**	Riziko je neakceptovatelné a musí být neprodleně zahájeny kroky k jeho odstranění.

Za horní mez akceptovatelnosti rizika bez další akce (ošetření rizika) byla v rámci této analýzy považována hodnota **16**. Rizika pod touto hranicí lze akceptovat.

2.4.6 Plán zvládání rizik

V rámci návrhu plánu zvládání rizik byla navržena opatření ke snížení hodnoty rizika.
U požadavků na zdroje bylo určeno, zda dané opatření (ne)bude vyžadovat dodatečné zdroje nad rámec stávajících, s následující logikou:
Finanční zdroje: uvedeno "NE", pokud opatření nevyžaduje finanční zdroje nebo zdroje jsou již alokovány (např. ve schváleném rozpočtu).
Lidské zdroje: uvedeno "ANO" v případech, kde je zřejmé, že k zavedení opatření nebudou stačit stávající lidské zdroje Společnosti a opatření by mělo vést k navýšení lidských zdrojů.
Technické zdroje: uvedeno "ANO" v případech, kdy realizace opatření bude spojena s nákupem nových nebo posílením stávajících technických zdrojů.
Informační zdroje: uvedeno "ANO" v případech, kdy k realizaci opatření je potřeba informační základna (její vytvoření nebo nákup) nebo stávající informační základna není dostatečná (např. potřeba proškolení pracovníků, vytvoření dokumentace, politiky, směrnice, postupů, prohloubení znalostí, know-how, doplnění evidencí, …).

II. PRAKTICKÁ ČÁST

3 CHARAKTERISTIKA ZVOLENÉHO OBJEKTU

Praktická část této bakalářské práce obsahuje popis a charakteristiku zvoleného objektu, analýzu rizik a návrh opatření pro zvýšení bezpečnosti. Vybraný objekt je jedním z obchodních domů řetězce, nabízejícího nábytek, bytové doplňky a služby spojené s oblastí bydlení. Vzhledem k citlivosti většiny informací obsažených v této bakalářské práci se autor s vedením společnosti domluvil, že v této práci nebudou uvedena jména ani konkrétní lokalita, a proto bude dále popisována lokalita, obchodní společnost i posuzovaný objekt anonymně s ohledem na ochranu citlivých informací.
Informace, které jsou v této analýze rizik použity, vycházejí z reálných diskusí se zástupci společnosti a jsou použity s jejich souhlasem stejně jako uveřejněné fotografie a další podobné materiály.

3.1 Obecný popis lokality

Vzhledem k tomu, že autor této bakalářské práce žije v Praze, tak se také hodnocený objekt nachází na území našeho hlavního města v jedné z mnoha komerčních zón. Tyto zóny lze obvykle nalézt podél hlavních příjezdových tras do Prahy. V okolí objektu se nacházejí podobné prodejny a multifunkční budovy, které kromě obchodních prostor nabízejí i kancelářské jednotky, kina, jídelní část a další možnosti relaxace nejen pro obyvatele nedalekého sídliště, ale také vesnic a menších měst v sousedství hranic Prahy. Z pohledu dopravní obslužnosti se jedná o lokalitu velmi dobře přístupnou, a to jak pro osobní automobily, tak pro nákladní dopravu, zásobující všechny prodejny a sklady v této oblasti. Zároveň je možno využít městskou a příměstskou hromadnou dopravu, jejíž dostupnost je v Praze také na vysoké úrovni. Komerční zóny podobné velikosti ročně navštíví miliony zákazníků, což přispívá nejen k atraktivitě těchto lokalit pro provozovatele a nájemce komerčních objektů, ale také to zvyšuje možná rizika spojená s hromaděním lidí, jako jsou různé stresové situace, případně možné fyzické útoky. Zároveň se tím také zvyšuje pravděpodobnost krádeží.

3.2 Obecný popis objektu

Jedná se o samostatně stojící vícepodlažní objekt ve obdélníkového půdorysu. Od podobných obchodních jednotek je oddělen silnicí a zelenými pásy vegetace. Na přední straně směrem k příjezdové cestě se nachází hlavní vchod. Na ploše před hlavním vchodem je situováno velké parkoviště pro zákazníky. Na jedné z podélných stran jsou umístěny

nákladní rampy a parkoviště pro kamionovou dopravu a další zásobování. Na další straně jsou umístěny obslužné vchody technického zázemí jako je sprinklerové hasicí zařízení, dieselagregát a další. Zároveň je zde místo pro napojení na hasičskou techniku. Střecha objektu je plochá stejně jako u podobných budov sloužících primárně jako obchodní a výstavní prostory. Po vstupu do objektu hlavním zákaznickým vchodem následuje foyer, ze kterého je možno pokračovat dále do budovy, a to buď přímo do prvního nadzemního podlaží nebo po schodišti do druhého nadzemního podlaží. V obou podlažích se nalézají prezentační prostory, které jsou logicky rozděleny do celků, věnovaných konkrétní části bytu/domu – předsíně, kuchyně, obývací pokoj, dětský pokoj, kancelář, koupelna, ložnice, zahrada a další. Vzhledem k tomu, že se jedná o prodejnu nábytku, je většina prodejních prostor zaplněna vystaveným nábytkem a bytovými doplňky. Skladové prostory jsou z pohledu od vchodu v zadní části budovy a od prodejních prostor jsou odděleny několika vchody přístupnými pouze zaměstnancům. Zároveň mají tyto prostory vlastní vstupy, kterými se doplňuje zboží. Tyto jsou přístupné ze strany budovy, kde jsou také nákladní rampy. Součástí budovy je i administrativní část, která je opět přístupná pouze zaměstnancům.

3.3 Obecný popis společnosti

Jedná se o nadnárodní společnost s několik desítek let dlouhou tradicí prodeje nábytku a bytových doplňků, která provozuje své prodejny v České republice i dalších lokalitách v Evropě. Prodejní plochou v řádu desítek tisíc metrů čtverečních se řadí mezi největší české prodejce. Společnost provozuje také e-shop, ve kterém je možno nakoupit i zboží, které na prodejnách není k dispozici. Většina položek je skladem k okamžitému odběru. Kromě prodeje nabízí společnost zákazníkům také konzultace spojené například s plánováním kuchyně, pracovny či kanceláře. Pro tuto činnost jsou vyškoleni specialisté na jednotlivé oblasti. Společnost nabízí také dopravu nakoupeného zboží na místo dle požadavku zákazníka, montáž a poprodejní podporu. V rámci řešení reklamací je k dispozici profesionální zákaznický servis.

3.4 Popis současného stavu

Aktuální stav bezpečnostních opatření v oblasti fyzické bezpečnosti je v posuzovaném objektu na vysoké úrovni, jelikož společnost zaměstnává odborníka, který se oblasti fyzické bezpečnosti věnuje několik desítek let.

3.4.1 Perimetrická ochrana

Je řešena pomocí kamerového systému a kamery jsou rozmístěny tak, aby bylo možno sledovat dění v téměř celém okolí budovy.

Obrázek 3_Kamera Illustra [13]

3.4.2 Plášťová ochrana

Všechna okna v objektu jsou chráněna magnetickými kontakty. Dveře a další vstupní prostory pro zaměstnance je možno otevřít pouze vstupní kartou, případně generálním klíčem, který je uzamčen v klíčovém trezoru a vydáván proti podpisu. Zákazníci do prodejny vstupují přes dvoje automatické skleněné posuvné dveře, které jsou otevřeny po celou prodejní dobu. Mimo prodejní dobu jsou dveře uzamčeny.

Obrázek 4_Vstupní systém Kantech [14]

3.4.3 Prostorová ochrana

Ve vnitřních prostorách prodejny, zázemí a skladových prostorách jsou nainstalovány PIR detektory a zároveň jsou všechny tyto prostory monitorovány kamerovým systémem.

Obrázek 5_Detektor pohybu PIR [vlastní]

Obrázek 6_Kamera Illustra [15]

3.4.4 Předmětová ochrana

Zboží v prodejně není chráněno magnetickými ani jinými ochrannými prvky a v také objektu nejsou instalovány bezpečnostní rámy.

3.4.5 Požární ochrana

V celém objektu je nainstalováno sprinklerové hasicí zařízení a rozmístěny hasicí přístroje, které jsou dobře přístupné. Hasicí přístroje jsou pravidelně kontrolovány externí firmou. V objektu jsou také rozmístěny automatické i manuální hlásiče požáru a OPPO. Cvičné požární poplachy jsou vyhlašovány minimálně 1× ročně.

Obrázek 7_OPPO [vlastní]

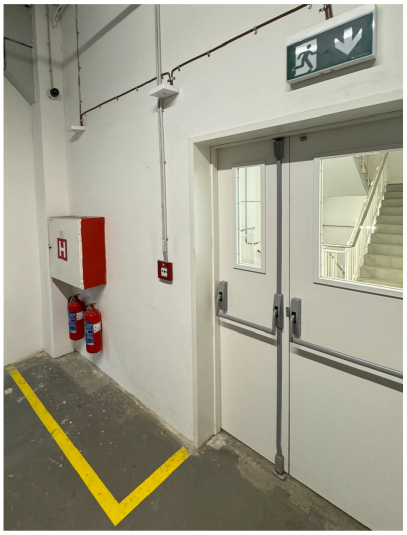
Obrázek 8_Hasicí přístroj [vlastní]

Obrázek 9_Manuální hlásič požáru [vlastní]

Obrázek 10_Detektor kouře [vlastní]

3.4.6 Nouzové východy a značení

Nouzové východy jsou přehledně označeny včetně grafického plánu evakuace.



Obrázek 11_Nouzový východ [vlastní]

Kamerové systémy, stejně jako další detektory, jsou napojeny na dohledové a poplachové centrum, které si provozuje společnost sama. Současně využívá služeb externího DPPC, které zajišťuje výjezd bezpečnostních pracovníků v případě poplachů. Na pokladnách a pracovištích se zvýšeným pohybem zákazníků, na kterých mohou vznikat stresové situace, např. na oddělení reklamací, jsou umístěna tísňová tlačítka. Jejich aktivace znamená okamžitý výjezd bezpečnostní služby a tento výjezd nelze odvolat. V posuzovaném objektu jsou také umístěny technologické prostředky ICT a zabezpečovací techniky, např. servery, úložiště atd., na kterých jsou uložena data. Místnost s těmito technologiemi je umístěna uvnitř budovy v prostorách s omezeným přístupem na kartu a zároveň střežena kamerami a pohybovými čidly.

V této kapitole byl charakterizován zvolený objekt z hlediska lokality a popisu samotného objektu. Dále byla stručně popsána společnost provozující tento objekt a aktuální stav vybraných bezpečnostních opatření v objektu. Tyto údaje byly na žádost vedení společnosti anonymizovány a všechny popisy jsou proto obecnější povahy.

4 ANALÝZA SOUČASNÉHO STAVU

4.1 Identifikace a hodnocení aktiv

Na základě metodiky popsané výše v teoretické části byla nejprve identifikována všechna aktiva, která jsou relevantní pro účel prováděné analýzy rizik. Tato aktiva byla rozdělena do tříd na primární a podpůrná.

1) **Primární aktiva**
    - Služba prodeje (proces) – jedná se o nejdůležitější aktivum obchodní společnosti, při jehož dlouhodobém ohrožení může dojít k až fatálním následkům.
    - Data o prodeji (informace) – toto je druhé velmi důležité aktivum, které musí být velmi dobře zabezpečeno.
    - Data o zákaznících (informace) – regulováno GDPR, v případě ztráty mohou hrozit i finanční postihy.
    - Data o skladových zásobách (informace) – tato data slouží jako vstup pro doplňování zboží a je tedy nezbytné, aby byla přesná a dostupná.
    - Data o zaměstnancích (informace) – regulováno GDPR, zároveň citlivá i v případě úniku uvnitř firmy.
2) **Podpůrná aktiva**
    - Zboží
    - Platební a pokladní terminály
    - Zabezpečovací technika
    - ICT vybavení
    - Zaměstnanci
    - Zákazníci
    - Dodavatelé
    - Budova

Mezi podpůrná aktiva řadíme všechna ostatní aktiva, která nebyla identifikována jako primární a zároveň by bez nich tato nemohla plnit svou primární funkci.

Následně bylo provedeno vyhodnocení těchto identifikovaných aktiv z hlediska důvěrnosti, integrity a dostupnosti a byla určena hodnota významu každého aktiva pro posuzovanou společnost.

Tabulka 7_Primární a podpůrná aktiva Společnosti [vlastní]

ID	Třída aktiv	Kategorie	Název aktiva	Význam aktiva		Klasifikace [1-4] C	I	A
1	Primární	Proces	Služba prodeje	4		2	2	4
2	Primární	Data	Data o prodeji	3		3	3	3
3	Primární	Data	Data o zákaznících	3		3	3	1
4	Primární	Data	Data skladových systémů	3		3	3	3
5	Primární	Data	Data o zaměstnancích	4		4	3	2
6	Podpůrné	Prodejna	Objekt prodejny v Praze	3		1	1	3
7	Podpůrné	Serverovna	Místnost, ve které jsou umístěny HW/SW prostředky ICT a zabezpečovací techniky	3		1	1	3
8	Podpůrné	HW/SW serverů	HW a SW serverů	3		2	3	3
9	Podpůrné	HW/SW úložišť	HW a SW úložišť	3		3	3	3
10	Podpůrné	HW/SW terminálových PC	HW a SW terminálových stanic na prodejně	2		2	2	2
11	Podpůrné	Platební a Pokladní terminály	Terminály pro zajištění kontaktních a bezkontaktních plateb zákazníky a pokladní terminály	3		2	3	3
12	Podpůrné	Switch (přepínač)	HW a SW síťových prvků	3		1	1	3
13	Podpůrné	PZTS	Poplachové a tísňové zabezpečovací systémy	3		3	2	2
14	Podpůrné	EPS	Elektronická požární signalizace	2		2	2	2
15	Podpůrné	ESKV	Elektronická kontrola vstupu	2		2	2	2
16	Podpůrné	VSS	Kamerový systém vně i uvnitř budovy	2		2	2	2
17	Podpůrné	SHZ	Samočinné hasicí zařízení – sprinklery, hasicí přístroje a další hasební prostředky	2		2	2	2

18	Podpůrné	Dieselagregát	Prostředky k zajištění nepřerušitelného napájení budovy – dieselagregát	2		2	2	2
19	Podpůrné	UPS	Prostředky k zajištění nepřerušitelného napájení ICT a dalších systémů – UPC	2		2	2	2
20	Podpůrné	Uživatel – interní	Skladníci, prodavači, management a ostatní zaměstnanci prodejny	3		3	3	3
21	Podpůrné	Uživatel – externí	Zákazníci pohybující se v prodejních prostorách	1		1	1	1
22	Podpůrné	Zboží prodej	Produkty vystavené v prodejních prostorách	3		2	2	3
23	Podpůrné	Zboží sklad	Produkty na skladě	3		2	2	3
24	Podpůrné	Dodavatel A	Dodavatelé technologických produktů jako energie, dohledové služby, konektivita atd.	3		1	1	3
25	Podpůrné	Dodavatel B	Dodavatelé zboží určeného k prodeji	3		1	1	3

Mezi primárními aktivy a podpůrnými aktivy mohou existovat závislosti, které je nutné identifikovat a správně popsat. Tyto závislosti mohou být použity při seskupování aktiv, když je to v rámci analýzy rizik výhodné. Závislosti mezi jednotlivými aktivy v identifikovanými v rámci této analýzy rizik naznačuje následující tabulka.

Tabulka 8_Vazby primární/podpůrná aktiva [vlastní]

	Primární aktiva				
Podpůrná aktiva	**Služba prodeje**	**Data o prodeji**	**Data o zákaznících**	**Data skladových systémů**	**Data o zaměstnancích**
Objekt prodejny v Praze	X				
Místnost, ve které jsou umístěny HW/SW prostředky ICT a zabezpečovací techniky	X				
HW a SW serverů	X	X	X	X	X
HW a SW úložišť	X	X	X	X	X
HW a SW terminálových stanic na prodejně	X	X	X	X	
Terminály pro zajištění kontaktních a bezkontaktních plateb zákazníky a pokladní terminály	X	X	X	X	
HW a SW síťových prvků	X				

Poplachové a tísňové zabezpečovací systémy	X				
Elektronická požární signalizace	X				
Elektronická kontrola vstupu	X				X
Kamerový systém vně i uvnitř budovy	X				
Samočinné hasicí zařízení – sprinklery, hasicí přístroje a další hasební prostředky	X				
Prostředky k zajištění nepřerušitelného napájení budovy – dieselagregát	X	X	X	X	
Prostředky k zajištění nepřerušitelného napájení ICT a dalších systémů – UPC	X	X	X	X	X
Skladníci, prodavači, management a ostatní zaměstnanci prodejny	X	X	X	X	X
Zákazníci pohybující se v prodejních prostorách	X	X	X		
Produkty vystavené v prodejních prostorách	X				
Produkty na skladě	X				
Dodavatelé technologických produktů jako energie, dohledové služby, konektivita atd.	X				
Dodavatelé zboží určeného k prodeji	X				

4.2 Identifikace a hodnocení hrozeb

V tomto kroku byly identifikovány hrozby, které se mohou na výše uvedených aktivech uplatnit. Při jejich identifikaci a hodnocení bylo postupováno podle metodiky popsané v teoretické části práce.

Tabulka 9_Katalog hrozeb [vlastní] [11]

	Hrozby	Úroveň
1	**Poškození nebo selhání technického anebo programového vybavení**	
1.1	Poškození nebo selhání technického vybavení (selhání HW/SW, infrastruktury, ztráta dat, selhání podpůrných zařízení atp.)	3
1.2	Nedostupnost Informačního systému, infrastruktury HW, aplikace, SW a nemožnost poskytování služeb a provozních činností	2
2	**Zneužití identity**	
2.1	Zneužití identity uživatele / admin	3
3	**Škodlivý kód (například viry, spyware, trojské koně)**	
3.1	Škodlivý kód (například malware, kyberútok) způsobí selhání HW a nedostupnost/ nefunkčnost IS/aplikace	2
4	**Narušení fyzické bezpečnosti**	
4.1	Narušení fyzické bezpečnosti (ztráta, odcizení nebo poškození aktiva)	4
4.2	Narušení / poškození – požár	1
4.3	Poškození vodou (záplava, povodeň, prasklé potrubí v budově atp.)	2
4.4	Narušení fyzické bezpečnosti – návštěvníci / externí subjekty osoby vstup do interních prostor	3
4.5	Narušení / poškození – vandalismus	3

5	**Zneužití nebo neoprávněná modifikace údajů (škodlivá činnost)**	
5.1	Zneužití údajů nebo jejich neoprávněná modifikace (předání obch. dat/ údajů, úmysl …)	2
6	**Nedodržení smluvního závazku ze strany dodavatele**	
6.1	Nedodržení smluvního závazku ze strany dodavatele (Smlouva, Bezpečnostní pravidla, zboží)	2
7	**Pochybení ze strany zaměstnanců/ Lidské selhání**	
7.1	Pochybení ze strany zaměstnanců – chyba zaměstnance (např. smazání dat, špatné vložená data, personální problémy, poškození infrastruktury, Chybné řídící rozhodnutí, Nedodržování dokumentovaných procedur, předpisů a směrnic)	3
8	**Zneužití vnitřních prostředků, sabotáž**	
8.1	Zneužití vnitřních prostředků, sabotáž – uživatelé, administrátor	3
9	**Dlouhodobé přerušení poskytování služeb el. komunikací, dodávky el. energie nebo jiných důležitých služeb**	
9.1	Dlouhodobé. přerušení poskytování služeb el. komunikací, dodávky el. energie nebo jiných důležitých služeb	2
	Ostatní hrozby	
10	Finanční ztráta a poškození reputace z narušení poskytování služeb zákazníkům	2
11	Epidemie (např. Covid-19 nebo jiné podobné nemoci)	2

4.3 Identifikace a hodnocení zranitelností

V tomto kroku byly identifikovány zranitelnosti, které mohou být zneužity jednou nebo více výše uvedenými hrozbami. Při jejich identifikaci a hodnocení bylo také postupováno podle metodiky popsané v teoretické části práce.

Tabulka 10_Katalog zranitelností [vlastní] [11]

	Zranitelnosti	Úroveň
Z1	Zastaralost aktiv – IT	1
Z2	Zastaralost aktiv – zabezpečovací technika	1
Z3	Nedostatečná ochrana vnějšího perimetru	2
Z4	Nedostatečné bezpečnostní povědomí uživatelů	3
Z5	Nevhodné nastavení přístupových oprávnění	3
Z6	Nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů	2
Z7	Nedostatečné monitorování činnosti uživatelů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování	3
Z8	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů	2
Z9	Nedostatečná ochrana aktiv	3
Z10	Nevhodná bezpečnostní architektura – zabezpečovací technika	1
Z11	Neschopnost včasného odhalení pochybení ze strany zaměstnanců	2
Z12	Nedostatek zaměstnanců s potřebnou odbornou úrovní	3

4.4 Identifikace a hodnocení zranitelností

Na základě hodnocení významu aktiv bylo provedeno hodnocení rizik pro skupinu primárních aktiv ohodnocených hodnotou 4 a na ně navázaných podpůrných aktiv. Zranitelnosti byly seskupeny a hodnota skupiny byla určena nejvyšší hodnotou zranitelnosti ve skupině.

Tabulka 11_Skupina aktiv 4 [vlastní] [11]

Skupina aktiv – Význam aktiva 4	
Primární aktiva	Služba – služba prodeje, Informace – data o zaměstnancích
Technické a programové vybavení (HW+SW)	HW/SW serverů, HW/SW úložišť, HW/SW terminálových PC, Platební a Pokladní terminály, Switch (přepínač)
Zabezpečovací technika	PZTS, EPS, ESKV, VSS, SHZ, Dieselagregát, UPS,
Uživatelé	Zaměstnanci; Zákazníci
Dodavatelé	Dodavatele produktů pro provoz prodejny jako energie, dohledové služby, konektivitu a další; Dodavatelé zboží určeného k prodeji
Zboží	Produkty vystavené na prodejní ploše a na skladě
Budova, Místnosti	Objekt prodejny v Praze; místnost, ve které jsou umístěny servery ICT a dohled

Tabulka 12_Hodnocení skupina 4 [vlastní] [11]

ID	Hrozba	Zranitelnosti	Hrozba (hodnocení)	Zranitelnost (hodnocení)	Riziko (hodnota)
1.1	Poškození nebo selhání technického vybavení	Z1, Z2, Z3, Z8, Z9, Z11, Z12	3	2	24
1.2	Nedostupnost Informačního systému a nemožnost poskytování služeb a provozních činností	Z1, Z2, Z3, Z8, Z9, Z11, Z12	2	3	24
2.1	Zneužití identity uživatele / admin	Z1, Z2, Z4, Z5, Z6, Z7, Z8, Z9, Z11, Z12	3	3	36
3.1	Škodlivý kód	Z1, Z3, Z4, Z5, Z6, Z7, Z8, Z9, Z11	2	3	24
4.1	Narušení fyzické bezpečnosti (ztráta, odcizení nebo poškození aktiva)	Z2, Z3, Z4, Z5, Z6, Z7, Z8, Z9, Z10, Z11, Z12	4	3	48
4.2	Narušení / poškození – požár	Z2, Z3, Z7, Z8, Z9, Z10, Z11	1	3	12
4.3	Poškození vodou	Z2, Z3, Z9, Z10	2	3	24
4.4	Narušení fyzické bezpečnosti – návštěvníci / externí subjekty osoby vstup do interních prostor	Z2, Z3, Z5, Z7, Z8, Z9, Z10	3	3	36
4.5	Narušení / poškození – vandalismus	Z2, Z3, Z7, Z8, Z9, Z10	3	3	36

5.1	Zneužití údajů nebo jejich neoprávněná modifikace	Z1, Z2, Z3, Z4, Z5, Z6, Z7, Z8, Z9, Z11, Z12	2	3	24
6.1	Nedodržení smluvního závazku ze strany dodavatele	Z7, Z8, Z9, Z12	2	3	24
7.1	Pochybení ze strany zaměstnanců	Z1, Z2, Z3, Z4, Z5, Z6, Z7, Z9, Z10, Z11, Z12	3	3	36
8.1	Zneužití vnitřních prostředků, sabotáž – uživatelé, administrátor	Z1, Z2, Z3, Z5, Z6, Z7, Z8, Z9, Z10, Z11	3	3	36
9.1	Dlouhodobé přerušení poskytování služeb el. komunikací, dodávky el. energie nebo jiných důležitých služeb	Z1, Z2, Z3, Z9	2	2	16
10	Finanční ztráta a poškození reputace z narušení poskytování služeb zákazníkům	Z4, Z6, Z7, Z8, Z9, Z11, Z12	2	3	24
11	Epidemie (např. Covid-19)	Z8, Z11, Z12	2	3	24

Stejným způsobem bylo provedeno hodnocení pro skupinu primárních aktiv s hodnotou 3 a na ně navázaných podpůrných aktiv.

Tabulka 13_Skupina aktiv 3 [vlastní] [11]

Skupina aktiv – Význam aktiva 3	
Primární aktiva	Data o prodeji, Data o zákaznících, Data skladových systémů
Technické a programové vybavení (HW+SW)	HW/SW serverů, HW/SW úložišť, HW/SW terminálových PC, Platební a Pokladní terminály
Zabezpečovací technika	Dieselagregát, UPS
Uživatelé	Zaměstnanci; Zákazníci
Dodavatelé	N/A
Zboží	N/A
Budova, Místnosti	N/A

Tabulka 14_Hodnocení skupina 3 [vlastní] [11]

ID	**Hrozba**	**Zranitelnosti**	**Hrozba** (hodnocení)	**Zranitelnost** (hodnocení)	**Riziko** (hodnota)
1.1	Poškození nebo selhání technického vybavení	Z1, Z2, Z3, Z8, Z9, Z11, Z12	3	2	18
1.2	Nedostupnost Informačního systému a nemožnost poskytování služeb a provozních činností	Z1, Z2, Z3, Z8, Z9, Z11, Z12	2	3	18
2.1	Zneužití identity uživatele / admin	Z1, Z2, Z4, Z5, Z6, Z7, Z8, Z9, Z11, Z12	3	3	27
3.1	Škodlivý kód	Z1, Z3, Z4, Z5, Z6, Z7, Z8, Z9, Z11	2	3	18

4.1	Narušení fyzické bezpečnosti (ztráta, odcizení nebo poškození aktiva)	Z2, Z3, Z4, Z5, Z6, Z7, Z8, Z9, Z10, Z11, Z12	4	3	36
4.2	Narušení / poškození – požár	Z2, Z3, Z7, Z8, Z9, Z10, Z11	1	3	9
4.3	Poškození vodou	Z2, Z3, Z9, Z10	2	3	18
4.4	Narušení fyzické bezpečnosti – návštěvníci / externí subjekty osoby vstup do interních prostor	Z2, Z3, Z5, Z7, Z8, Z9, Z10	3	3	27
4.5	Narušení / poškození – vandalismus	Z2, Z3, Z7, Z8, Z9, Z10	3	3	27
5.1	Zneužití údajů nebo jejich neoprávněná modifikace	Z1, Z2, Z3, Z4, Z5, Z6, Z7, Z8, Z9, Z11, Z12	2	3	18
6.1	Nedodržení smluvního závazku ze strany dodavatele	Z7, Z8, Z9, Z12	2	3	18
7.1	Pochybení ze strany zaměstnanců	Z1, Z2, Z3, Z4, Z5, Z6, Z7, Z9, Z10, Z11, Z12	3	3	27
8.1	Zneužití vnitřních prostředků, sabotáž – uživatelé, administrátor	Z1, Z2, Z3, Z5, Z6, Z7, Z8, Z9, Z10, Z11	3	3	27
9.1	Dlouhodobé přerušení poskytování služeb el. komunikací, dodávky el. energie nebo jiných důležitých služeb	Z1, Z2, Z3, Z9	2	2	12
10	Finanční ztráta a poškození reputace z narušení poskytování služeb zákazníkům	Z4, Z6, Z7, Z8, Z9, Z11, Z12	2	3	18
11	Epidemie (např. Covid-19)	Z8, Z11, Z12	2	3	18

V této kapitole byla zpracována analýza rizik. Při zpracování analýzy bylo postupováno na základě metodiky popsané v teoretické části této bakalářské práce. Výsledkem bylo ohodnocení jednotlivých rizik ohrožujících posuzované skupiny aktiv, které bylo v další kapitole použito pro identifikaci priorit opatření.

5 NÁVRH OPATŘENÍ KE ZVÝŠENÍ BEZPEČNOSTI

Na základě výsledků hodnocení rizik byl vypracován plán zvládání rizik pro skupinu aktiv s hodnotou 4. Plán obsahuje návrhy opatření na zmírnění rizik a zároveň identifikované požadavky na potřebné finanční, technické, lidské a informační zdroje.

S přihlédnutím k tomu, že žádný rizikový scénář nemá hodnocení v úrovni Kritické, nebyla tato kategorie uvažována při určování priorit jednotlivých navržených opatření.

Tabulka 15_Opatření – priorita [vlastní]

Úroveň		Priorita opatření
1–16	**Nízké**	3
17–32	**Střední**	2
33–48	**Vysoké**	1
49–64	**Kritické**	nebyla přiřazena

5.1 Ošetření rizik

V tabulce níže je seznam rizik, seřazený podle priorit. Ke každému riziku byla přiřazena varianta jeho ošetření v souladu s teoretickou částí práce.

Tabulka 16_Ošetření rizika [vlastní]

			Ošetření rizika			
ID Riziko	**Riziko Hodnota**	**Priorita**	**Modifikace**	**Vyhnutí**	**Akceptace**	**Přenesení**
4.1	48	1	x			
4.4	36	1	x			
4.5	36	1	x			
2.1	36	1	x			
7.1	36	1	x			
8.1	36	1	x			
1.1	24	2	x			
1.2	24	2		x		
3.1	24	2	x			
4.3	24	2	x			
5.1	24	2	x			
6.1	24	2				x
10	24	2				x
11	24	2				x
9.1	16	3				x
4.2	12	3			x	

5.2 Doporučená opatření

V následující tabulce jsou ke každému riziku navržena doporučená bezpečnostní a další opatření.

Tabulka 17_Navržená doporučená opatření [vlastní]

ID Riziko	Doporučená opatření
4.1	Vyžadovat a kontrolovat dodržování organizačních a technických opatření pro zajištění bezpečného používání aktiv, např. kontrola vstupu do objektu, zejména ve skladových prostorech. Zvážení instalace akustomagnetických detekčních rámů pro zvýšení ochrany zboží na prodejně. Zvážení posílení fyzické ostrahy uvnitř objektu a operátorů DPPC. Poučení zaměstnanců o bezpečnosti informací a o dodržování bezpečnostních pravidel.
4.4	Vyžadovat a kontrolovat dodržování organizačních a technických opatření pro zajištění bezpečného používání aktiv, např. kontrola vstupu do objektu, zejména ve skladových prostorách. Zvážit posílení obsluhy DPPC, případně ostrahy prodejny. Poučení zaměstnanců o bezpečnosti informací a o dodržování bezpečnostních pravidel.
4.5	Zvážit například instalaci kamer s IR spektrem. Prostory přístupné vně budovy posílit o další bezpečnostní prvek, například použít otřesová čidla na žebřících na vnějším plášti budovy.
2.1	Používat více faktorové ověřování uživatelů a administrátorů. Vytvoření separátních administrátorských účtů určených pouze ke správě. Poučení a zvýšení povědomí zaměstnanců o bezpečnosti informací a zneužití identity. Zavést pravidelná školení pro zaměstnance v oblasti informační bezpečnosti.
7.1	Definovat požadavky a pravidla pro používání aktiv. Poučení zaměstnanců o bezpečnosti informací a rizik při používání aktiv. Pravidelné školení zaměstnanců v oblasti kyberbezpečnosti a BOZP.
8.1	Definovat požadavky a pravidla pro používání aktiv. Implementovat centrální autorizační platformu pro řízení přístupových oprávnění. Implementovat segmentaci sítě a s její pomocí řídit přístupy uživatelů. Implementovat nástroje pro monitorování aktivit uživatelů.
1.1	Definovat požadavky a pravidla pro používání aktiv. Implementovat organizační a technická opatření pro zajištění bezpečného používání aktiv a provozu, včetně dostupnosti aktiv (dat a infrastruktury). Poučení a zvýšení povědomí zaměstnanců o bezpečnosti informací a o dodržování bezpečnostních pravidel.
1.2	Definovat úplné DR plány, které obsahují procesy a postupy reálně vedoucí k řešení krizových situací a tyto postupy pravidelně testovat. Zrevidovat úrovně SLA u dodavatelů technologií a služeb a případně upravit podle DR plánů. Zavést pravidelné školení pro zaměstnance v oblasti informační bezpečnosti.
3.1	Implementovat prostředky pro ochranu před škodlivým kódem. Zavést pravidelné školení pro zaměstnance v oblasti informační bezpečnosti.

4.3	Provést detailnější posouzení současných opatření a implementace technických opatření k minimalizaci poškození aktiv vodou.
5.1	Definovat požadavky a pravidla pro používání aktiv. Implementovat centrální autorizační platformu pro řízení přístupových oprávnění. Implementovat segmentaci sítě a s její pomocí řídit přístupy uživatelů. Implementovat nástroje pro prevenci a detekci kybernetických útoků a monitorování aktivit uživatelů.
6.1	Pravidelně vyhodnocovat dodávané služby dle stanovených kritérii smlouvy/ SLA a to i z pohledu bezpečnosti informací. Zrevidovat aktuální pojistné smlouvy.
10	Zrevidovat aktuální pojistné smlouvy. Poučení zaměstnanců o bezpečnosti informací a o dodržování bezpečnostních pravidel.
11	Zrevidovat aktuální pojistné smlouvy. Poučení zaměstnanců o bezpečnosti informací a o dodržování bezpečnostních pravidel.
9.1	Zrevidovat smlouvy s aktuálními poskytovateli a případně upravit poskytovaná SLA, aby byla v souladu s parametry záložních bateriových a dieselových systémů. Zrevidovat aktuální pojistné smlouvy.
4.2	Zajistit pravidelné kontroly hasebních prostředků a dalších instalovaných prvků požární ochrany. Pokračovat v provádění pravidelných požárních cvičení. Poučení zaměstnanců o pravidlech BOZP a požární ochrany.

5.3 Potřebné zdroje

V tabulce níže jsou v návaznosti na navržená opatření identifikovány jednotlivé oblasti zdrojů, navržených k realizaci daného opatření.

Tabulka 18_Potřebné zdroje k zajištění navržených opatření [vlastní]

	Zdroje							
	Finanční		**Lidské**		**Technické**		**Informační**	
ID Riziko	**Status**	**Pozn.**	**Status**	**Pozn.**	**Status**	**Pozn.**	**Status**	**Pozn.**
4.1	ANO	Nákup technologie	NE		ANO		ANO	Poučení / školení
4.4	ANO	Rozpočet na zdroje/ role	ANO		NE		ANO	Poučení / školení
4.5	ANO	Nákup technologie	NE		ANO		NE	

2.1	ANO	Nákup technologie	NE		NE		ANO	Poučení / školení
7.1	NE		NE		NE		ANO	Poučení / školení
8.1	ANO	Nákup služeb	NE		ANO	Nákup technologie	NE	
1.1	NE		NE		NE		ANO	Poučení / školení
1.2	ANO	Nákup služeb	NE		ANO		ANO	Poučení / školení
3.1	ANO	Nákup technologie	NE		ANO		ANO	Poučení / školení
4.3	ANO	Nákup služeb	NE		NE		NE	
5.1	ANO	Nákup služeb	NE		ANO	Nákup technologie	NE	
6.1	ANO	Pojištění	NE		NE		NE	
10	ANO	Pojištění	NE		NE		ANO	Poučení / Školení
11	ANO	Pojištění	NE		NE		ANO	Poučení / Školení
9.1	ANO	Nákup služeb	NE		NE		NE	
4.2	ANO	Nákup služeb	NE		NE		ANO	Poučení / Školení

V této kapitole byly popsány návrhy opatření ke zvýšení bezpečnosti. Jednotlivým opatřením byla určena priorita řešení a byly k nim identifikovány zdroje potřebné k jejich případné realizaci. Tato opatření zahrnují technické, organizační a administrativní kroky, které by měly být implementovány s cílem minimalizovat identifikovaná rizika a zlepšit celkovou bezpečnostní situaci. Z tabulek vyplývá, že ani pro jednu skupinu aktiv nebylo riziko ohodnoceno kategorií Kritické.

ZÁVĚR

Cílem této bakalářské práce bylo provedení analýzy současného stavu vybraného objektu a navržení bezpečnostních opatření.

První část práce byla věnována teoretickému základu, kde byly definovány a podrobně popsány základní pojmy, které tvoří důležité stavební kameny pro pochopení procesu analýzy rizik a z ní vyplývajícího efektivního řízení rizik.

V druhé části práce byly obecně popsány jednotlivé kroky zpracování analýzy a stručně specifikovány kvantitativní a kvalitativní metody pro analýzu rizik. Dále byl uveden rámec a podrobně představena metodika, podle které bylo postupováno při zpracování analýzy v praktické části.

V rámci třetí kapitoly byl popsán analyzovaný objekt, lokalita, společnost, která ho provozuje a aktuální stav vybraných bezpečnostních opatření. Tyto údaje byly na žádost vedení společnosti anonymizovány a všechny popisy jsou proto obecnější povahy.

Ve čtvrté kapitole byla zpracována analýza rizik. Výsledkem bylo ohodnocení jednotlivých rizik ohrožujících posuzované skupiny aktiv, které bylo v další kapitole použito pro identifikaci priorit opatření.

V poslední páté kapitole byly popsány návrhy opatření ke zvýšení bezpečnosti. Výsledky analýzy ukázaly, že žádný rizikový scénář nespadá do kritické kategorie. Scénáře hodnocené v kategorii vysokého rizika se týkají fyzické a kybernetické bezpečnosti. Doporučená opatření je možno realizovat buď formou úpravy aktuálních opatření, jako například posílení ostrahy nebo instalace detekčních rámů, nebo úpravou stávajících a zavedením nových procesů. Zároveň je doporučeno pravidelně školit zaměstnance, protože se jedná o důležité preventivní opatření, kterým je možno předejít budoucím škodám z nedbalosti či nevědomosti. Některé že scénářů hodnocených střední úrovní je možno přenést na jiný subjekt například formou pojištění a tím snížit jejich úroveň.

Tato bakalářská práce nabídla konkrétní a realizovatelné návrhy na zlepšení bezpečnostního stavu analyzovaného objektu, které mohou být v souladu s plánem hodnocené společnosti použity jako základ pro realizaci podrobnějších auditů dalších provozovaných objektů.

Závěrem je vhodné zdůraznit, že vedení společnost vnímá důležitost zabezpečení aktiv velmi zodpovědně a snaží se postupně přijímat rozhodnutí vedoucí k dalšímu posílení již realizovaných opatření a tím ke zlepšení bezpečnostního profilu společnosti.

SEZNAM POUŽITÉ LITERATURY

[1] *Heslo | Akademický slovník současné češtiny*, 2023. Online. Dostupné z: https://slovnikcestiny.cz/heslo/anal%C3%BDza/0/5796. [cit. 2023-12-19].

[2] *Metodiky – Výzkumný ústav bezpečnosti práce, v. v. i.*, 2022. Online. Dostupné z: https://vubp.cz/prevence-zavaznych-havarii/metodiky/. [cit. 2023-12-19].

[3] MAREK, Petr, 2011. Riziko a jeho pojetí: vědecké a umělecké. Online. *Český finanční a účetní časopis*. 2011-10-1, roč. 2011, č. 3, s. 4-5. ISSN 18022200. Dostupné z: https://doi.org/10.18267/j.cfuc.109. [cit. 2024-05-26].

[4] SMEJKAL, Vladimír a RAIS, Karel, 2013. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Expert (Grada). Praha: Grada. ISBN 9788024746449.

[5] *Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti.pdf*, 2022. Online. Národní úřad pro kybernetickou a informační bezpečnost – Podpůrné materiály. Dostupné z: https://nukib.gov.cz/download/publikace/podpurne_materialy/Prvodce%20zenm%20aktiv%20a%20rizik%20dle%20vyhlky%20o%20kybernetick%20bezpenosti.pdf. [cit. 2024-05-20].

[6] *Terminologický slovník – krizové řízení a plánování obrany státu – Ministerstvo vnitra České republiky*, 2016. Online. Dostupné z: https://www.mvcr.cz/clanek/terminologicky-slovnik-krizove-rizeni-a-planovani-obrany-statu.aspx. [cit. 2023-12-19].

[7] *What is the CIA triad?*, 2019. Online. In: What is the CIA triad? | CyberOne. Dostupné z: https://e7p6wefkwp4.exactdn.com/wp-content/uploads/2023/01/What-is-the-CIA-triad_431804671-550x500px.png?strip=all&lossy=1&w=418&ssl=1. [cit. 2024-05-20].

[8] *Co je CIA triáda informační bezpečnosti | Informační bezpečnost | Aptien*, 2023. Online. Dostupné z: https://aptien.com/cs/kb/articles/what-is-cia-triad. [cit. 2023-12-19].

[9] ŠEFČÍK, Vladimír, 2009. *Analýza rizik*. Zlín: Univerzita Tomáše Bati ve Zlíně. ISBN 9788073186968.

[10] KRULIŠ, Jiří, 2011. *Jak vítězit nad riziky: aktivní management rizik – nástroj řízení úspěšných firem*. Praha: Linde. ISBN 978-80-7201-835-2.

[11] *Nová vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti*, 2018. Online. Národní úřad pro kybernetickou a informační bezpečnost – Legislativa. Dostupné z: https://nukib.gov.cz/download/publikace/legislativa/vkb_82-2018sb.pdf. [cit. 2024-05-20].

[12] *Zákon o kybernetické bezpečnosti*, 2014. Online. Národní úřad pro kybernetickou a informační bezpečnost – Legislativa. Dostupné z: https://nukib.gov.cz/download/publikace/legislativa/181_2014_Sb.%20Platn%20znn.pdf. [cit. 2024-05-20].

[13] *Flex Gen4 2MP & 5MP PTZ*, c2024. Online. In: Flex Gen4 2MP & 5MP PTZ | Illustra. Dostupné z: https://illustracameras.com/wp-content/uploads/2023/04/FG4-PTZ-Combo-Image.jpg. [cit. 2024-05-20].

[14] *IoSmart Smart Card Readers and Cards*, c2020. Online. In: IoSmart Smart Card Readers and Cards. Dostupné z: https://www.kantech.com/ImagesDocDb/iosmart-card-reader_collage_p2_01_na_k.jpg. [cit. 2024-05-20].

[15] *Pro Gen4 Compact Camera*, c2024. Online. In: Pro Gen4 Compact Camera | Illustra. Dostupné z: https://illustracameras.com/wp-content/uploads/2024/01/Pro4-Compact-high-res-image-front-1.png. [cit. 2024-05-20].

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BOZP	bezpečnost a ochrana zdraví při práci
CIA	C-Confidentiality, I-Integrity, A-Availability
EPS	Elektronická požární signalizace
ESKV	Elektronický systém kontroly vstupu
GDPR	General Data Protection Regulation (Obecné nařízení o ochraně osobních údajů)
ICT	Information and Communication Technologies (Informační a komunikační technologie)
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OPPO	Obslužné pole požární ochrany
PZTS	Poplachové zabezpečovací a tísňové systémy
SHZ	Samočinná hasicí zařízení
SLA	Service-Level Agreement (Úroveň poskytovaných služeb)
TLP	traffic light protokol
UPS	Uninterruptible Power Supply (Nepřerušitelný zdroj napájení)
VoKB	Vyhláška o kybernetické bezpečnosti
VSS	Video Surveillance Systém (Kamerové dohledové systémy)
ZoKB	Zákon o kybernetické bezpečnosti

SEZNAM OBRÁZKŮ

SEZNAM TABULEK