Kybernetická bezpečnost subjektu

Bc. Karin Fialková

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. Karin Fialková**
Osobní číslo:	**L21296**
Studijní program:	**N1032A020002 Bezpečnost společnosti**
Specializace:	**Ochrana obyvatelstva**
Forma studia:	**Kombinovaná**
Téma práce:	**Kybernetická bezpečnost subjektu**

Zásady pro vypracování

1. Zpracujte teoretický vstup do dané problematiky.
2. Proveďte analýzu stavu vybrané oblasti kybernetické bezpečnosti subjektu.
3. Na základě výsledků analýzy navrhněte opatření ke zlepšení stávajícího stavu kybernetické bezpečnosti vybraného subjektu.
4. Sumarizujte získané výstupy diplomové práce.

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

Seznam doporučené literatury:

1. DOUCEK, Petr, Martin KONEČNÝ a Luděk NOVÁK. *Řízení kybernetické bezpečnosti a bezpečnosti informací.* Praha: Professional Publishing, 2019. ISBN 978-80-88260-39-4.
2. KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity.* Praha: CZ.NIC, z.s.p.o. CZ.NIC, 2019. ISBN 978-80-88168-31-7.
3. MCCARTHY, N.K. *The Computer Incident Response Planning Handbook.* United States of America: The McGraw-Hill Companies, 2012. ISBN 978-0-07-179039-0.

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. Karin Fialková

.....
podpis studenta

ABSTRAKT

Diplomová práce je svým tématem zaměřena na kybernetickou bezpečnost ve vybraném subjektu. Hlavním cílem diplomové práce je návrh opatření pro kybernetické bezpečnosti subjektu. Je rozdělena na dvě stěžejní části – teoretickou a praktickou. První část práce je v několika kapitolách zaměřena na teoretický základ dané problematiky a je zde řešena například základní terminologie, legislativní rámec a současný stav kybernetické bezpečnosti na území České republiky a Evropské unie a systém řízení bezpečnosti informací. Druhá část práce je zaměřena na základní charakteristiku vybraného subjektu, následné provedení analýzy vnitřního a vnějšího prostředí pomocí analýzy SWOT. Z výsledků analýzy jsou následně určeny informační a kybernetická aktiva a hrozby pro vybraný subjekt. Tyto aktiva a hrozby jsou následně využity do analýzy rizik, která je provedena pomocí nástroje RISKAN. Z této analýzy vyplývají závěry, na které je v poslední kapitole praktické části navrženo opatření.

Klíčová slova: aktivum, analýza rizik, hrozba, systém řízení bezpečnosti informací, kybernetická bezpečnost.

ABSTRACT

The thesis is focused on cyber security in the chosen subject. The main objective of the thesis is to propose measures for cyber security of the subjekt. It is divided into two main parts - theoretical and practical. The first part of the thesis is focused on the theoretical basis of the issue in several chapters and addresses, for example, the basic terminology, the legislative and the current state of cybersecurity in the Czech Republic and the EU and the information security management system. The second part of the thesis is focused on the basic characteristics of the chosen subject, followed by an analysis of the internal and external environment using SWOT analysis. The results of the analysis are then used to determine the information and cyber assets and threats to the chosen subjekt. These assets and threats are then used in the risk analysis, which is done using the RISKAN tool. From this analysis, conclusions are drawn and action is proposed in the last chapter of the practical section.

Keywords: Asset, Cyber Security, Information Security Management System, Risk Analysis, Threat.

Mé velké poděkování patří zejména panu Ing. Petru Svobodovi, Ph.D. za poskytnutí informací, cenných rad a času při vedení diplomové práce. Dále bych chtěla poděkovat jednatelům a kolegům daného subjektu za spolupráci, trpělivost, odborné konzultace a materiály pro zpracování.

Speciálně bych chtěla poděkovat mému manželovi, celé rodině a přátelům za velkou podporu během studia, která pro mě byla velmi důležitá.

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

Motto:

„Nebezpečné je všecko, kamaráde, kdyby nebylo, nestálo by za to žít.“

Oscar Wilde

OBSAH

ÚVOD

Se vzrůstající potřebou digitalizace a využívání internetu pro čím dál více běžných denních aktivit se navyšuje počet kybernetických útoků ať už na jednotlivce, soukromé firmy či subjekty veřejné správy a organizace. Většina těchto společnosti využívá elektronická média pro ukládání či sdílení citlivých informací, které jsou cílem kybernetických útoků čím dál častěji a společnosti čelí sofistikovanějším a téměř neodhalitelným útoků hackerů. Většina těchto organizací stojí před problémem, kdy jsou nuceny zvyšovat kybernetickou bezpečnost, aby byla zajištěna minimalizace těchto hrozeb a rizika ztráty osobních informací či know-how.

Tato diplomová práce se zabývá tématem kybernetické bezpečnosti výrobního subjektu s důrazem na identifikaci aktiv a hrozeb.

V teoretické části práce bude v několika kapitolách shrnuta problematika kybernetické bezpečnosti, definována základní terminologie – teorie informačních a komunikačních technologií a kybernetické bezpečnosti s důrazem na její definici, základní pojmy a tři její principy, mezi něž se řadí triáda CIA, prvky kybernetické bezpečnosti a životní cyklus kybernetické bezpečnosti. Dále bude uveden legislativní rámec, který svým obsahem vymezuje hlavní a související právní předpisy bezprostředně související s daným tématem. Předposlední kapitola bude věnovaná stavu kybernetické bezpečnosti na území České republiky a Evropské unie, kde budou shrnuty nejaktuálnější zprávy a statistiky, které byly v době zpracování práce k dispozici.

V úvodní kapitole praktické části se práce bude zaměřovat na podrobnou charakteristiku vybraného subjektu, jeho historii, organizační směrnici, rozdělení na jednotlivá střediska a definování dějů a procesů. Následně bude prostřednictvím SWOT analýzy definováno vnitřní a vnější prostředí a vybrána strategie vyhovující pro vybraný subjekt. Na základě této analýzy budou identifikována kybernetická aktiva a vybrané kybernetické hrozby. V další části bude vypracována analýza pomocí softwaru RISKAN. Na základě této analýzy rizik bude následně navrženo vhodné opatření.

CÍLE A POUŽITÉ METODY

V této kapitole jsou uvedeny hlavní a dílčí cíle a použité metody vypracování diplomové práce.

Hlavní cíl diplomové práce

- Návrh opatření ke zvýšení úrovně kybernetické bezpečnosti vybraného subjektu.

Dílčí cíle diplomové práce

- Rešerše problematiky kybernetické bezpečnosti subjektu.
- Analýza vnitřního a vnějšího prostředí vybraného subjektu.
- Identifikace kybernetických aktiv a hrozeb vybraného subjektu.
- Provedení analýzy rizik z hlediska kybernetické bezpečnosti vybraného subjektu.

Použité metody

- **Sběr dat a informací –** metoda byla využívána při zpracování teoretické části práce, dále při charakteristice vybraného subjektu a následně při vytváření podkladů pro analýzy.
- **Pozorování –** při charakteristice aktuálního stavu a definicí jednotlivých oddělení a jejich fungování.
- **Rozhovor –** pro lepší porozumění jednotlivých činností v subjektu bylo využito rozhovorů s jednotlivými vybranými zaměstnanci.
- **Analýza –** v práci byla aplikována pro analýzu vnějšího a vnitřního prostředí prostřednictvím SWOT analýzy pro určení silných a slabých stránek, příležitostí a hrozeb a následný výběr vhodné strategie subjektu. Dále bylo využito analýzy prostřednictvím softwaru RISKAN pro číselné vyhodnocení rizik.
- **Syntéza –** po každé provedené analýze byla provedena syntéza, kdy byly výsledky vyhodnoceny.
- **Dedukce –** pomocí dedukce byly ověřovány teoretické postupy na konkrétním příkladu vybraného subjektu.
- **Indukce** – po shrnutí jednotlivých analýz a pozorování byly uvedeny závěry.

Subjekt v celé práci není jmenován, a to z důvodu citlivosti zveřejněných dat.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ TERMINOLOGIE

Kapitola definuje základní pojmy vybraných odvětví, která tvoří teoretický základ pro vypracování praktické části diplomové práce. Definice pojmů je vytvořena na základě výkladového slovníku kybernetické bezpečnosti a skript Informační systémy Technické univerzity Ostrava.

1.1 Informační a komunikační technologie

Na úvod základní terminologie je nezbytné definování samotného informačního systému a jeho částí. V první řadě je nutné vysvětlení následujících pojmů: data, informace a informační technologie.

- **Data** jsou definována jako údaj – stav reálného světa, který lze získat několika různými způsoby, například měřením či pozorováním. (Hronek, 2007)
- **Informace** jsou na základě předchozí definice data, kterým byl přiřazen nějaký význam. Informace mají svou základní jednotku a tou je bit, který nabývá hodnot 0 a 1 („pravda – nepravda“, „ano – ne“). Druhou často používanou jednotkou je byte, kdy přepočet mezi těmito jednotkami je následující: 1 byte = 8 bitů. (Hronek, 2007)
- **Informační technologie** (IT) je taková technologie, která se soustřeďuje na zpracování informací. (Hronek, 2007)

1.1.1 Informační systém

Kapitola informační systém je věnována definici informačního systému a charakteristice jednotlivých jeho komponent.

Informační systém („dále jako IS“) je definován jako účelově uspořádaný celek, který je zodpovědný za shromažďování, zachovávání a zpřístupňování informací a dat. Pojem svým obsahem zahrnuje datové a informační zdroje, nosiče, technické, programové prostředky, pracovní prostředky, technologie, postupy, normy a pracovníky. (Jirásek, Novák a Požár, 2015).

Jinými slovy se informační systém skládá z následujících komponentů:

- **Hardware** („dále jako HW“) zahrnuje všechno technické vybavení, které umožňuje provoz počítačového systému. HW je dělen na vnitřní vybavení počítače a periferie. (Kolouch, 2016)

- Vnitřní vybavení počítače jsou části HW, které jsou nezbytné pro vlastní činnost počítače. Jedná se o základní desku, paměť, procesor a napájecí zdroj. Dále do běžného vnitřní vybavení jsou řazeny například: harddisk, grafická karta, mechanika paměťových médií, síťové komponenty či zvukové karty. (Kolouch, 2016)
- Periferie jsou ostatní části HW, které nejsou nutné k provozu počítače. Mezi základní součásti periferie jsou uváděny například: klávesnice, myš, monitor, externí paměťová zařízení či tiskárna. (Kolouch, 2016)

- **Software** („dále jako SW“) je definován jako veškeré programové vybavení, které je potřebné k provozu počítače. SW je dále dělen dle funkce do dvou základních částí – systémový a aplikační. (Kolouch, 2016)
  - **Systémový SW** – je nezbytný pro efektivní používání počítače. Jedná se o firmware a operační systém. Firmware je takový SW, který umožňuje částem HW činnost. Naopak Operační systém vytváří prostředí pro programy. (Kolouch, 2016)
  - **Aplikační SW** – zde jsou řazeny aplikace, které umožňují uživateli vykonávat činnost. Do této skupiny jsou řazeny kancelářské aplikace, grafické programy, vývojové nástroje či zábavní SW. (Kolouch, 2016)
- **Data a informace (Dataware) –** data jsou definována jako prvky, které svým obsahem nesou nějakou informační hodnotu, která je zpracovávána počítačem tak, aby vytvořila informaci pro příjemce. Data jsou tedy například různé grafy, čísla, mapy či transakce a mohou být uchovávána v textových či obrazových souborech. (Kolouch 2016)

  Informace jsou tedy data s nějakým určeným významem, které příjemci poskytují možnost ověření nebo zdokonalení jeho vlastností. (Kolouch, 2016)
- **Lidská část (Peopleware)** je definována jako efektivní fungování člověka v prostředí informačního systému, jeho znalosti, motivace či kompetence. (Hronek, 2007)
- **Organizační složka (Orgware)** je takový nástroj, který určuje pravidla pro provoz IS. Do této skupiny jsou řazeny pokyny a návody pro obsluhu, provozní pokyny,

určení zodpovědnosti, pokyny k archivaci či zásady pro údržbu a inovaci IS. (Hronek, 2007)

1.1.2 Počítačová síť

Počítačová síť je soustava zařízení – počítače, tiskárny apod., které jsou vzájemně propojeny, aby mezi nimi byla umožněna komunikace dle předem určených pravidel. Základní komponenty počítačových sítí jsou:

- Počítač.
- Síťový adaptér.
- Propojovací komponenty.
- Software.
- Komunikační protokoly. (Kolouch, 2016)

Tyto sítě jsou zpravidla užívány ke vzdálené správě, kdy správce sítě provádí pravidelnou údržbu či instalace nových programů či aktualizací. (Kolouch, 2016)

Počítačové sítě lze dělit dle několika různých kritérií. Jedná se například o druh a způsob připojení či účel provozování sítě. Nejznámější a nejpodstatnější dělení počítačové sítě je však dle velikosti. Tento způsob rozděluje sítě na: (Kolouch, 2016)

- Personal Area Network (PAN) – osobní počítačová síť je rozsahově nejmenší a probíhá zde propojení počítače, mobilních telefonů či notebooků v prostředí jedné osoby. (Kolouch, 2016)
- Local Area Network (LAN) – lokální sítě se řadí mezi nejznámější a nejrozsáhlejší a jsou využívány například ve firmách. Rozprostírá se do vzdálenosti stovek metrů. Nejrozšířenější je Ethernet a Wi-Fi. (Kolouch, 2016)
- Metropolitan Area Network (MAN) – metropolitní sítě mají propojovací funkci mezi lokálními sítěmi na území města do vzdálenosti desítek kilometrů. Zpravidla jsou využívány k propojení několika poboček firmy. (Kolouch, 2016)
- Wide Area Network (WAN) – rozsáhlé počítačové sítě, které bývají zpravidla veřejné a svou velikostí jsou rozsáhlejší než MAN. Typickým příkladem je Internet. (Kolouch, 2016)

1.2 Kybernetická bezpečnost

V následujících podkapitolách budou vymezeny základní pojmy kybernetické bezpečnosti a její principy.

1.2.1 Definice a základní pojmy kybernetické bezpečnosti

Tato kapitola je svým obsahem věnována základním pojmům a jejich definicím v oblasti kybernetické bezpečnosti.

Kybernetická bezpečnost - (Cyber Security) je definována jako souhrn právních, organizačních, technických a vzdělávacích prostředků, které svým obsahem vedou k zajištění ochrany kybernetického prostoru. (Doucek, Konečný a Novák, 2019).

Dle normy ISO/IEC 27101 je obsah kybernetické bezpečnosti vymezen jako aktivity, které mají za úkol udržení stability společnosti, udržení kontinuity a ochranu členů společnosti před riziky digitalizace. Kybernetická bezpečnost se soustřeďuje na zajištění v následujících oblastech:

- Stabilita a kontinuální funkce společnosti, organizace nebo národů.
- Ochrana vlastnictví lidí a organizací.
- Ochrana lidských životů a zdraví. (Doucek, Konečný a Novák, 2019).

Kybernetická bezpečnost se oproti informační bezpečnosti nezaměřuje pouze na ochranu důvěrnosti, integrity a dostupnosti, ale soustřeďuje se na řešení kybernetických incidentů. (Doucek, Konečný a Novák, 2019).

Kybernetický prostor – Cyber Space je takový prostor, který je složený z internetu a dalších počítačových sítí, digitálních zařízení, systémů, služeb a procesů, které v nich probíhají. Jedná se o veřejný prostor - není nikým vlastněn, a proto by měla být jeho bezpečnost zajišťována různými subjekty a jejich spoluprací. Nezbytné je sdílení informací a společný koordinovaný postup při vytváření opatření proti abnormalitám a bezpečnostním incidentům, které mají potenciál ohrozit nebo poškodit. Jednotlivé subjekty mají přesně danou svoji roli při ochraně kybernetického prostoru. (Kolouch, 2016)

Kybernetický prostor má několik základních charakteristik. Jedná se o následující:

- Anonymita – identita uživatele, který je součástí kyberprostoru, není prokazatelná.

- Asymetričnost – veškeré činnosti, které probíhají v kybernetickém prostoru, mohou mít významný vliv na ostatní uživatele.
- Neexistence hranice – v kyberprostoru nejsou aktivity nijak limitovány žádnou institucí, právním systémem či jinou suverenitou.
- Okamžitost – každá činnost zde provedená může mít během okamžiku vliv na celý svět.
- Volný vstup i ukončení pobytu v něm – přístup do kybernetického prostoru je možný pro kohokoli a kdykoli, zároveň také, ale kdykoli může bát ukončena jeho aktivita.
- Interakce – aktivita uživatelů může vytvářet znalosti a zároveň ovlivňovat ostatní uživatele. (Kolouch a Bašta, 2019)

Kybernetická hrozba je definována jako možnost poškození nebo narušení počítačové sítě či systému. Jedná se o akt, který směřuje ke změně informaci, aplikace či systému. V odborné literatuře jsou charakterizovány čtyři skupiny hrozeb a jejich vzájemný vztah. Skupiny hrozeb jsou:

- Únik informace.
- Narušení integrity.
- Potlačení služby.
- Nelegitimní použití. (Kolouch a Bašta, 2019)

Kybernetické hrozby jsou klasifikovány dle několika možných kritérií. Nejvíce využívány jsou řazení dle:

- Zdroje hrozby:
    - Hrozby způsobené člověkem – jedná se o hrozby úmyslně a neúmyslně způsobené.
    - Z nedbalosti.
    - Technické chyby.
    - Vis maior – vyšší moc. (Kolouch a Bašta, 2019)
- Zdroje působení – dle zdroje působení se dělí na vnitřní a vnější hrozby. (Kolouch a Bašta, 2019)

- Cíle hrozby:
    - Útok na CIA.
        - Důvěrnost.
        - Integrita.
        - Dostupnost. (Kolouch a Bašta, 2019)
    - Útok na některý z prvků kybernetické bezpečnosti:
        - Lidé.
        - Technologie.
        - Procesy. (Kolouch a Bašta, 2019)
- Motivace:
    - Finanční prospěch.
    - Konkurenční převaha.
    - Dokázání vlastních schopností.
    - Odplata.
    - Neplnění povinností. (Kolouch a Bašta, 2019)
- Typy hrozby:
    - Sociální inženýrství.
    - Botnet.
    - Malware.
    - Ransomware.
    - Spam/scam.
    - Podvodné nabídky.
    - Phishing.
    - Pharming.
    - Spear phishing.
    - Vishing.

- Smishing.
- Hacking.
- Sniffing.
- DoS, DDOS, DRDoS.
- Šíření závadového obsahu.
- Identity thef.
- ATP.
- Kyberterorismus.
- Kybernetické výpalné či vydírání. (Kolouch a Bašta, 2019)

Kybernetická bezpečnostní událost je dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti jako „*událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací“*. (Česko, 2014, §7)

Kybernetický bezpečnostní incident je definován v zákoně o kybernetické bezpečnosti „*jako narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události“.* (Česko, 2014, §7)

Při kybernetickém bezpečnostním incidentu dochází k narušení bezpečnosti informací, služeb a ICT systémů s nimi spojených. (Česko, 2014)

Kybernetický útok je vymezen jako takový útok, který je veden na IT infrastrukturu s cílem poškození a získání citlivých či strategicky významných informací. Takovýto útok je nejčastěji politicky či vojensky motivován. Jedná se o jakékoli úmyslné jednání útočníka v kybernetickém prostoru proti zájmům jiného subjektu. (Kolouch, 2016)

Mezi kybernetickým bezpečnostním incidentem a kybernetickým útokem je hlavní rozdíl ve způsobu zavinění. Bezpečnostní incident může být způsoben úmyslně, nedbalostí či vyšší mocí, u kybernetického útoku je jedná výhradně o úmysl člověka. (Kolouch, 2016)

Kybernetická kriminalita je charakterizována jako takový akt, který je soustřeďován proti počítačovému systému, síti, datům či uživatelům, nebo jednání, kdy je počítačový systém prostředkem pro páchání trestné činnosti. (Kolouch, 2016)

Nejčastější formou kybernetické kriminality je obecná kriminalita, která se odehrává v kybernetickém prostoru, kde je trestnou činnost možno páchat efektivněji a v kratším časovém úseku. (Kolouch, 2016)

Stav kybernetického nebezpečí je dle zákona o kybernetické bezpečnosti definován jako „*stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost služeb elektronických komunikací anebo bezpečnost a integrita sítí elektronických komunikací, a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací*“. (Česko, 2014, §21)

1.2.2 Principy kybernetické bezpečnosti

Pro účely kybernetické bezpečnosti jsou vymezeny tři principy neboli triády kybernetické bezpečnosti. Jedná se o:

- CIA.
- Prvky kybernetické bezpečnosti.
- Životní cyklus kybernetické bezpečnosti. (Kolouch a Bašta, 2019)

Triáda CIA

Z uvedených tří triád je triáda CIA označována za nejznámější a nejpoužívanější. Jednotlivá písmena zkratky svým významem popisují princip této triády. Písmeno C z anglického výrazu Confidentality – důvěrnost, písmeno I jako Integrity – celistvost a písmeno A jako Availability jako dostupnost.

Obrázek 1 Triáda CIA.
Zdroj: (Čermák, 2008)

V některé další oborné literatuře je možné nalézt triádu CIA doplněnou o další prvky. Jedná se o: P/C – Possession/Control, které vyjadřuje držení či kontrolu, A – Authenticity v překladu jako autentičnost a poslední U – Utility svým významem jako užitečnost. Takto doplněná triáda je pak nazývána jako princip Parkerian hexad. (Kolouch a Bašta, 2019)

Obrázek 2 Parkerian hexad.
Zdroj: (Čermák, 2008)

Důvěrnost – C – Confidentiality je definována jako skutečnost, že k informacím a datům mají přístup pouze oprávněné subjekty. Ve směrnici ISO/IEC 27000 informace podléhají bezpečnostním standardům, které svým obsahem definují, že tyto informace by měly být tříděny dle hodnoty, právních požadavků, citlivosti a kritičnosti. Zároveň by měly být pro manipulaci s nimi do praxe zavedeny určité postupy, které jsou v souladu klasifikačním schématem, které byly subjektem přijaty a mělo by být zamezeno neoprávněnému přístupu, nebo zneužití těchto informací, stejně tak by měla být přesně vymezeny a definovány možnosti manipulace a ukládání. (Kolouch a Bašta, 2019)

Jednotlivé klasifikace informací jsou v literatuře definovány v několika zdrojích. Tři nejznámější jsou dle:

- Zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.
- Klasifikace informací v komerční sféře.
- Traffic Light Protocol. (Kolouch a Bašta, 2019)

První uvedená klasifikace informací je definována zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti a to dle jejich schopností při neoprávněné manipulaci a nakládání způsobit újmu zájmům České republiky. Podle závažnosti případné újmy jsou informace děleny na:

- **Top secret** – **přísně tajné** informace, potenciál způsobit mimořádně vážnou újmu.
- **Secret** – **tajné** informace, potenciál způsobit vážnou újmu.
- **Confidential** – **důvěrné** informace, potenciál způsobit prostou újmu.
- **Restricted** – **vyhrazené** informace, nevýhodné pro zájmy ČR. (Česko, 2005)

Subjekty komerční sféry také přistupují ke klasifikaci informací. V tomto sektoru jsou informace selektovány následovně:

- **Chráněné** – do této skupiny jsou řazeny takové informace, jejichž špatná manipulace a nakládání by mohlo vést k závažnému poškození či zničení organizace. Jedná se například o únik strategických informací, kódu, zabezpečení, hesel a další. (Kolouch a Bašta, 2019)
- **Interní** – informace, které zahrnují například osobní údaje či smlouvy, kdy by při neoprávněném nakládání s nimi mohlo dojít k poškození organizace. (Kolouch a Bašta, 2019)
- **Citlivé** – do této skupiny jsou řazeny například informace, které ještě nebyly zveřejněny a mohou mít negativní dopad na organizaci. (Kolouch a Bašta, 2019)
- **Veřejné** – jsou informace, které jsou veřejnosti přístupné a jejich případná neoprávněná manipulace by neměla mít negativní vliv na organizaci. (Kolouch a Bašta, 2019)

Posledním uvedeným druhem klasifikace informací je takzvaný Traffic Light Protocol, jehož vznik se datuje do počátku roku 2000. Tento druh klasifikace vznikl za účelem zrychlení procesu výměny informací mezi zúčastněnými osobami a dle barevného rozlišení určuje další manipulaci s informacemi. Pro označování je využíváno barevné škály – červená, žlutá, zelená a bílá. (Kolouch a Bašta, 2019)

- Červená (TLP:RED) – červená barva označuje informace, které jsou určeny pouze pro zainteresované strany komunikace a není možné jejich zveřejnění. Tohoto využívají subjekty v případě, kdy by nesprávná manipulace mohla vést k narušení

soukromí, pověsti a jiné. Pro červeně označené informace platí, že nesmí být sdíleny s jinými stranami, které nejsou účastníky komunikace či setkání. Zároveň by jejich předávání mělo probíhat pouze verbálně nebo osobně. (Kolouch a Bašta, 2019)

- Žlutá (TLP:AMBER) – žlutě označené jsou informace, které podléhají omezenému zveřejnění, kdy jejich publikace může být uskutečněna pouze v organizaci, které se informace týká. Většinou se tohoto označení využívá v případech, kdy je nezbytná účinná reakce dalších účastníků. Nicméně přináší možné riziko pro soukromí nebo společnost v případě, kdy jsou zveřejňovány. Sdílení může probíhat mezi členy organizace a ostatními klienty dle pravidel, které si subjekt může definovat, ty však musí být důsledně dodržovány. (Kolouch a Bašta, 2019)
- Zelená (TLP:GREEN) – do zelené kategorie jsou řazeny informace, mohou být sdílené v rámci širší komunity nebo odvětví, ale i zde platí pro zveřejnění jistá omezení. Mohou být využívány za účelem zvýšení informovanosti všech účastníků komunikace. Platí zde zásada, že informace není tajná, ale nesmí být sdílena mimo zainteresovanou komunitu či odvětví. (Kolouch a Bašta, 2019)
- Bílá (TLP:WHITE) – informace, které jsou označeny bílou barvou, nepodléhají žádným omezením při manipulaci a jejich zveřejňování. Většinou svým obsahem nenesou riziko zneužití a nemají negativní vliv na určené subjekty. Sdílení informací v této barevné skupině není nijak omezeno a mohou být distribuovány bez dalších pravidel. (Kolouch a Bašta, 2019)

Na začátku roku 2023 vyla vydána aktualizovaná verze TLP, ve které se informace řadí do kategorií:

- TLP: RED.
- TLP AMBER + STRICT.
- TLP: AMBER.
- TLP: GREEN.
- TLP: CLEAR. (Circl.lu,2023)

Klasifikace informací na úrovni důvěrnosti je dále řešena ve vyhlášce č.82/2018 Sb., o kybernetické bezpečnosti, kde je využito takového třídění, které koresponduje se zásadami

TLP. Informace jsou zde selektovány na čtyři úrovně a využívány za podobných podmínek a zásad. Dělení úrovní a jejich odpovídající stupeň TLP je následující:

- Kritická úroveň – TLP:RED.
- Vysoká úroveň – TLP:AMBER.
- Střední úroveň – TLP:GREEN.
- Nízká úroveň – TLP:WHITE. (Česko, 2018)

Integrita – I – Integrity je druhým principem triády CIA. Integrita je definována jako jistota, že nedošlo ke změně obsahu informace. Zahrnuje platnost, konzistenci a přesnost. Integrita informací je zajišťována například pomocí kontrolních součtů, kódů či hašovacími funkcemi. Výkladový slovník kybernetické bezpečnosti dále definuje integritu sítě a dat. Integrita sítě je taková vlastnost, která zaručuje funkčnost a provozuschopnost sítí elektronických komunikací. Dále je zde zahrnuta i ochrana před poruchami, které jsou způsobené elektromagnetickým rušením, nebo provozním zatížením. Integrita systému je schopnost systému plnit svou funkci a zároveň odolávat neautorizovaným přístupům a provádění nesprávných změn. (Jirásek, Novák a Požár, 2015)

Za předpokladu narušení integrity může dojít ke změně informace, která nemusí být identifikována vůbec, nebo až za značně dlouhou dobu. (Kolouch a Bašta, 2019)

Integrita je ve vyhlášce 82/2018 Sb., o kybernetické bezpečnosti rozdělena dle hodnocení na stupnici od nízké až po kritickou. Podrobnější popisy jednotlivých úrovní a požadavků na ochranu aktiv jsou uvedeny v následující tabulce. (Česko, 2018)

Tabulka 1 Stupnice hodnocení integrity. Zdroj: (Česko, 2018)

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy povinné osoby.	Není vyžadována žádná ochrana.
Střední	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů povinné osoby a může se projevit méně závažnými dopady na primární aktiva.	Pro ochranu integrity j sou využívány standardní nástroje (například omezení přístupových práv pro zápis).
Vysoká	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva.	Pro ochranu integrity j sou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených komunikačními sítěmi je zajištěna pomocí kryptografických prostředků.
Kritická	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů povinné osoby s přímými a velmi vážnými dopady na primární aktiva.	Pro ochranu integrity j sou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (například pomocí technologie digitálního podpisu).

Dostupnost – A - Availability je třetím a posledním principem triády CIA, který je definován jako dostupnost informací tehdy, když jsou potřebné. Tato vlastnost hraje klíčovou roli pro každodenní provoz organizace. (Washington University in St. Louis, 2023)

Stupnice pro hodnocení dostupnosti informací je uvedena ve vyhlášce č. 82/1028 Sb., o kybernetické bezpečnosti stejně jako integrita od hodnoty nízké až po kritickou. Popis a požadavky na ochranu aktiva vymezuje tabulka níže.

Tabulka 2 Stupnice hodnocení dostupnosti. Zdroj: (Česko, 2018)

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).	Pro ochranu dostupnosti je postačující pravidelné zálohování.
Střední	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů povinné osoby.	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.
Vysoká	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za velmi důležitá.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.
Kritická	Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za kritická.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.

Prvky kybernetické bezpečnosti

Na zajištění kybernetické bezpečnosti se podílí tři hlavní prvky a jejich vzájemný vztah i interakce. Jedná se o lidi, technologie a procesy. (Kolouch a Bašta, 2019)

Lidé - jsou prvkem kybernetické bezpečnosti, který je často označován jako nejslabší článek, kdy jejich pochybení způsobuje kolaps celého systému. Lidé jsou zde děleni dle jednotlivých rolí či funkcí na:

- Strůjce.
- Příjemce pravidel.
- Subjekty, které je třeba chránit.
- Subjekty, které musí být proškoleni o pravidlech kybernetické bezpečnosti.
- Riziko či hrozbu. (Kolouch a Bašta, 2019)

Po lidi, kteří využívají služeb informačních a komunikačních technologií a pohybují se v kyberprostoru, je důležité, aby pochopili základní principy kybernetické bezpečnosti, chápali základní funkce počítačových systémů, správně využívali a analyzovali aplikace a v neposlední ředě se v oblasti kybernetické bezpečnosti vzdělávali. (Kolouch a Bašta, 2019)

Technologie – na technologie lze nahlížet ze dvou různých pohledů – z pohledu organizace a uživatele**.** Pro uživatele jsou technologie něčím, co zprostředkovává jejich pohyb

a využívání kyberprostoru. Oproti tomu pro organizace je technologie něco, co obsahuje velké množství zařízení, jedná se například o: (Kolouch a Bašta, 2019)

- Technologie pro uživatele například desktop či mobilní zařízení.
- Infrastrukturu sítě – LAN, Wi-Fi.
- Služby.
- Zabezpečovací prvky – firewall, IDS/IPS.
- Prvky v rámci infrastruktury, které jsou určené k autentizaci, autorizaci aj. (Kolouch a Bašta, 2019)

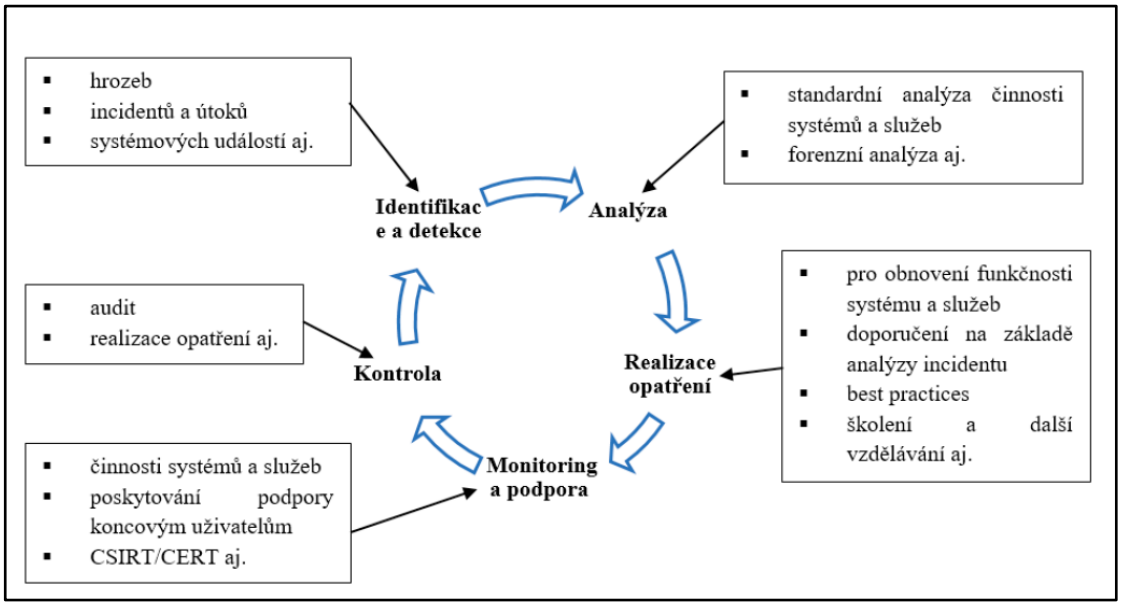
Procesy – jsou definovány jako nezbytné činnosti, které prostřednictvím technologií a služeb mohou být využívány lidmi. (Kolouch a Bašta, 2019)

„Z hlediska plynutí času je možné sledovat procesy:

- *Řízení aktiv a rizik:*
    - *Definování a kategorizace aktiv.*
    - *Analýza a kategorizace rizik.*
- *Implementace ICT a aplikací.*
- *Správa uživatelů a rolí.*
- *Autorizace a autentizace.*
- *Údržby (aktualizace systémů a služeb).*
- *Analýza nápravních opatření.*
- *Realizace nápravných opatření.*
- *Audit kybernetické bezpečnosti.*
- *Detekce anomálií či kybernetických útoků.*
- *Reakce na kybernetické toky či jiné incidenty.*
- *Procesy k zajištění kontinuity.*
- *školení a cvičení atd“.* (Kolouch a Bašta, 2019, str.61)

Životní cyklus kybernetické bezpečnosti

Posledním principem kybernetické bezpečnosti je životní cyklus, který funguje na principu fungování triády CIA a prvků kybernetické bezpečnosti během celého životního cyklu. Tento cyklus obsahuje tři stěžejní části – prevence, detekce a reakce. (Kolouch a Bašta, 2019)



Obrázek 3 Životní cyklus kybernetické bezpečnosti. Zdroj: (Kolouch a Bašta, 2019)

2 LEGISLATIVNÍ RÁMEC KYBERNETICKÉ BEZPEČNOSTI

Tato kapitola se soustřeďuje na legislativní rámec kybernetické bezpečnosti, zejména pak na rozbor zákonů a vyhlášek o kybernetické bezpečnosti, vybraných norem ISO, směrnic a metodik.

2.1 Zákony a vyhlášky

V této podkapitole jsou uvedeny vybrané zákony a vyhlášky související s problematikou kybernetické bezpečnosti či bezpečnosti jako takové.

Zákon je definován jako obecně závazný právní předpis, který byl přijat zákonodárnou mocí, v podmínkách České republiky se jedná o parlament. (SCS.ABZ.CZ, 2023)

Vyhláška je oproti zákonu druh podzákonného právního předpisu, který může být vydáván ústředními správními úřady. Právním předpisem obce nebo kraje je takzvaná obecně závazná vyhláška, která upravuje pravidla v jejich samostatné působnosti. (Iuridictum, 2021)

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

Zákon č.181/2014 Sb., o kybernetické bezpečnosti a změně souvisejících zákonů vyšel v platnost dne 29. srpna 2014 s účinností od 1. ledna 2015. Svým obsahem je rozdělen na čtyři jednotlivé části – první, třetí, pátou a šestou. Druhá a čtvrtá část tohoto zákona byly zrušeny. (Česko, 2018)

První část je rozdělena do šesti jednotlivých hlav a věnována základním ustanovením kybernetické bezpečnosti, vymezením základních pojmů a definování zástupců poskytovatele digitálních služeb. Jsou zde uvedeny základní pojmy, jako jsou: kybernetický prostor, kritická informační infrastruktura, bezpečnosti informací, významný IS -informační systém, správce IS, správce komunikačního systému, provozovatel informačního nebo komunikačního systému, základní služba a její informační systém, digitální služba a příslušné orgány a osoby, kterým je uložena nějaká povinnost v rámci zabezpečování kybernetické bezpečnosti. Dále je v této části definován systém zabezpečení kybernetické bezpečnosti, kde jsou charakterizovány bezpečnostní opatření, kybernetická bezpečnostní událost, kybernetický bezpečnostní incident a povinnost jednotlivých orgánů tento incident hlásit. V neposlední řadě zákon v první části řeší stav kybernetického nebezpečí, výkon státní správy, kontrolu, nápravná opatření a přestupky. (Česko, 2018)

Ve třetí části zákona jsou uvedeny změny zákona o elektronických komunikacích. Část pátá je věnována změně zákona o provozování rozhlasového a televizního vysílání. Poslední šestá část přesně definuje, kdy tento zákon nabývá účinnosti. (Česko, 2018)

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

Zákon č. 412/2005 Sb., o ochraně utajovaných informací ze dne 21. září 2005 svým obsahem vymezuje zásady pro stanovení utajovaných informací, přístupu k nim a další požadavky na ochranu. První část zákona definuje základní pojmy, jako jsou například utajovaná informace, zájmy ČR, odpovědná osobu po účely tohoto zákona, neoprávněnou osobu či bezpečnostní standardy. Druhá část je soustřeďována na ochranu utajovaných informací, kdy je vymezena újma zájmu ČR či nevýhodnost pro zájmy ČR, stupně utajení, druhy zajištění ochrany utajovaných informací, personální bezpečnost, podmínky přístupu fyzické osoby k jednotlivým stupňům utajení informací, administrativní bezpečnost, fyzická bezpečnost, bezpečnost informačních a komunikačních systémů, kryptografická ochrana, certifikace, osvědčení pro fyzické osoby a podnikatele, povinnosti při ochraně utajovaných informací a poskytování utajovaných informací v mezinárodním styku. Ve třetí části je řešena bezpečnostní způsobilost, kdy je definována citlivost, bezúhonnost, spolehlivost či osobní způsobilost pro účely tohoto zákona. Část čtvrtá vymezuje obecné zásady bezpečnostního řízení a jeho průběh a účastníky. Pátá část obsahuje role státní správy a jednotlivé úřady a instituce vykonávající úkoly státní správy v tomto odvětví. Části šestá, sedmá a osmá svým obsahem zajišťují kontrolu předpisů a činnosti úřadu a specifikuje přestupky – výši finanční pokuty za nedodržení předpisů. Na závěr jsou v deváté části uvedena přechodná a závěrečná ustanovení. (Česko, 2005)

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

Zákon č. 110/2019 Sb., o zpracování osobních údajů ze dne 12. března roku 2019 s účinností od 24. dubna téhož roku ve dvou částech vymezuje působnost zákona na základě výchozího předpisu Evropského parlamentu a Rady (EU) 2019/679. Zákon pojednává o:

- Zpracování osobních údajů.
- Ochraně osobních údajů a jejich zpracování v souvislosti s trestnou činností, zajišťování bezpečnosti ČR nebo zajišťování veřejného pořádku a vnitřní bezpečnosti.

- Ochraně osobních údajů při zajišťování obranných a bezpečnostních zájmů ČR.
- Úřadu, pověřenými osobami a činností.
- Přestupcích v rozsahu tohoto zákona.
- Přechodných, zrušovacích a závěrečných ustanoveních. (Česko, 2019)

2.1.4 Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky

Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky ze dne 22. dubna 1998 s účinností od 29. května roku 1998 definuje základní ustanovení a povinnosti s cílem zajistit svrchovanost a bezpečnost ČR, vymezuje povinnosti při vyhlášení nouzového stavu a stavu ohrožení státu. Součástí zákona je i bezpečnostní rada státu, personální zastoupení a rozsah pověření. (Česko, 1998)

2.1.5 Vyhláška č. 82/2018 – o kybernetické bezpečnosti

Vyhláška č. 82 ze dne 21. května roku 2018 svým obsahem definuje obsah a strukturu bezpečnostní dokumentace, bezpečnostní opatření, kybernetické bezpečnostní incidenty jejich typy, kategorie a hodnocení významnosti, způsoby a náležitosti jejich hlášení, oznámení o provedení opatření a způsob likvidace dat, provozních údajů a ostatních informací. (Česko, 2018)

2.1.6 Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích

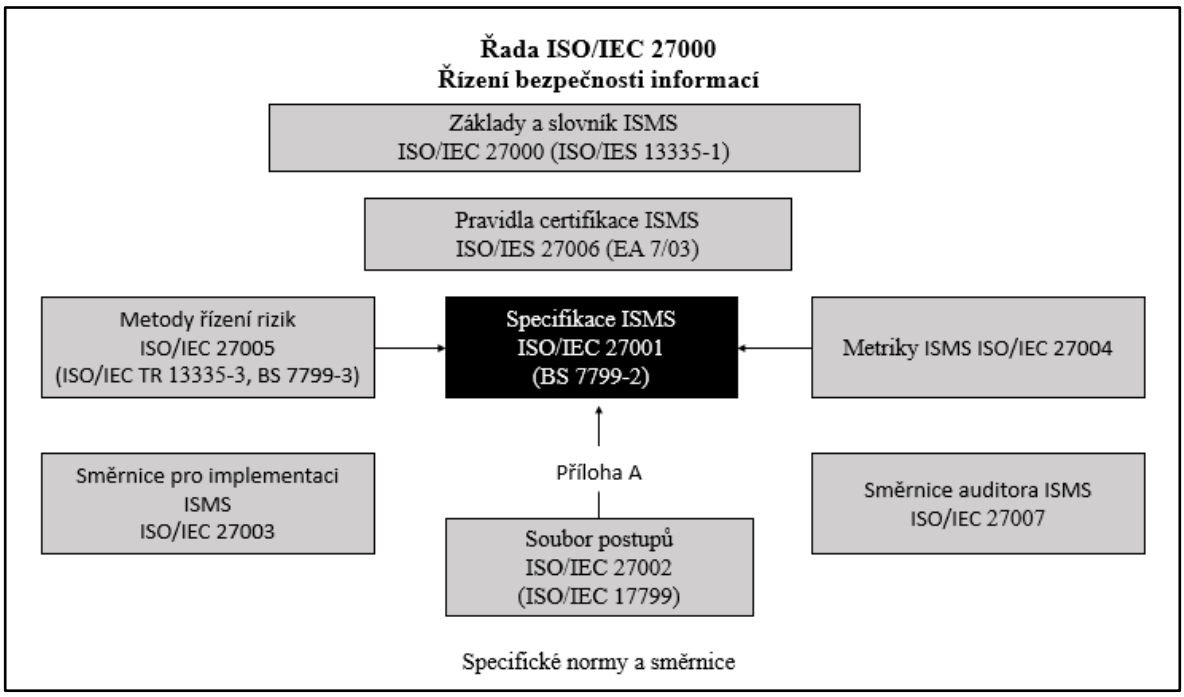
Tato vyhláška je platná od roku 2014 konkrétně od 14. prosince a definuje významné informační systémy a kritéria pro jejich určování. V průběhu roku 2020 byla vydána novela vyhlášky, která vymezuje a zpřesňuje kritéria pro určení významnosti informačního systému. (Česko, 2014)

2.2 Normy a standardy

Česká agentura pro standardizaci je státní příspěvková organizace zřízená na základě zákona č.265/2017 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů. Její zřízení probíhalo pro záštitou Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ) a od roku 2018 byly veškeré činnosti související s problematikou technických norem převzaty od ÚNMZ Českou agenturou pro standardizaci. (Agentura, © 2021)

Internationa Organization for Standardization (ISO) neboli mezinárodní organizace pro normalizaci je celosvětová federace normalizačních organizací, která sídlí v švýcarské Ženevě. ISO byla založena dne 23. února roku 1947. V současné době má tato organizace 105 řádných a 47 korespondenčních členů a 10 kandidátů na členství, kteří mají za úkol vytváření mezinárodních norem. ISO svou působností zaujímá celý svět, nicméně nejvýznamnější je rozšíření v evropských zemích.

Problematika řízení bezpečnosti informací byla zavedena jako řada norem ISO 27000 v roce 2005, je založena na principu PDCA a tvořena jednotlivými normami 27001 – 27007. (Doucek, Konečný a Novák, 2019)



Obrázek 4 Základní koncept řady ISO/IEC 27000 pro řízení bezpečnosti informací. Zdroj: (Doucek, Konečný a Novák, 2019), (vlastní tvorba)

ČSN EN ISO/IEC 27000 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník je první z řady norem a jejím hlavním úkolem je vytvoření a sjednocení odborného slovníku a definice základních modelů systému řízení bezpečnosti informací. (ČSN EN ISO/IEC 27000 Informační technologie, 2020)

ČSN EN ISO/IEC 27001 - Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací – Požadavky svým obsahem definuje základní specifikaci

systému řízení bezpečnosti informací ve společnosti a probíhá dle jejich požadavků certifikace příslušného systému řízení. ČSN EN ISO/IEC 27001 je možné zavést ve všech typech organizací. (ČSN EN ISO/IEC 27001 - Informační technologie, 2014)

ČSN EN ISO/IEC 27002 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací je norma, která se využívá k výběru a určení vhodných opatření v rámci řízení bezpečnosti informací. Dále ji mohou organizace využívat jako pokyny při implementaci. Lze ji také využít pro vývoj směrnic souvisejících se systémem bezpečnosti informací. (ČSN EN ISO/IEC 27002 Informační technologie, 2014)

ČSN EN ISO/IEC 27003 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací – Pokyny obsahují doporučení, možnosti a návody, tedy co by organizace měla, co může a co smí v souvislosti s požadavky na systém řízení bezpečnosti informací. Svým obsahem má tato norma doporučující charakter a organizace nemají povinnost tyto pokyny dodržovat. (ČSN EN ISO/IEC 27003 Informační technologie, 2018)

ČSN EN ISO/IEC 27004 Informační technologie - Bezpečnostní techniky - Řízení bezpečnosti informací - Monitorování, měření, analýza a hodnocení je dokument, který slouží organizacím při vyhodnocení bezpečnosti informací a efektivity systému řízení bezpečnosti informací. Norma stanovuje monitoring a měření výkonnosti bezpečnosti informací, efektivnosti systému řízení bezpečnosti informací, analýzu a vyhodnocení všech výsledků těchto měření. (ČSN EN ISO/IEC 27004 Informační technologie, 2018)

ČSN EN ISO/IEC 27005 Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací svým obsahem poskytuje doporučení pro řízení rizik bezpečnosti informací, definuje pravidla a postupy řízení rizik. Dále jsou zde vymezeny seznamy hrozeb a zranitelností pro vybraná aktiva. (ČSN EN ISO/IEC 27004 Informační technologie, 2018)

ČSN EN ISO/IEC 27006 Informační technologie - Bezpečnostní techniky - Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací norma slouží pro organizace, které se soustřeďují na audit a certifikaci systému řízení a poskytuje informace, dle kterých certifikační orgány v praxi musí postupovat při udílení certifikace. (ČSN EN ISO/IEC 27006 Informační technologie, 2021)

ČSN EN ISO/IEC 27007 Bezpečnost informací, kybernetická bezpečnost a ochrana soukromí - Směrnice pro audit systémů řízení bezpečnosti informací se soustřeďuje

na definici a stanovení pravidel a postupů, které jsou spojené s výkonem externích i interních auditů systému ISMS. (ČSN EN ISO/IEC 27007 Bezpečnost informací, 2020)

ČSN EN ISO/IEC 27032 Informační technologie - Bezpečnostní techniky - Směrnice pro kybernetickou bezpečnost je norma rozdělená do dvou částí, přičemž první se zabývá bezpečností kybernetického prostoru a poskytuje hlavně technická doporučení pro řešení obecných rizik kybernetické bezpečnosti. Ve druhé části je definována zejména spolupráce mezi zainteresovanými stranami při sdílení informací, koordinaci a zvládání bezpečnostních incidentů v kybernetickém prostoru. (ČSN EN ISO/IEC 27032 Informační technologie, 2013)

ČSN EN ISO/IEC 27033 Informační technologie - Bezpečnostní techniky - Bezpečnost sítě se svým obsahem soustřeďuje na vymezení různých aspektů síťové bezpečnosti. Norma je rozdělena na šest částí, jedná se o následující:

- Přehled a základní pojmy.
- Směrnice pro návrh a implementaci bezpečností sítě.
- Referenční síťové scénáře – hrozby, techniky návrhů a otázky řízení.
- Zajištění komunikace mezi jednotlivými sítěmi prostřednictvím bezpečnostních bran.
- Zprostředkování komunikace mezi sítěmi s použitím virtuálních privátních sítí.
- Zabezpečení přístupu k bezdrátové IP síti. (Doucek, Konečný a Novák, 2019)

2.3 Směrnice NIS II

Celým svým názvem Směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii je dokument, jehož hlavním cílem je rozvíjení schopností v oblasti kybernetické bezpečnosti v rámci Evropské unie, zmírnění hrozeb pro sítě a informační systémy, které jsou využívány k poskytování služeb v odvětvích kybernetické bezpečnosti a zajištění kontinuity v případě bezpečnostních incidentů za účelem zvyšování bezpečnosti Unie a jejího fungování v oblastech hospodářství a společnosti. (epravo.cz, 2023)

Současně směrnice určuje a rozšiřuje okruh povinných osob v oblasti kybernetické bezpečnosti a zároveň zpřísňuje požadavky na hlášení bezpečnostních incidentů, definuje

odpovědnost managementu organizace a upravuje sankce za nedodržení určených povinností. (epravo.cz, 2023)

Okruh povinných osob se ve znění této směrnice rozšiřuje na sektor IT služeb, výrobních podniků, poštovní a kurýrní služby nebo na organizace, které působí v oblasti výzkumu. Povinné osoby jsou takové osoby, které dosahují minimálně velikosti středního podniku a zaměstnávají minimálně 50 pracovníků a mají obrat nad 10 milionů eur. Ve směrnici se dělí na základní a důležité. U základních povinných osob musí být naplněna podmínka velikosti podniku a jedná se například o podniky z odvětví dopravy, zdravotnictví či veřejné správy. Mezi důležité povinné osoby budou spadat veškeré subjekty, které nepatří do základních. Zahrnují například poštovní a kurýrní služby, nakládání s odpady, chemický, potravinářský průmysl či vybrané sektory zpracovatelského průmyslu. (epravo.cz, 2023)

Směrnice do povinných osob neřadí například orgány veřejné správy v oblasti národní a veřejné bezpečnosti, obrany, vymáhání práva, soudní moc či národní banky. (epravo.cz, 2023)

2.4 Metodiky

V této kapitole budou popsány dvě nejznámější a nejvyužívanější metodiky pro zajištění bezpečnosti informací, které charakterizují základní vlastnosti bezpečnosti informačních systémů v rámci certifikace, klasifikace a posuzování. Jedná se o metodiky Control Objektives for Information and Related Technology – COBIT a metodiku s názvem Information Technology Infrastructure Library – ITIL.

2.4.1 COBIT

Control Objektives for Information and Related Technology, v překladu Kontrolní cíle pro informační a související technologie, je metodika, která zajišťuje efektivní řízení informací a informačních technologiích ve firmách. Hlavním cílem metodiky COBIT je poskytnout organizacím větší přizpůsobivost a specifikovat prostup při řešení systému správy a řízení informací a je koncipován tak, aby si organizace při vytváření vlastní strategie mohla přesně přizpůsobit přístup. (Smejkal, Sokol a Kodl, 2019)

Tato metodika je zaměřena na správnou synchronizaci IT procesů s cíli organizace, hodnocení výkonnosti a sofistikovanosti IT procesů a identifikaci odpovědností. (McCarthy, 2012)

COBIT lze aplikovat do prostředí jakékoli organizace s cílem zajištění kvality, kontroly a spolehlivosti informačních systémů. (TechTarget, 2021)

2.4.2 ITIL

ITIL neboli Information Technology Infrastructure Library je rámec ve formě několika sad knižních publikací, které svým obsahem popisují způsob řízení ICT služeb a infrastruktury. Je založena na zkušenostech z praxe a obsahuje knihovny, související publikace, konzultační služby, vzdělání a certifikace a ostatní nástroje. (Smejkal, Sokol a Kodl, 2019)

ITIL byla vyvinuta ve Velké Británii jako seskupené osvědčených postupů, které lze přizpůsobit každé organizaci. (McCarthy, 2012)

Mezi nejvýznamnější přínosy po zavedení ITIL do organizací jsou finanční úspora, spolehlivost IT služeb, efektivnější využívání ICT zdrojů a lepší úroveň komunikace IT s uživateli. (Smejkal, Sokol a Kodl, 2019)

3 KYBERNETICKÁ BEZPEČNOST V ČESKÉ REPUBLICE A EVROPSKÉ UNII

V následujících kapitolách budou popsány klíčové dokumenty kybernetické bezpečnosti, které jsou platné na území České republiky či Evropské unie. Jedná se o Národní strategii kybernetické bezpečnosti ČR, Akční plán k národní strategii kybernetické bezpečnosti ČR a Zprávu o stavu kybernetické bezpečnosti za rok 2021.

3.1 Národní strategie kybernetické bezpečnosti ČR

Národní strategie kybernetické bezpečnosti České republiky je dokument, který vyšel dne 2. prosince 2022 na období let 2021 – 2025. Strategie je cílena na bezpečnostní složky státu a další subjekty veřejné správy, ale zároveň podporuje a informuje ostatní části české společnosti, které se tak mají možnost dozvědět a lépe pochopit strategii státu při řešení kybernetických hrozeb. Dále má Národní strategie kybernetické bezpečnosti charakter informační, aby bylo možné využívat kyberprostor a moderní technologie bezpečně. (NÚKIB, 2022)

Dokument je dělen na tři hlavní strategické sekce a jejich jednotlivé strategické cíle. Jedná se o následující sekce: sebevědomě v kyberprostoru, silná a spolehlivá společenství a odolná společnost 4.0. Všechny tři sekce společně seskupují strategické cíle, jako jsou například: celonárodní přístup, sdílení informací, silné zabezpečení prvků kritické infrastruktury, prosazování zájmů ČR v zahraničí, mezinárodní spolupráce a vzdělávání. Hlavním cílem strategie je posílení bezpečnosti a odolnosti České republiky v kyberprostoru. (NÚKIB, 2022)

3.2 Akční plán k národní strategii kybernetické bezpečnosti ČR na období let 2021 až 2025

Akční plán k národní strategii kybernetické bezpečnosti ČR na období let 2021 až 2025 vyšel dne 26. července 2021 a je v gesci Národního úřadu pro kybernetickou a informační bezpečnost, který zajišťuje jeho vypracování. Jedná se o dokument, prostřednictvím kterého by mělo být naplněno a dosaženo vytyčených cílů obsažených v Národní strategii kybernetické bezpečnosti ČR pro stejné období. Pro jednotlivé sekce výše zmíněné strategie jsou určeny jednotlivé úkoly, každému úkolu je přidělen číselný kód, určen odpovědný subjekt a časový rámec, kdy má být určený úkol splněn. Například pro sekci Sebevědomě v kyberprostoru je jedním z úkolů efektivní a koordinovaná spolupráce mezi Národním

úřadem pro kybernetickou bezpečnost, Policií ČR a zpravodajskými službami v rámci kybernetické bezpečnosti. Pro tento úkol jsou jako odpovědný subjekt určeny NÚKIB, PČR a zpravodajské služby a úkol má být plněn průběžně. (NÚKIB, 2021)

3.3 Zpráva o stavu kybernetické bezpečnosti za rok 2021

Zpráva o stavu kybernetické bezpečnosti je dokument, jehož zpracování zajišťuje NÚKIB a je vydáván každý rok vždy zpětně. Zpráva svým obsahem definuje kybernetickou bezpečnost v daném roce, kybernetické hrozby a hlavní aktéry, cíle kybernetických útoků, vybraná opatření a výhled trendů na následující období, tedy na roky 2022 a 2023. (NÚKIB, 2022)

Ze zprávy je patrné, že rok 2021 zaznamenal nárůst škodlivých kybernetických aktivit, které probíhaly na celém území České republiky a evidoval je Národní bezpečnostní úřad pro kybernetickou bezpečnost a i dle Policie ČR došlo k nárůstu kybernetických kriminálních aktivit. Mezi nejčastější útoky jsou řazeny: phishing, podvodné e-maily a skenování vnější sítě. (NÚKIB, 2022)

NÚKIB vydal celkem 26 upozornění na aktuálně probíhající hrozby a celkem 157 kybernetických incidentů bylo řešeno ve spolupráci s NÚKIB. V roce 2021 bylo evidováno 9581 trestných činů v oblasti kybernetické kriminality a kriminality páchané na internetu. Bylo uspořádáno 14 tematických cvičení, kterých se účastnilo dohromady 490 účastníků. (NÚKIB, 2022)

Další významnou činností NÚKIB bylo uspořádání třetího ročníku Prague 5G Security Conference, která byla zaměřena na bezpečnost 5G sítí a technologií. Na této konferenci byly představeny Pražské návrhy týkající se kybernetické bezpečnosti přelomových technologií a Pražské návrhy týkající se diverzity dodavatelů komunikací. (NÚKIB, 2022)

NÚKIB se velmi angažuje i ve vzdělávání zaměstnanců veřejné správy a v organizaci online kurzů, jako jsou: Dávej kyber!, Šéfuj kyber!, Bezpečně v kyber!. V rámci vzdělávacího programu probíhaly další osvětové akce pro děti, mládež a širší veřejnost. (NÚKIB, 2022)

V době zpracování diplomové práce byla k dispozici Zpráva o stavu kybernetické bezpečnosti za rok 2021.

3.4 Národní úřad pro kybernetickou a informační bezpečnost

NÚKIB neboli Národní úřad pro kybernetickou a informační bezpečnost má v gesci problematiku kybernetické a informační bezpečnosti včetně ochrany utajovaných informací. Jedná se o ústřední správní orgán, který vznik dne 1. srpna 2017 zákonem č. 205/2017 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. Tento zákon nahradil starší zákon č. 181/2014 Sb., o kybernetické bezpečnosti. (NÚKIB, 2022)

Zástupce Národního úřadu pro kybernetickou a informační bezpečnost je součástí zasedání Bezpečnostní rady státu. Funkci zastává nynější ředitel Ing. Lukáš Kintr. Ředitel je zároveň členem Výboru pro kybernetickou bezpečnost. Tento výbor je jedním ze stálých pracovních orgánů Bezpečnostní rady státu k zajišťování kybernetické bezpečnosti České republiky. (NÚKIB, 2022)

Národní úřad pro kybernetickou bezpečnost je organizačně rozdělen do několika sekcí. Jedná se o sekce: personalistiky, práva a provozu, bezpečnosti, Národního centra kybernetické bezpečnosti (NCKB), informačních systémů, strategických agend a spolupráce a kabinet ředitele. V rámci každé uvedené sekce je zřízeno několik oddělení. Dále se v organizačním členění NÚKIB nachází bezpečnostní ředitel, manažer kybernetické bezpečnosti, architekt kybernetické bezpečnosti, auditor kybernetické bezpečnosti, interní auditor a pověřenec pro ochranu osobních údajů. Poslední organizační složkou je Rozkladová komise ředitele NÚKIB. (NÚKIB, 2022)

Jednou z výkonných sekcí Národního úřadu pro kybernetickou a informační bezpečnost je Národní centrum kybernetické bezpečnosti neboli NCKB, které se soustřeďuje na zajištění:

- Činnosti vládního CERT ČR.
- Prevenci před kybernetickými hrozbami, které jsou zaměřeny na prvky kritické infrastruktury a dalším významným informačním systémům.
- Řešení a koordinaci kybernetických bezpečnostních incidentů.
- Vzdělání v oblasti kybernetické bezpečnosti.
- Národní i mezinárodní spolupráci.
- Kybernetická cvičení.
- Výzkum a vývoj o oblasti kybernetické bezpečnosti.
- Vyhodnocení rizik a přijímání příslušných opatření.

- Plnění mezinárodních závazků na úrovni NATO a EU.
- Komunikační strategie v rámci kybernetické bezpečnosti.
- A další. (NCKB, 2022)

3.5 CERT A CSIRT

CERT neboli Computer Emergency Responce Team a CSIRT neboli Computer Security Incident Response Team jsou dva typy týmů, které svou působností zodpovídají za řešení bezpečnostních incidentů a hrozeb. Jedná se tedy o místo, kam je možné se obrátit při zjištění bezpečnostního incidentu pro pomoc, informace či spolupráci.

Tyto týmy působí v jednotlivých organizacích, jak v organizacích, které zprostředkovávají chod internetu, tak v organizacích, kde je internet využíván k hlavním činnostem společnosti. (Kolouch a Bašta, 2016)

CERT i CSIRT v organizacích představují tým, kam se mohou uživatelé obrátit pro pomoc se zjištěným bezpečnostním problémem, ten by měl být odpovědným týmem prozkoumán

a vydáno opatření. (Kolouch a Bašta, 2016)

CERT/CSIRT týmy jsou zapojeny do světové bezpečnostní infrastruktury, kde probíhá sdílení informací a dodržování stanovených formálních postupů. Obecně pak lze tyto týmy označovat jako část infrastruktury, která prověřuje a řeší bezpečnostní problémy internetu. Pro svou práci využívají svých zkušeností, předem připravených postupů, praxe a spolupráce s ostatními CERT/CSIRT týmy. (Kolouch a Bašta, 2016)

CERT/CSIRT tým by měl mít veřejně přístupné kontakty a pravidla činnosti, jako jsou:

- Kdo je provozovatel.
- Kdo jsou členové týmu.
- Jak a kdy je možné tým zastihnout a kontaktovat.
- Nabízené služby.
- Pole působnosti – na kterou oblast se tým soustřeďuje a zda je způsobilý vykonávat svou činnost. (Kolouch a Bašta, 2016)

Přítomnost alespoň jednoho CERT/CSIRT týmu je nezbytná v každé provozované síti. Na úrovni jednotlivých států mají svoji určenou roli vrcholové týmy – národní a vládní CERT/CSIRT. (Kolouch a Bašta, 2016)

Národní CERT/CSIRT je poslední kompetentní úřad, na který je možné se obrátit v případě žádosti o pomoc, zásah či intervenci. Jeho hlavním cílem je zajištění kontaktu mezi napadeným a zdrojem problému a zajistit úspěšné řešení. Tyto týmy zpravidla nemají možnost přímého zásahu. Dále je zodpovědný za vzdělání a spolupráci v rámci široké veřejnosti a internetové infrastruktury, podporuje vznik jednotlivých CERT/CSIRT týmů ve státě, zprostředkovává jejich uvedení do mezinárodního působiště a spolupracuje při zavádění standartních postupů a procedur. (Kolouch a Bašta, 2016)

Oproti tomu vládní CERT/CSIRT týmy se soustřeďují na bezpečnostní incidenty ohrožující bezpečnost státu a jeho služeb v oblastech státní správy a samosprávy. Dle zákona 181/2014 Sb., o kybernetické bezpečnosti jsou úkoly a kompetence vládního CERT/CSIRT týmu následující:

- Přijímat hlášení o kybernetických bezpečnostních incidentech a vyhodnocuje jejich obsah.
- Poskytovat metodickou pomoc určeným orgánům a osobám.
- Poskytovat součinnost při kybernetické bezpečnostní události.
- Přijímat údaje od národního CERT a zajišťovat jejich vyhodnocení.
- Provádět hodnocení zranitelností v oblasti kybernetické bezpečnosti.
- Plnit roli CSIRT dle předpisu EU, spolupracovat s ostatními týmy jiných členských států a další. (Česko, 2014)

CERT –EU je skupina pro reakci na počítačové hrozby, v orgánech, institucích a dalších subjektech EU, jejíž cílem je zajištění bezpečnosti infrastruktury IKT na všech uvedených úrovních EU. Skupina byla zřízena v roce 2011 se sídlem v Bruselu a tvoří ji tým 45 odborníků na IT bezpečnost. Tým shromažďuje, řídí, analyzuje a sdílí informace s orgány, institucemi a ostatními subjekty EU o hrozbách, zranitelnosti a incidentech, které bezprostředně souvisí s infrastrukturou IKT. Svou činností se soustřeďuje na prevenci, odhalování a zmírňování dopadů kybernetických útoků a reakcí na ně. (CERT-EU, 2023)

CERT-EU spolupracuje s ostatními skupinami CERT jednotlivých států v rámci EU i mimo ni a ostatními mezinárodními partnery, a tím pomáhají zlepšit a zprostředkovat výměnu informací v rámci EU i mimo ni. (CERT-EU, 2023)

4 DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI

Teoretická část byla věnována definicím a charakteristikám jednotlivých oblastí informačních a komunikačních technologií a kybernetické bezpečnosti. Dále byly vymezeny základní principy kybernetické bezpečnosti. Nedílnou součástí teoretické části je legislativní rámec, kde byly uvedeny klíčové zákony, vyhlášky, normy a metodiky kybernetické bezpečnosti. Stěžejními legislativními dokumenty jsou zákon č. 181/2014 Sb. o kybernetické bezpečnosti, vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti a směrnice NIS 2. V brzké době proběhne novelizace zákon 181/2014 Sb., o kybernetické bezpečnosti, který ve svém znění bude mít implementované zásady směrnice NIS 2. V závěrečné kapitole teoretické části byly uvedeny jednotlivé úřady či vybrané subjekty podílející se na zvyšování kybernetické bezpečnosti. Součástí kapitoly jsou i tři klíčové dokumenty zpracované Národním úřadem pro kybernetickou a informační bezpečnost. Jedná se o Národní strategii kybernetické bezpečnosti ČR, Akční plán k národní strategii kybernetické bezpečnosti ČR na období let 2021 až 2025 a Zprávu o stavu kybernetické bezpečnosti za rok 2021, která byla v době zpracování diplomové práce poslední vydanou.

II. PRAKTICKÁ ČÁST

5 CHARAKTERISTIKA VYBRANÉHO SUBJEKTU

Subjekt, který pro účely vypracování diplomové práce byl vybrán, je výrobní firma zabývající se zpracováváním kovů a jejich dílů. Jedná se o německou společnost vyrábějící nástavby pro užitková vozidla, přívěsy a návěsy nákladních automobilů.

5.1 Historie a oblast zaměření

Vznik společnosti se datuje od roku 1934, kdy Franz Xaver pokračoval v kolářské výrobě po svém otci. Během následujících několika desetiletí se společnost postupně rozvíjela a automatizovala. V této době se výroba zaměřovala na jednotlivé typy návěsů a přívěsů pro různé účely. Jednalo se především o vozy pro zemědělské a chladírenské využití a využití v dopravě. V devadesátých letech minulého století byla společnost zakoupena novým německým majitelem, který již byl vlastníkem jedné výrobní firmy. Nyní tyto dvě společnosti pracují navzájem provázaně a výrobní linky jsou na sobě závislé. (OS 45, 2022)

Společnost má mnoho poboček. Většina z nich je soustřeďována do zahraničí, zejména pak do Německa, kde je centrální sídlo společnosti, dále do České republiky, Španělska, Běloruska, Francie, Bulharska, Dánska či Rakouska. (OS 45, 2022)

Výrobní pobočka společnosti – vybraný subjekt je jedním z nejmodernějších výrobních závodů pro výrobu podvozkových rámů, přívěsů a návěsů, které splňují nejnovější standardy německé kvality. Sídlo společnosti se nachází v okrese Ústí nad Orlicí v Pardubickém kraji. Závod má taktéž dlouhou historii. Byl otevřen již v roce 1939 jako výrobní závod pro výrobu letadel. Následně výrobu převzal český spolek a probíhala zde výroba chladírenských vozů. V roce 1996 byl závod zakoupen německou společností. Výrobní závod má ve výrobě vozů dlouhou historii, která je známá svou kvalitou v oblasti výroby. (OS 45, 2022)

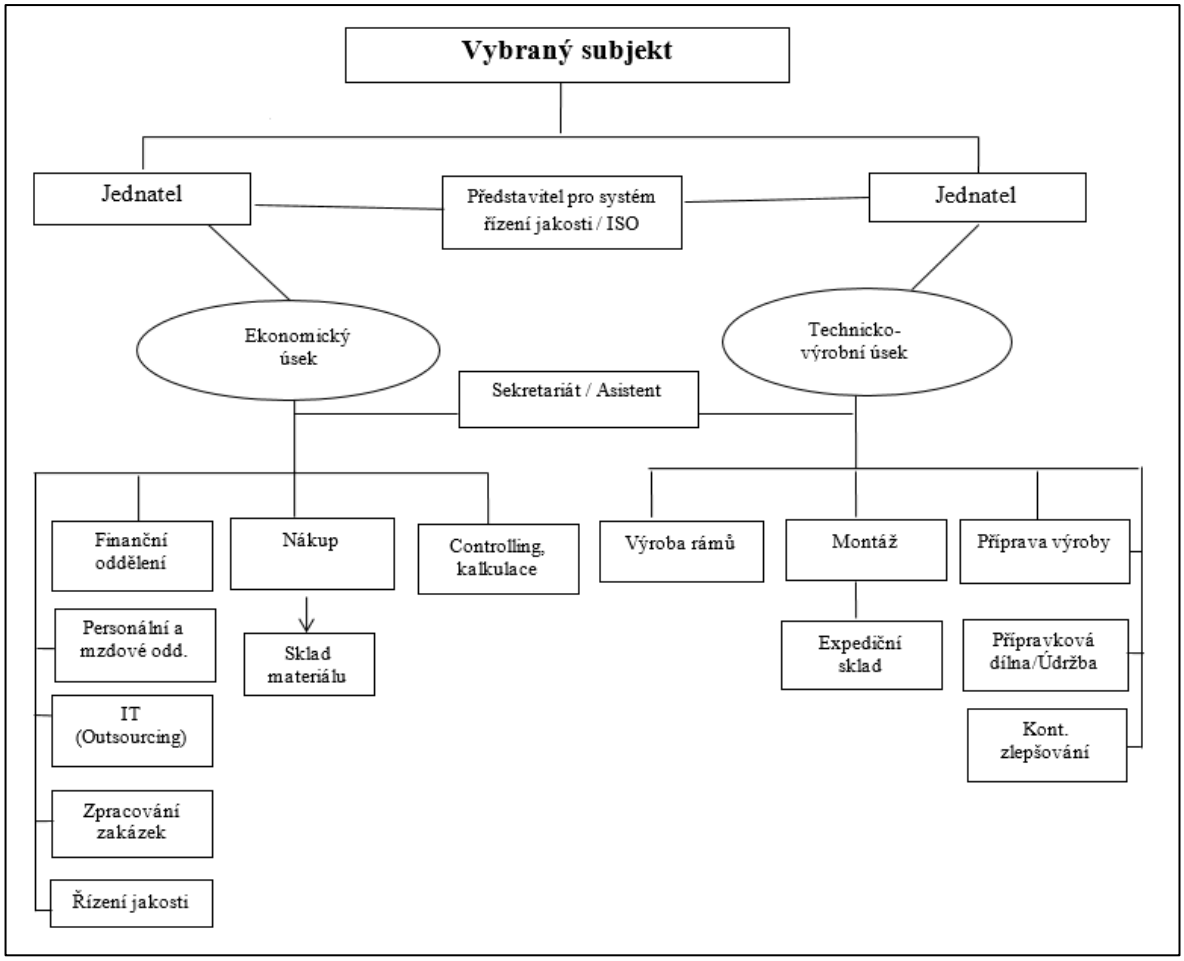
5.2 Struktura subjektu a jednotlivá střediska

Společnost zastupují dva hlavní jednatelé – ředitelé. Jeden z ředitelů má v gesci personální a finanční chod společnosti, druhý se zabývá technickou otázkou výroby a zajišťováním dodavatelů jak jednotlivých surovin, tak zpracovaných dílů a soustřeďuje se na oblast montáže a expedici hotových návěsů a přívěsů. Dle zaměření hlavních jednatelů se společnost dále dělí na technicko- výrobní a ekonomický úsek. Vzhledem ke skutečnosti, že výroba podvozkových rámů, návěsů a přívěsů probíhá ve dvou etapách, tak je technicko-výrobní úsek rozdělen na svařovny a montáž a dále na jednotlivá střediska. Každá ze dvou skupin má svého vedoucího. Ti mají na starosti fungování jednotlivých úseků. Jednotlivá

střediska mají každé svého vedoucího – mistra výroby, nebo kompetentní osobu, která je za svůj úsek zodpovědná. (OS 45, 2022)

Ostatní střediska lze označovat jako střediska nevýrobní. Jedná se především o sklady materiálu, kontrolu hotových výrobků, personální oddělení, finanční úsek, konstrukci, oddělení controllingu a kalkulací. Dále se zde nachází oddělení svářečské školy, údržby, nákupní oddělení a oddělení IT, které je zabezpečováno externí firmou, která sídlí v nedalekém městě. Výrobní závod nyní zaměstnává okolo 400 zaměstnanců. (OS 45, 2022)

Struktura společnosti je přehledněji zachycena v následujícím schématu.



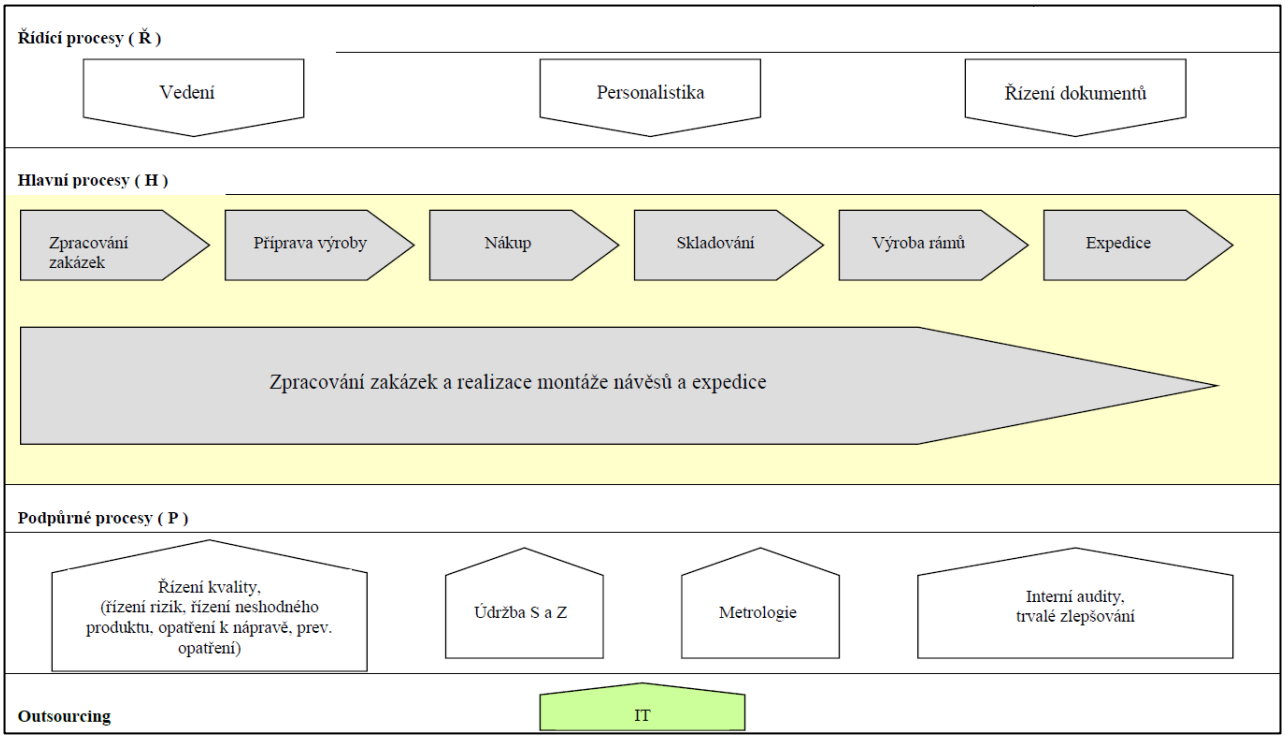
Obrázek 5 Schéma vybraného subjektu. Zdroj: (interní organizační směrnice), (vlastní)

5.3 Definice procesů ve společnosti

Společnost se řídí ISO normou 9001, která svým obsahem definuje a určuje řízení kvality a jeho požadavky v organizacích. Dle požadavků této normy byla vytvořena interní příručka systému řízení kvality. Příručka v několika kapitolách definuje historii a hlavní cíle společnosti, popis jednotlivých procesů, kontext organizace a jednotlivé části procesu

systému managementu kvality v oblastech vedení, plánování, podpory, provoz, hodnocení výkonosti a zlepšování. (OS 45, 2022)

Struktura procesů, které podléhají systému kvality řízení a určeného certifikačního auditu, který má v gesci kontrolu a dodržování uvedených jednotlivých bodů ISO normy, je uvedena na následujícím schématu. (OS 45, 2022)



Obrázek 6 Schéma procesů vybraného subjektu. Zdroj: (interní organizační směrnice), (vlastní)

5.4 Analýza vnitřního a vnějšího prostředí subjektu

Pro analýzu vnitřního a vnějšího bezpečnostního prostředí byla použita SWOT analýza, prostřednictvím které bude určena výsledná strategie, která může pomoci vybranému subjektu dosáhnout vymezených cílů a zároveň určí další postupy v následných analýzách této práce.

Konkrétní SWOT analýza pro vybraný subjekt této diplomové práce je uvedena na následujících stranách, kde jsou definovány silné, slabé stránky, příležitosti a hrozby, které společně tvoří vnitřní a vnější prostředí. Následně jsou jednotlivé složky označeny váhami a hodnoceny. Z každé jednotlivé části je uveden součet a provedeno vyhodnocení za vnitřní a vnější prostředí.

Tabulka 3 SWOT analýza subjektu. Zdroj: (vlastní)

SWOT analýza pro vybraný subjekt		
Vnitřní prostředí	**Silné stránky**	**Slabé stránky**
	Velikost firmy - součást koncernu	Nedostatečné školení zaměstnanců
	Kvalitní technické vybavení	Nevyhovující řízení rizik
	Organizační struktura	Nedostatečná zastupitelnost zaměstnanců
	Firemní know - how	Špatně definované odpovědnosti za aktiva
	Proaktivní management	Nedostatečné zabezpečení subjektu
Vnější prostředí	**Příležitosti**	**Hrozby**
	Implementace řízení rizik	Nedbalost zaměstnanců
	Zabezpečení zastupitelnosti zaměstnanců	Ztráta triády CIA
	Určení odpovědnosti	Nedůsledná kontrola systému
	Zabezpečení subjektu	Podceňování hrozeb pro subjekt
	Školení zaměstnanců	Nová konkurence

První částí vnitřního prostředí jsou silné stránky. Mezi silné stránky vybraného subjektu patří velikost firmy. Jedná se o německou společnost, která je součástí koncernu. Společnost sídlící v České republice je jedna z mnoha velkých poboček rozmístěných po celé Evropě. Hlavní sídlo sesterské společnosti se nachází v Německu, stejně tak mateřská společnost. Obchodování probíhá v rámci koncernu, kdy česká strana zajišťuje jak součásti, tak hotové produkty. Oproti tomu německá strana komunikuje a obchoduje s koncovým zákazníkem. Skutečnost, že je vybraný subjekt součást velké obchodní skupiny, zajištuje jeho stabilní pozici na evropském trhu.

Kvalitní technické vybavení je další uvedenou silnou stránkou. Subjekt disponuje technickým vybavením jak pro jednotlivé zaměstnance, tak technickým vybavením, které je nutné k samotné výrobě. Vybraní zaměstnanci jsou vybaveni technickým vybavením pro výkon své pracovní pozice. Pro skupinu technicko- hospodářských pracovníků se jedná zejména o notebooky, mobilní telefony, pevné linky, stolní počítače, tiskárny a další speciální vybavení například čtečky přístupových karet. Pro samotnou výrobní část subjektu jsou vyčleněny technické prostředky ve formě speciálního elektronického vybavení a několika moderních a nových robotizovaných pracovišť.

Organizační struktura subjektu je na svou velikost dobře přehledná a poskytuje přesné vymezení jednotlivých pracovišť a zároveň určuje hierarchii a vedoucí pracovníky. Hierarchie subjektu je zobrazena ve formě organizačního schématu v první kapitole praktické části této práce.

Jako každá výrobní společnost tak i vybraný subjekt vlastní své výrobní know – how. Jedná se o technické výrobní postupy, které jsou před konkurencí utajovány a vybraný subjekt a jeho výroby jsou jimi specifické.

Za výraznou silnou stránku subjektu lze označit jeho management. V české části společnosti je management velmi proaktivní, který se nebrání inovacím jak ve výrobním úseku, tak v ostatních částech společnosti. Každoročně subjekt prochází několika audity, kdy jsou jedním z témat novinky a postupné zlepšování výrobních a ostatních procesů. Management je otevřen názorům a návrhům ze stran zaměstnanců, tak i zavádění nových standardů.

Druhou částí vnitřního prostředí jsou slabé stránky. Jako slabou stránku vybraného subjektu lze uvést nedostatečné školení zaměstnanců v rámci problematiky kybernetické bezpečnosti a nevyhovující řízení rizik. Vysoká důvěra v technologie a neznalost aktuálních hrozeb dané problematiky je pro subjekt velmi slabou stránkou.

Subjekt má zastoupenou každou pracovní pozici, která je vytvořena. Na každé pracovní pozici, kromě těch výrobních, je z velké části pouze jeden pracovník, který má v gesci výkon pozice. V případech nepřítomnosti nebo neschopnosti daného jedince vykonávat svou funkci přechází jeho povinnosti na určeného zaměstnance či přímého nadřízeného. Ve vybraném subjektu není problematika zastupitelnosti dostatečně řešena, malé množství pracovních pozic je zabezpečeno vhodným náhradníkem, který je danou funkci schopen vykonávat. Tato skutečnost a bezpečnostní situace posledních let vedla společnost k vybavení vybraných klíčových zaměstnanců novým technickým vybavením a zřízením domácích kanceláří pro výkon zaměstnání formou home office. Tato forma je hojně využívána jak při krátkodobých, tak dlouhodobých absencích ze strany zaměstnanců, kdy prostřednictvím vzdáleného přístupu k intranetu společnosti si každý pověřený zaměstnanec vykonává své pracovní povinnosti z domova a přizpůsobuje si výkon práce svým časovým, zdravotním či jiným skutečnostem. Touto formou výkonu povolání je nedostatečná zastupitelnost z části řešena, nicméně nejsou ošetřeny případy, kdy dotyčný zaměstnanec není schopen výkonu práce v žádné míře.

Další slabou stránkou vybraného subjektu jsou špatně definované odpovědnosti za kybernetická a informační aktiva. Většinu aktiv spravuje IT technik, který je na celou společnost vymezen pouze jeden. Nicméně každý zaměstnanec, který má svěřena k výkonu povolání nějaká informační a kybernetická aktiva, by měl být odpovědný za jejich správné užívání dle směrnic společnosti.

Poslední vybranou slabou stránkou je fyzické zabezpečení celého subjektu. Vybraný subjekt má jednu hlavní vrátnici, která je otevřena 24 hodin 6 dní v týdnu. Od sobotního odpoledne do nedělního podvečera je vrátnice uzavřena a tím i celý komplex. Vrátnice je střežena kamerovým systémem stejně tak hlavní výrobní haly. Nicméně subjekt se rozprostírá na velké ploše, kterou z velké část ohraničuje pouze pletivový plot. Celý subjekt není pod kamerovým dohledem.

Vnější prostředí je tvořeno příležitostmi a hrozbami pro vybraný subjekt. Jako jedna z největších příležitostí je zlepšení zabezpečení vybraného subjektu. Dokonalejším a modernějším zabezpečením bude dosaženo větší bezpečnosti pro aktiva, která jsou klíčová pro vybraný subjekt.

Mezi další příležitosti je řazeno určení odpovědnosti za vybraná aktiva. Za předpokladu přesného stanovení, kdo za jaká aktiva odpovídá, kdyby byla odpovědnost přenesena na více zaměstnanců a tím by se subjekt stal v této části více samostatný a méně závislý na IT technikovi. V souvislosti s touto příležitostí je i nutné pravidelné školení zaměstnanců v oblasti kybernetické a informační bezpečnosti, které by zvyšovalo podvědomí všech pracovníků o nebezpečnosti a výskytu kybernetických hrozeb, nezbytnosti ochrany kybernetických a informačních aktiv a správné manipulace s nimi. Stejná důležitost je přiřazena i zabezpečení zastupitelnosti jednotlivých zaměstnanců a jejich kvalifikování pro určitou pracovní pozici, aby byla zajištěna adekvátní náhrada pro případ nepřítomnosti kompetentního zaměstnance.

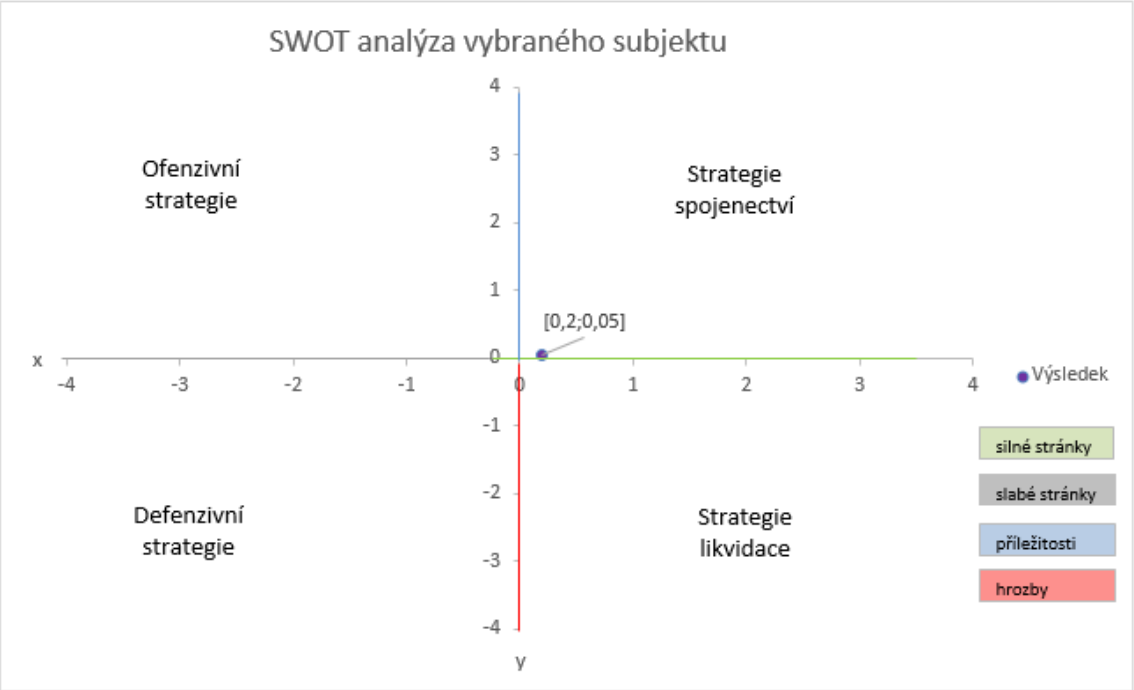
Druhou částí vnějšího prostředí jsou hrozby pro vybraný subjekt. Jako nejvýznamnější hrozbu lze označit ztrátu triády CIA, tedy narušení důvěrnosti, integrity a dostupnosti informací subjektu. Pokud dojde z jakéhokoli důvodu k narušení, nejsou v tu chvíli informace, které jsou vybraným pracovníkům k dispozici důvěryhodné, dostupné či komplexní a nelze s nimi nijakým způsobem pracovat. Mezi další významné hrozby je řazeno nedbalé chování zaměstnanců, kteří úmyslně či neúmyslně mohou být velkým zdrojem hrozeb jak pro vybraná aktiva, tak pro celou společnost. S chováním zaměstnanců úzce souvisí i nedůsledná kontrola systému či podceňování stávajících či nových hrozeb, se

kterými se vybraný subjekt potýká nebo může potýkat v následujících letech. Jako poslední významná hrozba byla definována nová konkurence na trhu. Uvedené složky, váhy a hodnocení byly konzultovány s odpovědným pracovníkem vybraného subjektu.

Tabulka 4 SWOT analýza subjektu – hodnocení jednotlivých složek. Zdroj: (vlastní)

Typ	Složka	Váha	Hodnocení	Výsledný součin	Výsledný součet
Silné stránky	Velikost firmy - součást koncernu	3	0,15	0,45	4
	Kvalitní technické vybavení	4	0,20	0,8	
	Organizační struktura	3	0,15	0,45	
	Firemní know - how	5	0,30	1,5	
	Proaktivní management	4	0,20	0,8	
Slabé stránky	Nedostatečné školení zaměstnanců	-2	0,15	-0,3	-3,8
	Nevyhovující řízení rizik	-3	0,20	-0,6	
	Nedostatečná zastupitelnost zaměstnanců	-4	0,15	-0,6	
	Špatně definované odpovědnosti za aktiva	-5	0,30	-1,5	
	Nedostatečné zabezpečení subjektu	-4	0,20	-0,8	
Příležitosti	Implementace řízení rizik	3	0,15	0,45	4
	Zabezpečení zastupitelnosti zaměstnanců	4	0,2	0,8	
	Určení odpovědnosti	4	0,2	0,8	
	Zabezpečení subjektu	5	0,3	1,5	
	Školení zaměstnanců	3	0,15	0,45	
Hrozby	Nedbalost zaměstnanců	-4	0,25	-1	-3,95
	Ztráta triády CIA	-5	0,30	-1,5	
	Nedůsledná kontrola systému	-4	0,20	-0,8	
	Podceňování hrozeb pro subjekt	-3	0,15	-0,45	
	Nová konkurence	-2	0,10	-0,2	
Vnitřní prostředí		**0,2**			
Vnější prostředí		**0,05**			

Dle výše uvedeného schématu strategií v jednotlivých kvartálech SWOT analýzy je patrné, že výsledek vnějšího a vnitřního prostředí se pohybuje v mezích prvního kvadrantu, který odpovídá strategii spojenectví, při které subjekt využívá k dosažení vytyčených cílů svých silných stránek.



Obrázek 7 Graf SWOT analýza. Zdroj: (vlastní)

Na základě této analýzy bude nejvýhodnějším řešením zavedení principu a zásad kybernetické bezpečnosti za podpory managementu, kdy bude na základě vyhodnocení analýzy RISKAN vytvořena interní směrnice pro zaměstnance, která bude návodem pro správné zacházení s kybernetickými aktivy.

6 IDENTIFIKACE KYBERNETICKÝCH A INFORMAČNÍCH AKTIV

Při posuzování aktuálního stavu kybernetické bezpečnosti byla vymezena a charakterizována vybraná aktiva, které následně budou využita v rámci analýzy rizik.

Aktiva jsou definována jako majetek společnosti, tedy vše, co společnost vlastní a je ekonomicky využitelné pro dané podnikání. Může být ve formě hmotné – budovy, počítačové systémy, sítě či energie, nebo ve formě nehmotné jako jsou informace, znalosti, data či programy. (Česko, 2018).

Aktiva jsou svou podstatou dělena na primární a podpůrná. Definice jednotlivých druhů aktiv je následující:

- Primární aktivum – je charakterizováno jako informace, jednotlivé procesy a činnosti, které v případě vlivu hrozeb mohou mít negativní vliv na celkový chod společnosti. (Kolouch a Bašta, 2019)
- Podpůrné aktivum – je technické vybavení, pracovníci či jednotliví subdodavatelé, kteří se podílejí na fungování a rozvoji organizace. (Kolouch a Bašta, 2019)

6.1 Primární aktiva subjektu

Pro vybranou společnost byla identifikována a blíže charakterizována následující primární aktiva.

6.1.1 Procesy a činnosti

Jednotlivé procesy a činnosti ve vybraném subjektu korespondují s organizační strukturou, která je dělena na jednotlivá oddělení a střediska. Tato kapitola se soustřeďuje na popis činností a procesů, které probíhají na jednotlivých odděleních a střediscích.

Oddělení jednatelů (č. 1) – v době zpracování diplomové práce jsou ve vedení české části společnosti dva hlavní jednatelé, kteří se soustřeďují na různá odvětví. Jedná se o:

- Finanční a personální jednatel – zodpovídá za veškeré finanční toky, které ve společnosti probíhají, schvaluje platby, podepisuje jednotlivé finanční smlouvy, zařizuje finanční a operativní leasingy a další. Dále je v jeho gesci personální problematika, kdy je zodpovědný za to, že ve společnosti bude

potřebné množství kvalifikovaných zaměstnanců na jednotlivých pozicích, které vyplývají z ročního výrobního a finančního plánu. (QMS 09, 2022)

- Technicko- výrobní jednatel – se soustřeďuje na výrobní plán a jeho technické zabezpečení, kdy plánuje výrobní zakázky a jejich načasování a zpracování, jednotlivé spolupráce se subdodavateli surovin či jednotlivých dílů, zabezpečuje modernizaci výroby a technické zdokonalování či robotizaci. (QMS 09, 2022)

Oddělení asistenta vedení společnosti (č. 2) – na tomto oddělení vykonává zaměstnanec podpůrné činnosti pro jednatele, zpracovává podklady a organizuje jednotlivé schůzky a soustřeďuje se na jejich průběh, dále je v jeho gesci fakturace největších zakázek pro společnost, je zodpovědný za aktuálnost všech smluv a organizačních směrnic. (QMS 09, 2022)

Personální oddělení (č. 3) – svou činností se zaměřuje na propagaci společnosti, nábor nových kvalifikovaných zaměstnanců, dále zodpovídá za aktuálnost školení potřebných pro výkon jednotlivých pracovních pozic. V neposlední řadě se personální oddělení soustřeďuje na zpracování mezd, spolupráci s externími agenturami práce o dodávání vybraných pracovníků na neobsazené pracovní pozice, komunikaci s jednotlivými úřady, jako jsou Úřad práce České republiky, Česká správa sociálního zabezpečení, či Český statistický úřad. Vzhledem ke skutečnosti, že společnost zaměstnává pracovníky různé národnosti, je pro toto oddělení nezbytná i komunikace s Policií ČR, respektive se Službou cizinecké policie. (QMS 10, 2022)

Oddělení vedoucí výroby (č. 4) – toto oddělení je zodpovědné za celou jednu výrobní část, ve které probíhá koordinace jednotlivých částí zakázek na určená výrobní střediska a jejich časové zpracování, má v organizačním schématu několik podřízených mistrů, se kterými každý den probírají výrobní plán a koordinují pracovní postupy. (QMS 10, 2022)

Finanční oddělení (č. 5) – zpracovává veškeré finanční toky ve společnosti, účtují jednotlivé faktury do účetního systému, vystavují faktury subdodavatelům a zpracovávají jednotlivé finanční analýzy. (OS 13, 2022)

Oddělení konstrukce (č. 6) – na tomto oddělení probíhá veškerá technická příprava obou částí výroby – jak části svařoven, tak části montáže. Zaměstnanci zde vytváří výkresy jednotlivých dílů a celých výrobků, tyto pak zakládají do interního systému a poskytují výkresy pro výrobní část, komunikují s oddělením konstrukce německé části společnosti a koordinují výslednou podobu zpracovaných výrobků. (QMS 14, 2022)

Oddělení kalkulace a ISO (č. 7) – zde probíhá kalkulace veškerých jednotlivých výrobků, které se svým obsahem liší. Zaměstnanec připravuje jednotlivé kalkulace na základě dodavatelských cen, režijních a ziskových přirážek. Dále zpracovává kalkulační analýzy a vyhodnocuje produktivitu jednotlivých středisek. Toto oddělení je i představitelem pro systém řízení jakosti – ISO, organizuje jednou za rok certifikační audit a veškeré činnosti s ním spojené. (QMS 13, 2022)

Oddělení controllingu (č. 8) – má za úkol vytváření jednotlivých analýz a vyhodnocení pro vybraný subjekt, sesterskou i mateřskou společnost, zpracovává finanční analýzy, je zodpovědné za tvoření ročního finančního plánu, vyhodnocení hospodářského výsledku za každý měsíc a jeho komparaci s vytvořeným plánem. Dále zpracovává analýzy pro jednotlivá oddělení a subdodavatele. (OS 10, 2022)

Oddělení nákupu (č. 9) – toto oddělení má za úkol vedení jednotlivých cenových nabídek, objednávku a materiálové zajištění výroby. Jednotliví zaměstnanci zpracovávají obchodní cenové nabídky a dle politiky společnosti vytvářejí objednávky na díly určené pro výrobu. Nákupní oddělení je rozděleno na dva segmenty, kdy jeden se soustřeďuje na nákup hutního materiálu, jako jsou plechy a pásnice a jejich prodej subdodavatelům. Druhý segment komunikuje se subdodavateli a zajištuje nákup dílů vyrobených z jednotlivých surovin. V gesci nákupního oddělení je i vyhodnocování jednotlivých dodavatelů. (QMS 11, 2022)

Oddělení zpracování zakázek (č. 10) – jedná se o oddělení, které je zodpovědné za přijetí a kompletní systémové ukončení zakázek. Zaměstnanec zde zpracovává přijetí zakázek, evidenci objednávek, implementaci do výrobního plánu a jejich ukončení. Svou pracovní náplní je úzce spojeno s oddělením kontroly, kdy koordinují ukončení hotových zakázek a jejich odeslání k zákazníkovi. (QMS 16, 2022)

Oddělení kontroly (č. 11) – zde jsou zaměstnanci zodpovědní za kontrolu jednotlivých hotových naskladněných výrobků, jejich odbavení. Dále se na tomto oddělení zpracovávají veškeré reklamace, které jsou subjektu nahlášeny. Jedná se o reklamace jak výrobků vyrobených zde, tak i nakupovaných dílů, které nejsou v požadované kvalitě či nesplňují vzhled výkresu. Oddělení kontroly dále zpracovává jednotlivé analýzy pro certifikační audit. (QMS 5, 2022)

Oddělení výroby – svařovny (č. 12) – do tohoto oddělení jsou zakomponovány tři jednotlivá střediska, která se podílejí na jedné části výroby. Každé středisko má svého hlavního mistra a na výrobku zpracovává jeho určenou část. Řídí se podle týdenního

případně měsíčního plánu výroby, na konci každého měsíce vytváří evidenci stavu rozpracované výroby, zpracovává podklady pro mzdy jednotlivých zaměstnanců a má zodpovědnost za každodenní chod výroby. (QMS 15, 2022)

Oddělení výroby – montáž (č. 13) – zde probíhá kompletace výrobků, kdy jednotliví zaměstnanci vytváří výrobek na přání zákazníka. Oddělení má jednoho hlavního vedoucího, který zodpovídá za plnění výrobního plánu montáže, zpracovává výrobní podklady a podklady pro mzdy jednotlivých zaměstnanců, v průběhu celého procesu provádí kontroly správnosti a úplnosti hotového výrobku. Následně je odpovědný za závěrečnou kontrolu hotového výrobku a celé jeho přezkoušení. Zaměstnanci na středisku díl následně označí identifikačním číslem a je odvezen na sklad hotové výroby a připraven k expedici. (QMS 17, 2022)

Oddělení údržby (č. 14) – zaměstnanci jsou zde zodpovědní za technickou podporu pro každé středisko, zabezpečují technický chod firmy a v případě výskytu řeší jednotlivé technické problémy spojené s výrobou či jednotlivými budovami. (QMS 8, 2022)

Oddělení skladů a expedice (č. 15) – toto středisko má v gesci příjem nakoupeného materiálu, veškerou jeho evidenci do systému, přijetí materiálu na určené sklady v souladu s organizační normou, evidenci palet či výdej materiálu na výrobní zakázky pro jednotlivá střediska. Dále je zodpovědné za každoročně prováděnou inventuru jednotlivých skladů, kdy probíhá inventarizace jednotlivých položek. (QMS 12, 2022)

Oddělení školicího střediska (č. 16) – školicí středisko je určené pro výběr vhodných zaměstnanců na jednotlivé výrobní pracovní pozice, zejména pro svářeče. Zaměstnanec na tomto středisku při výběru nového zaměstnance provede jeho částečné zaškolení a přezkoušení jeho schopností. Na základě výsledků tohoto přezkoušení je následně přijat do pracovního poměru, či nikoli. (QMS 10, 2022)

Oddělení IT (č. 17) - ve společnosti není oddělení IT interní, ale v rámci outsourcingu ho zajišťuje vybraná společnost z nedalekého města. V rámci spolupráce zajišťuje veškerou IT podporu pro chod společnosti, nakupuje a připravuje veškeré elektronické vybavení pro subjekt a jednotlivé pracovní pozice, vytváří privátní adresář, zajišťuje zálohování dat. V případě, že zaměstnanec potřebuje k výkonu své činnosti počítač či notebook, tak IT pracovník zřizuje emailové účty a jejich úpravy, administraci či školení. Dále je IT oddělení odpovědno za zprostředkování přístupu do interního systému, jako je: založení nového uživatele a jeho správu (hesla, změna jména apod.), přidělení práv ke skladům a

k referentům, editace hlaviček a patiček referentů na dokladech, reportování problémů a požadavků ke správcům interního systému, založení nových projektů pro firmu a následná kontrola průběhu projektů, technické zázemí pro běh systému - hardware (server, síť, možnost vzdálené správy) a software (OS a databáze). IT oddělení dále zajišťuje školení k software a hardware, interní telefonní linky a mobilní telefony, přístupy na internet a intranet. Dále má v gesci antivirovou kontrolu, která probíhá ve dvou samostatných systémech. (QMS 19, 2022)

Jedná se o antivirový systém na PC jednotlivých uživatelů a antivirový systém internetu.

- **Antivirový systém internetu –** kdy na vstupní bráně mezi internetem a vnitřní síti je nainstalován antivirový software, který skenuje veškerý provoz mezi internetem a vnitřní sítí. Výsledky jsou pak automaticky přeposílány do centrální konzole a následně IT oddělení k vyhodnocení. (QMS 19, 2022)
- **Antivirový systém na PC uživatelů –** kdy na každé stanici je nainstalován software, který chrání jednotlivé PC stanice. Aktuálnost virové databáze a správný chod celého systému na PC je zajištěn pomocí centrálního serveru. Nastavení serveru, kontrolu chyb při aktualizaci PC uživatelů a kontrolu výsledku antivirových testů provádí IT oddělení. (QMS 19, 2022)

6.1.2 Informace

Informace jsou klíčové pro každou firmu. Zde byly do skupiny informace zahrnuty klíčové strategické dokumenty, osobní citlivá data všech zaměstnanců a důležité dokumenty a smlouvy společnosti.

Všechny dokumenty jsou uchovávány dle směrnic společnosti v elektronické a fyzické podobě u pověřených osob. Citlivá data zaměstnanců jsou v písemné podobě uchovávána v trezoru na personálním oddělení, ostatní strategické dokumenty a citlivá data firmy jsou uchovávána na sekretariátu vedení společnosti či přímo u jednotlivých jednatelů.

Jednotlivá střediska, které zpracovávají a manipulují s různými typy dokumentů, budou níže definovány.

Oddělení jednatelů a oddělení asistenta vedení společnosti (č. 18) – uchovávají a manipulují s hlavními strategickými dokumenty celé společnosti, jedná se o know-how, jednotlivé rámcové smlouvy, obchodní dohody a smlouvy či koncernové dohody a záznamy z jednání. Dále jsou zde veškeré projektové dokumentace. (QMS 09, 2022)

Personální oddělení (č. 19) – zde jsou uchovány osobní informace zaměstnanců, jako jsou přiřazené osobní číslo, rodné číslo, adresy, kontaktní informace, informace o dosažených vzděláních, jednotlivé pracovní smlouvy a jejich podmínky, zařazení na střediska či pracovní pozici, včetně všech seznamů a popisů pracovních pozic. Dále jsou zde dokumenty systému odměňování, jako jsou souhrnné mzdové listy, podmínky motivačních a zaměstnaneckých bonusů a celý systém. (QMS 10, 2022)

Oddělení vedoucí výroby (č. 20) – vedoucí výroby má přístup k jednotlivým výrobním postupům, včetně všech výkresů a návodů, uchovává výrobní plány. (QMS 10, 2022)

Finanční oddělení (č. 21) – zde jsou uloženy veškeré účetní doklady, faktury, smlouvy o finančním a operativním leasingu na jednotlivá zařízení, měsíční zprávy o hospodářském výsledku a rozvahy v německé i české podobě a rozpočtová politika společnosti. (OS 13, 2022)

Oddělení konstrukce (č. 22) – zaměstnanci konstrukce uchovávají jednotlivé výkresy a návody pro technickou přípravu výroby. (QMS 14, 2022)

Oddělení kalkulace a ISO (č. 23) – v oddělení kalkulace jsou k dispozici jednotlivé dokumenty k tvorbě ceníku a podklady k certifikačnímu auditu. (QMS 13, 2022)

Oddělení controllingu (č. 24) – zde je uchováván roční finanční plán a podklady s ním související, či veškeré podklady pro vypracování požadovaných analýz pro jednotlivé subjekty. (OS 10, 2022)

Oddělení nákupu (č. 25) – manipuluje s jednotlivými cenovými nabídkami, účetními doklady či fakturami. (QMS 11, 2022)

Oddělení IT (č. 26) – spravuje záruční listy k jednotlivým zakoupeným zařízením, osobní data uživatelů či přístupová hesla. Dále spravuje veškerou dokumentaci k síťové struktuře, systémům a jednotlivým využívaným databázím. (QMS 5, 2022)

6.2 Podpůrná aktiva subjektu

Podpůrná aktiva vybraného subjektu jsou uvedena a podrobně charakterizována v následující kapitole.

6.2.1 Osoby - zaměstnanci

Jedním z klíčových aktiv pro fungování a prosperitu celé firmy jsou osoby, které se na všem podílejí. V této skupině aktiv byly rozděleny na:

- Vedení společnosti.
- Vedoucí pracovníky.
- Bezpečnostní správci a IT pracovníci.
- Uživatelé IS.
- Ostatní zaměstnanci.

Firma zaměstnává různé národnostní skupiny zaměstnanců, kteří jsou označováni jako externí zaměstnanci. Jejich zajištění probíhá přes externí agenturu práce. V současné době je ve společnosti zaměstnáváno 130 kmenových a 230 externích zaměstnanců. Kmenoví zaměstnanci jsou většinou technicko – hospodářští pracovníci zajišťující administrativní část výroby. Externí zaměstnanci a část kmenových zaměstnanců zajišťují především výrobní část. (QMS 10, 2022)

6.2.2 Prostory a objekty

Celý objekt je ohraničen zřetelnou hranicí, kterou tvoří oplocení. Uvnitř hranic objektu se nachází všechny administrativní budovy, výrobní haly, skladovací haly a vstupní brána.
Objekt je zčásti zabezpečen kamerovým systémem a bránou. Ke vstupu je nutná vlastní identifikace osoby pomocí vstupní čipové karty, v případě vstupu pracovníků dodavatelských subjektů je pracovník zkontrolován, uveden účel vstupu a následně vstup na omezenou dobu povolen. Nicméně vstup je omezen na prostor nakládky a vykládky, případně k pracovníkovi příjmu zboží. Ostatní místa nejsou zpřístupněna.
Celý objekt se skládá z vrátnice, dvou ubytovacích zařízení, stravovacího zařízení, dvou hlavních výrobních hal, administrativní budovy a několika skladů materiálu.

6.2.3 Software

Do této skupiny jsou řazeny programy, které svou podstatou zpracovávají data a podílí se na chodu společnosti. Jedná se o:

- Operační systém - Microsoft Windows, pro mobilní zařízení též Android.
- MS Office 2013 Pro – kancelářský balíček.
- Antivirový software – ESET, Agent ESMC.
- Webový prohlížeč – desktop PC Firefox / notebook Internet Explorer nebo jiný schválený software.

- Program na prohlížení PDF dokumentu.
- ESKON – identifikační a docházkový systém BIS.
- Interní informační systém HOC. (QMS 5, 2022)

Subjekt má vytvořen svoji vlastní webovou stránku. Její správa je zabezpečována centrální pobočkou v Německu. Náš výrobní závod proto nemá kompetence pro její vytváření ani správu.

6.2.4 Hardware

Aktiva v této skupině byla uvedena jako server, mobilní výpočetní technika, tiskárny, skenery a zálohovací zařízení. Server se nachází přímo v místnosti k tomuto účelu vytvořené – serverovna. Místnost je stabilně uzamčená a vstup do ní má pouze IT pracovník, který má od místnosti klíče. Náhradní klíče od místnosti jsou uchovávány v trezoru.
Každý zaměstnanec z řad technicko hospodářských pracovníků má ke svému výkonu povolání k dispozici:

- Mobilní zařízení – vybraní zaměstnanci jsou vybaveni mobilním telefonem, většina pracovníků má k dispozici notebook. Každé zařízení je chráněno heslem a povoleno užívat pouze učenému zaměstnanci. (QMS 5, 2022)
- Uživatelská periferie – jedná se o tiskárny, kopírky, skenery, počítačové klávesnice a myši, monitory, Wifi zařízení či čtečky vstupních čipových karet či čtečky platebních karet pro finanční oddělení. (QMS 5, 2022)
- Pevné zařízení – každý vybraný zaměstnanec má zřízenou pevnou telefonní linku pro účely interní komunikace. Za určitých podmínek lze na těchto linkách zprostředkovat i komunikaci mimo subjekt. Každý zaměstnanec má přidělenou svou zkratku telefonního čísla pro účely interní komunikace. Dále je k dispozici poštovní server a veřejný web. V případě, že zaměstnanec nemá k dispozici notebook, tak je mu přidělen pevný stolní počítač. (QMS 5, 2022)

6.2.5 Technická zařízení

Do této skupiny aktiv byly uvedeny náhradní zdroje, skartovací zařízení, které je přítomno na každém jednotlivém pracovišti, ostatní kancelářská technika, jako je například tiskárna velkých výkresů do výroby, či kamerový systém. Kamerový systém je orientován především na hranice objektu, bránu, vstupy do jednotlivých budov a hlavních výrobních hal.

6.2.6 Zásoby

Ve společnosti je velké množství zásob. Jedná se o zásoby dílů a surovin pro výrobu, náhradních dílů a vyřazených komponentů IT. Všechny uvedené druhy zásob mají svůj sklad, či místnost a skladovací pokyny dle směrnic a norem.

Skladové hospodářství je v kompetenci střediska skladů, které zajišťuje příjem a výdej zásob ke zpracování dodavatelům, či příjem a výdej do výrobního procesu. (QMS 12, 2022)

Komponenty IT, které jsou již vyřazeny, podléhají správě IT technika, skladování a jejich likvidace je zabezpečována právě oddělením IT. Dle interní směrnice nesmí být žádné zařízení použito pro více osob. V praxi to znamená, že pro každého zaměstnance je zařízen vlastní počítač či notebook a další komponenty, které po dobu svého pracovního poměru využívá. Po jeho skončení jsou dané věci znepřístupněny a vyřazeny. Za předpokladu, že je uživateli pořízen počítač či notebook, vytvořen uživatelský účet, ale uživatel ho nezačal ještě aktivně používat, a nakonec nenastoupil do pracovního poměru, tak toto zařízení nemusí být vyřazeno. Uživatelský účet je odstraněn a zařízení je poskytnuto dalším novým zaměstnancům. (QMS 5, 2022)

6.2.7 Bezpečnostní dokumenty

V rámci této kapitoly jsou zařazeny bezpečnostní dokumenty, směrnice pro uživatele a auditní zprávy. V rámci roku je ve firmě provedeno několik auditů a bezpečnostních kontrol. Zároveň zde probíhá pravidelné školení v rámci BOZP a PO. Tato školení jsou zprostředkována bezpečnostní externí kompetentní firmou, se kterou společnost spolupracuje. Jednotlivá školení probíhají dle středisek a dle pracovního zaměření.

Dále jsou zde uskutečňována dílčí specializovaná školení pro provoz jednotlivých pracovišť, která jsou potřebná dle zákona pro jejich výkon. (QMS 01, 2022)

6.2.8 Subdodavatelé

Subjekt využívá ke své činnosti velkého množství subdodavatelů. Jedná se o subdodavatele činností, které nejsou vykonávány kmenovými zaměstnanci, jako jsou: úklidové služby, stravovací služby, služby bezpečnostní agentury. Dále jsou využíváni dodavatelé jednotlivých technických zařízení.

6.2.9 Ostatní

Do skupiny ostatních aktiv byly zařazeny například klíče od místností, které jsou zpravidla umístěny v budově u vstupní brány. Každý zaměstnanec je povinen klíče od svého pracoviště při odchodu z firmy odevzdat pracovníkovi na vstupní bráně a při vstupu na pracoviště znovu vyzvednout. Vynášení klíčů či jakýchkoli jiných předmětů, které jsou v majetku společnosti, podléhá schválení vedoucího úseku či samotných jednatelů společnosti. Je uděleno písemně a jeho odevzdáním pracovníkovi vrátnice je povoleno odnášet předměty ze sídla firmy.

Přístupová hesla a kódy podléhají schválené bezpečnostní politice. Pro udělení přístupových hesel a oprávnění je třeba spolupráce IT speciality, který přístupová hesla udělí pro první přihlášení do systému. Po tomto přihlášení musí být hesla změněna na taková, která splňují podmínky pro velká a malá písmena, počet znaků a číslic. Heslo musí být každé tři měsíce změněno. Tato změna je hlídána automaticky, a pokud pracovník heslo sám nezmění, tak při přihlášení do systému po něm bude změna hesla požadována. Při nedodržení této podmínky bude zaměstnanci odepřen přístup do systému.

Speciální kapitolou je od roku 2020 nově zařazena práce na home office. Každý zaměstnanec ze skupiny technickohospodářských administrativních pracovníků má umožněn přístup k firemním serverům a aplikacím z domu. Přihlášení probíhá přes VPN a aplikaci v telefonu. Při tomto druhu práce je nezbytný dvojí bezpečnostní přístup. Nejprve jsou zadány údaje jako uživatelské jméno a heslo, následně je k heslu přiřazen z mobilní aplikace přístupový šestimístný kód, který je platný pouze po dobu 30 vteřin, poté je změněn. Při správné kombinaci přihlašovacích údajů a kontrolního kódu je umožněn přístup na firemní síť a aplikace.

Každý jednotlivý zaměstnanec – kmenový i externí – má svůj autentizační předmět. Jedná se o čipovou kartu, její použití při vstupu na pozemek společnosti a do jednotlivých budov je zaznamenáno na datovém médiu a její cesta je proto snadno dohledatelná. Každá budova má svůj přístupový bod. Čipová karta slouží také jako evidence docházky do zaměstnání. Docházkový systém je spravován IT specialistou a přístup do něj mají jen vybrané osoby z personálního oddělení a oddělení controllingu. Ostatní zaměstnanci mají docházkovou aplikaci přístupnou pouze se svým jménem, pouze pro informativní účely.

Ostatní aktiva jsou dále uživatelská dokumentace, která je pro každého přístupná a k dispozici v případě potřeby. Administrátorská dokumentace je poskytována pouze

v odůvodnitelných případech a spolupráci s IT. Provozní dokumentace je vedena na jednotlivých střediscích pod dohledem vedoucích pracovníků. Je po určenou dobu přítomna na pracovišti, vyplňuje se každý pracovní den a každý rok je předmětem auditních kontrol.

6.3 Fyzické zabezpečení

Následující kapitola je věnovaná zhodnocení stavu fyzického zabezpečení subjektu jako celku, tak i jeho částí.

Zabezpečení subjektu

Subjekt se nachází v rozsáhlém areálu, který po celém svém obvodu má vybudovaný plot. Vstupní brána je nepřetržitě hlídána bezpečnostní agenturou a vjezd a výjezd je monitorován. Administrativní budova je hlídána pouze kamerovým systémem, který je soustředěn na hlavní vstupní dveře. Samotné kanceláře jsou zabezpečeny uzamykatelnými dveřmi. Výrobní haly jsou po dohledem kamerového systému, ke kterému mají přístup pouze určené osoby.

Subjekt je z hlediska ochrany před přírodními vlivy a vnějšími hrozbami chráněn pouze elektronickou požární signalizací. Jinou formou ochrany podnik nedisponuje.

Subjekt má vyčleněn prostor pro nakládku a vykládku materiálu, která probíhá separovaně. Pravidelně při každém pohybu probíhá evidence a registrace příchozích produktů. Nakládka hotových výrobků a jejich expedice probíhá odděleně.

Zabezpečení jednotlivých zařízení

Zabezpečení jednotlivých zařízení probíhá dle jednotlivých organizačních směrnic, aby byl za předpokladu nekorektního zacházení minimalizován dopad na chod organizace.

Vzhledem ke skutečnosti, že za přítomnosti zaměstnanců v kancelářích je jejich kancelář přístupná všem ostatním, jsou jednotlivá zařízení pro zpracování informací situována tak, aby nebylo umožněno sledování. Dále jsou zabezpečena heslem, které podléhá heslové politice subjektu. Zařízení jsou chráněna před výpadkem napájení a je zajištěno náhradní napájení zdroje pro celý subjekt.

Probíhají zde pravidelné servisní prohlídky, kdy je jejich průběh a výsledek zaznamenáván.

Jednotlivá zařízení, která mají svěřeny zaměstnanci k výkonu povolání, je povoleno přemisťovat bez časového omezení. Tato činnost není nijak dále kontrolována. Zpracování informací a práce mimo prostory subjektu probíhají přes vzdálený přístup a jsou řízeny

pravidly organizace. Po ukončení či přerušení práce jsou zaměstnanci povinni zamknout zařízení.

Citlivé informace ve fyzické podobě jsou uchovávány v k tomu určených kartotékách či trezorech. Každý zaměstnanec odpovídá za dokumenty, které uchovává ve fyzické podobě na svém pracovišti.

Systém zálohování dat probíhá tak, že každý uživatel má na serveru vytvořen pracovníkem IT privátní adresář, který je pojmenován příjmením uživatele. Tyto adresáře na serveru jsou umístěny na diskovém poli RAID (zde je zajištěna bezpečnost dat při výpadku jednoho z disků diskového pole) a ještě je navíc prováděna každodenní automatická záloha dat na zálohovacím zařízení.

Všichni uživatelé mají povinnost používat tyto adresáře pro ukládání firemních dokumentů. Jedině tak bude zajištěno zálohování dat. Zálohování dat na lokálních discích není prováděno a tyto dokumenty nejsou chráněny proti ztrátě nebo poškození. Dále pak na serveru existují skupinové adresáře pro jednotlivá oddělení ve firmě. Tyto adresáře podléhají stejným opatřením proti ztrátě nebo poškození. Jakékoli dokumenty, určené pro oddělení, uložené na lokálních discích, nejsou a nebudou zálohovány. Zálohování je prováděno centrálně na zálohovací zařízení o kapacitě 8,2 TB umístěné v datovém rozvaděči v ústředně. Způsoby a nastavení zálohování provádí a definuje pracovník IT. Každý den je prováděna rozdílová záloha a každý 7. den plná. Tento počet umožňuje provést obnovu dat zpětně za 7 dnů. Záloha se provádí v nočních hodinách v pracovní dny a v sobotu.

6.4 Vztahy primárních a podpůrných aktiv

Pro úplnost identifikace aktiv vybraného subjektu bylo provedeno hodnocení jejich vzájemného vztahu. V následující tabulce je v levých sloupcích uvedeno primární aktivum a jeho typ, které je srovnáváno s podpůrnými aktivy uvedenými v horním řádku. Za předpokladu vzájemného propojení či vztahu mezi primárními a podpůrnými aktivy je v daném políčku označen puntíkem a zvýrazněno modrou barvou.

Název primárního aktiva	Typ primárního aktiva	Číslo	Podpůrné aktivum subjektu																										
			PW - vedení společnosti	PW - vedoucí pracovníci	PW - IT pracovníci	PW - uživatelé IS	PW - ostatní zaměstnanci	PO - vrátnice	PO - ubytovací zařízení	PO - stravovací zařízení	PO - výrobní haly	PO - administrativní budovy	PO - sklady materiálu	SW - operační systém	SW - MS Office 2013	SW - Antivirový software	SW - webový prohlížeč	SW - docházkový systém	SW - interní IS	HW - mobilní zařízení	HW - uživatelská periferie	HW - pevné zařízení	TZ - Technické zařízení	Z - Zásoby	BD - Bezpečnostní dokumenty	S -Subdodavatelé	O - Ostatní
Činnosti a procesy	Oddělení jednatelů	1.	•	•		•		•	•	•		•		•	•	•	•			•	•	•			•	•	•
	asistenta vedení společnosti	2.	•			•		•	•	•		•		•	•	•	•		•	•	•	•			•	•	•
	Personální oddělení	3.		•		•		•	•	•		•		•	•	•	•	•	•	•	•	•				•	•
	Oddělení vedoucí výroby	4.		•		•		•		•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•
	Finanční oddělení	5.		•		•		•		•		•		•	•	•	•		•	•	•	•	•				•
	Oddělení konstrukce	6.		•		•		•		•	•	•		•	•	•	•		•	•	•	•	•				•
	Oddělení kalkulace a ISO	7.		•		•		•		•	•	•		•	•	•	•		•		•	•					•
	Oddělení controllingu	8.		•		•		•		•		•		•	•	•	•	•	•		•	•					•
	Oddělení nákupu	9.		•		•		•		•		•	•	•	•	•	•		•	•	•	•				•	•
	Oddělení zpracování zakázek	10.		•		•		•		•	•	•	•	•	•	•	•		•	•	•	•					•
	Oddělení kontroly	11.		•		•	•	•		•	•	•	•	•	•	•	•		•	•	•	•					•
	Oddělení výroby – svařovny	12.		•			•	•		•	•		•										•	•		•	•
	Oddělení výroby – montáž	13.		•			•	•		•	•		•										•	•		•	•
	Oddělení údržby	14.		•		•	•	•		•	•		•	•	•	•	•		•	•	•	•		•		•	•
	Oddělení skladů a expedice	15.		•		•	•	•		•	•		•	•	•	•	•		•	•	•	•		•		•	•
	školicího střediska	16.		•		•		•		•				•	•	•	•		•	•	•	•					•
	Oddělení IT	17.		•		•		•		•		•	•	•	•	•	•		•	•	•	•		•	•	•	•

Obrázek 8 Vztahy primárních a podpůrných aktiv subjektu – činnosti a procesy.

Zdroj: (vlastní)

Název primárního aktiva	Typ primárního aktiva	Číslo	Podpůrné aktivum subjektu																									
			PW - vedení společnosti	PW - vedoucí pracovníci	PW - IT pracovníci	PW - uživatelé IS	PW - ostatní zaměstnanci	PO - vrátnice	PO - ubytovací zařízení	PO - stravovací zařízení	PO - výrobní haly	PO - administrativní budovy	PO - sklady materiálu	SW - operační systém	SW - MS Office 2013	SW - Antivirový software	SW - webový prohlížeč	SW - interní docházkový systém	SW - interní IS	HW - mobilní zařízení	HW - uživatelská periferie	HW - pevné zařízení	TZ - Technické zařízení	Z - Zásoby	BD - Bezpečnostní dokumenty	S -Subdodavatelé	O - Ostatní
Informace	Oddělení jednatelů	18.	•			•		•	•	•	•	•	•		•		•				•				•	•	•
	asistenta vedení společnosti	18.	•			•		•	•	•	•	•	•		•		•	•	•		•				•	•	•
	Personální oddělení	19.		•		•	•	•	•	•	•	•			•		•	•	•		•						•
	Oddělení vedoucí výroby	20.		•		•	•	•	•	•	•	•	•		•		•	•	•		•		•	•	•	•	•
	oddělení	21.	•	•		•		•		•		•			•		•		•		•		•			•	•
	Oddělení konstrukce	22.		•		•	•	•		•	•	•			•		•		•		•		•				•
	Oddělení kalkulace a ISO	23.		•		•	•	•		•	•	•			•		•		•		•						•
	Oddělení controllingu	24.	•	•		•		•		•		•			•		•	•	•		•						•
	Oddělení nákupu	25.		•		•	•	•		•	•	•	•		•		•		•		•			•		•	•
	Oddělení IT	26.	•	•		•	•	•		•	•	•		•	•	•	•		•		•		•	•	•	•	•

Obrázek 9 Vztahy primárních a podpůrných aktiv subjektu – informace.

Zdroj: (vlastní)

7 HROZBY PRO VYBRANÝ SUBJEKT

Každé aktivum podléhá určitým hrozbám, některé více a některé méně, dle charakteru a jejich vlastností.

7.1 Identifikace hrozeb

Pro společnost jsou vymezeny následující hrozby vzhledem k jejímu zaměření, zeměpisné poloze a podnebním podmínkám. Jednotlivé hrozby byly zařazeny do jednotlivých skupin – naturogenní, antropogenní a technogenní.

7.1.1 Naturogenní hrozby

Naturogenní hrozby jsou takové hrozby, které jsou zapříčiněné přírodními vlivy. Vzhledem k zeměpisnému umístění a podnebním podmínkám zde byly zařazeny následující hrozby – požár, vlhkost, mrazivé počasí, extrémní teploty, krupobití, srážky a extrémní deště, vítr, vichřice, hurikán, sníh a úder blesku. Tyto hrozby nejsou nijak ovlivnitelné, lze se na ně připravit a provést preventivní opatření. (Metych, 2023)

Tabulka 5 Vybrané naturogenní hrozby. Zdroj: (vlastní)

Typ hrozby	Číslo	Hrozba
Naturogenní hrozby	1.	Požár
	2.	Úder blesku
	3.	Vlhkost
	4.	Prach
	5.	Nevyhovující teplota

7.1.2 Antropogenní hrozby

Antropogenní hrozby jsou definované jako hrozby zapříčiněné lidským činitelem. Uvedené antropogenní hrozby byly vybrány jako jedny z nejpravděpodobnějších hrozeb, které mohou ve firmě nastat. (UNDRR, 2022)

Hrozby způsobené lidským faktorem lze dělit do dvou hlavních skupin. Jedná se o:

- Úmyslně způsobené.
- Způsobené nedbalostním jednáním. (Kolouch a Bašta, 2019)

Jedná se o: vnik neoprávněné osoby, krádež, únik informací, neadekvátní manipulaci, mechanické poškození, různé bezpečnostní incidenty, vandalismus, ztrátu přístupových údajů či autentizačních předmětů. (Kolouch a Bašta, 2019)

Jednou z velkých hrozeb je i externí úklidová firma, vzhledem ke skutečnosti, že pracovnice úklidu mají univerzální klíče a přístup do všech místností ve firmě, kromě serverovny. Jejich pohyb není ničím a nikým monitorován.

Tabulka 6 Vybrané antropogenní hrozby. Zdroj: (vlastní)

Typ hrozby	Číslo	Hrozba
Antropogenní hrozby	6.	Znehodnocení technického vybavení
	7.	Ztráta technického vybavení
	8.	Manipulace s daty
	9.	Chyba uživatele IT
	10.	Chyba správce IT
	11.	Vandalismus
	12.	Únik informací
	13.	Nedostatek personálu
	14.	Nedostatečné školení personálu
	15.	Narušení triády CIA
	16.	Kybernetické útoky

7.1.3 Technogenní hrozby

Přerušení dodávek energií, vody a plynu, únik nebezpečné látky, výpadek telekomunikace či špatné zabezpečení softwaru jsou vymezené technogenní hrozby pro firmu. Pro fungování a prosperitu podniku jsou zmíněné aspekty, jako je elektřina, voda, plyn velmi důležité vzhledem ke spoustě elektronických a výrobních zařízení. Výpadek telekomunikace či špatné zabezpečení softwaru mají největší vliv na administrativní část společnosti. V případě jejich narušení či výpadku by z velké části výrobní linky nebyly zastaveny.

Tabulka 7 Vybrané technogenní hrozby. Zdroj: (vlastní)

Typ hrozby	Číslo	Hrozba
Technogenní hrozby	17.	Selhání SW
	18.	Selhání HW
	19.	Neprovedená aktualizace
	20.	Výpadek interní sítě
	21.	Přerušení dodávek elektrické energie
	22.	Nevyhovující zabezpečení systému

8 ANALÝZA RIZIK PRO VYBRANÝ SUBJEKT A SUMARIZACE DAT

Kapitola se soustřeďuje na analýzu rizik ve vybraném subjektu, která bude provedena na základě identifikace jednotlivých primárních a podpůrných aktiv a jich ohrožující hrozby, které byly uvedeny v kapitolách výše.

Pro úplnost kapitoly je potřeba uvést definice dvou základních pojmů analýzy rizik, které ještě nebyly definovány. Jedná se o:

- **Riziko** je definováno jako možný výskyt nežádoucího jevu, který svým potenciálem může ohrozit různé druhy aktiv (Kolouch a Bašta, 2019)
- **Zranitelnost** – je vlastnost určitého aktiva, zpravidla se jedná o slabé místo, které může být hrozbou ovlivněno a zneužito (Kolouch a Bašta, 2019)

Analýza rizik byla vypracována pomocí softwaru RISKAN v několika dílčích krocích. V rámci tohoto softwaru byly vytvořeny číselníky, které hodnotí aktiva, hrozby a zranitelnost a byla vymezena stupnice rizika. Na základě číselného hodnocení aktiv a hrozeb bylo vypočítáno celkové riziko jim připadající.

8.1 Číselníky aktiv a hrozeb

Pro potřeby analýzy byly v softwaru RISKAN využity již předdefinované číselníky pro hodnocení aktiva, pravděpodobnost hrozby, jejichž hodnoty jsou uvedeny v následujících tabulkách.

Tabulka 8 Číselníky RISKAN. Zdroj: (RISKAN)

HODNOTA AKTIVA	
0	zanedbatelná
1	velmi nízká
2	nízká
3	střední
4	vysoká
5	velmi vysoká

PRAVDĚPODOBNOST HROZBY	
0	zanedbatelná
1	velmi nízká
2	nízká
3	střední
4	vysoká
5	velmi vysoká

8.2 Hodnocení zranitelnosti

Po vyhodnocení zranitelnosti aktiv byla použita tabulka hodnocení zranitelnosti z téhož zdroje.

Tabulka 9 Zranitelnost aktiva.
Zdroj: (RISKAN)

ZRANITELNOST AKTIVA	
0	zanedbatelná
1	velmi nízká
2	nízká
3	střední
4	vysoká
5	velmi vysoká

Vyhodnocení bylo vytvořeno za pomocí MS Excel, který byl exportován z prostředí RISKAN s již vyplněnými aktivy a hrozbami. Dle uvedené stupnice byla pro jednotlivá aktiva určena jejich zranitelnost uvedená níže v tabulce.

Z důvodu velkého obsahu byla tabulka zranitelnosti rozdělena do tří jednotlivých částí. Jedná se o:

- Zranitelnost primárních aktiv – činnosti a procesy.
- Zranitelnost primárních aktiv – informace.
- Zranitelnost podpůrných aktiv.

Uvedené tabulky jsou níže v kapitole umístěny postupně dle tří částí.

RISKAN RIZIKOVÝ KALKULÁTOR / T-SOFT		Aktiva	AKTIVA - CELKEM	Činnosti a procesy	Oddělení jednatelů	Oddělení asistenta vede	Personální oddělení	Oddělení vedoucí výrob	Finanční oddělení	Oddělení konstrukce	Oddělení kalkulace a IS	Oddělení controllingu	Oddělení nákupu	Oddělení zpracování za	Oddělení kontroly	Oddělení výroby - svařo	Oddělení výroby - monta	Oddělení údržby	Oddělení skladů a exped	Oddělení školícího střec	Oddělení IT
				1	1.1	1.2	1.3	1.4	1.5	1.6	1.7	1.8	1.9	1.10	1.11	1.12	1.13	1.14	1.15	1.16	1.17
		Hodnoty aktiv	5	5	4	3	4	5	5	4	4	3	2	3	2	4	4	2	2	2	5
			velmi vysoká	velmi vysoká	vysoká	střední	vysoká	velmi vysoká	velmi vysoká	vysoká	vysoká	střední	nízká	střední	nízká	vysoká	vysoká	nízká	nízká	nízká	velmi vysoká
Hrozby		Pravděpodobnost																			
HROZBY - CELKEM		5 velmi vysoká	5	5	4	4	5	4	5	4	4	4	4	4	4	4	4	4	4	4	5
1	Naturogenní hrozby	5 velmi vysoká	5	5	3	3	3	3	3	3	3	3	3	3	3	4	4	4	3	3	5
1.1	Požár	5 velmi vysoká	5	5	3	3	3	3	3	3	3	3	3	3	3	4	4	4	3	3	5
1.2	Úder blesku	2 nízká	3	3	1	1	1	1	2	1	1	1	1	1	1	2	2	2	1	1	3
1.3	Vlhkost	1 velmi nízká	4	3	1	1	2	1	2	1	1	1	1	1	2	2	2	2	3	1	2
1.4	Prach	3 střední	3	3	1	1	2	2	2	2	1	1	2	1	3	3	3	2	1	1	2
1.5	Nevyhovující teplota	1 velmi nízká	3	3	3	3	3	2	3	2	2	2	2	2	3	3	3	3	1	2	2
2	Antropogenní hrozby	5 velmi vysoká	5	5	4	4	5	4	5	4	4	4	4	4	4	4	4	4	4	4	5
2.1	Znehodnocení technického aktiv	4 vysoká	5	5	3	3	4	3	4	3	3	2	3	3	4	4	4	4	2	2	5
2.2	Ztráta technického vybavení	3 střední	5	5	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	5
2.3	Manipulace s daty	5 velmi vysoká	5	5	3	3	5	3	4	3	3	3	4	4	4	3	3	2	2	2	4
2.4	Chyba uživatele IT	5 velmi vysoká	4	4	1	3	3	3	4	3	3	3	3	4	4	1	1	1	2	2	4
2.5	Chyba správce IT	3 střední	4	4	2	3	3	3	4	3	3	3	3	3	3	2	2	1	2	2	4
2.6	Vandalismus	4 vysoká	5	5	1	2	4	2	5	3	2	2	2	2	2	3	3	3	2	2	4
2.7	Únik informací	5 velmi vysoká	5	5	3	3	5	3	5	3	3	3	3	4	3	1	1	1	1	1	4
2.8	Nedostatek personálu	3 střední	4	4	2	1	3	4	2	2	2	2	2	2	3	4	4	2	2	2	2
2.9	Nedostatečné školení personálu	3 střední	4	4	3	1	3	4	2	2	2	2	2	2	3	4	4	3	1	1	2
2.10	Narušení triády CIA	5 velmi vysoká	5	5	4	4	5	3	4	3	3	3	3	3	3	1	1	1	1	1	5
2.11	Kybernetické útoky	4 vysoká	4	4	4	3	4	3	3	3	3	3	3	3	3	1	1	1	1	1	4
3	Technické hrozby	5 velmi vysoká	4	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	2	2	3
3.1	Selhání softwaru	5 velmi vysoká	3	3	2	3	3	3	3	3	3	3	3	3	3	2	2	2	1	1	3
3.2	Selhání hardwaru	4 vysoká	4	3	2	3	3	3	3	3	3	3	3	3	3	1	1	2	1	1	3
3.3	Neprovedené aktualizace	2 nízká	3	3	1	3	2	2	2	2	2	2	2	2	2	1	1	1	1	1	3
3.4	Výpadek interní sítě	3 střední	3	3	2	3	3	3	3	3	3	3	3	3	3	1	1	2	2	2	2
3.5	Přerušení dodávek elektrické ene	4 vysoká	3	3	2	2	2	2	2	2	2	2	2	2	2	3	3	3	1	2	3
3.6	Nevyhovující zabezpečení systé	4 vysoká	3	3	3	3	3	3	3	3	3	3	3	3	3	1	1	1	1	1	2

Obrázek 10 Zranitelnost primárních aktiv – činnosti a procesy. Zdroj: (RISKAN), (vlastní)

RISKAN RIZIKOVÝ KALKULÁTOR T-SOFT			Aktiva	Informace	Oddělení jednatelů	Oddělení asistenta vede	Personální oddělení	Finanční oddělení	Oddělení konstrukce	Oddělení kalkulace a IS	Oddělení nákupu	Oddělení IT
				2	2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8
			Hodnoty aktiv	5	5	4	4	5	1	2	1	5
				velmi vysoká	velmi vysoká	vysoká	vysoká	velmi vysoká	velmi nízká	nízká	velmi nízká	velmi vysoká
Hrozby		Pravděpodobnost										
HROZBY - CELKEM		5	velmi vysoká	5	4	4	5	4	4	4	4	5
1	Naturogenní hrozby	5	velmi vysoká	4	3	3	4	2	4	2	2	4
1.1	Požár	5	velmi vysoká	4	3	3	4	2	4	2	2	3
1.2	Úder blesku	2	nízká	3	2	2	3	1	3	1	1	3
1.3	Vlhkost	1	velmi nízká	4	1	1	2	1	3	1	1	4
1.4	Prach	3	střední	3	1	1	2	1	3	1	1	3
1.5	Nevyhovující teplota	1	velmi nízká	3	2	2	3	2	3	1	1	3
2	Antropogenní hrozby	5	velmi vysoká	5	4	4	5	4	4	4	4	5
2.1	Znehodnocení technického aktiv	4	vysoká	5	4	3	5	3	4	3	3	5
2.2	Ztráta technického vybavení	3	střední	4	3	3	4	3	4	4	4	4
2.3	Manipulace s daty	5	velmi vysoká	5	3	4	5	4	3	3	4	5
2.4	Chyba uživatele IT	5	velmi vysoká	3	3	2	3	2	3	2	3	3
2.5	Chyba správce IT	3	střední	4	3	2	3	3	3	3	3	4
2.6	Vandalismus	4	vysoká	4	3	2	4	2	4	2	2	4
2.7	Únik informací	5	velmi vysoká	5	4	3	5	2	4	2	3	4
2.8	Nedostatek personálu	3	střední	3	2	1	2	3	2	2	1	3
2.9	Nedostatečné školení personálu	3	střední	3	2	1	2	3	3	2	1	3
2.10	Narušení triády CIA	5	velmi vysoká	4	4	3	4	3	4	2	3	4
2.11	Kybernetické útoky	4	vysoká	4	3	3	3	2	3	3	3	4
3	Technické hrozby	5	velmi vysoká	3	1	3	3	3	3	3	3	3
3.1	Selhání softwaru	5	velmi vysoká	3	1	3	3	3	3	3	3	3
3.2	Selhání hardwaru	4	vysoká	3	1	3	3	3	3	3	3	3
3.3	Neprovedené aktualizace	2	nízká	2	1	2	2	2	2	2	2	2
3.4	Výpadek interní sítě	3	střední	3	1	3	3	3	3	3	3	3
3.5	Přerušení dodávek elektrické ene	4	vysoká	3	1	3	3	3	3	3	3	3
3.6	Nevyhovující zabezpečení systé	4	vysoká	2	1	2	2	2	2	2	2	2

Obrázek 11 Zranitelnost primárních aktiv – informace. Zdroj: (RISKAN), (vlastní)

RISKAN RIZIKOVÝ KALKULÁTOR T-SOFT		Aktiva	Podpůrná aktiva	Hardware	Software	Osoby - zaměstnanci	Prostory a objekty	Technické zařízení	Zásoby	Bezpečnostní dokument	Subdodavatelé	Ostatní
			3	3.1	3.2	3.3	3.4	3.5	3.6	3.7	3.8	3.9
		Hodnoty aktiv	5	5	5	4	3	3	2	4	4	4
			velmi vysoká	velmi vysoká	velmi vysoká	vysoká	střední	střední	nízká	vysoká	vysoká	vysoká
Hrozby		Pravděpodobnost										
HROZBY - CELKEM		5 velmi vysoká	4	4	4	4	4	4	3	4	1	2
1	Naturogenní hrozby	5 velmi vysoká	3	2	2	3	2	3	1	3	1	0
1.1	Požár	5 velmi vysoká	3	2	2	3	2	2	1	3	0	0
1.2	Úder blesku	2 nízká	2	0	0	2	0	1	0	0	0	0
1.3	Vlhkost	1 velmi nízká	3	2	0	3	1	3	1	2	1	0
1.4	Prach	3 střední	3	2	0	1	1	3	1	2	0	0
1.5	Nevyhovující teplota	1 velmi nízká	1	0	0	1	0	1	0	0	0	0
2	Antropogenní hrozby	5 velmi vysoká	4	4	4	4	4	4	3	4	1	2
2.1	Znehodnocení technického aktiv	4 vysoká	4	4	4	4	0	4	2	2	1	1
2.2	Ztráta technického vybavení	3 střední	4	3	2	3	3	4	2	2	1	1
2.3	Manipulace s daty	5 velmi vysoká	3	2	3	3	2	3	2	2	1	1
2.4	Chyba uživatele IT	5 velmi vysoká	3	3	3	2	0	0	1	3	1	1
2.5	Chyba správce IT	3 střední	4	3	4	2	1	1	1	3	1	1
2.6	Vandalismus	4 vysoká	4	4	4	1	4	3	3	4	1	2
2.7	Únik informací	5 velmi vysoká	4	2	2	3	1	1	1	4	1	1
2.8	Nedostatek personálu	3 střední	2	1	1	2	1	1	1	2	1	1
2.9	Nedostatečné školení personálu	3 střední	3	1	1	2	1	1	1	3	1	1
2.10	Narušení triády CIA	5 velmi vysoká	4	1	1	3	1	1	1	4	1	1
2.11	Kybernetické útoky	4 vysoká	4	3	4	1	1	1	1	3	1	1
3	Technické hrozby	5 velmi vysoká	4	4	3	1	1	2	1	2	1	2
3.1	Selhání softwaru	5 velmi vysoká	3	2	3	1	1	2	1	2	1	2
3.2	Selhání hardwaru	4 vysoká	4	4	2	1	1	2	1	2	1	1
3.3	Neprovedené aktualizace	2 nízká	3	1	3	1	1	1	1	1	1	1
3.4	Výpadek interní sítě	3 střední	3	1	3	1	1	2	1	1	1	2
3.5	Přerušení dodávek elektrické ene	4 vysoká	3	3	3	1	1	2	1	1	1	2
3.6	Nevyhovující zabezpečení systé	4 vysoká	3	3	3	1	1	1	1	1	1	1

Obrázek 12 Zranitelnost podpůrných aktiv. Zdroj: (RISKAN), (vlastní)

8.3 Vyhodnocení analýzy rizik

Po určení a vyhodnocení zranitelnosti jednotlivých aktiv byla provedena analýza rizika. Riziko bylo vypočítáno dle následujícího vzorce,

$$R = A * H * Z$$

ve kterém jednotlivá písmena vyjadřují:

- R – výsledné riziko.
- A – hodnotu aktiva.
- H – pravděpodobnost uplatnění hrozby.
- Z – zranitelnost aktiv.

Výsledné riziko = Hodnota aktiva * Pravděpodobnost uplatnění hrozby * Zranitelnost aktiv

Výsledná analýza rizik je vyobrazena v barevném rozlišení, které bylo předem definováno a je následující:

- Nízké riziko v rozmezí 0 – 30 (označeno zelenou barvou).
- Střední riziko v rozmezí 31 – 60 (označeno žlutou barvou).
- Vysoké riziko v rozmezí 61 – 90 (označeno červenou barvou).

Výsledná analýza je rozdělena na stejné tři segmenty, jako byla rozdělena zranitelnost aktiv. Rozdělení je následující:

- Primární aktiva – činnosti a procesy.
- Primární aktiva – informace.
- Podpůrná aktiva.

RISKAN RIZIKOVÝ KALKULÁTOR / T-SOFT		Aktiva	AKTIVA - CELKEM	Činnosti a procesy	Oddělení jednatelů	Oddělení asistenta vede	Personální oddělení	Oddělení vedoucí výrob	Finanční oddělení	Oddělení konstrukce	Oddělení kalkulace a IS	Oddělení controllingu	Oddělení nákupu	Oddělení zpracování za	Oddělení kontroly	Oddělení výroby - svařo	Oddělení výroby - monta	Oddělení údržby	Oddělení skladů a expe	Oddělení školícího stře	Oddělení IT
				1	1.1	1.2	1.3	1.4	1.5	1.6	1.7	1.8	1.9	1.10	1.11	1.12	1.13	1.14	1.15	1.16	1.17
		Hodnoty aktiv	5	5	4	3	4	5	5	4	4	3	2	3	2	4	4	2	2	2	5
Generátor grafů	Export do XML		velmi vysoká	velmi vysoká	vysoká	střední	vysoká	velmi vysoká	velmi vysoká	vysoká	vysoká	střední	nízká	střední	nízká	vysoká	vysoká	nízká	nízká	nízká	velmi vysoká
Hrozby		Pravděpodobnost																			
HROZBY - CELKEM		5 velmi vysoká	90	90	58	43	72	54	90	43	43	32	29	43	29	58	58	29	22	22	90
1	Naturogenní hrozby	5 velmi vysoká	90	90	43	32	43	54	54	43	43	32	22	32	22	58	58	29	22	22	90
1.1	Požár	5 velmi vysoká	90	90	43	32	43	54	54	43	43	32	22	32	22	58	58	29	22	22	90
1.2	Úder blesku	2 nízká	22	22	6	4	6	7	14	6	6	4	3	4	3	12	12	6	3	3	22
1.3	Vlhkost	1 velmi nízká	14	7	3	2	6	4	7	3	3	2	1	2	3	6	6	3	4	1	7
1.4	Prach	3 střední	32	26	9	6	17	22	22	17	9	6	9	6	13	26	26	9	4	4	22
1.5	Nevyhovující teplota	1 velmi nízká	11	11	9	6	9	7	11	6	6	4	3	4	4	9	9	4	1	3	7
2	Antropogenní hrozby	5 velmi vysoká	90	90	58	43	72	54	90	43	43	32	29	43	29	46	46	23	17	17	90
2.1	Znehodnocení technického aktiv	4 vysoká	72	72	35	26	46	43	58	35	35	17	17	26	23	46	46	23	12	12	72
2.2	Ztráta technického vybavení	3 střední	54	54	26	26	35	43	43	35	35	26	17	26	17	35	35	17	17	17	54
2.3	Manipulace s daty	5 velmi vysoká	90	72	43	32	72	54	72	43	43	32	29	43	29	43	43	14	14	14	72
2.4	Chyba uživatele IT	5 velmi vysoká	72	72	14	32	43	54	72	43	43	32	22	43	29	14	14	7	14	14	72
2.5	Chyba správce IT	3 střední	43	43	17	19	26	32	43	26	26	19	13	19	13	17	17	4	9	9	43
2.6	Vandalismus	4 vysoká	72	72	12	17	46	29	72	35	23	17	12	17	12	35	35	17	12	12	58
2.7	Únik informací	5 velmi vysoká	90	90	43	32	72	54	90	43	43	32	22	43	22	14	14	7	7	7	72
2.8	Nedostatek personálu	3 střední	43	43	17	6	26	43	22	17	17	13	9	13	13	35	35	9	9	9	22
2.9	Nedostatečné školení personálu	3 střední	43	43	26	6	26	43	22	17	17	13	9	13	13	35	35	13	4	4	22
2.10	Narušení triády CIA	5 velmi vysoká	90	90	58	43	72	54	72	43	43	32	22	32	22	14	14	7	7	7	90
2.11	Kybernetické útoky	4 vysoká	58	58	46	26	46	43	43	35	35	26	17	26	17	12	12	6	6	6	58
3	Technické hrozby	5 velmi vysoká	58	54	35	32	43	54	54	43	43	32	22	32	22	35	35	17	9	12	54
3.1	Selhání softwaru	5 velmi vysoká	54	54	29	32	43	54	54	43	43	32	22	32	22	29	29	14	7	7	54
3.2	Selhání hardwaru	4 vysoká	58	43	23	26	35	43	43	35	35	26	17	26	17	12	12	12	6	6	43
3.3	Neprovedené aktualizace	2 nízká	22	22	6	13	12	14	14	12	12	9	6	9	6	6	6	3	3	3	22
3.4	Výpadek interní sítě	3 střední	32	32	17	19	26	32	32	26	26	19	13	19	13	9	9	9	9	9	22
3.5	Přerušení dodávek elektrické ene	4 vysoká	43	43	23	17	23	29	29	23	23	17	12	17	12	35	35	17	6	12	43
3.6	Nevyhovující zabezpečení systé	4 vysoká	43	43	35	26	35	43	43	35	35	26	17	26	17	12	12	6	6	6	29

Obrázek 13 Vyhodnocení rizik primárních aktiv – činnosti a procesy. Zdroj: (RISKAN), (vlastní)

RISKAN RIZIKOVÝ KALKULÁTOR
T-SOFT

Generátor grafů | Export do XML

				Aktiva	Informace	Oddělení jednatelů	Oddělení asistenta vede	Personální oddělení	Finanční oddělení	Oddělení konstrukce	Oddělení kalkulace a IS	Oddělení nákupu	Oddělení IT
					2	2.1	2.2	2.3	2.4	2.5	2.6	2.7	2.8
				Hodnoty aktiv	5	5	4	4	5	1	2	1	5
					velmi vysoká	velmi vysoká	vysoká	vysoká	velmi vysoká	velmi nízká	nízká	velmi nízká	velmi vysoká
Hrozby		Pravděpodobnost											
HROZBY - CELKEM		5	velmi vysoká		90	72	58	72	72	14	22	14	90
1	Naturogenní hrozby	5	velmi vysoká		58	54	43	58	36	14	14	7	54
1.1	Požár	5	velmi vysoká		58	54	43	58	36	14	14	7	54
1.2	Úder blesku	2	nízká		22	14	12	17	7	4	3	1	22
1.3	Vlhkost	1	velmi nízká		14	4	3	6	4	2	1	1	14
1.4	Prach	3	střední		32	11	9	17	11	6	4	2	32
1.5	Nevyhovující teplota	1	velmi nízká		11	7	6	9	7	2	1	1	11
2	Antropogenní hrozby	5	velmi vysoká		90	72	58	72	72	14	22	14	90
2.1	Znehodnocení technického aktiv	4	vysoká		72	58	35	58	43	12	17	9	72
2.2	Ztráta technického vybavení	3	střední		43	32	26	35	32	9	17	9	43
2.3	Manipulace s daty	5	velmi vysoká		90	54	58	72	72	11	22	14	90
2.4	Chyba uživatele IT	5	velmi vysoká		54	54	29	43	36	11	14	11	54
2.5	Chyba správce IT	3	střední		43	32	17	26	32	6	13	6	43
2.6	Vandalismus	4	vysoká		58	43	23	46	29	12	12	6	58
2.7	Únik informací	5	velmi vysoká		72	72	43	72	36	14	14	11	72
2.8	Nedostatek personálu	3	střední		32	22	9	17	32	4	9	2	32
2.9	Nedostatečné školení personálu	3	střední		32	22	9	17	32	6	9	2	32
2.10	Narušení triády CIA	5	velmi vysoká		72	72	43	58	54	14	14	11	72
2.11	Kybernetické útoky	4	vysoká		58	43	35	35	29	9	17	9	58
3	Technické hrozby	5	velmi vysoká		54	18	43	43	54	11	22	11	54
3.1	Selhání softwaru	5	velmi vysoká		54	18	43	43	54	11	22	11	54
3.2	Selhání hardwaru	4	vysoká		43	14	35	35	43	9	17	9	43
3.3	Neprovedené aktualizace	2	nízká		14	7	12	12	14	3	6	3	14
3.4	Výpadek interní sítě	3	střední		32	11	26	26	32	6	13	6	32
3.5	Přerušení dodávek elektrické ene	4	vysoká		43	14	35	35	43	9	17	9	43
3.6	Nevyhovující zabezpečení systé	4	vysoká		29	14	23	23	29	6	12	6	29

Obrázek 14 Vyhodnocení rizik primárních aktiv – informace. Zdroj: (RISKAN), (vlastní)

RISKAN RIZIKOVÝ KALKULÁTOR
T-SOFT

Generátor grafů | Export do XML

				Aktiva	Podpůrná aktiva	Hardware	Software	Osoby - zaměstnanci	Prostory a objekty	Technické zařízení	Zásoby	Bezpečnostní dokument	Subdodavatelé	Ostatní
					3	3.1	3.2	3.3	3.4	3.5	3.6	3.7	3.8	3.9
				Hodnoty aktiv	5	5	5	4	3	3	2	4	4	4
					velmi vysoká	velmi vysoká	velmi vysoká	vysoká	střední	střední	nízká	vysoká	vysoká	vysoká
Hrozby		Pravděpodobnost												
HROZBY - CELKEM		5	velmi vysoká		58	58	58	46	35	35	17	58	14	29
1	Naturogenní hrozby	5	velmi vysoká		43	36	36	43	22	22	7	43	3	0
1.1	Požár	5	velmi vysoká		43	36	36	43	22	22	7	43	0	0
1.2	Úder blesku	2	nízká		12	0	0	12	0	4	0	0	0	0
1.3	Vlhkost	1	velmi nízká		9	7	0	9	2	6	1	6	3	0
1.4	Prach	3	střední		22	22	0	9	6	19	4	17	0	0
1.5	Nevyhovující teplota	1	velmi nízká		3	0	0	3	0	2	0	0	0	0
2	Antropogenní hrozby	5	velmi vysoká		58	58	58	46	35	35	17	58	14	23
2.1	Znehodnocení technického aktiv	4	vysoká		58	58	58	46	0	35	12	23	12	12
2.2	Ztráta technického vybavení	3	střední		32	32	22	26	19	26	9	17	9	9
2.3	Manipulace s daty	5	velmi vysoká		54	36	54	43	22	32	14	29	14	14
2.4	Chyba uživatele IT	5	velmi vysoká		54	54	54	29	0	0	7	43	14	14
2.5	Chyba správce IT	3	střední		43	32	43	17	6	6	4	26	9	9
2.6	Vandalismus	4	vysoká		58	58	58	12	35	26	17	46	12	23
2.7	Únik informací	5	velmi vysoká		58	36	36	43	11	11	7	58	14	14
2.8	Nedostatek personálu	3	střední		17	11	11	17	6	6	4	17	9	9
2.9	Nedostatečné školení personálu	3	střední		26	11	11	17	6	6	4	26	9	9
2.10	Narušení triády CIA	5	velmi vysoká		58	18	18	43	11	11	7	58	14	14
2.11	Kybernetické útoky	4	vysoká		58	43	58	12	9	9	6	35	12	12
3	Technické hrozby	5	velmi vysoká		58	58	54	14	11	22	7	29	14	29
3.1	Selhání softwaru	5	velmi vysoká		54	36	54	14	11	22	7	29	14	29
3.2	Selhání hardwaru	4	vysoká		58	58	29	12	9	17	6	23	12	12
3.3	Neprovedené aktualizace	2	nízká		22	7	22	6	4	4	3	6	6	6
3.4	Výpadek interní sítě	3	střední		32	11	32	9	6	13	4	9	9	17
3.5	Přerušení dodávek elektrické ene	4	vysoká		43	43	43	12	9	17	6	12	12	23
3.6	Nevyhovující zabezpečení systé	4	vysoká		43	43	43	12	9	9	6	12	12	12

Obrázek 15 Vyhodnocení rizik podpůrných aktiv. Zdroj: (RISKAN), (vlastní)

Z výše uvedených tabulek vyhodnocení analýzy rizik byly definovány čtyři nejrizikovější skupiny aktiv a hrozby, které jednotlivá aktiva ovlivňují. Mezi nejrizikovější aktiva byla vyhodnocena:

- Oddělení jednatelů.
- Personální oddělení.
- Finanční oddělení.
- Oddělení IT.

Jedná se o oddělení, kde probíhají nejzásadnější činnosti pro subjekt a jsou zde uchovávány klíčové informace, včetně bezpečnostních dokumentů.

Mezi nejzávažnější hrozby pro tato aktiva jsou řazeny následující hrozby:

- Naturogenní – požár.
- Antropogenní – nevhodná manipulace s daty, narušení triády CIA, vandalismus či únik informací.
- Technogenní – nedosahují horní hranice rizika, nicméně jako největší hrozbu lze označit selhání hardwaru či softwaru.

Na základě výsledků analýzy rizik budou v následující kapitole navržena vhodná opatření pro nejrizikovější skupiny aktiv a hrozeb.

9 NÁVRH OPATŘENÍ PRO VYBRANÝ SUBJEKT

V společnosti není uvedená ISO norma 27000 nijak ukotvena, nicméně kybernetická bezpečnost a bezpečnost informací v gesci IT technika jsou na dobré úrovni a většinou pracovníků zásady přítomnosti na firemní sítí dodržovány. Zároveň přítomnost IT speciality je pravidelná a kontrola zařízení taktéž.

Největší hrozbou v této oblasti je neadekvátní manipulace. Proto jako jeden z návrhů na zlepšení je vzdělávání v rámci této oblasti, které neprobíhá, a proto jednotliví zaměstnanci nejsou dostatečně informováni o nových hrozbách. I když je firemní internetová síť kontrolována například pomocí povolených a zakázaných internetových stránek, průběžné vzdělávání je v této oblasti klíčové.

Pro firmu jako celek je největší antropogenní hrozbou narušení bezpečnosti při vniku neoprávněné osoby. I když společnost využívá kamerový systém, tak není nonstop hlídán a mimo oblast vrátnice nejsou nijak hlídány hranice celého objektu. Proto jako další návrh na zlepšení je uveden podrobný monitoring hranic a pozemků objektu.

S tím je úzce spojeno zabezpečení kanceláří. Po objektu dochází k velkému pohybu lidí, nicméně spousta pracovníků nedodržuje zásady bezpečnosti při opuštění svých kanceláří. Při narušení cizí osobou hrozí, že se cizí osoby dostanou k citlivým informacím, které jsou uchovávány v papírových podobách. Na firemní síť by se za předpokladu fungování neměl narušitel dostat vzhledem ke skutečnosti, že při neaktivitě na PC delší než dvě minuty se účet automaticky uzamkne a odhlásí. Pro jeho spuštění jsou potřeba uživatelské údaje a hesla.

Navržená opatření jsou rozdělena dle zákona o kybernetické bezpečnosti do dvou základních typů: organizační a technická opatření.

9.1 Opatření na úrovni organizace

Na úrovni celé organizace jsou povinni všichni určení zaměstnanci – zpravidla uživatelé informačních systémů, absolvovat školení kybernetické bezpečnosti formou výukových kurzů. Absolvování kurzů je zaměstnanci zprostředkováno dvěma způsoby: prostřednictvím Národního úřadu pro kybernetickou a informační bezpečnost, který pro tyto účely poskytuje kurz zdarma, případně prostřednictvím školení vybrané firmy zabývající se danou problematikou.

U stálých zaměstnanců je nezbytné provádění periodických školení kybernetické bezpečnosti. Vzhledem k rozvoji a rozsahu kybernetických hrozeb bude toto školení probíhat opakovaně dle požadavků zaměstnavatele.

Za předpokladu přijetí zaměstnance do pracovního poměru bude přesně definována odpovědnost za aktiva jemu svěřená. Za tímto účelem má každá pracovní pozice seznam aktiv, která po převzetí budou podepsána zaměstnancem, přímým nadřízeným a správcem IT.

Tato školení si kladou za cíl, aby zaměstnanec – uživatel informačních systémů byl schopen rozpoznat bezpečnostní kybernetický incident a následně postupovat dle jednotlivých kroků. Za předpokladu dodržování těchto opatření náleží zaměstnanci výplata motivačního ohodnocení vytvořeného pro tyto účely.

Národní úřad pro kybernetickou a informační bezpečnost poskytuje několik různých kurzů pro zaměstnance a management v rámci problematiky kybernetické bezpečnosti. Jako nejlepší a nejvýstižnější kurz byl vybrán „Dávej kyber!“. Tento kurz nabízí výuku problematiky hesel a přihlašování, metod odemykání zařízení, sociálního inženýrství, důvěryhodné komunikace, škodlivých souborů, ochrany zařízení, stahování aplikací či připojení a soukromí.

Obrázek 16 Kurz „Dávej kyber!“. Zdroj: (NÚKIB, 2022)

Dalším nezbytným opatřením je možná klasifikace informací, dle možných druhů třídění, se kterými vybraný subjekt pracuje a tyto informace uchovává. Nejvýhodnějším řešením by byla aplikace TLP protokolu, jehož princip je uveden v teoretické části diplomové práce.

9.2 Technická opatření

Mezi nejvýznamnější naturogenní hrozby patří požár a vzhledem ke skutečnosti, že vybraný subjekt nemá instalovanou elektrickou požární signalizaci, je jeden z návrhů na zlepšení její zajištění pro hlavní administrativní budovu. V administrativní budově jsou situovány všechny čtyři nejrizikovější skupiny aktiv, na která má případný požár zásadní vliv.

EPS – elektrická požární signalizace

Elektrická požární signalizace je využívána ke zvýšení ochrany budov před požárem. EPS musí být využívána v takových objektech, kde je předpoklad většího počtu osob a kde je předpoklad zdlouhavé a problematické evakuace. Dle těchto podmínek není v subjektu vytvořena povinnost aplikovat EPS, ale vzhledem ke skutečnosti uchovávání velkého množství citlivých dat v administrativních budovách, by bylo vhodné EPS využívat. (Hošek, 2013)

Elektrická požární signalizace se skládá z následujících komponentů:

- Hlásiče požárů.
- Ústředny EPS.
- Doplňující zařízení.

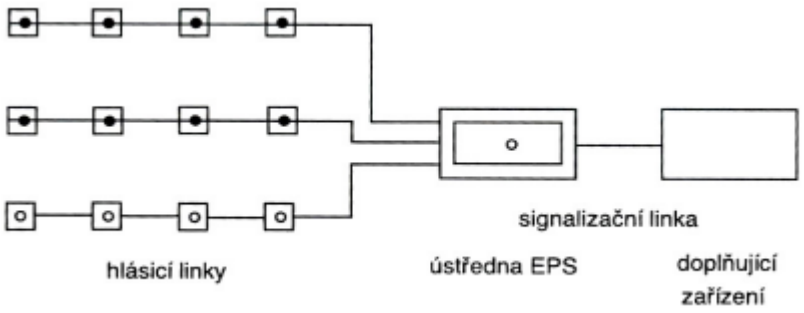
Hlásiče požáru monitorují a vyhodnocují konkrétní fyzikální parametry a jejich okamžité změny, které značí vznik požáru. Dělí se na dva základní typy: Tlačítkové hlásiče a samočinné hlásiče. U tlačítkových hlásičů je vyslání signálu závislé na lidském vyhodnocení, kdy člověk musí zmáčknout tlačítko a tím vyslat signál do ústředny EPS. Samočinné hlásiče jsou samostatné a pracují bez zásahu člověka. Vyhodnocení a spuštění signálu probíhá automaticky. (Hošek, 2013)

Ústředny EPS mají několik základních funkcí. Jedná se o:

- Vyhodnocování signalizace hlásičů.
- Ovládání připojených zařízení.
- Kontrolu provozuschopnosti.

- Zprostředkování napájení. (Hošek, 2013)

Mezi doplňující zařízení EPS je možné uvést například obslužné pole požární ochrany, klíčový trezor požární ochrany, zařízení pro odvod tepla a kouře, protipožární únikové dveře či zařízení dálkového přenosu.



Obrázek 17 Schéma elektrické požární signalizace. Zdroj: (Hošek, 2013)

Existují tři druhy elektrické požární signalizace: jednodruhová, vícestupňová a systémy EPS. Jednodruhová EPS je charakteristická tím, že obsahuje pouze jednu nebo více hlavních ústředen, ke kterým jsou připojeny hlásiče požáru. Oproti tomu vícedruhová EPS má hlavní a k nim vedlejší ústředny. K těmto ústřednám jsou připojeny samočinné nebo tlačítkové hlásiče požáru či další vedlejší ústředny nižších stupňů. Poslední variantou jsou systémy EPS, které mohou být buď s kolektivní, nebo individuální adresací. EPS s kolektivní adresací jsou takové, kdy ústředna není schopna rozpoznat, ze kterého konkrétního hlásiče přichází požární signál. EPS s individuální adresací pracuje na principu identifikace stavu jednotlivých hlásičů požáru na hlásící lince prostřednictvím komunikace mezi prvky. Tím je umožněna rychlá identifikace hlásiče, který požární poplach hlásí. (Hošek, 2013)

9.3 Organizační směrnice kybernetické bezpečnosti

Kromě výše uvedených návrhů opatření byla vytvořena organizační směrnice kybernetické bezpečnosti pro vybraný subjekt. Směrnice se svým obsahem soustřeďuje na vybrané zásady chování zaměstnanců s cílem zvýšení úrovně kybernetické bezpečnosti. Vzhledem ke svému rozsahu je uvedena v příloze P1.

ZÁVĚR

V této diplomové práci byla řešena problematika kybernetické bezpečnosti a posouzení jejího stavu ve vybraném subjektu.

První část byla soustředěna na vypracování teoretického podkladu práce, kde byly vymezeny základní pojmy vybraného tématu, dále legislativní rámec a zhodnocení aktuálního stavu na území ČR a EU.

Ve druhé části práce byl charakterizován vybraný subjekt, jeho organizační strukturu a mapu procesů, které zde probíhají. V rámci analýzy vnitřního a vnějšího prostředí byla vytvořena SWOT analýza, pomocí které byly určeny silné a slabé stránky, příležitosti a hrozby podniku, které byly následně blíže charakterizovány. Pomocí číselného hodnocení jednotlivých částí analýzy byla určena strategie podniku.

Dalším krokem práce byla identifikace aktiv a hrozeb. Pro subjekt byla vymezena kybernetická a informační aktiva na základě vyhlášky o kybernetické bezpečnosti, ve které jsou aktiva dělena na primární a podpůrná. Pro každou skupinu byly vytvořeny dílčí seznamy aktiv. Hrozby byly vybrány dle zdroje hrozby na antropogenní, technogenní a naturogenní. Každá skupina má zastoupení hrozeb aplikované přímo na vybraný subjekt.

Analýza rizik byla vytvořena za pomoci softwaru RISKAN, kdy nejdříve byly vytvořeny jednotlivé seznamy pro hrozby a aktiva, které byly podle definovaných stupnic číselně ohodnoceny. Následně byla vytvořena tabulka zranitelnosti jednotlivých aktiv, která byla využita k výslednému číselnému hodnocení rizika.

Z výsledné analýzy vyplynula čtyři nejzranitelnější oddělení a několik významných hrozeb, které byly z velké většiny antropogenního původu.

V návaznosti na výslednou analýzu rizik byla navržena jednotlivá opatření na úrovni organizační a technické.

V závěrečné části práce byla vytvořena směrnice kybernetické bezpečnosti, která obsahuje zásady kybernetické bezpečnosti a funguje jako manuál pro každého jednotlivého zaměstnance. Tato směrnice bude předána vedení společnosti s cílem jejího schválení a implementace.

SEZNAM POUŽITÉ LITERATURY

Agentura: Česká agentura pro standardizaci. In: *Česká agentura pro Standardizaci* [online]. © 2021 [cit. 2023-04-24]. Dostupné z: https://www.agentura-cas.cz/o-nas/agentura/

Availability. In: *Washington University in St. Louis: Office of Information Security* [online]. St. Louis, © 2023 [cit. 2023-04-24]. Dostupné z: https://informationsecurity.wustl.edu/items/availability/

Circl.lu: Traffic Light Protocol (TLP) version 2 - Classification and Sharing of Sensitive Information [online], 2023. Luxembourg. [cit. 2023-04-26]. Dostupné z: https://www.circl.lu/pub/traffic-light-protocol/#traffic-light-protocol-tlpv2

COBIT. In: *TechTarget* [online]. 2021, 2021 [cit. 2023-04-24]. Dostupné z: https://www.techtarget.com/searchsecurity/definition/COBIT

Co je NCKB. In: *Národní centrum kybernetické bezpečnosti* [online]. Praha, 2022, 2022 [cit. 2023-02-16]. Dostupné z: https://www.govcert.cz/cs/

Computer Emergency Response Team for the EU institutions, bodies and agencies (CERT-EU), © 2023. *European Union* [online]. [cit. 2023-04-24]. Dostupné z: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/institutions-and-bodies-profiles/cert-eu_cs

ČESKO, 1998. Ústavní zákon č. 110 ze dne 22. dubna 1998: o bezpečnosti České republiky. In: *Sbírka zákonů České republiky*. 1998, ročník 1998. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=110/1998&typeLaw=zakon&what=Cislo_zakona_smlouvy

ČESKO, 2018. Vyhláška č. 82 ze dne 21. května 2018: o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti). In: *Sbírka zákonů České republiky*. 2018. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=82/2018&typeLaw=zakon&what=Cislo_zakona_smlouvy

ČESKO, 2014. Vyhláška č. 317 ze dne 15. prosince 2014: o významných informačních systémech a jejich určujících kritériích. In: *Sbírka zákonů České republiky*. 2014. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=317/2014&typeLaw=zakon&what=Cislo_zakona_smlouvy

ČESKO, 2019. Zákon č.110 ze dne 12. března 2019: o zpracování osobních údajů. In: *Sbírka zákonů České republiky*. 2019. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=110/2019&typeLaw=zakon&what=Cislo_zakona_smlouvy

ČESKO, 2014. *Zákon č. 181/2014 Sb.: ze dne 23. července 2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*. In: . Sbírka zákonů České republiky, 2014. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=181/2014&typeLaw=zakon&what=Cislo_zakona_smlouvy

ČESKO, 2005. Zákon č. 412 ze dne 21. září 2005: o ochraně utajovaných informací a o bezpečnostní způsobilosti. In: *Sbírka zákonů České republiky*. 2005. Dostupné také z: https://aplikace.mvcr.cz/sbirka-zakonu/SearchResult.aspx?q=412/2005&typeLaw=zakon&what=Cislo_zakona_smlouvy

ČERMÁK, Miroslav, 2008. CIA: Důvěrnosti-Integrita-Dostupnost. *Clever and Smart* [online]. [cit. 2023-04-24]. Dostupné z: https://www.cleverandsmart.cz/duvernost-integrita-dostupnost/

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

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

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

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

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

ČSN EN ISO/IEC 27005 *Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací*, 2009. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Třídící znak 369790.

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

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

ČSN EN ISO/IEC 27032 *Informační technologie - Bezpečnostní techniky - Směrnice pro kybernetickou bezpečnost*, 2013. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Třídící znak 369790.

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

HOŠEK, Zdeněk, 2013. Elektrická požární signalizace. *České vysoké učení technické v Praze* [online]. Praha [cit. 2023-04-25]. Dostupné z: http://fire.fsv.cvut.cz/vzdelavani/technici/6/6-5_Zarizeni_EPS.pdf

HRONEK, Jiří. Informační systémy. In: *Univerzita Palackého v Olomouci* [online]. Olomouc, 2007, 2007 [cit. 2023-04-24]. Dostupné z: https://phoenix.inf.upol.cz/esf/ucebni/infoSys.pdf

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.

KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.

MCCARTHY, N.K. *The Computer Incident Response Planning Handbook.* United States of America: The McGraw-Hill Companies, 2012. ISBN 978-0-07-179039-0.

METYCH, Michele, ©2023. Natural Disaster. *Britannica* [online]. [cit. 2023-04-25]. Dostupné z: https://www.britannica.com/science/natural-disaster

NÚKIB: Akční plán k národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025, 2022. In: *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Brno [cit. 2023-04-25]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/

NÚKIB: Národní strategie kybernetické bezpečnosti České republiky na období let 2021-2025, 2022. In: *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Brno [cit. 2023-04-25]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/

NÚKIB. In: *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Praha, 2022, 2022 [cit. 2023-02-16]. Dostupné z: https://nukib.cz/cs/o-nukib/

NÚKIB: Základy kybernetické bezpečnosti "Dávej kyber!", 2022. NÚKIB [online]. Brno [cit. 2023-04-24]. Dostupné z: https://osveta.nukib.cz/course/view.php?id=123

NÚKIB: Zpráva o stavu kybernetické bezpečnosti za rok 2021, 2022. In: *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Brno [cit. 2023-04-25]. Dostupné z: https://www.nukib.cz/cs/kyberneticka-bezpecnost/strategie-akcni-plan/

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.

Organizační struktura. In: *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Praha, 2022, 2022 [cit. 2023-02-16]. Dostupné z: https://nukib.cz/cs/o-nukib/organizacni-struktura-uradu/

Pojem zákon. In: *SCS.ABZ.CZ: Slovník cizích slov* [online]. © 2023, 2023 [cit. 2023-04-24]. Dostupné z: https://slovnik-cizich-slov.abz.cz/web.php/slovo/zakon

Přichází směrnice NIS 2 a s ní revoluce v oblasti kybernetické bezpečnosti. In: *Epravo.cz* [online]. Praha, 2023, 2023 [cit. 2023-04-24]. Dostupné z: https://www.epravo.cz/top/clanky/prichazi-smernice-nis-2-a-sni-revoluce-voblasti-kyberneticke-bezpecnosti-115821.html

UNDRR - United Nations Office for Disaster Risk Reduction: Hazard, 2022. *UNDRR - United Nations Office for Disaster Risk Reduction* [online]. [cit. 2023-04-25]. Dostupné z: https://www.undrr.org/terminology/hazard

Vyhláška. In: *Iuridictum: Encyklopedie o právu* [online]. 2021, 2021 [cit. 2023-04-24]. Dostupné z: https://iuridictum.pecina.cz/w/Vyhl%C3%A1%C5%A1ka

Interní dokumentace – příručky QMS

- QMS 01 Řízení systémových dokumentů.
- QMS 05 Řízení neshod, reklamací a nápravných opatření.
- QMS 08 Řízení údržby strojů a zařízení, IT a PP.
- QMS 09 Proces vedení společnosti.
- QMS 10 Proces personalistiky.
- QMS 11 Proces nakupování.
- QMS 12 Proces skladování.
- QMS 13 Proces trvalého zlepšování.
- QMS 14 Proces technické přípravy výroby.
- QMS 15 Proces výroby rámů.
- QMS 16 Proces zpracování zakázek.
- QMS 17 Řízení zakázky a montáže návěsů.
- QMS 18 Proces řízení jakosti.
- QMS 19 Proces řízení IT.

Interní dokumentace – organizační směrnice

- Organizační směrnice č. 13
- Organizační směrnice č. 10
- Organizační směrnice č. 45

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

COBIT	Control Objektives for Information and Related Technology
CERT	Computer Emergency Responce Team
CSIRT	Computer Security Incident Response Team
HW	Hardware
EPS	Elektrická požární signalizace
IKT	Informační a komunikační technologie
ICT	Information and Communication Technologies
IS	Informační systém
ISO	International Organization of Standardization
IT	Informační technologie
ITIL	Information Technology Infrastructure Library
LAN	Local Area Network
GDPR	General Data Protection Regulation
MAN	Metropolitan Area Network
NCKB	Národní centrum kybernetické bezpečnosti
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
SW	Software
TLP	Taffic light protocol
PAN	Personal Area Network
PC	Personal computer
RAID	Redundant Array of Inexpensive Disks
ÚNMZ	Úřad pro technickou normalizaci, metrologii a státní zkušebnictví
VPN	Virtual Private Network
WAN	Wide Area Network

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: ORGANIZAČNÍ SMĚRNICE KYBERNETICKÉ BEZPEČNOSTI

Zásady kybernetické bezpečnosti na pracovišti				**QMS 35**	
Obsah:					
1. Účel směrnice 2					
2. Kontrola a aktualizace uvedených zásad 2					
3. Cíl směrnice 2					
4. Zásady kybernetické bezpečnosti subjektu 2					
4.1. Hlavní bezpečnostní pravidlo 2					
4.2. Nepoužívat soukromá zařízení pro pracovní účely 2					
4.3. Nepoužívat soukromé účty pro pracovní účely a obráceně 2					
4.4. Omezení přístupu k pracovním zařízením 3					
4.5. Zabezpečení pracovních účtů hesly 3					
4.6. Nesdělovat jiným osobám přihlašovací údaje 3					
4.7. Využívání vícefaktorové autentizace při práci mimo organizaci 3					
4.8. Ukládání dat na určená uložiště 3					
4.9. Nepřipojovat žádná zařízení k PC 4					
4.10. Neotvírat a neodpovídat na podezřelé emaily 4					
5. Závěrečná ustanovení 4					
6. Přílohy 4					
Výtisk podléhá revizi:		(ANO)		~~(NE)~~	
Vypracoval:	Fialková Karin	Podpis:		Zpracováno:	15.4.2023

Obrázek 18 Úvodní strana organizační směrnice. Zdroj: (vlastní)

1. ÚČEL SMĚRNICE

Tento dokument popisuje postupy a zásady kybernetické bezpečnosti na pracovišti. Dokumentem se musí řídit všichni pracovníci společnosti, kteří z něj byli řádně proškoleni. Směrnice je určena pro potřeby subjektu, pro který je vytvořena.

2. KONTROLA A AKTUALIZACE UVEDENÝCH ZÁSAD

Kontrola a aktualizace níže uvedených zásad bude probíhat za spolupráce s oddělením IT.

3. CÍL SMĚRNICE

Cílem směrnice kybernetické bezpečnosti je zvýšení úrovně znalostí vybraných zaměstnanců, kteří aktivně využívají aktiva subjektu. Dále směrnice poskytuje návod, co dělat v definovaných situacích a prostřednictvím toho minimalizovat riziko vzniku kybernetických incidentů.

4. ZÁSADY KYBERNETICKÉ BEZPEČNOSTI SUBJEKTU

Každý nově příchozí zaměstnanec je povinen absolvovat školení zásad kybernetické bezpečnosti, které je v gesci pověřeného a školeného IT pracovníka v oblasti kybernetické bezpečnosti, který mu sdělí a podrobně vysvětlí jednotlivé zásady a nutnost jejich dodržování.

4.1. Hlavní bezpečnostní pravidlo

Mezi nejzásadnější pravidlo kybernetické bezpečnosti je řazeno respektování bezpečnostních pokynů specialisty v organizaci. V subjektu je odpovědná osoba za kybernetickou bezpečnost pracovník IT a jeho pokyny je zaměstnanec povinen se řídit. Stejně tak je cílovou osobou pro hlášení bezpečnostních incidentů.

4.2. Nepoužívat soukromá zařízení pro pracovní účely

Zaměstnanec je povinen pro pracovní účely využívat pouze ta zařízení, která mu byla přidělena. Tato zařízení podléhají kontrole a zabezpečení dle směrnic subjektu a splňují určené požadavky. Za předpokladu užívání soukromých zařízení není zajištěna potřebná kontrola a zabezpečení, v takových situacích hrozí vznik kybernetických bezpečnostních incidentů a ztráta triády CIA.

4.3. Nepoužívat soukromé účty pro pracovní účely a obráceně

Soukromé účty a aplikace nejsou pod kontrolou organizace a jejich využívání v pracovním prostředí na pracovních zařízení je potenciální hrozbou a může dojít například k infikování firemní sítě.

4.4. Omezení přístupu k pracovním zařízením

Za předpokladu opuštění pracoviště a ponechání zařízení bez dozoru, je zaměstnanec povinen toto zařízení uzamknout, stejně tak uzavřít a zabezpečit veškeré dokumenty proti zneužití.

4.5. Zabezpečení pracovních účtů hesly

Každé zařízení musí být chráněno heslem, které je v souladu s heslovou politikou organizace Heslo musí splňovat požadavky na délku a množství znaků, kdy musí být minimálně písmen dlouhé a musí být využito malých a velkých písmen a číslic. Další zásadou je obměna hesla. Heslo musí být měněno každé 3 měsíce, kdy po sobě jdoucí hesla nemohou být podobná. Výzva ke změně hesla je rozesílána automatiky oddělením IT na pracovní mailovou adresu 14 dní před vypršením platnosti. Za předpokladu, že zaměstnanec nestihne heslo do této doby změnit, při následujícím přihlášení bude uživatel nejprve vyzván ke změně hesla, následně mu bude umožněn přístup k jeho pracovnímu účtu.

4.6. Nesdělovat jiným osobám přihlašovací údaje

Zaměstnanec disponuje několika různými hesly, jako jsou: hesla do zařízení, do interního systému a do docházkového systému. Tyto hesla jsou důvěrná a jejich sdílení znamená porušení zásad kybernetické bezpečnosti a zvyšuje se tím hrozba vzniku kybernetického incident.

4.7. Využívání vícefaktorové autentizace při práci mimo organizaci

V rámci využívání pracovních zařízení a práce na dálku je nezbytně nutné používat vícefaktorovou autentizaci. Pro přístup k interním systémům je nutné připojení přes VPN a mobilní aplikaci, kdy po zadání přihlašovacích údajů je nutné přidání vygenerovaného bezpečnostního kódu z této aplikace.

4.8. Ukládání dat na určená uložiště

Pro potřeby zálohování dat je nezbytné, aby zaměstnanci na pracovních zařízeních využívali určená uložiště, na kterých dochází k pravidelnému zálohování. Tím je zajištěno, že nedojde ke ztrátě pracovních dat.

4.9. Nepřipojovat žádná zařízení k PC

K pracovním zařízením není dovoleno připojovat soukromá zařízení. Za předpokladu nutnosti využívat zařízení, která musí být připojena, musí být podána žádost, která bude posouzena a následně IT technikem připojované zařízení zakoupeno a připraveno k dalšímu použití. Připojení k pracovnímu zařízení musí být IT technikem povoleno.

4.10. Neotvírat a neodpovídat na podezřelé emaily

Pro emailovou komunikace musí být využíván pouze určený pracovní email, který je zabezpečený proti nevyžádané poště. Nicméně kybernetické útoky jsou čím dále sofistikovanější, a proto je zaměstnanec povinen podezřelé emaily neotvírat a bezprostředně nahlásit IT možný problém.

5. ZÁVĚREČNÁ USTANOVENÍ

Zpracovatel zodpovídá za seznámení se směrnicí vedoucích pracovníků, kteří dále zajistí proškolení svých podřízených v potřebném rozsahu.

6. PŘÍLOHY

Příloha A: Prezenční listina ze školení

Příloha A. Prezenční listina ze školení

PREZENČNÍ LISTINA ZE ŠKOLENÍ

Téma:

Středisko:

Školení provedl: **Datum:**

Poř.č.	Jméno	Podpis	Poř.č.	Jméno	Podpis

Obrázek 19 Prezenční listina ze školení. Zdroj: (vlastní)