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 PRO DANOU SPOLEČNOST

PROPOSAL FOR THE INTRODUCTION OF SECURITY MEASURES FOR THE COMPANY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Matúš Krídla**
AUTHOR

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

BRNO 2021

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Matúš Krídla**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2020/21

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 pro danou společnost

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:

Cílem práce je pomocí systému řízení bezpečnosti informací vytvořit návrh opatření proti bezpečnostním hrozbám pro danou společnost. Práce se nezabývá zavedením ISMS v plném rozsahu, ale jen vybraných částí.

Základní literární prameny:

ČSN ISO/IEC 27001, Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky, Praha: Český normalizační institut, 2014.

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

DOUCEK P., L. NOVÁK a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2008. ISBN 80-86898-38-5.

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

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2020/21

V Brně dne 28.2.2021

L. S.

Mgr. Veronika Novotná, Ph.D. ředitel	doc. Ing. Vojtěch Bartoš, Ph.D. děkan

Abstrakt

Táto diplomová práca sa zaoberá návrhom a zavedením bezpečnostných opatrení pre danú spoločnosť. Prvá časť práce sa venuje všeobecnému úvodu do danej problematiky, opisuje a definuje jednotlivé pojmy z teoretického hľadiska. Druhá časť popisuje súčasný stav a analýzu vybraných oblasti danej spoločnosti. Výstupom tejto práce je zvýšenie povedomia o bezpečnostných hrozbách a návrhom opatrení prospievajúcich k zvýšeniu bezpečnosti informácií.

Abstract

This diploma thesis deals with the design and implementation of security measures for a given company. The first part of the work deals with a general introduction to the issue, describes and defines the various concepts from a theoretical point of view. The second part describes the current state and analysis of selected areas of the company. The output of this work is to raise awareness of security threats and propose measures to increase information security.

Klíčová slova

Informačná bezpečnosť, aktíva, ISO/IEC 27000, zodpovednosť, riziko, opatrenia

Key words

Information security, assets, ISO/IEC 27000, responsibilty, risk, countermeasures

Bibliografická citácie

KRÍDLA, Matúš. *Návrh zavedení bezpečnostních opatření pro danou společnost* [online]. Brno, 2021 [cit. 2021-05-16]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/134697. 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 citácia použitých prameňov je úplná, že som v práci neporušil autorské práva (v zmysle zákona č. 121/2000 Zb. o práve autorskom a o právach súvisiacich s právom autorským).

V Brne dňa 16. 5. 2021

…… podpis študenta

Poďakovanie

Týmto by som chcel poďakovať môjmu vedúcemu práce Ing. Petrovi Sedlákovi za cenné informácie a rady pri písaní tejto práce ale aj počas celého štúdia. Taktiež by som chcel poďakovať vedeniu spoločnosti KRIDLA s.r.o za sprostredkovanie podkladov a informácií.

OBSAH

ÚVOD

Zabezpečenie je oblasť, ktorá je vo všeobecnosti mnohokrát príliš zanedbávaná a podceňovaná. V súčasnej dobe, v ktorej mnoho firiem a spoločnosti nedokáže fungovať bez informačných a komunikačných technológii, je vyžadované riadiť zabezpečenie informácií. Faktom však je, že dnešná doba, v ktorej žijeme sa uberá smerom, kedy rozvoj informačných a komunikačných technológii sa rozvíja takým tempom, ktorý nie je možné mať pod kontrolou. Presne z tohto dôvodu sa stále viac rozširuje a zvyšuje nebezpečenstvo sieťových útokov a je čoraz viac pravdepodobné, že informačné aktíva firiem a spoločností budú ohrozované.

Práve preto je veľmi potrebné zavedenie bezpečnostných opatrení, ktoré znížia počet a dopad spomínaných útokov. Najlepšie by bolo, aby každá spoločnosť riadila bezpečnosť informácii cielene a efektívne ju rozvíjala. Z tohto dôvodu je veľmi dôležité nezanedbávať túto problematiku a brať ju ako systémový celok riadenia bezpečnosti informácií. Ak by sa tento systém zaviedol, zvýšila by sa kompletná informačná bezpečnosť vo firme či spoločnosti a následne by sa tak znížila tvorba a následky rizík, ktoré môžu byť pre dané spoločnosti veľkou finančnou hrozbou.

1 TEORETICKÉ VÝCHODISKA PRÁCE

Teoretická časť tejto práce sa zaoberá vysvetlením základných pojmov a názvosloví ktoré sú potrebné na pochopenie danej problematiky.

1.1 Základné pojmy a názvoslovia

V danej kapitole si zadefinujeme jednotlivé pojmy ktoré úzko súvisia s preberanou problematikou riadenia bezpečnosti.

- **IT** (Information Technology) – Informačné technológie
- **ICT** (Information nad Communication Technology) – informačné a komunikačné technológie
- **IS** (Information System) – informačný systém
- **ISMS** (Information Security Managment System) – Systém riadenia informačnej bezpečnosti

(1)

- **Informácia**

Forma údaju ktorá popisuje reálne prostredie, jeho stav a procesy ktoré v nej prebiehajú. V informatike tvoria kódované dáta informáciu (kódovaním je myslená fyzikálna interpretácia v prenosovom médiu alebo úložnom zariadení, nie kryptografia. (1)

- **Dáta**

Plnenie informácie ktorú vytvára. Je to informácia vo formalizovanej podobe ktorá slúži na spracovanie, komunikáciu alebo vyhodnocovanie. (2)

- **Prenos dát**

Taktiež nazývaná digitálna komunikácia, je to prenos digitalizovaného signálu alebo digitálnej správy pomocou prenosového prostredia. (2) Prenosovým prostredím sa myslí metalický, optický kábel alebo bezdrôtový prenos. (1)

- **Informačný systém**

Presná definícia informačného systému nám nie je známa ale môže to byť chápané ako systém vzájomne prepojených procesov a informáciami (1)

- **Sieťová infraštruktúra**

Všetky sieťové prvky a zariadenia, ktoré sú použité na realizáciu ICT prostredia nazývame sieťová infraštruktúra. (1)

- **Počítačová sieť**

Prostredie slúžiace na komunikáciu medzi užívateľmi siete a je to súčasťou sieťovej infraštruktúry. (1)

- **Dôvernosť**

(Confidentality) – Zaistiť aby mali prístup k informácií len užívatelia s oprávnením. (1)

- **Integrita**

(Integriy) – Zaistenie toho aby boli všetky informácie správe a kompletné. (1)

- **Dostupnosť**

(Availability) – Zaistiť aby mali užívatelia s oprávnením okamžitý prístup k informácií v požadovaný čas (1)

- **Aktívum**

(Asset) - Celkový Nehmotný alebo hmotný majetok (2)

- **Hrozba**

(Treat) - Událosť pri ktorej je ohrozená bezpečnosť (1)

- **Zraniteľnosť**

(Vulnerability) - Slabé miesto daného aktíva (1)

- **Opatrenie**

(Countremeasure) – Zníženie hrozby pomocou nejakej aktivity (1)

- **Riziko**

(Risk) – Kombinácia zranitelnosti, hrozby a dopadu na aktívum (1)

- **Dopad**

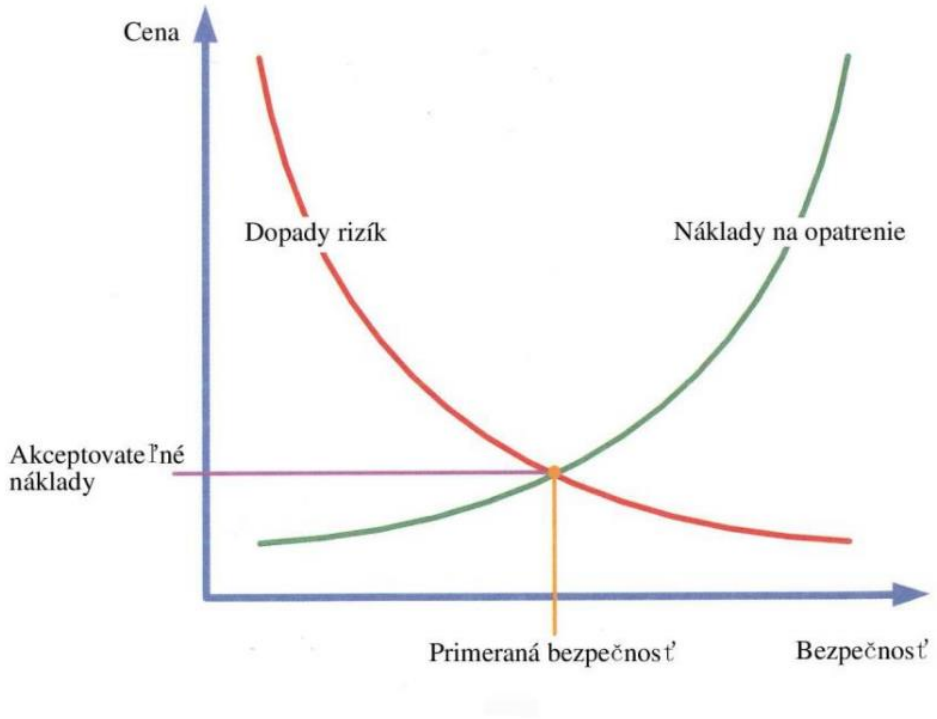
(Impact) – Dôsledok pôsobenia hrozby a následného vzniku škody (1)

1.2 Primeraná bezpečnosť

Rozmer vynaloženého úsilia a investícií, ktorú spoločnosť vložila do bezpečnosti IS, musí vždy zodpovedať hodnote a dôležitosti aktív a tiež miere možných rizík.

Práve to stanovuje najmä spomínaná bezpečnostná politika spoločnosti.

Presnú predstavu o tejto problematika nám udáva graf, ktorý poukazuje na primeranú bezpečnosť za prijateľné náklady (1).



Obrázok 1: Primeraná bezpečnosť (zdroj: 2)

1.3 ISMS

Samotná definícia ISMS, vychádza už zo samostatného názvu ISMS (Information Security Managment Systems), čo v preklade znamená systém riadenia informačnej bezpečnosti. Spočíva v riadení informačnej bezpečnosti všetkých atribútov, ktoré to

obnáša. Dôležité je si uvedomiť, že daný systém riadenia informačnej bezpečnosti je len časťou systému riadenia organizácie ako celku (3).

ISMS vychádza z využitia modelu PDCA, takzvaného Demingovho modelu, ktorý pozostáva zo 4 etáp:

- **Ustavenie ISMS**
  - **Riadenie rizík** (Risk Management) **–** koordinácia, ktorá je nevyhnutná pri kontrole a riadení spoločnosti, pričom berie ohľad na možné riziká.
  - **Hodnotenie rizík** (Risk Assessment) – postup, pri ktorom sa analyzujú a následne vyhodnocujú riziká.
  - **Analýza rizík** (Risk Analysis) – využivanie informácii, ktoré pracuje na základe istých pravidiel a používa sa na odhadnutie miery rizík a tiež na určenie ich zdrojov.
  - **Vyhodnotenie rizika** (Risk Evaluation) – postup, pri ktorom sa porovnávajú odhadované riziká s kritériami pre určenie ich významu.
  - **Zvládanie rizík** (Risk Treatment) – postup, pri ktorom prebieha výber a príjem opatrení znižujúcich dané riziká.
  - **Akceptácia rizika** (Risk Acceptance) – rozhodnutie akceptovať dané riziko.
  - **Prehlásenie o aplikovateľnosti** (Statement of Aplicability) – doklad, ktorý obsahuje popis opatrení v ISMS spoločnosti. (1)
- **Zavedenie a prevádzka ISMS**
  - Účinnosť informačnej bezpečnosti (Information Security Effectiveness) – udáva rozsah, zahŕňajúci bezpečnosť informácií, ktorý napĺňa ciele spoločnosti.
  - Miera (Measure) – určuje a poukazuje na potrebu informácií.
  - Meranie (Measurement) – postup, ktorý spočíva v nadobúdaní informácií o efektivite ISMS.
  - Záznam – doklad, potvrdenie o tom, či je dosiahnutý požadovaný výsledok či dôkaz o aktivite v riadení kvality. (1)
- **Monitorovanie a skúmanie ISMS**
  - Audit (Audit) – samostatný, systematický a dokumentovaný postup, ktorý podľa predom stanovených kritérií, slúži na objektívne posudzovanie.

- Skúmanie (Review) - Stanovuje či je predmet skúmania vhodný, primeraný a účinný k dosiahnutiu stanovených cieľov. (1)

- **Údržba a zlepšovanie ISMS**
  - Nezhoda (Nonconformity) - nesplnenie a nedodržanie požiadaviek.
  - Náprava (Correction) – kroky ktoré odstraňujú nezhody.
  - Opatrenia k náprave (Correction Action) – kroky, ktoré odstraňujú dôvody nezhody.
  - Preventívne opatrenia (Preventive action) – sú to kroky, ktoré odstraňujú potencionálne nezhody.
  - Bezpečnostná politika (Security event) – sú to predpisy, ktoré určujú riadiaci systém, distribúciu a ochranu aktív.
  - Bezpečnostná udalosť (Security Policy) – identifikovaná situácia v ktorej sa nachádza systém, služba alebo sieť a ktorá poukazuje na to že mohlo dôjsť k porušeniu bezpečnostnej politiky alebo mohli zlyhať bezpečnostné opatrenia.
  - Bezpečnostný incident (Security Incident) – pojem, ktorý označuje nejakú nepríjemnú či neštandardnú situáciu a ktorá smeruje k tomu, že budú narušené pravidla bezpečnosti v spoločnosti.
  - Riadenie kontinuity spoločnosti (Business Continuity Management) – BCM je činnosť, ktorá je úzko spojená a podriadená podnikaniu. Môže tiež umožniť prevádzkový a strategický rámec, ktorý nám dáva pohľad na to akým spôsobom spoločnosť poskytuje svoje produkty a služby a v akom rozmere je spoločnosť odolná proti ich narušeniu, poškodeniu či strate.
  - Systém riadenia kontinuity spoločnosti (Business Continuity management system) – BCMS je postup riadenia, ktorý podporuje vedenie spoločnosti, ktorý identifikuje možné dopady strát a cieľom tohto procesu je vytvorenie takých postupov a prostredia, ktoré umožnia zaistenie kontinuity a obnovenie kľúčových procesov a činnosti danej spoločnosti. (1)

1.4 Demingov cyklus PDCA

Jedná sa o metódu ktorá nám slúži na postupné zlepšovanie všetkých možných činností napríklad kvality služieb, procesov či výrobkov a pod. Forma zlepšovania prebieha opakovaním štyroch základných činností čo už uvádza názov PDCA (Plan, Do, Check, act) (1)

- **Plan** (Plánuj)

Stanoviť ciele a procesy potrebné na dosiahnutie požadovaných výsledkov

- **Do** (Rob)

Vykonať ciele ktoré sme si v predchádzajúcom bode stanovili

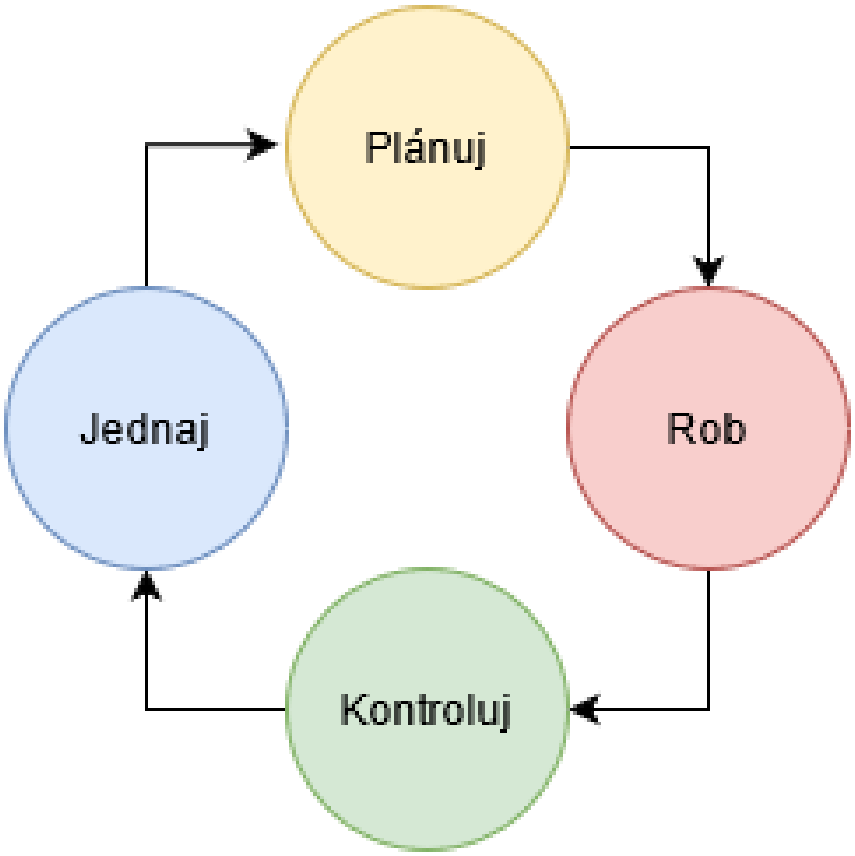
- **Check** (Kontroluj)

Počas tejto fázy sa vyhodnocujú údaje a výsledky ktoré sme nazhromaždili pri fáze „Do“

- **Act** (Jednaj)

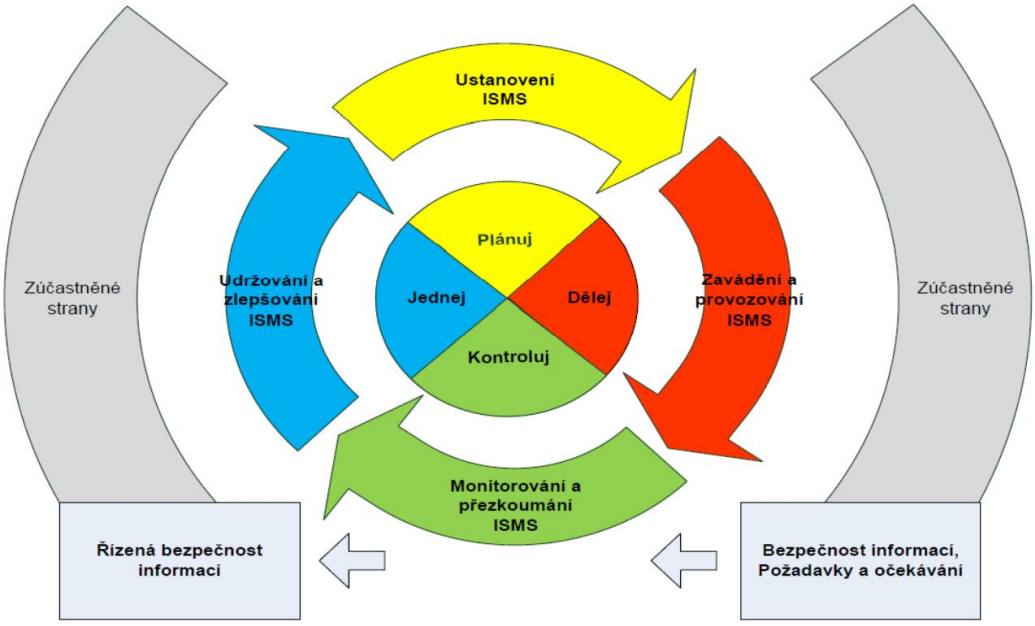
Táto fáza sa zaoberá vylepšením procesu pomocou informácií ktoré sme nazhromaždili počas dvoch predchádzajúcich procesov. (1)

Dôležitou súčasťou celého modelu je ich samotná dokumentácia. Procesy je potrebné identifikovať, popísať a zdokumentovať. Na základe dokumentácie riadiť a následne ich priebeh optimalizovať. (1)



Obrázok 2: PDCA cyklus (zdroj: vlastné spracovanie)

Takzvaným duchovným otcom PDCA cyklu je Walter Shewahart (1891-1967) ale neskôr bol vylepšený americkým štatistikom W.Edwards Demingom (1900-1993). Deming bol taktiež spolutvorcom TQM. TQM – Total Quality Managment je nastroj riadenia ktorý využíva komplexnú metódu riadenia s dôrazom na riadenie kvality vo všetkých cykloch organizácie. (4)



Obrázok 3: Demingov model (zdroj: 1)

1.5 Bezpečnostné hrozby

Jednou z vlastností hrozby je možná schopnosť spôsobiť nepriaznivý incident kde následkom môže byť poškodenie spoločnosti, jej systému a aktív. (1)

1.5.1 Základné rozdelenie hrozieb

Pôvod hrozieb môže byť rôzny. Buď je to prírodná hrozba (blesk, požiar, zemetrasenie, pôvodne), alebo môžu byť hrozby spôsobené ľudským faktorom (chyba užívateľa, odposluch, a pod.).

Ďalšie delenie hrozieb je na úmyselné (úmyselné poškodenie, odcudzenie) a náhodné (vymazanie súborov).

Ďalšie hľadisko, podľa ktorého delíme hrozby je hľadisko bezpečnosti a na základe toho je žiadúce, aby tak ako úmyselné aj náhodné hrozby boli identifikované a nájdené a mala by byť odhadnutá ich pravdepodobnosť a úroveň.

Ďalej sa hrozby podľa zdroja delia na vonkajšie a vnútorné a podľa dopadu na systém na aktívne a pasívne.

Už pri samotnej realizácií (napríklad pri analýze rizík) sa odporúča zoskupiť hrozby a to podľa toho na aké aktívum pôsobia :

- Operačný systém
- Aplikácia
- Databáza
- Sieť
- Klient (1)

1.5.2 Posúdenie hrozieb

Pri posudzovaní hrozieb vždy pozeráme v akej sú závislosti od nasledujúcich otázok:

- **Strata dôvernosti** – k tej môže dôjsť napríklad voči zákazníkovi, právnej zodpovednosti, finančnej strate či ohrozeniu osobnej bezpečnosti
- **Strata integrity** – táto strata môže viesť k narušeniu funkčnosti organizácie či k prijatiu zlých rozhodnutí
- **Strata dostupnosti** – jej následkom môže byť neschopnosť vykonávať kritické činnosti spoločnosti
- **Strata individuálnej zodpovednosti** – pri tejto strate môže dôjsť k špionáži, krádeži či akémukoľvek podvodu
- **Strata autentickosti** – táto strata môže viesť napríklad k tomu, že budú použité neplatné dáta, ktoré budú viesť k neplatným výsledkom
- **Strata spoľahlivosti** – na základe tejto straty sa spoločnosť môže dostať k nespoľahlivým dodávateľom či de motivácií zamestnancov

Dôležité je nezabudnúť na následné dopady hrozby. Keď sa pozrieme napríklad na výpadok elektrickej energie, ta môže mať zlý dopad nielen na dostupnosť dát ale tiež môže pri dlhodobom výpadu spôsobiť ohrozenie pôsobenia spoločnosti, prípadne môže ohroziť aj fyzickú integritu človeka. Preto je vždy dôležité myslieť na možné následky hrozieb až do ich najmenších podrobností. (1)

1.5.3 Najčastejšie hrozby

Zlyhanie dodávky energie – pri tomto zlyhaní môžu nastať problémy z hľadiska integrity a následne to môže byť príčinou ďalších porúch.

Škodlivý software – táto hrozba môže zmariť autentizáciu a všetky s ňou súvisiace bezpečnostné služby a funkcie. Ako následok môže byť strata dostupnosti

Zlyhanie hardvéru – Tieto poruchy techniky napríklad v sieti môžu spôsobiť, že dôjde k zničeniu dostupnosti akýchkoľvek informácií, ktoré sú spracované alebo uchované v danej sieti. Jednou z najčastejších príčin zlyhania hardvéru je napríklad slabá údržba, nezrozumiteľné postupy pri zabezpečení údržby HW alebo nevhodné umiestnenie HW (prach, vlhkosť, teplota).

Zlyhanie komunikačných služieb – Poruchy a chyby komunikačných zariadení a služieb často ohrozujú dostupnosť informácií ktoré sú prenášané prostredníctvom týchto komunikačných služieb. Všetko závisí od príčiny chyby alebo poruchy a v tejto závislostí sa pozeráme na komunikáciu vonkajšiu a vnútornú (1)

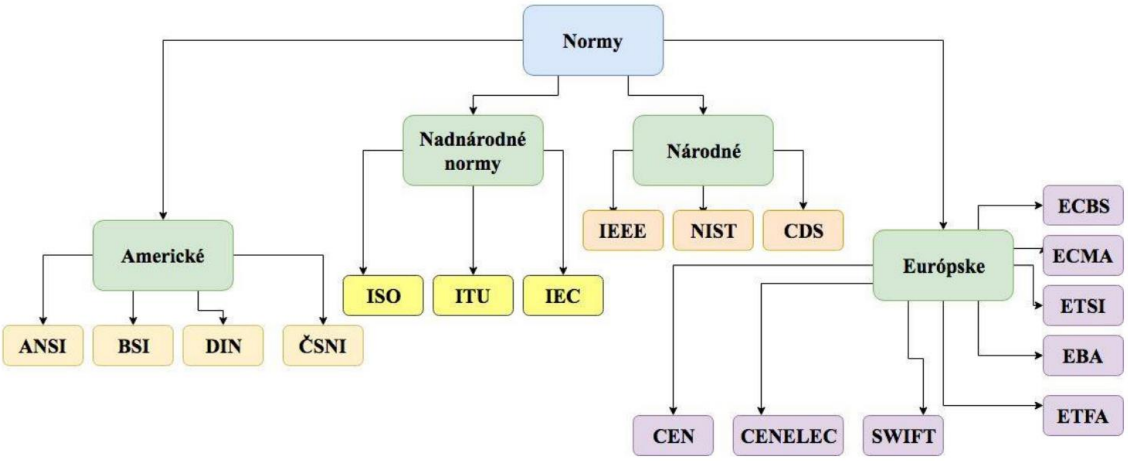
1.6 Normy

Štandard

Je to dohovor ktorý obsahuje technické špecifikácie alebo iné kritéria, ktoré sú dôsledne stanovené a používané ako pravidlá, smernice ale aj ako definície vlastností, ktoré charakterizujú a zabezpečujú že procesy, výroby, materiály či služby sú také ako boli na začiatku stanovené (napr. telefóne či čipové karty, komunikačný protokol, politika poskytovania služieb) (1)

Norma

Pravidlo ktoré obsahuje odporučenie pre dané riešenie alebo štandard (v ICT oblasti sa konkrétne jedná o smernicu alebo predpis ktorý je vydávaný rôznymi výrobcami či užívateľmi IT – jedná sa preto o odporučenie štandardov ktoré je možné použiť k realizácií kompatibilného žiadaného riešenia) (1)

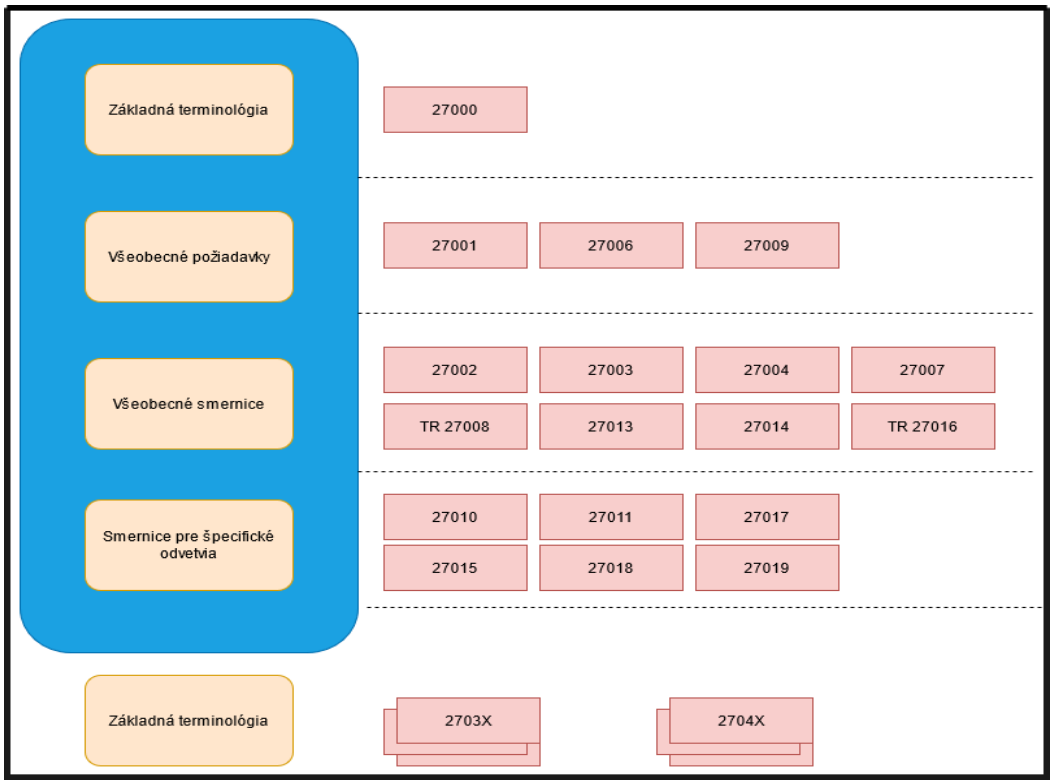


Obrázok 4: Normy a normalizačné inštitúcie (zdroj: vlastné spracovanie)

ISO (the International Organization for Standardization) je skraka pre Mediznárodnú organizáciu pre štandardizáciu, ktorá koordinuje, štandardizuje a normalizuje technnickú činnosť v medzinárodnom meradle. (5)

IEC (the Internation Electrotechnical Commission) je skratka pre medzinárodnú organizáciu pre ktorú vytvára a publikuje „International Standards for all electrical, electronic and related technologies“ veobecne známe skôr pod pojmom „elektrotechnológia“ (1)

Medzinárodné štandardy pre manažment systémov poskytujú model akým spôsobom nastaviť a prevádzkovať systém manažérstva informačnej bezpečnosti. Tento model vzišiel na základe konsenzu expertov v jednotlivých oblastiach a výsledkom je najmodernejší medzinárodný súbor postupov a noriem. ISMS je názov pre Information Security Managment Systems, teda systémy manažérstva informačnej bezpečnosti. Majú pomáhať organizáciám rôzneho zamerania a veľkosti pomôcť pri implementácií a prevádzkovaní ISMS. ISMS je systematický prístup pre vytváranie. Implementáciu prevádzku, monitorovanie, kontrolovanie, udržiavanie a zlepšovanie informačnej bezpečnosti organizácie na dosiahnutie jej biznis cieľov (6)



Obrázok 5: Rodina noriem 27xxx (zdroj: vlastné spracovanie)

ISO/IEC 27000 – Information technology – Security techniques – Information managment systems overview and vocabulary

- Úvod do ISMS
- Zahrňuje základné pojmy a definície pre oblasť ISMS
- Poskytuje prehľad noriem z rady 27000 (7)

ISO/IEC 27001 – Information technology – Security techniques – Information security managment systems – Requirements

- Je to stručnejšia norma
- V tejto norme sa definujú požiadavky na zriadenie, implementáciu, prevádzku, monitoring, kontrolu, údržbu a spôsoby na zlepšovanie systému riadenia informačnej bezpečnosti
- Porovnáva činnosti ktoré vykonáva organizácie a hrozby, ktorým môže potenciálne čeliť
- Požiadavky sú zadefinované tak aby bol tento štandard všeobecne použiteľný

- V rámci ISO 27001 je väčšinu požiadaviek na ISMS nutných splniť pre certifikáciu podľa tejto normy (7)

ISO/IEC 27002 – Information technology – Security techniques – Code for practice for information security managment (8)

- Presne definuje ciele jednotlivých oblastí informačnej bezpečnosti a zahŕňa zoznam opatrení a funkcií na dosiahnutie týchto cieľov

Pokrýva tieto oblasti v rámci informačnej bezpečnosti :

- Bezpečnostná politika
- Organizácia informačnej bezpečnosti
- Personálna bezpečnosť
- Fyzická bezpečnosť
- Manažment vzťahov medzi dodávateľmi alebo poskytovateľmi služieb
- Prevádzka systémov a komunikácie
- Manažment aplikačných a sieťových služieb
- Riadenie prístupu
- Obstarávanie, vývoj a údržba systémov
- Riešenie bezpečnostných incidentov
- Manažment kontinuity činnosti
- Legislatívne kritéria

ISO/IEC 27036 – Information technology – Security techniques – Information security for supplier relationships (9)

- Táto medzinárodná norma poskytuje ďalšie podrobné pokyny na vykonávanie kontrol so vzťahmi s dodávateľmi, ktoré sú opísané ako všeobecné odporúčania v ISO/IEC 27002

Norma ISO/IEC 27036 sa skladá z nasledujúcich častí :

- Časť 1: prehľad a koncepty
- Časť 2 : Požiadavky

- Časť 3: Pokyny pre bezpečnosť dodávateľského reťazca informačných a komunikačných technológií
- Časť 4 : Pokyny pre bezpečnosť cloudových služieb

1.7 Analýza rizík

Analýza rizík je zameraná na ohodnotenie pravdepodobnosti vzniku bezpečnostných incidentov a ich následkov, prípadne na ohodnotenie identifikovaných aktív, hrozieb a zraniteľnosti. Vykonáva sa v rozličných úrovniach podrobnosti v závislosti od účelu analýzy, požiadaviek, dostupnosti informácií či od možnosti organizácie (personálnych, časových, finančných)

Analýza využíva kvalitatívnu alebo kvantitatívnu metodiku, prípadne kombináciu oboch. (10)

1.7.1 Kvalitatívna analýza rizík

Táto analýza spočíva v tom, že používa stupnicu kvalifikačných atribútov na opis rozsahu následkov (napr. vysoká, stredná a nízka) a pravdepodobnosť ich vyskytnutia. Výhodou kvalitatívnej analýzy rizík je jej jednoduché pochopenie pre všetky zainteresované strany, zatiaľ čo nevýhodou je závislosť od subjektívneho výberu stupnice

Stupnice sú upravované alebo prispôsobované tak, aby vyhovovali rôznym možnostiam ktoré môžu nastať. Kvalitatívny odhad sa najčastejšie používa:

- Na mapovanie začiatočných činností pri identifikácií rizík
- V prípadoch kde sa nachádza rozhodovanie
- Ak sú zdroje alebo dáta nevhodné na využitie kvantitatívnej metódy (10)

1.7.2 Kvantitatívna analýza rizík

Pri používaní kvantitatívnej analýzy rizík sa využíva stupnica s číselnými hodnotami. Platnosť použitých modelov, úplnosť a presnosť číselných hodnôt nám určujú kvalitu analýz. Výhodou kvantitatívnej analýzy rizík je že vo väčšine prípadov používa historické dáta a tie poskytujú výhodu. Nevýhodou je nedostatok takýchto dát pre nové riziká alebo

slabé miesta informačnej bezpečnosti analyzovanej spoločnosti. Nevýhoda nastáva keď fakty o kontrolovaných dátach nesú k dispozícii a tým sa vytvára ilúzia o presnosti výsledkov (10)

1.7.3 Kombinovaný prístup

Ďalšou, v poradí treťou z možností je kombinovaný prístup. Na začiatku sa realizuje počiatočná analýza rizík prevádzaná na hrubej úrovni pre všetky systémy informačných technológií, ktorá sa pri každom prípade sústredí na hodnotu systému IT pre činnosť spoločnosti a na vážne riziká ktorým je systém informačných technológií vystavený. V spomínaných systémoch ktoré sú identifikované ako veľmi významne pre spoločnosť a vystavené vysokým rizikám by prvotne mala byť zrealizovaná podrobná analýza rizík. Pre všetky ostatné systémy by mal byť vybraný a aplikovaný základný prístup. Práve tento výber ktorý je kombináciou tých najlepších možností umožňuje minimalizovať úsilie a čas venovaný na určenie ochranných opatrení pri čom stále zabezpečuje že vysoké riziká systému sú chránené prislúchajúcim spôsobom. (1)

1.7.4 Podrobný prístup

Podrobný prístup detailne analyzuje riziká systému IT ktoré obsahujú identifikáciu rizík s nimi súvisiacich a odhad ich veľkosti. Daná analýza zaháňa hĺbkovú revíziu v každom z týchto krokov :

- Stanovenie hraníc revízie – je prevádzané ešte pred identifikáciou a hodnotením aktív. Umožňuje nám definovať to ktorých prvkov sa bude analýza týkať.
- Identifikácia aktív – pri tejto identifikácií sa berie do úvahy to, že systém IT netvorí len HW a SW ale všetky aktíva ktoré sú súčasťou organizácie (Služby, informácie a pod.).
- **Ohodnotenie aktív** – sú priradené hodnoty, ktoré reprezentujú ich význam. Vstupné údaje hodnôt aktív zaisťujú ich vlastníci a používatelia napríklad formou dotazníka. Daná hodnota nemusí byť určená ohodnotením ale taktiež z jej dopadov na spoločnosť pri strate dôvernosti, dostupnosti a integrity

- **Hodnotenie hrozieb** - hodnotenie hrozieb je dané do súvislosti s identifikovanými aktívami spoločnosti.
- **Odhad zraniteľnosti** – tento odhad slúži na odhalenie slabých miest v spoločnosti, postupoch, personálu manažmentu, administrácií, jeho fyzickom prostredí alebo v komunikačnom zariadení ktoré môžu byť využité zdrojom hrozby a zapríčiniť tak škody na spomínaných aktívach spoločnosti
- **Identifikácia plánovaných a existujúcich ochranných opatrení** – do analýzy rizík zaradujeme aj danú identifikáciu plánovaných alebo existujúcich bezpečnostných opatrení. Výsledkom tejto identifikácie je tiež zoznam všetkých existujúcich a všetkých plánovaných bezpečnostných opatrení. (1)

2 ANALÝZA SÚČASNÉHO STAVU

Táto kapitola ma za úlohu predstavenie základných informácií o spoločnosti a analýza aktuálneho vnímania bezpečnosti informácií

2.1 Predstavenie spoločnosti

Obrázok 6:Logo spoločnosti (zdroj:8)

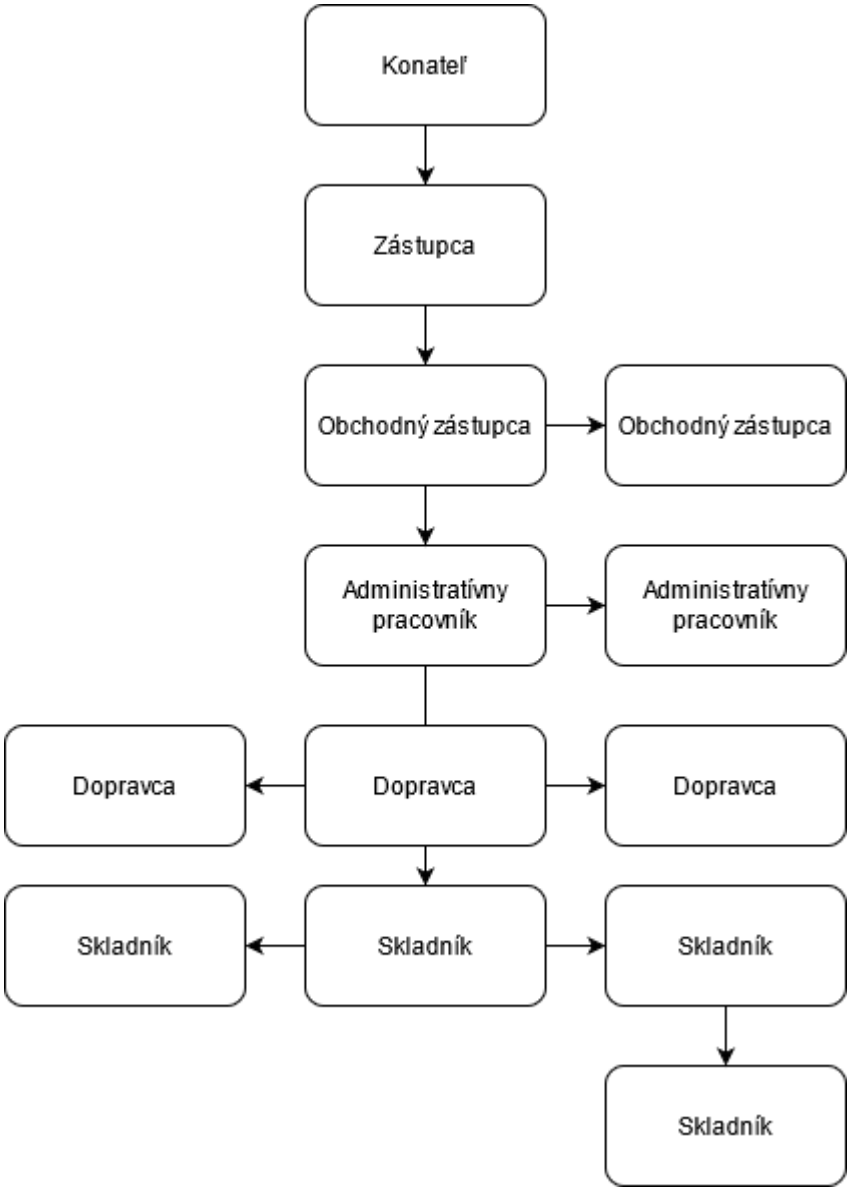
Daná spoločnosť KRÍDLA s.r.o, ktorá je predmetom skúmania tejto práce je pokračovateľom veľkoobchodnej činnosti firmy Krídla VEĽKOOBCHOD. Vznik tejto firmy je v r. 1991 so sídlom v Prešovskom kraji konkrétne v meste Humenné. Jej hlavnou podnikateľskou činnosťou je dodávanie širokého sortimentu do škôl, kancelárií, úradov a podobne. V súčasnosti ponúka široký sortiment tovaru ako je :

- Školské a kancelárske potreby
- Drogéria
- Obaly a puzdra
- Batérie a žiarovky
- Atramentové kazety a tonery
- Pečiatky

Táto prosperujúca firma sa na trhu s drží hlavne vďaka pravidelne udržiavaným kontraktom pre úrady, školstvo, firmy a taktiež vďaka cenám dodávky, ktoré má nízke. Ponúkaný sortiment dodáva nielen v rámci svojho sídla ale tiež aj do miest ako sú Košice či Prešov. (11)

2.1.1 Organizačná štruktúra

Konateľ danej spoločnosti momentálne zamestnáva 11 zamestnancov. Dvaja z nich sa venujú administratívnej činnosti, ktorá zahŕňa najmä predaj a vybavujú tiež spisovú agendu všetkého druhu. Ďalší dvaja pracujú na pozícii obchodných zástupcov. Ich hlavná úloha spočíva v cestovaní, získavaní klientov a vybavovaní kontraktov pre firmu. Medzi dôležité pracovné miesta vo firme patrí tiež pozícia skladníka (4) a vodiča (3). Náplňou práce skladníka je príprava a naloženie objednaného tovaru, ktorý vodič následne dodá zákazníkovi.



Obrázok 7: Organizačná štruktúra (zdroj: vlastné spracovanie)

2.1.2 Sídlo

Sídlo spoločnosti sa nachádza na východe Slovenska, v meste Humenné. Všetky priestory ako sklady a kancelárie sú umiestnené v areáli. Pri vstupe do areálu je veľké parkovisko a hlavný vstup do budovy. Jedná sa o jednoposchodovú budovu červenej farby, kde na prednej stene je tiež umiestnené logo spoločnosti. V prednej časti budovy sú kancelárske priestory a vzorkovňa a tie sú prepojené so zadnou časťou kde sa nachádzajú sklady s tovarom. V zadnej časti areálu sú vstupy do skladov, slúžiace aj na príjem a výdaj tovaru. Celý areál je oplotený a chránený kamerovým systémom a alarmom. Vždy po zatvorení firmy sa celý areál uzamkne a aktivuje sa alarm. V areáli sú tiež 2 strážne psy.

2.1.3 HW

Spoločnosť disponuje 9 pracovnými stanicami od spoločnosti Lenovo. Jedná sa o 4 notebooky a 5 stolných počítačov. Jeden z počítačov a tiež notebook sa nachádzajú v kancelárii konateľa spoločnosti. Ďalšie 4 zariadenia sa nachádzajú vo vedľajšej miestnosti a sú určené pre obchodných zástupcov a administratívnych pracovníkov. Posledné 2 zariadenia sa nachádzajú priamo v sklade a sú určené pre všetkých zamestnancov na to, aby si vedeli dohľadať zostatok a tiež zistiť umiestnenie tovaru.

Stolový počítač je Lenovo V530 v prevedení Tower a notebooky sú Lenovo ThinkPad E580.

Obrázok 8: Lenovo V530(zdroj: (12))

- CPU - Intel Core i3 8100 Coffee Lake
- GPU - Intel UHD Graphics 630
- HDD – 1TB 7 200 ot./min
- RAM – 4GB DDR4 2400 Mhz

Obrázok 9: ThinkPad E580(zdroj: (13))

- CPU - Intel Core i5 8250U Kaby Lake R
- GPU - Intel UHD Graphics 620
- HDD – 1TB 5 400 ot./min
- RAM – 8GB DDR4 2400Mhz

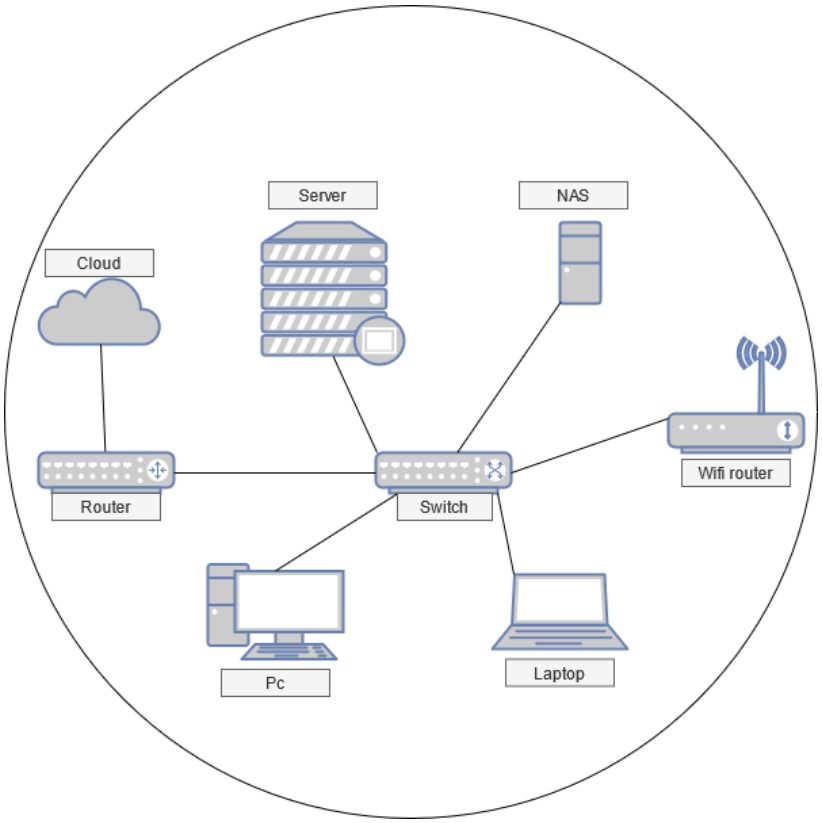
2.1.4 SW

Spoločnosť pracuje len s jedným operačným systémom. Na každom počítačovom zariadení či už stolovom počítači alebo notebooku je nainštalovaný operačný systém Windows 10 .

2.1.5 Sieť

V spoločnosti je využívané jednoduché zapojenie siete, ktorá je rozdelená na jednu podsieť. Toto riešenie bolo zavedené v takomto režime z dôvodu, že v spoločnosti

sa nezdržiavajú zákazníci. Práve preto nie je potrebné rozdelenie na viacero podsieti z hľadiska bezpečnosti. Všetky zariadenia sú pripojené na sieť cez switch. Aby bola pokrytá celá prevádzka, sú tam zavedené a využívané dve wifi zariadenia.



Obrázok 10: Zapojenie siete (zdroj: vlastné spracovanie)

2.1.6 Serverovňa

Na server v spoločnosti je vyčlenená samostatná miestnosť, ktorá sa nachádza na prevádzke. Prístup je možný len v doprovode konateľa spoločnosti, ktorý je ako jediný vlastník prístupového kľúča. Miestnosť je pravidelné čistená a klimatizovaná. Na servery je nainštalovaný operačný server windows server 2008. Údržbu a správu servera má na starosti externá firma z Prešova.

2.1.7 Zálohovanie

Zálohovanie danej spoločnosti je riešené tromi spôsobmi. Prvý spôsob zahŕňa zálohovanie všetkých pracovných staníc na server, ktorý sa nachádza v oddelenej

miestnosti v priestoroch hlavnej budovy. Druhý a tretí spôsob sa sústredí na zálohovanie dát zo skladového systému, ktoré sú pre firmu najkritickejšie. Jedná sa o zariadenie NAS, ktoré je umiestnené v kancelárií konateľa spoločnosti a na druhú zálohu sú využívané priestory cloudu od Googlu. Všetky spomenuté zálohy sa vykonávajú v 24h intervaloch a to vždy až po ukončení pracovnej smeny. Prvá záloha bola úplná a zvyšne prírastkové. Konateľ spoločnosti si taktiež každý deň zálohuje dáta na vlastné USB zariadenie. Najkritickejšie dáta spoločnosti sú uchované v 4 kópiách.

2.2 Analýza vybraných procesov

Na to aby sme mali prehľad o momentálnej situácii v rámci bezpečnostných opatrení spoločnosti nám slúži analýza podľa normy ISO/IEC 27036, ktorá udáva prehľad o už používaných opatreniach vo firemných procesoch. Pre lepšiu prehľadnosť je analýza spracovaná v tabuľkách. V ľavom hornom rohu je uvedený názov analyzovanej oblasti a na pravej strane od názvu je dané, či sa jedna o proces z hľadiska dodávateľa, nadobúdateľa alebo to platí rovnako v oboch prípadoch. V riadku pod tým sa v ľavej časti nachádza otázka, zisťujúca aktuálny stav procesu a na pravej strane je už uvedený stav so zadefinovanými možnosťami. Možnosti aké ma stav definované sa nachádzajú pod tabuľkou.

Názov oblasti	Dodávateľ/Nadobúdateľ
Otázka	Stav

Stav ma definované tieto možnosti – áno, čiastočne, nie

2.2.1 Proces dohody

Organizácie môžu nadobúdať rôzne dodávateľské vzťahy. Vhodné vzťahy medzi nadobúdateľmi a dodávateľmi sa dosahujú nielen pomocou dohôd definujúcich úlohy ale aj pomocou zodpovednosti v oblasti bezpečnosti informácií s ohľadom na dodávateľský vzťah.

Proces akvizície	Nadobúdateľ
Je vytvorená stratégia na riadenie vzťahu s dodávateľmi ?	ANO
Je daná stratégia vybudovaná na tolerancii rizika informačnej bezpečnosti ?	NIE
Je vytvorený rámec kritérií na hodnotenie riadenia bezpečnosti dodávateľov ?	NIE

Proces dodávky	Dodávateľ
Je vytvorená stratégia vzťahu s nadobúdateľmi ?	ANO
Je daná stratégia založená na tolerancii k riziku informačnej bezpečnosti ?	NIE
Je vytvorený rámec kritérií na hodnotenie riadenia bezpečnosti nadobúdateľov ?	NIE

2.2.2 Procesy umožňujúce realizáciu projektu

Pri organizácií projektu sú tiež veľmi dôležité procesy, ktoré nám umožňujú daný projekt zrealizovať. Tie sa zaoberajú zabezpečením toho, aby zdroje (finančné, ľudské...) potrebné pri realizácií projektu spĺňali potreby a očakávania zainteresovaných strán

Riadenie infraštruktúry	Nadobúdateľ
Poskytuje spoločnosť fyzickú bezpečnostnú infraštruktúru ?	ČIASTOČNE
Poskytuje spoločnosť logickú bezpečnostnú infraštruktúru ?	ČIASTOČNE
Má spoločnosť definované pohotovostné opatrenia v dodávateľských vzťahoch ?	NIE

Riadenie portfólia projektu	Dodávateľ
Kategorizuje spoločnosť dodávateľov podľa citlivosti informácií ?	ČIASTOČNE
Posudzuje bezpečnosť informácií ?	NIE

Riadenie ľudských zdrojov	Dodávateľ
Má spoločnosť zaistené potrebné ľudské zdroje ?	ANO
Majú potrebné kompetencie na pracú s informáciami ?	ANO
Majú informácie a znalosti ktoré sú v súlade s potrebami informačnej bezpečnosti v dodávateľských vzťahoch ?	ČIASTOČNE

Riadenie kvality	Dodávateľ
Má spoločnosť zavedený proces riadenia kvality pri riadení informačnej bezpečnosti v dodávateľských vzťahoch ?	NIE

2.2.3 Projektové procesy

Dôsledným riadením a podporou projektu ktoré pokrývajú jedného alebo viacerých dodávateľov sa zaoberajú takzvané projektové procesy.

Plánovanie projektu	Dodávateľ
Má spoločnosť zavedený proces plánovania projektu, zameraný na informačnú bezpečnosť ?	NIE

Posúdenie a proces kontroly projektu	Nadobúdateľ
Má spoločnosť ako nadobúdateľ alebo ako dodávateľ zavedený proces posudzovania a kontroly projektu pri riadení informačnej bezpečnosti v dodávateľských vzťahoch	NIE

Riadenie rozhodnutí	Dodávateľ
Je v spoločnosti zavedený proces ktorý rozhoduje o kvalite informačnej bezpečnosti v dodávateľských vzťahoch	NIE

Riadenie rizík	Nadobúdateľ
Je v spoločnosti vypracovaný rámec rizík informačnej bezpečnosti ?	ČIASTOČNE
Posudzuje spoločnosť obchodných partnerov z hľadiska informačnej bezpečnosti ?	ĆIASTOČNE
Má spoločnosť spravený zoznam aktív ?	NIE
Sú k aktívam priradený vlastníci ?	NIE

Riadenie konfigurácie	Nadobúdateľ
Je zavedený proces na riadenie konfigurácie pri správe informačnej bezpečnosti v dodávateľských vzťahoch ?	NIE

Riadenie informácií	Dodávateľ
Sú v spoločnosti role a zodpovednosti bezpečnosti informácií ?	ANO
Je vytvorená bezpečnostná politika na prístup k informáciám ?	ČIASTOČNE

Sú hodnotené informácie podľa ich citlivosti ?	ANO

Proces merania	Dodávateľ
Je zavedený proces merania ktorý analyzuje opatrenia na zabezpečenie informácií ?	NIE
Je zavedený proces na preukázanie vyspelosti informačnej bezpečnosti v dodávateľských vzťahoch ?	NIE
Je vytvorený proces ktorý podporuje efektivitu riadenia procesov ?	NIE

2.2.4 Plánovanie vzťahov

Vzťah z dodávateľmi	Nadobúdateľ
Je vytvorený plán vzťahov s dodávateľmi ?	ČIASTOČNE
Rieši plán informačnú bezpečnosť v dodávateľskom vzťah	ČIASTOČNE
Je v tom pláne zahrnutý plán obnovy ?	NIE

2.2.5 Výber dodávateľa

Proces výberu dodávateľa	Nadobúdateľ
Je pri výbere dodávateľa braný ohľad na jeho informačnú bezpečnosť ?	ČIASTOČNE
Existujú kritéria pri výbere dodávateľa ?	ANO
Je vytvorený tender na výber dodávateľa ?	NIE
Je vytvorená dohoda o mlčanlivosti ?	ČIASTOČNE

2.2.6 Dohody o dodávateľských vzťahoch

	Nadobúdateľ
Je podpísaná dohoda o vzťahu s dodávateľom zabezpečená ?	ANO
Je vytvorený postup riadenia zmien v informačnej bezpečnosti ?	NIE
Je vytvorený postup riadenia incidentov v oblasti bezpečnosti informácií ?	NIE
Sú vytvorené mechanizmy zničenia informácií ?	ČIASTOČNE
Je vytvorený plán ukončenia ?	NIE
Je vytvorený prechodný plán ?	NIE

2.2.7 Riadenie dodávateľských vzťahov

	Nadobúdateľ
Je vytvorený auditný plán ?	NIE
Je vedená história zmien informačnej bezpečnosti ?	NIE
Je vytvorený zoznam nápravných opatrení ?	NIE

2.2.8 Ukončenie dodávateľských vzťahov

	Nadobúdateľ
Je vytvorený komunikačný plán súvisiaci s ukončením dodávky	NIE
Je vymenovaná osoba, zodpovedná za ukončenie dodávky produktu alebo služby ?	ANO
Existujú osvedčenia o zničení majetku ?	NIE

Je vytvorená správa o vykonaní odstránenia logických a fyzických prístupových práv ?	NIE

2.3 Súhrn analýzy

Z tejto analýzy vyplýva, že spoločnosť veľmi nedbá na bezpečnosť informácií v dodávateľských vzťahoch.

V rámci procesu akvizície a dodávky má spoločnosť vytvorenú stratégiu na riadenie a to rovnako z pozície nadobúdateľa aj dodávateľa. Na druhej strane ani v jednej pozícii nemá spoločnosť zabezpečenú danú stratégiu a to z pohľadu tolerancie k riziku informačnej bezpečnosti. Zistili sme tiež, že rámec kritérií na hodnotenie riadenia bezpečnosti nadobúdateľov v tejto spoločnosti chýba.

V oblasti riadenia infraštruktúry spoločnosť len čiastočne poskytuje logickú a fyzickú bezpečnosť, no čo sa týka pohotovostných opatrení v dodávateľských vzťahoch, tak tie spoločnosť zadefinované nemá. Keď sme sa pozreli na riadenie portfólia projektu, tak v tomto smere spoločnosť len čiastočne kategorizuje dodávateľov podľa citlivosti informácií, ale bezpečnosť informácií neposudzuje vôbec. Spomínané riadenie projektu je síce zanedbávané, no riadenie ľudských zdrojov má spoločnosť zaistené. Sú tam zahrnuté aj potrebné kompetencie na prácu s informáciami a čiastočne informácie a znalosti, ktoré sú v súlade s potrebami informačnej bezpečnosti v dodávateľských vzťahoch. Tak ako boli zanedbané predošlé procesy v rámci zabezpečenia informácií je taktiež zanedbaný aj proces riadenia kvality.

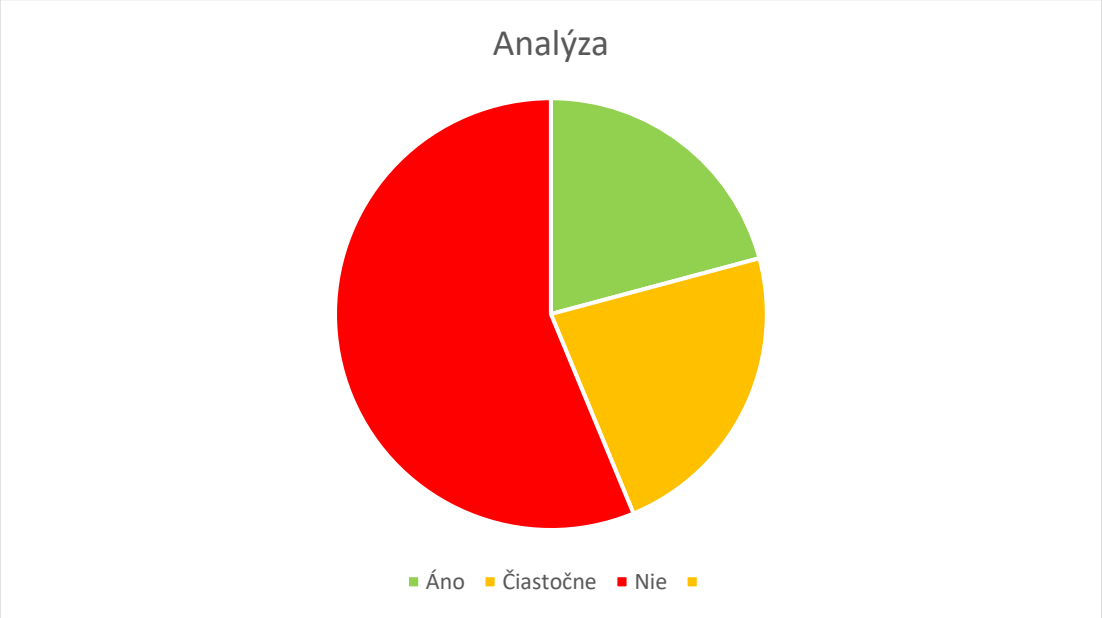
Na začiatku je veľmi dôležité plánovanie projektu, ktoré je v spoločnosti zanedbané. Firma zanedbala nie len spomínané plánovanie, ale aj posúdenie a proces kontroly a tiež proces ktorý rozhoduje o kvalite pri riadení informačnej bezpečnosti v dodávateľských vzťahoch. Pri realizácií takéhoto projektu je tiež dôležité klásť dôraz na možné riziká. Práve z tohto dôvodu má firma aspoň čiastočne vypracovaný plán na riadenie rizík a tiež posudzuje obchodných partnerov z hľadiska informačnej bezpečnosti. Vytváranie projektov tiež spočíva v klasifikácií a overovaní potrebných informácií. Firma si v tejto oblasti určila role a zodpovednosti, venovala sa a hodnotila informácie podľa ich citlivosti, no bezpečnostná politika na prístup k daným informáciám je riešená

len okrajovo. Meraniu opatrení, preukázaniu vyspelosti informačnej bezpečnosti a efektivite riadenia procesov na zabezpečenie informácií sa firma nevenuje vôbec.

Pri plánovaní dodávateľských vzťahov sme zistili, že firma nemá dostatočne zabezpečené a podchytené vytváranie daných vzťahov. Spoločnosť má medzery už v počiatočnom procese a to pri výbere dodávateľa, kde len čiastočne berie ohľad na jeho informačnú bezpečnosť, no tender na výber nie je zadefinovaný vôbec. Naopak má však zadefinované aspoň isté kritéria pri spomínanom výbere a tiež čiastočne vytvorenú dohodu o mlčanlivosti. Hoci dohoda o vzťahu s dodávateľom je zabezpečená, postup riadenia zmien a incidentov tu zasa absentuje. Tiež tu vôbec nie je vytvorený plán ukončenia, prechodný plán a v rámci riadenia dodávateľských vzťahov ani auditný plán. Firma si nevedie históriu zmien informačnej bezpečnosti a nemá tiež vytvorený zoznam nápravných opatrení.

V poslednom kroku realizácie projektu, do ktorého spadá ukončenie dodávateľských vzťahov, nie je vytvorený ani komunikačný plán súvisiaci s ukončením dodávky, neexistujú žiadne osvedčenia o zničení majetku a jediné čo má v tomto bode firma podchytené je že má vymenovanú osobu, ktorá je zodpovedná za ukončenie dodávky.

Z celkového počtu analýzy spoločnosť splňuje 9 požiadavkou, nespĺňa 28 požiadavkou a čiastočne splňuje 12.



Obrázok 11: Koláčový graf plnenia opatrení (zdroj: vlastné spracovanie)

3 VLASTNÉ NÁVRHY NA RIEŠENIE

Táto kapitola vlastného návrhu riešenia sa delí do niekoľkých častí. Prvá časť sa zameriava na rozsah a hranice ISMS, ktoré sú vysvetlené v teoretickej časti tejto práce. Ďalšia kapitola sa venuje analýze rizík, kde sú v úvode identifikované aktíva a hrozby a následne ich zraniteľnosti. Po porovnaní všetkých troch údajov dostaneme maticu rizík, ktorá slúži ako záchytný bod pre spoločnosť na ktoré hrozby a aktíva je potreba si dať najväčší pozor. Podľa výsledkov analýzy sú navrhnuté opatrenia vyplývajúce z normy ISO/IEC 27036 a ich následná časová implementácia a ekonomické zhodnotenie

3.1 Rozsah a hranice ISMS

Na začiatok je potrebné uviesť že cieľom práce je zavedenie vybranej časti ISMS. Keďže spoločnosť ma stabilné miesto na trhu a slabé povedomie o problematike informačnej bezpečnosti v dodávateľských vzťahoch, sú pre túto prácu vybrané opatrenia na zlepšenie firemných procesov podľa normy ISO/IEC 27036, ktorá sa zaoberá problematikou bezpečnosti v dodávateľských vzťahoch.

Každý dodávateľský vzťah v organizácií má konkrétny účel. S rastom každej firmy, rastie aj počet dodávateľských vzťahov. Veľké firmy majú zvyčajne mnoho takýchto vzťahov, keďže sú v pozícií nadobúdateľa a majú vysoký počet produktov a služieb od iných spoločností. V bode, kedy má spoločnosť mnoho takýchto vzťahov, je pre ňu čoraz ťažšie zabezpečiť, aby riziká informačnej bezpečnosti, ktoré vznikajú v rámci týchto dodávateľských vzťahov boli primerané monitorované a riešené.

Pri podpore a dodávaní produktu alebo služby je dôležité dbať na prenesené informácie na druhú stranu. Tieto informácie musia byť primerane chránené prostredníctvom uzatvorenia dohody medzi nadobúdateľom a dodávateľom. Daná dohoda by mala obsahovať súbor kontrol a zodpovedností, ktoré boli vzájomne dohodnuté. Absencia takejto dohody môže mať vplyv na informačnú bezpečnosť jednej zo zainteresovaných strán.

3.2 Analýza rizík

S analýzou rizík sa pracuje hlavne za účelom identifikácie zraniteľných miest organizácie a môže slúžiť aj rovnako ako záchytný bod pre spoločnosť, na čo si dať pri riadení bezpečnosti pozor.

V prvej časti sú identifikované aktíva a následné ich ohodnotenie. Ďalej sa sú spomenuté nájdené hrozby a pravdepodobnosť ich vzniku. Na konci analýzy sa nachádza matica rizík ktorá zhodnocuje jej výsledky.

3.2.1 Identifikácia aktív

V tejto kapitole sú identifikované aktíva a ich následné ohodnotenie. Pre účely tejto práce je zvolené klasické delenie do štyroch skupín – dáta, hardware, software a služby kde sa primárne zameriavame na dodávateľské vzťahy, teda služby.

Tabuľka 1: Klasifikačné schéma pre hodnotenie aktív (zdroj: vlastné spracovanie)

Klasifikačné kritérium	Klasifikačný stupeň
Žiadny dopad	1
Zanedbateľný dopad	2
Stredný dopad na spoločnosť	3
Vážny dopad na spoločnosť	4
Existenčné problémy	5

Na výpočet hodnoty aktíva bol použitý nasledujúci algoritmus :

$$\frac{(Dôvernosť + Integrita + Dostupnosť)}{3}$$

Tabuľka 2: Identifikácia a hodnotenie aktív (zdroj: vlastné spracovanie)

Typ	Aktivum (A)	Zdroj	Dôvernosť	Integrita	Dostupnosť	Hodnota
Dáta	Dáta o zamestnancoch	Server, Pc	4	3	3	3
	Dáta o zákaznikoch	Server, Pc	5	3	3	4
	Skladové dáta	Server, Pc	4	5	5	5
	Zálohy	Server, cloud, NAS	5	5	5	5
Hardware	Pracovné stanice		3	2	3	3
	Server		5	5	5	5
	NAS		5	5	5	5
Software	Operačný systém	Server, Pc	4	4	4	4
	Tangram	Server, Pc	3	5	5	4
	Antivírusový software		4	5	5	5
	Webdispečing	Pc	2	2	2	2
Služby	Elektrická energia	Sídlo	3	3	4	3
	Internetové pripojenie	Sídlo	3	3	5	4
	Cloudové služby	Poskytovateľ	5	5	5	5
	Ekonomické služby	Server	5	5	4	5
	Doménové služby	Server	5	1	1	2
	Dodávateľské služby	Poskytovateľ	3	3	3	3
	Upratovacie služby	Poskytovateľ	2	2	2	2
	Tangram support	Poskytovateľ	5	5	5	5
	Webdispečing support	Poskytovateľ	2	2	2	2
	IT support	Poskytovateľ	5	4	5	5

Z výsledkov identifikácie a hodnotenia aktív nám vyplýva, že najkritickejšie pre spoločnosť sú tie aktíva, ktoré sa pohybujú okolo záloh a skladových dát. Spomínané dáta sa nachádzajú na servery a sú zálohované na cloud a NAS. Zo služieb je potrebné upriamiť pozornosť na ekonomické služby, IT support a Tangram support, ktoré majú prístup ku kritickým dátam a sú zraniteľné. Ak by tieto služby neboli k dispozícii alebo nedostatočne zabezpečené, mohlo by spoločnosti spôsobiť veľké škody.

3.2.2 Identifikácia hrozieb a zraniteľnosti

Táto časť sa zaoberá identifikáciou hrozieb. Na začiatku je vždy veľmi dôležité určiť o aký typ hrozby sa jedná. Následne je k hrozbám priradená ich pravdepodobnosť a príklad, ktorý môže nastať. Výstupom identifikácie hrozieb je ich pravdepodobnosť ktorá nám slúži na výpočet rizika v matici nižšie.

Tabuľka 3: Identifikácia hrozieb (zdroj: Vlastné spracovanie)

Typ	Hrozba
Fyzický prístup	Zničenie zariadenia
	Zlyhanie zariadenia
	Krádež zariadenia
Prístup k informáciam a informačným systémom na pracovisku	Neumýselné poškodenie dát na pracovisku
	Neoprávanené použitie zariadenia
	Krádež dát z pracoviska
Vzdialený prístup k informáciám a informačným systémom	Neumýselné poškodenie dát cez vzdialený prístup
	Zneužitie prístupu do IS
	Zlyhanie služieb
Spracovanie informácií mimo pracoviska	Nezákonné spracovanie dát mimo pracoviska
	Falšovanie dát mimo pracoviska
Ukladanie dát mimo pracoviska	Únik dát uložených mimo pracoviska

Klasifikačná schéma pravdepodobnosti výskytu daných hrozieb je hodnotená podľa nasledujúcej schémy

Tabuľka 4: Klasifikačná schéma pravdepodobnosti (zdroj: vlastné spracovanie)

Pravdepodobnosť hrozby	Klasifikačný stupeň
Náhodná	1
Nepravdepodobná	2
Pravdepodobná	3
Veľmi pravdepodobná	4
Trvalá	5

Tabuľka 5: Zoznam hrozieb s ich pravdepodobnosťou (zdroj: vlastné spracovanie)

Hrozba	P	Príklad hrozby
Zničenie zariadenia	1	Poškodenie hrubou silou
Zlyhanie zariadenia	3	Nedostatnčná údržba zariadenia
Krádež zariadenia	2	Nedostatočné zabezpečenie zariadenia
Neumýselné poškodenie dát na pracovisku	3	Slabo zaškolený personál
Neoprávnené použitie zariadenia	2	Zmazanie neuležných zmien
Krádež dát z pracoviska	2	Nedostatočné prístupové povolenia
Neumýselné poškodenie dát cez vzdialený prístup	3	Nedostatok povedomia o bezpečnosti
Zneužitie prístupu do IS	3	Prístup k interným dátam spoločnosti
Zlyhanie služieb	4	Útok škodlivým kódom
Nezákonné spracovanie dát mimo pracoviska	3	Zlé zaoškolený personál dodávateľa
Falšovanie dát mimo pracoviska	3	Nedostatočná bezpečnosť Pc u dodávateľa
Únik dát uložených mimo pracoviska	5	Poškodenie mena spoločnosti

Stredný stĺpec s označením „P“ nám udáva pravdepodobnosť danej hrozby.

3.2.3 Matica zraniteľnosti

Matica zraniteľnosti nám slúži na odhalenie slabého miesta. Zraniteľnosť sa určuje na základe pravdepodobnosti danej hrozby a k tomu priliehajúceho aktíva. Na odhad zraniteľnosti je použitá nasledujúca klasifikačná tabuľka.

Tabuľka 6: Klasifikačná schéma zraniteľnosti (zdroj: vlastné spracovanie)

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

Tabuľka 7: Matica zraniteľnosti (zdroj: vlastné spracovanie)

Zraniteľnosť [V]		Zdroj	Dáta				Hardware			Software				Služby									
		Aktívum	Dáta o zamestnancoch	Dáta o zákazníkoch	Skladové dáta	Zálohy	Pracovné stanice	Server	NAS	Operačný systém	Tangram	Antivírusový software	Webdispečing	Elektrická energia	Internetové pripojenie	Cloudové služby	Ekonomické služby	Doménové služby	Dodávateľské služby	Upratovacie služby	Tangram support	Webdispečing support	It Support
		Zdroj	Server, Pc	Server, Pc	Server, Pc	Server, cloud, Nas				Server, Pc	Server, Pc	Server, Pc	Pc	Sídlo	Sídlo	Poskytovateľ	Server	Server	Poskytovateľ	Poskytovateľ	Poskytovateľ	Poskytovateľ	Poskytovateľ
		A	3	4	5	5	3	5	5	4	4	5	2	3	4	5	5	2	3	2	5	2	5
Hrozba	T																						
Zničenie zariadenia	1		0	0	0	0	2	3	3	0	0	0	0	0	0	0	0	0	0	2	0	0	2
Zlyhanie zariadenia	3		0	0	0	0	3	4	4	0	0	0	0	0	0	0	0	0	0	2	0	0	3
Krádež zariadenia	2		0	0	0	0	2	3	3	0	0	0	0	0	0	0	0	0	0	2	0	0	2
Neumýselné poškodenie dát na pracovisku	3		3	3	4	4	3	4	3	2	4	4	2	0	0	0	0	0	0	2	0	0	4
Neoprávnené použitie IS na pracovisku	2		3	4	3	2	3	3	3	2	3	3	2	0	0	0	0	0	0	2	0	0	4
Krádež dát z pracoviska	2		2	3	4	4	3	3	3	3	3	3	2	0	0	0	0	0	0	2	0	0	3
Neumýselné poškodenie dát cez vzdialený prístup	3		3	3	4	4	3	4	4	3	3	3	2	2	3	0	5	3	2	0	5	2	4
Zneužitie prístupu do IS cez vzdialený prístup	3		3	3	4	4	3	4	4	3	3	3	2	2	3	0	5	3	2	0	5	2	4
Zlyhanie služieb	4		0	0	0	0	3	4	4	3	3	5	2	3	4	5	4	3	2	0	5	0	5
Nezákonné spracovanie dát mimo pracoviska	3		3	3	4	4	0	0	0		4	0	0	0	1	3	3	3	4	0	4	3	4
Falšovanie dát mimo pracoviska	3		4	5	4	2	0	0	0		5		0	0	1	4	4	4	4	0	5	2	5
Únik dát uložených mimo pracovisko	4		0	0	0	5	0	0	0		0	0	0	0	0	5	4		4	3	5	2	5

3.2.4 Matica rizík

Na výpočet rizika bola zvolená metóda ktorý využíva tri parametre A, T, V. Každé z týchto písmen predstavuje : A – hodnota aktíva, T – pravdepodobnosť hrozby a V – zraniteľnosť aktíva danou hrozbou. Po vynásobení týchto parametrov dostaneme hodnotu v rozmedzí 0 – 125.

Klasifikácia rizík je udelená podľa nasledujúcej schémy.

Tabuľka 8: Klasifikačná schéma pre úroveň rizika (zdroj: vlastné spracovanie)

Úroveň rizika	Klasifikačný stupeň
Bezvyznamné riziko	0-10
Akceptovateľné riziko	11-20
Nízke riziko	21-30
Nežiadúce riziko	31-60
Neprijateľné riziko	61-125

Tabuľka 9: Matica rizík (zdroj: vlastné spracovanie)

Zraniteľnosť [V]		Dáta				Hardware			Software				Služby									
Zdroj		Server, Pc	Server, Pc	Server, Pc	Server, cloud, Nas				Server, Pc	Server, Pc	Server, Pc	Pc	Sídlo	Sídlo	Poskytovateľ	Server	Server	Poskytovateľ	Poskytovateľ	Poskytovateľ	Poskytovateľ	Poskytovateľ
Aktívum		Dáta o zamestnancoch	Dáta o zákazníkoch	Skladové dáta	Zálohy	Pracovné stanice	Server	NAS	Operačný systém	Tangram	Antivírusový software	Webdispečing	Elektrická energia	Internetové pripojenie	Cloudové služby	Ekonomické služby	Doménové služby	Dodávateľské služby	Upratovacie služby	Tangram support	Webdispečing support	It Support
	A	3	4	5	5	3	5	5	4	4	5	2	3	4	5	5	2	3	2	5	2	5
Hrozba	T																					
Zničenie zariadenia	1					6	15	15														10
Zlyhanie zariadenia	3					27	60	60											12			45
Krádež zariadenia	2					12	30	30											8			20
Neumýselné poškodenie dát na pracovisku	3	27	36	60	60	27	60	45	24	48	60	12							12			60
Neoprávnené použitie IS na pracovisku	2	18	32	30	20	18	30	30	16	24	30	8							8			40
Krádež dát z pracoviska	2	12	24	40	40	18	30	30	24	24	30	8							8			30
Neumýselné poškodenie dát cez vzdialený prístup	3	27	36	60	60	27	60	60	36	36	45	12	18	36		75	18	18		75	12	60
Zneužitie prístupu do IS cez vzdialený prístup	3	27	36	60	60	27	60	60	36	36	45	12	18	36		75	18	18		75	12	60
Zlyhanie služieb	4					36	80	80	48	48	100	16	36	64	100	80	24	24		100		100
Nezákonné spracovanie dát mimo pracoviska	3	27	36	60	60					48				12	45	45	18	36		60	18	60
Falšovanie dát mimo pracoviska	3	36	60	60	30					60				12	60	60	24	36		75	12	75
Únik dát uložených mimo pracovisko	4				100										100	80		48	24	100	16	100

3.2.5 Zhodnotenie

Tabuľka 10: Neprijateľné riziká (zdroj: vlastné spracovanie)

Hrozba	Úroveň rizika	Aktívum	Zdroj
Neúmyselné poškodenie dát cez vzdialený prístup	75	Ekonomické služby	Server
	75	Tangram support	Poskytovateľ
Zneužitie prístupu do IS cez vzdialený prístup	75	Ekonomické služby	Server
	75	Tangram support	Poskytovateľ
Zlyhanie služieb	80	Server	
	80	NAS	
	100	Antivírusový software	Server, Pc
	64	Internetové pripojenie	Sídlo
	100	Cloudové služby	Poskytovateľ
	80	Ekonomické služby	Server
	100	Tangram support	Poskytovateľ
	80	It support	Poskytovateľ
Falšovanie dát mimo pracoviska	75	Tangram support	Poskytovateľ
Únik dát uložených mimo pracoviska	100	Zálohy	Server, Cloud, NAS
	100	Cloudové služby	Poskytovateľ
	80	Ekonomické služby	Server
	100	Tangram support	Poskytovateľ
	80	It support	Poskytovateľ

V tabuľke vyššie sú riziká, ktoré majú na spoločnosť najväčší dopad. Najzraniteľnejšie dáta sú pre spoločnosť skladové dáta, ktoré sa nachádzajú v zálohách. Zálohy sú uskladnené na serveri a na NAS. Na záver sa využíva cloudová služba na uloženie záloh. Z toho nám vyplýva, že najkritickejšie sú služby, ktoré majú prístup k týmto zariadeniam a k dátam samotným. Spoločnosť by mala brať v úvahu, že služby, ktoré využíva majú priamy prístup na server a do IS spoločnosti. Na to nám slúži norma ISO/IEC 27036, ktorá sa zoberá bezpečnosťou v dodávateľských vzťahoch

3.2.6 Výber bezpečnostných opatrení

Nasledujúce opatrenia boli vybrané na základe analýzy a požiadaviek firmy. Opatrenia sú vybrané podľa normy ISO/IEC 27036 a určujú aké procesy má spoločnosť vylepšiť alebo zaviesť aby bola bezpečnosť informácií v dodávateľských vzťahoch na vyššej úrovni.

Tabuľka 11: Bezpečnostné opatrenia (zdroj: vlastné spracovanie)

6. Riadenie informačnej bezpečnosti v dodávateľských vzťahoch
6.1 Proces dohody
6.1.1 Proces akvizície
6.1.2 Proces dodania
6.2 Organizačné procesy
6.2.2 Proces riadenia infraštruktúry
6.2.3 Proces správy portfólia projektu
6.2.4 Proces riadenia ľudských zdrojov
6.3 Projektové procesy
6.3.1 Proces plánovania projektu
6.3.4 Proces riadenia rizík
7. Informačná bezpečnosť v inštancii dodávateľského vzťahu
7.1 Proces plánovania dodávateľského vzťahu
7.2 Proces výberu dodávateľa
7.3 Proces dohody v dodávateľskom vzťahu
7.4 Proces riadenia dodávateľského vzťahu
7.5 Proces ukončenia dodávateľského vzťahu

3.3 Návrh bezpečnostných opatrení

V tejto kapitole je uvádzané riešenie opatrení podľa normy ISO/IEC 27036. Norma obsahuje rady pre spoločnosti ako má upraviť alebo zaviesť nové firemné procesy na riadenie bezpečnosti. Aby bolo jasne rozpoznateľné číslovanie kapitol práce od číslovania opatrení podľa danej normy, tak je každé opatrenie označené veľkým písmenom „A“. Forma je braná podľa znenia normy, kde na začiatku je určený cieľ

daného opatrenia a následné činnosti na splnenie daného cieľa. Pre lepšiu priehľadnosť je vytvorená tabuľka, ktorá určuje aký cieľ je potrebný na splnenie jednotlivých opatrení.

3.3.1 Proces dohody A.6.1

A.6.1.1 Proces akvizície

Cieľ : Vytvoriť plán vzťahu s dodávateľmi, ktorý je :
1. Založený na tolerancii rizika
2. Definuje základné pokyny dodržiavania bezpečnostných opatrení pri plánovaní, príprave, správe a ukončení obstarávania produktu (9)

Činnosti

a) Definovať, implementovať, udržiavať a zlepšovať stratégiu vzťahov s dodávateľmi, ktorá obsahuje :
    1. Motívy riadenia, potreby a očakávania pri obstarávaní produktov
    2. Záväzok manažmentu prideliť potrebné zdroje
    3. Rámec riadenia rizík v oblasti bezpečnosti informácií
    4. Rámec, ktorý sa má použiť pri definovaní požiadaviek na bezpečnosť informácií počas procesu plánovania dodávateľského vzťahu
    5. Rámec kritérií výberu dodávateľa, ktorý sa má použiť pri výbere dodávateľa
    6. Požiadavky na bezpečnosť informácií na vysokej úrovní
b) Vymenovať zodpovednú osobu, ktorá bude mať na starosti podmienky vymenované vyššie a zabezpečiť, aby bola daná osoba pravidelne a primerané trénovaná
c) Zabezpečiť, aby sa stratégia vzťahov s dodávateľmi prehodnocovala najmenej raz ročne.

A.6.1.2 Proces dodania

Cieľ : Vytvoriť plán, ktorý bude určovať vzťah s nadobúdateľom, ktorý je :
1. Založený na tolerancii rizika
2. Definuje základné pokyny dodržiavania bezpečnostných opatrení pri plánovaní, príprave, správe a ukončení obstarávania produktu (9)

Činnosti

d) Definovať, implementovať, udržiavať a zlepšovať stratégiu vzťahov s dodávateľmi ktorá obsahuje :
   1) Motívy riadenia, potreby a očakávania od dodávania produktov
   2) Záväzok manažmentu prideliť potrebné zdroje
   3) Rámec riadenia rizík v oblasti bezpečnosti informácií
   4) Rámec, ktorý sa má použiť pri definovaní požiadaviek na bezpečnosť informácií počas procesu plánovania dodávateľského vzťahu
   5) Rámec kritérií výberu dodávateľa, ktorý sa má použiť pri výbere dodávateľa
   6) Požiadavky na bezpečnosť informácií na vysokej úrovní

e) Vymenovať zodpovednú osobu, ktorá bude mať na starosti podmienky vymenované vyššie a zabezpečiť, aby bola daná osoba pravidelne a primerané trénovaná

f) Zabezpečiť, aby sa stratégia vzťahov s dodávateľmi prehodnocovala najmenej raz ročne.

3.3.2 Organizačné procesy A.6.2

A.6.2.2 Proces riadenia infraštruktúry

Cieľ : Pripraviť infraštruktúru, ktorá podporuje organizáciu pri riadení informačnej bezpečnosti v dodávateľských vzťahoch (9)

Činnosti

a) Definovať, implementovať, udržiavať a zlepšovať fyzickú a logickú bezpečnostnú infraštruktúru na ochranu majetku ako sú informácie a informačné systémy.
b) Definovať, implementovať, udržiavať a zlepšovať pohotovostné opatrenia, aby sa zabezpečilo, že obstarávanie alebo dodávka produktu alebo služby môže pokračovať v prípade prerušenia spôsobeného ľudskou alebo prírodnou príčinou.

A.6.2.4 Proces riadenia ľudských zdrojov

Cieľ : Zabezpečiť, aby spoločnosť ako nadobúdateľ ale aj ako dodávateľ mala k dispozícií potrebné ľudské zdroje, ktoré majú kompetencie a sú pravidelne udržiavané pre potreby informačnej bezpečnosti v dodávateľských vzťahoch. (9)

Činnosti

a) Zvážiť školenie o informačnej bezpečnosti ako časť procesu riadenia ľudských zdrojov .
    1) Pokyny a pravidlá bezpečnosti informácií, ako napríklad politika v oblasti bezpečnosti informácií, klasifikácia informácií, najmä pre pracovníkov ktorí sa priamo podieľajú na dodávateľských vzťahoch .
    2) Požiadavky na informačnú bezpečnosť, všeobecne definované v zmluve o dodávateľskom vzťahu, ktoré poukazujú na potreby a očakávania nadobúdateľa.

b) Identifikovať a zhodnotiť personál, vzhľadom na ich prístup a schopnosť zverejňovať alebo upravovať informácie v rámci dodávateľského vzťahu.
c) Zaistiť, aby klasifikovaný personál, najmä ten, ktorý sa zaoberá informačnou bezpečnosťou mal adekvátne kompetencie a kvalifikácie.
d) Školiť pracovníkov, aby zvládali prácu s citlivými informáciami a ako s nimi zaobchádzať.
e) Zabezpečiť, aby boli dôkladne a pravidelne vykonávané trestné kontroly a previerky osôb, ktoré zabezpečujú príjem kľúčových pozícií v dodávateľských vzťahoch, pokiaľ to umožňuje zákon.
f) Zaviesť a vymedziť záchytné body a ich zálohy pre kritické aspekty každého dodávateľského vzťahu, ktorý zahŕňa tiež prevádzku a údržby. Zabezpečiť tiež minimálny dopad v prípade odchodu personálu z organizácie.

3.3.3 Projektové procesy A.6.3

A.6.3.1 Proces plánovania projektu

Cieľ : Zaviesť proces riadenia projektu, zameraný na bezpečnosť informácií v dodávateľských vzťahoch. (9)

Činnosti

a) Zaviesť proces plánovania projektu, zameraný na informačnú bezpečnosť, ktorý by mal obsahovať :
    1) Vplyv na náklady projektu, plány a harmonogram požiadaviek na informačnú bezpečnosť pre aktíva, ktoré sú použité pri obstarávaní alebo dodávaní produktu alebo služby.
    2) Zakomponovanie informačnej bezpečnosti do príslušných projektových rolí.
    3) Zabezpečiť citlivé interné informácie, ktoré môžu byť narušené dodávateľským vzťahom.
    4) Zdroje, ktoré sú potrebné na zabezpečenie aktív .

Proces riadenia rizík A6.3.4

Cieľ : Neustále sa zameriavať na riziká informačnej bezpečnosti v dodávateľských vzťahoch a v rámci ich životného cyklu. Pravidelne ich preskúmavať, hlavne ak nastanú nejaké právne, politické alebo obchodné zmeny v zmluvách. (9)

Činnosti

a) Definovať, implementovať, udržiavať a zlepšovať rámec riadenia rizík informačnej bezpečnosti, ktorý definuje toleranciu rizík organizácie a môže byť použitý na identifikáciu, priradenie a zaobchádzanie bezpečnostných rizík, ktoré sprevádzajú :
    1) Existujúce prípady obstarávania či dodávania produktu alebo služby.
    2) Dodávatelia alebo nadobúdatelia zapojení v týchto prípadoch.

    Je potrebné dbať na to, aby bola jasne určená definícia tohto rámca :

    1) Sledovať smer podnikania danej spoločnosti, zvážiť právne, regulačné, architektonické, politické a zmluvné požiadavky platné pre spoločnosť.
    2) Posudzovať a zvážiť dodávateľov na základe :
        i. Histórie, napríklad predchádzajúcich a súčasných obchodných dohôd
        ii. Zmluvných dohôd (dohody o dodávateľských vzťahoch a dohody o mlčanlivosti)
        iii. Informačnej bezpečnosti
        iv. Schopnosti preukázať vyspelosť v informačnej bezpečnosti
b) Aplikovať tento rámec riadenia rizík informačnej bezpečnosti :
    1) Na klasifikáciu existujúcich prípadov obstarávania alebo dodávania produktu alebo služby
    2) Na klasifikáciu dodávateľov alebo nadobúdateľov zapojených v týchto prípadoch
    3) Kedy:

i. Pri definícií stratégie vzťahu medzi dodávateľom alebo nadobúdateľom
ii. Pri plánovaní obstarania alebo dodania produktu alebo služby

3.3.4 Proces plánovania dodávateľského vzťahu A7.1

Cieľ : Vytvoriť plán obsahujúci vzťahy s dodávateľmi, na ktorom je zdokumentované rozhodnutie prijaté vedením, ktoré iniciuje obstarávanie produktu alebo služby z hľadiska informačnej bezpečnosti týkajúce sa tohto obstarávania. (9)

Vstupy :

a) Stratégia vzťahov s dodávateľmi
b) Motívy, potreby a očakávania vedenia pri obstarávaní produktu alebo služby
c) Rozsah obstarávania produktov alebo služieb, ktoré sa plánujú obstarať
d) Existujúca dokumentácia riadenia vzťahov s dodávateľmi, napríklad plány vzťahov s dodávateľmi a dohody

Činnosti :

a) Identifikovať a vyhodnotiť riziká informačnej bezpečnosti, ktoré sprevádzajú obstarávanie produktu alebo služby založené na rámci riadenia rizík v oblasti bezpečnosti informácií :

Nadobúdateľ zabezpečí posúdenie rizika informačnej bezpečnosti na základe týchto podmienok:

1) Kritickosť produktu alebo služby
2) Právne a regulačné obmedzenia

b) Identifikovať prijateľnú úroveň rizík vzťahujúcich sa na potenciálny dodávateľsky vzťah
c) Identifikovať a vyhodnotiť možnosť liečby identifikovaných a vyhodnotených rizík

d) Definovať a implementovať plán liečby rizík v oblasti informačnej bezpečnosti pre identifikované a vyhodnotené riziká, ktoré sa majú zmierniť na prijateľnú úroveň rizika
e) Poradiť spoločnosti v rámci podnikania, konkrétne v oblasti hodnotenia rizík informačnej bezpečnosti a plánovania liečby ako vstupu do rokovania o dohode o vzťahu s dodávateľom
f) Definovať plán dodávateľských vzťahov pre produkt alebo službu, ktorá sa plánuje obstarať.

Plán dodávateľského vzťahu by mal obsahovať minimálne tieto požiadavky :

1) Špecifikácie výrobku alebo služby, ktoré sa majú obstarať, ich rozsah, druh a povaha
2) Aktíva, ako napríklad servery, databázy, aplikácie, sieťová infraštruktúra, ktoré majú význam bezpečnosti pri používaní
3) Vstupy klasifikácie informácií nadobúdateľa
4) Právne a regulačné požiadavky jurisdikcie nadobúdateľa a oblasti zákonov a predpisov
5) Úlohy a zodpovednosti v oblasti bezpečnosti informácií v rámci organizácie nadobúdateľa
6) Informácie nadobúdateľa, ktoré sú zdieľané s poskytovateľom služby
7) Minimálne požiadavky na bezpečnosť informácií, ktoré musia byť vopred dohodnuté s určeným dodávateľom na zabezpečenie produktu alebo služby. Tieto podmienky musia byť odvodené priamo z posúdenia rizika a plánu liečby v oblasti bezpečnosti informácií a mali by sa definovať aj vzhľadom na kritickosť produktu alebo služby.
    i. Klasifikácia informácií vykonaná nadobúdateľom
    ii. Požiadavky na bezpečnosť informácií definované v existujúcich dohodách

Všetky definované požiadavky by mali byť klasifikované s výrazom „NESMIE“ aby sa odlíšili od odporúčaní.

Výstupy:

a) Posúdenie rizík informačnej bezpečnosti a plán liečby spojený s produktom alebo službou ktoré sa majú obstarať
b) Zdokumentované rozhodnutie vedenia, v ktorom sa uvádza schválenie posúdenia rizika informačnej bezpečnosti a plán liečby. Spolu s informáciami musí byť zdokumentované aj rozhodnutie neobstarať si produkt alebo službu z bezpečnostných dôvodov, ktoré videli k tomuto rozhodnutiu
c) Plán vzťahov s dodávateľmi

3.3.5 Proces výberu dodávateľa A7.2

Cieľ: Vybrať dodávateľa, ktorý poskytuje primerané informačné zabezpečenie produktu alebo služby. (9)

Vstupy:

a) Stratégia vzťahu s dodávateľom
b) Plán vzťahu s dodávateľom
c) Existujúce kritéria výberu dodávateľa definované v obstarávaných produktoch alebo službách
d) Existujúce dohody o mlčanlivosti pri obstarávaní produktov alebo služieb

Činnosti:

a) Definovať a implementovať kritéria výberu dodávateľov, ktoré by mali obsahovať:
    1) Prijatie požiadaviek na informačnú bezpečnosť od dodávateľa, ktoré sú definované v tendri
    2) Splatnosť dodávateľa v oblasti zabezpečenia informácií, ktorú je možné žiadať od dodávateľa a to na základe certifikátu ISO/IEC 27001 alebo poskytnutie

3) Podmienky, ktoré určujú že môže byť dodávateľ auditovaný nadobúdateľom alebo 3. stranou na splnenie požiadaviek na bezpečnosť informácií
4) Akceptácia prechodu, keď produkt alebo službu, ktorá sa môže obstarať, už predtým prevádzkovala alebo vyrábala spoločnosť nadobúdateľom alebo iným dodávateľom
5) Prijatie výpovede na zachovanie bezpečnosti informácií v prípade vypovedania zmluvy
6) Správa kapacity dodávateľa
7) Finančná sila dodávateľa
8) Lokácia dodávateľa, od ktorého bude produkt alebo služba dodávaná. V tejto identifikácií danej lokácie je potrebné :
    i. Identifikovať všetky potenciálne právne riziká vyplývajúce z rozdielu v zákonoch a iných právnych predpisoch
    ii. Vyhodnotiť environmentálne hrozby ako je miestna kriminalita alebo geopolitické problémy a ich potencionálne dopady

b) Pripraviť dohodu o mlčanlivosti na ochranu aktív, informácií a informačných systémov nadobúdateľa
c) Pripraviť tender na výber dodávateľa ktorý by mal najmä obsahovať :
    1) Špecifikácie produktu alebo služby
    2) Požiadavky na bezpečnosť informácií, podľa ktorých sa má pri dodávaní postupovať
    3) Úrovne služieb alebo kľúčové ukazovatele výkonu poskytovateľa
    4) Pokuty, ktoré je možné udeliť poskytovateľovi v prípade nesúladu požiadaviek na bezpečnosť informácií
d) Zhromažďovať dokumenty obsahujúce odpovede od potenciálnych dodávateľov a na základe kritérií vyhodnotiť ich výber
e) Vybrať dodávateľa na základe vyhodnotenia týchto dokumentov

Výstupy:

a) Kritéria výberu dodávateľa

b) Dohoda o mlčanlivosti
c) Tender výberu dodávateľa
d) Výsledky vyhodnotenia dokumentov a odpovedí od dodávateľov
e) Výber potenciálneho dodávateľa, ktorý splnil kritéria

3.3.6 Proces dohody v dodávateľskom vzťahu A7.3

Cieľ : Uzavrieť dohodu o dodávateľskom vzťahu, ktorá sa zameriava na :
1) Úlohy a zodpovednosti informačnej bezpečnosti nadobúdateľa a dodávateľa
2) Proces prechodu ak bola služba alebo produkt predtým obstarávana inou stranou
3) Riadenie zmien v informačnej bezpečnosti
4) Správa incidentov informačnej bezpečnosti
5) Monitorovanie a presadzovanie súladu
6) Proces ukončenia (9)

Vstupy:

a) Stratégia vzťahov s dodávateľmi
b) Tender nadobúdateľa
c) Dokument s odpoveďou dodávateľa

Činnosti:

a) Definovať dohodu s druhou stranou o dodávateľských vzťahoch, špecifickú pre plánovanú dodávku produktu alebo služby. Táto dohoda by mala:
    1) Byť v súlade s dokumentom verejného tendra nadobúdateľa a s dokumentom odpovede dodávateľa obsahujúci:
        i. Požiadavky na bezpečnosť informácií, ktoré je potreba dodržiavať

ii. Úrovne služieb alebo kľúčových ukazovateľov výkonu, ktoré treba dodržiavať

2) Zamerať sa na roly a zodpovednosti informačnej bezpečnosti, ktoré budú pridelené kompetentným osobám.
3) Riešiť v rámci aspektov informačnej bezpečnosti subdodávateľov dodávateľa a ich dohôd o informačnej bezpečnosti.
4) Riešiť prechod na dodávku produktu alebo služby, v prípade ak už bol predtým produkt alebo služba vyrobený či prevádzkovaný nadobúdateľom alebo iným dodávateľom a to s cieľom zabezpečenia jeho kontinuity. Dôležité je vymedziť plán prechodu a to uvedením požiadaviek na bezpečnosť informácií, ktoré musí nadobúdateľ aj dodávateľ počas prechodu spĺňať. Nesmie sa zabudnúť aby definícia daného plánu, ktorá musí byť v súlade s príslušnými požiadavkami v rámci bezpečnosti informácii bola na vysokej úrovni. V závere je potrebné aby bol plán prechodu odsúhlasený dodávateľom aj nadobúdateľom a zdokumentovaný v dohode o dodávateľskom vzťahu.
5) Riešiť zmeny a mimoriadne udalosti , porušenia alebo iné incidenty, ktoré môžu mať vplyv na bezpečnosť informácií dodávateľa alebo nadobúdateľa, a ktoré sú súčasťou rozsahu dodávky produktu alebo služby. Nutné je najmä:
    i. Jasne a zreteľne definovať postup riadenia zmien v informačnej bezpečnosti, na ktorom sa dohodnú obe strany a zdokumentovať všetky dodávateľské vzťahy v dohode aby boli zabezpečené požadované zmeny ovplyvňujúce informačnú bezpečnosť. Požadované zmeny musia byť včas schválené nadobúdateľom a uplatňované dodávateľom.
    ii. Jasne a zreteľne definovať postup riadenia incidentov bezpečnosti informácií, na ktorom sa dohodnú obe strany, aby bolo zabezpečené, že všetky incidenty v rámci bezpečnosti, vyskytujúce sa počas dodávky produktu alebo služby , sa identifikujú, okamžite nahlásia a vyšetria a budú sa brať do úvahy zmluvné, právne a regulačné hľadiska a požiadavky (v ISO/IEC

27035 je poskytnuté usmernenie k riadeniu incidentov bezpečnosti informácií)

6) Obsahovať zistenia ako :
    1) Bude nadobúdateľ monitorovať a vynucovať aby boli dodržané všetky podmienky informačnej bezpečnosti
    2) Dodávateľ sa zaviaže k dodržiavaniu podmienok. Obe strany definujú a zavádzajú v dohode najmä tieto prvky :
        i. Na strane nadobúdateľa :
            1. Špecifický plán, ktorý monitoruje a presadzuje požiadavky na informačnú bezpečnosť, a ktorý popisuje:
            a. Druhy monitorovacích činností, kde patrí analýza rizík a audit, spôsob a frekvencia vykonávania a oznamovania ich výsledkov
            b. Riadenie a sledovanie nápravných opatrení, ktoré sú iniciované dodávateľom
        ii. Na strane dodávateľa
            1. Proces, ktorý identifikuje, iniciuje, riadi, zaznamenáva, hlási a ukončuje opravné opatrenia, ktoré vyplývajú z výsledkov donucovacích a monitorovacích činností nadobúdateľa. Tento proces musí byť v súlade s príslušnými požiadavkami na bezpečnosť informácií, definovaných v stratégií vzťahu nadobúdateľa

7) Zamerať sa na duševné vlastníctvo produktu alebo služby a tiež na aktíva, vytvorené dodávateľom aj nadobúdateľom.
8) Obsahovať podmienky, na základe ktorých má jedna zo zainteresovaných strán právo vypovedať túto dohodu počas jej realizovania, napríklad ak dodávateľa nie je schopný splniť požiadavky na informačnú bezpečnosť, ktorá je zadefinovaná v dohode

9) Určiť sankcie ,ktoré môžu byť uvalené na nadobúdateľa alebo dodávateľa a to v prípade, že nebudú dodržané požiadavky na informačnú bezpečnosť uvedené v dohode o dodávateľskom vzťahu
10) Definovať povinnosti, ktoré sa týkajú bezpečnosti informácií a požiadavky súvisiace s kontinuitou služieb s ohľadom na ukončenie dohody. Plán ukončenia musí definovať a odsúhlasiť dodávateľ aj nadobúdateľ a musí byť zdokumentovaný a vypracovaný v dodatku dohody o dodávateľskom vzťahu. Je potrebné aby daná definícia tohto plánu bola v súlade s príslušnou informačnou bezpečnosťou na vysokej úrovni. Plán ukončenia obsahuje najmä :
    i. Vymedzenie požiadaviek na bezpečnosť informácií, ktoré majú obe strany dodržiavať, aby sa mohla dohoda ukončiť
    ii. Identifikovanie aktív, ktoré sú používané v rámci dohody a po skončení sa vrátia nadobúdateľovi, dodávateľovi alebo budú postúpené inému dodávateľovi alebo budú zničené či zadržané dodávateľom alebo nadobúdateľom.
    iii. Mechanizmy slúžiace na prenos aktív, pri ktorých bolo zistené, že sa vrátia späť nadobúdateľovi, postúpia ďalšiemu dodávateľovi alebo sa vrátia dodávateľovi.
    iv. Mechanizmy, ktoré slúžia na zničenie aktív, ktoré boli identifikované a určené na zničenie
    v. Uistenie, ktoré preukazuje, že vybrané aktíva boli zničené a doložené osvedčenie o vykonanom zničení
    vi. Obdobie predania produktu a služby, ktoré bude použité v prípade, že sa rozhodne produkt alebo službu previesť späť na nadobúdateľa alebo posunúť inému dodávateľovi
    vii. Záväzok, že nebudú zverejnené citlivé informácie a to v období po ukončení platnosti dohody o dodávateľskom vzťahu
    viii. Časový rozsah, ktorý určuje vykonanie ukončovacieho postupu

b) Schváliť definovanú dohodu o dodávateľských vzťahoch s druhou stranou.

Výstupy:

a) Podpísaná a schválená dohoda o vzťahu s dodávateľom
b) Postup riadenia zmien v informačnej bezpečnosti
c) Postup riadenia incidentov v oblasti informačnej bezpečnosti
d) Plán ukončenia

   Prípadne:

e) Prechodný plán
f) Monitorovanie súladu nadobúdateľa, vynucovací plán a postupy
g) Prijatie monitorovanie súladu a plán presadzovania
h) Proces vybavovania nápravných opatrení

3.3.7 Proces riadenia dodávateľského vzťahu A7.4

Cieľ : Udržiavať informačnú bezpečnosť počas obdobia trvania dodávateľského vzťahu v súlade s dohodou a brať ohľad najmä na:
1) Prechod dodávania produktu alebo služby ak bola predtým prevádzkovaná alebo vyrábaná nadobúdateľom alebo iným dodávateľom
2) Tréning personálu, ktorý je ovplyvnený požiadavkami na informačnú bezpečnosť definovaných v dohode
3) Správu zmien a incidentov, ktoré môžu mať dopad na zabezpečenie informácií o produkte alebo o poskytovanej službe
4) Monitorovanie a presadzovanie súladu dodávateľa s definovanými ustanoveniami o bezpečnosti informácií daných v dohode o dodávateľskom vzťahu (9)

Vstupy:

a) Rozhodnutie o tom, kým bude vykonávané monitorovanie dodávateľa pri dodržiavaní predpisov a realizovanie vynucovacích činností
b) Výsledky z minulých monitorovaní, donucovacích činnosti a trendy v čase

Činnosti :

a) Zabezpečiť aby dohoda o dodávateľských vzťahoch bola prijatá druhou stranou a aby plne pochopila aspekty bezpečnosti informácií, ktoré sa v nej nachádzajú
b) Uskutočňovať aby bol prechod produktu alebo služby v súlade s plánom prechodu, ktorý bol schválený a včas informovať druhú stranu o možných neočakávaných udalostiach objavených počas tejto činnosti
c) Riadiť aby incidenty a zmeny v rámci informačnej bezpečnosti boli v súlade s dohodnutými postupmi
d) Pravidelne zabezpečovať tréning personálu, ktorý sa môže podieľať na realizácií plánu ukončenia
e) Spravovať ďalšie zmeny, ak sú oznámené druhou stranou, na ktorú sa nevzťahuje postup riadenia bezpečnosti informácií, a ktoré môžu mať vplyv na dodávku produktu alebo služby:
    1) Zmena podnikania, poslania alebo prostredia organizácie
    2) Zmena finančnej sily organizácie
    3) Zmena vlastníctva organizácie alebo vytváranie spoločných podnikov
    4) Zmena miesta, z ktorého sa produkt alebo služba obstaráva
    5) Zmena úrovne informačnej bezpečnosti organizácie, napríklad dosiahnutie alebo strata certifikácie ISI/IEC
    6) Zmena schopnosti podporovať požadované schopnosti kontinuity podnikania
    7) Zmena právnych, regulačných a zmluvných požiadaviek vzťahujúcich sa na organizáciu

    Na základe správy týchto zmien bude vyžadované, aby notifikovaná strana vykonala nasledovné:

    1) Zabezpečiť identifikáciu a vyhodnotenie rizík informačnej bezpečnosti, ktoré sú spojené s touto zmenou spolu s možnosťami ich príslušného zaobchádzania.
    2) Zabezpečiť to, aby bol plán liečby bezpečnostných rizík schválený, definovaný a vykonaný obomi zúčastnenými stranami.

3) Zabezpečiť dohodu s druhou stranou o vykonaných zmenách v dohode o dodávateľských vzťahoch, ktoré obsahujú postup riadenia zmien, a incidentov v informačnej bezpečnosti a plán ukončenia.
4) Schváliť aktualizáciu dohody o vzťahu s dodávateľom

f) Zabezpečiť aby sledovanie súladu a vymáhacie činnosti zodpovedali príslušnému plánu a procesu vybavovania nápravných opatrení. V prípade zmien v rizikách informačnej bezpečnosti alebo nezhody auditu, nadobúdateľ s podporou dodávateľa by mali :
   1) Identifikovať a vyhodnotiť dopady na informačnú bezpečnosť vyplývajúcich z týchto zmien, resp. nezhôd
   2) Zistiť či sú aspekty informačnej bezpečnosti správne určené a zvážiť ich zmenu
   3) Určiť, aké nápravné opatrenia by mali byť definované a implementované v dohodnutý časový rozsah na získanie prijateľného levelu bezpečnosti v rozsahu obstarávaného produktu alebo služby
   4) Dohodnúť sa s dodávateľom, ktoré zmeny sa majú vykonať a kedy majú byť implementované
   5) Schváliť aktualizovaný dodávateľský vzťah

Výstupy:

a) Hodnotenie rizík informačnej bezpečnosti a správy z auditu týkajúce činnosti v oblasti monitorovania a presadzovania súladu
   Prípadne :
b) Posúdenie rizika bezpečnosti informácií, ktorý sa týka zmien, na ktoré sa nevzťahuje postup riadenia bezpečnostných zmien
c) Správa o vykonaní prechodného plánu
d) História zmien informačnej bezpečnosti a správy s ňou súvisiace
e) História bezpečnostných incidentov a správy s ňou súvisiace
f) Schválená aktualizovaná dohoda o vzťahu s dodávateľom
g) Zoznam, ktorý obsahuje nápravné opatrenia, ktoré boli dohodnuté a aktuálny stav

3.3.8 Proces ukončenia dodávateľského vzťahu A7.5

Cieľ :
a) Chrániť dodanie produktu alebo služby počas jeho ukončenia, aby sme zabránili akýmkoľvek bezpečnostným, právnym a regulačným dopadom počas procesu ukončenia
b) Ukončiť dodávku produktu alebo služby v súlade s plánom ukončenia (9)

Vstupy:

a) Rozhodnutie vedenia nadobúdateľa alebo dodávateľa o ukončení dodávky produktu alebo služby

b) Posledná dostupná verzia dohody o dodávateľských vzťahoch ktorá obsahuje plán ukončenia dohody

Prípadne:

c) Existujúce dohody o mlčanlivosti, ktoré ustanovuje dodávateľ.

Činnosti:

a) Vyjasniť si so stranou, ktorá rozhodla o ukončení dodávania produktu alebo služby, či jej rozhodnutie súvisí s oblasťou informačnej bezpečnosti

Ak áno, strany, ktoré sú oboznámené s ukončením dohody musia urobiť nasledovné:

1) Identifikovať a odstrániť riziká informačnej bezpečnosti, ktoré sú spojené s daným motívom informačnej bezpečnosti
2) Zaistiť, aby bol vytvorený, definovaný a aplikovaný plán liečby rizík pre nájdené a vyhodnotené riziká, ktoré je potrebné zmierniť

b) Dohodnúť sa s dodávateľov a rozhodnúť, či dodanie produktu alebo služby bude zrušené alebo sa prevedie naspäť na nadobúdateľa alebo iného dodávateľa.

c) Definovať a aplikovať komunikačný plán na informovanie interných zamestnancov a tretích strán, že dodanie produktu alebo služby bude ukončené
d) Vymenovať osobu, zodpovednú za spracovanie ukončenia dodávky produktu alebo služby v súlade s plánom ukončenia
e) Zabezpečiť aktuálny súpis majetku, ktorý sa používa pri dodávke produktu alebo služby
f) Vybrať a dohodnúť sa s druhou stranou na aktívach ktoré budú
    1) Vrátené nadobúdateľovi alebo postúpene inému dodávateľovi
    2) Vrátene dodávateľovi
    3) Zničené alebo zadržané nadobúdateľom alebo dodávateľom
g) Vykonať ukončenie dodávky produktu alebo služby v súlade s plánom ukončenia
h) Zaistiť, aby logické a fyzické prístupové práva udelené druhej strane boli včas odstránené
i) Dohodnúť sa s druhou stranou na ukončení dodávaného produktu alebo služby

Výstupy:

a) Komunikačný plán súvisiaci s ukončením dodávky produktu alebo služby
b) Vymenovanie osoby zodpovednej za ukončenie dodávky produktu alebo služby
c) Aktualizovaný súpis majetku, ktorý sa používa v rámci dodávky produktu alebo služby
d) Správa o ukončení plánu

    Prípadne:

e) Posúdenie rizík informačnej bezpečnosti a plán obnovy spojený s motiváciou informačnej bezpečnosti, dané ukončením dodávky produktu alebo služby
f) Správa o vykonaní prechodného plánu
g) Osvedčenia o zničení majetku
h) Správa o vykonaní odstránenia logických a fyzických prístupových práv

3.3.9 Súhrn cieľov vybraných opatrení

Pre lepší prehľad jednotlivých cieľov každého z vybraných opatrení je vytvorenia tabuľka.

6.1.1 Proces akvizície Vytvoriť plán ktorý bude určovať vzťah s dodávateľmi ktorý je : 1) Založený na tolerancii rizika 2) Definuje základné pokyny dodržiavania bezpečnostných opatrení pri plánovaní, príprave, správe a ukončenia obstarávanie produktu
6.1.2 Proces dodania Vytvoriť plán ktorý bude určovať vzťah s dodávateľmi ktorý je : 1) Založený na tolerancii rizika 2) Definuje základné pokyny dodržiavania bezpečnostných opatrení pri plánovaní, príprave, správe a ukončenia obstarávanie produktu
6.2.2 Proces riadenia infraštruktúry Pripraviť infraštruktúru ktorá podporuje organizáciu pri riadení informačnej bezpečnosti v dodávateľských vzťahoch
6.2.3 Proces správy portfólia projektu Zaviesť procese pre posúdenie bezpečnosti informácií a celkových dopadov obchodných vzťahov v závislosti pre každý jeden projekt
6.2.4 Proces riadenia ľudských zdrojov Zabezpečiť aby spoločnosť ako nadobúdateľ ale aj ako dodávateľ mala k dispozícií potrebné ľudské zdroje, ktoré majú kompetencie a sú pravidelne udržiavané potrebám informačnej bezpečnosti v dodávateľských vzťahoch
6.3.1 Proces plánovania projektu

Zaviesť proces riadenia projektu, zameraný na bezpečnosť informácií v dodávateľských vzťahoch
6.3.4 Proces riadenia rizík Neustále sa zameriavať na riziká informačnej bezpečnosti v dodávateľských vzťahoch a v rámci ich životného cyklu. Pravidelne ich preskúmavať, hlavne ak nastanú nejaké právne, politické alebo obchodné zmeny v zmluvách
7.1 Proces plánovania dodávateľského vzťahu Vytvoriť plán vzťahov s dodávateľmi, na ktorom je zdokumentované rozhodnutie prijaté vedením, ktoré iniciuje obstarávanie produktu alebo služby z hľadiska informačnej bezpečnosti týkajúce sa tohto obstarávania
7.2 Proces výberu dodávateľa Vybrať dodávateľa, ktorý poskytuje primerané informačné zabezpečenie produktu alebo služby .
7.3 Proces dohody v dodávateľskom vzťahu Uzavrieť dohodu o dodávateľskom vzťahu ktorá sa zameriava na : 1) Úlohy a zodpovednosti informačnej bezpečnosti nadobúdateľa a dodávateľa 2) Proces prechodu ak bola služba alebo produkt predtým obstarávania inou stranou 3) Riadenie zmien v informačnej bezpečnosti 4) Správa incidentov informačnej bezpečnosti 5) Monitorovanie a presadzovanie súladu 6) Proces ukončenia
7.4 Proces riadenia dodávateľského vzťahu Udržiavať informačnú bezpečnosť počas obdobia trvania dodávateľského vzťahu v súlade s dohodou a brať ohľad najmä : 1) Prechod dodávania produktu alebo služby ak bola predtým prevádzkovaná alebo vyrábaná nadobúdateľom alebo iným dodávateľom 2) Trénovať personál ktorý je ovplyvnený požiadavkami na informačnú bezpečnosť definovaných v dohode

3) Spravovať zmeny a incidenty, ktoré môžu mať dopad na zabezpečenie informácií o produkte alebo o poskytovanej službe 4) Monitorovať a presadzovať súlad dodávateľa s definovanými ustanoveniami o bezpečnosti informácií daných v dohode o dodávateľskom vzťahu
7.5 Proces ukončenia vzťahu s dodávateľom 1) Chrániť dodanie produktu alebo služby počas jeho ukončenia, aby sme zabránili akýmkoľvek bezpečnostným, právnym a regulačným dopadom počas procesu ukončenia 2) Ukončiť dodávku produktu alebo služby v súlade s plánom ukončenia

3.4 Časový plán a ekonomické zhodnotenie

V tejto časti sa venujeme približnému časovému plánu a ekonomickému zhodnoteniu, ktoré som zostavil. Plán zavedenia alebo úpravy firemných procesov je na odporúčaniach, ktoré idú za sebou a sú dané normou. Počas zhotovovania daného plánu a následného zhodnotenia som prihliadal najmä na náročnosť práce. Tiež som bral ohľad na rozsah práce, ktorý je potrebné uskutočniť pri každej činnosti. Podľa daného plánu by mala implementácia začať v 22. týždni aktuálneho roku. Ukončenie by malo byť začiatkom 24. týždňa. Nakoľko sa jedná iba o približný časový plán a môžu nastať akékoľvek neočakávané situácie, je až do konca 25. týždňa vytvorená časová rezerva, ktorá nám zabezpečí dostatok času na doriešenie daných situácii. Prehľad daného časového plánu a finančného zhodnotenia je zobrazený v tabuľkách nižšie. Pre lepší prehľad činností, ktoré boli naplánované som vyhotovil Ganttov diagram.

Tabuľka 12 : Časový plán implementácie jednotlivých opatrení (zdroj: vlastné spracovanie)

Procesy	Trvanie hodín (h)
6.1.1 Vytvoriť plán vzťahu s dodávateľmi	8
6.1.2 Vytvoriť plán vzťahu s nadobúdateľmi	8
6.2.2 Pripraviť podpornú infraštruktúru	8
6.2.4 Zabezpečenie ľudských zdrojov	2
6.2.5 Zaviesť proces plánovania projektu	4
6.3.1.1 Definovať rámec riadenia rizík	6
6.3.1.2 Aplikovať rámec riadenia rizík	2
7.1.1 Posúdenie rizík obstarávaných produktov	2
7.1.2 Plán liečby obstarávaných produktov	2
7.2.1 Definovať kritéria výberu dodávateľa	6
7.2.2 Pripraviť dohodu o mlčanlivosti	4
7.2.3 Pripraviť tender na výber dodávateľa	8
7.3.1 Vytvoriť dohodu s druhou stranou o riadení zmien	4
7.3.2 Vytvoriť dohodu s druhou stranou o riadení incidentov	2
7.4 Vytvoriť plán monitorovania dodržiavania bezpečnosti	8
7.5.1 Vytvoriť súpis aktív používaných v dohode	4
7.5.2 Vytvoriť plán ukončenia	8

Tabuľka 13: Ganttov diagram (zdroj: vlastné spracovanie)

Názov činností	Čas	22. týždeň					23. týždeň					24.týždeň					25.týždeň				
		Po	Ut	St	Št	Pi	Po	Ut	St	Št	Pi	Po	Ut	St	Št	Pi	Po	Ut	St	Št	Pi
6.1.1 Vytvoriť plán vzťahu s dodávateľmi	8	8																			
6.1.2 Vytvoriť plán vzťahu s nadobúdateľmi	8		8																		
6.2.2 Pripraviť podpornú infraštruktúru	8			8																	
6.2.4 Zabezpečenie ľudských zdrojov	2				2																
6.2.5 Zaviesť proces plánovania projektu	4				4																
6.3.1.1 Definovať rámec riadenia rizík	6				2	4															
6.3.1.2 Aplikovať rámec riadenia rizík	2					2															
7.1.1 Posúdenie rizík obstarávaných produktov	2					2															
7.1.2 Plán liečby obstarávaných produktov	2						2														
7.2.1 Definovať kritéria výberu dodávateľa	6						6														
7.2.2 Pripraviť dohodu o mlčanlivosti	4							4													
7.2.3 Pripraviť tender na výber dodávateľa	8							4	4												
7.3.1 Vytvoriť dohodu s druhou stranou o riadení zmien	4								4												
7.3.2 Vytvoriť dohodu s druhou stranou o riadení incidentc	2									2											
7.4 Vytvoriť plán monitorovania dodržiavania bezpečnosti	8										8										
7.5.1 Vytvoriť súpis aktív používaných v dohode	4											4									
7.5.2 Vytvoriť plán ukončenia	8											4	4	Rezerva							

Tabuľka 14 : Náklady na implementáciu jednotlivých opatrení (zdroj: vlastné spracovanie)

Procesy	Kč
6.1.1 Vytvoriť plán vzťahu s dodávateľmi	160€
6.1.2 Vytvoriť plán vzťahu s nadobúdateľmi	160€
6.2.2 Pripraviť podpornú infraštruktúru	160€
6.2.4 Zabezpečenie ľudských zdrojov	40€
6.2.4 Zaviesť proces plánovania projektu	80€
6.3.1.1 Definovať rámec riadenia rizík	120€
6.3.1.2 Aplikovať rámec riadenia rizík	40€
7.1.1 Posúdenie rizík obstarávaných produktov	40€
7.1.2 Plán liečby obstarávaných produktov	40€
7.2.1 Definovať kritéria výberu dodávateľa	120€
7.2.2 Pripraviť dohodu o mlčanlivosti	80€
7.2.3 Pripraviť tender na výber dodávateľa	160€
7.3.1 Vytvoriť dohodu s druhou stranou o riadení zmien	80€

7.3.2 Vytvoriť dohodu s druhou stranou o riadení incidentov	40€
7.4 Vytvoriť plán monitorovania dodržiavania bezpečnosti	160€
7.5.1 Vytvoriť súpis aktív používaných v dohode	80€
7.5.2 Vytvoriť plán ukončenia	160€

Následne sme zistili, že spoločnosť vykázala za rok 2020 celkové výnosy 1 983 021€. (14) Počet pracovných dní v roku 2020 bol 251, čo v prepočte vychádza, že ak by firma stratila kontrolu nad systémom, alebo by bolo podobným štýlom zamedzenie vykonávania podnikateľskej činnosti v dodávateľských vzťahoch, v priemere na jeden deň by bola v strate približne 7900€. Návrh zmien v existujúcich procesoch alebo zavedenie nových procesov podľa nami navrhnutej normy by ju stálo jednorazovo niečo okolo 1720€, z čoho vyplýva, že ak by firma investovala a zaviedla spomínané bezpečnostné opatrenia znížila by riziká úniku informácii alebo prípadné sankcie pre dodávateľov na ktorých strane by problém nastal.

ZÁVER

Cieľom tejto práce bol návrh zavedenia bezpečnostných opatrení pre danú spoločnosť. Cieľ bol úspešne splnený po tom čo sa na základe analýzy aktuálneho stavu a analýzy rizík odporučili opatrenia podľa normy ISO/IEC 27036 ako zvýšiť bezpečnosť informácií v dodávateľských vzťahoch.

V prvej časti sme si definovali Teoretické východiská z danej problematiky preberanej v práci. Vysvetlené základné pojmy, princípy použitých analýz a normy o ktoré sa práca opiera.

Druhá časť práce bola venovaná danej spoločnosti, kde bolo stručne opísané zázemie firmy, organizačná štruktúra a aktuálny stav v spoločnosti. Následne bola vytvorená analýza súčasného stavu bezpečnosti informácií v dodávateľských vzťahoch. Po zosumarizovaní výsledkov nám graf ukázal že spoločnosť sa v dodávateľských vzťahoch zameriava na bezpečnosť minimálne.

Tretia kapitola sa venovala samotnému návrhu riešenia. Na začiatku bola spravená analýza rizík kde sme ohodnotené aktíva porovnali s pravdepodobnosťou danej hrozby a vytvorením matice zraniteľnosti dostali maticu rizík. Výsledná matica nám slúžila ako pomôcka pri návrhu riešenia a taktiež pre spoločnosť aby si zvýšila povedomie o bezpečnosti informácií pri dodávateľských vzťahoch. Následne boli podľa normy ISO/IEC 27036 navrhnuté bezpečnostné opatrenia ako upraviť firemné procesy a zvýšiť bezpečnosť informácií v spoločnosti.

ZOZNAM POUŽITÝCH ZDROJOV

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

(2) POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-868-9838-5.

(3) *DOUCEK, Petr. Řízení bezpečnosti informací: 2. rozšířené* vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-0508.

(4) *PDCA history [online]. 2016 [cit. 2021-05-15].* Dostupné z: https://www.allaboutlean.com/pdca-history/

(5) *ISO - International Organization for Standardization [online]. [*cit. 2021-05-16]. Dostupné z: https://www.iso.org/about-us.html

(6) *ČSN ISO/IEC 27001: Informační technologie - Bezpečnostní techniky*. Systémy managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut, 2014.

(7) *ČSN ISO/IEC 27000 - Information technology — Security* techniques — Information security management systems — Overview and vocabulary. 5. vydání. Švajčiarsko: Mezinárodní organizace pro normalizaci.

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

(9) *ČSN ISO/IEC 27036: Information technology — Security techniques*. Information security for supplier relationships - Part 2 : Requirements. Švýcarsko: Mezinárodní organizace pro normalizaci, 2014.

(10) *ČSN ISO/IEC 27005: Informační technologie - Bezpečnostní techniky*. Řízení bezpečnosti informací. 2. vydání. Praha: Český normalizační institut, 2013.

(11) *Logo KRIDLA s.r.o [online]. [cit.* 2021-05-15]. Dostupné z: http://www.kridla.sk/

(12) *Lenovo: V530 Tower [online]. [cit. 2021-05-15]*. Dostupné z: https://www.lenovo.com/cz/cs/desktops/lenovo/v-series-tower-desktop-lenovo/Lenovo-V530-15ICB-Desktop/p/11LV1VDV530

(13) *Lenovo: ThinkPad E580 [online]. [cit. 2021-05-15]*. Dostupné z: https://www.lenovo.com/cz/cs/laptops/thinkpad/edge-series/ThinkPad-E580/p/22TP2TEE580

(14) *Finstat [online]. [cit. 2021-05-16]. Dostupné z*: https://www.finstat.sk/36466778

ZOZNAM POUŽITÝCH OBRÁZKOV

ZOZNAM POUŽITÝCH TABULIEK