
# VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

## FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

## ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS


# NÁVRH ZAVEDENÍ BEZPEČNOSTNÍCH OPATŘENÍ NA ZÁKLADĚ ISMS PRO MALÝ PODNIK

DESIGN OF SECURITY COUNTERMEASURES IMPLEMENTATION BASED ON ISMS FOR SMALL COMPANY

**DIPLOMOVÁ PRÁCE**
MASTER'S THESIS


**AUTOR PRÁCE** — **Bc. Michal Tomko**
AUTHOR

**VEDOUCÍ PRÁCE** — **Ing. Petr Sedlák**
SUPERVISOR



**BRNO 2019**

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

# Zadání diplomové práce

| | |
|---|---|
| Ústav: | Ústav informatiky |
| Student: | **Bc. Michal Tomko** |
| Studijní program: | Systémové inženýrství a informatika |
| Studijní obor: | Informační management |
| Vedoucí práce: | **Ing. Petr Sedlák** |
| Akademický rok: | 2018/19 |

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

## Návrh zavedení bezpečnostních opatření na základě ISMS pro malý podnik

**Charakteristika problematiky úkolu:**

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

**Cíle, kterých má být dosaženo:**

Hlavním cílem diplomové práce je vytvořit návrh zavedení bezpečnostních opatření pro malý podnik v souladu se systémem řízení bezpečnosti informací. Základem pro úspěšný návrh bezpečnostních opatření je analýza současného stavu společnosti, z které bude samotný návrh vycházet. Účelem této práce nebude kompletní zavedení systému řízení bezpečnosti informací, ale pouze návrh vybraných částí, které povedou ke snížení rizik na úroveň, která bude pro společnost akceptovatelná.

**Základní literární prameny:**

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

ČSN ISO/IEC 27002. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Soubor postupů. Praha: Český normalizační institut, 2014.

DOUCEK, Petr. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2018/19.

V Brně, dne 28. 2. 2019

L. S.

| | |
|---|---|
| doc. RNDr. Bedřich Půža, CSc. | doc. Ing. et Ing. Stanislav Škapa, Ph.D. |
| ředitel | děkan |

**Abstrakt**

Diplomová práca sa zaoberá problematikou zavedenia bezpečnostných opatrení v súlade s ISMS pre malú spoločnosť. Hlavnou náplňou diplomovej práce bude návrh zavedenia bezpečnostných opatrení v spoločnosti. Riešenie návrhu vychádza z analýzy súčasného stavu spoločnosti, vrátane všetkých dôležitých častí a asistovaného zhodnotenia, ktoré bolo vypracované spolu so zodpovednými osobami.

**Kľúčové slová**

systém riadenia bezpečnosti informácií, ISO/IEC 27000, analýza rizík,

**Abstract**

The master`s thesis deals with implementation of security countermeasures in accordance with information security management system for small company. Main concern of the master`s thesis will be design of security countermeasures in company. Solution of the design comes from the analysis of current state of the company including all important parts and assist evaluation which has been processed along with responsible persons.

**Key words**

information security management system, ISO/IEC 27000, risk analysis,

**Bibliografická citácia**

TOMKO, Michal. *Návrh zavedení bezpečnostních opatření na základě ISMS pro malý podnik*. Brno, 2019. Dostupné také z: https://www.vutbr.cz/studenti/zav-prace/detail/119785. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

**Čestné prehlásenie**

Prehlasujem, že predložená diplomová práca je pôvodná a spracoval som ju samostatne. Prehlasujem, že citácie použitých prameňov sú úplné, že som vo svojej práci neporušil autorské práva (v zmysle Zákona č. 121/2000 Zb., o práve autorskom a o právach súvisiacich s právom autorským).

V Brne dne 5. mája 2019

……

podpis študenta

**Poďakovanie**

Chcel by som sa poďakovať vedúcemu mojej diplomovej práce pánovi Ing. Petrovi Sedlákovi za jeho ústretový prístup, cenné rady a pripomienky pri riešení práce.

# Obsah

# ÚVOD

Bezpečnosť je oblasť, ktorá je častokrát vo všeobecnosti veľmi podceňovaná. Obzvlášť v dnešnej dobe, kedy firmy bez informačných a komunikačných technológií nedokážu existovať a je potrebné riadiť bezpečnosť informácií. Fakt je ten, že sa nachádzame v dobe, kedy sa informačné a komunikačné technológie rozvíjajú nekontrolovateľným tempom a riziko sieťových útokov je čoraz väčšie a pravdepodobnosť ohrozenia informačných aktív firmy je veľmi vysoká.

Je preto nutné zaviesť také bezpečnostné opatrenia, ktoré množstvo a dopad týchto útokov eliminujú. Ideálnym riešením je, aby bolo možné riadiť bezpečnosť cielene a účinne ju rozvíjať. Preto je dôležité na túto problematiku pozerať ako na systém riadenia bezpečnosti informácií. Zavedením tohto systému zvýšime celkovú informačnú bezpečnosť v spoločnosti a znížime vznik a dopad rizík, ktoré môžu spoločnosť finančne ohroziť.

# CIELE PRÁCE

Cieľom tejto diplomovej práce je návrh bezpečnostných opatrení na základe identifikácie zraniteľných miest, podľa systému riadenia bezpečností informácií. Po ich implementácií sa dosiahne lepšia úroveň informačnej bezpečnosti čo bude viesť k zníženiu rizík na prijateľnú úroveň, ktorú spoločnosť neohrozí. Celá práca je rozdelená na tri časti.

Cieľom teoretických východísk je oboznámiť čitateľov tejto diplomovej práce so základnými pojmami, ktoré sú nevyhnutné pre pochopenie danej problematiky.

V časti analýza súčasného stavu je cieľom čo najlepšie vyhodnotiť súčasný stav bezpečnosti spoločnosti takým spôsobom, aby jej výstupom bolo možné určiť na aké typy bezpečnostných opatrení sa bude potrebné zamerať v návrhovej časti.

Cieľom návrhovej časti je špecifikovať bezpečnostné opatrenia, ktoré keď sa implementujú, zvýšia bezpečnosť informácií v spoločnosti a znížia dopad rizík na prijateľnú úroveň. Navrhnuté opatrenia by mali primárne cieliť na neprijateľné a nežiadúce riziká, ktoré spoločnosti hrozia.

# 1 TEORETICKÉ VÝCHODISKÁ PRÁCE

V tejto časti sú spomenuté základné teoretické pojmy, z ktorých budem vychádzať v návrhovej časti práce.

## 1.1 Definícia základných pojmov

Táto časť je venovaná definícii základných pojmov, ktoré by mali čitateľa uviesť do danej problematiky.

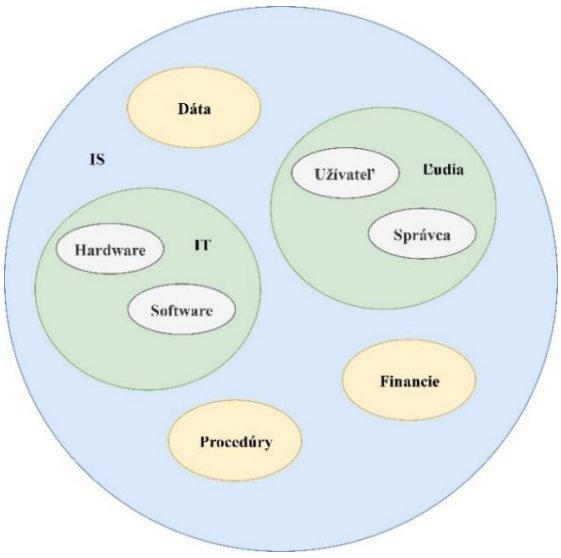
**Dáta** – Formalizovaná reprezentácia pojmov alebo údajov, ktoré vznikajú, sú uchovávané a ďalej spracovávané v rámci výkonu činnosti spoločnosti, alebo v súvislosti s ňou tak, aby bolo možné ich sprístupnenie, interpretácia alebo spracovanie, či už človekom, alebo automatizovanými prostriedkami (7).

**Informácie** – Tvoria kódované dáta, pod čím sa rozumie fyzická interpretácia v úložnom zariadení, prenosovom médiu (1). Inak povedané je to typ dát, ktorých obsah už je zrozumiteľný pre ľudí. Informácie predstavujú najdôležitejšie aktívum informačného systému (7).

**Užívateľ** – Subjekt schopný interaktívne využívať k svojej činnosti informačný systém (7).

**Administrátor** – Subjekt, ktorý je zodpovedný za funkčnosť IS (7).

**Informačný systém** – Systém vzájomne prepojených informácií a procesov, ktoré s nimi navzájom spolupracujú (1). Informačný systém integruje dáta, technické a programové vybavenie, finančné prostriedky a procedúry a pracovníkov (7).




Obrázok 1: Schéma jednotlivých zložiek informačného systému (zdroj: vlastné spracovanie)

**Počítačová sieť** – Môžeme chápať ako otvorený systém s deterministickým chovaním, pomocou ktorého spolu môžu jednotlivé uzly v sieti spoľahlivo komunikovať. Medzi prvky počítačovej siete patrí sieťová infraštruktúra a koncové uzly (2).

**Sieťová infraštruktúra** – Patria do nej všetky sieťové prvky a zariadenia použité pri realizácií ICT prostredia (1). Delíme ju na pasívnu vrstvu a aktívne prvky. Úlohou pasívnej vrstvy je vedenie dát. Aktívne prvky riadia tok dát (2).

**Aktívum –** Je to čokoľvek čo má pre spoločnosť nejakú hodnotu (3). Je to celkový hmotný a nehmotný majetok firmy (1).

**Hrozba** – Je to udalosť, ktorá ohrozuje bezpečnosť spoločnosti (1).

**Zraniteľnosť** – Jedná sa o slabé miesto aktíva (1).

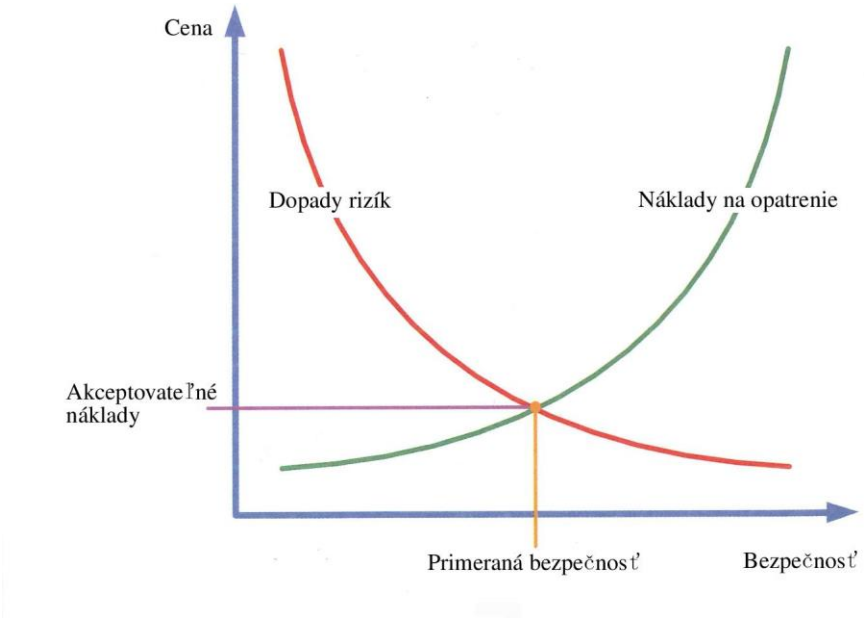
**Bezpečnostné opatrenie** – Bezpečnostným opatrením realizujeme zabezpečenie aktív (7). Ide o činnosť, ktorá má za účel znížiť hrozbu (1).

**Audit** – jedná sa o systematický, nezávislý a dokumentovaný proces určený na získanie výsledkov a ich objektívne vyhodnotenie, aby sa určilo, do akej miery sú splnené kritériá spoločnosti (5).

**Bezpečnostná udalosť** – Jedná sa o identifikovaný stav systému, služby alebo siete, ktoré poukazuje na možné porušenie bezpečnostnej politiky poprípade na zlyhanie bezpečnostných opatrení. Taktiež môže ísť o úplne novú situáciu, ktorá ešte nikdy predtým nenastala a môže byť dôležitá z pohľadu bezpečnosti informácií (3).

**Bezpečnostný incident –** Pokiaľ hrozba pôsobí na dané aktívum dlhšie, tak sa časom môže stať z bezpečnostnej udalosti bezpečnostný incident. Je to jedna, alebo viacero nechcených, alebo neočakávaných bezpečnostných udalostí, u ktorých už hrozí kompromitácia činností, alebo ohrozenie bezpečnosti informácií a s tým spojené finančné straty (3).

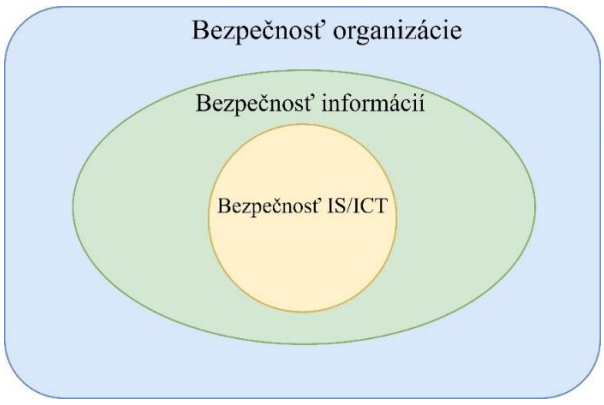
**Primeraná bezpečnosť –** Hodnota aktíva a miera možných pôsobiacich rizík, by mali priamo úmerne odpovedať veľkosti úsilia a investícií do jeho bezpečnosti. To je väčšinou stanovené bezpečnostnou politikou organizácie (1).




Obrázok 2: Graf primeranej bezpečnosti (zdroj: upravené podľa 1)

## 1.2 Informačná bezpečnosť

**Bezpečnosť informácií** – Taktiež nazývaná ako informačná bezpečnosť rieši ochranu informácií a ich dostupnosť. Je zameraná na širokú škálu hrozieb a zaisťuje tak kontinuitu činností organizácie, minimalizuje straty v spoločnosti a maximalizuje návratnosť podnikateľských príležitostí a investícií (4). Je vo vzájomnom súlade s pojmami bezpečnosť organizácie a bezpečnosť IS/ICT. Bezpečnosť organizácie, ktorá je najvyššie postavená a zahŕňa aj bezpečnosť IS/ICT a bezpečnosť informácií zaisťuje bezpečnosť objektu a majetku organizácie. Bezpečnosť informácií zahŕňa okrem bezpečnosti IS/ICT aj prácu s informáciami v nedigitálnej podobe. Aktíva informačného systému, ktoré sú podporované informačnými a komunikačnými technológiami chráni bezpečnosť IS/ICT (1). Vzájomný vzťah medzi bezpečnosťou v organizácií je možné vidieť na nasledujúcom obrázku.




Obrázok 3: Vzájomné vzťahy bezpečnosti v organizácií (zdroj: upravené podľa 1)

Vo všeobecnosti môžeme hovoriť o bezpečnosti informácií ako o zachovaní dôvernosti, integrity a dostupnosti informácií taktiež nazývanú ako CIA triádu (3).

**Dôvernosť (C)** – Znamená zaistenie prístupu informácií iba oprávnenému užívateľovi (3).

**Integrita (I)** – Znamená zaistenie toho, aby informácie boli správne a úplné (3).

**Dostupnosť (A)** – Znamená, aby informácie boli prístupné oprávnenému užívateľovi. v okamihu keď ich potrebuje (3).


Obrázok 4: CIA triáda (zdroj: vlastné spracovanie)

**Bezpečnostný mechanizmus** – Jedná sa o techniku, ktorá sa použije pri implementácií bezpečnosti (1).

**Bezpečnostná funkcia** – Jedná sa o funkciu produktu alebo systému, ktorá prispieva k jeho bezpečnosti (1).

## 1.3 Kybernetická bezpečnosť

Jedná sa o súhrn všetkých právnych, organizačných, technických a vzdelávacích opatrení, ktoré smerujú k zaisteniu ochrany informačných a komunikačných systémov, ktoré tvorí kybernetický priestor a dáta, ktoré sú v nich uložené a prenášané. Je nutné je budovať s plnou podporou organizácie vedenia (9). V Českej republike sa kybernetickou a informačnou bezpečnosťou zaoberá Národný úrad pre kybernetickú a informačnú bezpečnosť (11).

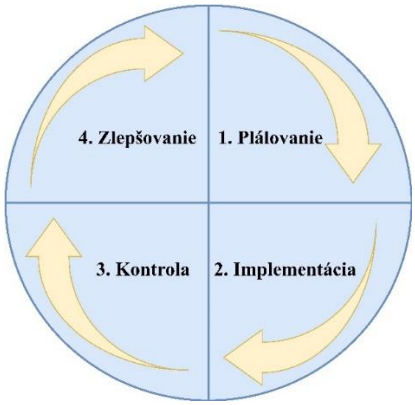
**Kybernetický priestor** – Je reprezentovaný Internetom. Ide o digitálne prostredie, ktoré umožňuje vznik, spracovanie a výmenu informácií tvorených informačnými systémami, službami a sieťami elektronických komunikácií (10).

## 1.4 ISMS

Systém riadenia bezpečnosti informácií, alebo v skratke ISMS, je časť celkového systému riadenia organizácie, založenej na prístupe k rizikám jednotlivých činností. ISMS je zamerané na ustanovenie, zavádzanie, prevádzku, monitorovanie, preskúmavanie, údržbu a zlepšovanie bezpečnosti informácií (3). ISMS je rovnako ako statné systémy riadenia založené na princípe Demingovho cyklu.

**Demingov Cyklus** – Taktiež nazývaný PDCA cyklus. Jedná sa o metódu postupného zlepšovania kvality služieb, procesov, aplikácií alebo dát formou opakovaného vykonávania 4 činností:

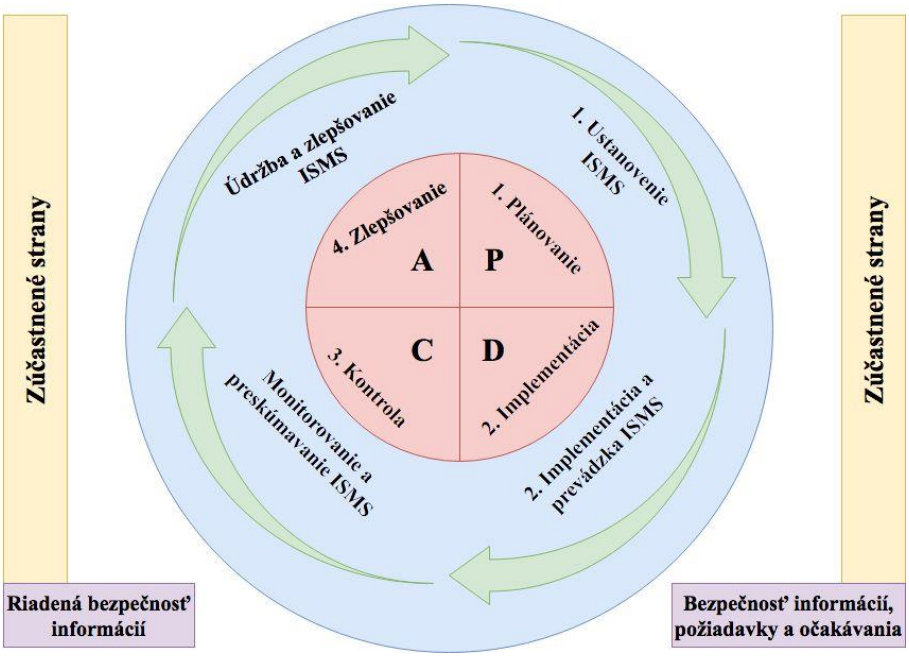
- **Plan (P)** – Naplánovanie toho čo chceme zlepšiť.
- **Do (D)** – Implementácia činností podľa plánu.
- **Check (C)** – V tejto časti kontrolujeme realizované výsledky oproti plánovaným výsledkom.
- **Act (A)** – Vykonanie dodatočných úprav na základe 3. fázy Demingovho cyklu a plošná implementácia zlepšenia (8)




Obrázok 5: Etapy PDCA cyklu (zdroj: vlastné spracovanie)

V prípade ISMS  etapy Demingovho cyklu vyzerajú nasledovne:

- **Ustanovenie ISMS –** Cieľom prvej etapy je upresnenie rozsahu a hraníc, ktorých sa ISMS týka a stanoviť si zrozumiteľné manažérske zadanie a na základe ohodnotenia rizík, vybrať nevyhnutné bezpečnostné opatrenia (6).
- **Implementácia a prevádzka ISMS** – Cieľom druhej etapy je systematicky a účelne presadiť nevyhnutné bezpečnostné opatrenia do chodu organizácie (6).
- **Monitorovanie a preskúmavanie ISMS** – Cieľom tretej etapy je zaistenie spätnej väzby, pravidelného sledovania a hodnotenia úspešných a nedostatočných stránok ISMS (6).
- **Údržba a zlepšovanie ISMS** – Cieľom poslednej etapy je realizácia možných zlepšení ISMS. Či už sústavným zlepšovaním systému, alebo odstraňovaním zistených slabín a nedostatkov, na ktoré sme prišli v tretej fáze (6).




Obrázok 6: PDCA cyklus použiteľný pre ISMS (zdroj: upravené podľa 1)

### 1.4.1 Ustanovenie ISMS

Ustanovenie ISMS je prvou etapou budovania ISMS. Sú pri nej upresnené správne formy riešenia bezpečnosti informácií. Táto etapa má veľmi veľký vplyv a zásadný dopad na fungovanie ISMS v priebehu jeho celého životného cyklu. Pri ustanovení ISMS by sa mali vykonávať nasledujúce skupiny činností:

- Definícia rozsahu, hraníc a väzieb ISMS,
- Definícia a odsúhlasenie Prehlásenia o politike ISMS,
- Riadenie rizík,
- Súhlas vedenia organizácie s navrhovanými zvyškovými rizikami a so zavedením ISMS (6).

**Definícia rozsahu a hraníc**

Ide o vytvorenie osnovy, na základe čoho bude možné stanoviť rozsah a hranice ISMS. V tejto časti si musíme pripomenúť organizačnú štruktúru, umiestnenie lokality a využívané technológie pre prenos a spracovanie informácií. Z hľadiska praktického presadenia ISMS sa môžeme k stanoveniu rozsahu postaviť dvoma spôsobmi:

- **Prvý spôsob** – Rozsah ISMS je identický s rozsahom organizácie od samého počiatku. Veľká výhoda pozostáva v tom, že riadenie od začiatku rieši bezpečnosť informácií v celej organizácií. To však vyžaduje značné finančné náklady a nie vždy sa to dá realizovať (6).
- **Druhý spôsob** – Ďalšou variantov je aby bolo ISMS aplikované iba na jasne definovanú časť organizácie (na vybrané pobočky, určené organizačné celky alebo na ucelený IS. Pri tejto variante je hlavnou výhodou, že na jednotlivé časti môžeme sústrediť vyššiu mieru úsilia (6).

**Prehlásenie o politike ISMS**

Jedná sa o rozsahovo krátky, ale významovo veľmi dôležitý dokument, ktorý prezentuje záujem vedenia organizácie o ISMS a definuje kľúčové podmienky pre ohodnotenie rizík. Vzniká na základe špecifických potrieb danej organizácie. Z praktického hľadiska je dôležité, aby politika ISMS:

- Upresnila ciele ISMS a definovala základný smer a rámec pre riadenie bezpečnosti informácií,
- Brala ohľad na ciele a požiadavky organizácie a súvisiace zákonné, regulatívne a zmluvné požiadavky,
- Vytvorila žiadúce väzby, ktoré sú potrebné pre vybudovanie a údržbu ISMS v danej organizácií,
- Stanovila kritéria, podľa ktorých sú popisované a hodnotené riziká,
- Bola schválená vedením organizácie (6).

**Riadenie rizík**

Riadenie rizík je kľúčovým nástrojom pre systematické riadenie bezpečnosti informácií. Dobrá znalosť bezpečnostných rizík umožňuje výber a presadenie vhodných bezpečnostných opatrení a účinné vynakladanie úsilia pri presadzovaní bezpečnostných opatrení, ktoré tým prinášajú väčšiu efektivitu. Riadenie rizík je základom pre každé ISMS a ovplyvňuje jeho efektivitu fungovania (6). Usporiadanú terminológiu spojenú s riadením rizík a jednotlivými vzťahmi sú zobrazené na obrázku číslo 7.


Obrázok 7: Terminológia spojená s riadením rizík (zdroj: vlastné spracovanie)

- **Riadenie rizík** – Koordinované vykonávanie činností vedúcich k riadení a kontrole organizácie s ohľadom na riziká,
- **Hodnotenie rizík** – Celkový proces analýzy a vyhodnotenia rizík,
- **Analýza rizík** – Systematické používanie informácií k odhadu miery rizika a určeniu jeho zdrojov,
- **Vyhodnotenie rizík** – Proces, pri ktorom porovnávame odhadnuté riziko voči daným kritériám pre určenie jeho významu,
- **Zvládanie rizík** – Proces, pri ktorom vyberáme a prijmeme opatrenia pre zmenu rizika,
- **Akceptácia rizika -** Rozhodnutie sa o tom, že dané riziko prijmeme (6).

**Prehlásenie o aplikovateľnosti**

Jedná sa o dokument obsahujúci a popisujúci vybrané ciele opatrení a jednotlivé bezpečnostné opatrenia, ktoré sú relevantné a aplikovateľné na ISMS organizácie. Musí obsahovať:

- Ciele a bezpečnostné opatrenia a dôvody pre ich výber,
- Ciele a bezpečnostné opatrenia, ktoré sú už v organizácií implementované,
- Vyradené ciele a bezpečnostné opatrenia vrátane dôvodu ich vyradenia (6).

### 1.4.2 Implementácia a prevádzka ISMS

Pri druhej etape zavádzania ISMS sa sústredíme na presadzovanie všetkých bezpečnostných opatrení tak, ako boli navrhnuté v prvej etape životného cyklu ISMS. Nemalo by sa zabudnúť na prípravu jednotlivých plánov, kde sú upresnené termíny a zodpovedné osoby. Všetky bezpečnostné opatrenia by mali byť zdokumentované v **Príručke bezpečnosti informácií**, v ktorej by mali byť vysvetlené bezpečnostné princípy všetkým užívateľom a manažérom. V priebehu tejto fázy je nutné vykonať nasledujúce činnosti:

- Formulovať plán zvládania rizík a začať s jeho zavedením,
- Zaviesť plánované bezpečnostné opatrenia a sformulovať Príručku bezpečnosti informácií,
- Definovať program budovania bezpečnostného povedomia a vykonať prípravu zaškolení všetkých pracovníkov z oblasti riadenia bezpečnosti,
- Upresniť spôsoby merania účinnosti bezpečnostných opatrení a sledovať stanovené ukazovatele,
- Zaviesť postupy a ďalšie opatrenia pre rýchlu detekciu a reakciu na bezpečnostné incidenty,
- Riadiť zdroje, dokumenty a záznamy ISMS (6).

**Plán zvládania rizík**

Je to dôležitý dokument popisujúci všetky činnosti ISMS, ktoré sú potrebné pre riadenie bezpečnostných rizík, stanovené ciele a priority činností v oblasti ISMS, potrebné zdroje a obmedzujúce faktory. Taktiež by sa mala určiť zodpovednosť za vykonanie naplánovaných činností. Východiskom pre jeho zostavenie sú dva základné zdroje informácií pre ISMS:

- Podklady získané pri ustanovení ISMS. Jedná sa hlavne o výsledky riadení rizík zdokumentované v správe o hodnotení rizík a v prehlásení o aplikovateľnosti,
- Podnety získané pri pravidelnom prehodnocovaní ISMS vedením organizácie, ktoré by mali byť zozbierané v správe o stave ISMS (6).

**Príručka bezpečnosti informácií**

Ide o dokument, v ktorom sú definované stanovené bezpečnostné pravidlá a zodpovednosti. Príručka bezpečnosti informácií v sebe zahŕňa dokumenty typu bezpečnostné politiky a smernice (6).

**Budovanie bezpečnostného povedomia**

Rozvoj ISMS a pravidelná zmena pracovníkov v spoločnosti vyžadujú trvalý a nekonečný proces, ktorý rozhoduje o efektivite ISMS. Cieľom je prehlbovanie bezpečnostného povedomia, za ktorým sa skrýva premietnutie všetkých definovaných pravidiel a postupov do skutočného chovania všetkých zodpovedných osôb v spoločnosti (6).

**Meranie účinnosti ISMS**

Ide o vyhodnotenia a analýzu jednotlivých už zavedených bezpečnostných opatrení. Je nutné definovať a pravidelne sledovať objektívne údaje (6).

### 1.4.3 Monitorovanie a preskúmavanie ISMS

Hlavným cieľom tretej fázy zavádzania ISMS je zaistenie spätnej väzby. Malo by teda ísť o preverenie všetkých aplikovaných bezpečnostných opatrení a ich dôsledkov na ISMS. To začína u priamej kontroly zodpovedných osôb zo strany nadriadených. Dôležitú rolu tu zohráva aj nezávislé posúdenie fungovania a účinnosti ISMS pomocou interných auditov. V priebehu tejto fáze je nutné vykonať nasledujúce činnosti:

- Monitorovať a overiť účinnosť presadenia bezpečnostných opatrení,
- Vykonať interné audity ISMS,
- Prichystať správu o stave ISMS a na jej základe prehodnotiť ISMS na úrovniach vedení organizácie (6).

### 1.4.4 Údržba a zlepšovanie ISMS

Poslednou štvrtou fázou zavádzania ISMS je jeho neustála údržba a zlepšovanie. V tejto časti je potrebné zbierať podnety k zlepšeniu ISMS a k napraveniu všetkých nedostatkov, ktoré sa v ISMS objavujú. V priebehu tejto fázy je nutné vykonať tieto činnosti:

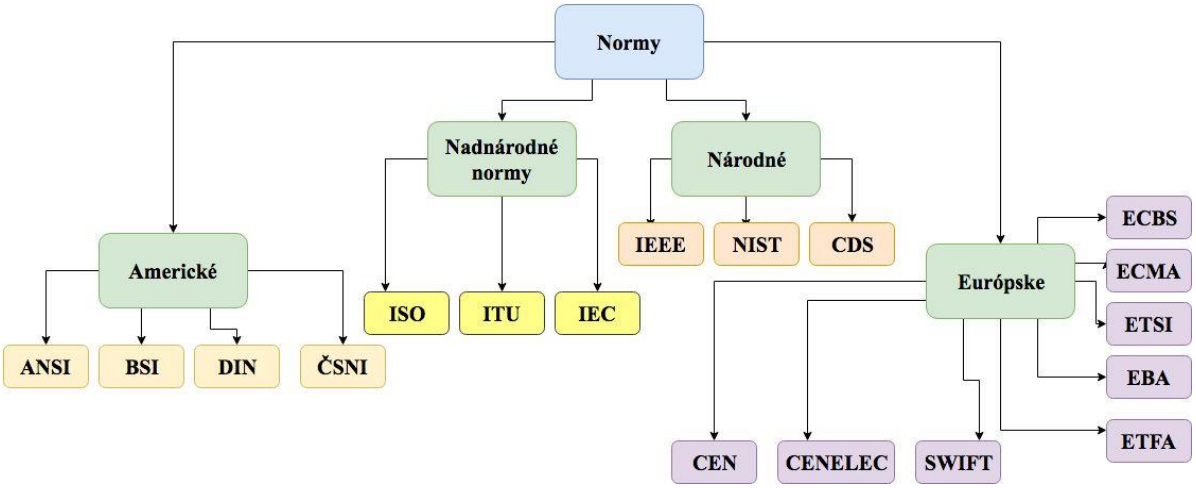
- Zaviesť identifikované možnosti zlepšenia ISMS a to predovšetkým na základe predchádzajúceho vedenia,
- Vykonať zodpovedajúce nápravné a preventívne opatrenia pre odstránenie nedostatkov (6).

## 1.5 Normy

Táto časť sa zaoberá normalizačnými inštitúciami, ktoré sa zaoberajú štandardizačnou činnosťou a štandardizáciou bezpečnosti IT na rôznych úrovniach. Bude tu predstavených viacero normalizačných inštitúcií. Predtým je ale potrebné vysvetliť si rozdiel medzi štandardom a normou.

**Štandard** – Dokument obsahujúci technické špecifikácie alebo iné podobné presne stanovené kritéria dôsledne používané ako pravidlá, smernice alebo definícia charakteristických vlastností, ktoré zabezpečujú, že materiály, výrobky, procesy alebo služby spĺňajú presne stanovené kritéria (1).

**Norma** – Odporučenie k danému štandardu alebo riešeniu. Jedná sa o odporúčania použiteľných štandardov k realizácií požadovaného riešenia (1).




Obrázok 8: Štruktúra noriem a prehľad normalizačných inštitúcií (zdroj: vlastné spracovanie)

### 1.5.1 Nadnárodné normalizačné inštitúcie

Medzi najznámejšie organizácie vydávajúce nadnárodné normy patria organizácie spomenuté nižšie.

**International Organisation for Standardization (ISO)** – Poslaním organizácie ISO je podporovať rozvoj štandardizačných aktivít vo svete so zameraním na uľahčenie medzinárodných zmien tovaru a služieb a na spoluprácu vo sfére vedeckých, technologických a ekonomických aktivít (1)

**International Telecommunications Union (ITU) –** Medzinárodná organizácia spadajúca pod OSN (1).

**International Electrotechnical Comission (IEC) -** Celosvetová organizácia, ktorá pripravuje a vydáva medzinárodné normy z oblasti elektrotechniky, elektroniky a podobným odvetviam (1).

### 1.5.2 Národné normalizačné inštitúcie

Normalizáciu v oblasti IT v jednotlivých štátoch zaisťujú národné normalizačné organizácie, ktoré sú väčšinou členskými organizáciami ISO alebo IEC.

**American National Standards Institute (ANSI) –** Inštitúcia umožňujúca vývoj amerických národných noriem kvalifikovaným skupinám (1).

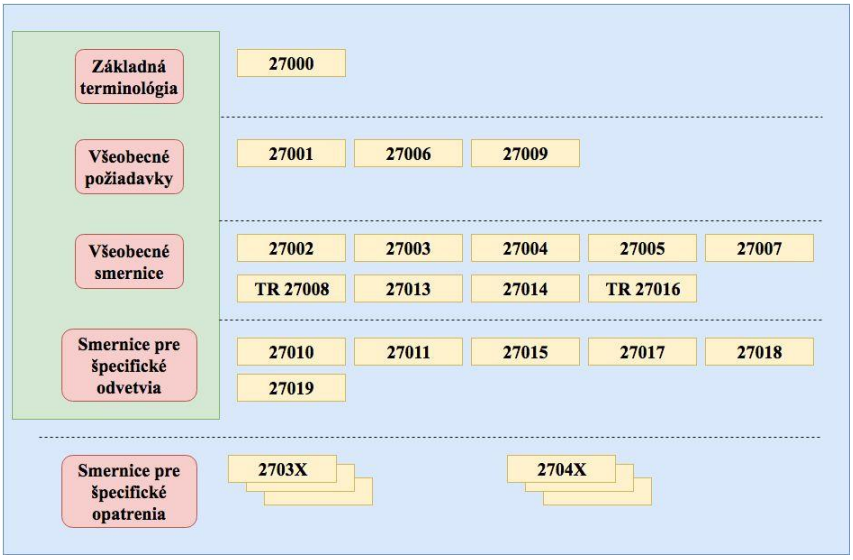
**British Standard Institute (BSI)** – Inštitúcia vytvárajúca britské národné normy (1).

**Deutsches Institut für Normung (DIN)** – Nemecká inštitúcia vytvárajúca národné normy (1).

**Český normalizačný inštitút (ČSNI) –** Bol zriadený ako štátna príspevková organizácia. Jeho činnosť je zameraná na tvorbu českých technických noriem, ich distribúciu a vydávanie, poskytnutie informácií o technických normách a spoluprácu s nevládnymi medzinárodnými a európskymi normalizačnými organizáciami (1).

### 1.5.3 Normy vzťahujúce sa k problematike ISMS

Väčšina noriem, vzťahujúcich sa k problematike ISMS vychádza z rady 27K. Ich štruktúru a rozdelenie môžete vidieť na obrázku číslo 9.




Obrázok 9: Vzájomné vzťahy medzi normami vzťahujúcich sa k problematike ISMS (zdroj: vlastné spracovanie)

### a) Normy popisujúce základnú terminológiu

**ČSN ISO/IEC 27000**: *ISMS - prehľad a slovník*

Táto medzinárodná forma poskytuje slovník definícií a použitých termínov v rade noriem ISMS. Organizácie tak môžu za použitia noriem ISMS vyvinúť a implementovať rámec pre riadenie bezpečnosti svojich bezpečnostných aktív a pripraviť nezávislé ohodnotenie svojich ISMS týkajúcich sa ochrany informácií, ktoré im boli zverené zákazníkmi alebo tretími stranami (1).

### b) Normy popisujúce všeobecné požiadavky

**ČSN ISO/IEC 27001:** *ISMS – Požiadavky*

Norma špecifikuje požiadavky na cyklus formalizovaných ISMS v kontexte celkových rizík činností organizácie. Cyklom je myslené ustanovenie, zavádzanie a prevádzku, monitorovanie a preskúmanie, a nakoniec udržiavanie a zlepšovanie. Definuje požiadavky na bezpečnostné opatrenia upravených na základe potrieb organizácií či jej častí. Norma má 38 strán a bola preložená z anglického originálu (1).

**ČSN ISO/IEC 27006:** *Požiadavky na orgány vykonávajúce audit a certifikáciu ISMS*

Norma špecifikuje požiadavky a poskytuje odporúčania pre orgány vykonávajúce audit a certifikáciu ISMS a doplňuje požiadavky obsiahnuté v normách ČSN ISO/IEC 17021 a ČSN ISO/IEC 27001. Primárne je určená k podpore procesu akreditácie certifikačných orgánov poskytujúcich certifikácie ISMS (1).

**ČSN ISO/IEC 27009:** *Špecifické aplikácie normy ISO/IEC 27001 - Požiadavky*

Norma definuje požiadavky k použitiu normy ISO/IEC 27001 pre špecifické odvetvia (12).

**c) Normy popisujúce všeobecné smernice**

**ČSN ISO/IEC 27002:** *ISMS – Súbor postupov*

Norma poskytuje zoznam všeobecne akceptovaných cieľov kontroly a osvedčených postupov, ktoré sa majú použiť ako návod pri výbere a vykonávaní kontrol na dosiahnutie informačnej bezpečnosti (5).

**ČSN ISO/IEC 27003:** *Smernice pre implementáciu ISMS*

Norma poskytujúca praktické pokyny a ďalšie informácie pre zriadenie, implementáciu, prevádzku, monitorovanie, kontrolu, udržiavanie a zlepšovanie ISMS v súlade s normou ČSN ISO/IEC 27001 (5).

**ČSN ISO/IEC 27004:** *Riadenie bezpečnosti informácií – Merania*

Norma poskytujúca odporúčania pre vývoj a používanie metrík a pre merania účinnosti zavedeného ISMS a účinnosti opatrení alebo skupín opatrení uvedených v ČSN ISO/IEC 27001. Predmetom programu merania bezpečnosti informácií je implementácia týchto odporúčaní (1).

**ČSN ISO/IEC 27005:** *Riadenie rizík bezpečnosti informácií*

Norma poskytujúca odporúčania pre riadenie rizík v oblasti bezpečnosti informácií. Postup opísaný v tejto norme podporuje všeobecné koncepty špecifikované v ČSN ISO/IEC 27001 (5).

**ČSN ISO/IEC 27007:** *Smernice pre audit ISMS*

Norma poskytujúca odporúčania pre vykonávanie auditov ISMS, ako aj odporúčania o spôsobilosti audítorov ISMS, okrem odporúčaní obsiahnutých v norme ISO 19011, ktorá sa vzťahuje na systémy riadenia vo všeobecnosti (5).

**ČSN ISO/IEC TR 27008:** *Smernice pre audítorov ISMS*

Technická správa poskytujúca odporúčania k preskúmavaniu, zavádzaniu a prevádzke opatrení vrátane kontroly technickej zhody opatrení IS podľa štandardov ustanovených danou organizáciou (5).

**ČSN ISO/IEC 27013:** *Smernice pre integrovanú implementáciu noriem ISO/IEC 27001 a ISO/IEC 20000-1*

Norma poskytujúca odporúčania pre integrovanú implementáciu noriem ISO/IEC 27001 a ISO/IEC 20000-1 pre organizácie, ktoré majú v pláne:

- implementovať normu ISO / IEC 27001, ak už ISO / IEC 20000-1 je zavedená, alebo naopak,
- spoločne implementovať ISO / IEC 27001 a ISO / IEC 20000-1,
- integrovať existujúce systémy riadenia ISO / IEC 27001 a ISO / IEC 20000-1 (5).

**ČSN ISO/IEC 27014:** *Správa bezpečnosti informácií*

Norma poskytujúca odporúčania o princípoch a procesoch pre správu bezpečnosti informácií, pomocou ktorej môžu organizácie hodnotiť, riadiť a monitorovať riadenie informačnej bezpečnosti (5).

**ČSN ISO/IEC TR 27016:** *Riadenie bezpečnosti informácií – Organizačná ekonomika*

Technická správa poskytuje metodiku, ktorá organizáciám umožní pochopiť po ekonomickej stránke, ako presnejšie ohodnotiť svoje informačné aktíva, ohodnotiť potenciálne riziká, oceniť hodnotu ochranných opatrení a odhadnúť optimálnu úroveň zdrojov, ktoré sa majú použiť na zabezpečenie informačných aktív organizácie (5).

**d) Normy popisujúce smernice pre špecifické odvetvia**

**ČSN ISO/IEC 27010:** *Smernice pre riadenie bezpečnosti informácií pre medzi-odvetvové a medzi-organizačné komunikácie*

Norma poskytujúca odporúčania, ktoré sú nad rámec odporúčaní zahrnutých v norme ISO/IEC 27000 pre implementáciu ISMS v rámci komunít zdieľajúcich informácie a dodatočne poskytujúcich kontroly a návody týkajúce sa iniciovania, implementácie, udržiavania a zlepšovania informačnej bezpečnosti v medzi- organizačné a medziodvetvové komunikácie (5).

**ČSN ISO/IEC 27011:** *Smernice pre riadenie bezpečnosti informácií pre telekomunikačné organizácie na základe ISO/IEC 27002*

Norma poskytujúca odporúčania podporujúce implementáciu riadenia bezpečnosti informácií v telekomunikačných organizáciách (5).

**ČSN ISO/IEC TR 27015:** *Smernice pre riadenie bezpečnosti informácií pre finančné služby*

Technická správa poskytujúca odporúčania popri odporúčaní uvedených v norme ISO/IEC 27000 (5).

**ČSN ISO/IEC 27017:** *Kódex postupov pre kontroly informačnej bezpečnosti založených na norme ISO/IEC 27002 pre cloudové služby*

Kódex poskytujúci odporúčania pre kontroly informačnej bezpečnosti vzťahujúce sa na poskytovanie a využívanie cloudových služieb (5).

**ČSN ISO/IEC 27018:** *Kódex postupov na ochranu osobných údajov vo verejných cloudových úložiskách*

Kódex ustanovujúci všeobecne prijateľné kontrolné objekty, kontroly a odporúčania pre implementačné opatrenia na ochranu osobných údajov v súlade so zásadami ochrany osobných údajov v norme ISO / IEC 29100 pre verejné prostredie cloud computingu (5).

**ČSN ISO/IEC TR 27019:** *Smernice pre riadenie bezpečnosti informácií pre energetický priemysel.*

Technická správa poskytujúca odporúčania ohľadom riadenia bezpečnosti informácií pre energetický priemysel (5).

**ČSN ISO/IEC 27799:** *Riadenie bezpečnosti informácií v zdravotníctve podľa za použitia normy ISO/IEC 27002*
Norma poskytujúca odporúčania na podporu implementácie riadenia bezpečnosti informácií v zdravotných organizáciách (5).

## 1.6 Analýza rizík

Analýza rizík je proces, kedy sa snažíme pochopiť podstatu rizika a stanoviť jeho úroveň. Vďaka analýze rizík je možné určiť hodnotu informačných aktív, identifikovať možné hrozby a zraniteľnosti, ktoré už existujú alebo ešte len môžu existovať. Ďalej sa identifikujú stávajúce opatrenia a ich súčasný účinok na identifikované riziká, určujú sa potenciálne dopady a stanoví sa úroveň rizík podľa stanovených kritérií. Analýza rizík môže byť kvalitatívna, alebo kvantitatívna, ale často sa v praxi používa kombinácia týchto dvoch metód (14).

### 1.6.1 Kvalitatívna analýza

Kvalitatívna analýza používa k popisu potenciálnych následkov široký rozsah kvalifikačných atribútov. Jej výhodou je, že jej jednoduché pochopenie. Medzi nevýhody patrí závislosť na subjektívnom výberu rozsahu hodnotenia. Tento rozsah je možné upraviť alebo prispôsobiť spôsobom, ktorý bude odpovedať okolnostiam a pre rôzne riziká sa dajú použiť rôzne popisy. Najčastejšie sa používa:

- Ako počiatočná preverovacia činnosť k identifikácií rizík, ktoré vyžadujú podrobnejšiu analýzu,
- Pri prípadoch, kde je tento druh analýzy vhodné použiť pre rozhodovanie,
- Pri prípadoch, kde sú číselné údaje alebo zdroje pre kvantitatívnu analýzu rizík nevhodné (14).

Pri kvantitatívnej analýze je odporúčané pracovať so skutočnými informáciami a dátami, ktoré máme k dispozícií (14).

### 1.6.2 Kvantitatívna analýza

Pri analýze rizík kvantitatívnou metódou sa používa stupnica s číselnými hodnotami. Túto stupnicu používame pre následky a pravdepodobnosť a na určenie stupnice používa dáta z rôznych zdrojov. Kvalita analýzy závisí na presnosti a úplnosti číselných hodnôt a platnosti použitých modelov. Pri kvantitatívnej analýze sa často pracuje s historickými informáciami a dátami. Jej výhoda je priama súvislosť s cieľmi bezpečnosti informácií a záujmami organizácie. Nevýhodou kvantitatívnej analýzy je nedostatok dát a informácií u nových rizík alebo slabých miest v bezpečnosti alebo keď nemáme k dispozícií konkrétne dáta čo môže mať za následok mylný dojem o presnosti výsledkov. Spôsob akým sú následky a pravdepodobnosť vyjadrené sa budú meniť podľa typu rizika a účelu (14).

### 1.6.3 Fázy analýzy rizík

Fázy analýzy rizík môžeme rozdeliť do troch častí:

**Prvá fáza**

V prvej fáze je cieľom identifikovať a ohodnotiť aktíva spoločnosti na základe možného dopadu pri porušení dostupnosti, dôvernosti alebo integrity (1).

- **Identifikácia aktív –** Mali by byť identifikované všetky aktíva spoločnosti. Jedná sa o všetko čo má pre spoločnosť hodnotu a vyžaduje ochranu. Kvalita identifikácie aktív ovplyvní celkové množstvo informácií nazbieraných v priebehu posúdenia rizík (1).
- **Ohodnotenie aktív –** Po identifikácií aktív nasleduje ich ohodnotenie. Tie reprezentujú význam daného aktíva pre činnosť spoločnosti. Vstupné údaje sú väčšinou zaistené vlastníkmi a užívateľmi aktív (1)

**Druhá fáza**

V druhej fáze je cieľom identifikovať a ohodnotiť hrozby pôsobiace na aktíva a možné zraniteľnosti, ktoré im hrozia a na základe toho stanoviť úroveň rizika (1).

- **Hodnotenie aktív –** Hrozba je niečo, čo môže poškodiť aktívum spoločnosti. Môžu byť prírodného, alebo ľudského pôvodu a môžu byť úmyselné, alebo náhodné (1).
- **Odhad zraniteľnosti –** Cieľom je odhalenie slabých miest vo fyzickom prostredí, spoločnosti, postupoch, personálu manažmentu, administrácií HW, SW, alebo v komunikačnom zariadení, ktoré môžu byť využité zdrojom hrozby a spôsobiť škodu na aktívach (1).
- **Úroveň rizika –** Je vypočítaná na základe hodnoty aktíva, jeho hrozieb a zraniteľností (14).

**Tretia fáza**

Treťou fázou analýzy rizík je výber ochranných opatrení vďaka čomu sa minimalizujú prípadné riziká (1).

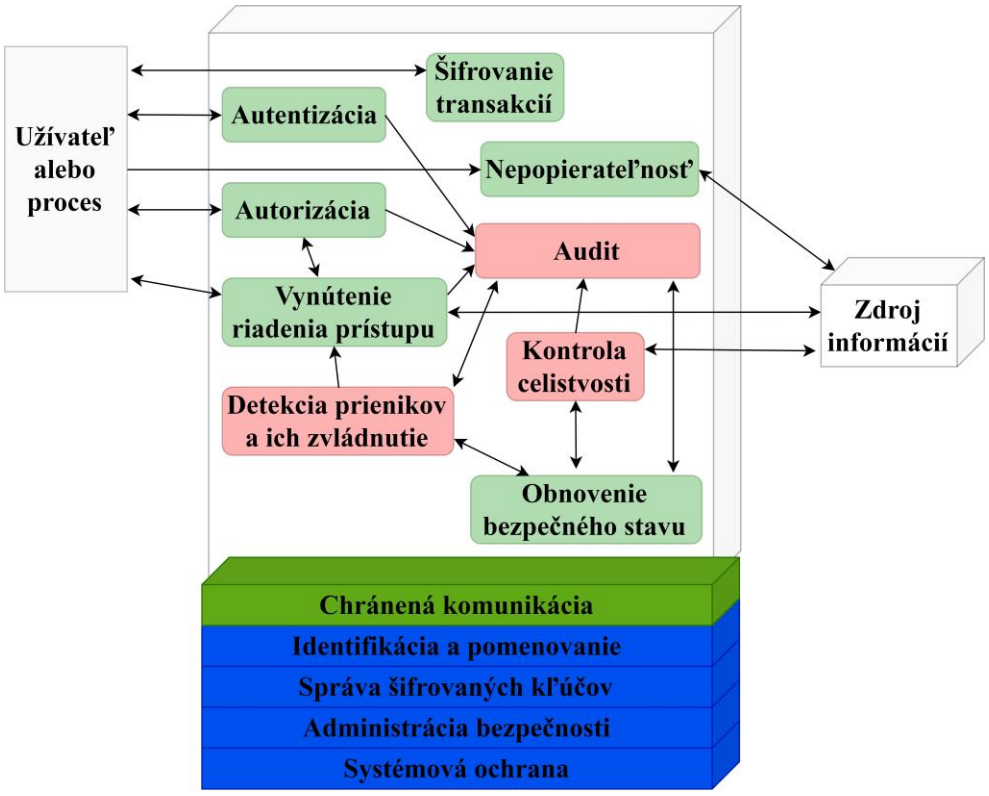
- **Ochranné opatrenia** – Medzi základné kategórie opatrení patrí riadenie a politika bezpečnosti IT, kontrola bezpečnostnej zhody, riešenie incidentov, personálne opatrenie, prevádzkové problémy, plánovanie kontinuity činnosti spoločnosti, fyzická bezpečnosť (1).

## 1.7 Bezpečnostné opatrenia

Cieľom je stanoviť minimálnu sadu ochranných bezpečnostných opatrení slúžiacich k ochrane všetkých, alebo len nejakých častí systémov IT. Potrebnej ochrany je možné dosiahnuť pomocou použitia katalógov ochranných opatrení, ktoré už navrhujú a popisujú sady ochranných opatrení k ochrane systémov IT proti najbežnejším hrozbám. Základné rozlíšenie bezpečnostných opatrení delíme na:

- Preventívne,
- Detekcia a reakcia,
- Podporné (1).

Rozlíšenie bezpečnostných opatrení je znázornené na obrázku číslo 10. Modrá farba značí podporné opatrenia, zelená preventívne a červená detekciu a reakciu.



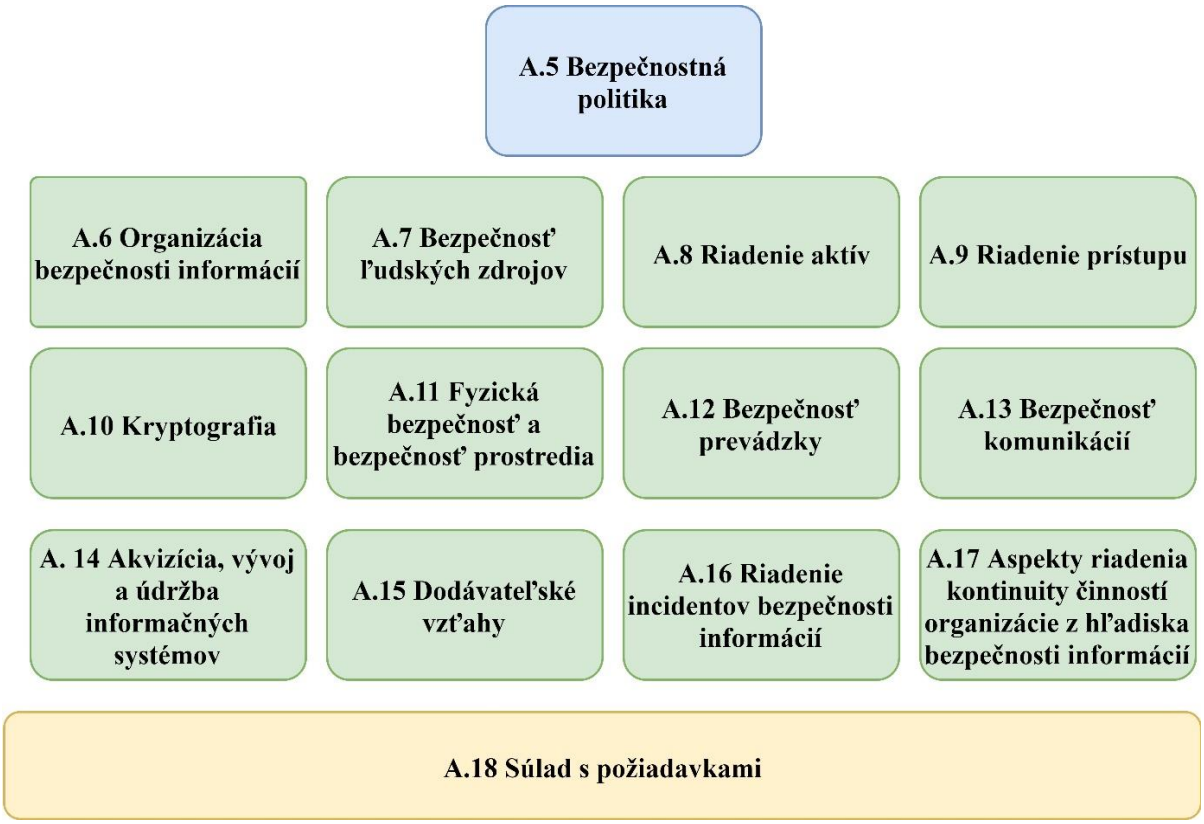

Obrázok 10: Rozlíšenie bezpečnostných opatrení (zdroj: upravené podľa 1)

### 1.7.1 Výber bezpečnostných opatrení

Princípom bezpečnostných opatrení je minimalizácia rizík. V dnešnej dobe existuje množstvo noriem a metodík, z ktorých si môžeme vybrať bezpečnostné opatrenia. Medzi najdôležitejšie sú zaradené všeobecne aplikované ochranné opatrenia. Jedná sa o tieto základné kategórie:

- Riadenie politiky bezpečnosti,
- Kontrola bezpečnostnej zhody,
- Riešenie incidentov,
- Personálne opatrenia,
- Prevádzkové problémy,
- Plánovanie kontinuity činnosti spoločnosti,
- Fyzická bezpečnosť (1).

V prípade tejto práce budú zavedené bezpečnostné opatrenia v súlade s ISMS. Súbor pre riadenie bezpečnosti informácií popisuje norma **ČSN ISO/IEC 27002:2014**. Odporúčania normy obsahuje 113 bezpečnostných opatrení rozdelených do 14 oblastí.




Obrázok 11: Oblasti ISMS podľa normy ISO/IEC 27002 (zdroj: vlastné spracovanie)

# 2 ANALÝZA SÚČASNÉHO STAVU

Táto kapitola je venovaná predstaveniu spoločnosti. Budem popisovať v akom obore spoločnosť podniká, aké služby poskytuje zákazníkom, aký má stav sieťovej infraštruktúry a vykonám analýzu vybraných oblastí.

## 2.1 Základné informácie o spoločnosti

Spoločnosť si nepraje, aby bolo jej meno v tejto práci spomenuté, pretože sa jedná o problematiku, pri ktorej sa odhaľujú citlivé informácie spoločnosti, čo by mohlo viesť k ich zneužitiu . Z toho dôvodu ju budem označovať len ako spoločnosť.

Právna forma spoločnosti je spoločnosť s ručením obmedzeným. Spoločnosť sa zaoberá ekonomickými činnosťami a na trhu už pôsobí vyše 10 rokov. Poskytuje komplexné poradenské služby pre malé a stredné podnikateľské subjekty.

Medzi ich základné služby patrí: spracovanie jednoduchého a podvojného účtovníctva, mzdy a personalistika, daňové poradenstvo a daňový audit. Taktiež ponúka na prenájom vlastné virtuálne kancelárie iným začínajúcim spoločnostiam.

## 2.2 Organizačná štruktúra

V súčasnosti v spoločnosti pracuje 12 zamestnancov.Za chod celej firmy zodpovedá konateľ, ktorý je zároveň majiteľom firmy. Reprezentuje samotnú spoločnosť a vykonáva všetky dôležité firemné rozhodnutia ako napríklad uzatváranie partnerstiev s novými zákazníkmi, tvorba obchodnej stratégie firmy, nákup hmotného a nehmotného majetku a zároveň musí dohliadať na chod celej firmy. V kancelárií má k dispozícií asistenta, ktorý rieši jednoduché organizačné a personálne problémy.

Jednotlivý pracovníci majú pridelený určitý počet klientov, pre ktorých spracovávajú požadované agendy, čím sa rozumie spracovanie jednoduchého poprípade podvojného účtovníctva, spracovania miezd a daňových priznaní podľa platnej legislatívy.

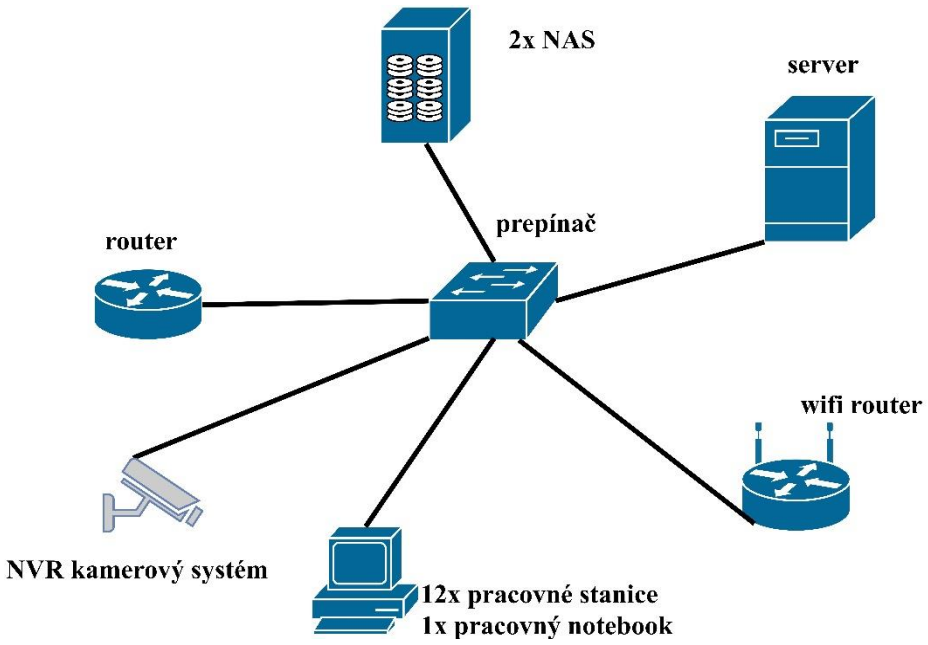
V spoločnosti je zamestnaný IT technik, ktorý zodpovedá za bezpečnosť a správny chod celej siete.

## 2.3 Popis sídla

Sídlo spoločnosti sa nachádza v Žiline, na pokraji mesta v časti obytnej zóny mimo záplavovú oblasť. V jej blízkosti sa nachádza niekoľko rodinných domov a zhruba 100 metrov od sídla vedie železničná trať. Okolie spoločnosti je oplotené a strážené bezpečnostnými kamerami. Vstup do objektu vedie popri hlavnej ceste a je zabezpečený samonosnou posuvnou bránou na diaľkové ovládanie. Vstup do budovy je zabezpečený alarmom, ktorý sa musí vždy pred samotným vstupom deaktivovať a pri odchode zase zapnúť. Kľúče od budovy má konateľ spoločnosti a jeho asistentka. Na prízemí sa nachádzajú skladové a archivačné priestory, sociálne zariadenie a kancelária majiteľa firmy. Na poschodí sú 3 kancelárie. Jednotlivé miestnosti sú navzájom prepojené. Politika fyzickej bezpečnosti nie je písomne zdokumentovaná ale postupy medzi zamestnancami existujú.

## 2.4 Popis siete

V tejto časti popíšem schému siete spoločnosti. Ako prvé zariadenie, do ktorého je zapojený kábel od poskytovateľa internetu je router s funkciami firewall a NAT. Router je prepojený s prepínačom, ktorý má funkcionalitu VLAN na logické oddelenie sietí a predovšetkým zvýšenú bezpečnosť. Ďalej sa v sieti nachádza server, 2x NAS na zálohy dát, wifi router, pracovné stanice zamestnancov, pracovný notebook obchodného riaditeľa a NVR kamerový systém.




Obrázok 12: Popis siete (zdroj: vlastné spracovanie)

## 2.5 Logické rozdelenie siete

Táto kapitola bude popisovať logické rozdelenie siete vďaka funkcionalite VLAN na prepínači. Fyzická sieť je rozdelená na 4 časti respektíve do štyroch VLAN. Jednotlivé časti VLAN budem označovať ako V1,V2,V3,V4. V1 tvorí deväť pracovných staníc a server. V2 tvoria dva dátové úložiská NAS a server. V3 tvorí server a NVR kamerový systém. Poslednú časť siete V4 tvorí wifi router, ktorý sprostredkováva pripojenie pre hostí.

## 2.6 Serverovňa

Serverovňa sa nachádza v samostatnej miestnosti, ktorá je zamknutá. Prístup do nej majú iba IT technik a majiteľ firmy. Miestnosť je plne klimatizovaná s dobrým prúdením vzduchu. V serverovni sa nachádza hardwarový server, na ktorom je nainštalovaný operačný systém Windows server 2016. Na serveri sa nachádza databáza účtovného softwaru, informačný systém a dáta z lokálnych počítačov. Server okrem iného poskytuje DHCP a FTP služby a taktiež sa na ňom nachádza firewall. Na serveri je nainštalovaná najnovšia verzia antivírového programu ESET file security a ESET remote administrator, ktorého výhodou je správa všetkých licencií z jedného miesta cez webový prehliadač. V serverovni sa okrem iného nachádzajú dva dátové úložiská NAS a UPS jednotky

## 2.7 Pracovné stanice

V spoločnosti sa nachádza 12 pracovných staníc, na ktorých je operačný systém windows 10. Na každej z nich je taktiež nainštalovaná najnovšia verzia antivírového programu ESET Smart Security Premium. Podobne tomu je aj u pracovného notebooku konateľa spoločnosti. Každá pracovná stanica má pri sebe záložný UPS zdroj, ktorý má za účel ochrániť dáta v prípade výpadku elektriny.

## 2.8 Wifi-router

Bezdrôtové pripojenie slúži predovšetkým na sprostredkovanie internetu pre hostí, ktorí navštívia firmu. O zabezpečenie bezdrôtového pripojenia je postarané vďaka WPA2 šifrovaniu.

## 2.9 Kamerový systém

Celý objekt je strážený bezpečnostnými IP kamerami. Všetky kamery sú napojené na NVR jednotku, ktorá je vybavená slotom na pevný SATA disk na zálohu dát. Sledovanie záznamu je umožnené 24 hodín vďaka funkcií nočného videnia. Ďalšou dobrou funkcionalitou je to, že v prípade straty signálu alebo neoprávneného vstupu do objektu v stanovených hodinách sa zo zariadenia odošle varovný e-mail. Napájanie kamier je realizované cez POE v dátovom kábli.

## 2.10 Zálohy dát

V spoločnosti prebiehajú dva typy záloh. Každá záloha má presne nastavený čas a dátum kedy sa má spustiť. Pre každú z týchto záloh je pripravené dátové úložisko NAS, ktoré má zrkadlené disky pre väčšiu bezpečnosť a dostupnosť dát. Prvý typ zálohy je záloha účtovníckych dát, ktorá prebieha každý deň a spúšťa sa presne o polnoci. Druhý typ zálohy je záloha lokálnych dát z pracovných staníc, ktorá prebieha na konci týždňa a tiež je naplánovaná, aby sa spustila o polnoci. Zálohy dát sú ešte kvôli dodatočnej bezpečnosti každého štvrťroka skopírované a archivované na externý disk. Záloha dát prebieha pomocou SSL šifrovaného spojenia, ale samotné dáta šifrované nie sú. Je tu však jeden problém a to je obnova dát zo zálohy, ktorú spoločnosť v pravidelných intervaloch nevykonáva.

## 2.11 Užívateľské prístupy

Užívateľské prístupy sú rozdelené na dva účty. Prvý účet je pre zamestnanca a druhý pre administrátora. Rozdiel medzi nimi je v oprávneniach, ktoré majú. Účet zamestnanca má obmedzený prístup k adresárom a má zakázané púšťať niektoré aplikácie. Na druhej strane účet administrátora má plné práva a tým pádom aj prístup ku všetkým adresárom. Prístup na všetky pracovné stanice je zabezpečený heslom. Heslo má stanovenú minimálnu dĺžku 15 znakov a musí tam byť minimálne jedno veľké, malé písmeno a jedna číslica. Potenciálny problém v zabezpečení je však ten, že heslá nemajú nastavenú ich exspiráciu. Ďalším bezpečnostným problémom je to, že zamestnanecké heslá pre užívateľské kontá na jednotlivé stanice sú takmer identické s tým, že posledný znak hesla je číslica, ktorá sa rovná číslu pracovnej stanice čo reprezentuje potenciálne veľké bezpečnostné riziko v tom, že pokiaľ dôjde k odcudzeniu hesla jednej pracovnej stanice útočník nemusí dlho premýšľať a zistí, že má prístup aj k ostatným pracovným staniciam.

## 2.12 Záložné zdroje

Záložné UPS zdroje sú dôležité pri výpadku elektrickej energie. Nachádzajú sa v serverovni a sú dva. Jeden napája server a druhý napája router, prepínač, NVR jednotku a dátové úložiská NAS. Okrem záložných zdrojov, ktoré sa nachádzajú v serverovni, má spoločnosť malé záložné zdroje, ktoré napájajú pracovné stanice.

## 2.13 Požiadavky spoločnosti

Po konzultácií s vedením spoločnosti som zistil, že hlavným cieľom spoločnosti nie je nechať sa certifikovať. Vzhľadom na veľkosť pobočky a dostupnosť finančných zdrojov by to nebolo možné. Spoločnosť si však uvedomuje dôležitosť bezpečnosti a finančné riziká, ktoré môžu nastať v prípade, že nie sú zavedené dostatočné bezpečnostné opatrenia. Jej hlavnou požiadavkou je posúdenie súčasného stavu bezpečnostných opatrení, identifikácia zraniteľných miest, nedostatkov a následný návrh nutných bezpečnostných opatrení.

## 2.14 Asistované zhodnotenie

Na to aby, som si mohol urobiť predstavu o stave celkovej bezpečnosti som vypracoval asistované zhodnotenie spolu so zodpovednými pracovníkmi firmy. Na jeho vypracovanie som použil pomôcku k auditu bezpečnostných opatrení poskytnutú NÚKIB. Jedná sa o vyhlášku č. 316/2014 Sb. Dokument, pomocou ktorého som robil asistované zhodnotenie bol príliš komplexný a niektoré časti sa na mnou vybranú spoločnosť nevzťahovali, preto boli vynechané a venoval som sa iba relevantným častiam.

### 2.14.1 ISMS

Tabuľka 1: Asistované zhodnotenie: ISMS (zdroj: vlastné spracovanie)

| | |
|---|---|
| Stanovený rozsah a hranice ISMS? | Neaplikované |
| Stanovená bezpečnostná politika ISMS | Neaplikované |
| Sú zavedené a schválené bezpečnostné politiky v oblasti ISMS, zavedené príslušné bezpečnostné opatrenia? | Neaplikované |
| Sú zavedené nasledujúce procesy?<br>-monitorovanie účinnosti bezpečnostných opatrení<br>- vyhodnotenie vhodnosti a účinnosti bezpečnostnej politiky<br>- audit kybernetickej bezpečnosti (aspoň 1x ročne)<br>- vyhodnotenie účinnosti ISMS | Neaplikované |
| Je vykonávaná aktualizácia ISMS a súvisiaca dokumentácia na základe zistených auditov a penetračných testov? | Neaplikované |
| Je riadená prevádzka a zdroje ISMS, zaznamenávané činnosti spojené s ISMS a súvisiacim riadením rizík? | Neaplikované |

Spoločnosť o systéme riadenia bezpečnosti informácií nemá vôbec žiadne povedomie a tým pádom nespĺňa žiadny z uvedených požiadaviek.

### 2.14.2 Riadenie aktív

Tabuľka 2: Asistované zhodnotenie: Riadenie aktív (zdroj: vlastné spracovanie)

| | |
|---|---|
| Sú identifikované a evidované aktíva? | Aplikované |
| Je stanovená bezpečnostná politika pre klasifikáciu aktív? | Neaplikované |
| Je stanovený vlastník aktíva – osoba zodpovedná za stav daného aktíva? | Čiastočne aplikované |
| Sú aktíva hodnotené z hľadiska dostupnosti, dôvernosti a integrity? | Čiastočne aplikované |
| Pri hodnotení dôležitosti aktív je predovšetkým posudzované:<br>- rozsah a dôležitosť osobných údajov<br>- rozsah určených právnych povinností<br>- rozsah narušenia vnútorných riadiacich a kontrolných činností<br>- poškodenie verejných, obchodných alebo ekonomických záujmov<br>- možné finančné straty<br>- dopady s narušením dôvernosti, integrity, dostupnosti<br>- dopady na zachovanie dobrého mena spoločnosti | Neaplikované |
| Sú stanovené pravidlá ochrany, nutné pre zabezpečenie jednotlivých úrovní aktív s tým, že:<br>- sú určené spôsoby rozlišovania jednotlivých úrovní aktív<br>- sú stanovené pravidlá pre manipuláciu a evidenciu s aktívami podľa úrovni aktív, vrátane pravidiel pre bezpečné elektronické zdieľanie a fyzické prenášanie aktív<br>- sú stanovené prípustné spôsoby používania aktív<br>- sú zavedené pravidlá ochrany odpovedajúcich aktív<br>- sú určené spôsoby pre spoľahlivé mazanie alebo ničenie technických nosičov dát s ohľadom na úroveň aktív | Čiastočne aplikované |

Pri tejto časti som zistil, že spoločnosť si pravidelne svoje aktíva zaznamenáva a pravidelne ich identifikuje, ale čo sa evidencie týka tak ich nečlení na hlavné a podporné aktíva. Bezpečnostnú politiku pre klasifikáciu aktív spoločnosť stanovenú nemá. Väčšina aktív má prideleného vlastníka, ale len u veľmi málo z nich je definované do akej miery môže vlastník s aktívom manipulovať a aké mu z toho vyplývajú povinnosti. Medzery v tejto oblasti má spoločnosť aj v samotnej dokumentácií, ktorá nie je úplne kompletná. Čo sa týka bezpečnej práce a manipulácie s aktívami, pracovníci firmy musia na začiatku absolvovať interné školenia ohľadom manipulácie s aktívami a bezpečného zdieľania a fyzického prenášania aktív. Taktiež boli poučení o prípustnom spôsobe používania aktív ale spoločnosť nemá pevne stanovené pravidlá ochrany aktív.

### 2.14.3 Riadenie rizík

Tabuľka 3: Asistované zhodnotenie: Riadenie rizík (zdroj: vlastné spracovanie)

| | |
|---|---|
| Je zavedený proces identifikácie a riadenia rizík? | Neaplikované |
| Sú stanovené metodiky pre identifikáciu a hodnotenie rizík vrátane stanovení kritérií pre ich prijateľnosť? | Neaplikované |
| Ak sú riziká ohodnotené je spracované prehlásenie o aplikovateľnosti, ktoré obsahuje prehľad zavedených bezpečnostných opatrení? | Neaplikované |
| Je spracovaný plán a zavedený plán zvládania rizík, ktorý obsahuje:<br>- ciele a prínosy bezpečnostných opatrení<br>-určenie zodpovednej osoby za ich presadenie<br>- zdroje(finančné, informačné, ľudské, technické)<br>- termín zavedenia a popis väzieb medzi rizikom a bezpečnostným opatrením | Neaplikované |
| Sú zvážené hrozby, súvisiace s:<br>- porušením bezpečnostnej politiky, prevedením neoprávnených činností, zneužitím oprávnenia zo strany užívateľov a administrátorov<br>- poškodením/zlyhaním technického/programového vybavenia<br>- zneužitím identity fyzickej osoby<br>- škodlivým kódom<br>- narušením fyzickej bezpečnosti<br>- zneužitím alebo neoprávnenou modifikáciou údajov<br>- trvalo pôsobiacimi hrozbami<br>- odcudzením alebo poškodením aktíva | Čiastočne aplikované |
| Sú zvážené zraniteľnosti, súvisiace s:<br>- nedostatočnou ochranou vonkajšieho perimetra<br>- nedostatočným bezpečnostným povedomím užívateľov a administrátorov<br>- nevhodným nastavením prístupových oprávnení<br>- nedostatočnými postupmi pri identifikovaní a odhalení negatívnych bezpečnostných javov, kybernetických bezpečnostných udalostí/incidentov<br>- nedostatočným monitorovaním činností užívateľov a administrátorov a neschopnosťou odhaliť ich nevhodné, alebo závadné spôsoby správania | Čiastočne aplikované |

Spoločnosť nemá oficiálne stanovený proces ani metodiky pre identifikáciu, riadenie a hodnotenie rizík. Plán zvládania spoločnosť vypracovaný nemá. Čo sa týka hrozieb a zraniteľností spoločnosť už nejaké opatrenia vykonáva. Hlavne v oblasti bezpečnosti ľudských zdrojov, riadenia prístupu a bezpečného správania užívateľov, fyzickej bezpečnosti, bezpečnosti pred škodlivým kódom a overovania identity užívateľov.

### 2.14.4 Bezpečnosť ľudských zdrojov

Tabuľka 4: Asistované zhodnotenie: Bezpečnosť ľudských zdrojov (zdroj: vlastné spracovanie)

| | |
|---|---|
| Je stanovená bezpečnostná politika pre bezpečnosť ľudských zdrojov? | Aplikované |
| Je stanovená bezpečnostná politika pre bezpečné správanie užívateľov? | Aplikované |
| Je stanovený plán bezpečnostného povedomia a v súlade s ním je zaistené poučenie užívateľov, administrátorov a osôb zastávajúcich bezpečnostné role o ich povinnostiach a o bezpečnostnej politike formou vstupných a pravidelných školení? | Čiastočne aplikované |
| Je zabezpečená kontrola dodržiavania bezpečnostnej politiky zo strany užívateľov, administrátorov a osôb zastávajúcich bezpečnostné role? | Neaplikované |
| Je zaistené vrátenie zverených aktív a odobratie prístupových oprávnení pri ukončení zmluvného vzťahu zamestnávateľa so zamestnancom? | Čiastočne aplikované |
| Sú o školeniach vedené prehľady, ktoré obsahujú predmet školenia a zoznam osôb, ktoré školenie absolvovali? | Aplikované |
| Sú stanovené pravidlá pre určenie zodpovedných osôb, ktoré budú zastávať bezpečnostné role, role administrátorov alebo užívateľov? | Aplikované |
| Je hodnotená účinnosť plánu rozvoja bezpečnostného povedomia, vykonaných školení a ďalších činností spojených s prehlbovaním znalostí o bezpečnostnom povedomí? | Neaplikované |
| Sú určené pravidlá a postupy pre riešenie prípadov porušenia stanovených bezpečnostných pravidiel zo strany užívateľov, administrátorov a osôb zastávajúcich bezpečnostné role? | Čiastočne aplikované |
| Je zaistená zmena prístupových oprávnení pri zmene postavenia užívateľov, administrátorov alebo osôb zastávajúcich bezpečnostné role? | Čiastočne aplikované |

Zamestnanci spoločnosti boli na začiatku poučení o bezpečnosti a ochrane zdravia pri práci a sú v tejto oblasti pravidelne preškoľovaní. V spoločnosti je zaistené vrátenie zverených aktív, ale na odobranie prístupových oprávnení už tak veľký dôraz kladený nie je. Technik na to nie je dopredu upozornený a tak sa častokrát stáva, že sa v systéme nachádzajú staré užívateľské kontá, ktoré by tam už nemali byť. Bezpečnostné školenia sa v spoločnosti vykonávajú v nepravidelných intervaloch. V prípade, že dôjde k porušeniu bezpečnostných pravidiel zo strany zamestnancov, o ktorých boli vopred poučení zamestnávateľ im môže udeliť sankcie na základe pracovnej zmluvy.

### 2.14.5 Riadenie prevádzky a komunikácie

Tabuľka 5: Asistované zhodnotenie: Riadenie prevádzky a komunikácie (zdroj: vlastné spracovanie)

| | |
|---|---|
| Je stanovená bezpečnostná politika pre riadenie prevádzky a komunikácie? | Neaplikované |
| Je stanovená bezpečnostná politika pre bezpečnosť komunikačnej siete? | Neaplikované |
| Je stanovená bezpečnostná politika pre zálohovanie a obnovu dát? | Neaplikované |
| Je stanovená bezpečnostná politika pre riadenie technických zraniteľností? | Neaplikované |
| Je stanovená bezpečnostná politika pre bezpečné odovzdávanie a výmenu informácií? | Neaplikované |
| Je stanovená bezpečnostná politika pre poskytovanie a získanie licencií programového vybavenia a informácií? | Neaplikované |
| Je stanovená bezpečnostná politika pre dlhodobé ukladanie a archiváciu informácií? | Neaplikované |
| Je vykonávané pravidelné zálohovanie a overovanie použiteľnosti vykonaných záloh? | Čiastočne aplikované |
| Prevádzkové pravidlá a postupy orgánov a osôb obsahujú:<br>- práva a povinnosti osôb zastávajúcich bezpečnostné role, administrátorov a užívateľov<br>- postupy pre spustenie/ukončenie chodu systému, pre reštart alebo obnovenie chodu systému po zlyhaní a pre ošetrenie chybových stavov alebo mimoriadnych javov<br>- postupy pre sledovanie kybernetických bezpečnostných udalostí a pre ochranu prístupu k záznamom o týchto činnostiach<br>- kontakt na zodpovedné osoby, ktoré sú určené ako podpora pri riešení neočakávaných systémových alebo technických problémov<br>- postupy riadenia a schvaľovania prevádzkových zmien<br>- postupy pre sledovanie, plánovanie a riadenie kapacity ľudských a technických zdrojov. | Čiastočne aplikované |
| Je zaistená bezpečnosť a integrita komunikačných sietí a bezpečnosť komunikačných služieb podľa nástroja pre ochranu integrity komunikačných sietí? | Neaplikované |
| Sú určené pravidlá a postupy pre ochranu informácií, ktoré sú prenášané komunikačnými sieťami? | Neaplikované |

Vyššie uvedené politiky nie sú oficiálne definované ale dané problémy, ktoré popisujú, už vo firme riešené sú akurát im chýba oficiálna podoba v podobe dokumentov. Vo firme je riešený systém zálohovania dát, ktorý prebieha v pravidelných intervaloch, ale overovanie použiteľnosti záloh je nepravidelne vykonávané vo veľmi veľkých časových úsekoch.

### 2.14.6 Riadenie prístupu a bezpečné chovanie užívateľov

Tabuľka 6: Asistované zhodnotenie: Riadenie prístupu a bezpečné chovanie užívateľov (zdroj: vlastné spracovanie)

| | |
|---|---|
| Je stanovená bezpečnostná politika pre riadenie prístupu? | Čiastočne aplikované |
| Je stanovená bezpečnostná politika pre bezpečné používanie mobilných zariadení? | Neaplikované |
| Má každý užívateľ svoje vlastné autentizačné údaje? | Aplikované |
| Je obmedzené prideľovanie administrátorských oprávnení? | Aplikované |
| Je prideľovanie a odoberanie prístupových oprávnení vykonávané v súlade s politikov riadenia prístupu? | Čiastočne aplikované |
| Je vykonávané pravidelné preskúmavanie nastavení prístupových oprávnení vrátane rozdelenia jednotlivých užívateľov v prístupových skupinách alebo rolách? | Neaplikované |
| Je využívaný nástroj pre riadenie prístupových oprávnení? | Neaplikované |
| Sú zavedené bezpečnostné opatrenia potrebné pre bezpečné používanie mobilných zariadení? | Neaplikované |

Každý zamestnanec v spoločnosti má svoje vlastné autentizačné údaje k pracovnej stanici ale ako som sa dozvedel od technika, heslá pre bežného užívateľa sú takmer autentické, čo predstavuje obrovské bezpečnostné riziko, v prípade, že sa potenciálnemu útočníkovi heslo podarí získať. Jediný rozdiel v heslách je posledná číslica, ktorá označuje číslo pracovnej stanice. Administrátorské oprávnenia má len konateľ firmy a zodpovedný technik, ktorý na všetko dohliada.

### 2.14.7 Riadenie kontinuity činnosti

Tabuľka 7: Asistované zhodnotenie: Riadenie kontinuity činností (zdroj: vlastné spracovanie)

| | |
|---|---|
| Sú stanovené ciele a stratégia riadenia kontinuity činností formou určenia:<br>- minimálnych úrovní poskytovaných služieb informačného a komunikačného systému?<br>- doby obnovenia chodu, počas ktorého bude po kybernetickom bezpečnostnom incidente obnovená minimálna úroveň poskytovaných služieb informačného a komunikačného systému?<br>- doby obnovenia dát po kybernetickom bezpečnostnom incidente | Neaplikované |
| Sú vyhodnocované a dokumentované možné dopady bezpečnostných incidentov a posúdené riziká súvisiace s ohrozením kontinuity činnosti? | Neaplikované |
| Sú stanovené, aktualizované a pravidelne testované plány kontinuity činností informačného a komunikačného systému? | Neaplikované |
| Sú realizované opatrenia pre zvýšenie odolnosti informačného a komunikačného systému voči bezpečnostnému incidentu? | Čiastočne aplikované |
| Sú stanovené a aktualizované postupy na prevedenie bezpečnostných opatrení? | Neaplikované |

Z vyššie uvedených opatrení je akurát riešené zvýšenie odolnosti informačného a komunikačného systému vďaka UPS záložným zdrojom, firewallu a antivírového programu.

### 2.14.8 Fyzická bezpečnosť

Tabuľka 8: Asistované zhodnotenie: Fyzická bezpečnosť (zdroj: vlastné spracovanie)

| | |
|---|---|
| Je definovaná bezpečnostná politika pre fyzickú bezpečnosť? | Aplikované |
| Sú prijaté opatrenia k zamedzeniu neoprávneného vstupu do vymedzených priestorov, kde sú spracovávané informácie a umiestnené technické aktíva informačného a komunikačného systému? | Aplikované |
| Sú prijaté opatrenia k zamedzeniu poškodenia a zásahom do vymedzených priestorov, kde sú uchovávané informácie a umiestnené technické aktíva informačného a komunikačného systému? | Aplikované |
| Je predchádzané poškodeniu, krádeži alebo kompromitácií aktív alebo prerušenia poskytovania služieb informačného alebo komunikačného systému? | Aplikované |
| Sú uplatnené prostriedky fyzickej bezpečnosti pre zaistenie ochrany na úrovni objektov? | Aplikované |
| Sú uplatnené prostriedky fyzickej bezpečnosti pre zaistenie ochrany v rámci objektov zaistením zvýšenej bezpečnosti vymedzených priestorov, v ktorých sú umiestnené technické aktíva informačného a komunikačného systému? | Aplikované |

Fyzickú bezpečnosť má spoločnosť zvládnutú dokonale. Celý objekt je oplotený a vstup do objektu je zabezpečený posuvnou bránou na diaľkové ovládanie. Objekt je navyše monitorovaný IP kamerami. Vnútro objektu je zabezpečené alarmom, uzamykateľnými miestnosťami a obmedzením prístupu do častí ako je napríklad serverovňa.

### 2.14.9 Overenie identity užívateľov

Tabuľka 9: Asistované zhodnotenie: Overenie identity užívateľov (zdroj: vlastné spracovanie)

| | |
|---|---|
| Sú používané nástroje pre overenie identity užívateľov, administrátorov informačného a komunikačného systému? | Aplikované |
| Nástroj pre overovanie identity užívateľov zaisťuje:<br>- minimálnu dĺžku hesla 8 znakov?<br>- minimálne jedno veľké a malé písmeno, číslicu a špeciálny znak?<br>- dobu kedy platnosť hesla expiruje, ktorá nepresahuje 100 dní? | Čiastočne aplikované |
| Je používaný nástroj pre overenie identity, ktorý:<br>- zamedzuje opätovnému používaniu hesiel a neumožní viac ako jednu zmenu hesla jedného užívateľa v priebehu 24 hodín?<br>- vykonáva opätovné overenie identity po určenej dobe nečinnosti?<br>- zaisťuje, že minimálna dĺžka hesla administrátorov je 15 znakov? | Čiastočne aplikované |

Spoločnosť používa nástroj pre overenie všetkých užívateľov v podobe mena a hesla. Na heslo sú kladené špecifické požiadavky v podobe dĺžky hesla, malých a veľkých písmen a špeciálnych znakov a u administrátorov sú tieto kritéria ešte väčšie. Problém však je v expirácií hesla, ktoré nemá stanovenú dobu expirácie. Taktiež nie je ošetrené opätovné používanie hesiel a overenie identity v prípade veľmi dlhej doby nečinnosti.

### 2.14.10 Riadenie prístupových oprávnení

Tabuľka 10: Asistované zhodnotenie: Riadenie prístupových oprávnení (zdroj: vlastné spracovanie)

| | |
|---|---|
| Je používaný nástroj, ktorý zaisťuje riadenie prístupových oprávnení:<br>- pre prístup k jednotlivým dátam a aplikáciám?<br>- pre čítanie, zápis a zmenu oprávnení dát? | Čiastočne aplikované |
| Je zaistené logovanie zmeny prístupových oprávnení? | Neaplikované |

Pre riadenie prístupových oprávnení k jednotlivým aplikáciám a dátam má na starosti IT technik. Logovanie zmeny prístupových oprávnení nastavené nie je.

### 2.14.11 Ochrana pred škodlivým kódom

Tabuľka 11: Asistované zhodnotenie: Ochrana pred škodlivým kódom (zdroj: vlastné spracovanie)

| | |
|---|---|
| Je používaný nástroj pre ochranu informačného a komunikačného systému pred škodlivým kódom, ktorý zaistí overenie a stálu kontrolu:<br>- komunikácie medzi vnútornými a vonkajšími sieťami?<br>- serverov a zdieľaných dátových úložísk?<br>- pracovných staníc? | Aplikované |
| Je vykonávaná pravidelná aktualizácia nástoja pre ochranu pred škodlivým kódom, jeho definícií a signatúr? | Aplikované |

Spoločnosť používa antivírový program od spoločnosti ESET. Ktorý zaisťuje kontrolu nad bodmi spomenutými vyššie. Taktiež dbá na platnosť licencie a na to, aby bol antivírový program pravidelne aktualizovaný.

### 2.14.12 Zaznamenávanie činností

Tabuľka 12: Asistované zhodnotenie: Zaznamenávanie činností (zdroj: vlastné spracovanie)

| | |
|---|---|
| Je používaný nástroj pre zaznamenávanie činností informačného a komunikačného systému, ktorý zaisťuje:<br>- zber informácií o prevádzkových a bezpečnostných činnostiach?<br>- ochranu získaných informácií pred neoprávneným čítaním a zmenou? | Neaplikované |
| Pomocou nástroja pre zaznamenávanie činností informačného a komunikačného systému je zaznamenávané:<br>- prihlásenie a odhlásenie užívateľov a administrátorov?<br>- činnosti vykonané administrátormi?<br>- činnosti vedúce k zmene prístupových oprávnení?<br>- zahájenie a ukončenie činností technických aktív?<br>- automatické varovné alebo chybové hlásenia technických aktív?<br>- prístupy záznamov o činnostiach, pokusy o ich manipuláciu?<br>- použitie mechanizmov identifikácie a autentizácie vrátane zmeny údajov? | Neaplikované |
| Sú záznamy činností uvedených vyššie uchovávané minimálne 3 mesiace? | Neaplikované |
| Minimálne raz za 24 hodín je vykonávaná synchronizácia jednotného systémového času technických aktív patriacich do informačného a komunikačného systému? | Neaplikované |

Spoločnosť nepoužíva nástroj pre zaznamenávanie činnosti informačného a komunikačného systému.

### 2.14.13 Detekcia kybernetických bezpečnostných udalostí

Tabuľka 13: Asistované zhodnotenie: Detekcia kybernetických bezpečnostných udalostí (zdroj: vlastné spracovanie)

| | |
|---|---|
| Je používaný nástroj pre detekciu kybernetických bezpečnostných udalostí, ktorý zaistí overenie, kontrolu a prípadné zablokovanie komunikácie:<br>- medzi vnútornými a vonkajšími sieťami?<br>- v rámci vnútornej komunikačnej siete?<br>- serverov patriacich do informačného a komunikačného systému? | Čiastočne aplikované |

### 2.14.14 Aplikačná bezpečnosť

Tabuľka 14: Asistované zhodnotenie: Aplikačná bezpečnosť (zdroj: vlastné spracovanie)

| | |
|---|---|
| Sú vykonávané bezpečnostné testy zraniteľností aplikácií, ktoré sú prístupné z vonkajšej siete? | Neaplikované |
| Je zaistená stála ochrana aplikácií, informácií dostupných z vonkajšej siete? | Aplikované |
| Je zaistená stála ochrana transakcií? | Čiastočne aplikované |

### 2.14.15 Kryptografické prostriedky

Tabuľka 15: Asistované zhodnotenie: Kryptografické prostriedky (zdroj: vlastné spracovanie)

| | |
|---|---|
| Pre používanie kryptografickej ochrany je alebo sú stanovené:<br>- úroveň ochrany s ohľadom na typ a silu kryptografického algoritmu?<br>- pravidlá kryptografickej ochrany informácií pri prenose po komunikačných sietí alebo uloženie na technické nosiče dát? | Aplikované |
| Sú používané kryptografické prostriedky, ktoré zaistia ochranu dôvernosti a integrity predávaných alebo ukladaných dát a preukázanie zodpovednosti za vykonané činnosti? | Čiastočne aplikované |
| Je stanovaný systém správy kľúčov, ktorý zaistí generovanie, distribúciu, ukladanie, archiváciu, zmenu, zničenie, kontrolu a audit kľúčov? | Neaplikované |

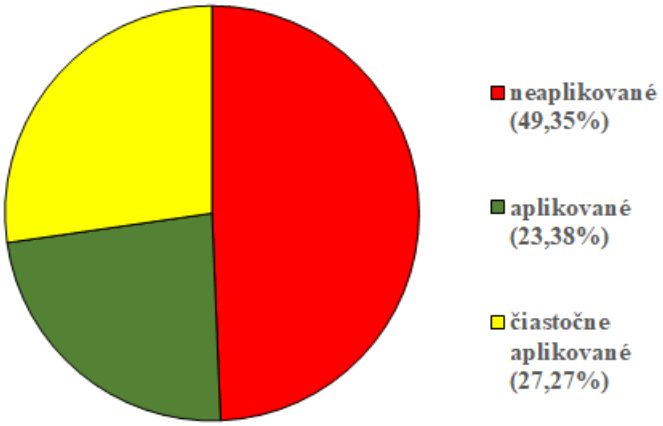
### 2.14.16 Zaistenie úrovne dostupnosti

Tabuľka 16: Asistované zhodnotenie: Zaistenie úrovne dostupnosti (zdroj: vlastné spracovanie)

| | |
|---|---|
| Je používaný nástroj pre úrovne dostupnosti informácií, ktorý zaisťuje:<br>- dostupnosť informačného a komunikačného systému?<br>- odolnosť informačného a komunikačného systému voči kybernetickým bezpečnostným incidentom, ktoré by mohli znížiť dostupnosť?<br>- zálohovanie dôležitých technických aktív informačného a komunikačného systému za:<br>1. využitím redundancie v návrhu riešenia<br>2. zaistením náhradných technických aktív v určenom čase | Čiastočne aplikované |

## 2.15 Súhrnné zhrnutie asistovaného zhodnotenia

Pre lepšiu orientáciu súčasného stavu bezpečnostných opatrení v spoločnosti som zhrnul výsledky jednotlivých častí asistovaného zhodnotenia do koláčového grafu, ktorý reprezentuje manažérsky výstup asistovaného zhodnotenia.




Obrázok 13: Výstup asistovaného zhodnotenia (zdroj: vlastné spracovanie)

# 3 VLASTNÝ NÁVRH RIEŠENIA

Táto časť práce je venovaná vlastnému návrhu riešenia, ktorý obsahuje analýzu rizík, návrh bezpečnostných opatrení, časový plán implementácie a ekonomické zhodnotenie navrhnutých bezpečnostných opatrení.

## 3.1 Rozsah a hranice ISMS

Táto kapitola definuje v akom rozsahu bude ISMS riešené. Cieľom tejto práce nie je pokryť celý rozsah. Vzhľadom na finančné možnosti a veľkosť organizácie by to ani nebolo možné. Preto zvolím druhý spôsob spomenutý v teoretickej časti, v ktorom sa zameriam len na určité časti a to predovšetkým na tie, ktoré boli z pohľadu asistovaného zhodnotenia najkritickejšie.

## 3.2 Analýza rizík

Analýza rizík je dôležitou časťou pri návrhu bezpečnostnej politiky riadenia rizík. Je vykonaná za účelom identifikácie zraniteľných miest spoločnosti a slúži ako podklad pre návrh bezpečnostných opatrení. Ako prvé som identifikoval a ohodnotil aktíva danej spoločnosti. Po nich nasleduje vypracovanie zoznamu hrozieb a zraniteľností. Finálna časť analýzy pozostáva zo spracovania matice zraniteľností a rizík vďaka čomu budem vedieť aké bezpečnostné opatrenia budem musieť navrhnúť aby sa znížila celková úroveň rizika v spoločnosti.

### 3.2.1 Identifikácia a ohodnotenie aktív

Prvým krokom k úspešnej analýze rizík patrí identifikácia aktív a ich následné ohodnotenie. Aktíva som rozčlenil do 4 skupín podľa ich typu: dáta, hardware, software a služby. Hodnotu každého identifikovaného aktíva som vypočítal na základe dôsledkov porušenia niektorého z atribútov CIA triády čiže dôvernosti, integrity a dostupnosti. Klasifikáciu aktív som rozdelil do 5 úrovní na základe normy ISO/IEC 27005 od menej dôležitých aktív, u ktorých poškodenie spôsobí minimálne následky až po tie najdôležitejšie, ktorých poškodenie môže ohroziť existenciu spoločnosti. Klasifikačné schéma aktív popisuje tabuľka číslo 17.

Tabuľka 17: Klasifikačné schéma pre hodnotenie aktív (zdroj: vlastné spracovanie)

| Klasifikačné kritérium | Klasifikačný stupeň |
|---|---|
| Žiadny dopad na spoločnosť | 1 |
| Zanedbateľný dobad na spoločnosť | 2 |
| Problémy alebo finančné straty | 3 |
| Vážne problémy alebo finančné straty | 4 |
| Existenčné problémy spoločnosti | 5 |

Na výpočet hodnoty aktíva som použil nasledujúci súčtový algoritmus.

$$\text{Hodnota aktíva} = \frac{(\text{Dôvernosť} + \text{Integrita} + \text{Dostupnosť})}{3}$$

Tabuľka 18: Zoznam aktív a ich celkovej hodnoty (zdroj: vlastné spracovanie)

| Typ | Aktívum (A) | Zdroj | C | I | A | H |
|---|---|---|---|---|---|---|
| Dáta | Dáta o zákazníkoch | Informačný systém, databáza, PC, notebook | 5 | 5 | 5 | 5 |
| | Dáta o zamestnancoch | Server | 5 | 5 | 5 | 5 |
| | Interné dáta | Server, PC, notebook | 4 | 5 | 5 | 5 |
| | Zálohy dát | Server, IP kamery, PC, notebook | 5 | 5 | 5 | 5 |
| Hardware | Server | | 5 | 5 | 5 | 5 |
| | PC | | 4 | 4 | 4 | 4 |
| | Notebook | | 4 | 4 | 4 | 4 |
| | Pasívne sieťové prvky | Kabeláž, zásuvky | 3 | 3 | 4 | 3 |
| | Aktívne sieťové prvky | Switch, router | 4 | 5 | 5 | 5 |
| | Firewall | | 5 | 5 | 5 | 5 |
| | NAS | | 5 | 5 | 5 | 5 |
| | NVR kamerový systém | | 2 | 5 | 3 | 3 |
| | Alarm | | 3 | 4 | 4 | 4 |
| Software | Operačný systém | Server, PC, notebook, mobil | 3 | 4 | 4 | 4 |
| | Softwér kamier | NVR kamerový systém | 2 | 3 | 2 | 2 |
| | Účtovný software | Server | 5 | 5 | 5 | 5 |
| | Databáza | Server | 5 | 5 | 5 | 5 |
| | Antivírový program | Server, PC, notebook | 3 | 4 | 5 | 4 |
| | FTP klient | Server, PC, notebook | 3 | 3 | 4 | 3 |
| | Informačný systém | Server | 5 | 5 | 5 | 5 |
| Služby | Internetové pripojenie | Sídlo spoločnosti | 4 | 4 | 5 | 4 |
| | Elektrická energia | Sídlo spoločnosti | 4 | 4 | 5 | 4 |
| | Doménové služby | Server | 2 | 3 | 3 | 3 |
| | Webové služby | Poskytovateľ | 2 | 3 | 3 | 3 |
| | Služba záloh | NAS | 4 | 5 | 4 | 4 |
| | Služba IP kamier | NVR kamerový systém | 2 | 3 | 2 | 2 |
| | FTP | Server | 3 | 4 | 4 | 4 |
| | DHCP | Server | 3 | 4 | 4 | 4 |
| | Team viewer | PC, notebook | 4 | 4 | 4 | 4 |

Z tabuľky číslo 18 môžeme vidieť všetky identifikované aktíva spoločnosti vrátane ich hodnoty a ktoré z nich sú kritické. Ohrozenie týchto aktív môže pre spoločnosť znamenať

existenčné problémy a preto je nutné zaviesť potrebné bezpečnostné opatrenia, aby sa eliminovali možné hrozby a ich dopad.

### 3.2.2 Identifikácia hrozieb a zraniteľností

V tejto časti sú identifikované potenciálne hrozby a zraniteľnosti, ktoré môžu hroziť aktívam spoločnosti. Je potrebné povedať, že na jedno aktívum môže súčasne pôsobiť viacero hrozieb a pre jednu konkrétnu hrozbu je možné uviesť viacero príkladov zraniteľnosti. Na základe všetkých identifikovaných aktív v spoločnosti som zistil nasledujúci zoznam hrozieb:

Tabuľka 19: Zoznam identifikovaných hrozieb (zdroj: vlastné spracovanie)

| Typ | Hrozba [T] |
|---|---|
| Fyzické poškodenie | Poškodenie vodou |
| | Vznik požiaru |
| | Poškodenie hrubou silou |
| | Znečistenie/prach |
| | Nadmerné prehrievanie zariadenia |
| | Korózia |
| | Mráz |
| | Blesk |
| Prírodná udalosť | Záplavy |
| | Zemetrasenie |
| Strata základných služieb | Prerušenie dodávky elektriny |
| | Zlyhanie telekomunikačných zariadení |
| | Výpadok internetového pripojenia |
| Ohrozenie informácií | Odpočúvanie |
| | Špionáž |
| | Krádež |
| | Prezradenie |
| | Modifikácia/Falšovanie |
| | Zmazanie |
| | Odhalenie pozície |
| Technické zlyhanie | Zlyhanie zariadenia |
| | Chybné fungovanie |
| | Nesprávna údržba |
| Neoprávnené činnosti | Neoprávnené použitie zariadenia |
| | Použitie neoficiálneho aplikačného vybavenia |
| | Neoprávnené získanie prístupových údajov |
| Ohrozenie funkčnosti | Nesprávna manipulácia |
| | Odoprenie činností |
| | Nedostatočný počet pracovníkov |

Tabuľku číslo 19 som upravil a k zoznamu hrozieb som pridal pravdepodobnosť jej vzniku a konkrétny príklad zraniteľnosti. Klasifikačné schéma pravdepodobnosti hrozieb je nasledovné:

Tabuľka 20: Klasifikačné schéma pre hodnotenie hrozieb (zdroj: vlastné spracovanie)

| Pravdepodobnosť hrozby | Klasifikačný stupeň |
|---|---|
| Veľmi nízka | 1 |
| Nízka | 2 |
| Stredná | 3 |
| Veľmi vysoká | 4 |
| Vysoká | 5 |

Tabuľka 21: Zoznam hrozieb vrátane ich pravdepodobnosti naplnenia a príkladom zraniteľnosti (zdroj: vlastné spracovanie)

| Hrozba [T] | P | Príklad zraniteľnosti |
|---|---|---|
| Poškodenie vodou | 2 | Zaobchádzanie s vodou |
| Vznik požiaru | 3 | Zaobchádzanie s horľavými látkami |
| Poškodenie hrubou silou | 1 | Ulomenie krehkých častí |
| Znečistenie/prach | 5 | Nánosy prachu na ventilátoroch |
| Nadmerné prehrievanie zariadenia | 5 | Nedostatočná cirkulácia vzduchu |
| Korózia | 1 | Nedostatočne odolný materiál voči korózií |
| Mráz | 1 | Slabá odolnosť káblových chráničiek voči mrazu |
| Blesk | 3 | Nechránené časti vodivých zariadení |
| Záplavy | 1 | Priestory v záplavovej oblasti |
| Zemetrasenie | 1 | Prírodná katastrofa |
| Prerušenie dodávky elektriny | 3 | Neplánovaná odstávka |
| Zlyhanie telekomunikačných zariadení | 3 | Rušenie komunikácie |
| Výpadok internetového pripojenia | 3 | Problém na strane poskytovateľa |
| Odpočúvanie | 3 | Nedostatočná ochrana sieťovej infraštruktúry |
| Špionáž | 1 | Nedostatočná ochrana sieťovej infraštruktúry |
| Krádež informácií | 3 | Nedostatočná ochrana priestorov |
| Prezradenie údajov | 2 | Nedostatočne vyškolený personál |
| Modifikácia/falšovanie informácií | 4 | Nedostatočná bezpečnosť pracovných staníc |
| Zmazanie informácií | 4 | Poškodené úložné médium |
| Odhalenie pozície citlivých informácií | 1 | Nevhodný spôsob a zabezpečenie údajov |
| Zlyhanie zariadenia | 3 | Používanie zariadenia napriek prekročeniu doby životnosti |
| Chybné fungovanie | 3 | Nesprávne nastavenie zariadenia |
| Nesprávna údržba | 4 | Nedostatočne vyškolený personál |
| Neoprávnené použitie zariadenia | 4 | Získanie prístupových údajov |
| Použitie neoficiálneho aplikačného vybavenia | 2 | Nedostatočne vyškolený personál |
| Neoprávnené získanie prístupových údajov | 3 | Slabé heslo |
| Nesprávna manipulácia | 4 | Nedostatočne vyškolený personál |
| Odoprenie činností | 4 | Nevhodné nastavenie |
| Nedostatočný počet pracovníkov | 3 | Chrípková epidémia |

### 3.2.3 Matica zraniteľnosti

Maticu zraniteľnosti som vytvoril spojením tabuľky aktív, hrozieb a zraniteľností a vďaka nej som dostal relevantné vstupné dáta pre zostavenie matice rizík. Predstavuje pravdepodobnosť

hrozby v závislosti na hodnote daného aktíva spoločnosti. Klasifikačné schéma zraniteľností je nasledovné:

Tabuľka 22: Klasifikačné schéma pre hodnotenie zraniteľností (zdroj: vlastné spracovanie)

| Zraniteľnosť | Klasifikačný stupeň |
|---|---|
| Veľmi nízka | 1 |
| Nízka | 2 |
| Stredná | 3 |
| Veľmi vysoká | 4 |
| Vysoká | 5 |

Tabuľka 23: Matica zraniteľností (zdroj: vlastné spracovanie)

| | | | Dáta | | | | Hardware | | | | | | | | | Software | | | | | | | | Služby | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Zraniteľnosť [V]** | | **Zdroj** | Informačný systém, databáza, PC, notebook | Server | Server, PC, notebook | Server, IP kamery, PC, notebook | | | | Kabeláž, zásuvky | Switch, router | | | | | Server, PC, notebook, mobil | NVR kamerový systém | Server | Server | Server, PC, notebook | Server, PC, notebook | Server | Sídlo spoločnosti | Sídlo spoločnosti | Server | Poskytovateľ | NAS | NVR kamerový systém | Server | Server | PC, notebook |
| | | **Aktívum** | Dáta o zákazníkoch | Dáta o zamestnancoch | Interné dáta | Zálohy dát | Server | PC | Notebook | Pasívne sieťové prvky | Aktívne sieťové prvky | Firewall | NAS | NVR kamerový systém | Alarm | Operačný systém | Softwér kamier | Účtovný software | Databáza | Antivírový program | FTP klient | Informačný systém | Internetové pripojenie | Elektrická energia | Doménové služby | Webové služby | Služba záloh | Služba IP kamier | FTP | DHCP | Team viewer |
| | | **A** | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 3 | 5 | 5 | 5 | 3 | 4 | 4 | 2 | 5 | 5 | 4 | 3 | 5 | 4 | 4 | 3 | 3 | 4 | 2 | 4 | 4 | 4 |
| **Hrozba** | **T** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Poškodenie vodou | 2 | | | | | | 3 | 3 | 2 | 1 | 3 | 3 | 3 | 1 | 2 | | | | | | | | 3 | 3 | | | | | | | |
| Vznik požiaru | 3 | | | | | | 3 | 3 | 2 | 2 | 3 | 3 | 3 | 2 | 2 | | | | | | | | 3 | 3 | | | | | | | |
| Poškodenie hrubou silou | 1 | | | | | | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | | | | | | | | 2 | 2 | | | | | | | |
| Znečistenie/prach | 5 | | | | | | 3 | 3 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | | | | | | | | | | | | | | | | |
| Nadmerné prehrievanie zariadenia | 5 | | | | | | 4 | 3 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | | | | | | | | | | | | | | | | |
| Korózia | 1 | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | | | | | | | | | | | | | | | |
| Mráz | 1 | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 2 | 2 | | | | | | | | | | | | | | | | |
| Blesk | 3 | | | | | | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | | | | | | | | | | | | | | | | |
| Záplavy | 1 | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | | | | | | | 1 | 1 | | | | | | | |
| Zemetrasenie | 1 | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | | | | | | | | | | | | | | | | |
| Prerušenie dodávky elektriny | 3 | | 4 | 4 | 4 | 3 | 5 | 4 | 3 | 1 | 4 | 4 | 3 | 2 | 2 | | | | | | | | 4 | 5 | 4 | 4 | 5 | 3 | 2 | 2 | |
| Zlyhanie telekomunikačných zariadení | 3 | | 4 | 4 | 4 | 3 | 5 | 3 | 3 | 3 | 5 | 4 | 4 | 3 | 3 | | | | | | | | 5 | | | | | | | | |
| Výpadok internetového pripojenia | 3 | | 2 | 2 | 2 | 2 | 5 | 3 | 3 | 3 | 5 | 4 | 3 | 3 | 3 | | | | | | | | | | | | | | | | |
| Odpočúvanie | 1 | | | | | | | | | | | | | | | | | | | | | | 4 | | 3 | 2 | 3 | 3 | | | 1 |
| Špionáž | 3 | | 5 | 5 | 5 | 3 | 5 | 3 | 3 | 1 | 4 | 3 | 4 | 3 | 2 | 1 | 3 | 4 | 4 | 3 | 2 | 4 | 4 | | 3 | 2 | 3 | 3 | | | 1 |
| Krádež | 2 | | 5 | 5 | 5 | 5 | 2 | 2 | 4 | 1 | 2 | 2 | 2 | 2 | 2 | | | | | | | | | | | | | | | | |
| Prezradenie | 4 | | 5 | 5 | 5 | 2 | | | | | | | | | | | | | | | | | | | | | | | | | |
| Modifikácia/Falšovanie | 4 | | 5 | 5 | 5 | 5 | | | | | | | | | | 5 | 3 | 5 | 5 | 4 | 4 | 5 | | | | | | | | | |
| Zmazanie | 1 | | 5 | 5 | 5 | 5 | | | | | | | | | | | | | | | | | | | | | | | | | |
| Odhalenie pozície | 4 | | 3 | 2 | 3 | 2 | 3 | 1 | 1 | 1 | 2 | 2 | 3 | 1 | 1 | | | | | | | | | | | | | | | | |
| Zlyhanie zariadenia | 3 | | | | | | 5 | 3 | 3 | 2 | 4 | 4 | 3 | 2 | 2 | | | | | | | | | | | | | | | | |
| Chybné fungovanie | 3 | | | | | | 4 | 2 | 2 | 1 | 3 | 3 | 2 | 2 | 2 | 4 | 2 | 4 | 4 | 3 | 2 | 4 | | | | | | | | | |
| Nesprávna údržba | 4 | | | | | | 3 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | | | | | | | | | | | | | | | | |
| Použitie neoficiálneho aplikačného vybaver | 2 | | | | | | | | | | | | | | | 5 | 3 | 5 | 5 | 4 | 3 | 5 | | | | | | | | | |
| Nesprávna manipulácia | 4 | | 5 | 5 | 5 | 5 | 4 | 3 | 3 | 1 | 4 | 4 | 4 | 3 | 3 | 4 | 2 | 4 | 4 | 3 | 2 | 4 | | | | | | | | | |
| Odoprenie činností | 4 | | | | | | 4 | 2 | 2 | 1 | 3 | 3 | 2 | 2 | 2 | | | | | | | | 4 | | 3 | 2 | 3 | 3 | | | 1 |
| Nedostatočný počet pracovníkov | 3 | | | | | | | | | | | | | | | | | 2 | 2 | | | 2 | | | | | | | | | |

### 3.2.4 Matica rizík

Matica rizík znázorňuje všetky riziká, ktoré spoločnosti hrozia. Mojím cieľom bude zamerať sa na tie najkritickejšie, ktoré by mali závažný dopad na fungovanie spoločnosti a navrhnúť bezpečnostné opatrenia, ktoré ich eliminujú alebo ich znížia na takú úroveň, ktorá bude pre spoločnosť prijateľná. Pre výpočet miery rizika **R** som použil trojparametrovú metódu. Parametre sú:

- **A** – Hodnota aktíva
- **T** – pravdepodobnosť hrozby
- **V** – zraniteľnosť aktíva

Mieru rizika som vypočítal nasledovne:

R = A * T * V

Keďže v matici mi najvyššia hodnota vyšla číslo 100 tak úroveň rizika je hodnotená pomocou schémy uvedeného v tabuľke číslo 24.

Tabuľka 24: Klasifikačné schéma pre hodnotenie rizík (zdroj: vlastné spracovanie)

| Klasifikačné kritérium | Klasifikačný stupeň |
|---|---|
| Bezvýznamné riziko | 0-10 |
| Akceptovateľné riziko | 11.20 |
| Mierne riziko | 21-30 |
| Nežiadúce riziko | 31-60 |
| Neprijateľné riziko | 61-100 |

Tabuľka 25: Matica rizík (zdroj: vlastné spracovanie)

| | | | Dáta | | | | Hardware | | | | | | | | | Software | | | | | | | | Služby | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Riziko [R]** | | **Zdroj** | Informačný systém, databáza, PC, notebook | Server | Server, PC, notebook | Server, IP kamery, PC, notebook | | | | Kabeláž, zásuvky | Switch, router | | | | | Server, PC, notebook, mobil | NVR kamerový systém | Server | Server | Server, PC, notebook | Server, PC, notebook | Server | Sídlo spoločnosti | Sídlo spoločnosti | Server | Poskytovateľ | NAS | NVR kamerový systém | Server | FTP | Server | PC, notebook |
| | | **Aktívum** | Dáta o zákazníkoch | Dáta o zamestnancoch | Interné dáta | Zálohy dát | Server | PC | Notebook | Pasívne sieťové prvky | Aktívne sieťové prvky | Firewall | NAS | NVR kamerový systém | Alarm | Operačný systém | Softvér kamier | Účtovný software | Databáza | Antivírový program | FTP klient | Informačný systém | Internetové pripojenie | Elektrická energia | Doménové služby | Webové služby | Služba záloh | Služba IP kamier | FTP | DHCP | Team viewer | |
| | | **A** | 5 | 5 | 5 | 5 | 5 | 4 | 4 | 3 | 5 | 5 | 5 | 3 | 4 | 4 | 2 | 5 | 5 | 4 | 3 | 5 | 4 | 4 | 3 | 3 | 4 | 2 | 4 | 4 | 4 | |
| **Hrozba** | **T** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Poškodenie vodou | 2 | | | | | | 30 | 30 | 16 | 6 | 30 | 30 | 30 | 6 | 16 | | | | | | | | 24 | 24 | | | | | | | | |
| Vznik požiaru | 3 | | | | | | 45 | 36 | 24 | 18 | 45 | 45 | 45 | 18 | 24 | | | | | | | | 24 | 24 | | | | | | | | |
| Poškodenie hrubou silou | 1 | | | | | | 10 | 8 | 8 | 6 | 10 | 10 | 10 | 6 | 8 | | | | | | | | 8 | 8 | | | | | | | | |
| Znečistenie/prach | 5 | | | | | | 75 | 60 | 60 | 30 | 50 | 50 | 50 | 30 | 40 | | | | | | | | | | | | | | | | | |
| Nadmerné prehrievanie zariadenia | 5 | | | | | | 100 | 60 | 60 | 30 | 50 | 50 | 50 | 30 | 40 | | | | | | | | | | | | | | | | | |
| Korózia | 1 | | | | | | 5 | 4 | 4 | 3 | 5 | 5 | 5 | 3 | 4 | | | | | | | | | | | | | | | | | |
| Mráz | 1 | | | | | | 5 | 4 | 4 | 3 | 5 | 5 | 5 | 6 | 8 | | | | | | | | | | | | | | | | | |
| Blesk | 3 | | | | | | 30 | 24 | 24 | 18 | 30 | 30 | 30 | 18 | 24 | | | | | | | | | | | | | | | | | |
| Záplavy | 1 | | | | | | 5 | 4 | 4 | 3 | 5 | 5 | 5 | 3 | 4 | | | | | | | | 4 | 4 | | | | | | | | |
| Zemetrasenie | 1 | | | | | | 5 | 4 | 4 | 3 | 5 | 5 | 5 | 3 | 4 | | | | | | | | | | | | | | | | | |
| Prerušenie dodávky elektriny | 3 | | 60 | 60 | 60 | 45 | 75 | 48 | 36 | 9 | 60 | 60 | 45 | 18 | 24 | | | | | | | | 48 | 60 | 36 | 36 | 60 | 18 | 24 | 24 | | |
| Zlyhanie telekomunikačných zariadení | 3 | | 60 | 60 | 60 | 45 | 75 | 36 | 36 | 36 | 75 | 60 | 60 | 27 | 36 | | | | | | | | 60 | | | | | | | | | |
| Výpadok internetového pripojenia | 3 | | 30 | 30 | 30 | 30 | 75 | 36 | 36 | 27 | 75 | 60 | 45 | 27 | 36 | | | | | | | | | | | | | | | | | |
| Odpočúvanie | 1 | | | | | | | | | | | | | | | | | | | | | | 16 | | 9 | 6 | 9 | 6 | | | 4 | |
| Špionáž | 3 | | 75 | 75 | 75 | 75 | 75 | 36 | 36 | 9 | 60 | 45 | 60 | 27 | 24 | 12 | 18 | 60 | 60 | 36 | 18 | 60 | 48 | | 27 | 18 | 36 | 18 | | | 12 | |
| Krádež | 2 | | 50 | 40 | 50 | 50 | 20 | 16 | 32 | 12 | 20 | 20 | 20 | 12 | 16 | | | | | | | | | | | | | | | | | |
| Prezradenie | 4 | | 100 | 100 | 100 | 40 | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Modifikácia/Falšovanie | 4 | | 100 | 100 | 100 | 100 | | | | | | | | | | 80 | 24 | 100 | 100 | 64 | 64 | 100 | | | | | | | | | | |
| Zmazanie | 1 | | 25 | 25 | 25 | 25 | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Odhalenie pozície | 4 | | 60 | 40 | 60 | 40 | 60 | 16 | 16 | 12 | 40 | 40 | 45 | 12 | 16 | | | | | | | | | | | | | | | | | |
| Zlyhanie zariadenia | 3 | | | | | | 75 | 36 | 36 | 18 | 60 | 60 | 45 | 18 | 24 | | | | | | | | | | | | | | | | | |
| Chybné fungovanie | 3 | | | | | | 60 | 24 | 24 | 9 | 45 | 45 | 30 | 18 | 24 | 48 | 12 | 60 | 60 | 36 | 18 | 60 | | | | | | | | | | |
| Nesprávna údržba | 4 | | | | | | 60 | 32 | 32 | 24 | 40 | 40 | 60 | 24 | 32 | | | | | | | | | | | | | | | | | |
| Použitie neoficiálneho aplikačného vybaver | 2 | | | | | | | | | | | | | | | 40 | 12 | 50 | 50 | 32 | 18 | 50 | | | | | | | | | | |
| Nesprávna manipulácia | 4 | | 100 | 100 | 100 | 100 | 80 | 48 | 48 | 12 | 80 | 80 | 80 | 36 | 48 | 64 | 16 | 80 | 80 | 48 | 24 | 80 | | | | | | | | | | |
| Odoprenie činností | 4 | | | | | | 80 | 32 | 32 | 12 | 60 | 60 | 40 | 24 | 32 | | | | | | | | 64 | | 36 | 24 | 48 | 24 | | | 16 | |
| Nedostatočný počet pracovníkov | 3 | | | | | | | | | | | | | | | | | 30 | 30 | | | 30 | | | | | | | | | | |

### 3.2.5 Zhodnotenie analýzy rizík

Z matice rizík môžeme vidieť výstup, vďaka ktorému môžeme vidieť zoznam všetkých rizík vrátane toho, ktoré z nich majú najväčší dopad na spoločnosť. V tabuľke číslo 26 je zoznam všetkých neprijateľných rizík.

Tabuľka 26: Zoznam neprijateľných rizík (zdroj: vlastné spracovanie)

| Hrozba | Úroveň rizika | Aktívum | Zdroj |
|---|---|---|---|
| Znečistenie/prach | 75 | Server | |
| Nadmerné prehrievanie zariadenia | 100 | Server | |
| Prerušenie dodávky elektriny | 75 | Server | |
| Zlyhanie telekomunikačných zariadení | 75 | Server | |
| Výpadok internetového pripojenia | 75 | Server | |
| Špionáž | 75 | Dáta o zákazníkoch | Informačný systém, databáza, PC, notebook |
| | 75 | Dáta o zamestnancoch | Server |
| | 75 | Interné dáta | Server, PC, notebook |
| | 75 | Zálohy dát | Server, IP kamery, PC, notebook |
| | 75 | Server | |
| Prezradenie | 100 | Dáta o zákazníkoch | Informačný systém, databáza, PC, notebook |
| | 100 | Dáta o zamestnancoch | Server |
| | 100 | Interné dáta | Server, PC, notebook |
| Modifikácia/Falšovanie | 100 | Dáta o zákazníkoch | Informačný systém, databáza, PC, notebook |
| | 100 | Dáta o zamestnancoch | Server |
| | 100 | Interné dáta | Server, PC, notebook |
| | 100 | Zálohy dát | Server, IP kamery, PC, notebook |
| | 80 | Operačný systém | Server, PC, notebook, mobil |
| | 100 | Účtovný software | Server |
| | 100 | Databáza | Server |
| | 64 | Antivírový program | Server, PC, notebook |
| | 100 | Informačný systém | Server |
| Zlyhanie zariadenia | 75 | Server | |
| Nesprávna manipulácia | 100 | Dáta o zákazníkoch | Informačný systém, databáza, PC, notebook |
| | 100 | Dáta o zamestnancoch | Server |
| | 100 | Interné dáta | Server, PC, notebook |
| | 100 | Zálohy dát | Server, IP kamery, PC, notebook |
| | 80 | Server | |
| | 80 | Aktívne sieťové prvky | Switch, router |
| | 80 | Firewall | |
| | 80 | NAS | |
| | 64 | Operačný systém | Server, PC, notebook, mobil |
| | 80 | Účtovný software | Server |
| | 80 | Databáza | Server |
| | 80 | Informačný systém | Server |
| Odoprenie činností | 80 | Server | |

Ako je možné vidieť z tabuľky väčšina neprijateľných rizík sa týkajú hlavne serveru a dát. Je to logické, keďže server poskytuje väčšinu služieb, ktoré sú potrebné k činnosti spoločnosti a jeho poškodenie by malo katastrofálne dopady na spoločnosť. V prípade dát sa jedná hlavne o hrozby, kedy môže dôjsť k vyzradeniu údajov tretej strane alebo ich modifikácia. V obidvoch prípadoch môžu mať následky týchto hrozieb kritický dopad na spoločnosť. Ostatné hrozby týkajúce sa hlavne modifikácie alebo nesprávnej manipulácie s aktívom, čo

môže ohroziť činnosť viacerých aktív spoločnosti. Neprijateľné riziká sú také, ktoré môžu vážne ohroziť pôsobenie spoločnosti a je preto zaviesť také príslušné bezpečnostné opatrenia, ktoré úroveň rizika znížia na prijateľnú úroveň.

Taktiež je potrebné zmieniť nežiadúce riziká, ktoré delilo od toho, aby sa stali neprijateľným rizikom, len jeden bod. Týmto rizikám je nutné venovať pozornosť a taktiež navrhnúť bezpečnostné opatrenia, ktoré znížia ich úroveň. Zoznam týchto rizík je možné vidieť v tabuľke číslo 27.

Tabuľka 27: Zoznam nežiadúcich hrozieb s úrovňou rizika 60 (zdroj: vlastné spracovanie)

| Hrozba | Úroveň rizika | Aktívum | Zdroj |
|---|---|---|---|
| Znečistenie/prach | 60 | PC | |
| | 60 | Notebook | |
| Nadmerné prehrievanie zariadenia | 60 | PC | |
| | 60 | Notebook | |
| Prerušenie dodávky elektriny | 60 | Dáta o zákazníkoch | Informačný systém, databáza, PC, notebook |
| | 60 | Dáta o zamestnancoch | Server |
| | 60 | Interné dáta | Server, PC, notebook |
| | 60 | Aktívne sieťové prvky | Switch, router |
| | 60 | Firewall | |
| | 60 | Elektrická energia | Sídlo spoločnosti |
| Zlyhanie telekomunikačných zariadení | 60 | Dáta o zákazníkoch | Informačný systém, databáza, PC, notebook |
| | 60 | Dáta o zamestnancoch | Server |
| | 60 | Interné dáta | Server, PC, notebook |
| | 60 | Aktívne sieťové prvky | Switch, router |
| | 60 | Internetové pripojenie | Sídlo spoločnosti |
| Výpadok internetového pripojenia | 60 | Aktívne sieťové prvky | Switch, router |
| Špionáž | 60 | Aktívne sieťové prvky | Switch, router |
| | 60 | NAS | |
| | 60 | Účtovný software | Server |
| | 60 | Databáza | Server |
| | 60 | Informačný systém | Server |
| Odhalenie pozície | 60 | Server | |
| Zlyhanie zariadenia | 60 | Aktívne sieťové prvky | Switch, router |
| | 60 | Firewall | |
| Chybné fungovanie | 60 | Server | |
| | 60 | Účtovný software | Server |
| | 60 | Databáza | Server |
| | 60 | Informačný systém | Server |
| Nesprávna údržba | 60 | Server | |
| | 60 | NAS | |
| Odoprenie činností | 60 | Aktívne sieťové prvky | Switch, router |
| | 60 | Firewall | |

Znečistenie a nadmerné prehrievanie je typické pre stolné počítače a notebooky hlavne v prípade, že sa prach usadí na ventilátore a môže dôjsť k poškodeniu zariadenia. Prerušenie dodávky elektriny by malo za následok nedostupnosť dát a nepoužiteľnosť zariadení

závislých na elektrickej energii. U zlyhania telekomunikačných zariadení môže dôjsť opäť k zabráneniu prenosu. U špionáže hrozí riziko odchytenia citlivých údajov, ktoré putujú po sieti. Pri zlyhaní zariadenia, chybného fungovania, nesprávnej údržby alebo odoprenia činnosti hrozí spoločnosti to, že dané aktíva nebude môcť využívať alebo ich bude možné použiť ale len v obmedzenom rozsahu čo môže mať nežiadúce následky.

## 3.3 Výber bezpečnostných opatrení

Na základe analýzy rizík musím vybrať vhodné bezpečnostné opatrenia. Touto problematikou sa zaoberá norma ISO/IEC 27002.

Na základe výsledkov analýzy v spoločnosti som vybral vhodné bezpečnostné opatrenia, ktoré eliminujú dopad rizík zmienených v kapitole 4.2.5.

Tabuľka 28: Zoznam vybraných bezpečnostných opatrení (zdroj: vlastné spracovanie)

| **A.5 Politika bezpečnosti informácií** |
|---|
| A.5.1 Smerovanie bezpečnosti informácií vedením organizácie |
| A.5.1.1 Politiky pre bezpečnosť informácií |
| A.5.1.2 Preskúmanie politík pre bezpečnosť informácií |
| **A.6 Organizácia bezpečnosti informácií** |
| A.6.1 Interná organizácia |
| A.6.1.1 Role a zodpovednosti bezpečnosti informácií |
| A.6.1.3 Kontakt s príslušnými orgánmi a autoritami |
| A.6.2 Mobilné zariadenia a práca na diaľku |
| A.6.2.2 Práca na diaľku |
| **A.7 Bezpečnosť ľudských zdrojov** |
| A.7.2 V priebehu pracovného vzťahu |
| A.7.2.1 Zodpovednosti vedenia organizácie |
| A.7.2.2 Povedomie, vzdelávanie a školenie bezpečnosti informácií |
| A.7.3 Ukončenie a zmena pracovného vzťahu |
| A.7.3.1 Zodpovednosti pri ukončení alebo zmene pracovného vzťahu |
| **A.8 Riadenie aktív** |
| A.8.1 Zodpovednosť za aktíva |
| A.8.1.1 Zoznam aktív |
| A.8.1.2 Vlastníctvo aktív |
| A.8.1.3 Prípustné použitie aktív |
| A.8.2 Klasifikácia informácií |
| A.8.2.1 Klasifikácia informácií |
| A.8.2.2 Označovanie informácií |
| A.8.2.3 Manipulácia s aktívami |

| |
|---|
| **A.9 Riadenie prístupu** |
| A.9.1 Požiadavky organizácie na riadenie prístupu |
| A.9.1.1 Politika riadenia prístupu |
| A.9.2 Riadenie prístupu užívateľov |
| A.9.2.1 Registrácia a zrušenie registrácie užívateľa |
| A.9.2.2 Správa užívateľských prístupov |
| A.9.2.3 Správa privilegovaných prístupových práv |
| A.9.2.4 Správa tajných autentizačných informácií užívateľov |
| A.9.2.5 Preskúmanie prístupových práv užívateľov |
| A.9.2.6 Odobranie alebo úprava prístupových práv |
| A.9.3 Zodpovednosti užívateľov |
| A.9.3.1 Používanie tajných autentizačných informácií |
| **A.10 Kryptografia** |
| A.10.1 Kryptografické opatrenia |
| A.10.1.1 Politika pre použitie kryptografických opatrení |
| A.10.1.2 Správa kľúčov |
| **A.11 Fyzická bezpečnosť a bezpečnosť prostredia** |
| A.11.2 Zariadenia |
| A.11.2.4 Údržba zariadenia |
| A.11.2.5 Premiestnenie zariadenia |
| A.11.2.8 Užívateľské zariadenia bez obsluhy |
| A.11.2.9 Zásada prázdneho stolu a prázdnej obrazovky monitoru |
| **A.12 Bezpečnosť prevádzky** |
| A.12.1 Prevádzkové postupy a zodpovednosti |
| A.12.1.1 Dokumentované prevádzkové postupy |
| A.12.2 Ochrana proti malware |
| A.12.2.1 Opatrenia proti malware |
| A.12.3 Zálohovanie |
| A.12.3.1 Zálohovanie informácií |
| A.12.5 Správa prevádzkového software |
| A.12.5.1 Inštalácia software na prevádzkové náklady |
| **A.13 Bezpečnosť komunikácií** |
| A.13.1 Správa bezpečnosti siete |
| A.13.1.1 Opatrenia v sieti |
| A.13.1.3 Princíp oddelenia v sieti |
| A.13.2 Prenos informácií |
| A.13.2.1 Politiky a postupy pri prenose informácií |
| **A.15 Dodávateľské vzťahy** |
| A.15.1 Bezpečnosť informácií v dodávateľských vzťahoch |
| A.15.1.1 Politika bezpečnosti informácií pre dodávateľské vzťahy |
| **A.16 Riadenie incidentov bezpečnosti informácií** |
| A.16.1 Riadenie incidentov bezpečnosti informácií a zlepšovania |
| **A.17 Aspekty riadenia kontinuity činností organizácie z hľadiska bezpečnosti** |

| |
|---|
| **informácií** |
| A.17.1 Kontinuita bezpečnosti informácií |
| A.17.1.1 Plánovanie kontinuity bezpečnosti informácií |
| A.17.1.4 Verifikácia, preskúmanie a vyhodnotenie kontinuity bezpečnosti informácií |
| **A.18 Súlad s požiadavkami** |
| A.18.1 Súlad s právnymi a zmluvnými požiadavkami |
| A.18.1.4 Súkromie a ochrana osobných údajov |

## 3.4 Návrh zavedenia bezpečnostných opatrení

Táto časť sa zaoberá návrhom bezpečnostných opatrení, ktoré som vyberal na základe výstupu analýzy rizík. Navrhnuté opatrenia zmiernia dopad neprijateľných a nežiadúcich rizík.

### 3.4.1 Politiky bezpečnosti informácií – A.5

Táto podkapitola sa zaoberá bezpečnostnými opatreniami spomenutými v kapitole A.5, ktorú rieši norma ČSN ISO/IEC 27002. Cieľom tejto kapitoly je vypracovať a formálne zdokumentovať politiku bezpečnosti informácií v spoločnosti.

#### A.5.1 Smerovanie bezpečnosti informácií vedením organizácie

**Cieľ:** Určiť smer a vyjadriť podporu bezpečnosti informácií zo strany vedenia v súlade s požiadavkami týkajúcich sa činností organizácie a príslušnými zákonmi a smernicami (3).

#### A.5.1.1 Politiky pre bezpečnosť informácií

Z analýzy som zistil, že v spoločnosti už existujú určité pravidlá pre politiku bezpečnosti avšak nie sú zdokumentované. Je treba spísať ucelený dokument pre bezpečnosť informácií, ktorý bude zahŕňať všetky relevantné časti týkajúce sa bezpečnosti informácií. Taktiež je potrebné predať nové povinnosti spojené s dokumentáciou ISMS a jej spravovaním zodpovednej osobe. V prípade, že to nebude možné musí sa vytvoriť nová pozícia, čo je lepšie riešenie ale finančne nákladnejšie, ktorá bude mať tieto povinnosti na starosť. Pre realizáciu tohto dokumentu je potrebné získať súhlas a podporu od vedenia spoločnosti.

Dokument by mal obsahovať nasledujúce časti:

1. Úvodné ustanovenie spoločnosti o zásadách bezpečnosti informácií
2. Ciele a zásady bezpečnosti informácií

3. Organizáciu bezpečnosti
4. Klasifikáciu a riadenie informačných aktív
5. Personálnu bezpečnosť
6. Fyzickú bezpečnosť a bezpečnosť prostredia
7. Riadenie bezpečnosti komunikácií a prevádzky
8. Riadenie prístupu
9. Vývoj a údržbu systému
10. Riadenie kontinuity prevádzky
11. Súlad s požiadavkami
12. Regulačné, legislatívne a zmluvné požiadavky na bezpečnosť informácií
13. Kritéria hodnotenia rizík
14. Stanovenie zodpovedností pre bezpečnosť informácií
15. Záverečné ustanovenia

#### A.5.1.2 Preskúmanie politík pre bezpečnosť informácií

Kontrola politiky pre bezpečnosť informácií by mala byť vykonávaná v pravidelných intervaloch minimálne jeden krát za rok, alebo vždy po vykonaní nejakých významných zmien, aby sa zistili prípadné nedostatky a vyhodnotila sa jej úspešnosť. Vedenie spoločnosti musí tieto zmeny schváliť. Audit by mal byť vykonaný nezávislou osobou. Výsledky z každého preskúmania politiky pre bezpečnosť informácií by mali byť uchované vo forme záznamov, aby sa k ním dalo dostať.

### 3.4.2 Organizácia bezpečnosti informácií A.6

Táto podkapitola sa zaoberá bezpečnostnými opatreniami spomenutými v kapitole A.6, ktorú rieši norma ČSN ISO/IEC 27002. Cieľom tejto kapitoly je riadiť bezpečnosť informácií a pevne ustanoviť role a zodpovednosti pre riadenie bezpečnosti informácií a určiť kvalifikovanú osobu, ktorá bude mať tieto zodpovednosti na starosť. Táto kapitola sa okrem iného zaoberá aj bezpečnostnými opatreniami pri výkonu práce mimo pracovné priestory.

#### A.6.1 Interná organizácia

**Cieľ:** Ustanoviť rámec riadenia pre zahájenie a riadenie implementácie a prevádzky bezpečnosti informácií v organizácií (3).

### A.6.1.1 Role a zodpovednosti bezpečnosti informácií

Keďže spoločnosť, pre ktorú je tento návrh vypracovaný sa radí medzi malý podnik nemá zmysel určovať role typu architekt kybernetickej bezpečnosti a auditor kybernetickej bezpečnosti. Zodpovednosti týchto ľudí môže spoločnosť riešiť dočasným outsourcingom. Zodpovednosti manažéra kybernetickej bezpečnosti by mala prevziať osoba, ktorá bude zodpovedná za ISMS. Pokiaľ je to finančne možné mala by byť pre tieto zodpovednosti vytvorená nová pozícia, na ktorú bude dosadený kvalifikovaný človek. Vzhľadom na veľkosť spoločnosti a v prípade nedostatku finančných prostriedkov tieto zodpovednosti môžu byť pridelené IT technikovi, ktorý sa v danej oblasti musí najskôr vyškoliť.

### A.6.1.3 Kontakt s príslušnými orgánmi a autoritami

Manažér kybernetickej bezpečnosti musí dodržiavať primeraný vzťah s príslušnými orgánmi a autoritami. Keďže je nutné poznať aktuálne zákony a povinnosti je potrebné, aby tieto veci manažér kybernetickej bezpečnosti sledoval a bol včas informovaný o dôležitých zmenách. Vzhľadom na GDPR musia byť zavedené určité postupy komunikácie s príslušným dozorným orgánom Českej republiky a to v prípade narušenia bezpečnosti osobných údajov.

## A.6.2 Mobilné zariadenia a práca na diaľku

**Cieľ:** Zaistiť bezpečnosť, pri použití mobilných zariadení a práci na diaľku (3).

### A.6.2.2 Práca na diaľku

Spoločnosť povoľuje prácu na diaľku len vo výnimočných prípadoch. Na vzdialené pripojenie využíva Teamviewer, čo je nákladovo úspornejšia a alternatíva k VPN. K pripojeniu na vzdialený počítač, alebo server je vždy potrebné využívať zabezpečené pripojenie a používať vždy oficiálnu verziu programu Teamviewer, ktorá bude pravidelne aktualizovaná so všetkými bezpečnostnými funkciami ako napríklad dvoj-faktorová autentifikácia. Heslo pre prístup do tohto programu musí spĺňať silné kritéria pre administrátorské heslo:

- Dĺžka hesla aspoň 15 znakov
- Heslo musí obsahovať 1 malé, veľké písmeno, číslicu a špeciálny charakter
- Zabezpečiť opakované zadávania hesla po neúspešných pokusoch na prihlásenie aby sa zamedzilo možnosti útoku hrubou silou.

Funkcia typu „Easy Access“ čo znamená nezadávanie hesla pre prístup na vzdialený počítač musí byť vypnutá. Taktiež musí byť nastavený takzvaný „whitelist“ na počítači, ku ktorému sa budú zamestnanci pripájať čo je zoznam počítačov, ktorým bude povolený prístup pre

vzdialenú komunikáciu. Zamestnanci by mali mať počas vzdialenej komunikácie také práva, ktoré sú nevyhnutné k vykonávaniu ich činnosti.

### 3.4.3 Bezpečnosť ľudských zdrojov A.7

Táto podkapitola sa zaoberá bezpečnostnými opatreniami spomenutými v kapitole A.7, ktorú rieši norma ČSN ISO/IEC 27002. Spoločnosť už politiku pre bezpečnosť ľudských zdrojov a bezpečné správanie užívateľov definovanú má, takže v tejto oblasti nie sú potrebné žiadne výrazné zmeny. Je ale potrebné zapracovať na pláne bezpečnostného povedomia, ktorý spoločnosť nemá formálne vypracovaný a nie je meraná jeho účinnosť a na kontrole procesov, v prípade ukončenia pracovného pomeru, ako je vrátenie požadovaných aktív a odstránenie všetkých užívateľských účtov a prístupov.

#### A.7.2 V priebehu pracovného vzťahu

**Cieľ:** Zaistiť, aby si zamestnanci a zmluvné strany boli vedomé a plnili svoje povinnosti v oblasti bezpečnosti informácií (3).

#### A.7.2.1 Zodpovednosti vedenia organizácie

Vedenie organizácie musí zaistiť kontrolu dodržiavania bezpečnostnej politiky formou logov, ktoré budú sledované. Cieľom je, aby malo vedenie organizácie prehľad o tom, či aktivity, ktoré zamestnanci vykonávajú sú v súlade s dodržovaním bezpečnosti informácií. V prípade porušenia bezpečnostnej politiky, musia byť stanovené príslušné sankcie odpovedajúce závažnosti a dopadu porušenia bezpečnostnej politiky. Zamestnanci by taktiež mali mať k dispozícií nejaký anonymný kanál, v rámci, ktorého môžu posielať svoje návrhy na zlepšenie a sťažnosti.

#### A.7.2.2 Povedomie, vzdelávanie a školenie bezpečnosti informácií

Plán bezpečnostného povedomia by mal byť zostavený manažérom kybernetickej bezpečnosti, ktorý určí rozsah potrebných bezpečnostných školení pre spoločnosť a na základe tohto rozsahu vypracuje podrobný plán bezpečnostného povedomia. Každé školenie by malo mať jasne definované pre koho je určené a povinné, jeho cieľ, formu výuky, dĺžku trvania a záverečný test s cieľom získať spätnú väzbu aby sa zistilo, na ktorých oblastiach sa musí zapracovať.

### A.7.3 Ukončenie a zmena pracovného vzťahu

**Cieľ:** Chrániť záujmy organizácie v rámci procesu zmeny alebo ukončenia pracovného vzťahu (3).

#### A.7.3.1 Zodpovednosti pri ukončení alebo zmene pracovného vzťahu

V spoločnosti treba spísať presný proces navrátenia všetkých aktív, ktoré boli zamestnancovi zverené na začiatku pracovného vzťahu. To isté platí aj pre všetky prístupové účty a práva, ktoré musia byť po jeho odchode bezodkladne odstránené. Najvhodnejším riešením je stiahnuť vypracovaný dokument s databázy, v ktorom bude zoznam všetkých príslušných aktív, prístupových práv a oprávnení zamestnanca a informácie na koho sa obrátiť s odovzdaním aktíva alebo odobraním prístupových účtov a oprávnení. S týmto papierom bude musieť zájsť za zodpovednými osobami, ktoré svojim podpisom potvrdia, že dané aktívum bolo vrátené a v prípade prístupových účtov a práv odstránené.

### 3.4.4 Riadenie aktív A.8

Táto podkapitola sa zaoberá bezpečnostnými opatreniami spomenutými v kapitole A.8, ktorú rieši norma ČSN ISO/IEC 27002.

#### A.8.1 Zodpovednosť za aktíva

**Cieľ:** Identifikovať aktíva organizácie a definovať zodpovednosti k ich primeranej ochrane (3).

#### A.8.1.1 Zoznam aktív

Spoločnosť už svoje aktíva eviduje ale ich evidencia nie je úplne dostatočná. Na základe odporúčaní v norme ČSN ISO/IEC 27002 navrhujem rozčleniť aktíva do 4 skupín ako som to vykonal v analýze rizík.

- Hardware
- Software
- Dáta
- Služby

Tieto aktíva musia byť uchovávané v databáze. Záznam by mal vyzerať nasledovne:

Tabuľka 29: Príklad záznamu v dokumente zoznamu aktív (zdroj: vlastné spracovanie)

| Aktívum | Typ aktíva | Popis | Dátum | Vlastník |
|---|---|---|---|---|

Kontrola aktív by mala prebiehať v pravidelných intervaloch aspoň jeden krát za rok.

#### A.8.1.2 Vlastníctvo aktív

Vlastník aktíva bude uvedený počas evidencie aktív. Vlastník aktíva musí mať presne určené zodpovednosti a práva.

#### A.8.1.3 Prípustné použitie aktív

Je potrebné vytvoriť dokument obsahujúci informácie a prípustnom použití aktív spoločnosti. Pravidlá definované v tomto dokumente musia z hľadiska bezpečnosti platiť pre všetkých zamestnancov rovnako.

### A.8.2 Klasifikácia informácií

**Cieľ:** Zaistiť, aby informácie získali odpovedajúcu úroveň ochrany v súlade s ich dôležitosťou pre organizáciu (3).

#### A.8.2.1 Klasifikácia informácií

Za klasifikáciu informácií sú zodpovedný vlastníci aktíva. Informácie sa musia triediť podľa dopadu a kritickosti. Vzhľadom k GDPR si spoločnosť musí dať pozor, aby uchovávala len tie informácie, ktoré potrebuje pre svoju činnosť a uchovávať minimálne množstvo osobných údajov. Informácie budú rozdelené podľa klasifikácie na tri skupiny

- Verejné – informácie, ktoré môžu byť zverejnené
- Interné – informácie, ktoré musia zostať v rámci perimetru firmy
- Chránené – citlivé informácie, ktoré sú určené len pre vybraný okruh ľudí a osobné údaje

Dopad bude rozdelený na päť úrovní od žiadneho dopadu v prípade modifikácie, poškodenia alebo straty až po vážne finančné problémy.

Kompletný záznam klasifikácie informácie môže vyzerať nasledovne:

Tabuľka 30: Príklad záznamu v dokumente klasifikácií informácií (zdroj: vlastné spracovanie)

| Informácia | Popis | Klasifikácia | Dopad |
|---|---|---|---|

#### A.8.2.2 Označovanie informácií

Informácie, ktoré sú identifikované ako chránené musia byť označené a zodpovedá za to ich vlastník. Spôsob označenia musí byť zverejnený.

#### A.8.2.3 Manipulácia s aktívami

Na základe typu informácie musí byť zabezpečený aj ich prístup. Chránené papierové informácie sa musia uchovať na dôvernom mieste, aby sa znížilo riziko ich odhalenia neoprávneným osobám. Digitálne informácie, ktoré sa radia medzi chránené sa musia posielať vždy zašifrované a to len osobám, ktoré na to majú oprávnenie.

### 3.4.5 Riadenie prístupu A.9

Táto podkapitola sa zaoberá bezpečnostnými opatreniami spomenutými v kapitole A.8, ktorú rieši norma ČSN ISO/IEC 27002.

#### A.9.1 Požiadavky organizácie na riadenie prístupu

**Cieľ:** Obmedziť prístup k informáciám a vybaveniu pre spracovanie informácií (3).

#### A.9.1.1 Politika riadenia prístupu

V spoločnosti sa o riadenie prístupu stará technik avšak neexistuje žiadny oficiálny dokument, v ktorom by bola politika riadenia prístupu presne definovaná. Je však nastavená na serveri v rámci Active directory ale vzhľadom na zmeny, ktoré sa robili v kapitole A.8.2 je potrebné preskúmať či súčasná politika týmto zmenám vyhovuje. Pokiaľ nie, tak je potrebné vykonať zmeny v súlade s kapitolou A.8.2. Čo sa týka fyzického prístupu v tomto smere už má spoločnosť zavedené dostatočné bezpečnostné opatrenia. Po preskúmaní politiky riadenia prístupu a vykonania potrebných zmien sa musí aktuálny stav zdokumentovať a pravidelne aktualizovať.

#### A.9.2 Riadenie prístupu užívateľov

**Cieľ:** Zaistiť oprávnený prístup užívateľov a predchádzať neoprávnenému prístupu k systémom a službám (3).

#### A.9.2.1 Registrácia a zrušenie registrácie užívateľa

Za prideľovanie a odoberanie prístupových práv vrátane vytváraní užívateľov je zodpovedný IT technik. Preto navrhujem aby sa vypracoval ucelený zoznam všetkých užívateľov, ktorý bude prehľadný a bude sa pravidelne aktualizovať. Mal by obsahovať názov užívateľa, pod ktorým sa vlastník prihlasuje do operačného systému alebo služby, stručný popis či sa jedná o pridanie alebo odobranie užívateľa, aké má práva, kto je jeho vlastník, informáciu o akú službu sa jedná a dátum. Záznam môže vyzerať nasledovne:

Tabuľka 31: Príklad záznamu v zozname registrovaných užívateľov (zdroj: vlastné spracovanie)

| Užívateľ | Popis | Práva | Vlastník | Software | Dátum |
|---|---|---|---|---|---|

#### A.9.2.2 Správa užívateľských prístupov

Za správu užívateľských prístupov zodpovedá podobne ako v časti A.9.2.1 IT technik. Užívateľský prístup zamestnanca musí byť vytvorený len vtedy, pokiaľ si to vyžaduje jeho

pozícia. Na základe jeho pozície a písomným súhlasom priameho nadriadeného mu potom bude vytvorený užívateľský prístup vrátane príslušných prístupových oprávnení. Z toho vyplýva, že užívateľské prístupy sa budú zaznamenávať v zozname už počas registrácie alebo zrušenia užívateľa.

### A.9.2.3 Správa privilegovaných prístupových práv

Privilegované práva musia byť pridelené len osobám starajúcim sa o samotné riadenie prístupu a správu IT infraštruktúry. Privilegované práva totiž znamenajú absolútnu kontrolu, ktorú z hľadiska bezpečnosti nie je vhodné udeliť bežným užívateľom. O pridelení privilegovaných práv musí byť vždy informovaný konateľ, IT technik a manažér kybernetickej bezpečnosti pokiaľ túto rolu nebude zastávať IT technik. Za žiadnych okolností nesmú byť udelené privilegované prístupové práva bežným užívateľom!

### A.9.2.4 Správa tajných autentizačných informácií užívateľov

Heslá užívateľov musia byť zašifrované pomocou hashovacej funkcie. Pri výbere hashovacej funkcie sa musí dbať na jej aktuálnosť, aby nebola použitá zastaralá technológia. Pri ukladaní sa musí uložiť len samotný hash hesla, ktorý musí byť uchovaný v priečinku do ktorého majú prístup len privilegovaní užívatelia.

### A.9.2.5 Preskúmanie prístupových práv užívateľov

Za preskúmanie prístupových práv je zodpovedný IT technik. Vzhľadom na veľkosť spoločnosti navrhujem aby sa prístupové práva preskúmavali jeden krát za pol rok.

### A.9.2.6 Odobranie alebo úprava prístupových práv

K odobraniu, alebo úprave prístupových práv, musí dôjsť ihneď počas ukončenia pracovného pomeru zamestnanca, alebo pokiaľ zamestnanec mení svoju pracovný pozíciu, ktorá si vyžaduje zmenu prístupových práv. Táto zmena musí byť zaevidovaná v zozname, ktorý bol vytvorený v časti A.9.2.1.

## A.9.3 Zodpovednosti užívateľov

**Cieľ:** Docieliť toho aby boli užívatelia zodpovedný za ochranu svojich autentizačných informácií (3).

### A.9.3.1 Používanie tajných autentizačných informácií

Vzhľadom na výsledky analýzy v asistovanom zhodnotení je potrebné vykonať niekoľko zásadných opatrení. Je potrebné, aby bola zapnutá funkcia, ktorá vynucuje pravidelnú zmenu hesla pre užívateľov v pravidelných intervaloch 90 dní. Musí byť prísne zakázané aby prístupové heslá boli napísané na viditeľnom mieste a aby zamestnanci svoje heslá niekomu prezradili. Taktiež každé heslo musí vyhovovať presne stanoveným kritériám:

- Dĺžka hesla minimálne 15 znakov
- Heslo obsahuje aspoň 1 malé a veľké písmeno, číslicu a špeciálny charakter.

### 3.4.6 Kryptografia A.10

Táto podkapitola sa zaoberá bezpečnostnými opatreniami spomenutými v kapitole A.10, ktorú rieši norma ČSN ISO/IEC 27002.

#### A.10.1 Kryptografické opatrenia

**Cieľ:** Zaistiť riadne a efektívne používanie kryptografie k ochrane dôvernosti, autentickosti a integrity informácií (3).

##### A.10.1.1 Politika pre použitie kryptografických opatrení

Keďže spoločnosť spracováva finančné výkazy svojich zákazníkov, je potrebné zaviesť potrebné bezpečnostné opatrenia aj v tejto oblasti. Vhodným opatrením je šifrovanie diskov pracovných staníc a sieťových diskov, na ktoré sa ukladajú citlivé dáta. Je teda potrebné vybrať vhodný nástroj, ktorý využíva aktuálne šifrovacie mechanizmy. Vzhľadom na to, že spoločnosť používa produkty od firmy ESET, som sa rozhodol pre voľbu ďalšieho produktu od tejto firmy a to konkrétne ESET Endpoint Encryption Pro Edition. Tento program ponúka komplexnú sadu funkcií, ktorá je pre potreby firmy úplne postačujúca:

- Šifrovanie diskov,
- Šifrovanie výmenných médií (napríklad USB kľúčov na základe firemnej politiky),
- Šifrovanie súborov a zložiek,
- Šifrovanie obsahu emailov,
- Šifrovanie virtuálnych diskov.

##### A.10.1.2 Správa kľúčov

Za správu kľúčov bude zodpovedný IT technik, ktorý bude mať na starosti ich údržbu, pridávanie a odstraňovanie spolu s užívateľmi.

### 3.4.7 Fyzická bezpečnosť a bezpečnosť prostredia A.11

Táto podkapitola sa zaoberá bezpečnostnými opatreniami spomenutými v kapitole A.11, ktorú rieši norma ČSN ISO/IEC 27002. Túto časť má spoločnosť zabezpečenú najlepšie. Vyplýva to aj z asistovaného zhodnotenia, pri ktorom mi vyšli všetky časti zelené. Preto sa budem zaoberať opatreniami, ktoré ešte v spoločnosti nie sú dodržiavané.

#### A.11.2 Zariadenia

**Cieľ:** Predchádzať strate, poškodeniu, krádeži alebo kompromitácií aktív a prerušeniu činnosti organizácie (3).

#### A.11.2.4 Údržba zariadenia

Za každé aktívum, vrátane jeho údržby zodpovedá jeho vlastník. Zariadenie musí byť udržované pravidelne na základe pokynov uvedených v jeho príručke. V prípade dlhšieho nepoužívania sa musí kontrolovať jeho stav aspoň jeden krát za štvrťrok.

#### A.11.2.5 Premiestnenie zariadenia

V prípade premiestnenia aktív musí byť spísaný protokol a informované zodpovedné osoby. V prípade spoločnosti to bude jej konateľ, ktorý tento presun musí schváliť.

#### A.11.2.8 Užívateľské zariadenia bez obsluhy

Pre aktíva, ktoré sa používajú bez potreby obsluhy je potrebné, aby z hľadiska bezpečnosti bol prístup k nim obmedzený.

#### A.11.2.9 Zásada prázdneho stolu a prázdnej obrazovky monitoru

Cieľom zásady prázdneho stolu a prázdnej obrazovky monitoru je zníženie rizika straty, neoprávnenému prístupu a vyzradeniu informácií neoprávneným osobám. Na stole musia byť len veci potrebné k výkonu zamestnanca. V prípade, že zamestnanec pracuje s citlivými údajmi, nesmie ich nechať bez dozoru a v prípade jeho odchodu musia byť odložené na bezpečné miesto. Taktiež v prípade odchodu musí uzamknúť svoju obrazovku monitoru, ktorá musí byť zabezpečená heslom.

### 3.4.8 Bezpečnosť prevádzky A.12

Táto podkapitola sa zaoberá bezpečnostnými opatreniami spomenutými v kapitole A.12, ktorú rieši norma ČSN ISO/IEC 27002.

#### A.12.1 Prevádzkové postupy a zodpovednosti

**Cieľ:** Zaistiť správnu a bezpečnú prevádzku, ktorá bude vybavená pre spracovanie informácií (3).

#### A.12.1.1 Dokumentované prevádzkové postupy

Cieľom tohto opatrenia je aby boli zdokumentované všetky prevádzkové postupy a boli dostupné. Je teda potrebné aby bola vypracovaná prehľadná dokumentácia prevádzkových postupov v súlade s bezpečnosťou informácií.

#### A.12.2 Ochrana proti malware

**Cieľ:** Zaistiť, aby informácie a vybavenie pre spracovanie informácií bolo chránené proti malvérovým hrozbám (3).

### A.12.2.1 Opatrenia proti malware

Spoločnosť už nejaké ochranné opatrenia proti malware zavedené má. Ako ochranné opatrenie sa používa antivírus od spoločnosti ESET, ktorý je nainštalovaný na všetkých pracovných staniciach, notebooku konateľa firmy a serveri. Antivírus musí byť pravidelne aktualizovaný, aby sa zaistila najväčšia dostupná ochrana. Taktiež by mali byť zapnuté všetky bezpečnostné funkcie.

Prehľad bezpečnostných funkcií, ktoré musia byť zapnuté:

1. **Sekcia ochrany počítača**

- Rezidentná ochrana súborového systému – jedná sa o kontrolu všetkého čo sa deje. V rámci tejto funkcie musí byť povolená kontrola:
    - lokálnych diskov
    - výmenných médií
    - sieťových diskov

  Taktiež musí byť povolená kontrola škodlivého kódu pri nasledujúcich udalostiach:

    - otváranie súboru
    - vytvorenie súboru
    - spustenie súboru
    - prístup k výmennému médiu
- Ochrana webovej kamery – ochrana pred zneužitím a pokusmi o špehovanie
- HIPS – detekcia a prevencia nechceného správania sa aplikácií

2. **Sekcia ochrany internetu**

- Ochrana prístupu na web – detekcia a blokovanie webu s škodlivým obsahom
- Ochrana poštových klientov – kontrola emailov
- Antispamová ochrana – detekcia a ochrana spamových emailov
- Anti-Phishing ochrana – detekcia a blokovanie phishingových webových stránok

3. **Sekcia ochrany siete**

- Firewall – filter internetovej komunikácie. Dodatočné funkcie musia byť navolené podľa potreby organizácie.
- IDS – ochrana pred sieťovými útokmi
- Botnet – ochrana pred botnetmi

4. **Sekcia bezpečnostných nástrojov**

- Ochrana online platieb – ochrana online bankovníctva a platobných webových stránok.
- Anti-Theft - ochrana PC v prípade odcudzenia

Dodatočné funkcie, ktoré musia byť zapnuté a nakonfigurované na serveri:

- Vzdialená správa koncových staníc – umožňuje komplexný prehľad nad bezpečnosťou jednotlivých pracovných staníc vďaka webovej konzoly nainštalovanej na serveri.

### A.12.3 Zálohovanie

**Cieľ:** Ochrániť dáta proti strate (3).

#### A.12.3.1 Zálohovanie informácií

Spoločnosť už zavedené opatrenia v tejto oblasti má. Na zálohu dát spoločnosť využíva dve sieťové disky typu NAS. Existujú dve typy záloh, ktoré prebiehajú v pravidelných intervaloch a prenos dát je šifrovaný. Systém záloh nemusí byť menený, ale musí sa vykonávať pravidelné testovanie obnovy dát zo zálohy. Vzhľadom na veľkosť podniku navrhujem testovať obnovu dát jeden krát mesačne. Politika zálohovania ale nie je zdokumentovaná, preto navrhujem vypracovať ucelený dokument, v ktorom budú uvedené nasledujúce veci:

- Aké dáta sa zálohujú
- V akom čase prebiehajú zálohy
- Kam sa dáta zálohujú
- Spôsob prenosu dát a o aký typ zálohy sa jedná
- Zabezpečenie záloh
- Postup obnovy dát

### A.12.5 Správa prevádzkového software

**Cieľ:** Zaistiť integritu prevádzkových systémov (3).

#### A.12.5.1 Inštalácia software na prevádzkové systémy

Je potrebné vypracovať podrobný zoznam softwarového vybavenia, ktorý zamestnanci potrebujú na vykonávanie svojej činnosti. Musia sa používať len programy s oficiálnou licenciou, ktoré budú definované v tomto zozname. Pokiaľ nastane situácia, kedy zamestnanec potrebuje na svoju pracovnú stanicu nainštalovať nový program, musí sa najskôr poradiť so zodpovednou osobou. Tou bude IT technik, ktorý bude schopný posúdiť jeho

bezpečnosť a konateľ firmy, ktorý rozhodne o tom, či je program nevyhnutný pre činnosť zamestnanca.

### 3.4.9 Bezpečnosť komunikácie A.13

Táto podkapitola sa zaoberá bezpečnostnými opatreniami spomenutými v kapitole A.13, ktorú rieši norma ČSN ISO/IEC 27002.

#### A.13.1 Správa bezpečnosti siete

**Cieľ:** Zaistiť ochranu informácií v sieti a jej podporných prostriedkoch pre spracovávanie informácií (3).

#### A.13.1.1 Opatrenie v sieti

Väčšina zariadení v sieti má k dispozícii aplikačný firewall. Ten musí byť nakonfigurovaný a spravovaný zodpovednou osobou. V prípade spoločnosti táto zodpovednosť pripadne na IT technika.

#### A.13.1.3 Princíp oddelenia v sieti

Sieť spoločnosti už je rozdelená do VLAN na 4 časti. Všetky tieto siete sú od seba navzájom oddelené. Tieto bezpečnostné opatrenia vykonával IT technik. Je potrebné aby všetky tieto časti boli zdokumentované. Dokumentácia sa musí zhodovať s aktuálnym nastavením.

#### A.13.2 Prenos informácií

**Cieľ:** Zaistiť bezpečnosť informácií pri ich prenose v rámci organizácie a s externými subjektami (3).

#### A.13.2.1 Politiky a postupy pri prenose informácií

Politika prenosu informácií musí byť formálne zdokumentovaná. Pri vytváraní dokumentu by sa mal brať dôraz na:

- Akým spôsobom sa dáta v sieti budú prenášať
- Dovolené typy informácií, ktoré sa môžu po sieti prenášať

Malo by byť taktiež definované a blokované prístupy na stránky s potenciálne nechceným a nebezpečným obsahom.

### 3.4.10 Dodávateľské vzťahy A.15

Táto podkapitola sa zaoberá bezpečnostnými opatreniami spomenutými v kapitole A.15, ktorú rieši norma ČSN ISO/IEC 27002.

#### A.15.1 Bezpečnosť informácií v dodávateľských vzťahoch

**Cieľ:** Zaistiť ochranu aktív organizácie, ku ktorej majú dodávatelia prístup

#### A.15.1.1 Politika bezpečnosti informácií pre dodávateľské vzťahy

Politika bezpečnosti informácií pre dodávateľské vzťahy musí byť zdokumentovaná ako súčasť zmluvy o poskytovaní servisných služieb. Štruktúra SLA zmluvy by mala vyzerať nasledovne:

- Názov objednávateľa a poskytovateľa služieb
- Preambula
- Predmet zmluvy – špecifikácia poskytovaných služieb
- Miesto plnenia – miesto poskytovania služieb
- Špecifiká platnosti, predĺženia, rozšírenia a ukončenie servisnej zmluvy
- Spôsob a podmienky zabezpečenia technickej a systémovej podpory
- Povinnosti poskytovateľa
- Povinnosti objednávateľa
- Ostatné povinnosti zmluvných strán
- Cenník a platobné podmienky
- Zodpovednosť za škody a pokuty
- Záverečné ustanovenia

Politika bezpečnosti informácií by mala byť spracovaná okrem iných vecí v sekcií „ostatné povinnosti zmluvných strán“. Malo by v nej byť uvedené k akým dátam má poskytovateľ služieb prístup a aké dáta o spoločnosti zhromažďuje a ukladá.

### 3.4.11 Riadenie incidentov bezpečnosti informácií A.16

Táto podkapitola sa zaoberá bezpečnostnými opatreniami spomenutými v kapitole A.16, ktorú rieši norma ČSN ISO/IEC 27002.

### A.16.1 Riadenie incidentov bezpečnosti informácií a zlepšovania

**Cieľ:** Zaistiť odpovedajúci a efektívny prístup k zvládaniu incidentov bezpečnosti informácií, zahrňujúci komunikáciu ohľadom bezpečnostných udalostí a slabých miest (3).

Pre riadenie incidentov musí byť vypracovaný dokument, v ktorom bude definovaný postup riešenia incidentov vzhľadom na jeho závažnosť. Tak ako aj aktíva firmy, musia byť incidenty klasifikované od stupnice 1-5 kedy 1 značí najväčšiu prioritu pri riešení a 5 prioritu najmenšiu. Musí byť definovaný čas, za ktorý sa má daný incident vyriešiť a spôsob akým sa budú incidenty riešiť (pri urgentných incidentov treba kontaktovať zodpovedné osoby). Za dohlaď nad prichádzajúcimi incidentami by mal byť zodpovedný manažér kybernetickej bezpečností. Všetky aktuálne incidenty vrátane ich závažnosti a času do kedy musia byť vyriešené, by mali byť viditeľné v nástroji, ktorý umožní ich správu. Po vyriešení každého incidentu sa musí vykonať jeho dokumentácia, aby sa vedelo, ako sa má postupovať v rovnakých situáciách a urýchlil sa celý proces.

## 3.4.12 Aspekty riadenia kontinuity činností organizácie z hľadiska bezpečnosti informácií A.17

Táto podkapitola sa zaoberá bezpečnostnými opatreniami spomenutými v kapitole A.17, ktorú rieši norma ČSN ISO/IEC 27002.

### A.17.1 Kontinuita bezpečnosti informácií

**Cieľ:** Kontinuita bezpečnosti informácií musí byť súčasťou systému riadenia kontinuity činnosti organizácie (3).

#### A.17.1.1 Plánovanie kontinuity bezpečnosti informácií

V rámci udržania kontinuity činnosti musí byť vypracovaný ucelený dokument, ktorý bude slúžiť ako manuál v prípade vypuknutia nejakého bezpečnostného incidentu. Je potrebné aby dokument obsahoval:

- Scenáre, ktoré môžu nastať,
- Bezpečnostné opatrenia, ktoré sa musia vykonať, aby sa zamedzilo úniku informácií,
- Kľúčové činnosti, ktoré sa musia vykonať, aby sa čím skôr obnovila kontinuita činnosti.

### A.17.1.4 Verifikácia, preskúmanie a vyhodnotenie kontinuity bezpečnosti informácií

Cieľom je, aby sa všetky navrhnuté opatrenia v manuály pravidelne overovali a vyhodnocovala sa ich efektivita a účinnosť. Vzhľadom na veľkosť spoločnosti navrhujem aby sa tieto opatrenia preskúmavali jeden krát do roka pokiaľ to nebude potrebné vykonať skôr z dôvodu, že sa napríklad objavia nové hrozby, ktoré by spoločnosti mohli hroziť. Tento manuál treba pravidelne udržiavať a doplňovať o nové aktuálne scenáre.

### A.17.2 Redundancia

**Cieľ:** Zaistiť dostupnosť vybavení pre spracovanie informácií (3).

### A.17.2.1 Dostupnosť vybavenia pre spracovanie informácií

Spoločnosť už má kúpené záložné zdroje pre server a pracovné stanice v prípade výpadku elektriny. Je však potrebné aby tieto zariadenia mali pridelené vlastníka, ktorý bude kontrolovať ich funkčnosť a životnosť.

### 3.4.13 Súlad s požiadavkami A.18

Táto podkapitola sa zaoberá bezpečnostnými opatreniami spomenutými v kapitole A.18, ktorú rieši norma ČSN ISO/IEC 27002.

### A.18.1 Súlad s právnymi a zmluvnými požiadavkami

**Cieľ:** Vyvarovať sa porušeniu zákonných, predpisových, alebo zmluvných povinností týkajúcich sa bezpečnosti informácií a akýchkoľvek bezpečnostných požiadaviek (3).

Spoločnosť musí dbať na dodržiavanie zmluvných podmienok, ktoré má uzavreté s dodávateľmi programového vybavenia. Každá zmluva musí byť pred jej podpísaním schválená konateľom firmy a musia byť vopred známe podmienky prípustného používania aktív vrátane výšky sankcií v prípade porušenia zmluvných podmienok.

### A.18.1.4 Súkromie a ochrana osobných údajov

Jednotlivé zákony a nariadenia od Európskej Únie o ochrane súkromia a osobných údajov spoločnosť musí dodržiavať. Spoločnosť musí dávať pozor aké informácie uchováva a na spracovanie osobných údajov musí od osoby, ktorej údaje chce evidovať vyžiadať písomný súhlas. Za tieto veci bude zodpovedná osoba, ktorá vykonáva funkciu manažéra kybernetickej bezpečnosti v spoločnosti.

## 3.5 Časový plán implementácie navrhnutých bezpečnostných opatrení

Pre jednotlivé navrhnuté bezpečnostné opatrenia som zostavil približný časový plán implementácie. Pri jeho zostavovaní som bral do úvahy náročnosť a rozsah práce, ktorý sa musí vykonať v každej činnosti. Implementácia by mala začať v 36. týždni tohto roku a mala by skončiť v strede 41 týždňa. Najdlhší čas je potrebný na zostavenie samotnej politiky pre bezpečnosť informácií, počas ktorej sa spisuje komplexný dokument, ktorý vedenie organizácie oboznamuje s navrhnutými bezpečnostnými opatreniami. Celkový počet hodín, ktoré sú potrebné na implementáciu je 216. Jedná sa však iba o približnú dobu trvania implementácie a preto je potrebné vyhradiť si nejakú časovú rezervu v prípade, že sa implementácia nestihne urobiť včas. Na tú je vyhradený koniec 41. týždňa implementácie a celý 42. týždeň. Celkový prehľad navrhnutých bezpečnostných opatrení vrátane ich časovej náročnosti je zobrazuje tabuľka číslo 31. Okrem samotnej tabuľky som vytvoril Ganttov diagram pre grafické znázornenie naplánovaných činností v čase vrátane potrebnej rezervy.

Tabuľka 32: Približný časový plán implementácie navrhnutých bezpečnostných opatrení (zdroj: vlastné spracovanie)

| **Názov činnosti** | **Časová náročnosť [h]** |
|---|---|
| A.5.1.1 Politiky pre bezpečnosť informácií | 24 |
| A.5.1.2 Preskúmanie politík pre bezpečnosť informácií | 2 |
| A.6.1.1 Role a zodpovednosti bezpečnosti informácií | 4 |
| A.6.1.3 Kontakt s príslušnými orgánmi a autoritami | 4 |
| A.6.2.2 Práca na diaľku | 6 |
| A.7.2.1 Zodpovednosti vedenia organizácie | 4 |
| A.7.2.2 Povedomie, vzdelávanie a školenie bezpečnosti informácií | 16 |
| A.7.3.1 Zodpovednosti pri ukončení alebo zmene pracovného vzťahu | 4 |
| A.8.1.1 Zoznam aktív | 6 |
| A.8.1.2 Vlastníctvo aktív | 2 |
| A.8.1.3 Prípustné použitie aktív | 4 |
| A.8.2.1 Klasifikácia informácií | 16 |
| A.8.2.2 Označovanie informácií | 2 |
| A.8.2.3 Manipulácia s aktívami | 2 |
| A.9.1.1 Politika riadenia prístupu | 8 |
| A.9.2.1 Registrácia a zrušenie registrácie užívateľa | 4 |
| A.9.2.2 Správa užívateľských prístupov | 2 |
| A.9.2.3 Správa privilegovaných prístupových práv | 2 |
| A.9.2.4 Správa tajných autentizačných informácií užívateľov | 4 |
| A.9.2.5 Preskúmanie prístupových práv užívateľov | 2 |
| A.9.2.6 Odobranie alebo úprava prístupových práv | 2 |
| A.9.3.1 Používanie tajných autentizačných informácií | 2 |
| A.10.1.1 Politika pre použitie kryptografických opatrení | 6 |
| A.10.1.2 Správa kľúčov | 4 |
| A.11.2.4 Údržba zariadenia | 2 |
| A.11.2.5 Premiestnenie zariadenia | 2 |
| A.11.2.8 Užívateľské zariadenia bez obsluhy | 2 |
| A.11.2.9 Zásada prázdneho stolu a prázdnej obrazovky monitoru | 2 |
| A.12.1.1 Dokumentované prevádzkové postupy | 8 |
| A.12.2.1 Opatrenia proti malware | 4 |
| A.12.3.1 Zálohovanie informácií | 4 |
| A.12.5.1 Inštalácia software na prevádzkové náklady | 4 |
| A.13.1.1 Opatrenia v sieti | 4 |
| A.13.1.3 Princíp oddelenia v sieti | 4 |
| A.13.2.1 Politiky a postupy pri prenose informácií | 8 |
| A.15.1.1 Politika bezpečnosti informácií pre dodávateľské vzťahy | 8 |
| A.16.1 Riadenie incidentov bezpečnosti informácií a zlepšovania | 8 |
| A.17.1.1 Plánovanie kontinuity bezpečnosti informácií | 8 |
| A.17.1.4 Verifikácia, preskúmanie a vyhodnotenie kontinuity bezpečnosti informácií | 4 |
| A.17.2.1 Dostupnosť vybavenia pre spracovanie informácií | 4 |
| A.18.1.4 Súkromie a ochrana osobných údajov | 8 |
| **Celkom** | **216** |

| Názov činnosti | Čas [h] | 36. Týždeň | | | | | 37. Týždeň | | | | | 38. Týždeň | | | | | 39. Týždeň | | | | | 40. Týždeň | | | | | 41. Týždeň | | | | | 42. Týždeň | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | Po | Út | St | Št | Pi | Po | Út | St | Št | Pi | Po | Út | St | Št | Pi | Po | Út | St | Št | Pi | Po | Út | St | Št | Pi | Po | Út | St | Št | Pi | Po | Út | St | Št | Pi |
| A.5.1.1 Politiky pre bezpečnosť informácií | 24 | 8 | 8 | 8 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| A.5.1.2 Preskúmanie politík pre bezpečnosť informácií | 2 | | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| A.6.1.1 Role a zodpovednosti bezpečnosti informácií | 4 | | | | 4 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| A.6.1.3 Kontakt s príslušnými orgánmi a autoritami | 4 | | | | 2 | 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| A.6.2.2 Práca na diaľku | 6 | | | | | 6 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| A.7.2.1 Zodpovednosti vedenia organizácie | 4 | | | | | | 4 | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| A.7.2.2 Povedomie, vzdelávanie a školenie bezpečnosti informácií | 16 | | | | | | 4 | 8 | 4 | | | | | | | | | | | | | | | | | | | | | | | | | | |
| A.7.3.1 Zodpovednosti pri ukončení alebo zmene pracovného vzťahu | 4 | | | | | | | | 4 | | | | | | | | | | | | | | | | | | | | | | | | | | |
| A.8.1.1 Zoznam aktív | 6 | | | | | | | | | 6 | | | | | | | | | | | | | | | | | | | | | | | | | |
| A.8.1.2 Vlastníctvo aktív | 2 | | | | | | | | | 2 | | | | | | | | | | | | | | | | | | | | | | | | | |
| A.8.1.3 Prípustné použitie aktív | 4 | | | | | | | | | | 4 | | | | | | | | | | | | | | | | | | | | | | | | |
| A.8.2.1 Klasifikácia informácií | 16 | | | | | | | | | | 4 | 8 | 4 | | | | | | | | | | | | | | | | | | | | | | |
| A.8.2.2 Označovanie informácií | 2 | | | | | | | | | | | | 2 | | | | | | | | | | | | | | | | | | | | | | |
| A.8.2.3 Manipulácia s aktívami | 2 | | | | | | | | | | | | 2 | | | | | | | | | | | | | | | | | | | | | | |
| A.9.1.1 Politika riadenia prístupu | 8 | | | | | | | | | | | | | 8 | | | | | | | | | | | | | | | | | | | | | |
| A.9.2.1 Registrácia a zrušenie registrácie užívateľa | 4 | | | | | | | | | | | | | | 4 | | | | | | | | | | | | | | | | | | | | |
| A.9.2.2 Správa užívateľských prístupov | 2 | | | | | | | | | | | | | | 2 | | | | | | | | | | | | | | | | | | | | |
| A.9.2.3 Správa privilegovaných prístupových práv | 2 | | | | | | | | | | | | | | 2 | | | | | | | | | | | | | | | | | | | | |
| A.9.2.4 Správa tajných autentizačných informácií užívateľov | 4 | | | | | | | | | | | | | | | 4 | | | | | | | | | | | | | | | | | | | |
| A.9.2.5 Preskúmanie prístupových práv užívateľov | 2 | | | | | | | | | | | | | | | 2 | | | | | | | | | | | | | | | | | | | |
| A.9.2.6 Odobranie alebo úprava prístupových práv | 2 | | | | | | | | | | | | | | | 2 | | | | | | | | | | | | | | | | | | | |
| A.9.3.1 Používanie tajných autentizačných informácií | 2 | | | | | | | | | | | | | | | | 2 | | | | | | | | | | | | | | | | | | |
| A.10.1.1 Politika pre použitie kryptografických opatrení | 6 | | | | | | | | | | | | | | | | 6 | | | | | | | | | | | | | | | | | | |
| A.10.1.2 Správa kľúčov | 4 | | | | | | | | | | | | | | | | | 4 | | | | | | | | | | | | | | | | | |
| A.11.2.4 Údržba zariadenia | 2 | | | | | | | | | | | | | | | | | 2 | | | | | | | | | | | | | | | | | |
| A.11.2.5 Premiestnenie zariadenia | 2 | | | | | | | | | | | | | | | | | 2 | | | | | | | | | | | | | | | | | |
| A.11.2.8 Užívateľské zariadenia bez obsluhy | 2 | | | | | | | | | | | | | | | | | | 2 | | | | | | | | | | | | | | | | |
| A.11.2.9 Zásada prázdneho stolu a prázdnej obrazovky monitoru | 2 | | | | | | | | | | | | | | | | | | 2 | | | | | | | | | | | | | | | | |
| A.12.1.1 Dokumentované prevádzkové postupy | 8 | | | | | | | | | | | | | | | | | | 4 | 4 | | | | | | | | | | | | | | | |
| A.12.2.1 Opatrenia proti malware | 4 | | | | | | | | | | | | | | | | | | | 4 | | | | | | | | | | | | | | | |
| A.12.3.1 Zálohovanie informácií | 4 | | | | | | | | | | | | | | | | | | | | 4 | | | | | | | | | | | | | | |
| A.12.5.1 Inštalácia software na prevádzkové náklady | 4 | | | | | | | | | | | | | | | | | | | | 4 | | | | | | | | | | | | | | |
| A.13.1.1 Opatrenia v sieti | 4 | | | | | | | | | | | | | | | | | | | | | 4 | | | | | | | | | | | | | |
| A.13.1.3 Princíp oddelenia v sieti | 4 | | | | | | | | | | | | | | | | | | | | | 4 | | | | | | | | | | | | | |
| A.13.2.1 Politiky a postupy pri prenose informácií | 8 | | | | | | | | | | | | | | | | | | | | | | 8 | | | | | | | | | | | | |
| A.15.1.1 Politika bezpečnosti informácií pre dodávateľské vzťahy | 8 | | | | | | | | | | | | | | | | | | | | | | | 8 | | | | | | | | | | | |
| A.16.1 Riadenie incidentov bezpečnosti informácií a zlepšovania | 8 | | | | | | | | | | | | | | | | | | | | | | | | 8 | | | | | | | | | | |
| A.17.1.1 Plánovanie kontinuity bezpečnosti informácií | 8 | | | | | | | | | | | | | | | | | | | | | | | | | 8 | | | | | | | | | |
| A.17.1.4 Verifikácia, preskúmanie a vyhodnotenie kontinuity bezpečnosti informácií | 4 | | | | | | | | | | | | | | | | | | | | | | | | | | 4 | | | | | | | | |
| A.17.2.1 Dostupnosť vybavenia pre spracovanie informácií | 4 | | | | | | | | | | | | | | | | | | | | | | | | | | 4 | | | | | | | | |
| A.18.1.4 Súkromie a ochrana osobných údajov | 8 | | | | | | | | | | | | | | | | | | | | | | | | | | | 8 | Rezerva | | | | | | |

Obrázok 14: Ganttov diagram (zdroj: vlastné spracovanie)

## 3.6 Ekonomické zhodnotenie

Vzhľadom na to, že spoločnosť už má kúpenú väčšinu potrebného hardvéru a softvéru tak najväčšou položkou budú náklady na implementáciu jednotlivých činností. Tie predstavujú počet hodín vynásobených hodinovou sadzbou odborníka, ktorý bude dané opatrenia zavádzať. Tá môže byť hodne individuálna v závislosti na skúsenosti odborníka. Ja som počítal z hodinovou sadzbou 850 Kč. Tabuľka číslo 32 zobrazuje prehľad nákladov na jednotlivé bezpečnostné opatrenia. Celkové náklady na implementáciu tvoria sumu vo výške 183 600 Kč.

Tieto náklady sa spoločnosti ihneď vrátia v prípade väčšieho kybernetického útoku, ktorý by bez vykonaných bezpečnostných opatrení spoločnosť zasiahol. Ako príklad uvediem Ransomware útok. Jedná sa o druh škodlivého programu, ktorý zašifruje všetky dáta spoločnosti, ku ktorým má prístup a útočník potom od spoločnosti požaduje výkupné za ich dešifrovanie. Môj osobný odhad je, že výška výkupného by sa mohla pohybovať v rozmedzí od 50 000 Kč – 100 000 Kč vzhľadom na citlivé dáta. Navyše by spoločnosť prišla o ušlý zisk, za čas, ktorý by nemala k dispozícií svoje dáta. Vzhľadom na ročný obrat sa denný zisk firmy pohybuje v rozmedzí od 30 000 Kč – 40 000 Kč. Ako je teda možné vidieť, tak náklady na bezpečnostné opatrenia sa spoločnosti vrátia v prípade zabránenia väčšieho bezpečnostného incidentu.

Tabuľka 33: Prehľad nákladov (zdroj: vlastné spracovanie)

| Názov činnosti | Náklady implementácie |
|---|---|
| A.5.1.1 Politiky pre bezpečnosť informácií | 20 400,00 Kč |
| A.5.1.2 Preskúmanie politík pre bezpečnosť informácií | 1 700,00 Kč |
| A.6.1.1 Role a zodpovednosti bezpečnosti informácií | 3 400,00 Kč |
| A.6.1.3 Kontakt s príslušnými orgánmi a autoritami | 3 400,00 Kč |
| A.6.2.2 Práca na diaľku | 5 100,00 Kč |
| A.7.2.1 Zodpovednosti vedenia organizácie | 3 400,00 Kč |
| A.7.2.2 Povedomie, vzdelávanie a školenie bezpečnosti informácií | 13 600,00 Kč |
| A.7.3.1 Zodpovednosti pri ukončení alebo zmene pracovného vzťahu | 3 400,00 Kč |
| A.8.1.1 Zoznam aktív | 5 100,00 Kč |
| A.8.1.2 Vlastníctvo aktív | 1 700,00 Kč |
| A.8.1.3 Prípustné použitie aktív | 3 400,00 Kč |
| A.8.2.1 Klasifikácia informácií | 13 600,00 Kč |
| A.8.2.2 Označovanie informácií | 1 700,00 Kč |
| A.8.2.3 Manipulácia s aktívami | 1 700,00 Kč |
| A.9.1.1 Politika riadenia prístupu | 6 800,00 Kč |
| A.9.2.1 Registrácia a zrušenie registrácie užívateľa | 3 400,00 Kč |
| A.9.2.2 Správa užívateľských prístupov | 1 700,00 Kč |
| A.9.2.3 Správa privilegovaných prístupových práv | 1 700,00 Kč |
| A.9.2.4 Správa tajných autentizačných informácií užívateľov | 3 400,00 Kč |
| A.9.2.5 Preskúmanie prístupových práv užívateľov | 1 700,00 Kč |
| A.9.2.6 Odobranie alebo úprava prístupových práv | 1 700,00 Kč |
| A.9.3.1 Používanie tajných autentizačných informácií | 1 700,00 Kč |
| A.10.1.1 Politika pre použitie kryptografických opatrení | 5 100,00 Kč |
| A.10.1.2 Správa kľúčov | 3 400,00 Kč |
| A.11.2.4 Údržba zariadenia | 1 700,00 Kč |
| A.11.2.5 Premiestnenie zariadenia | 1 700,00 Kč |
| A.11.2.8 Užívateľské zariadenia bez obsluhy | 1 700,00 Kč |
| A.11.2.9 Zásada prázdneho stolu a prázdnej obrazovky monitoru | 1 700,00 Kč |
| A.12.1.1 Dokumentované prevádzkové postupy | 6 800,00 Kč |
| A.12.2.1 Opatrenia proti malware | 3 400,00 Kč |
| A.12.3.1 Zálohovanie informácií | 3 400,00 Kč |
| A.12.5.1 Inštalácia software na prevádzkové náklady | 3 400,00 Kč |
| A.13.1.1 Opatrenia v sieti | 3 400,00 Kč |
| A.13.1.3 Princíp oddelenia v sieti | 3 400,00 Kč |
| A.13.2.1 Politiky a postupy pri prenose informácií | 6 800,00 Kč |
| A.15.1.1 Politika bezpečnosti informácií pre dodávateľské vzťahy | 6 800,00 Kč |
| A.16.1 Riadenie incidentov bezpečnosti informácií a zlepšovania | 6 800,00 Kč |
| A.17.1.1 Plánovanie kontinuity bezpečnosti informácií | 6 800,00 Kč |
| A.17.1.4 Verifikácia, preskúmanie a vyhodnotenie kontinuity bezpečnosti informácií | 3 400,00 Kč |
| A.17.2.1 Dostupnosť vybavenia pre spracovanie informácií | 3 400,00 Kč |
| A.18.1.4 Súkromie a ochrana osobných údajov | 6 800,00 Kč |
| **Celkom** | **183 600,00 Kč** |

## 3.7 Prínos práce

Hlavným prínosom práce je zvýšenie bezpečnosti informácií vo firme na základe noriem rady ČSN ISO 27 000. Zameral som sa predovšetkým na tie opatrenia, ktoré cielili na bezpečnostné riziká, ktoré mi z analýzy vyšli ako tie najväčšie. Tým som docielil celkové zníženie rizika na prijateľnú úroveň vďaka čomu, je spoločnosť chránená pred takými rizikami, ktoré by mohli výrazne ovplyvniť jej finančnú situáciu.

Ako príklad môže poslúžiť ochrana pred bezpečnostným incidentom, ktorý by mal za následok znemožnenie práce zamestnancov na niekoľko dní. Môže sa napríklad jednať a výpadok komunikačnej infraštruktúry, čo by ohrozilo činnosť všetkých zamestnancov alebo strata dôležitých dát zamestnancov, ktoré už zo zálohy nešli obnoviť. Vzhľadom na to, že spoločnosť musí generovať zisk tak si nemôže dovoliť ušlý zisk, ktorý by vplyvom bezpečnostných rizík mohol nastať. Celková suma, ktorá bola vynaložená na návrh bezpečnostných opatrení zhruba predstavuje zhruba 5% ročného zisku čo je pre spoločnosť prijateľný výdaj.

# 4 ZÁVER

Celá práca pozostáva z troch častí. V teoretických východiskách som popísal všetky potrebné pojmy, ktoré boli potrebné pre pochopenie danej problematiky a s ktorými som pracoval v návrhovej časti.

V analýze súčasného stavu som identifikoval, kde sa spoločnosť nachádza, popísal som stav siete a použil som pomôcku asistovaného zhodnotenia od Národného úradu pre kybernetickú a informačnú bezpečnosť. Táto pomôcka slúži pre identifikáciu aktuálneho stavu jednotlivých oblastí na základe, ktorých som získal výstup k návrhu bezpečnostných opatrení.

V návrhovej časti som ešte vykonal analýzu rizík, výstupom ktorej bola matica rizík. Vďaka nej som mohol vybrať opatrenia, ktoré sa vzťahujú na jednotlivé typy neprijateľných a nežiadúcich rizík. Taktiež slúžila aj ako návrh pre politiku riadenia rizík. Jednotlivé opatrenia som navrhoval v súlade s normou ČSN ISO 27 002. Na konci som vypracoval približný časový plán implementácie navrhnutých opatrení vrátane ekonomického zhodnotenia. Všetky požiadavky, ktoré spoločnosť stanovila ako aj ciele tejto práce boli splnené.

# ZOZNAM POUŽITÝCH ZDROJOV

(1) ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. 1. vydání. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

(2) ONDRÁK, V. Prednášky - počítačové sítě. Brno: VUT Fakulta podnikatelská, 2013.

(3) ČSN ISO/IEC 27001. *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky*. 2. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

(4) ČSN ISO/IEC 27002. *Informační technologie - Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Soubor postupů.* Praha: Český normalizační institut, 2014.

(5) ISO/IEC 27000. *Information technology — Security techniques — Information security management systems — Overview and vocabulary.* 5. vydání. Švýcarsko: Mezinárodní organizace pro normalizaci, 2018.

(6) DOUCEK, NOVÁK a SVATÁ, Řízení bezpečnosti informací, Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.

(7) MLÝNEK, Jaroslav. *Zabezpečení obchodních informací*. Brno: Computer Press, 2007, 154 s. ISBN 978-80-251-1511-4.

(8) Managementmania*: Demingův cyklus (Deming Cycle, PDCA Cycle)* [online]. 2016 [cit. 2019-01-17]. Dostupné z: https://managementmania.com/cs/deminguv-cyklus

(9) AUTOCONT*: Důvody pro opatření, budovaná s podporou vedení* [online]. [cit. 2019-01-17]. Dostupné z: https://www.autocont.cz/aktuality/openspace/kyberneticka-bezpecnost/proc?AspxAutoDetectCookieSupport=1

(10) SEDLÁK, P. Prednášky - Oborové managementy bezpečnosti IS. Brno: VUT Fakulta podnikatelská, 2018.

(11) Národní centrum kybernetické bezpečnosti*: CO JE NCKB* [online]. [cit. 2019-01-17]. Dostupné z: https://www.govcert.cz/

(12) DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Vyd. 1. Brno: Computer Press, 2004, 190 s. ISBN 80-251-0106-1.

(13) RiskAnalysisConsultants: *Řada norem ISO/IEC 27000* [online]. [cit. 2019-01-19]. Dostupné z: http://www.rac.cz/rac/homepage.nsf/CZ/ISO27000

(14) ČSN ISO/IEC 27005. *Informační technologie - Bezpečnostní techniky - Řízení bezpečnosti informací*. 2. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

(15) DOUCEK, Petr. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

# ZOZNAM SKRATIEK

**IT** – Informačné technológie (Information Technology)

**ICT** – Informačné a komunikačné technológie (Information and Communication Technology)

**IS** – Informačný systém (Information System)

**IMS** – Integrovaný systém riadenia (Integrated Management System)

**ISMS** – Systém riadenia bezpečnosti informácií (Information Security Management System)

**C** – Dôvernosť (Confidentiality)

**I** – Integrita (Integrity)

**A** – Dostupnosť (Availability)

**NÚKIB -** Národný úrad pre kybernetickú a informačnú bezpečnosť

**ISO -** Medzinárodná organizácia pre normalizáciu (International Organisation for Standardization)

**ITU** – Medzinárodná telekomunikačná únia (International Telecommunications Union**)**

**ANSI** – Americká štandardizačná organizácia (American National Standards)

**BSI** – Britská štandardizačná organizácia (British Standard Institute)

**DIN –** Nemecká štandardizačná organizácia (Deutsches Institut für Normung)

# ZOZNAM OBRÁZKOV

# ZOZNAM TABULIEK