Informační bezpečnost subjektu

Bc. Kamila Chlupová

Diplomová práce
2023

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav ochrany obyvatelstva

Akademický rok: 2022/2023

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Kamila Chlupová**
Osobní číslo:	**L21149**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Specializace:	**Ochrana obyvatelstva**
Forma studia:	**Kombinovaná**
Téma práce:	**Informační bezpečnost subjektu**

Zásady pro vypracování

1. Zpracujte teoretický vstup do dané problematiky.
2. Proveďte analýzu stávající informační bezpečnosti z hlediska fyzické bezpečnosti u vybraného subjektu.
3. V důsledku zjištěných informací navrhněte opatření na zlepšení současného stavu.
4. Ověřte navržená opatření u vybraného subjektu.

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

Seznam doporučené literatury:

1. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity.* Praha: CZ.NIC, z.s.p.o., 2019. ISBN 978-80-88168-31-7.
2. MCCARTHY, N.K. *The Computer Incident Response Planning Handbook.* United States of America: The McGraw-Hill Companies, 2012. ISBN 978-0-07-179039-0.
3. SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2019. ISBN 978-80-7380-765-8.

Další odborná literatura dle doporučení vedoucího diplomové práce.

Vedoucí diplomové práce: **Ing. Petr Svoboda, Ph.D.**
Ústav ochrany obyvatelstva

Datum zadání diplomové práce: **1. prosince 2022**
Termín odevzdání diplomové práce: **28. dubna 2023**

L.S.

doc. Ing. Zuzana Tučková, Ph.D.
děkanka

prof. Ing. Dušan Vičar, CSc.
ředitel ústavu

V Uherském Hradišti dne 2. prosince 2022

PROHLÁŠENÍ AUTORA
DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

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

Prohlašuji,

- že jsem na diplomové práci pracoval 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 obsahově totožné.

V Uherském Hradišti, dne: 28.4.2023

Jméno a příjmení studenta: Bc. Kamila Chlupová

.....
podpis studenta

ABSTRAKT

Předložená diplomová práce se zaměřuje na informační bezpečnost a fyzické zabezpečení vybraného subjektu. Teoretická část definuje základní terminologii, právní ukotvení a standardy informační bezpečnosti, vztah mezi informační a kybernetickou bezpečností, fyzickou bezpečnost a analýzu rizik. Praktická část obsahuje charakteristiku vybraného subjektu a sestavuje aktuální stav fyzického zabezpečení dle příslušné ISO normy, pomocí kterého jsou analyzovány nedostatky. Na základě vyhodnocení je zvoleno opatření pro zvýšení fyzické bezpečnosti, jehož proces je zaznamenán ve vytvořeném modelu. Konkrétní varianty jsou posouzeny pomocí multikriteriální analýzy. Návrh optimální možnosti obsahuje kalkulaci a posouzení vhodnosti odborníkem z praxe a provozovatelem subjektu.

Klíčová slova: analýza současného stavu, fyzická bezpečnost, informace, informační bezpečnost, ochranná opatření, zabezpečení.

ABSTRACT

The presented diploma thesis focuses on information security and physical security of the selected entity. The theoretical part defines the basic terminology, legal anchoring and standards of information security, the relationship between information and cyber security, physical security and risk analysis. The practical part contains the characteristics of the selected entity and compiles the current state of physical security according to the relevant ISO standard, with the help of which deficiencies are analyzed. Based on the evaluation, a measure to increase physical security is chosen, the process of which is recorded in the created model. Specific variants are assessed using multicriteria analysis. The proposal of the optimal option includes a calculation and assessment of suitability by a practitioner and operator of the entity.

Keywords: Analysis of the Current State, Physical Security, Information, Information Security, Protective Measures, Security.

Tímto bych ráda poděkovala vedoucímu mé diplomové práce panu Ing. Petru Svobodovi, Ph.D. za jeho čas věnovaný při vedení práce a za poskytnutí užitečných rad při zpracování diplomové práce. Dále bych chtěla poděkovat Janu Brehovému, provozovateli vybraného subjektu, a Bc. Martinu Filovi, odbornému pracovníkovi, za jejich vstřícnost a ochotu poskytnout mi potřebné informace.

Na závěr bych chtěla vyjádřit svoji vděčnost svým blízkým, kteří mě v průběhu celého studia neustále podporovali a nabízeli mi pomoc v jakékoliv situaci. Moji nejbližší mi dodávali velkou dávku motivace a inspirace, a bez jejich podpory bych nedokázala úspěšně dokončit tuto cestu.

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

OBSAH

ÚVOD

Téma, které je rok od roku více aktuální. To je informační bezpečnost subjektu. S rozvojem technologií v průběhu několika let se informace, v jakékoliv podobě, stávají velmi zranitelným prvkem. I přes to, že již několik let existují zákony na ochranu informací a dat, tak s rozvojem technologií a nových přístupů, jsou opatření určené k minimalizaci tohoto rizika stále více ohrožovány a napadány. Hrozby, které by mohly tyto faktory ovlivňovat, se nachází všude okolo nás. V důsledku toho je třeba stávající opatření inovovat tak, aby byla zajištěna adekvátní ochrana informačních aktiv v tomto stále se rozvíjejícím prostředí. Vzhledem k tomu, že prostředky jsou navrženy tak, aby způsobily škodlivé následky, je důležité rychle reagovat na aktuální situaci a zajistit nezbytná bezpečnostní opatření. K co nejúčinnější ochraně dat a informací je třeba včasně reagovat, upravovat nebo stanovovat nová ochranná opatření. Je tedy zásadní rychle se přizpůsobit aktuální situaci.

Informační bezpečnost vybraného subjektu je důležitý prvek zabezpečující ochranu informačních aktiv. Diplomová práce se bude zabývat jednou z těchto oblastí, a to konkrétně zajištěním bezpečnosti fyzické. Pro tuto práci byla vybrána střelnice HABRESTO ARMS s.r.o.

Práce se v části teoretické bude orientovat na vymezené oblasti, jež se týkají informační bezpečnosti. V praktické části diplomové práce bude uvedena charakteristika vybraného subjektu. Dále bude vymezeno aktuální fyzické zabezpečení, které bude sestaveno podle příslušné ISO normy. Na základě tohoto posouzení bude zpracována analýza zaměřující se na plynoucí nedostatky.

Po vyhodnocení všech analýz bude vybráno opatření, které je třeba zajistit pro zvýšení fyzické bezpečnosti vybraného subjektu. Pro identifikované opatření bude sestaven model prezentující proces konkrétního postupu, jenž napomůže při výběru vhodných variant. Tyto možnosti budou charakterizovány a následně bude pomocí multikriteriální analýzy zvolena ta nejoptimálnější. Konečný výběr jedné z variant bude také obsahovat kalkulaci finálního návrhu, jenž bude posouzen odborníkem z praxe a zhodnocen samotným provozovatelem střelnice.

CÍL PRÁCE A POUŽITÉ METODY

V této kapitole je uveden hlavní cíl diplomové práce, na který navazují vymezené dílčí cíle této práce. Obsažené informace v nich definují, čím se práce bude zabývat. Dále bude tato kapitola zahrnovat metody, jež si autorka stanovila a použila při zpracování diplomové práce.

Hlavní cíl diplomové práce

- Návrh opatření ke zvýšení úrovně informační bezpečnosti vybraného subjektu z hlediska fyzického zabezpečení.

Dílčí cíle diplomové práce

- Rešerše problematiky informační bezpečnosti subjektu.
- Posouzení shody stavu fyzické bezpečnosti subjektu s požadavky normy Systému řízení informační bezpečnosti („rodina“ norem 27000).
- Provedení SWOT analýz za účelem určení strategií zlepšení úrovně informační bezpečnosti vnitřního a vnějšího prostředí z hlediska fyzické bezpečnosti.
- Kalkulace návrhu opatření ke zvýšení úrovně informační bezpečnosti vybraného subjektu z hlediska fyzického zabezpečení.
- Ověření navržených opatření.

Použité metody

- Sběr dat a informací – metoda byla uplatněna při zpracování teoretické části práce a následně také v praktické části, pomocí níž byly získávány informace o vybraném subjektu.
- Pozorování – pro popis současného stavu fyzického zabezpečení subjektu byla využita metoda pozorování.
- Analýza – metoda byla aplikována v praktické části diplomové práce k posouzení aktuálního fyzického zabezpečení. Pomocí kvantitativní SWOT analýzy byla identifikována vhodná strategie vnějšího a vnitřního prostředí subjektu. Ohodnocení možných variant bylo provedeno pomocí multikriteriální analýzy.
- Syntéza – metoda byla využita k integraci a vyhodnocení výsledků z předchozích analýz.

- Modelování – metoda byla využita pro tvorbu modelu přístupového diagramu, který vizualizuje a optimalizuje řízený proces přístupu osob.
- Komparace – bylo využito v praktické části diplomové práce při porovnávání vlastností u vybraných zařízení.
- Indukce – byla využita při posuzování aktuálního stavu fyzické bezpečnosti.
- Dedukce – byla využita při vyhodnocování závěrů ze zpracovaných analýz.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ TERMINOLOGIE

Pro pochopení a porozumění popisovaného tématu je nutné vymezit základní pojmy a termíny týkající se informační bezpečnosti. Samotná bezpečnost informací je obsažena v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, která tuto bezpečnost definuje jako zajištění dat a informací z hlediska důvěrnosti, integrity a dostupnosti. (Česko, 2014)

Informační bezpečnost je součástí bezpečnostního systému organizace, pod kterou spadá také bezpečnost informatická obsahující informační systém organizace, zpravidla automatizovaný. Bezpečnost informací je však určena k ochraně jakýchkoliv údajů, informací či dat organizace ve všech formách. Je tedy povinna zajistit ochranu i listinných dokumentů v podobě zápisů z jednání, poznámek, výkresů, obrázků, vnitropodnikové pošty, zásilek, zpráv apod. Do této bezpečnosti spadají také veškeré přenosy dat a informací za pomocí přenosů poštovních, osobních, telefonických, datových nebo také faxových. (Porada, 2019)

K tomu, aby mohla být zajištěna bezpečnost informací, jsou potřeba převážně potřebná data a informace. Za **data**, která jsou označována také jako údaje, lze považovat skutečnosti dosažené pozorováním, čtením, měřením, vážením, kreslením apod. Jedná se tedy o výstižnost určitých myšlenek a skutečností, které mohou být přenášeny či dále zpracovávány a jejich podoba je předepsaná. Může se ale také jednat o objektivní a sledovatelná fakta uložená na nějakém médiu, které je možno předávat. Data, jsou také považována za zkratkovitě profesionální označení vyznačující čísla, zvuky, obrazy nebo třeba vybraný text. Data, která jsou ukládána v souborech, jsou označována jako databáze či datové zdroje, které potom mohou tvořit informaci, avšak všechna data se nutně nemusejí stát informací. Aby se data stala informací, musejí přinášet potřebné osobě něco nového a objektivního, a proto je tedy můžeme označovat jako základní materiál pro informace. (Požár, 2005)

Každá **informace** je tedy tvořená ze zpracovaných dat. Informace vycházejí z odrážené reality v aktuálním okamžiku, a proto tedy není možné je měnit. Pouze pomocí dat lze získávat další poznatky o realitě, avšak v jiném časovém úseku. Informace však nemá jednotné vyjádření, protože je v různých oborech chápána několika způsoby. Obecně lze však definovat informaci jako zprávu popisující určité skutečnosti, které se právě dějí a pro příjemce jsou do té doby neznámé. Tato zpráva se v běžném životě může člověku

promítnout v kterémkoliv multimédiu či při rozhovoru s jinou osobou. V důsledku získání těchto informací jsou lidé seznamováni a obeznámeni s fakty a dokáží se tak lépe orientovat ve společenském prostředí. (Požár, 2005)

Informace jako taková se nachází i v několika zákonech. V zákoně č.106/1999 Sb., o svobodném přístupu k informacím (Česko, 1999) v §3 odst.3, ji lze označit za *„jakýkoliv obsah nebo jeho část v jakékoliv podobě, zaznamenaný na jakémkoliv nosiči, zejména obsah písemného záznamu na listině, záznamu uloženého v elektronické podobě nebo záznamu zvukového, obrazového nebo audiovizuálního.“*

Zákon č. 101/2000 Sb., o ochraně osobních údajů (Česko, 2000) tento pojem uvádí pod § 4 jako: *„Informace, které se vztahují k určité osobě, jsou osobními údaji.“* Již z těchto dvou zákonů je patrná rozdílnost ve vymezení pojmu informace, která se liší dle toho, v jakém oboru a v jakém zájmu je s ní nakládáno.

Pro účely této práce je důležité objasnit pojem **informační systém** označovaný zkratkou IS. Informační systém je založen na propojení vazeb a vzájemných vztahů, které obsahují jednotlivé prvky. Tyto prvky jsou tvořeny lidmi, hardwarem, programy, normami, technologiemi apod. (Požár, 2005)

Jedná se tedy o funkční celek, jehož úkolem je zaručit bezpečné shromažďování, uchovávání, předávání, zpracovávání a zpřístupňování informací a dat, které jsou v tomto IS obsaženy. Součásti informačního systému jsou i informační a komunikační technologie, které slouží k přenosu a zpracování informací, jež jsou označovány za výpočetní techniku obsahující také odpovídající programové vybavení. (Doucek, Konečný a Novák, 2019)

Jako další pojem, který je nutno vymezit, je pojem **bezpečnost**. Tento pojem je v oboru informační bezpečnosti označován jako vlastnost určitého objektu nebo subjektu vyjadřující danou míru či stupeň ochrany proti vnějším či vnitřním hrozbám a škodám. (Požár, 2005)

Zajištění bezpečnosti v dnešní době již není jen v kompetenci státu, i když stát zde pořád hraje primární roli, ale jde i o právnické a fyzické osoby, na které jsou kladeny mnohem větší bezpečnostní požadavky související se zabezpečením jejich aktivit před útoky. Z hlediska bezpečnosti je také nutné vymezit základní otázky týkající se bezpečnosti. Tyto otázky se týkají subjektu, který má být zabezpečen, chráněných zájmů daného subjektu, před jakou hrozbou mají být chráněny a dále také jaké prostředky budou použity k zabezpečení chráněných zájmů. Osoby, podílející se na bezpečnosti, jakož i stát, se snaží

dosáhnout stavu „absolutního bezpečí“, který však není možné zajistit. Vždy totiž bude existovat riziko či hrozba, jež mohla zůstat opomenutá a v rámci bezpečnosti tak nezajištěná. Hlavním smyslem stavu bezpečí však není postihnout všechna reálná či méně nereálná rizika nebo nepředvídatelná či předvídatelná rizika, protože tím by naopak mohl vzniknout systém opatření popírající bezpečnost z hlediska aplikace a implementace. (Kolouch a Bašta, 2019)

Bezpečnost je v rámci informačního systému pojímána jako soubor snažící se co nejvíce zamezit možným škodám, ztrátám či zničením podstatných prvků, tedy informačních aktiv, která jsou pro daný subjekt klíčová. Toto zabezpečení se děje pomocí tzv. triády CIA, která je již výše zmíněná zákonem o kybernetické bezpečnosti. Jedná se tedy o koncept zajišťující důvěrnost (Confidentality), integritu (Integrity) a dostupnost (Availability). (Česko, 2014)

Důvěrností je vymezena takzvaná oprávněnost k určité informaci jen takovým uživatelům či technologiím, které k této informaci mají umožněn přístup. Při zajištění principu důvěrnosti se tedy k těmto informacím dostane pouze takový uživatel, který k nim má umožněn přístup či manipulování s nimi. **Integrita** je označována jako zajištění správnosti či úplnosti veškerých informací. Pokud je integrita správně nastavena, je zaručena její vysoká ochrana před nežádoucí změnou dat, která může mít v informačním systému podobu např. škodlivého kódu či viru. Integrita je tedy prevence a ochrana před nežádoucí modifikací dat a informací, jež je důležitá pro zachování jejich správnosti. **Dostupnost**, již z podstaty slova, vyjadřuje schopnost systému zajistit požadovanému subjektu danou informaci včas. Z hlediska dostupnosti je tedy důležitá kontrola dostupnosti určených dat a informací, které jsou poskytovány pověřeným uživatelům. O to, aby bylo garantováno, že určitá data a informace budou v případě potřeby dostupná, je postaráno v rámci správného nastavení zabezpečujícího mechanismu informačního systému. (Chapple, Stewart a Gibson, 2018)

Využívání principů triády CIA, která se řadí mezi nejpoužívanější a nejznámější triádu kybernetické bezpečnosti, bez využití další principů a metod zajišťujících komplexní bezpečnost podniku, je však již v dnešní době považováno za nedostačující, a právě proto bývá vztahována pouze k bezpečnosti zajišťující ochranu informací. (Kolouch a Bašta, 2019)

Kybernetickou bezpečností se myslí soubor organizačních, technických, právních či vzdělávacích prostředků, jejichž cílem je zajistit ochranu prvků informačních

a komunikačních technologií, dat, informací, uživatelů, aplikací, jakož i celých počítačových systémů. V rámci využití těchto počítačových systémů a dalších služeb je schopna zabezpečit určenou organizaci před kybernetickou hrozbou či útokem. V důsledku toho také řeší následky těchto incidentů a zajišťuje také obnovení provozuschopnosti všech informačních služeb a systémů souvisejících s informační bezpečností. (Kolouch a Bašta, 2019)

Pojmem **hrozba** se označuje aktivita, osoba, událost nebo síla, která může negativně působit na aktiva. Negativní působení lze vymezit jako poškození, ztráta hodnoty či důvěry, která může způsobit škodu, ale i zničení organizace jako celku. Škoda způsobená hrozbou na určité aktivum bývá označována jako dopad hrozby, do nějž jsou zahrnuty náklady spojené se znovuobnovením poškozeného aktiva či s odstraněním následků v daném subjektu. (Smejkal, Sokol a Kodl, 2019)

Hrozby pocházejí z vnějšku, ale i zevnitř organizace. Lze je rozdělit na hrozby:

- Přírodní a fyzické – jedná se o požáry, přerušení elektrického proudu v důsledku silného větru, povodně, tornáda apod.
- Technologické a technické – zahrnující poruchy způsobené programy, nosiči dat, počítači, technologickými prostředky apod.
- Lidské – rozdělující se na:
    - Neúmyslné – způsobené lidskou nevědomostí či neplněním povinností.
    - Úmyslné – které se rozdělují dle působení na:
        - Vnitřní – způsobené chamtivými a zlomyslnými zaměstnanci, hosty či návštěvníky dané organizace za účelem poškození.
        - Vnější – jedná se hackery, teroristy či konkurenční společnost. (Doucek, Konečný a Novák, 2019)

Aktivum vychází z hmotných i nehmotných statků a jedná se o vše, co má pro majitele organizace jistou hodnotu. Mezi hmotnými aktivy jsou zahrnuty veškeré technické prostředky. U nehmotných aktiv se jedná o pracovní postupy, služby, software organizace, data a další. (Doucek, Konečný a Novák, 2019)

Ve vyhlášce č. 82/2018 Sb., o kybernetické bezpečnosti jsou v § 2 rozděleny aktiva na primární, podpůrná a technická přičemž:

- Primární aktivum je charakterizováno jako služba poskytovaná v rámci informačního nebo komunikačního systému.
- Podpůrné aktivum zahrnuje technické aktivum, zaměstnance a dodavatele, kteří se zúčastňují provozu, rozvoje, správy nebo bezpečnosti v rámci informačního a komunikačního systému.
- Technickým aktivem, je označováno technické vybavení, programové vybavení, komunikační prostředky či objekty, v kterých se toto aktivum nachází. (Česko, 2018)

Riziko také nemá jednoznačnou definici, která by ho vymezovala. V terminologickém slovníku Ministerstva vnitra České republiky (2016) je uvedeno definice rizika jako *„možnost, že s určitou pravděpodobností vznikne událost, kterou považujeme z bezpečnostního hlediska za nežádoucí.“* Jedná se tedy o situace, které se odchylují od skutečných a očekávaných výsledků, nebezpečí plynoucí ze špatného rozhodnutí, pravděpodobnost vzniknutí ztráty či nezdaru nebo také tzv. vznik čistého rizika, tedy výskyt negativního odchýlení od požadovaného cíle. (Smejkal, Sokol a Kodl, 2019)

Za vznik rizika se považuje společné působení hrozby a aktiva. Tímto vzájemným působením vzniká situace, která později může způsobit škodu. Riziko vyjadřuje velikost míry ohrožení každého aktiva či míry možného působícího nebezpečí. Úroveň rizika se však stanovuje ohodnocením aktiva, které může způsobit škodu jak samotnému vlastníkovi, tak i celé organizaci. Z tohoto ohodnocení také vyplývá zranitelnost aktiv nebo také samotná úroveň hrozby. (Porada, 2019)

Zranitelnost je pojem spojený s vlastností aktiva. Jejím vyjádřením je určeno, jak moc může být narušeno aktivum v případě působení hrozby. Označuje se za určitou slabinu či nedostatek aktiva, či jeho části, kterých by mohla využít daná hrozba ke vzniku nežádoucí události. (Porada, 2019)

Zranitelností je tedy myšleno slabé místo aktiv či opatření, kterých může potencionální hrozba využít. Je rozdělována na zranitelnost *„fyzickou, technických a programových prostředků, nosičů dat, elektromagnetických zařízení, komunikačních systémů a kabelových rozvodů a také zranitelnost personální.“* (Doucek, Konečný a Novák, 2019, str. 25)

Opatření je určitý postup, procedura, proces či jakýkoliv technický prostředek, který byl vybrán k tomu, aby zmírnil či eliminoval působící hrozbu, snížil odhalenou zranitelnost

anebo snížil samotné riziko, které s sebou přináší dopady. Organizace či subjekty se snaží vždy navrhnout taková opatření, která povedou k prevenci rizik nebo při vzniku rizika k rychlému překonání toho stavu, který způsobuje dopady označované za škody. (Smejkal, Sokol a Kodl, 2019)

Opatření se rozděluje podle charakteru na:

- Administrativní – vedoucí k vytvoření směrnic v organizacích, týkajících se např. zajištění zálohy či archivace dat.
- Fyzické – využitím např. zámků, trezorů pro ukládání důležitých dokumentů nebo čipových karet, které umožňují přístup do režimových prostorů.
- Technické a technologické – týkající se autentizace a autorizace sloužící k možnosti užívání informačního systému organizace ve způsobu hesel. (Doucek, Konečný a Novák, 2019)

Pokud se opatření týká zabezpečení cíle subjektu či organizace, je možno ho členit na prevenční, detekční a korekční. Prevenční a detekční opatření je navrženo k ochraně před vznikem hrozby a jedná se o minimalizaci a včasné odhalení případných hrozeb či nebezpečí. (Doucek, Konečný a Novák, 2019)

Dopad Ministerstvo vnitra (2016, str. 14) v terminologickém slovníku vymezuje jako *„následek určitého činu nebo události.“* Dopad, způsobený incidentem bezpečnosti informací, působí obvykle jen na část aktiv nebo také na více aktiv zároveň. Účinek dopadu je rozdělován na okamžitý (provozní) nebo budoucí (obchodní). Součástí budoucího účinku jsou také finanční a tržní následky. Okamžitý dopad je rozdělován na další dvě skupiny, a to na přímý nebo nepřímý dopad. Hodnota, vyplývající z prvního posuzování dopadu je obvykle vysoká, ale při opakovaném měření, kterému předchází stanovení ochranných opatření, se ve většině případů snižuje. (ČSN ISO/IEC 27005, 2019)

2 PRÁVNÍ RÁMEC A STANDARDY INFORMAČNÍ BEZPEČNOSTI

Pro účely této diplomové práce budou v této kapitole vymezeny základní zákony, normy a směrnice zajišťující informační bezpečnost. Tyto normativní předpisy a dokumenty byly vytvořeny za účelem nutné ochrany a zabezpečování potřebných informací u všech jednotlivců, ale i organizací. Je tedy důležité, aby tyto skupiny zákony znaly, správně jejich obsah aplikovaly či používaly, a hlavně také aby jich nezneužívaly ve svůj prospěch.

Zákon č. 2/1993 Sb., Listina základních práv a svobod

Listina základních práv a svobod je určena pro všechny bez rozdílu. Vymezuje právo na život, osobní svobodu, zachování lidské důstojnosti, svobodu pohybu, pobytu, náboženského vyznání, vlastnictví majetku a další. Z hlediska informační bezpečnosti vymezuje právo na informace, kde stanovuje nepřístupnost cenzury a svobodné vyhledávání, přijímání či rozšiřování informací bez omezení. Dále také poskytuje ochranu před zasahováním do soukromého či rodinného života a s tím související ochranu zabývající se neoprávněným shromažďováním, zveřejňováním či jiným zneužitím údajů osob. Bezpečnost informací je zde zaručena zákazem porušení listovního tajemství či jiných záznamů a písemností, které jsou součástí soukromí osoby nebo se zasílají prostřednictvím pošty. V tomto duchu je zachována také bezpečnost zpráv zasílaných pomocí mobilního telefonu, telegrafu či jiných technických prostředků. (Česko, 1993)

Zákon č. 89/2012 Sb., občanský zákoník

Občanský zákoník, v souladu s předchozím zákonem, stanovuje právo na ochranu života a zdraví, a také cti, důstojnosti a soukromí, s čímž také souvisí ochrana informací jako taková. V občanském zákoníku je stanovena ochrana, zabývající se zneužitím a prozrazením důvěrných údajů či sdělení bez právního důvodu, která se poskytuje při uzavírání smluv a dohod. (Česko, 2012)

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

Zákon se použije při zpracovávání osobních údajů, které stanovuje nařízení Evropského parlamentu a Rady EU 2016/679 ze dne 27. dubna 2016. Jedná se o údaje, které jsou součástí evidencí či zpracování osobních údajů o fyzické osobě, u které se nejedná o domácí či výlučně osobní činnosti. Tyto údaje jsou v rámci zákona nezbytné pro splnění požadovaných povinností stanovených oprávněným správcem či při úkolu, který je prováděn při výkonu veřejné moci. Stanovuje také způsobilost dítěte pro udělení souhlasu

s uchováním osobních údajů, informační povinnost spojenou se zpracováním osobních údajů, mlčenlivost osob pracujících s těmito údaji, ochranu zdroje a obsahu informací nebo také informování o opravě, výmazu a omezení zpracování. Mimo to také stanovuje požadované zabezpečení těchto informací a stanovuje také výši přestupků při porušení tohoto zákona. (Česko, 2019)

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

Tento zákon stanovuje, jaké informace se zařazují do utajovaných informací, přičemž utajovanou informaci definuje jako informaci v jakékoliv podobě, která je zaznamenána na jakémkoliv nosiči, jejímž vyzrazením či zneužitím by mohla způsobit újmu České republice nebo také informace nevhodná v souladu s tímto zájmem. Klasifikuje stupně utajovaných informací na příště tajné, tajné, důvěrné a vyhrazené. V souladu s tímto vymezením definuje zajištění požadované ochrany utajovaných informací pomocí:

- Personální bezpečnosti – kterou tvoří vybrané fyzické osoby mající přístup k těmto informacím, jakož i k ověřování podmínek pro jejich přístup, jejich výchovu či ochranu.
- Průmyslové bezpečnosti – zabývající se systémem opatření, který zajišťuje podmínky pro přístup podnikateli k utajovaným informacím a také kontroluje nakládání s takovou informací.
- Administrativní bezpečnosti – jedná se o systém opatření při jakémkoliv manipulováním s touto informací, do které spadá příjem, evidence, zpracování, odesílání, přeprava, přenášení, ukládání, skartace, archivace apod.
- Fyzické bezpečnosti – která je určena k zabránění či ztížení přístupu neoprávněnému uživateli k utajovaným informacím.
- Bezpečnosti informační nebo pomocí komunikačních systémů – ta se zabývá zajištěním jednak důvěrnosti, integrity a dostupnosti dané utajované informace, ale také odpovědností správ a uživatelů systému v rámci jejich činností.
- Kryptografické bezpečnosti – označovanou za systém opatření zahrnující kryptografické materiály a metody sloužící k zajištění ochrany při zpracování, přenosu nebo ukládání utajovaných informací. (Česko, 2005)

Dále jsou zde uvedeny další požadavky na ochranu utajovaných informací, jakož i vymezení citlivých činností spolu s podmínkami, které souvisejí s jejím výkonem, včetně výkonu státní správy. (Česko, 2005)

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti

Tento zákon se zabývá úpravou práv a povinností osob a jejich působností a pravomocemi orgánů veřejné moci v oblasti kybernetické bezpečnosti, zpracovává příslušný předpis EU a upravuje zajištění bezpečnostních sítí týkajících se elektronických komunikací a informačních systémů. Jeho působnost však nezahrnuje informační nebo komunikační systémy, které obsahují utajované informace. Zákon dále stanovuje bezpečnostní opatření v souvislosti s kybernetickou bezpečností, které zajišťuje pomocí organizačních a technických opatřeních a stanovuje práva a povinnosti správce informačního systému, jakož i všech zúčastněných osob. Tento zákon také vymezuje kybernetickou bezpečnostní událost jako možné způsobení narušení bezpečnosti informací v rámci IS nebo i narušení bezpečnosti služeb či integrity sítí elektronických komunikací, v důsledku čehož poté nastává kybernetický bezpečnostní incident. Dále také vymezuje povinnosti spojené s hlášením, evidencí, varováním či stanovením opatření v souvislosti se vznikem tohoto incidentu. Zákon také vymezuje činnosti dohledových pracovišť, mezi které patří národní CERT a vládní CERT. (Česko, 2014)

Tato dohledová pracoviště jsou určeny k přijímání, evidenci a uchovávání kontaktních údajů od orgánů a osob, které jsou v tomto zákoně vymezeny pod § 3 písm. a), b) a h) a údaje vyhodnocuje. Dále pracoviště plní funkci kontaktního místa pro tyto orgány a osoby, poskytuje jim metodickou podporu a pomoc. V případě vzniku kybernetického bezpečnostního incidentu předává údaje o incidentech příslušnému Úřadu. V neposlední řadě také národní i vládní CERT provádějí hodnocení zranitelností v oblasti kybernetické bezpečnosti. (Kolouch a Bašta, 2019)

Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti

Tato vyhláška je zpracována na základě předpisu EU, který byl vydaný Evropským parlamentem a Radou EU dne 6. července 2016, a má tak napomoci k zajištění vysoké společenské úrovně bezpečnosti sítí a IS v Unii. Je určena pro informační a komunikační systémy, kterých využívá poskytovatel digitálních služeb a zabývá se vymezením bezpečnostní dokumentace, bezpečnostním opatřením, kategoriemi, typy a hodnocením při určování významnosti kybernetického bezpečnostního incidentu, reaktivním opatřením

včetně výsledků, kontaktními údaji pro oznámení a také samotnou likvidací dat, provozních údajů a stanovením formy pro likvidaci. Vyhláška obsahuje bezpečnostní opatření, v rámci kterých stanovuje práva a odpovědnosti povinným osobám, které se týkají organizačního a technického zajištění bezpečnosti. Toto zajištění bezpečnosti je rozděleno pod příslušné paragrafy, které se rozdělují dle příslušných odvětví. Přílohu této vyhlášky pak tvoří stupnice, pomocí kterých jsou hodnocena aktiva a rizika. Tyto stupnice jsou rozděleny na jednotlivé úrovně důvěrnosti jako nízká, střední, vysoká a kritická. Dále jsou v příloze vymezeny možné zranitelnosti a hrozby, které mohou nastat u informačního a komunikačního systému. Vyhláška také obsahuje příklady týkající se likvidace aktiv dle úrovně důvěrnosti. (Česko, 2018)

Skupina norem ISO 27000

Různé smlouvy a stanovené předpisy od oprávněných organizací v rámci těchto prostředků vyžadují, aby byla splněna ochrana důvěrných informací pomocí přijetí standardů, ale již přesně nespecifikují, jak tohoto dosáhnout. Právě díky vzniku řady některých norem či nástrojů vedoucím ke komplexnímu zvládnutí otázek týkající se bezpečnostní praxe, lze subjektům pomoci při zajišťování potřebné oblasti či při zavádění požadovaných procesů v organizaci a to tím, že využijí těchto norem, které nejsou závazné. (McCarthy, 2012)

Mezinárodní organizace pro normalizace (ISO) zřizuje svoji podkomisi označovanou jako *„JTC1/SC27 – bezpečnostní techniky IT“*, která je odpovědná za normalizaci bezpečnosti informací, a to tak, že bude vydávat provázané normy a přístupy, které budou stanovovat pravidla týkající se systémů řízení bezpečnosti informací. Tato odpovědnost byla projevena organizací ISO v roce 2015 vydáním nové rodiny norem ISO 27000, která se zaměřuje právě na bezpečnost informací. (Doucek, Konečný a Novák, 2019)

Tato řada norem je také označována ve spojení „best practices“ a její aplikování a dodržování v organizaci hraje velký význam při zajišťování bezpečnosti informačních a komunikačních systémů. Normy obsahují řadu doporučení, postupů a principů, které se týkají informační bezpečnosti a jsou mezinárodně uznávané. (Porada, 2019)

Tyto evropské a mezinárodní normy byly převzaty do českého souboru norem a v praxi nesou označení českých technických norem uvedených pod zkratkou ČSN, přičemž za touto zkratkou následuje identifikátor pro přejímaný dokument. (Peková, 2020)

Mezi základ skupiny ISO norem, týkající se bezpečnosti informací, lze vymezit soubor norem dělící se na:

- ČSN EN ISO/IEC 27000 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník: norma obsahuje systémy řízení bezpečnosti informací (ISMS) a vymezení související terminologie a dále uvádí normy, které specifikují požadavky, popisují obecné směrnice a směrnice specifické pro jednotlivá odvětví. (ČSN EN ISO/IEC 27000, 2020)
- ČSN EN ISO/IEC 27001 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky: norma upřesňuje požadavky vedoucí k neustálému zlepšování systému řízení bezpečnosti informací, kterými jsou stanovení kontextu a vůdčích rolí, plánování, podpora, provozování, hodnocení výkonnosti, stanovování nápravných opatření či stanovení požadavků na posouzení a ošetření rizik týkajících se bezpečnosti informací. (ČSN EN ISO/IEC 27001, 2014)
- ČSN EN ISO/IEC 27002 Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací: tato norma slouží organizacím jako postup, pomocí kterého se mohou řídit při zavádění systému řízení bezpečnosti informací, vytváření směrnic nebo také k implementování úkonů, pomocí kterých budou zavedena ochranná opatření, přičemž charakter normy je pouze doporučující. (ČSN EN ISO/IEC 27002, 2014)
- ČSN ISO/IEC 27003 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Pokyny: v normě jsou uvedeny podrobné pokyny k ISMS, které rozvíjejí další doporučení, možnosti a oprávnění, přičemž samotný základ těchto pokynů vychází z normy ISO/IEC 27001. (ČSN ISO/IEC 27003, 2018)
- ČSN ISO/IEC 27004 Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Monitorování, měření, analýza a hodnocení: obsahem normy je směrnice, která má organizaci napomoci ke splnění požadavků vycházejících z normy ISO/IEC 27001, a zároveň tak napomáhá při hodnocení výkonnosti bezpečnosti informací a také k efektivnímu ISMS. (ČSN ISO/IEC 27004, 2018)

- ČSN ISO/IEC 27005 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací: norma se zabývá řízením rizik bezpečnosti informací v organizaci a uvádí metody, pomocí kterých se identifikují aktiva, hrozby a zranitelnost, přičemž však nespecifikuje nutnost použití této metody, nýbrž je na organizaci, jaký postup si stanoví. (ČSN ISO/IEC 27005, 2019)
- ČSNEN ISO/IEC27006 Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací: norma upřesňuje nároky včetně doporučení pro orgány, které se zabývají auditem a certifikací ISMS a má jim tak napomoci k efektivnímu užití a harmonizaci s ostatními příslušnými normami, přičemž ji lze aplikovat i pro interní hodnocení organizací či jiných auditních procesech. (ČSN EN ISO/IEC 27006, 2021)
- ČSN ISO/IEC 27007Informační technologie, kybernetická bezpečnost a ochrana soukromí – Směrnice pro audit systémů řízení bezpečnosti informací: hlavním předmětem normy je poskytnou informace a pokyny auditorům a organizacím provádějící interní audit ISMS (první stranou) nebo externí audit ISMS (druhou stranou) dle jejich potřebného rozsahu, předmětu a složitosti. (ČSN ISO/IEC 27007, 2020)

V roce 2023 také proběhne aktualizace normy ČSN EN ISO/IEC 27002, která bude platná od 1. května 2023 a její nový název bude znít: Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí – Opatření informační bezpečnosti. (TECHNOR, © 2020-2022)

Dále se také chystá nová verze normy ČSN EN ISO/IEC 27005, kde výše zmíněná má platnost do konce ledna 2023. Její aktualizované vydání bude uvedeno pod názvem: Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí – Pokyny pro řízení rizik bezpečnosti informací. Hlavními změnami bude sjednocení s dalšími nově aktualizovanými normami, přizpůsobení obsahu ostatním normám, sjednocení všech příloh do jedné nebo také zavedení nového konceptu týkajícího se možných scénářů rizik. (Information security, cybersecurity and privacy protection, © 2022)

Směrnice NIS 1

Směrnice NIS 1 byla přijata Evropským parlamentem a Radou EU dne 6. července 2016 a její celý název zní: *„Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne*

6. července 2016, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.“ V ČR se tato směrnice zapracovala do českého právního řádu v roce 2018. (Kučínský, 2016)

Pro její dlouhý a nesnadno zapamatovatelný název vznikla používaná zkratka NIS nebo také Směrnice NIS, která je označením celého anglického názvu *„The Directive on security of network and information systems.“* Členské státy EU od vydání této směrnice měly za úkol vybudovat národní CSIRT (Computer Security Incident Response Team), který v ČR zajišťuje společnost CZ.NIC. Jak již také bylo uvedeno výše, ČR také disponuje CERTem (Computer Emergency Response Team) ve formě NÚKIBu, kde je vzájemná propojenost těchto institucí a také spolupráce s agenturou ENISA. (Kresa, 2018)

ENISA je Agentura EU pro kybernetickou bezpečnost, která má za úkol zajistit kybernetickou bezpečnost v celé Evropě pomocí vysoké společenské úrovně. Vznikla v roce 2014 a přispívá také v oblasti kybernetické politiky EU a spolupráce v rámci členských států a orgánů EU. Jejím hlavním cílem je tedy na základě šíření znalostí a posilováním důvěry propojit ekonomiku a odolnost infrastruktury EU a pomocí těchto nástrojů zajistit digitální bezpečnost v celé Evropě. ENISA upozorňuje na to, že právě kyberzločinci jsou bezpodmínečnou hrozbou pro vnitřní bezpečnost EU a on-line občany. Tuto skutečnost připomínají na pandemii COVID-19, která byla pro zločince rájem pro jejich lovení obětí, což bylo zapříčiněno větší návštěvností osob na internetu. Tyto osoby v rámci pandemie využívaly internet k udržení jednak pracovních vztahů, ale i osobních. Kyberzločinci tak zneužívali převážně podniky s elektronickým obchodem a elektronickými platbami, a také systémy v oblasti zdravotní péče. (ENISA, 2005)

Duračinská (2016) vymezuje směrnici NIS ve svém článku jako Network Information Security a považuje ji za dokument, který dokáže ucelit zajištění bezpečnosti napříč všemi členskými státy EU. Směrnice NIS má jak organizační, tak legislativní charakter. Jedním z důležitých kroků je přijetí strategie a aplikace do strategie národní. Ta už by měla obsahovat konkrétní strategické cíle včetně opatření k zajištění bezpečnosti sítí a IS, které budou vykonávány daným členským státem. Dále tato směrnice vytváří povinnost na zřízení centrálního orgánu, který bude řídit kybernetickou bezpečnost i v rámci přeshraniční spolupráce za pomoci odpovídajících technických, finančních, ale i lidských zdrojů. Směrnice také uvádí skupiny provozovatelů dotčených jejím zavedením v rámci organizace a jejím následný dodržováním. Tyto skupiny rozděluje na provozovatele základních služeb a provozovatele elektronických služeb. (Duračinská, 2016)

Povinnosti těchto skupin jsou v každé kategorii odlišné. Za provozovatele základních služeb se dle této směrnice míní všechny subjekty, které poskytují klíčovou službu spojenou s ekonomickou či společenskou činností a narušení těchto služeb na sítích nebo informačních systémech by při vzniku incidentu mohlo významně omezit jejich funkčnost. Poskytovatelé digitálních služeb mají z hlediska této směrnice méně povinností, které musí plnit. Uplatňuje se u nich, oproti poskytovatelům základních služeb, tzv. zásada harmonizace, která stanovuje uložení povinností jen v míře, kterou vymezuje směrnice NIS. Jedná se o skupinu, která poskytuje služby týkající se on-line tržiště, internetového vyhledávače nebo cloud computingu, který směrnice vymezuje jako *„službu umožňující přístup k rozšiřitelnému a přizpůsobitelnému úložišti výpočetních zdrojů, které lze sdílet.“* Z této skupiny byly také vyřazeny malé podniky a mikropodniky. (Kučínský, 2016)

Směrnice NIS2

Tato směrnice má být zdokonalením předchozí směrnice NIS 1, která bude ještě více prohlubovat zabezpečení týkající se kybernetické bezpečnosti. Oficiálně byla tato směrnice NIS2 publikována v Úředním věstníku EU na konci roku 2022. Do poloviny ledna 2023 pak musel být její text přeložen do národního práva, kde je také stanovena lhůta na 21 měsíců, během které je stát povinen její obsah začlenit do národní legislativy, pomocí změny aktuálního zákona o kybernetické bezpečnosti. Dle těchto informací by nová směrnice měla začít platit ke konci roku 2024, přičemž od tohoto okamžiku by mělo vstoupit v platnost také plnění povinností od subjektů dosud nezačleněných do těchto směrnic. (NÚKIB, 2023 a)

Důvodem vzniku nové směrnice byla bezpodmínečně také aktuální situace ve světě týkající se digitalizace, která svým rychlým rozvojem umožňuje vzniku nových hrozeb v kyberprostoru. Škody, které by v důsledku vzniklých hrozeb mohly působit na jednotlivé podniky, mohou mít finanční charakter nebo způsobují dlouhodobou nefunkčnost systémů společnosti. Zároveň se očekává, že takovéto útoky budou stále častější, a proto byla nutnost vytvořit na úrovni organizacích nové nástroje a zdokonalit ty stávající. Toto zdokonalení povede ke komplexnímu zajištění bezpečnosti globálního a otevřeného internetu. Nová směrnice se bude týkat jak státních, tak i soukromých subjektů, které budou zařazeny do skupin dle oborů. Právě u soukromých firem se rapidně zvýší počet subjektů, které budou povinny tuto směrnici začlenit do své organizace, což může být poměrně problematické, protože spousta takovýchto subjektů dosud nemá ve svém

podniku kybernetickou bezpečnost zahrnutou. Předběžný počet, kterých by se povinná směrnice měla dotýkat, je okolo 6000 firem. (Chvalkovská, 2022)

Směrnice tak bude muset být aplikována u organizací, které mají více než 50 zaměstnanců v rámci propojených podniků nebo také u subjektů převyšující roční obrat nebo bilanční sumu v hodnotě 10 milionů eur. Mimo to si mohou členské státy určit i další významné organizace, které do tohoto výčtu nespadají. Tato směrnice je v rámci určení dotčených organizací také propojena se směrnicí CERT, která se zaměřuje na odolnost kritických entit, tzn. kdo do této směrnice spadá, tak je automaticky zařazen i do směrnice NIS2. (Thein.eu, 2022)

Sasková (2022), ve své konferenci týkající se představení nové směrnice NIS 2, mimo jiné také uvádí kritéria, za kterých budou určovány ostatní organizace nesplňující základní podmínky. Pomocí národního řízení rizik tak může stát rozhodnout o dalších subjektech, které budou podléhat regulaci dle doplňujících kritérií. Tyto doplňující kritéria vymezují společnosti, které jsou:

- *„Jediným poskytovatelem služby, která je nezbytná v členském státě ze sociálního nebo ekonomického hlediska.*
- *Poskytovatelem služby, jejíž narušení by mohlo mít významný dopad na veřejnou bezpečnost nebo zdraví osob.*
- *Poskytovatelem služby, jejíž narušení by mohlo vyvolat významné riziko, zejména s přeshraničním dopadem.“* (Sasková, 2022)

Mimo výše vymezených pokut, které organizacím hrozí, do sankcí také spadají další donucovací prostředky. Jedná se např. o pozastavení licence nebo odebrání certifikace ke konkrétní službě či přímý zákaz fyzické osobě ve výkonu řídící funkce, která je součástí regulované organizace. (Sasková, 2022)

Dle Agentury ENISA by se kybernetická bezpečnost měla zlepšit na základě zapojení nových zájmových oblastí do národních strategií. Jednalo by se o samotné řízení zranitelností, kybernetickou hygienu či dodavatelský řetězec. Nové oblasti by tak vytvářely nové nápady a myšlenky, které by měly být více sdíleny mezi členskými státy, čímž by se posilovala mezinárodní spolupráce důležitá pro kybernetickou bezpečnost nás všech. Společnost ENISA tak byla směrnicí NIS 2 pověřena k řadě úkolů, kterými bude pozvednuta úroveň této bezpečnosti. V rámci úkolů má tak vylepšit evropský registr zranitelností, který je důležitý pro řešení kybernetických sítí. Důležitým bodem bude také

sdílení výročních kybernetických zpráv týkajících se bezpečnostního stavu EU, které by mohlo jednotlivým členským státům napomoci při vytváření bezpečnostních strategií souvisejících mimo jiné také s aktuálně možnými hrozby a útoky. Agentura je tak pomocníkem, který se bude snažit u všech členských států směrnici NIS 2 zavést podle předepsaných postupů, které budou obohaceny o šablony a nástroje vzniklé na základě nahlášených kybernetických incidentů. (ENISA, 2023)

Změny, které směrnice NIS 2 přináší, se týkají také rozdělení regulovaných subjektů. Ty se nově z několika dosavadních kategorií budou dělit na dvě skupiny, a to na základní subjekt a důležitý subjekt. Pod základní subjekt budou spadat všechny povinné osoby, které jsou v rámci regulace považovány za nejdůležitější z hlediska ochrany. Skupina důležité subjekty bude tedy zahrnovat zbývající povinné osoby, u kterých je pravděpodobnost vzniku kybernetického rizika menší než u skupiny předchozí. I z hlediska stanovování povinností budou tyto skupiny rozdělovány na dva režimy – režim vyšších povinností(essential) a režim nižších povinností (important). Režimy byly zavedeny k tomu, aby na menší firmy nebyly kladeny vysoké nároky a povinnosti, jak je to u organizací velkých. Jedná se o tzv. princip dvourychlostní kybernetické bezpečnosti, který také zajišťuje, že v jedné organizaci bude aplikovaný pouze jeden z těchto vymezených režimů, i přesto, že daná společnost bude spadat pod více než jednu regulovanou službu. Díky své velikosti, jak již bylo uvedeno výše, a také dle vymezených služeb uvedených v přílohách směrnice, budou muset organizace tuto směrnici plnit. (NÚKIB, 2023 b)

Regulované služby, vymezené v přílohách směrnice, jsou rozdělené podle velikosti podniků a stanovených režimů, do kterých spadají a jsou znázorněny na následujícím obrázku, který je dostupný také na portále NÚKIB.

Obrázek 1 Regulované služby (NÚKIB, 2023 b)

3 INFORMAČNÍ A KYBERNETICKÁ BEZPEČNOST

Informační bezpečnost je úzce propojena s kybernetickou bezpečností, a proto je pro účely této diplomové práce potřebné tento vztah objasnit a upřesnit tak některé souvislosti mezi těmito pojmy. V následujících podkapitolách bude prvotně určena stručná historie kyberzločinců, kteří se s postupem času vyvíjeli a snažili se o prolomení informační a kybernetické bezpečnosti. Dále bude následovat samotné vymezení vztahu mezi těmito pojmy, rozdělení informací z hlediska důvěrnosti a také vymezení systémů řízení bezpečnosti informací.

3.1 Historie kyberzločinu

V dnešní době jsou počítačové systémy považovány za samozřejmost jak u jedinců, tak i u organizací či vládních institucí. Každý zástupce skupiny, spadající do informačního světa, je přesvědčen o tom, že jsou tyto systémy důvěryhodné, a tak jejich obezřetnost s vkládáním důležitých informací do počítače upadá. V důsledku toho je nutné co nejlépe zabezpečit tyto informace pomocí dostupných nástrojů, které budou poskytovat uživatelům dostatečnou ochranu před zločinci, kteří se dopouštějí kybernetické kriminality za účelem dosažení zisku, tedy získání cenných informací. Již od 70. letech docházelo k nejrůznějším útokům, které se snažily narušit správné fungování systémů. Jednalo se ku příkladu o útok nazývaný phreaking, dále poté vznik prvního počítačového červu nazývaného Morrisův červ nebo také první útok v roce 1989 zvaný ransomware, který zablokoval data organizace v oblasti zdravotnictví za vidinou zaplacení výkupného. V 90. letech, kdy se výrazně rozšířil webový prohlížeč a elektronická pošta, došlo také k rozvoji nástrojů využívaných kyberzločinci. Ti mohli pomocí vylepšených metod posílat jednak škodlivé viry přes internet cílící na webové prohlížeče nebo také napadnout uživatele pomocí phishingových útoků. Od roku 2000 útočníci přišli s novým útokem souvisejícím se ztrátou identity, která byla realizována odcizením osobních údajů z databází a následným využitím těchto informací za účelem zneužití v rámci např. finančních podvodů nebo zakládání kreditních karet na cizí jméno. (Death, 2017)

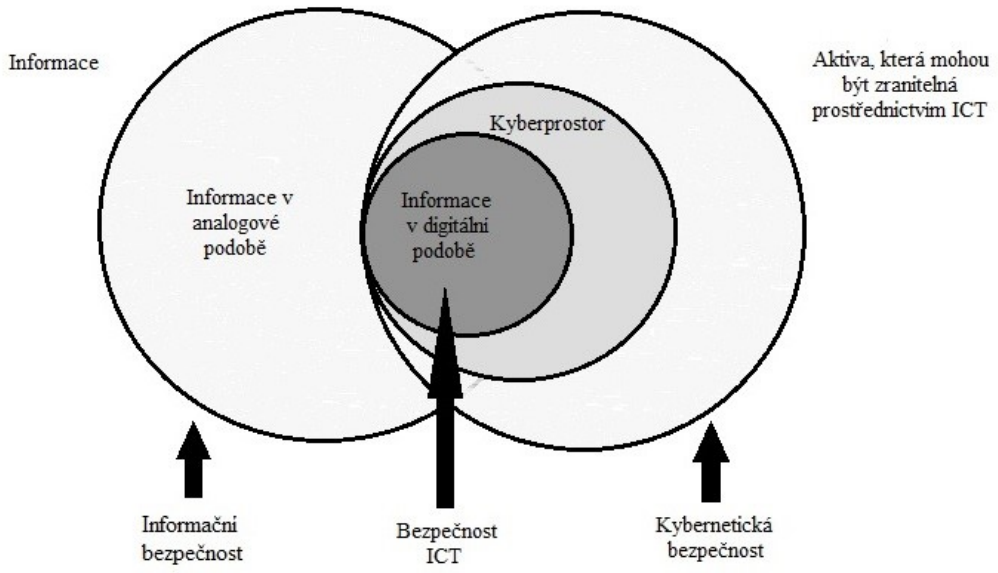
V současné době jsou, dle zprávy o stavu kybernetické bezpečnosti ČR za rok 2021, za nejčastější způsoby útoku považovány podvodné e-maily, skenování vnější sítě, škodlivý obsah a v největším zastoupení phishing, který se s postupem času rozvíjí a přináší tak mnohem více propracovaný postup, díky kterému může uživatel na vybraný subjekt snadněji zaútočit. Zprava také přináší informace týkající se nárůstu kybernetických

bezpečnostních incidentů, kterých v roce 2021 bylo 157, přičemž v roce 2020 se jednalo o 99 incidentů. Mezi nejzávažnější hrozby patřil také ransomwarový útok, u kterého se během posledních let začíná měnit jeho užití. Jedná se o využívání služby, prostřednictvím kyberkriminální skupiny, označovanou jako ransomware-as-a-service. Tu skupina prodává za určitý finanční obnos, který se odvíjí od nabízené služby komukoliv, kdo chce provést ransomware útok. V roce 2021 bylo v souvislosti s tímto útokem několikrát zaznamenáno tzv. dvojí vydírání, kdy byly pomocí útoku soubory společnosti prvně zašifrovány a poté vyjmuty ze systému. Informace obsažené v odcizených souborech pak sloužily k vydírání a požadování výkupného za výhružky zveřejnění či prodání těchto informací. (NÚKIB, 2022)

3.2 Vztah informační a kybernetické bezpečnosti

Doucek spolu s dalšími autory (2019) uvádí, že hlavním principem informační bezpečnosti je zachování důvěrnosti, dostupnosti a integrity, přičemž kybernetickou bezpečnost označuje jako soubor činností, která řeší celý kybernetický incident, do něhož spadá právě i informační bezpečnost. O kybernetický incident se jedná převážně tehdy, pokud jeho dopad zasáhne celý stát. Informační incident lze zase definovat jako situace, kdy budou požadované služby nedostupné. Oba pojmy mají tedy za cíl chránit informace v digitální podobě, které se nacházejí v kyberprostoru. (Doucek, Konečný a Novák 2019)

Toto tvrzení je také znázorněno na obrázku níže.



Obrázek 2 Informační a kybernetická bezpečnost,
(Doucek, Konečný a Novák, 2019), vlastní zpracování

V publikaci nazvané Výkladový slovník kybernetické bezpečnosti je uvedeno, že informační bezpečnost slouží *„k zachování dostupnosti informací a schopnosti s nimi pracovat v rozsahu přidělených opatření.“* Její součástí a hlavním úkolem pak má být ochrana a zabezpečení počítačů pomocí šifrovacích nástrojů a také předcházení a odhalování hrozícího nebezpečí, které by mohlo narušit funkčnost systémů. Kybernetická bezpečnost je v tomto slovníku vymezena jako souhrn opatření vedoucích k zajištění bezpečnosti kybernetického prostoru pomocí právních, organizačních, technických či vzdělávacích prostředků. (Jirásek, Novák a Požár, 2022, str. 23)

Na webu cybersecurity.cz (2017) je kybernetická bezpečnost popsána jako odvětví výpočetní techniky, označované také jako informační bezpečnost, která je aplikována jak u počítačů, tak i u sítí. Informační bezpečnost zde pak má plnit roli ochránce zejména informací a majetku před možnými útoky, přičemž však musí zaručit přístup a správnost těchto hodnot uživatelům systému. Celá strategie informační bezpečnosti je poté zaměřena na zabránění nevhodného chování počítačů, které je způsobováno nežádoucí událostí nebo činností. (NÚKIB, 2022)

3.3 Systém řízení bezpečnosti informací

Každá organizace různé velikosti v dnešní době využívá informační systémy, které ji napomáhají v jejím provozu a také jako podpora procesů na všech úrovních organizací. Stejně tak jako se vyvíjely tyto informační systémy, tak se rozvíjely i informační technologie, což také vedlo ke změně přístupu zabezpečování zpracovaných, ukládaných a přenášených informací. Z dříve užívaného uzavřeného výpočetního prostředí, které bylo zajišťováno pomocí fyzických kontrol za pomoci automatizovaného systému řízení, se vývoj přesunul na architekturu globálních informačních systémů vztažených k modelům informačních a komunikačních technologií v rámci služeb. Tyto nové služby musely obsahovat dostatečné funkce a informace vedoucí ke správnému realizování potřebných a nezbytných procesů v dané organizaci. Služby tak obecně musí zajistit kvalitu, která povede k podpoře a růstu zabezpečení ve vybrané společnosti. Poskytované služby tedy zajišťují zabezpečení dat proti neoprávněnému přístupu, odcizení či zničení. (Smejkal, Sokol a Kodl, 2019)

K tomu, aby bylo řízení bezpečnosti informací účinné, cílené a účelně rozvíjené, je nutné na tento proces řízení nahlížet jako na systém řízení bezpečnosti informací označovaný anglickou zkratkou ISMS (Information Security Management System). Tento systém je

označován jako jedna z částí, která spadá do systému řízení celé organizace a jeho cílem je přistupovat k rizikovým činnostem, v rámci kterých se provádí zavádění, provoz, přezkoumávání, monitorování či zlepšování bezpečnosti informací. (Doucek, Konečný a Novák, 2019)

Porada (2019) ve své publikaci uvádí, že obsahem ISMS mají být směrnice, politiky, postupy nebo také vhodné zdroje včetně činností, kterých organizace užívá, aby mohla lépe chránit její informační aktiva a dosáhnout tak požadovaných cílů.

Kolouch a Bašta (2019) jsou přesvědčeni, že pomocí tohoto systému lze zavést soubor opatření obsahující pravidla, díky nimž bude možno zajistit integritu, důvěrnost a dostupnost informací, což také napomůže k větší jistotě k zainteresovaným stranám, které se dostávají do kontaktu s některými riziky v rámci procesů organizace. Jak dále uvádějí, tento systém je aplikovatelný jak na malé, tak na velké organizace, zároveň se však v rámci organizace může uplatnit jen na některou z jejich částí. Rozdílnost strategie ISMS je poté ovlivněna právě velikostí daného subjektu, která v menších organizacích nebývá tak detailní, jako u velkých korporací. (Kolouch a Bašta, 2019)

Celé řízení informační bezpečnosti většinou započíná jmenováním pověřené osoby odpovědné za toto řízení, přičemž v současném čase se také formuluje základní organizační a technické bezpečnostní opatření, které by mělo být zavedeno ve všech organizacích nehledě na jejich velikost. Poté následuje analýza rizik a z jejich výsledků se tvoří příslušné návrhy ke zvládání problémových oblastí. Po vytvoření adekvátních návrhů se pokračuje s další potřebnou implementací organizačních a technických opatření, které dosud nebyly stanoveny. Veškerá opatření by se měly pravidelně kontrolovat a hodnotit, aby se předcházelo neočekávaným událostem v důsledku změny některého z rizik. Překontrolování a následné hodnocení se v zásadě aplikuje podle Demingova PDCA cyklu, který vychází ze čtyř základních kroků, které jsou označeny jednotlivými písmeny, a to:

- P – plan – plánuj,
- D – do – dělej,
- C – check – kontroluj,
- A – act – jednej. (Šulc, 2018)

Při použití modelu PDCA v rámci ISMS v organizaci se následně děje rozdělení do sedmi základních částí, pomocí kterých se řídí kybernetická a informační bezpečnost. Jedná se o:

- Kontext organizace –sloužící k uvedení všech zainteresovaných stran včetně stanovení rozsahu a hranic ISMS.
- Vůdčí role – stanovení osob z vrcholového vedení, které budou poukazovat na význam informační a kybernetické bezpečnosti všemi možnými prostředky.
- Plánování – obsahuje řízení rizik spolu s vytyčením cílů kybernetické a informační bezpečnosti.
- Podpora – zahrnuje vyčlenění nezbytných zdrojů, oprávnění u vyčleněných osob nebo také potřebné dokumentování informací.
- Provozování – pomocí určených plánů ke splnění cílů a vyhodnocených rizik jsou v souladu s provozem organizace pravidelně tvořeny nezbytná bezpečnostní opatření.
- Hodnocení výkonnosti – sloužící k monitoringu a následnému vyhodnocení zajištěných oblastí týkajících se kybernetické a informační bezpečnosti.
- Zlepšování – navazuje na předchozí bod, kdy jsou v důsledku zjištěných nedostatků plánována účinnější opatření zajišťující bezpečnost, popř. u fungujících systémů se jedná o jejich zkvalitňování. (Doucek, Konečný a Novák, 2019)

Ke správnému aplikování ISMS na výše vymezené a závazné prvky řízení se využívá normy ISO/IEC 27001, ve které se nacházejí požadavky uplatňující model PDCA, pomocí kterých dochází při splnění povinných závazků v této normě k vytvoření funkčního a smysluplného celku ISMS. Další následující norma ISO/IEC 27002 již neuvádí povinné požadavky, ale zaobírá se pouze vhodnými a doporučenými postupy nepodléhajícími závaznosti. (Doucek, Konečný a Novák, 2019)

Více podrobností o těchto normách obsahuje kapitola 2. této diplomové práce.

4 FYZICKÁ BEZPEČNOST

Fyzická bezpečnost, nebo také ochrana majetku, je označována jako jedna z nejstarších druhů ochrany pomocí ochranných opatření. Mezi první a mnohdy i jediné ochranné prostředky se zařazovala mechanická zábranná zařízení. Až s odstupem času a rozvojem tohoto oboru byly používány bezpečnostní technologie zahrnující elektronické systémy. (Lukáš, 2013)

Fyzická bezpečnost představuje dva možné významy, a to stav nebo soubor opatření. Stavem je označována situace, kdy se posuzuje stupeň možného bezpečí nebo nebezpečí u vybraného subjektu, který může být zasažen potencionální hrozbou ve fyzické podobě. Jedná se tedy o posouzení aktuálního zabezpečení u referenčního objektu, pomocí kterého může na základě stanovení potřebného opatření eliminovat možná hrozící nebezpečí. To lze zajistit právě pomocí fyzické bezpečnosti, jinak označované jako soubor opatření, které zajišťuje požadovaný stav bezpečí pomocí mechanických zábranných prostředků a systémů. (Lukáš, 2013)

Zajištění fyzické bezpečnosti je z hlediska ochrany informačních aktiv také vymezeno v zákonu č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Tato bezpečnost je zde rozdělena pomocí vymezení prostorů, v kterých se nacházejí důležité informace a data, a to na objekty, zabezpečenou oblast a jednací oblast. (Česko, 2005)

Cílem fyzické bezpečnosti u vybraného subjektu je pomocí správně aplikovaných ochranných opatření možného narušitele:

- Odradit nebo odstrašit – zajišťováno zejména perimetrickou a plášťovou ochranou.
- Zabránit vniku, zpozdit či ztížit – zajišťováno všemi druhy ochrany (perimetrická, plášťová, prostorová, předmětová).
- Identifikovat – při překonání ochrany zajišťováno pomocí technických prostředků, které tuto situaci detekují.
- Zadržet – zajišťováno pomocí fyzické ostrahy. (Lukáš, 2013)

4.1 Systém fyzické bezpečnosti

Cílem tohoto systému je pachateli fyzickou cestou znemožnit nebo ztížit přístup k důležitým aktivům pomocí stanovení a aplikování ochranných opatření. K tomu, aby byla provedení těchto opatření fyzické bezpečnosti úspěšná, je třeba dbát na čtyři základní faktory, a to:

- Komplexnost – je důležité dbát na rozsah a vzájemné propojení ochranných opatření a detekčních účinků.
- Vícestupňovost – je potřebné stanovit jednotlivé části, do kterých se budou zařazovat příslušná opatření, přičemž každá tato část bude vykonávat svoji funkci odděleně.
- Automatizace – je nutné využívat automatických prostředků, které dokážou identifikovat možná narušení a dále o tomto předají signál na dohledové pracoviště či pověřené osobě nebo také zásahové jednotce.
- Průlomová odolnost – při zabezpečování objektu je důležité stanovení adekvátní průlomové odolnosti, která by měla být vyhodnocena na odpovídající dobu, a to nejlépe tak, aby pro možného pachatele nebyla únosná, přičemž se počítá i s jeho schopnostmi a vybavením určeným k prolomení fyzické bezpečnosti. (Lukáš, 2013)

4.2 Základní druhy ochrany objektů

V podkapitolách níže jsou uvedeny základní druhy ochrany objektů, u kterých je vždy třeba zprvu posoudit jejich aktuální stav a následně zhodnotit pomocí jakých opatření lze zvýšit bezpečnost v daném prostředí. Základní druhy ochrany objektů tak popisují, jakými možnými prostředky je možné stav fyzické bezpečnosti zajistit.

4.2.1 Klasická ochrana

Tento typ ochrany se řadí mezi vývojově nejstarší a také nejrozšířenější způsob, jak zabezpečit požadovaný objekt. Mechanické prostředky, které byly zařazeny mezi hlavní prostředky této ochrany, se postupem času s vývojem nových technologií stávaly důvěryhodnějšími, avšak i přesto se nejedná o prvky zajišťující dostačující ochranu před možností narušení pachatelem. Mezi mechanické prostředky zajišťující klasickou ochranu lze zařadit např. ploty, zábrany, zámky, mříže nebo z historického hlediska také

pevnosti, truhlice či pancéřové pokladny. Klasickou ochranu tedy využívá převážné každý subjekt v rámci svého základního zabezpečení pomocí mechanických zábran, které slouží k prvotnímu odstrašení možného pachatele. Tyto zábrany však nejsou z hlediska bezpečnosti adekvátní a jejich odolnost bývá časově omezená, a proto je důležité tyto prvky ochrany kombinovat s dalšími možnostmi zabezpečení. (Uhlář, 2005)

4.2.2 Technická ochrana

Technická ochrana zahrnuje takové prostředky, které se řadí mezi nejvíce věrohodné a nezdolné. Hlavním principem je pomocí odpovídajících technických prostředků zajistit bezpečnost takovým způsobem, který bude případnému pachateli co nejvíce znemožňovat dokončení či samotné započetí jeho protiprávního jednání či opuštění chráněného prostoru. Pokud bude vybraný prostor z hlediska bezpečnosti pomocí technických prostředků dostatečně střežen, je vysoká pravděpodobnost odhalení pachatele v daném objektu téměř okamžitě. Za technický prostředek lze považovat jakýkoliv detekční systém, pomocí kterého je monitorována situace v chráněném prostoru a informace z něj jsou předávány na příslušné zařízení či pověřené osobě. Jak je tedy zřejmé, aplikováním technických prostředků nedochází k fyzickému zabránění pachateli k narušení prostoru, ale při kombinaci klasické a technické ochrany je toto zabránění možné a nejvíce využívané. (Uhlář, 2005)

Technické prostředky zpravidla zastupují také mechanické zábranné systémy, poplachové a tísňové systémy, kamerové systémy, systémy kontrol a vstupů a elektrické zabezpečovací signalizace, díky nimž se zajišťuje požadovaná úroveň zabezpečení vybraného objektu, kterou pachatel nepřekoná, pokud však nemá schopnosti, které převyšují tato bezpečnostní opatření. (Lukáš, 2013)

Technickou ochranu lze dle Uhláře (2005, str. 18) rozdělit z hlediska začlenění do zabezpečovacího systému na čtyři skupiny, a to z hlediska:

- *„Prostorového zaměření,*
- *Způsobu předání poplachového signálu,*
- *Kategorie rizikovosti chráněného objektu,*
- *Stupně zabezpečení chráněného objektu.“*

Pro účely této diplomové práce bude vymezeno následujíce pouze hledisko prostorového zaměření.

Z hlediska prostorového zaměření

Technická ochrana z hlediska prostorového zaměření je dělena na pět druhů, které zajišťují bezpečnost vymezeného prostoru. Tyto druhy jsou označovány jako:

- **Perimetrická ochrana –** neboli obvodová ochrana, která je zajišťována pomocí bezpečnostních opatření vztahujících se k obvodu (perimetru) pozemku, jež se nachází v chráněném objektu a také prostor mezi tímto perimetrem a chráněným objektem.
- **Plášťová ochrana –** jedná se o souhrn bezpečnostních opatření aplikovaných na plášti chráněného objektu, jimiž jsou většinou míněny budovy – ty jsou zpravidla chráněny prostředky (mechanickými překážkami), které jsou využitelné k odhalení, znemožnění průchodu, zastrašení či zpoždění narušitele, tedy zdi, okna, dveřní prostory či např. kamerové systémy.
- **Prostorová ochrana –** jedná se o bezpečnostní opatření, které slouží ke zpoždění nebo odhalení potencionálního pachatele uvnitř chráněné budovy, která bývá proti tomuto narušení vybavena zpravidla na chodbách, schodištích či místnostech technickými prostředky jako jsou kamerové a zámkové systémy, poplachové zabezpečovací systémy, mříže či dveře.
- **Předmětová ochrana –** zahrnuje bezpečnostní opatření, které je aplikováno proti odcizení či neoprávněné manipulaci s chráněnými aktivy, jimiž jsou myšleny veškeré cenné předměty nacházející se uvnitř budovy a vyžadují zabezpečení pomocí např. vitrín, trezorů, kamerových systémů, skleněných tabulí nebo také poplachových zabezpečovacích systémů. (Lukáš, 2011)

Uhlář (2005) také ve své publikaci uvádí možnost kombinovat tyto druhy ochrany a zavést tak bezpečnostní opatření v rámci všech, což označuje pojmem vícestupňová ochrana, která u objektů s vysokými riziky lépe zabezpečuje chráněná aktiva.

Aby však bylo zajištění technické ochrany z hlediska prostorového vymezení efektivní, je nutné vynaložit na bezpečnostní opatření v rámci jednotlivých typů ochrany pouze takovou výši finančních prostředků, které nebudou převyšovat hodnotu chráněných aktiv anebo také schopnosti možných narušitelů. (Lukáš, 2011)

4.2.3 Fyzická ochrana

Fyzická ochrana je zajišťována pomocí osob, které se ve vymezeném chráněném prostoru nacházejí trvale či dočasně dle stanovených režimových opatření. Jejich hlavním cílem je ochrana vymezených aktiv, tedy pozorovat a zajišťovat situaci v tomto prostoru a v případě potřeby adekvátně reagovat. Osoby vykonávající tuto ochranu mohou být hlídači, vrátní, strážní, pracovníci bezpečnostních agentur, policisté, přičemž jejich specializace se odvíjí od kategorie chráněného objektu a potřeby zajištění bezpečnosti. (Lukáš, 2013)

Fyzická ochrana je z hlediska celkového zabezpečení objektu v převážné většině aplikovaná až jako jedno ze závěrečných opatření zajišťující bezpečnost a také je považována jako jedna z nejlepších možností ochrany. Toto tvrzení je umocněno tím, že zbývající druhy ochrany nedokážou zajistit tak dobře požadovanou bezpečnost jako samotný člověk. Na druhou stranu, je ale investice do této ochrany největší. Počáteční náklady zahrnující výzbroj, výstroj či základní výcvik jsou malé, ale finanční prostředky na platy osobám zajišťujícím bezpečnost jsou stálé, a také z dlouhodobého hlediska vysoké. Je tedy důležité efektivně kombinovat i ostatní prostředky ochrany, aby docházelo k co největšímu souhrnnému zabezpečení. (Uhlář, 2005)

4.2.4 Režimová ochrana

Pomocí režimové ochrany jsou stanovena opatření obsahující zásady, směrnice, pravidla a ochranu osob ve vymezených prostorách v rámci chráněného subjektu. Tato opatření jsou administrativně operačního charakteru a jejich vytvořením vzniká ucelený soubor, který je v souladu s provozem chráněného subjektu a zajištuje požadované zabezpečení. V praxi se tedy může jednat o příslušné kompetence při pohybu osob po objektu a při vstupu do zabezpečovaných oblastí a jejich následná kontrola, omezení pro vjezd a výjezd dopravních prostředků a jejich kontrola nebo také pravidla sloužící k zajištění kontroly při vnášení či odnášení materiálu apod. (Lukáš, 2013; Kyncl, 2014)

Režimová opatření v souvislosti s její ochranou lze také dále rozdělit na vnější, týkající se zpravidla vstupu a výstupu z objektu, přičemž jejich kontrola bývá zajišťována ostrahou, tedy pomocí fyzické ochrany a vnitřní, které představují bezpečnostní procesy uvnitř chráněného subjektu, jako je např. stanovení zvláštního režimu, zajištění skladového režimu a další. (Uhlář, 2005)

Mezi hlavní problém se však neřadí vytvoření těchto režimových opatření, nýbrž jejich následná implementace a prosazení v rámci chráněného subjektu, což může být značně komplikované, protože je třeba spolupráce všech podílejících se osob. (Uhlář, 2005)

5 ANALÝZA RIZIK V PODMÍNKÁCH INFORMAČNÍ BEZPEČNOSTI

Všechny organizace uskutečňují dané aktivity, které mohou obsahovat podnikatelská rizika. Takováto rizika bezpodmínečně nepříznivě ovlivňují chod a provoz organizací a v důsledku toho jsou ohroženy také jejich cíle a naplňování strategií. Míru rizika v tomto případě ovlivňuje dopad, který subjekt negativně zasáhne a také určitá pravděpodobnost vzniku rizika. Vzhledem k těmto okolnostem by tedy každá organizace měla mít určeno jaká rizika přijme a jak je bude řídit. A u informačních systémů je to ohledně přijetí rizik stejné jako u podnikání. K tomu, aby mohly být určena rizika a stanoveny hrozby, které organizaci hrozí, je nutné provést analýzu rizik, jejíž cílem je pak jednotlivá rizika identifikovat a číselně ohodnotit jejich přijatelnost pro daný subjekt. Díky tomuto identifikování a ohodnocení je pak určena pravděpodobnost výskytu rizika a možný dopad pro organizaci. (Požár, 2005)

Definici analýzy rizik popisuje Porada (2019, str.150) jako *„proces definování hrozeb, pravděpodobnosti jejich uskutečňování a dopadu na aktiva, tedy stanovení rizik a jejich závažnosti.“* Dále také uvádí, že následující činností po analýze rizik je jejich řízení.

Je však důležité zmínit, že analýza rizik není pro organizaci vytvářena pouze jedenkrát, ale jako pravidelně se opakující proces. Analýza rizik se sice pokouší identifikovat všechna rizika, ale poskytuje pouze výčet těch, které se v organizaci v daném čase právě vyskytují. Je tedy důležitá její pravidelná aktualizace, která by měla být provedena při všech významných změnách týkajících se informačních systémů či při výskytu nových hrozeb. Interval přepracování celkové analýzy rizik by se měl odvíjet od velikosti dané organizace a také v důsledku závislosti na jejich informačních technologiích. (Požár, 2005)

Analýza rizik se pro posuzovaný subjekt obvykle zpracovává ve dvou podobách. Jedná se o:

- Orientační analýzu rizik – ta je prováděna v situacích, kdy je třeba zhodnotit, která např. část, aktivum, místnost, budova jsou pro posuzovaný subjekt klíčové jednak z hlediska fungování a také pro určení nejkritičtějších oblastí subjektu.
- Detailní analýzu rizik – je zpracována u vymezených oblastí a činností, které jsou vyhodnoceny z předchozí orientační analýzy rizik, a to pomocí vhodných metod určených pro analýzu rizik. (Smejkal a Rais, 2011)

Analýza rizik je důležitým krokem při řízení bezpečnosti informací a jejím zpracováním poskytuje odpovědi na tři základní otázky:

- *„Co se stane, když nebudou informace chráněny?*
- *Jak může být porušena bezpečnost informací?*
- *S jakou pravděpodobností se to stane?“* (Lukáš, 2015, str. 99)

Analýza rizik, jak uvádí Porada (2019), tedy zahrnuje dvě hlavní fáze, a to identifikace rizik a řízení rizik. Do fáze identifikace rizik spadají jednotlivé kroky:

- Identifikace aktiv – definuje vybraný subjekt a následně se zabývá charakteristikou aktiv tohoto subjektu.
- Určení hodnoty aktiv – začíná stanovením hodnot u jednotlivých aktiv a určením jejich významu pro daný subjekt a poté také určení dopadu, který by subjektu nastal v případě ztráty, poškození či změny z hlediska jeho chování či existence.
- Identifikace hrozeb a zranitelností – kde jsou vymezeny možné situace a děje, které mohou negativně působit na stanovený subjekt a současně také určení jeho slabých míst, jež by mohly vyvolat hrozbu.
- Stanovení závažnosti hrozeb a míry zranitelností – zde se určuje možná pravděpodobnost, při které hrozba může vzniknout a také stanovení do jaké míry je subjekt zranitelný vůči vymezeným hrozbám, přičemž vztah mezi hrozbou a zranitelností je označován jako riziko. (Požár, 2019; Shameli-Sendi, 2015)

Po první fázi následuje řízení rizik. Tento pojem je označován za proces, jenž má vymezen působení aktuálních či budoucích negativních faktorů ovlivňující subjekt a jeho hlavním cílem je tak stanovit potřebná rozhodnutí, která budou eliminovat negativní jevy a posilovat možné příležitosti vedoucí ke snížení hrozícího rizika na přijatelnou úroveň. Následuje stanovení opatření, které je posuzováno z hlediska ekonomického, technického, sociálního a politického a je označováno za rozhodovací proces v rámci analýzy rizik vytvářející preventivní či regulační opatření. (Porada, 2019)

Ve druhé fázi řízení rizik je tedy nutné u vyhodnocených identifikovaných rizik:

- Zhodnotit možné dopady plynoucí z hrozeb na charakterizovaná aktiva a na samotnou činnost organizace.
- Definovat úrovně všech rizik.

- Posoudit úroveň akceptovatelnosti jednotlivých rizik a stanovit možné řešení v případě, kdy není možné je přijmout. (Porada, 2019)

Možnosti, které se nabízejí pro řešení konkrétního rizika jsou následující:

- Přijmutí rizika, kdy je organizace plně seznámena s riziky a rozhodne se je akceptovat.
- Vyhnutí se riziku, kdy je z organizace vyloučena činnost, která přináší jedno nebo více rizik.
- Převedení rizika, kde je veškerá nebo částečná odpovědnost spojená s takovýmto rizikem převedena na jinou osobu.
- Zmírnění rizika, kdy jsou stanovena v organizaci taková opatření vedoucí ke snížení úrovně rizika pod přijatelnou mez organizace. (Shameli-Sendi, 2015)

Základní rozdělení metod analýzy rizik je děleno na kvalitativní a kvantitativní metody a je vymezeno pomocí základního hlediska, a to je způsob vyjádření veličin v analýze rizik. V analýze rizik se používají tyto metody odděleně nebo jako jejich kombinace. Následující podkapitoly jsou určeny pro jejich vymezení.

5.1 Kvalitativní metody

Hlavní princip kvalitativních metod je založen na identifikaci závažnosti možného dopadu a také na stanovení pravděpodobnosti vzniku události. Rizika v těchto metodách bývají hodnocena pomocí číselných stupnic nebo pomocí slovního hodnocení a mají stanovený svůj možný rozsah, který vychází z kvalifikovaného odhadu. Jedná se o více subjektivnější metody, které se ale vyznačují svou rychlostí a jednoduchostí. Vzhledem k subjektivnímu ohodnocení může docházet k nepřesnostem vycházejícím z charakterizování konkrétní hrozby, kde je sice stanovena její úroveň, ale jen pomocí číselných stupnic či slovního vyjádření, které není definováno z pohledu finanční stránky a může tak přinést problémy při stanovování nákladovosti. Tyto metody jsou vhodné při detailní analýze rizik, která upřesňuje postupy a také pokud subjekt nemá dostatečné a potřebné číselné údaje pro využití kvantitativních metod při analýze rizik. (Smejkal a Rais, 2011)

5.2 Kvantitativní metody

Princip kvantitativních metod se odráží od matematického výpočtu rizika, který je stanoven z četnosti výskytu hrozby a jejího dopadu. Při stanovení pravděpodobnosti vzniku

možného incidentu a odhadnutí jeho dopadu je použito numerického ocenění. Dopad je tedy vyjádřen pomocí finančních výrazů, např. v „tisících Kč“, nejčastěji ve formě roční předpokládané ztráty. Provedení těchto metod je z hlediska získání potřebných údajů časově náročné, ale výsledek v podobě konkrétního finančního ohodnocení u jednotlivých rizik naproti tomu zdokonaluje a ulehčuje celkové zvládání rizik ve vybraném subjektu. Nevýhodou při použití těchto metod také může být formalizovaný postup, který zahltí pověřeného hodnotitele velkým množstvím dat, z čehožpak může nastat situace, kdy nebudou obsaženy a vymezeny všechny podrobnosti a individuality ve vybraném subjektu způsobující zranitelnost. K docílení kvalitních výsledků při použití kvantitativních metod je důležité klást důraz na kvalitu získaných informací. (Smejkal a Rais, 2011)

6 DÍLČÍ ZÁVĚR

Úvod teoretické části diplomové práce se zaměřuje na popis základní terminologie a právního rámce a standardů týkajících se informační bezpečnosti. Další kapitola se věnuje identifikaci vztahu informační a kybernetické. Součástí této kapitoly je rovněž popis systému řízení bezpečnosti informací. Kapitola fyzické bezpečnosti dále uvádí, jaké jsou základní druhy ochrany objektů a jakými prostředky je třeba ji zabezpečit. Závěrem teoretické části je popsána analýza rizik a následně také základní rozdělení jejich metod.

Z uvedených dostupných literárních zdrojů v této části práce je důležité zmínit, že je nezbytné věnovat se oblasti fyzické bezpečnosti, která je významná nejen pro ochranu informačních aktiv společnosti. Pro zachování bezpečnosti informací je důležité také vycházet z odpovídacích předpisů či definovaných ISO norem, jež vymezují práva a povinnosti subjektům, ale také určité povinné či doporučující postupy.

Za pomoci tohoto shrnutí dostupných literárních zdrojů bude v praktické části diplomové práce provedena analýza současného stavu informační bezpečnosti z hlediska bezpečnosti fyzické, která bude pokračovat analýzou rizik a dalšími úkony, které je třeba stanovit pro návrh, jenž by splňoval zlepšení současného stavu.

II. PRAKTICKÁ ČÁST

7 POPIS A ANALÝZA SOUČASNÉHO STAVU FYZICKÉ BEZPEČNOSTI Z HLEDISKA INFORMAČNÍ BEZPEČNOSTI

V úvodu této kapitoly bude charakterizován vybraný subjekt určený pro splnění cílů této diplomové práce. Subjekt byl vybrán na základě rozhodnutí autorky práce, která tuto společnost navštěvuje.

Hlavní částí této kapitoly bude popis a analýza současného stavu informační bezpečnosti z hlediska fyzické bezpečnosti.

Informační aktiva společnosti se nacházejí jednak na externích místech či uložištích, ale také přímo ve vymezeném subjektu, kde je nutné zhodnotit, jak je z hlediska zabezpečení zajištěna jejich ochrana. K tomu, aby mohla být analyzována ochrana informačních aktiv, je nezbytné posoudit aktuální fyzické zabezpečení vybraného subjektu, které lze považovat jako zásadní pro zajištění bezpečnosti těchto aktiv.

Popis současného stavu fyzické bezpečnosti z hlediska informační bezpečnosti bude vymezen dle normy ČSN EN ISO/IEC 27002, v níž je obsažen postup při posuzování stavu bezpečnosti, dle kterého budou v této práci zapracovány příslušné kapitoly. Fyzická bezpečnost a bezpečnost prostředí je v této normě dělena na zabezpečené oblasti a zařízení, přičemž dále obsahují upřesňující podkapitoly týkající se bezpečnosti. (ČSN EN ISO/IEC 27002, 2014)

Vše, co daná norma požaduje a vybraný subjekt ve své společnosti nemá zavedeno, bude v každé podkapitole uvedeno pomocí doplňujícího opatření. Tento postup zajistí, že zabezpečení vybrané společnosti bude odpovídat standardům zmiňované normy.

Historie vzniku organizace

Firma HABRESTO ARMS s.r.o. vznikla v roce 2018 jako samostatná společnost, jež byla založena jedním z jednatelů firmy HABRESTO s.r.o., z které organizace původně vzešla. Jedná se o rodinnou firmu a při vzniku nového subjektu, který je předmětem této diplomové práce, se k původnímu zažitému názvu pouze připojil dovětek, a to ARMS – zbraně. Jak už ze samotného názvu vyplývá, jedná se o subjekt zabývající se jednak prodejem zbraní, ale také samotným provozováním střelnice. (HABRESTO ARMS s.r.o., 2021)

Společnost sídlí v Jihomoravském kraji v obci Ježkovice, která leží 10 km západně od města Vyškova. Tato obec se rozprostírá na Drahanské vrchovině a má 381 obyvatel.

Vybraný subjekt se v obci nachází v klidné lokalitě, která je z převážné většiny obklopena poli a lesy. Celý objekt, ve kterém se firma nachází, dříve sloužil jako JZD, a tak je jeho rozloha poměrně velká, a to 30.186,55 m². Mimo společnost, která sídlí v tomto objektu, se zde nacházejí ještě další budovy, které postupně procházejí rekonstrukcí a současně plní úlohu skladovacích prostor.

Situační pozice vymezeného subjektu je uvedena níže na obrázku č. 3.

Obrázek 3 Situační pozice HABRESTO ARMS s.r.o. (mapy.cz)

Samotná střelnice byla připravena k provozu začátkem roku 2021, ale její provoz byl omezován vládními opatřeními, kvůli kterým musela být uzavřená. Na plno se tak její provoz spustil až ke konci tohoto roku, přičemž prodej zbraní, střeliva a dalšího příslušenství omezen nebyl.

Předmět činnosti

Jak již bylo uvedeno výše, organizace se specializuje na prodej zbraní a provoz střelnice. Mezi její hlavní předmět činnosti lze tedy uvést:

- Nákup, prodej, přeprava, půjčování či uschování zbraní a střeliva.
- Provozování střelnice.
- Výcvik a výuka mířené či taktické střelby se zbraní.
- Praktická i teoretická příprava na zkoušku odborné způsobilosti k získání zbrojního průkazu.

Od konce roku 2022 střelnice disponuje také tzv. „Killhousem 360°“. Jedná se o unikátní taktickou střelnici, která byla připravena a navržena za pomoci členů speciálních jednotek a slouží primárně pro střelbu a výcvik technik CQB (Close Quarters Battle) a taktické střelby za různých akustických a také světelných podmínek s možností střelby do všech směrů. Technika CQB je zaměřena na provedení boje v uzavřených objektech na krátkou vzdálenost a je využívána armádou a speciálními jednotkami. (HABRESTO ARMS s.r.o., 2021)

Nově je také možné na střelnici, mimo přípravy na zkoušky odborné způsobilosti, vykonat samotnou zkoušku k získání zbrojního průkazu. Tuto službu organizace zavedla, aby pro zákazníky umožnila vykonat kompletní kurz včetně zkoušky, kterou doposud museli absolvovat u jiné společnosti.

Mimo hlavní předmět činnosti se střelnice může pronajímat k firemním akcím či rodinným oslavám. Střelnice je také využívána městskou policií, státní policií, pořádkovými jednotkami, prvosledovými zásahovými jednotkami i speciálními jednotkami různých státních útvarů. Tyto útvary zde upevňují a rozšiřují své střelecké schopnosti jak už pravidelným výcvikem, tak i v rámci různých mezinárodních mistrovství, kde vybraný subjekt plní roli pronajímatele. (HABRESTO ARMS s.r.o., 2021)

Společnost HABRESTO ARMS s.r.o. je také oficiálním partnerem několika zahraničních a českých společností, mezi kterými vyniká Česká zbrojovka a.s., se kterou vybraný subjekt začal spolupracovat na nejvyšší partnerské úrovni v nedávné době.

Organizační struktura

Hlavním jednatelem společnosti a také hlavním správcem střelnice je Jan Brehový, který odpovídá za celou organizaci a provoz s ní spojený. Dále také zajišťuje mezinárodní obchod týkající se zbraní, střeliva, příslušenství a jeho následný prodej.

Dalšími členy této společnosti jsou dva správci střelnice, kteří jsou podřízeni hlavnímu jednateli. Ti se převážně specializují na střelecké kurzy a zážitkovou střelbu.

Účetnictví je zajišťováno externí firmou, která také vytváří dokumentaci související se životním prostředím, BOZP, GDPR, PO, HACCP a COVID-19.

Externí firmou je také zajištěn běžný provozní úklid, který je na střelnici vykonáván 3x do týdne v době přítomnosti jednoho ze správců střelnice.

Provozní doba střelnice se odvíjí od rezervovanosti střelnice uskutečňované pomocí webového rezervačního systému, popřípadě po telefonické domluvě a také dle prodeje zboží. Z toho důvodu je organizační struktura společnosti poměrně malá, ale pro aktuální potřebu společnosti z hlediska organizačního dostatečná.

7.1 Zabezpečené oblasti

Vymezení a implementace opatření si v zabezpečených oblastech dle ISO normy 27002 (2014, str. 33) klade za cíl *„zabránit neoprávněnému fyzickému přístupu, poškození a narušování informací a vybavení pro zpracování informací organizace“*.

Jak již bylo nastíněno, následující podkapitoly se budou zabývat aktuálním zhodnocením fyzické bezpečnosti a bezpečnosti prostředí u vybraného subjektu a také možnou implementací bezpečnostních opatření, které jsou doporučené dle výše zmíněné normy.

7.1.1 Fyzický bezpečnostní perimetr

Vymezený subjekt provozovatele střelnice se nachází v areálu, který je vlastněn majitelem pozemku, přičemž však za jeho ochranu odpovídá provozovatel střelnice. Za bezpečnostní perimetr lze tedy považovat samotné ohraničení celého areálu, v kterém se subjekt nachází.

Perimetr pozemku je zabezpečen pomocí mechanického zábranného systému, a to plotu, který je situován kolem celého objektu. Jedná se o pletivový plot o výšce 1,6 m a jeho výplet je tvořen dráty. Na několika úsecích tento plot však neodpovídá požadovanému bezpečnostnímu stavu. I přestože byla nedávno provedena oprava, významná část původního materiálu nebyla vyměněna a je jasně patrné, že jeho zabezpečující funkce nejsou dostatečné. Riziková místa se nacházejí na severní a jižní straně pozemku. Severní část je po celé délce obklopena polem.

Obrázek 4 Severní část oplocení (vlastní)

Plot na jižní straně je umístěn okolo zpevněné cesty, která je dále vedena po západní straně pozemku a místní občané ji využívají k rekreačním procházkám. Za nedostatečně zabezpečený úsek lze také považovat východní perimetr, kde se nachází hlavní vstup do pozemku.

Obrázek 5 Jižní část oplocení (vlastní)

Na východní straně pozemku se nachází vstupní brána, která je zabezpečena pomocí visacího zámku, který je instalován z vnitřní strany brány. Tato brána bývá otevřená jen v přítomnosti jednoho ze správců střelnice, který vlastní klíč k zámku nebo také při otevření majitelem pozemku či údržbářem. Pro otevření brány je nutné otevřít vstupní

branku, kterou osoba projde a dostane se na vnitřní stranu pozemku k visacímu zámku. Alternativně je možné použít mezery mezi kovovými tyčemi na bráně, do kterých osoba zasune ruku a odemkne tento zámek. Brána je otevřená vždy, pokud se někdo z interních osob nachází v areálu, převážně tedy dle stanovené otevírací doby střelnice.

Obrázek 6 Hlavní vstupní brána (vlastní)

Za bránou je umístěna automatická závora od společnosti TOR-MASTER s.r.o. fungující prostřednictvím GSM modulu, pomocí které je zákazníkům umožněn vstup na pozemek, pokud jedou automobilem. GSM modul obsahuje svoji SIM kartu a je instalován na pohon závory. V případě prozvonění telefonního čísla této SIM karty z ověřeného a uloženého mobilního zařízení dojde k jejímu otevření. Modul obsahuje také definované příkazy, které jsou vysílány pomocí odeslání příslušné SMS zprávy z mobilního telefonu. Závoru jsou oprávněny obsluhovat všechny interní osoby, tedy majitel pozemku, správci střelnice a údržbář.

V případě pěšího způsobu je však možné závoru lehce obejít. Závora je také umístěna jen přes jednu polovinu celé šíře brány a její celková délka je 3,5 m. V případě tedy, že je brána na straně závory otevřená, tak druhou polovinu brány, při které závora není, lze snadno otevřít a překonat tak tuto bariéru, která má zabraňovat vstupu nepovolaných osob na pozemek.

Samotný perimetr pozemku je u hlavního vstupu také zabezpečen třemi kamerami, které jsou umístěny na nedaleké budově. Jedna kamera monitoruje vstupní bránu do pozemku a ostatní dvě jsou instalovány k účelu hlídání přístupových cest vedoucích k budově střelnice. Jedná se o kamery od výrobce DAHUA TECHNOLOGY, které jsou bezdrátově připojeny přes Wi-Fi síť vedenou z budovy střelnice, přičemž elektrická energie je vedena přes příslušný kabel přímo do sítě instalované v budově, na které jsou kamery umístěny. Na této budově lze nalézt také další tři kamery, jedná se však pouze o atrapy. Všechny výše zmíněné kamery jsou přiblíženy obrázkem č. 7.

Obrázek 7 Kamery u hlavní vstupní brány

(vlastní)

To, co kamery snímají, je poté přenášeno obrazem na monitor umístěný v budově střelnice. Hlídání perimetru pozemku tak náleží hlavnímu správci střelnice, popřípadě ostatním správcům, kterým je v době jejich přítomnosti umožněno sledovat aktuální situaci a v případě neoprávněného vstupu osob tak mohou ihned zasáhnout. Další kamera zajišťující bezpečnostní perimetr je umístěna na samotné budově střelnice, která se nachází na druhé straně pozemku oproti vstupu. Je tedy zřetelné, že prostor mezi těmito dvěma úseky není nijak střežen. Pokud výše uvedené osoby nemohou sledovat aktuální situaci přenášenou z kamer na monitor, tak má pouze hlavní správce střelnice možnost tento přenos sledovat ze služebního mobilního telefonu, na kterém je k tomuto účelu nainstalovaná příslušná aplikace.

Kamera zajišťující bezpečnost budovy střelnice je umístěna nad hlavním vstupem, jejíž princip fungování je obdobný jako u kamer na budově u vstupní brány, přičemž je však připojena do sítě pomocí ethernetového kabelu. Ten zajišťuje její připojení k datové síti. Kamera tedy snímá vchodové dveře a jejich přilehlé okolí. Na zadní straně budovy jsou umístěny pouze dvě makety kamer, které mají odstrašit případné narušitele. Na obrázku č. 8 lze vidět monitor, přes který správce z budovy střelnice sleduje pomocí kamerového systému aktuální situaci ve vymezeném objektu.

Obrázek 8 Monitor s kamerami (vlastní)

Za část spadající do bezpečnostního perimetru lze považovat také veškeré ostatní budovy, které jsou součástí areálu. Ostatních budov, vyjma střelnice, je na pozemku ještě pět. Tyto budovy jsou zatím nevyužívány a probíhá v nich rekonstrukce, kterou má na starosti majitel pozemku. Jedna budova je však po domluvě s majitelem využívána provozovatelem střelnice k uskladnění potřebných prostředků důležitých k provozu střelnice. Tato budova je tvořena z plechových stěn a střechy a není vybavena žádným bezpečnostním zařízením.

Na pozemku se také nachází volně stojící rozvodna elektrické energie, která je zabezpečená pouze mechanickým zámkem. Nachází se také blízko oplocení, které je lehce překonatelné a její ochrana není jiným způsobem zajištěna. Je tedy snadné ji poškodit.

Obrázek 9 Rozvodna elektrické energie

(vlastní)

Vymezení doplňujícího opatření:

- Zajistit fyzický stav perimetrické ochrany tak, aby neobsahoval místa, kudy lze lehce proniknout.
- Zavést vnější ochranu oken v přízemí budovy střelnice.
- Zřídit recepci s obsluhou či zajistit řízený přístup osob pomocí jiných technických prostředků.
- Vybudovat fyzické bariéry po areálu společnosti.
- Zřízení komunikační místnosti pro ochranu informačních aktiv společnosti.

7.1.2 Fyzické kontroly vstupu

Fyzická kontrola vstupu v tomto subjektu není zajištěna žádnou externí firmou, která by monitorovala situaci na celém pozemku nebo uvnitř budovy střelnice. Bezpečnost je zajištěna na perimetru pozemku pouze podle výše vymezených prvků, a to pomocí oplocení, uzamknuté hlavní brány mimo provozní dobu, elektronické závory nebo kamer umístěných u vstupu do areálu. Tím, že po celém areálu, mimo budovu střelnice, nejsou umístěny téměř žádné zabezpečovací prvky, je těžké odhalit neoprávněný pohyb osob

po pozemku. Jediná možnost, jak lze aktuálně zamezit průniku těchto osob do areálu, je identifikovat tyto osoby u vstupní brány pomocí zřízeného kamerového systému, pokud však pověřená osoba hlídající hlavní vstup do pozemku tento pohyb zaznamená.

Budova střelnice, ve které se nacházejí informační aktiva, je již zabezpečovacími prvky opatřena. Jedná se o výše zmíněný kamerový systém umístěný na budově, ale také další prostředky zabraňující vstupu nepovolaným osobám. Lze zde zařadit hlavní vstupní dveře. Jedná se o plastové dveře, které mají z vnitřní strany umístěnou klasickou dveřní kliku a z venkovní strany jsou opatřeny tzv. koulí, která zabraňuje otevření dveří z této strany. Dveře jsou také zabezpečeny elektrickým zámkovým zařízením, a to elektrickým otvíračem dveří od společnosti Tokoz a.s., který funguje na principu signalizace stavu otevřených nebo zavřených dveří. Pokud jsou dveře zavřené, je k jejich otevření třeba zmáčknout příslušné tlačítko, které přenáší napětí do dveří, na základě čehož se dveře otevřou. Po zavření dveří a zaklapnutí zámku je k jejich otevření opět třeba využít zmíněné tlačítko. Pověřený pracovník díky tomuto prostředku reguluje pohyb osob v budově. Zda osoby budou mít vstup umožněn, pracovník rozhoduje na základě kamerového záznamu přenášeného pomocí monitoru. Dveře lze také otevřít příslušným klíčem z vnitřní i venkovní strany. Budova disponuje dalšími dveřmi, jež se nacházejí v zadní části. Jedny jsou umístěny v kotelně a druhé ve spojovací chodbě zadní části komplexu.

Pro fyzické kontroly vstupu je společností zajištěn systém hlavního a vedlejšího klíče. Provozovatel střelnice je jedinou osobou vlastnící hlavní klíč, jenž mu umožňuje přístup do celého areálu včetně místností v budově střelnice. Vedlejší klíč mají přiděleny ostatní interní osoby, díky kterému mohou otevřít hlavní bránu, vstupní branku, dveře budovy střelnice a vybrané vnitřní místnosti, jež nepodléhají omezení.

Příchod možných návštěv má na starosti vždy hlavní správce střelnice či ostatní správci, přičemž tato osoba není za návštěvu považována po vstupu na pozemek, ale až po příchodu do hlavní budovy střelnice, kde je takto označena pověřenou osobou. K návštěvám není vedena žádná evidenční kniha, kde by se zaznamenávala přítomnost těchto osob, a to z toho důvodu, že jejich pohyb v budově je omezen pouze na hlavní příchozí místnost, kde je návštěva pod dohledem vedoucího pracovníka. Takto je nakládáno i se zákazníky, kteří si jdou zakoupit zbraně, střelivo či ostatní nabízené příslušenství. Tyto osoby nemají oprávnění bez souhlasu pověřené osoby vstupovat do ostatních prostor střelnice.

Evidence členů střelnice či osob, které si rezervovaly střelecký stav, je vedena pomocí provozního deníku. Jedná se tedy o všechny osoby, které budou provádět střelbu. Provozní deník je vyplněn těmito osobami dle uvedeného záhlaví, které obsahuje:

- Datum střelby,
- Jméno a příjmení,
- Číslo zbrojního/osobního průkazu nebo datum narození,
- Podpis. (HABRESTO ARMS s.r.o., 2022)

Takto se do provozního deníku zapisují i správci střelnice, kteří jsou přítomni. Dokument lze tedy považovat za evidenci osob aktuálně se nacházejících v budově střelnice. Provozní deník je umístěn vždy u vstupního pultu, kde zasedá hlavní správce střelnice a jeho bezpečnost proti odcizení nebo zneužití dat či informací je zabezpečena pouze dozorem hlavního správce střelnice.

Samotné pracovníky střelnice, tedy hlavní a ostatní správce střelnice, lze identifikovat pomocí visačky. Tu jsou povinni nosit ihned po příchodu na pracoviště. Vzhledem k malé organizační struktuře společnosti se všichni pracovníci dobře znají. To je v případě, kdy je třeba identifikovat určité osoby v areálu, považováno za výhodu.

Vymezení doplňujícího opatření:

- Zaznamenávat datum a čas příchodu a odchodu všech návštěv.
- Vytvořit fyzickou záznamovou knihu, do které se budou zapisovat návštěvy nebo také elektronický auditní záznam všech přístupů.
- Vytvořit metodiku, pomocí které se budou kontrolovat a aktualizovat přístupová práva jednotlivých osob, které bude možno v případě potřeby zrušit.

7.1.3 Zabezpečení kanceláří, místností a vybavení

Komplexní zabezpečení místností v objektu je zajištěno pomocí bezpečnostního systému od společnosti Paradox. Při odchodu interních osob z budovy střelnice je pomocí kódovací klávesnice aktivována ochrana před vstupem neoprávněných osob. Kódy, za pomocí kterých je tento systém spuštěn, mají přiděleni všichni správci střelnice a údržbář, přičemž každá z těchto osob má stanoven svůj unikátní kód. Při zadání kódu dojde provozovateli střelnice pomocí SMS zprávy upozornění, které obsahuje informace o tom, kdo do objektu vstupuje, kdo systém aktivuje nebo také při případném narušení objektu

včetně určení konkrétní místnosti, ve kterých k narušení došlo. Celý zabezpečovací systém obsahuje několik prvků, z kterých je složen. Jedná se o hlavní řídící panel, kódovací klávesnici, komunikátor, bezdrátová čidla a zdroj napájení.

Obrázek 10 Kódovací klávesnice (vlastní)

Hlavní řídící panel propojený s čidly při narušení detekuje signál, který poté předá na zabudovaný komunikátor. Ten, jednak ve formě SMS zprávy, ale také pomocí zvukové signalizace, spouští alarm. Signalizační zařízení je zabudováno v zabezpečovacím systému. Bezpečnostní systém obsahuje také zabudovaný zdroj napájení, jehož součástí je také záložní baterie, jejíž činnost je zahájena při výpadku elektrické energie. Na obrázku č. 11 je vyobrazena hlavní řídící jednotka, obsahující také záložní zdroj elektrické energie, která je umístěna v trezorové místnosti.

Obrázek 11 Hlavní řídící jednotka (vlastní)

Vybrané místnosti střelnice jsou vybaveny pohybovými čidly od společnosti DAHUA TECHNOLOGY s.r.o., které jsou napojeny na zabezpečovací systém pomocí kabeláže umístěné ve stropních prostorách. Čidla jsou rozmístěna ve všech důležitých místnostech společnosti, které si za pomoci externího bezpečnostního technika zvolila vybraná společnost. Celkem jich je uvnitř celé budovy umístěno deset. Pohybová čidla fungují pomocí PIR senzorů, které detekují pohyb v okolí, kde je měřeno infračervené záření. V případě zaznamenání pohybu je vyslán signál do řídící jednotky, která následně spustí alarm.

Všechna okna jsou umístěna ve výšce 1,6 m. V hlavní místnosti jsou chráněna bezpečnostními skly Connex 6.6.2, kde se navíc jedná o okna špaletová. Na všech subjektem vybraných oknech jsou také umístěna otřesová čidla, která snímají možné vibrace, jež pomocí bezdrátového signálu vyrozumí řídící jednotku. Ta spouští alarm. Pokud některé z oken zůstane otevřené, zabezpečovací systém na tento fakt upozorní pověřenou osobu, která je povinna sjednat nápravu. I přesto, že tak neučiní, lze budovu zakódovat.

Subjekt pro ochranu informačních aktiv také využívá ocelový trezor umístěný v trezorové místnosti, do kterého jsou ukládána citlivá data a informace. Trezorové dveře dodané od společnosti JINOVA ČESKÉ TREZORY s.r.o. odpovídají bezpečnostní třídě 1 a normě

ČSN EN 114-1.K jejich otevření musí osoba znát číselný kód na instalovaný elektronický zámek a vlastnit příslušný klíč. Přístup do trezoru je umožněn všem správcům střelnice.

Obrázek 12 Trezorové dveře (vlastní)

Prostory střelnice jsou také opatřeny množstvím kamer instalovaných na vybraných strategických místech. Instalované kamery byly zakoupeny od stejné společnosti jako venkovní. Taktéž fungují na stejném principu a jejich záznam je ukládán pomocí softwarové aplikace zakoupené od této společnosti. Počet kamer, které monitorují budovu zevnitř, je dvacet dva.

Vymezení doplňujícího opatření:

- Není stanoveno.

7.1.4 Ochrana před vnějšími a přírodními hrozbami

Již z vymezeného bezpečnostního perimetru vyplývá, že ochrana před vnějšími hrozbami není dostatečně zajištěna. Špatný stav perimetrické ochrany je zcela zřetelný a pro potencionální pachatele je tak lehkou překážkou, kterou lze lehce překonat. Vniknutí na pozemek již bylo společností zaznamenáno. Neoprávněný vstup však nebyl zaznamenán

bezpečnostními prvky, ale místními obyvateli, kteří o této skutečnosti informovali provozovatele střelnice. Z hlediska eliminování potencionálních rizik je tedy nutné zlepšit tento nevyhovující stav zvýšením zabezpečovacích prvků.

V budově střelnice jsou umístěny na označených místech hasicí přístroje a dva vnitřní hydranty. Naproti budově je podle příslušné legislativy umístěna požární nádrž. Požární kontroly jsou v subjektu pravidelně a řádně plněny.

I když se subjekt nenachází v záplavovém území, již musel tomuto přírodnímu jevu čelit. Záplava prvního patra byla zapříčiněna silnými dešti, v důsledku čehož se přivalila voda, která se ze západní strany valila přímo ze zemědělských polí. Z tohoto důvodu je potřeba, aby subjekt disponoval technickými prostředky, které by dokázaly toto riziko eliminovat.

Vymezení doplňujícího opatření:

- Získat doporučení od specialisty, jenž se bude zabývat možnou záplavou.
- Na základě výše uvedeného doporučení aplikovat případná opatření.

7.1.5 Práce v zabezpečených oblastech

Místnosti, kde se nacházejí důležité informace, jsou v subjektu patřičně chráněny. Některé důležité informace a data se však nacházejí v zásuvce stolu hlavního správce střelnice, která není nijak zabezpečena.

Obrázek 13 Stůl hlavního správce
(vlastní)

Toto místo je vždy střeženo hlavním správcem střelnice a také pomocí kamerového systému. V době jeho nepřítomnosti nejsou ostatní osoby oprávněny manipulovat s těmito aktivy. Jsou pouze povinny zaznamenávat podezřelé situace. Ostatní důležité dokumenty bývají umístěny v ocelovém trezoru, který se nachází v trezorové místnosti, přičemž však pokud jsou užívány, mohou být umístěny i v zásuvce stolu. Pro práci v zabezpečených oblastech není vytvořena žádná dokumentace. Vše je dohodnuto pouze na základě ústní dohody.

Vymezení doplňujícího opatření:

- Zajistit lepší umístění dat a informací pro zvýšení jejich ochrany před nebezpečím.

7.1.6 Oblasti pro nakládku a vykládku

Příjem a výdej zboží je zajišťován externími firmami. Tyto firmy vjíždí do areálu hlavní bránou přes elektronickou závoru k hlavnímu vchodu střelnice, kde je zboží přebíráno. Vstup do budovy střelnice je těmto osobám zakázán. Zboží tak předají, popřípadě převezmou před hlavními dveřmi a areál opouštějí. Samotná nakládka a vykládka zboží je v kompetenci všech správců střelnice. Pracovníci jsou povinni stav a obsah zásilek ihned po převzetí zkontrolovat vizuálně i obsahově. Jsou také seznámeni s tím, že přijaté a vydávané zboží je umístěno ve skladu a trezorové místnosti odděleně, aby nedošlo k jeho záměně. V případě chybného dodání zboží ze strany dodavatelů, zprostředkovávaného externími firmami, je zboží vráceno zpět a reklamováno, popřípadě je distributor obeznámen s chybějícím počtem v obsahu zásilky. Reklamaci zboží má na starost pouze hlavní správce střelnice. Po kontrole je zboží zapsáno do skladového systému společnosti.

Vymezení doplňujícího opatření:

- Není stanoveno.

7.2 Zařízení

Z normy ČSN EN ISO/IEC 27002 (2014, str. 36) vyplývá, že hlavním cílem, který se týká vymezeného zařízení v subjektu, je *„zabránit ztrátě, poškození, odcizení nebo kompromitaci aktiv a přerušení provozu organizace“*. Níže tedy budou tato zařízení popsány z hlediska aktuálního stavu ve vymezeném subjektu.

7.2.1 Umístění zařízení a jeho ochrana

Za zařízení, obsahující citlivé informace a důležitý software, jsou společností označeny notebooky a služební mobilní telefon hlavního správce střelnice. Notebook provozovatele střelnice je umístěn v prostoru, hned za hlavními dveřmi v místě, kde zasedá, přičemž externí osoby do tohoto prostoru mají přístup zakázán. Jeho fyzické zabezpečení před krádeží či zneužitím je však zajištěno pouze střežením pomocí pracovníků střelnice, jež jsou povinni pozorovat neobvyklé chování osob v budově střelnice. Služební telefon nosí provozovatel vždy při sobě. Jeho odcizení je tak prakticky nemožné. Zařízení obsahující velké množství informací, je zabezpečeno pomocí základního šifrování. Správci střelnice si mohou pro pracovní účely donést své vlastní zařízení. Z těchto zařízení však mohou užívat pouze webové stránky střelnice, kde se nachází rezervační systém a také webový e-shop společnosti se zbraněmi, střelivem a ostatním příslušenstvím. Tato zařízení je povinen zkontrolovat hlavní správce střelnice.

Část prostoru hlavní místnosti budovy označované jako kuchyňka je určena ke konzumaci jídla a pití. U klíčových zařízení je konzumace potravin zakázána. Kouření je zakázáno v celém areálu.

Zařízení je umístěno na vyšším místě pro případ možné záplavy. Před požárem jsou citlivá data a informace umístěny v trezorové místnosti, která je opatřena nehořlavými dveřmi. Na střelnici je instalován hromosvod, který chrání budovu a zařízení před zásahem blesku nebo souvisejícími důsledky tohoto rizika. Přepěťová ochrana je zajištěna ve všech rozvaděčích pomocí proudových chráničů. Místa, kde může vzniknout nebezpečí související s výraznou změnou teploty či vlhkosti, jsou opatřena příslušnými bezpečnostními čidly, jež jsou napojeny na bezpečnostní systém Paradox.

Hlavní rozvodna elektrické energie je umístěna ve venkovním prostředí a je opatřena mechanickým zámkem, který ji částečně chrání před poškozením. Rozvodna bývá pravidelně kontrolována.

Vymezení doplňujícího opatření:

- Zajistit kvalitnější ochranu zařízení, která by vedla k zamezení neoprávněného přístupu cizím osobám pomocí technických prostředků.

7.2.2 Podpůrné služby

Přívod elektrické energie do střelnice zajišťuje hlavní rozvodna. Střelnice nevyužívá žádný zdroj nepřerušovaného napájení. V případě výpadku elektrické energie je datové připojení včetně kamerového systému neprovozuschopné. Pouze zabezpečovací systém od společnosti Paradox je po výpadku elektřiny funkční ještě několik hodin.

Na pozemku je k dispozici záložní zdroj vody v podobě studny, nicméně tato voda nevyhovuje požadavkům pro pití a je vhodná pouze pro průmyslové nebo jiné hospodářské účely. Pokud dojde k poruše vzduchotechniky, je střelnice neprovozuschopná, jelikož v této situaci není k dispozici náhradní varianta pro zajištění bezpečného provozu. Nouzové osvětlení se nachází na cedulích vyznačujících únikovou cestu. Svoji funkci je schopno plnit pomocí zabudovaných baterií po dobu šesti hodin. Vypínače a ventily pro odpojení elektrické energie, vody a přívodu tepla jsou umístěny v rozvodnách, které se nacházejí v šatně pro zaměstnance, skladu a v kotelně. Kontrola všech těchto zařízení, které podléhají revizím, je pravidelně prováděna dle zákonů a příslušných norem.

Vymezení doplňujícího opatření:

- Instalovat v subjektu záložní zdroj elektrické energie, který by zajišťoval provoz při výpadku elektrické energie z vnější sítě.

7.2.3 Bezpečnost kabelových rozvodů

Kabely od hlavní elektrické rozvodny umístěné ve venkovním prostředí, jsou do střelnice vedeny pod zemí. Veškerá kabeláž, na kterou jsou napojeny technické prostředky, je vybavena bezhalogenovými protipožárními dráty s požární odolností 60 minut a prochází stropními prostory, kromě kabelů umístěných v propojovacích chodbách, které jsou uložené v kabelových protipožárních žlabech. Ochrana kabeláže, která není umístěna ve stropních prostorech, je zajištěna pomocí kamerového systému. Kabely jsou také označeny v příslušném rozvaděči. Datová a síťová kabeláž je oddělená ve své vlastní liště. Přístup ke kabeláži v místě vstupu a výstupu u budovy je pod zemí a není žádným jiným způsobem chráněn. Kontroly zajišťující bezpečnost kabelových rozvodů jsou společností prováděny pravidelně dle stanovených intervalů.

Vymezení doplňujícího opatření:

- Není stanoveno.

7.2.4 Údržba zařízení

Zařízení je kontrolováno dle doporučení výrobce jen v místě k tomu určeném ve stanoveném období. Dokumentace obsahující záznam o pravidelných kontrolách je vedena externí firmou. Při vrácení zařízení z údržby jsou odpovědní pracovníci povinni provést kontrolu funkčnosti zařízení a také kontrolu, zda nebylo se zařízením nevhodně zacházeno.

Vymezení doplňujícího opatření:

- Vytvořit záznamovou knihu, v které se budou zapisovat veškeré preventivní kontroly, nápravné údržby či identifikované skutečnosti týkající se výskytu podezřelých i skutečných chyb.

7.2.5 Přemístění aktiv

Ostatní správci střelnice nemají oprávnění k tomu, aby jakkoliv přemísťovali aktiva společnosti. Jediný, kdo takto může činit, je hlavní správce střelnice, který však pracovní notebook zanechává v prostorách organizace a jediné zařízení, které je jím tedy přemísťováno je služební mobilní telefon.

Papírová forma informačních aktiv je umístěna v prostorách vybraného subjektu, ale nikdo z pracovníků není oprávněn tyto aktiva přemísťovat. Ve společnosti tak není zpracována žádná metodika, která by uváděla, jak s těmito aktivy zacházet mimo prostory organizace. V rámci užívání aktiv v organizaci jsou pracovníci obeznámeni s pravidly, jak s technickými zařízeními zacházet. Je tedy zakázáno stahovat jakýkoliv software, aplikace nebo soubory, které by mohly narušit bezpečnost počítače. Co se týče dat a informací v papírové podobě, interní osoby, vyjma provozovatele střelnice, nemají umožněno s těmito aktivy jakkoliv manipulovat. Fyzické uložení aktiv lze považovat za nedostatečné, neboť aktiva jsou umístěna v zásuvce stolu provozovatele, která není žádným způsobem zabezpečena, avšak přístup k ní mají ostatní pracovníci zakázán. V organizaci není zaveden žádný pravidelný interval školení týkající se přemisťování aktiv. Společnost má na všech počítačích nainstalovaný antivirový program ESET k ochraně aktiv.

Vymezení doplňujícího opatření:

- Není stanoveno.

7.2.6 Bezpečnost zařízení a aktiv mimo prostory organizace

Pro bezpečnost zařízení a aktiv mimo prostory organizace není zpracována žádná vnitřní norma. To je způsobeno tím, že technické vybavení, které správci střelnice využívají, není používáno mimo prostory organizace. Pracovníci střelnice tak vykonávají svoji práci na těchto zařízeních pouze v prostorách tohoto subjektu. Hlavní správce střelnice z externího prostředí využívá kancelářský software, konkrétně aplikaci Outlook, pomocí níž vyřizuje pracovní záležitosti. Dále si s sebou odnáší služební mobilní telefon, na kterém má nainstalovaný příslušný software, pomocí kterého sleduje aktuální bezpečnost střelnice. Hlavní správce uvádí, že je seznámen s možnými riziky a pravidly, jak v tomto prostředí pracovat a zacházet s těmito zařízeními.

Vymezení doplňujícího opatření:

- Není stanoveno.

7.2.7 Bezpečná likvidace nebo opakované použití zařízení

Všechna zařízení jsou společností využívána po celou dobu jejich funkčnosti. Pokud je však některé zařízení nevyhovující z hlediska jeho užívání, bývá vyřazeno. Všechna vyřazená zařízení jsou znehodnocena přímo v subjektu určenými pracovníky. Nevyhovující vybavení je zničeno za pomocí fyzické síly a příslušných nástrojů a následně je připraveno k ekologické likvidaci. Společnost neprodává žádné již nepotřebné zařízení, aby zabránila možnému zneužití citlivých informací a dat, které jsou v nich uloženy.

Vymezení doplňujícího opatření:

- Není stanoveno.

7.2.8 Neobsluhovaná uživatelská zařízení

Zařízení nejsou nijak fyzicky chráněna v době, kdy nejsou obsluhována. Přístup k nim není znemožněn, jsou volně dostupná. Tiskárna a skener nevyužívají možnosti kódování. Z notebooku je každý pracovník povinen se odhlásit, přičemž opětovné přihlášení vyžaduje znovu zadání přihlašovacího jméno a hesla uživatele. Uživatelé zařízení jsou pouze formálně poučeni o možných rizicích a jejich odpovědnostech. Vnitřní norma zde není zavedena.

Vymezení doplňujícího opatření:

- Zavést ve společnosti pravidelné školení pracovníků střelnice týkající se ochrany těchto zařízení.

7.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru

K užívání zařízení jsou všechny interní osoby proškoleny vstupním školením, které nemá opakovací charakter. Při dokončení jakékoliv činnosti na těchto zařízeních jsou povinni řádně ukončit požadovanou činnost, například odhlášením se ze zařízení. K tomu však není vytvořena žádná vnitřní směrnice. Informace a data v papírové formě jsou pracovníky ihned po vytištění odebrány a hlavním správcem střelnice uloženy v příslušné složce v zásuvce stolu. Tento stůl není opatřen zabezpečovacími prvky. Po skončení pracovní doby se nejdůležitější aktiva ukládají do ocelového trezoru umístěného v trezorové místnosti. Všichni pracovníci jsou poučeni o okamžitém ukládání zpracovaných citlivých informací či dat a jsou seznámeni s možnými riziky, která hrozí v případě zanechání těchto informací na volně přístupných místech v prostorách organizace.

Vymezení doplňujícího opatření:

- Zajistit, aby papírová forma aktiv společnosti byla ukládána na méně rizikové místo, které bude opatřeno zabezpečujícími prvky a prostředky.

8 SWOT ANALÝZA

Na základě posouzení stávajícího fyzického zabezpečení ve vymezeném subjektu v předchozí kapitole bude vytvořena SWOT analýza za účelem určení vhodných strategií pro oblasti subjektu. Po vytvoření analýzy bude vyhodnoceno, kde se tyto oblasti nacházejí.

Calicchio (2021) ve své publikaci uvádí, že se jedná o metodu vytvořenou v 60. až 70. letech 20. století na Stanfordské univerzitě, jejíž cílem bylo strategicky ohodnotit podnik či jeho projekt, v důsledku kterého by bylo ulehčeno učinit rozhodnutí, které by zajišťovalo dosažení požadovaného cíle.

Albert Humphrey je považován za autora této metody, který společně se svým týmem vymyslel postup, jak zajistit bezchybnost při plánování strategií u vymezených organizací. Tento postup je označován za techniku, kterou později nazval SWOT analýza, kde vymezil zásadní záměr, a to charakterizovat hlavní vnitřní a vnější faktory skládající se ze čtyř kvadrantů. (Sikorová, 2019)

Jedná se o souhrnnou techniku kvalitativního vyhodnocení, jež lze použít v kterékoliv sféře. Její název je odvozen ze začínajících anglických písmen, tedy:

- S – Strengths (silné stránky)
- W – Weaknesses (slabé stránky)
- O – Opportunities (příležitosti)
- T – Threats (hrozby) (Sedláček, 2015)

Tyto kategorie jsou dále rozřazeny na vnitřní a vnější prostředí, které hodnotí zkoumané faktory. Vnitřní prostředí zahrnuje silné a slabé stránky, vnější prostředí pak příležitosti a hrozby. (Sedláček, 2015)

Po charakterizování zkoumaných faktorů je sestavena hodnotící stupnice se specifikovaným rozmezím, pomocí které se určují v každém kvadrantu váhy, přičemž jejich hodnota je stanovena posudkem kompetentního experta. U slabých stránek a hrozeb je používáno záporné znaménko. Matice je považována za vyhodnocenou, jakmile je proveden součet všech kategorií, pomocí kterého se následně přiřadí odpovídající strategie. (Vaněk, Mikoláš, Žváková, 2012)

Pro stanovení potřebné a efektivní strategie je klíčové vzájemně propojovat hrozby a příležitosti spolu se silnými a slabými stránkami společnosti, v důsledku čehož se vytvářejí různé strategické varianty, které se následně hodnotí. Při adekvátně zvolené strategii jsou eliminovány slabé stránky a hrozby působící na organizaci, a naopak také využívány budoucí příležitosti a silné stránky. (Sedláček, 2015)

Pomocí identifikování vzájemného působení silných a slabých stránek na jedné straně a příležitostí a hrozeb na straně druhé, je možné identifikovat kvalitativní informace vedoucí ke čtyřem základním přístupům strategie. Jedná se o strategie označované jako:

- Strategie SO – pokud má společnost silné stránky propojeny s identifikovanými příležitostmi, je zvolena *„agresivně růstově orientovaná strategie“* označovaná jinými slovy jako strategie max – max.
- Strategie WO – jinak definovaná jako max – min, pomocí které je vyjádřeno zdolání slabých stránek tím, že budou maximálně zvýšeny příležitosti. Je vybrána v případech, kdy prostředí disponuje dostatečným množstvím příležitostí, ale i kvantitou slabých stránek.
- Strategie ST – při výběru strategie min – max je zásadní v dostatečném předstihu identifikovat hrozby za pomoci silných stránek. Jedná se tedy o strategii dosahující eliminace hrozeb a maximalizování silných stránek, jež je označována jako diverzifikační.
- Strategie WT – jedná se o strategii obranou pojmenovanou slovy min – min. Ta je vybrána v případě, kdy v subjektu převažují slabé stránky a hrozby, z čehož vyplývá nutnost jejich včasného eliminování. (Sedláček, 2015)

SWOT analýza bude sestavena dvakrát, a to jako analýza vnějšího prostředí a analýza vnitřního prostředí vymezeného subjektu, kde budou identifikovány silné stránky, slabé stránky, příležitosti a hrozby vycházející ze zkoumaného aktuálního stavu. Rozdělení analýz je stanoveno dle základních druhů ochrany objektů identifikovaných v teoretické části práce, přičemž tedy analýza vnějšího prostředí bude zahrnovat perimetrickou a plášťovou ochranu a analýza vnitřního prostředí se bude skládat z prostorové a předmětové ochrany.

8.1 SWOT analýza vnějšího prostředí

Pro zpracování analýzy vnějšího prostředí byly pomocí rozboru současného fyzického zabezpečení určeny potřebné části SWOT analýzy, které jsou nutné pro následující hodnocení. Níže je uvedena tabulka č. 1, která je vymezuje. Následující podkapitoly pak tyto faktory dále rozvádějí.

Tabulka 1 Stanovení faktorů vnějšího prostředí (vlastní)

INTERNÍ PROSTŘEDÍ	SILNÉ STRÁNKY	SLABÉ STRÁNKY
	Klidná lokalita	Oplocení
	Zabezpečení oken	Kamerový systém
	Bezpečnostní systém Paradox	Absence fyzické ostrahy areálu
	Finanční prostředky	Zajištění hlavní rozvodny elektrické energie
EXTERNÍ PROSTŘEDÍ	PŘÍLEŽITOSTI	HROZBY
	Zajištění dostatečného oplocení	Vandalismus
	Rozšíření kamerového systému	Vloupání
	Aplikace bezpečnostních prvků u vstupní brány	Neoprávněný pohyb osob v areálu
	Bezpečnostní agentura	Cílené odpojení elektrické energie

8.1.1 Silné stránky

Klidná lokalita – poloha vybraného subjektu na okraji obce zajišťuje nízkou fluktuaci lidí. To může vést k menší kriminalitě, jelikož umístění společnosti není pachatelům tak na očích. Je třeba ale mít na paměti, že klidná lokalita naopak některým potencionálním zlodějům může připadat dostupnější. Minimálně pro zajištění sledování pohybu osob ve společnosti je snížený počet lidí považován za kladný faktor.

Zabezpečení oken – výplň oken v klíčových místnostech je zajištěna bezpečnostními skly, jejichž odolnost snižuje možné narušení. Okna jsou navíc špaletová a jsou zabezpečena pomocí otřesových čidel.

Bezpečnostní systém Paradox – pomocí tohoto systému je zabezpečeno vniknutí osob do budovy střelnice. Jedná se o zabezpečení, díky jemuž jsou chráněny všechny přístupové

dveře a okna. Tyto prvky jsou chráněny pomocí čidel, které jsou napojeny na zabezpečovací systém Paradox.

Finanční prostředky – jsou důležité pro správu celého areálu, jehož rozloha je velká. Jako silnou stránku lze tedy považovat finanční prostředky, které je provozovatel střelnice ochoten poskytnout pro zlepšení stavu zabezpečení celého vnějšího perimetru a následně i celého areálu, včetně budovy střelnice.

8.1.2 Slabé stránky

Oplocení – plot, který se nachází okolo celého areálu, nesplňuje požadované zabezpečení. To vyplývá i z analýzy současného stavu uvedeného v kapitole 7.1.1, která navíc obsahuje i demonstrující fotografie. Ve stejné kapitole lze naleznout také podrobný popis stávajícího oplocení.

Kamerový systém – kamery ve vnějším prostředí jsou umístěny pouze u hlavní vstupní brány. Jedna se také nachází na budově střelnice u vchodových dveří. Počty kamer jsou však z hlediska zajištění bezpečnosti neadekvátní, neboť jejich pokrytí není zajištěno po celém areálu pozemku.

Absence fyzické ostrahy areálu – jako další slabou stránku vnějšího prostředí lze uvést absenci externí firmy (bezpečnostní agentury), která by mohla tak rozsáhlý areál střežit, čímž by se více eliminovalo riziko vniknutí neoprávněných osob na pozemek.

Zajištění hlavní rozvodny elektrické energie – toto zařízení, nacházející se ve vnějším prostředí, je chráněno pouze visacím zámkem. Nicméně tento bezpečnostní prvek je snadno zranitelný. Ochrana tohoto zařízení není zajištěna ani kamerovým systémem.

8.1.3 Příležitosti

Zajištění dostatečného oplocení – k tomu, aby nemohla být narušena bezpečnost střelnice či celého objektu, je nutné zakoupit a instalovat nové oplocení kolem celého perimetru. Realizace by vedla k minimalizaci hrozby vniknutí.

Rozšíření kamerového systému – tímto opatřením, za podmínky rozšíření stávajícího kamerového systému po celém areálu, by byl zprostředkován přenos záznamu z kamer na monitor umístěný v budově střelnice, kde by pracovníci měli možnost kontrolovat aktuální situaci na vymezeném území.

Aplikace bezpečnostních prvků u vstupní brány – ke zkvalitnění ochrany vstupní brány je navrhnuto zakoupení a následné provedení montáže technických prostředků, které by se zaměřovaly na řízenou kontrolu vstupu osob, čímž by se zvyšovala úroveň zabezpečení u hlavní vstupní brány.

Bezpečnostní agentura – v případě nesouhlasu společnosti se zakoupením zabezpečujících prvků, lze tato opatření nahradit prostřednictvím externích firem, a to konkrétně vybranou bezpečnostní agenturou, jejíž zaměstnanci by zastupovaly funkce technických prostředků. Ochraňovali by tak celý vymezený subjekt při pravidelných obchůzkách a hlídáním vstupu v časech provozní doby střelnice.

8.1.4 Hrozby

Vandalismus – z hlediska současného zabezpečení perimetru pozemku vyplývá, že u této hrozby existuje vysoká pravděpodobnost jejího vzniku. Potencionální vandalové by tak v důsledku nedostatečného zajištění perimetru mohli snadněji poškodit a odcizit majetek nacházejí se v areálu společnosti, ale i v samotné budově střelnice. Momentální stav oplocení není pro pachatele velkou překážkou, ale do budovy je značně ztížen její přístup, který zajišťuje zabezpečovací systém společnosti.

Vloupání – při překonání oplocení hrozí riziko vloupání, v jehož důsledku by společnosti bezpochyby vznikla škoda na majetku. Vloupáním je myšlený vstup neoprávněných osob do areálu společnosti či do budovy střelnice za překonání zabraňujících překážek, které jsou zastoupeny technickými prostředky subjektu. Zdolání těchto bariér následně umožňuje pachatelům odcizit, poškodit či znehodnotit aktiva společnosti.

Neoprávněný pohyb osob v areálu – v důsledku již výše charakterizovaných faktorů lze vyvodit, že i tato hrozba může narušit celkovou bezpečnost společnosti.

Cílené odpojení elektrické energie – při překonání mechanického zámku, který zabezpečuje hlavní rozvodnu elektrické energie, může nekompetentní osoba cíleně odpojit hlavní zdroj elektrické energie, jež zabezpečuje provoz střelnice. Z toho vyplývá, že při realizování této hrozby dojde k nezajištění dodávky elektrického proudu do budovy, což může vést až k uvedení střelnice mimo provoz.

Po identifikaci faktorů je nutné provést stanovení jejich vah a ohodnotit je. Hodnotící stupnice důležitosti je u silných stránek a příležitostí stanovena od 1 do 5, přičemž číslo 5 vyjadřuje největší prioritu. Slabé stránky a hrozby jsou hodnoceny pomocí stejné

stupnice, avšak jsou vyjádřeny zápornými čísly. Celková hodnota vah v každém z kvadrantů odpovídá po sečtení číslu 1. Zde také platí, čím větší je numerická hodnota váhy, tím více je hodnocený faktor pro organizaci klíčový. Ohodnocení těchto faktorů bylo zpracováno autorkou práce spolu se správci střelnice. Posouzení je zaznamenáno níže v přiložené tabulce.

Tabulka 2 Stanovení vah a hodnocení vnějšího prostředí (vlastní)

Interní prostředí	**Silné stránky**	**Váha**	**Hodnocení**	**Slabé stránky**	**Váha**	**Hodnocení**
	Klidná lokalita	0,1	2	Oplocení	0,5	–5
	Zabezpečení oken	0,2	3	Kamerový systém	0,2	–3
	Bezpečnostní systém Paradox	0,4	5	Absence fyzické ostrahy areálu	0,1	–2
	Finanční prostředky	0,3	3	Zajištění hlavní rozvodny	0,2	–4
Externí prostředí	**Příležitosti**	**Váha**	**Hodnocení**	**Hrozby**	**Váha**	**Hodnocení**
	Zajištění dostatečného oplocení	0,4	5	Vandalismus	0,1	–2
	Rozšíření kamerového systému	0,1	2	Vloupání	0,2	–3
	Aplikace bezpečnostních prvků u vstupní brány	0,4	5	Neoprávněný pohyb osob v areálu	0,4	–5
	Bezpečnostní agentura	0,1	2	Cílené odpojení elektrické energie	0,3	–4

8.1.5 Stanovení celkového výsledku SWOT analýzy a určení strategie vnějšího prostředí

Po sestavení ohodnocení a přiřazení příslušných vah je důležité také stanovit celkový výpočet, který povede k určení příslušné strategie. Výpočet stanovených faktorů se provede vynásobením definovaných vah a ohodnocením důležitosti. Výpočet tedy bude vypadat následovně:

$$f_1, f_2, f_x, \ldots = \text{váha x hodnocení}$$

Součin těchto čísel u všech faktorů se poté sečte, na základě čehož je znám výsledek jednotlivých kvadrantů SWOT analýzy. Sečtení bude provedeno pomocí níže uvedeného vzorce:

$$S, W, O, T = f_1 + f_2 + f_x + \ldots$$

Výpočet jednotlivých kvadrantů je zaznamenán v přiložené tabulce č. 3.

Tabulka 3 Součet všech kvadrantů vnějšího prostředí (vlastní)

Výsledek silné stránky	0,2 + 0,6 + 2,0 + 0,9 = **3,7**
Výsledek slabé stránky	(-2,5) + (-0,6) + (-0,2) + (-0,8) = **–4,1**
Výsledek příležitosti	2,0 + 0,2 + 2,0 + 0,2 = **4,4**
Výsledek hrozby	(-0,2) + (-0,6) + (-2,0) + (-1,2) = **–4,0**

Následně bude sečteno zvlášť interní a externí prostředí SWOT analýzy, a to součtem silných a slabých stránek a následně také součtem příležitostí a hrozeb pomocí vzorce:

$$IP = S + W$$

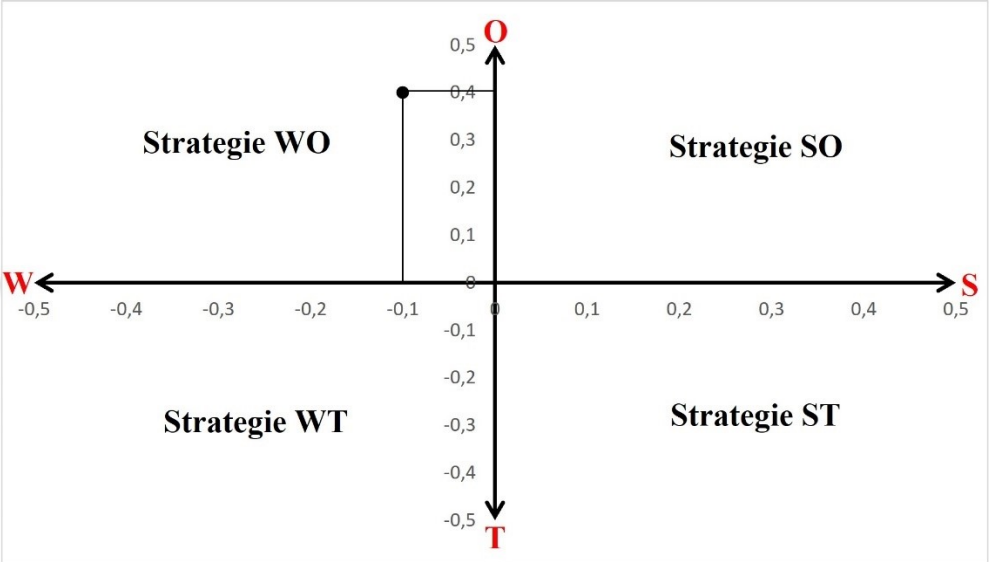
$$EP = O + T$$

Výsledek součtu, který je zaznamenán v tabulce č. 4, je vyjádřen zkratky IP (interní prostředí) a EP (externí prostředí).

Tabulka 4 Výsledek součtu IP a EP vnějšího prostředí (vlastní)

IP	3,7 + (–4,1) = **–0,1**
EP	4,4 + (–4,0) = **0,4**

Na základě stanovení tohoto výpočtu byl vytvořen obrázek č. 14 s grafem, podle kterého je vybrána strategie WO, jež se vyznačuje tím, že stanovené příležitosti se pokusí maximalizovat, aby byly co nejvíce potlačeny slabé stránky společnosti, které jsou pro podnik nepříznivé.



Obrázek 14 Vybraná strategie vnějšího prostředí (vlastní)

8.2 SWOT analýza vnitřního prostředí

Analýza vnitřního prostředí byla zpracována totožně jako ta předchozí. Za vnitřní prostředí jsou považovány veškeré prostory a aktiva nacházející se uvnitř budovy společnosti. V tabulce č. 5 je uvedena SWOT analýza tohoto prostředí. Následující podkapitoly budou blíže specifikovat stanovené prvky.

Tabulka 5 Stanovení faktorů vnitřního prostředí (vlastní)

INTERNÍ PROSTŘEDÍ	SILNÉ STRÁNKY	SLABÉ STRÁNKY
	Pohybová a otřesová čidla	Absence EPS
	Vstup osob do budovy	Uložení dokumentů
	Kvantita dveří	Ochrana serverů
	Trezorová místnost	Nedostatečná ochrana zařízení
EXTERNÍ PROSTŘEDÍ	PŘÍLEŽITOSTI	HROZBY
	Nákup trezoru pro uchování dokumentů	Krádež
	Zakoupení a připojení EPS	Sabotáž
	Posílení ochrany serveru	Požár
	Investice do bezpečnostních komponentů pro vybraná zařízení	Nefunkčnost bezpečnostního systému Paradox

8.2.1 Silné stránky

Pohybová a otřesová čidla – jsou společností využívány ve všech prostorách budovy k detekci nežádoucího narušení. Tato čidla jsou napojena na zabezpečovací systém a samotný podnik jej specifikuje jako účinnou a plnohodnotnou ochranu.

Vstup osob do budovy – vstup je řízen pomocí elektronického dveřního zámku, tzn. že do objektu střelnice se dostanou pouze ty osoby, které správci střelnice vpustí. Tímto opatřením je eliminováno riziko neoprávněného vstupu cizích osob.

Kvantita dveří – počet dveří v prostorách organizace je považován za významný faktor při průniku cizích osob. Všechny dveře jsou po skončení pracovní doby zamknuty, a tím se zvyšuje ochrana před pohybem nekompetentních osob, které tak mají v důsledku toho ztížený přístup do kterýchkoliv místností.

Trezorová místnost – ve společnosti je zavedena k uložení patřičné dokumentace, ve které se nacházejí strategické informace a data, jejichž ochrana je pro subjekt zásadní z hlediska zabezpečení těchto aktiv.

8.2.2 Slabé stránky

Absence EPS – podle autorky práce je absence elektronického požárního systému nedostatkem, který lze označit za riziko, jež by mohlo způsobit škody na majetku společnosti. V důsledku tohoto tvrzení lze říci, že vybraný subjekt není schopen včasně detekovat a signalizovat vznik možného požáru. Při absenci EPS se tak požár může rychle šířit a způsobit ještě větší ztráty, v důsledku čehož by se společnost mohla dostat až do existenčních problémů.

Uložení dokumentů – neuvážené zakládání dokumentace do nezabezpečené zásuvky stolu hlavního správce střelnice v průběhu pracovní doby je definováno jako nedostatek, který lze zařadit do slabých stránek společnosti. Hlavní slabinou tohoto faktoru je snadné odcizení uložených aktiv ve formě informací a dat, která jsou pro společnost zásadní, a proto je třeba toto nebezpečí zajistit či odstranit.

Ochrana serveru – serverovna se nachází na dámských toaletách a její hlavní řídící prvky jsou opatřeny bezpečnostní schránkou, ve které se tento řídící prvek nachází. Vybrané zabezpečení je dodáváno přímo od výrobce tohoto serveru. Schránka, opatřená mechanickým zámkem, je však lehce překonatelná pouhým vypáčením dvířek a její

umístění je potencionálnímu pachateli snadno dostupné. Pro zvýšení bezpečnosti je třeba tento fakt umístit do slabých stránek.

Nedostatečná ochrana zařízení – jedná se o technické zařízení, zejména služební notebooky, které nedisponují žádným fyzicky zabraňujícím prvkem, který by zamezil snadnému odcizení zařízení. Je tak třeba se na tento faktor zaměřit a zajistit dostatečnou ochranu veškerého klíčového zařízení.

8.2.3 Příležitosti

Nákup trezoru pro uchování dokumentů – pro bezpečné uchování strategické dokumentace je potřebné, aby společnost zakoupila trezor, do kterého by se tyto dokumenty ukládaly. Společnost sice vlastní jeden ocelový trezor, který je umístěný v trezorové místnosti, avšak jeho velikost neodpovídá potřebám vybraného subjektu.

Zakoupení a připojení EPS – zákony subjektu nepřikazují tento systém používat, ale jeho využití by umožnilo společnosti včasné odhalení vzniku požáru díky signalizačním zařízením, spuštění alarmu nebo automatickému spuštění bezpečnostních prvků pro potlačení požáru. Instalováním EPS a jeho propojením se stávajícím bezpečnostním systémem Paradox by subjekt výrazně eliminoval možná požární rizika a zvýšil by tak bezpečnost své organizace.

Posílení ochrany serveru – z výše uvedeného popisu slabých stránek společnosti vyplývá, že hlavní server společnosti není dostatečně chráněn. I když je opatřen bezpečnostní schránkou a připevněn ke stropním panelům, nachází se v místnosti bez kamerového systému. Pro zvýšení jeho bezpečnosti by bylo vhodné jej celý spolu s bezpečnostní schránkou umístit do police skříně vybavené mechanickým zámkem. Na samotnou bezpečnostní schránku lze také zakoupit magnetické senzory, které by bylo možno napojit na stávající bezpečnostní systém. Tímto by bylo zajištěno posílení ochrany serveru.

Investice do bezpečnostních komponentů pro vybraná zařízení – při nákupu a následné instalaci těchto prvků na vybraná zařízení, jimiž se v tomto případě myslí převážně pracovní notebooky, se zajistí jejich zabezpečení před hrozbou krádeže či neoprávněné manipulace. Implementace ochranných opatření tak dokáže snížit neočekávanou hrozbou.

8.2.4 Hrozby

Krádež – hrozba krádeže klíčových informací, dat a zařízení byla zpozorována autorkou práce na základě analýzy slabých stránek. Pokud není zabezpečení těchto aktiv v budově

střelnice dostatečné, existuje vysoká pravděpodobnost, že potenciální zloděj bude schopen tato aktiva snadno odcizit.

Sabotáž – tato riziková situace hrozí jak od interních, tak externích osob. Sabotáží se v tomto případě rozumí fyzické poškozování majetku společnosti, které je úmyslné a narušuje tak její chod.

Požár – hrozba požáru je v budově střelnice vysoká. Jak již bylo zmíněno, společnost nevlastní automatický systém, který by ji na tuto skutečnost upozornil. V budově se sice nacházejí vnitřní požární hydranty a hasicí přístroje, ale ty jsou potřeba až v případě detekování této hrozby.

Nefunkčnost bezpečnostního systému Paradox – v případě vzniku této hrozby dojde ke snížení bezpečnosti vnitřních prostor, jelikož většina zabezpečovacích opatření, realizovaných za pomoci technických prostředků, je propojena s tímto bezpečnostním systémem.

Jako u vnějšího prostředí, budou nyní jednotlivé faktory ohodnoceny pomocí již vymezených stupnic. Toto hodnocení je zaznamenáno v tabulce č. 6 níže.

Tabulka 6 Stanovení vah a hodnocení vnitřního prostředí (vlastní)

Interní prostředí	**Silné stránky**	**Váha**	**Hodnocení**	**Slabé stránky**	**Váha**	**Hodnocení**
	Pohybová a otřesová čidla	0,4	5	Absence EPS	0,1	–2
	Vstup osob do budovy	0,3	4	Uložení dokumentů	0,3	–4
	Kvantita dveří	0,1	2	Ochrana serveru	0,3	–4
	Trezorová místnost	0,2	3	Nedostatečná ochrana zařízení	0,3	–4
Externí prostředí	**Příležitosti**	**Váha**	**Hodnocení**	**Hrozby**	**Váha**	**Hodnocení**
	Nákup trezoru pro uchování dokumentů	0,3	4	Krádež	0,2	–3
	Zakoupení a připojení EPS	0,1	2	Sabotáž	0,1	–2
	Posílení ochrany serveru	0,2	3	Požár	0,2	–3
	Investice do bezpečnostních komponentů pro vybraná zařízení	0,4	5	Nefunkčnost bezpečnostního systému Paradox	0,5	–5

8.2.5 Stanovení celkového výsledku SWOT analýzy a určení strategie vnitřního prostředí

Výpočet SWOT analýzy bude proveden za pomoci již dříve sestaveného vzorce, tedy součinem jednotlivých vah a hodnocení u identifikovaných faktorů. Po tomto kroku je nutné také sečíst jednotlivé kvadranty, což je znázorněno níže.

Tabulka 7 Součet všech kvadrantů vnitřního prostředí (vlastní)

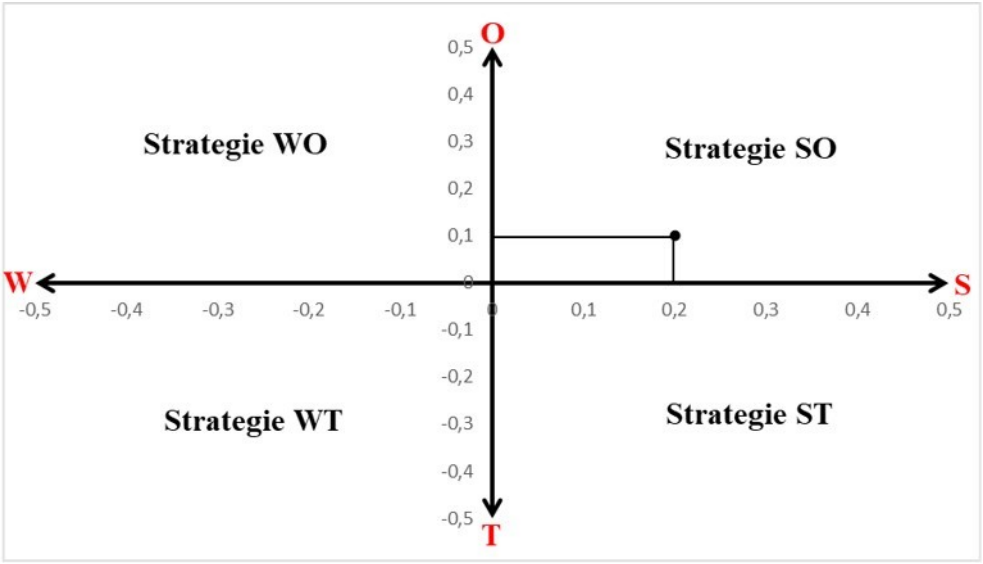
Výsledek silné stránky	2,0 + 1,2 + 0,2 + 0,6 = **4,0**
Výsledek slabé stránky	(-0,2) + (-1,2) + (-1,2) + (-1,2) = **–3,8**
Výsledek příležitosti	1,2 + 0,2 + 0,6 + 2,0 = **4,0**
Výsledek hrozby	(-0,6) + (-0,2) + (-0,6) + (-2,5) = **–3,9**

Pro určení vhodné strategie společnosti je nutné sečíst interní prostředí a externí prostředí, jež je označováno pomocí stejné zkratky jako u analýzy vnějšího prostředí.

Tabulka 8 Výsledek součtu IP a EP
vnitřního prostředí (vlastní)

IP	4,0 + (–3,8) = **0,2**
EP	4,0 + (–3,9) = **0,1**

Po výpočtu, uvedeného v tabulce č. 8, autorka práce vytvořila graf pomocí zanesení příslušných hodnot, z kterého bude určena odpovídající strategie.



Obrázek 15 Vybraná strategie vnitřního prostředí (vlastní)

Z vytvořeného grafu na obrázku č. 15 byla určena agresivně růstově orientovaná strategie, jež se zaměřuje na využití identifikovaných silný stránek v rámci uvedených příležitostí. Ty by měla společnost aplikovat v případě, že se bude tímto plánem řídit, aby bylo dosaženo kvalitního zabezpečení subjektu.

9 NÁVRH NA ZABEZPEČENÍ ŘÍZENÉHO VSTUPU OSOB

Tato kapitola diplomové práce se v počátku bude zabývat vyhodnocením výše vytvořených analýz, kde bude navrženo opatření, které je třeba zajistit pro zvýšení informační bezpečnosti z hlediska fyzické bezpečnosti.

Na základě toho bude vytvořen model, který bude znázorňovat kroky vedoucí k zajištění řízeného vstupu osob. Model bude obsahovat také jednotlivé přístupy osob. Z navrženého modelu budou vycházet možné varianty na zabezpečení, které budou následně popsány. Ty budou dále vyhodnoceny pomocí multikriteriálního hodnocení. U identifikované optimální varianty bude vytvořena cenová nabídka, která bude následně ověřena provozovatelem střelnice a příslušným odborným pracovníkem.

9.1 Vyhodnocení analýz

Po analyzování současného stavu fyzické bezpečnosti, týkajícího se ochrany informačních aktiv, jsou identifikována nebezpečí, která mohou nejvíce ohrozit vybraný subjekt. Při prozkoumání fyzického bezpečnostního perimetru a fyzických kontrol vstupu bylo stanoveno nejvíce doplňujících opatření, které je třeba implementovat pro zajištění standardů, jež vyplývají z vybrané ISO normy. U dalších podskupin spadajících do zabezpečených oblastí je identifikováno jen menší množství těchto opatření. Pokud by však společnost eliminovala rizika nacházející se na samotném perimetru pozemku, tak je vysoká pravděpodobnost, že by neoprávněné osoby měly více znesnadněný přístup do dalších prostor. Je tedy důležité zaměřit se na správnou oblast, která by nejvíce napomohla k ochraně informačních aktiv a celkovému zajištění stavu bezpečnosti.

Zařízení zahrnovala druhou hlavní skupinu, která byla analyzována. Z té byly zjištěny nedostatky týkající se umístění informačních aktiv. Je tedy třeba přijmout vhodná opatření, pomocí kterých by společnost dosáhla kvalitnějšího ukládání dokumentace obsahující strategické informace a data. Implementace by mohla být realizována nákupem a instalací technických prostředků v podobě trezorů, do kterých by byly dokumenty ukládány a zároveň by tak byla zachována jejich nedotknutelnost pro přístup ze strany cizích osob.

Zpracovaná SWOT analýza vnějšího prostředí přináší výběr WO strategie znamenající převahu slabých stránek a dostupných příležitostí. V důsledku toho je patrné, že je třeba na co nejmenší možnou míru snížit faktory nacházející se v kvadrantu slabých stránek, kterých bude dosaženo vhodným využitím příležitostí, jež má společnost k dispozici.

Konkrétně je tedy třeba zakoupit nebo zásadně opravit stávající oplocení, vyřešit otázku zajištění vstupu osob do areálu, rozšířit stávající kamerový systém a pomocí technických prostředků lépe zabezpečit hlavní rozvodnu elektrické energie.

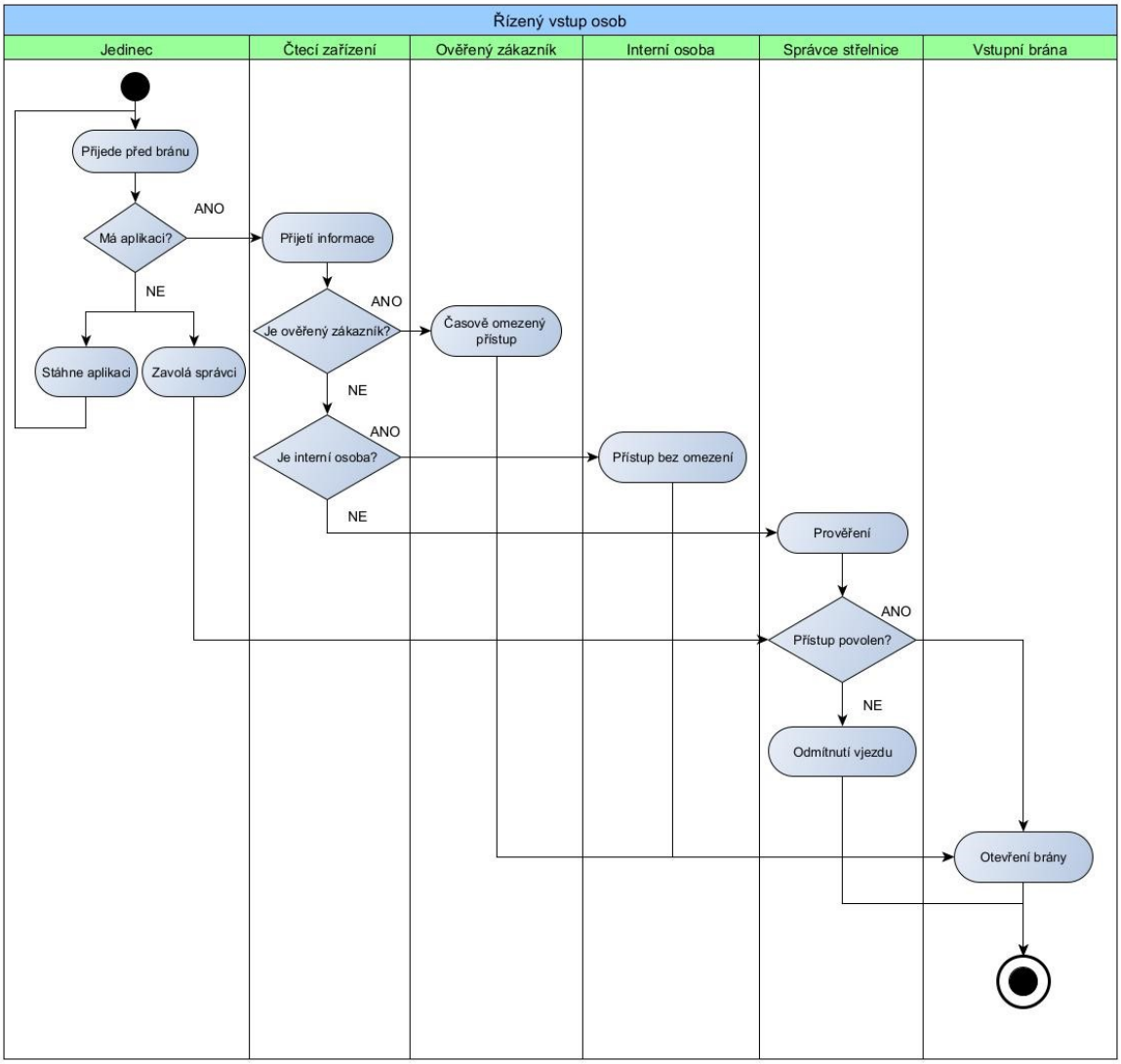
SWOT analýza vnitřního prostředí identifikovala strategii SO, u které je třeba využít předností silných stránek, které za pomoci příležitostí mohou pozvednout kvalitu bezpečí. Za nejsilnější faktory, vycházející ze silných stránek, byla určena pohybová a otřesová čidla spolu se vstupem osob do budovy. Tyto silné stránky je tedy třeba rozšířit o příležitost v podobě investice do bezpečnostních komponentů, což bude pro společnost představovat ještě větší ochranu informačních aktiv a zamezení vstupu neoprávněných osob. V případě, že by společnost nemohla již tyto faktory dále rozšířit, měla by se zaměřit na širší okruh zabezpečení, jenž je uveden v analýze vnějšího prostředí, a to na perimetrickou ochranu.

Na základě tohoto vyhodnocení se autorka práce rozhodla zaměřit na perimetrickou ochranu, konkrétně na řízený vstup osob do areálu, který z hlediska zajištění ochrany informačních aktiv vyhodnotila jako nejzranitelnější. Jedná se o nejvíce rizikové místo, jež ve vybraném subjektu může zásadně ohrozit bezpečnost a v důsledku toho vyvolat škodu. Společnost tento faktor doposud zajišťuje pouze pomocí brány a elektronické závory. Oba tyto prostředky jsou však v době přítomnosti interních osob otevřeny. Při nedostatečném zajištění tohoto rizika je vysoká pravděpodobnost jeho vzniku plynoucího z nezabezpečeného přístupu osob do areálu. Je tedy důležité stanovit a aplikovat patřičná opatření, jež budou toto nebezpečí eliminovat. Autorka se tak pokusí navrhnout vhodné varianty, jak dosáhnout uspokojivého stavu pro snížení tohoto rizika dle možností a specifikací vybrané společnosti.

9.2 Modelování přístupového diagramu

Na základě předchozí kapitoly, kde se autorka práce rozhodla pro navrhnutí opatření týkající se zabezpečení řízeného vstupu osob, bude tato část definovat jednotlivé kroky, jak ochranu vstupu zajistit.

Nepostradatelnou součástí je stanovit si jednotlivé činnosti, pomocí kterých bude tento řízený vstup koordinován. Z tohoto důvodu byl vytvořen algoritmus konkrétních fází, který bude znázorněn pomocí vývojového diagramu.



Obrázek 16 Vývojový diagram (vlastní)

Vývojový diagram uvedený na obrázku č. 16 byl zpracován v programu yED Graph Editor a popisuje, jak by měl budoucí technický prostředek, zajišťující řízený vstup osob, principiálně fungovat. V tomto případě je počítáno s tím, že vybraná technologie, zabezpečující stanovené opatření, bude složena ze zařízení obsahujícího vybraný software, pomocí kterého bude vykonávat svoji činnost. Zařízení bude řízeno na dálku pomocí počítačového programu.

Níže budou charakterizovány jednotlivé entity obsažené v uvedeném modelu. Počátek tohoto modelu označuje příjezd osoby (jedince) před hlavní bránu areálu střelnice, kde bude umístěna vybraná technologie.

Jedinec

Jedná se o každou osobu, která chce vstoupit na pozemek střelnice. Aby však mohl jedinec do areálu vstoupit musí mít nainstalovanou požadovanou aplikaci, přes kterou se propojí s čtecím zařízením u vstupní brány. O této skutečnosti se osoba bude moci dozvědět také z informační cedule situované u vstupní brány, nebo také při online rezervaci stavu střelnice na internetových stránkách společnosti. Pro případ, kdy si zákazník pojede pouze pro předem objednané zboží, bude upozorněn na tento fakt hlavním správcem střelnice, protože vyzvednutí objednávky je možné pouze po předchozí telefonické domluvě. I přes to, že aplikaci člověk nemá, může zavolat na uvedené telefonní číslo na informační tabuli, které ho odkáže na správce střelnice, jež mu přístup na základě posouzení umožní nebo zamítnou. Při povolení vjezdu osob do areálu, budou však pověření pracovníci povinni kontrolovat jejich pohyb.

Čtecí zařízení

Popisuje zařízení, které bude přijímat informace od vstupujících osob. Hlavní funkcí pak bude ověření oprávnění u osob vstupujících do areálu střelnice. Čtecí zařízení musí být propojeno s nainstalovanou aplikací na mobilním telefonu osob. Pomocí toho vybraná technologie ověří identitu osoby a umožní jí vstup. Regulace vstupu osob na střelnici bude zahrnovat dva přístupy, a to přístup s omezením u ověřeného zákazníka a přístup bez omezení u interních osob.

Ověřený zákazník

Tato skupina zahrnuje stálé a ověřené zákazníky střelnice, kteří mají umožněn přístup s omezením. Osoby tak budou mít povoleno vstoupit na pozemek subjektu až po schválení a začlenění hlavním správcem střelnice do tohoto přístupu. Regulace vstupu osob by u ověřených zákazníků také zahrnovala omezení na určené dny a hodiny, kdy by jedinci měli povoleno do areálu vstupovat. Rozmezí tohoto časového úseku se bude odvíjet od stanovené otevírací doby střelnice. Přístup s omezením by měl stanovená také určitá pravidla. Autorka práce tyto pravidla charakterizovala následovně:

- Po otevření vstupní brány jste oprávněn jet pouze k budově střelnice.
- Nevstupujte na zakázaná místa označená výstražnými cedulemi.
- Zbytečně se nezdržujte na pozemku areálu.

- Je zakázáno vypůjčit nebo přenechat mobilní zařízení s povoleným přístupem jiné osobě než té, které je to umožněno.
- V případě ztráty mobilního zařízení kontaktujte hlavního správce střelnice.
- Je zakázáno navštěvovat areál střelnice mimo vymezenou otevírací dobu.
- Při porušení pravidel hrozí pokuta a odepření přístupu.

Pokud by osoba některé z výše uvedených pravidel porušila, tak jí hlavní správce střelnice přístup s omezením deaktivuje, a také by jí mohl udělit pokutu.

Interní osoba

Interní osoby, kterými se myslí všichni správci střelnice, údržbář a majitel pozemku, by se zařazovali do přístupu bez omezení. Ten by umožnoval vstup do areálu společnosti kdykoliv, i mimo otevírací dobu.

Správce střelnice

Tato skupina zahrnuje veškeré správce střelnice, kteří budou odpovědní za regulaci vstupu osob do areálu a také za řešení případných problémů s aplikací nebo čtecím zařízením.

Vstupní brána

Tato entita zahrnuje elektronickou bránu, která je instalovaná k ovládání vstupu a výstupu osob z areálu střelnice. Brána je propojena a přijímá informace ze čtecího zařízení, které ověřuje identitu osob. Brána může být otevřena také samotnými správci střelnice na dálku, kteří vstup příslušné osobě schválí.

Všechny výše uvedené jednotlivé kroky autorka sestavila za pomoci správců střelnice, jež jí poskytli informace o tom, jaká mají kritéria pro zakoupení technologického zařízení, které by splňovalo jejich požadavky na zajištění řízené kontroly vstupu.

Namodelovaný diagram prezentuje návrh algoritmu budoucího zařízení, které by zabezpečovalo řízený vstup osob do areálu společnosti. Při aplikování tohoto opatření se jednoznačně zvýší úroveň zabezpečení vybraného subjektu, a to tím, že pohyb osob v areálu bude regulován a povolen jen určeným osobám. Na základě těchto faktů bude analyzována vhodná technologie.

9.3 Varianty zabezpečení objektu

K tomu, aby mohly být určeny nejvíce vhodné varianty na zabezpečení perimetrické ochrany, je žádoucí identifikovat všechna požadovaná kritéria. Provozovatel společnosti se formulováním jeho požadavků podílel na tvorbě vývojového diagramu znázorněného v předchozí kapitole. Dle jeho subjektivního názoru je vytvořený algoritmus s několika přístupy dostatečný a plně odpovídá jeho představám. Autorka práce tak dále navrhne varianty na zabezpečení řízeného vstupu od několika firem, které zvolí na základě průzkumu aktuálních možností na trhu. Ty následně posoudí pomocí multikriteriálního hodnocení.

Níže uvedené varianty budou sestaveny z vybraných interkomů a čtecích zařízení, které jsou klíčové pro zajištění kontrolovaného přístupu osob. Jejich výběr byl sestaven po kontaktování několika firem zabývajících se řízeným přístupem osob, které autorce práce na základě jejich požadavků pomohly s výběrem. Většina internetových e-shopů v tomto odvětví také nabízí nakonfigurovat si zařízení dle stanovených požadavků.

Varianta č. 1

První možností je instalace RFID čtečky ARCS-CQ/BT vyrobené od francouzské společnosti STiD, která je kompatibilní pro čtení karet, čipů či QR kódů. Používá nejvyšší stupeň zabezpečení (uznávaný standard EAL úrovně 5+) a lze ji propojit s NFC technologiemi a s mobilním telefonem za pomocí Bluetooth. Čtečka je vybavena dotykovým displejem, pomocí kterého lze různě kombinovat a násobit identifikaci uživatelů. Jedná se o dvojitou identifikaci, kdy je třeba pro povolení přístupu osob do areálu zadat např. identifikační kartu + pin kód nebo také přiložit čip a zadat QR kód. Pomocí vybraného způsobu užívání zabezpečení lze také oddělit interní osoby od ostatních. Toto zařízení je vhodné také při používání mobilní aplikace STiD Mobile ID, která disponuje 6 možnými režimy, jež může provozovatel střelnice přidělovat. Každý režim je specifický v přikládání mobilního zařízení k vybrané čtečce. (STiD, © 2021)

Na obrázku č. 17 níže je znázorněno čtecí zařízení popisované pro variantu č. 1.

Obrázek 17 ARCS-CQ/BT
(STiD, © 2021)

Varianta č. 2

Jedná se o zařízení od společnosti 2N Telekomunikace a.s., která se zaměřuje na vývoj a výrobu prostředků a informačních a komunikačních technologií pro fyzickou bezpečnost. Konkrétně jde tedy o bezpečnostní interkom2N® IP VERSO, který by obsahoval také vstupní čtečku 2N® Access Unit. Toto zařízení lze nakonfigurovat dle potřeb zákazníka pomocí kompatibilních modulů a dalších příslušenství. Výběrem licence se určuje, kolik osob bude zařízení možno užívat, přičemž lze zvolit i variantu neomezeného počtu uživatelů. Interkom obsahuje také kameru s nočním viděním, která je v zařízení umístěna tak, aby byla na první pohled skryta. K interkomu lze také připojit stávající kamerový systém, jež bude zabezpečovat slepá místa. Lze ho tedy spárovat se současným bezpečnostním systémem Paradox. Další možností je také instalace libovolného počtu tlačítek pro volání a dálkovou komunikaci se správci střelnice. Při vybrání vhodného modulu lze umožnit osobám přístup mimo jiné také pomocí mobilní aplikace 2N® Mobile Key, která disponuje několika přístupy a je pro uživatele ke stažení zcela zdarma. K tomuto prostředku je možno také integrovat výstupní čtečku, která by osobám umožnila po přiložení mobilního zařízení areál střelnice opustit. Veškerá zařízení od této společnosti má pod správou aplikace 2N® Access Commander (2N Telekomunikace, © 2023)

Základní potřebné zařízení, které by zabezpečovalo spolu se čtecím zařízením řízený vstup osob, je uvedeno na obrázku č. 18, a to konkrétně bezpečnostní interkom.

Obrázek 18 2N® IP VERSO
(2N Telekomunikace, © 2023)

Obrázek č. 18 znázorňuje bezpečnostní interkom s kamerou a možností volání. Další uvedený obrázek, označen č. 19 uvádí, jak vypadá konkrétní čtecí zařízení instalované v tomto interkomu.

Obrázek 19 2N® Access Unit
(2N Telekomunikace, © 2023)

Varianta č. 3

Třetí vybrané čtecí zařízení je Datalogic Gryphon GFE4400 s rozhraním RS232, pomocí kterého jsou přenášena data ze čtecího zařízení na příslušný počítač. Toto zařízení od společnosti Datalogic S.p.A je zabudováno do vstupního sloupku, který může být dále opatřen interkomem, dle přání zákazníků. Zařízení je schopno číst různé 1D a 2D kódy, poštovní nebo také složené kódy a je navrženo tak, aby mohlo tyto kódy přesně snímat při tolerovaném pohybu, což je důležité při využití mobilních zařízení, které disponují požadovanou aplikací pro QR kódy. Po instalaci zařízení je možné jej hned používat.

Skládá se z materiálu, který je odolný vůči dezinfekčním prostředkům a roztokům. A to z toho důvodu, aby mohlo být provedeno jeho pravidelné čištění. Zároveň je také opatřen těsnícím krytem, jež zajišťuje ochranu proti vodě. Snadno také dokáže dešifrovat vadné či špatné kódy. Čtecí zařízení je vybaveno patentovanou technologií označovanou jako zelený bod, kterou vytvořila výše uvedená společnost. Po správném načtení vygenerovaného kódu, jež je spravován v rámci webového uživatelského rozhraní, se rozsvítí zelená kontrolka, která označuje správné načtení kódu. (Datalogic S.p.A., © 2012-2020; Datalogic ADC, Inc., © 2012-2015)

Na obrázku č. 20 je vyobrazeno konkrétní čtecí zařízení specifikované v této variantě.

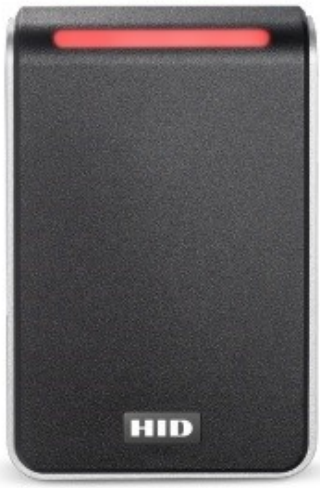
Obrázek 20 Datalogic Gryphon GFE4400
(Datalogic ADC, Inc., © 2012-2015)

Varianta č.4

Čtecí zařízení HID® Signo™ Reader S40 vyrábí spolčenost HID Global. Toto zařízení je specializováno na identifikaci osob pomocí RFID technologie. Její princip spočívá v přiložení odpovídajícího prvku (karty, klíče, čipy, atp.) k tomuto čtecímu zařízení, které provede verifikaci uživatele. Mimo výše uvedené prvky lze také k zařízení přiložit mobilním telefon, jenž obsahuje aplikaci HID Mobile Access, kterou osoba užívá jako ověřovací identifikátor. Mobilní aplikace po připojení s Bluetooth se nemusí do určité vzdálenosti dotýkat s instalovaným čtecím zařízením. Díky vytvořené softwarové aplikaci, která přijímá data ze čtecího zařízení, lze do určité míry nastavit také patřičná omezení týkající se řízeného vstupu osob. Čtečka je také zabezpečena protokolem OSDF, který zajišťuje obousměrnou komunikaci mezi tímto zařízením a řídící jednotkou. Na tomto zařízení je možnost aplikovat úsporný režim, který bude snižovat elektrickou energii v době klidového režimu čtecího zařízení. Instalace je možná do příslušného

sloupku. Ten dále může disponovat dalšími technickými prostředky, jež by zvyšovaly zabezpečení vybraného subjektu. Může se jednat o kameru či tlačítko na zavolání, pomocí kterého se osoby spojí se správcem střelnice. Zařízení je konstruováno tak, aby bylo chráněno proti přírodním hrozbám nebo vandalismu. (HID Global Corporation, © 2022)

Popisované zařízení je uvedeno na obrázku č. 21.



Obrázek 21 HID® Signo™ Reader S40
(HID Global Corporation, © 2022)

9.4 Posouzení identifikovaných variant

Všechny vymezené varianty čtecího zařízení k zabezpečení subjektu před hlavní bránou, jsou následně zapracovány dle předem stanovených kritérií v tabulce č. 9 a jsou určeny ke znázornění potřebných informací, dle kterých bude identifikována optimální možnost, jež bude zajišťovat regulaci osob ve vymezeném subjektu. Hodnocení uživatelské přívětivosti bude provedeno na základě stupnice obsahující čtyři úrovně: velmi dobrá, dobrá, uspokojivá a nedostatečná. Ostatní kritéria budou stanovena na základě specifikovaných parametrů, kterými disponují. Výběr kritérií byl konzultován s provozovatelem střelnice.

Tabulka 9 Vymezení kritérií (vlastní)

Kritéria Varianty	Užívaná frekvence	Napájení	Formát identifikátoru	Softwarová aplikace	Uživatelská přívětivost
ARCS-CQ/BT	13.56 MHz	12 V	RFID, Bluetooth, kód s dotykovým LCD displejem	Aplikace SECARD, aplikace STiD Mobile ID	uspokojivá
2N® IP VERSO	13.56 MHz nebo 125kHz	PoE nebo externí zdroj 12 V	RFID, Bluetooth modul, dotykový displej s klávesnicí, kamera, integrovaný mikrofon	2N Access Commander, aplikace My2N, aplikace 2N Mobile Key	dobrá
Datalogic Gryphon GFE4400	X	12 V nebo akumulátor	RFID, QR kód, 1D kódy, 2D kódy, Hikvision DS-KIS702	Systém MemberPro, rozhraní rezervačního systému, aplikace pro QR kódy	velmi dobrá
HID® Signo™ Reader S40	13,56MHz nebo 125kHz	12 V	RFID, Hikvision DS-KIS702, Bluetooth	Systém MemberPro, rozhraní rezervačního systému, HID Mobile Access®	dobrá

Na základě kritérií, která jsou uvedena v tabulce č. 9, bude vytvořena matice multikriteriálního hodnocení. Pro každé kritérium bude definována hodnotící stupnice od 1 do 5, přičemž hodnota 1 znamená nejlepší hodnocení. Váhy budou určeny tak, aby po jejich sečtení u jednotlivých kritérií byl výsledek roven jedné. Celkové hodnocení bude autorka posuzovat spolu s provozovatelem střelnice a s ostatními správci. Multikriteriální analýza bude vycházet z obecně stanoveného a závazného postupu.

Kritéria byla ohodnocena váhami následujícím způsobem:

- Užívaná frekvence – 0,1

- Napájení – 0,2
- Formát identifikátoru – 0,3
- Softwarová aplikace – 0,3
- Uživatelská přívětivost – 0,1

Hodnocení kritérií bylo určováno pomocí vymezeného intervalu hodnotící stupnice, a to u každého faktoru individuálně.

Po sestavení kvantifikace bude proveden součin vah a hodnocení. Všechny součiny u kritérií se v příslušném řádku sečtou a vznikne tak celkové ohodnocení vybrané varianty. V tabulce č. 10 jsou uvedeny výpočty včetně ohodnocení, jež budou rozhodující v určení optimální varianty. Rozhodnutí o nejlepší možnosti je uvedeno v posledním sloupci tabulky.

Tabulka 10 Multikriteriální analýza (vlastní)

Kritéria Varianty	Užívaná frekvence	Napájení	Formát identifikátoru	Softwarová aplikace	Uživatelská přívětivost	Suma	Pořadí
ARCS-CQ/BT	0,1 × 2 = 0,2	0,2 × 4 = 0,8	0,3 × 2 = 0,6	0,3 × 3 = 0,9	0,1 × 4 = 0,4	**2,9**	**4.**
2N® IP VERSO	0,1 × 1 = 0,1	0,2 × 3 = 0,6	0,3 × 2 = 0,6	0,3 × 2 = 0,6	0,1 × 3 = 0,3	**2,2**	**2.**
Datalogic Gryphon GFE4400	0,1 × 2 = 0,2	0,2 × 3 = 0,6	0,3 × 1 = 0,3	0,3 × 2 = 0,6	0,1 × 1 = 0,1	**1,8**	**1.**
HID® Signo™ Reader S40	0,1 × 1 = 0,1	0,2 × 4 = 0,8	0,3 × 2 = 0,6	0,3 × 2 = 0,6	0,1 × 3 = 0,3	**2,4**	**3.**

Autorka práce posuzovala čtyři varianty od rozdílných společností a hledala přitom tu nejvíce vhodnou variantu, jež by ve vybrané společnosti zajistila požadovanou bezpečnost týkající se řízeného vstupu osob. Na základě uvedené charakteristiky,

kterou získala po prozkoumání aktuálních možností nabízejících se na trhu, a při následném výběru za spolupráce odborníka z praxe, byla vybrána varianta č. 3 od společnosti Datalogic S.p.A, která byla vyhodnocena v multikriteriální matici jako optimální.

Autorka práce spolu s osobou pracující v tomto oboru vytvořila na vybrané zařízení cenovou nabídku, která také zahrnuje nejen samotné čtecí zařízení, ale i ostatní příslušenství spojené s instalací vybraného čtecího zařízení. V cenové nabídce není uvedena související kabeláž a přenos dat, neboť tyto oblasti jsou již v rámci podniku zavedeny a nevyžadují tak zapracování do návrhu.

Kalkulace vjezdového terminálu obsahující vybrané zařízení z přechozích variant, je uvedena v tabulce č. 11. Mimo uvedené čtecí zařízení je v cenové nabídce zahrnuta také ostatní technologie, která je nezbytná pro uvedení čtecího zařízení do provozu. Ceny jsou uvedeny bez DPH a nezahrnují montážní práce.

Tabulka 11 Cenová nabídka vjezdového terminálu (vlastní)

Položka	**Název**	**Cena**
1.	Datalogic Gryphon GFE4400	5 347 Kč
2.	Komunikační převodník RS232/ETH	3 376 Kč
3.	Napájecí zdroj 12 V / 4,5A + AKU	6 380 Kč
4.	Relé modul 0/2 ETH	3 289 Kč
5.	Vjezdový terminál – sloupek	30 000 Kč
6.	Hikvision DS-KIS702 vrátník/interkom	9 019 Kč
7.	Ubiquiti UniFi Switch USW-16	7 759 Kč
Cena celkem bez DPH:		**65 170 Kč**

Následující tabulka č. 12 vymezuje cenový přehled týkající se potřebného aplikačního softwaru Member Pro, pomocí kterého lze definovat potřebná oprávnění. Software pracuje na operačním programu Windows a jeho data a informace jsou ukládána do SQL databáze, konkrétně databázového systému Firebird. Vybrané čtecí zařízení je tedy propojeno s tímto softwarem, jež zabezpečuje veškerou správu tohoto prostředku. Pomocí tohoto programu lze tedy nakonfigurovat uživatelská oprávnění. V tomto případě se může jednat o vytvoření

přístupů na řízený vstup osob, vedení evidence vstupujících osob, zavedení docházkového systému pracovníků či získání reportů, statistik a vytíženosti střelnice. Tento program se také v případě potřebné aktualizace zvládne sám aktualizovat, tudíž je jeho spravovaná bezpečnost vždy pod ochranou a software tak zajišťuje provoz vždy s nejnovější verzí.

V souladu s tímto programem je nutné také vymezit roční poplatky za webové rozhraní tohoto systému a webové rozhraní aplikace QR kód, pomocí které osoby mohou přikládat ke čtečce svá mobilní zařízení na základě předdefinovaných oprávnění. Webová aplikace také může sloužit k registraci nových členů.

Tabulka 12 Cenová nabídka na aplikační software (vlastní)

Položka	**Název**	**Cena**
1.	Serverová licence systému MemberPro	54 640 Kč
2.	Roční poplatek za webové rozhraní rezervačního systému	6 600 Kč
3.	Webová aplikace pro QR kódy	25 000 Kč
4.	Roční poplatek za webové rozhraní aplikace QR kód	6 600 Kč
Cena celkem bez DPH:		**96 640 Kč**

Poslední cenový rozpočet bude zahrnovat počítačový server, dále k němu potřebný operační systém Windows Server 2019 Essential a následně také záložní zdroj pro možný výpadek elektrické energie a externí pevný disk pro ukládání dat.

Tabulka 13 Cenová nabídka příslušenství (vlastní)

Položka	**Název**	**Cena**
1.	DELL PE T150 / XE2334 / 16 GB / 2x 2TB_7,2k / H355 / 2xGL / iD_BAS / 1x300W / 3yBas_NBD	35 842 Kč
2.	MS WINDOWS Server 2019 Essential - ROK ENG	8 895 Kč
3.	APC Smart-UPS 750VA (500 W) LCD 230 V	10 388 Kč
4.	WD Elements Desktop 4TB Ext. 3.5” USB 3.0, Black	2 449 Kč
Cena celkem bez DPH:		**57 574 Kč**

Součtem těchto tří cenový nabídek dostaneme konečnou cenu, a to **219 384 Kč**. Tato cena zahrnuje stanovené optimální čtecí zařízení včetně veškeré technologie, která je potřebná

pro následnou instalaci těchto prvků. V cenové nabídce nejsou zahrnuty montážní práce a hodnota zařízení je uvedena bez DPH. Sestavením tohoto návrhu vznikla vybranému subjektu možnost aplikovat jej a zajistit tak řízený vstup osob do areálu.

9.5 Ověření návrhů

Návrh, který byl pomocí výsledků z multikriteriální analýzy autorkou práce vybrán, bude následně ohodnocen provozovatelem a zároveň hlavním správcem střelnice, který posoudí, zda je tato volba adekvátní a odpovídající pro zvýšení bezpečnosti perimetrické ochrany.

Provozovatel subjektu, který se účastnil ohodnocování a stanovování vah specifikovaných kritérií, obdržel výsledek z multikriteriálního hodnocení. Následně mu byl předložen finální návrh, dle kterého by se realizovalo zajištění řízeného vstupu osob v podobě popisu konkrétního zařízení včetně příslušenství s cenovou nabídkou. S ohledem na získané informace vyjádřil souhlas s nákupem a instalací daného zařízení u vstupní brány areálu střelnice. Tento souhlas je dále uveden v příloze P1.

V průběhu zhotovení této práce se provozovatel střelnice rozhodl zajistit další nedostatek perimetrické ochrany, a to oplocení včetně nové elektronické vjezdové brány. Vybraný betonový plot, který má dosahovat výšky 2,5 metru má již správce zakoupen. Na plot bude také instalován ostnatý drát, který bude více odrazovat možné pachatele. Samotný plot má provozovatel již objednán a nyní čeká na jeho doručení a následnou montáž. Při výběru elektronické brány pro vjezd na střelnici bude provozovatel dbát na to, aby brána odpovídala technickým prostředkům specifikovaným v návrhu a byla s nimi sladitelná. Díky tomuto rozhodnutí bude vytvořený návrh autorkou práce možno realizovat ihned po dokončení prací spojených s budováním nového oplocení.

V příloze práce P2 se nachází také potvrzení odborníka z praxe, kde je uvedeno, že zvolené technické zařízení je kompatibilní s již existujícím zabezpečovacím systémem od společnosti Paradox, tudíž je možné využít také jeho funkcí, jež by mohly zvýšit stávající perimetrické zabezpečení. Zejména pak zakódování celého areálu po skončení pracovní doby, díky kterému se přes hlavní bránu do areálu nikdo nedostane, přičemž jakékoliv narušení by provozovateli střelnice bylo hlášeno přes již zmíněný systém Paradox prostřednictvím mobilní aplikace. Dále je v této příloze uvedeno, že daný odborník souhlasí s výběrem identifikované možnosti, která je pro vybraný subjekt spolu s dalšími technickými prostředky nejlepším řešením z navrhovaných variant pro řízený vstup osob do areálu střelnice.

ZÁVĚR

Tato diplomová práce měla za úkol posoudit a zhodnotit aktuální stav informační bezpečnosti z hlediska fyzické bezpečnosti dle normy ČSN EN ISO/IEC 27002 a na základě provedených analýz vytvořit návrh fyzického zabezpečení týkající se řízeného přístupu osob, který bude odpovídat stanoveným cílům práce.

Přínosem teoretické části práce bylo vymezení základních pojmů, právních předpisů a standardů a systému řízení bezpečnosti informací týkajících se informační bezpečnosti a také určení základních druhů ochrany objektů, které se orientují na fyzické zabezpečení. Poslední kapitola této části práce také specifikovala postup analýzy rizik.

Praktická část diplomové práce definuje základní popis vybraného subjektu, tedy společnosti HABRESTO ARMS s.r.o., u kterého byla provedena deskripce a analýza současného stavu fyzické bezpečnosti z hlediska informační bezpečnosti. Při posuzování byla navrhnuta doplňující opatření, kterými tento subjekt nedisponuje a bylo třeba je stanovit pro ochranu informačních aktiv nacházejících se ve vybraném subjektu. Po provedení SWOT analýz byly stanoveny odpovídající strategie pro dané prostředí. U vnějšího prostředí byla vymezena strategie WO, jež se zakládá na maximalizování příležitostí vedoucích k potlačení slabých stránek. U vnitřního prostředí se jednalo o strategii SO, kde je důležité využít silných stránek v rámci uvedených příležitostí.

Nejrizikovější oblastí bylo určeno vnějšího prostředí, konkrétně perimetrická ochrana společnosti. U ní byly zjištěny nedostatky jako je nezajištění dostatečného oplocení, nezabezpečená ochrana při vstupu osob do areálu společnosti nebo také nedostatečně střežený perimetr. Na základě toho se autorka práce zaměřila na řízený vstup osob do areálu. Pomocí navrženého modelu procesu byly identifikovány odpovídající varianty. Nejvíce vyhovující varianta byla vybrána po provedení multikriteriální analýzy, a to čtecí zařízení Datalogic Gryphon GFE4400. Zařízení bylo doplněno o další nezbytné technologie a výsledkem byla kompletní cenová nabídka pro zajištění řízeného přístupu osob. Navrhované řešení bylo zhodnoceno provozovatelem střelnice a odborným pracovníkem, kteří s ním souhlasí.

Při realizaci navrhovaného opatření by společnost docílila minimalizace hrozby plynoucí z neoprávněného vstupu osob do areálu střelnice, čímž by se jednoznačně snížily také další rizika s tím spojené. Provozovatel společnosti již zahájil přestavbu stávajícího oplocení a vstupní brány, po kterém bude návrh autorky práce realizovat a aplikovat ho.

V závěru lze konstatovat, že fyzická bezpečnost subjektů z hlediska ochrany informací patří mezi kritické faktory. Při úniku, ztrátě nebo modifikaci důležitých dat a informací hrozí dotčeným subjektům škoda. Nezanedbatelným rizikem je i možnost likvidace samotné společnosti v důsledku ztráty klíčových informací. Proto je důležité věnovat této oblasti patřičnou pozornost, pečlivě analyzovat současný stav a následně implementovat vhodná opatření na zabezpečení fyzického prostoru a infrastruktury, aby byly informace chráněny před neoprávněným přístupem a manipulací.

Díky tomuto shrnutí lze uvést, že cíle diplomové práce byly splněny.

„Bez fyzické bezpečnosti je bezpečnost informací pouhým nápadem.“

(Gene Spafford)

SEZNAM POUŽITÉ LITERATURY

2N TELEKOMUNIKACE, © 2023. 2N® IP Verso: Instalační manuál. *2N* [online]. Praha: 2N TELEKOMUNIKACE [cit. 2023-04-15]. Dostupné z: https://wiki.2n.com/hipve/inst/latest/cs

CALICCHIO, Stefano, 2021. *SWOT analýza ve 4 krocích: Jak využít matici SWOT pro změnu v kariéře a podnikání* [online]. Itálie: StreetLib SRL [cit. 2023-04-09]. ISBN 9791220842044. Dostupné z: https://books.google.cz/books/about/SWOT_ANALÝZA_VE_4_KROCÍCH_Jak_využ%C3%ADt.html?id=hhBBEAAAQBAJ&redir_esc=y

CYBERSECURITY.CZ, 2017. Kybernetická bezpečnost (Cyber Security): Definice. *Cybersecurity*[online]. Cybersecurity.cz [cit. 2023-02-24]. Dostupné z: https://www.cybersecurity.cz/basic.html

ČESKO, 1993. *Usnesení č. 2/1993 Sb., Usnesení předsednictva České národní rady o vyhlášení LISTINY ZÁKLADNÍCH PRÁV A SVOBOD jako součástí ústavního pořádku České republiky*. In: Sbírka zákonů České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/1993-2

ČESKO, 1999. *Zákon č. 106/1999 Sb., o svobodném přístupu k informacím*. In: Sbírka zákonů České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/1999-106

ČESKO, 2000. *Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů*. In: Sbírka zákonů České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/2000-101

ČESKO, 2005. *Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti*. In: Sbírka zákonů České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/2005-412

ČESKO, 2012. *Zákon č. 89/2012 Sb., občanský zákoník*. In: Sbírka zákonů České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/2012-89

ČESKO, 2014. *Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti*. In: Sbírka zákonů České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/2014-181

ČESKO, 2018. *Vyhláška č. 82/2018 Sb., Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)*. In: Sbírka zákonů České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/2018-82

ČESKO, 2019. *Zákon č. 110/2019 Sb., o zpracování osobních údajů*. In: Sbírka zákonů České republiky. Dostupné také z: https://www.zakonyprolidi.cz/cs/2019-110

ČSN EN ISO/IEC 27000, 2020. *Informační technologie – Bezpečnostní techniky: Systémy řízení bezpečnosti informací – Přehled a slovník*. 5. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Třídící znak 369790.

ČSN EN ISO/IEC 27001, 2014. *Informační technologie – Bezpečnostní techniky: Systémy řízení bezpečnosti informací – Požadavky*. 2. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Třídící znak 369797.

ČSN EN ISO/IEC 27002, 2014. *Informační technologie – Bezpečnostní techniky: Soubor postupů pro opatření bezpečnosti informací*. 2. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Třídící znak 369798.

ČSN EN ISO/IEC 27006, 2021. *Informační technologie – Bezpečnostní techniky: Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Třídící znak 369790.

ČSN EN ISO/IEC 27007, 2020. *Informační technologie, kybernetická bezpečnost a ochrana soukromí: Směrnice pro audit systémů řízení bezpečnosti informací*. 3.vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Třídící znak 369790.

ČSN ISO/IEC 27003, 2018. *Informační technologie – Bezpečnostní techniky: Systémy řízení bezpečnosti informací – Pokyny*. 2. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Třídící znak 369790.

ČSN ISO/IEC 27004, 2018. *Informační technologie – Bezpečnostní techniky: Řízení bezpečnosti informací – Monitorování, měření, analýza a hodnocení*. 2. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Třídící znak 369790.

ČSN ISO/IEC 27005, 2019. *Informační technologie - Bezpečnostní techniky: Řízení rizik bezpečnosti informací*. 3.vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Třídící znak 369790

DATALOGIC S.P.A., © 2012-2020. GRYPHON™ I GFE4400 2D. In: *Datalogic: Empower your vision* [online]. Itálie: Datalogic [cit. 2023-04-20]. Dostupné z: https://cdn.datalogic.com/Download?iddwnfile=28382

DEATH, Darren, 2017. *Information Security Handbook* [online]. Birmingham: Packt Publishing [cit. 2023-02-24]. ISBN 978-1-78847-883-0. Dostupné z: https://edu.anarcho-copy.org/Against%20Security%20%20Self%20Security/Information_Security_Handbook_Develop_a_threat_model_and_incident.pdf#page25

DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK, 2019. *Řízení kybernetické bezpečnosti a bezpečnosti informací*. Praha: Professional Publishing. ISBN 978-80-88260-39-4.

DURAČINSKÁ, Zuzana, 2016. NIS: Co přináší nová směrnice EU o síťové a informační bezpečnosti? *Nic.cz*[online]. IT Systems [cit. 2023-02-14]. Dostupné z: https://www.nic.cz/files/nic/doc/ITSystems_NIS_102016.pdf

ENISA, 2005. About ENISA – The European Union Agency for Cybersecurity. *ENISA* [online]. © 2005-2023 by the European Union Agency for Cybersecurity. [cit. 2023-02-14]. Dostupné z: https://www.enisa.europa.eu/about-enisa/about-enisa-the-european-union-agency-for-cybersecurity

ENISA, 2023. Supporting the implementation of Union policy and law regarding cybersecurity.: NIS Directive. *ENISA* [online]. © 2005-2023 by the European Union Agency forCybersecurity. [cit. 2023-02-20]. Dostupné z: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new

HABRESTO ARMS S.R.O., 2021. *Interní směrnice: Organizační dokumentace*. Ježkovice: HABRESTO ARMS.

HABRESTO ARMS S.R.O., 2022. *Interní směrnice: Provozní řád*. Ježkovice: HABRESTO ARMS.

HID GLOBAL CORPORATION, © 2022. HID® Signo™: The Signature Line of Access Control Readers. In: *Hidglobal* [online]. United States: HID Global Corporation/ASSA ABLOY AB. [cit. 2023-04-20]. Dostupné z: https://www.hidglobal.com/sites/default/files/documentlibrary/pacs-hid-signo-reader-br-en_0.pdf

CHAPPLE, Mike, James Michael STEWART a Darril GIBSON, 2018. *CISSP® Certified Information Systems Security Professional: Official Study Guide*. 8th Edition. Indianapolis: Wiley. ISBN ISBN 978-1-119-47593-4.

CHVALKOVSKÁ, Pavla, 2022. Mezinárodní kybernetická bezpečnost: Novou směrnici NIS 2 bude muset splnit více než 6 000 českých firem. *KYBEZ* [online]. © GORDIC spol.s r.o. [cit. 2023-02-20]. Dostupné z: https://www.kybez.cz/novou-smernici-nis-2-bude-muset-splnit-vice-nez-6-000-ceskych-firem/

Information security, cybersecurity and privacy protection: Guidance on managing information security risks, © 2022. *ISO.org* [online]. Switzerland: ISO [cit. 2023-04-17]. Dostupné z: https://www.iso.org/standard/80585.html#page-top

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR, 2022. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Páté doplněné a upravené vydání. Přeložil Karel VAVRUŠKA. Praha: Česká pobočka AFCEA. ISBN 978-80-908388-4-0.

KOLOUCH, Jan a Pavel BAŠTA, 2019. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o. CZ.NIC. ISBN 9788088168317.

KRESA, Dan, 2018. MEZINÁRODNÍ KYBERNETICKÁ BEZPEČNOST: EU: Začátek platnosti NIS a nové plány kybernetické bezpečnosti. *KYBEZ* [online]. © GORDIC spol. s r.o. [cit. 2023-02-14]. Dostupné z: https://www.kybez.cz/eu-zacatek-platnosti-nis-a-nove-plany-kyberneticke-bezpecnosti/

KUČÍNSKÝ, Adam, 2016. Zákon o kybernetické bezpečnosti a směrnice NIS. *Interní audit a informační technologie* [online]. Český institut interních autorů, 1-4 [cit. 2023-02-14]. Dostupné z: https://www.interniaudit.cz/download/diskuze/pdfclanky/diskuse.15-kucinsky-adam.pdf

KYNCL, Jaromír, 2014. *Bezpečnost objektu ve světle moderních technologií*. Praha: Komora podniků komerční bezpečnosti České republiky. ISBN 978-80-260-7115-0.

LUKÁŠ, Luděk, 2011. *Bezpečnostní technologie, systémy a management I*. Zlín: VeRBuM. ISBN 978-80-87500-05-7.

LUKÁŠ, Luděk, 2013. *Bezpečnostní technologie, systémy a management III*. Zlín: VeRBum. ISBN 978-80-87500-35-4.

LUKÁŠ, Luděk, 2015. *Bezpečnostní technologie, systémy a management*. Zlín: Radim Bačuvčík - VeRBuM. ISBN 978-80-87500-35-4.

MCCARTHY, N.K., 2012. *The Computer Incident Response Planning Handbook: Executable Plans for Protecting Information at Risk*. New York: McGraw-Hill. ISBN 978-0-07-179039-0.

MINISTERSTVO VNITRA ČR, 2016. Terminologický slovník pojmů z oblasti krizového řízení, ochrany obyvatelstva, environmentální bezpečnosti a plánování obrany státu. *Ministerstvo vnitra České republiky* [online]. Praha: MV ČR [cit. 2022-12-09]. Dostupné z: https://www.mvcr.cz/soubor/terminologicky-slovnik-mv-verze-ke-stazeni.aspx

NÚKIB, 2022. Zpráva o stavu kybernetické bezpečnosti České republiky za rok 2021. In: *Nukib.cz* [online].[cit. 2023-02-24]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kybernetick_bezpenosti_2021.pdf

NÚKIB, 2023a. Obecné informace o směrnici NIS2 a budoucí národní úpravě. *NÚKIB* [online]. [cit. 2023-02-16]. Dostupné z: https://osveta.nukib.cz/mod/page/view.php?id=2582

NÚKIB, 2023b. NIS 2: 3. Rozdělení povinných organizací. *Nis2.nukib.cz* [online]. NÚKIB [cit. 2023-02-20]. Dostupné z: https://osveta.nukib.cz/mod/page/view.php?id=2617

PEKOVÁ, Andrea, 2020. Co je užitečné vědět o normách a dalších dokumentech. *Česká společnost pro jakost* [online]. Česká společnost pro jakost [cit. 2023-03-06]. Dostupné z: https://www.csq.cz/infocentrum/odborne-clanky/detail/co-je-uzitecne-vedet-o-normach-a-dalsich-dokumentech

PORADA, Viktor, 2019. *Bezpečnostní vědy: úvod do teorie, metodologie a bezpečnostní terminologie*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-758-0.

POŽÁR, Josef, 2005. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-86898-38-5.

SASKOVÁ, Vladěna, 2022. Virtuální konference – Směrnice NIS 2: Nová strategie kybernetické bezpečnosti EU. In: *Nis2.tech* [online]. [cit. 2023-02-23]. Dostupné z: https://www.youtube.com/watch?v=fc2sgeo7esk&t=369s

SEDLÁČEK, Stanislav, 2015. Analýza SWOT na odvětvové úrovni sociálního dialog. In: *Svaz průmyslu a dopravy České republiky* [online]. Praha [cit. 2023-04-09]. Dostupné z: https://www.google.com/url?client=internalelementcse&cx=014240574969914480226:nbaphozlqi&q=https://www.spcr.cz/images/stories/Projekty/SWOT_analyza.pdf&sa=U&ved=2ahUKEwim_72I8JvAhXiQfEDHQGIC8IQFnoECAUQAg&usg=AOvVaw3J033ojiwaLfDa9jQYD2qJ

SHAMELI-SENDI, Alireza, Rouzbeh AGHABABAEI-BARZEGAR a Mohamed CHERIET, 2015. Taxonomy of information security risk assessment (ISRA). *Computers & Security* [online]. © 2015 Elsevier, 14-30 [cit. 2023-03-20]. Dostupné z: doi:https://doi.org/10.1016/j.cose.2015.11.001

SIKOROVÁ, Magdaléna, 2019. SWOT – strategie vašeho projektu snadno a rychle. *Projektově*[online]. Ostrava: © Projektově.CZ [cit. 2023-04-09]. Dostupné z: https://www.projektove.cz/blog/swot-strategie-vaseho-projektu-snadno-a-rychle

SMEJKAL, Vladimír a Karel RAIS, 2011. *Řízení rizik ve firmách a jiných organizacích* [online]. 3. rozšířené a aktualizované vydání. Praha: © Grada Publishing [cit. 2023-03-21]. ISBN 978-80-247-7005-5. Dostupné z: https://www.bookport.cz/e-kniha/rizeni-rizik-ve-firmach-a-jinych-organizacich-1242833/

SMEJKAL, Vladimír, Tomáš SOKOL a Jindřich KODL, 2019. *Bezpečnost informačních systémů podle zákona o kybernetické bezpečnosti*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-765-8.

STID, © 2021. ARCS-CQ/BT: 13.56 MHz + Bluetooth® + QR Code touchscreen / keypad reader. *Stid-security* [online]. France: STiD [cit. 2023-04-15]. Dostupné z: https://stid-security.com/en/products/arc-cq-13-56-mhz-qr-code-touchscreen-keypad-readers

ŠULC, Vladimír, 2018. *Kybernetická bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. ISBN 978-80-7380-737-5.

TECHNOR, © 2020-2022. ČSN EN ISO/IEC 27002 Informační bezpečnost, kybernetická bezpečnost a ochrana soukromí: Opatření informační bezpečnosti. *Technické normy ČSN* [online]. Praha: TECHNOR print [cit. 2023-04-17]. Dostupné z: https://www.technicke-normy-csn.cz/csn-en-iso-iec-27002-369798-249194.html#

THEIN.EU, 2022. NIS 2: Koho se nová směrnice bude týkat: *Thein* [online]. [cit. 2023-02-20]. Dostupné z: https://www.thein.eu/cs/security/nis2/#

UHLÁŘ, Jan, 2005. *Technická ochrana objektů II. díl: Elektrické zabezpečovací systémy II*. Praha: Policejní akademie České republiky. ISBN 80-725-1189-0.

VANĚK, Michal, Milan MIKOLÁŠ a Kateřina ŽVÁKOVÁ, 2012. Evaluation methods of SWOT analysis. *GeoScience Engineering* [online]. 58(2), 23-26 [cit. 2023-04-09]. ISSN 1802-5420. Dostupné z: http://gse.vsb.cz/2012/LVIII-2012-2-23-31.pdf

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

atp.	a tak podobně
BOZP	Bezpečnost a ochrana zdraví při práci
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity, Availability
CQB	Close Quarters Battle
CSIRT	Network and Information Systems
ČR	Česká republika
ČSN	České technické normy
DPH	Daň z přidané hodnoty
EAL	Evaluation Assurance Level
ENISA	European Network and Information Security Agency
EP	Externí prostředí
EU	Evropská unie
GDPR	General Data Protection Regulation
HACCP	Hazard Analysis and Critical Control Points
ID	Identification
IEC	International Electrotechnical Commission
Inc.	Incorporated
IP	Interní prostředí
IS	Informační systém
ISMS	Information Security Management System
ISO	International Organization for Standardization
JZD	Jednotné zemědělské družstvo
kHz	Kilohertz
LCD	Liquid Crystal Display

MhZ	Megahertz
NFC	Near Field Communication
NIS	Network and Information Systems
NÚKIB	Národní úřad pro kybernetickou bezpečnost
OSPF	Open Shortest Path First
PDCA	Plan, Do, Check, Act
PO	Požární ochrana
PoE	Power over Ethernet
RFID	Radio Frequency Identification
S.p.A.	Societá per Azioni
s.r.o.	společnost s ručením omezeným
SMS	Short message service
SQL	Structured Query Language
V	Volt

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: SOUHLAS PROVOZOVATELE VYBRANÉHO SUBJEKTU

HABRRSTO ARMS s.r.o.

Jan Brehový

Provozovatel střelnice

Souhlas se stanoveným návrhem pro řízený vstup osob do areálu

Já, Jan Brehový, jakožto provozovatel střelnice HABRESTO ARMS s.r.o., souhlasím s vybranou variantou, kterou navrhla autorka diplomové práce a schvaluji následný nákup a instalaci tohoto zařízení u vstupní brány areálu pozemku, které bude regulovat pohyb osob. Potvrzuji také, že vybrané technické zařízení odpovídá všem mým požadavkům, které jsou důležité pro zajištění bezpečnosti areálu. Významným prvkem je také skutečnost, že vybraná společnost nabízí softwarovou aplikaci s budoucí podporou, která umožňuje definovat přístupová práva pro různé osoby a zároveň umožňuje propojení zařízení s aktuálním bezpečnostním systémem Paradox.

Tímto podpisem stvrzuji, že po instalaci oplocení a elektrické vstupní brány, zrealizuji tento návrh řízeného vstupu osob.

Za společnost HABRESTO ARMS s.r.o.

Datum: 22.4.2023

.....

Jan Brehový

PŘÍLOHA P II.: PROHLÁŠENÍ ODBORNÉHO PRACOVNÍKA

Prohlášení odborného pracovníka

Prohlašuji, že jako odborný pracovník v oboru bezpečnostních systémů souhlasím s tím, že varianty navržené v diplomové práci byly pečlivě zvažovány a vybrány dle nejlepších možností v souladu s nejnovějšími poznatky a potřebnými specifikacemi. Dále potvrzuji, že zvolená nejoptimálnější varianta je adekvátní a kompatibilní s bezpečnostním systémem Paradox.

Rovněž potvrzuji, že návrh včetně cenové nabídky je správně sestaven. Cena byla uvedena v souladu s aktuálními tržními podmínkami a zohledňuje všechny potřebné součásti, technologie a aplikační software nutný pro realizaci a implementaci návrhu. Celkově považuji tento návrh za kvalitní a pro budoucího klienta výhodný.

Fila

.....

Bc. Martin Fila

Luxart s.r.o.

Datum: 23.4. 2023