Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Řízení rizik bezpečnosti informací v podniku

Bc. Yulia Zhuleeva

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Yulia Zhuleeva

Systémové inženýrství a informatika
Informatika

Název práce

Řízení rizik bezpečnosti informací v podniku

Název anglicky

Risk management of information security in the Enterprise

Cíle práce

Primárním cílem práce je posoudit zabezpečení informací ve vybraném podniku pomoci řady norem ISO/IEC 27000, na základě čehož navrhnout vhodná opatření. Dílčími cíli jsou shrnovat základy příslušných bezpečnostních standardů a postupy systému řízení bezpečnosti informací, identifikovat rizika, zhodnotit je a odhadnout jejich dopad na zabezpečení podnikových aktiv.

Metodika

Diplomová práce se skládá z teoretické a praktické části. Teoretická část formou literární rešerše charakterizuje použité bezpečnostní normy a definuje pojmy, které souvisejí s řízením rizik a bezpečností informací. Praktická část se zabývá analýzou zranitelných oblastí podniku, hodnocením nalezených rizik a vytvářením strategie jejich zvládnutí.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

risk management, normy ISO/IEC 27000, ISMS, bezpečnost informací, bezpečnostní opatření, hrozby, rizika, aktiva

---

Doporučené zdroje informací

ANDERSON, R. Security engineering. Indianapolis: Wiley Publishing, 2008. ISBN 978-04-7006-852-6.

ČSN ISO/IEC 27001. Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

ČSN ISO/IEC 27002. Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

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

ONDRÁK, V. – SEDLÁK P. – MAZÁLEK V. Problematika ISMS v manažerské informatice. Vyd. 1. Brno: CERM, 2013. ISBN 978-80-7204-872-4.

POŽÁR, J. *Informační bezpečnost.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

Předběžný termín obhajoby

2019/20 LS – PEF

Vedoucí práce

Ing. Mgr. Vladimír Očenášek, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 11. 9. 2018

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2018

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 27. 03. 2020

Čestné prohlášení

Prohlašuji, že svou diplomovou práci " Řízení rizik bezpečnosti informací v podniku" jsem vypracovala samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autorka uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne 31. 3. 2020 _____

Poděkování

Ráda bych touto cestou poděkovala panu Ing. Mgr. Vladimíru Očenáškovi, Ph.D. za vedení práce, odbornou pomoc a připomínky, které pomohly vytvořit tuto práci.

Řízení rizik bezpečnosti informací v podniku

Souhrn

Diplomová práce se zabývá analýzou prostředí vybrané společnosti na předmět zabezpečení informací a návrhem bezpečnostních opatření dle řady norem ISO/IEC 27000. Teoretická část práce vysvětluje pojmy z oblasti informační bezpečnosti, popisuje systém řízení bezpečnosti informací (zkráceně ISMS) a postupy ho zavádění, a určuje požadavky na informační bezpečnost dle legislativních a normativních rámců. V analytické části práce je provedeno zkoumání současného stavu bezpečnosti, analýza rizikových oblastí a návrh vhodných opatření vedoucích ke zmírnění těchto rizik a zvyšujících zabezpečení podnikových dat. Závěr práce shrnuje poznatky, hodnotí výsledky práce a uvádí doporučení.

Klíčová slova: Řízení rizik, normy ISO/IEC 27000, ISMS, bezpečnost informací, bezpečnostní opatření, hrozby, rizika, aktiva.

Risk management of information security in the Enterprise

Summary

The diploma thesis is focused on the analysis of the information security in the selected company and the design of security measures based on ISO/IEC standards 27000 series. The theoretical part explains the concepts of the information security, describes the information security management system and procedures for its implementation, determines information security requirements according to law and international standards. The practical part analyses the current security state of the organization and its risk areas to mitigate these risks and increase the security of business data. The conclusion summarizes the findings, evaluates the results of the work and gives recommendations.

Keywords: Risk management, ISO/IEC 27000 standards, ISMS, information security, security measures, threats, risks, assets.

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Kybernetická bezpečnost se rychle vyvinula z technické disciplíny na strategickou. Globalizace a internet daly lidem, organizacím a národům obrovskou moc, založenou na neustále se rozvíjejících síťových technologiích. Informační technologie představují širokou platformu pro rychlé progresivní změny v ekonomice a stávají kritickým faktorem úspěchů organizací. A zároveň s rostoucí závislosti světa na mocném, ale zranitelném internetu v kombinaci s rušivými schopnostmi kybernetických útočníků přichází ohrožení národní a mezinárodní bezpečnosti.

« Zda se jedná o vyvíjeni kompletní bezpečnostní politiky pro společnost nebo se tvoří pro jednorázový projekt, uprostřed leží vrcholové rozhodnutí o prioritách – kolik vynaložit na ochranu a proti čemu. Jedná se o řízení rizik a mělo by to být provedeno i nad rámec rizik v oblasti IT. »(Anderson, 2008).

Vzhledem k tomu, že jedním z neevidentních rizik zavádění IT ve společnosti, je ohrožení bezpečnosti informačních systémů a dat, které zpracovávají, dostava se do popředí zájmu organizací po celém světě. Podniky a organizace jsou nuceny vytvářet efektivní přístupy při zabezpečení svých informačních systémů. Kvůli narůstající konkurenci vznikl nový fenomén počítačové kriminality. Nasazením ICT technologií ztrácí firma svůj lokální charakter a dochází k bezpečnostním hrozbám. Informační bezpečnost se musí budovat a neustálé se inovovat v organizacích. Řízení jejich bezpečnosti se pak stává jedním z průřezových profilu managementu.

Daná diplomová práce je určena pro podniky menší velikosti, které se začínají uvažovat o důležitosti a nevyhnutelnosti zavedení opatření, sloužících pro zabezpečení podnikových informací a osobních údajů svých zákazníků, které zpracovává. Pokud ve společnosti narůstá množství potenciálně ohrožených zařízení a zároveň existuje nedostatek bezpečnostního povědomí potřebného k řízení bezpečnostních rizik, je nezbytně nutné se zabývat rozvíjením, zavedením a údržbou ochranných procesů proti různým druhům hrozeb.

Z toho důvodu, že daná analýza rizik probíhá v prostředí reálné společnosti, název této společnosti by měl zůstat v anonymitě s cílem prevence proti zneužití informací uvedených v práci. Dále bude se jmenována jako společnost „Milá papírna“.

2 Cíl práce a metodika

Cílem práce je vypracování analýzy zabezpečení informací v rámci společnosti, zaměřené nejen na nalezení slabých míst v zabezpečení provozovaných informačních a komunikačních prostředků, ale rovněž na celkovou bezpečnostní politiku organizace. Na analýzu se navazují nezbytné opatření pro zesílení úrovně bezpečnosti všech podnikových aktiv.

Práce je rozdělena do tří částí. V první části jsou uvedeny zásadní terminy a východiska, je popsán systém řízení bezpečnosti informací, mezinárodní standardy bezpečnosti a legislativní požadavky, na které se opírá tento systém. V druhé části práce bude provedena analýza prostředí společnosti a rizik, které jí hrozí. Na základě těchto poznatků v poslední třetí části je představen návrh zavedení ISMS a zaopatření odhalených rizik. Analýza a následný návrh opatření se provádí na základě metodik a technik popsaných v řadě norem ISO/IEC 27000 a zejména v normách ISO/IEC 27001 a ISO/IEC 27002. Standard ISO 27001 popisující požadavky na ISMS byl zvolen jako model, kterým by se podnik měl řídit během nastavování svých procesů a činnosti. Další norma ISO 27002 obsahující doporučována opatření a nejlepší praktiky pro zabezpečení informací byla použita pro výběr nejvhodnějších opatření pro zavedení do prostředí společnosti.

3 Teoretická východiska

První část dané práce se zabývá vysvětlením základních pojmů a názvosloví souvisejících s procesem řízení rizik informační bezpečnosti a implementaci systému řízení informační bezpečnosti ISMS včetně přínosu jeho zavedení, zde též budou popsány zákony a normy, které se týkají informační bezpečnosti.

3.1 Základní pojmy

Aktivum (Asset). Aktivum je hmotný nebo nehmotný majetek, jakož jsou peněžní a nepeněžní prostředky, nemovitost, práce, informace atd., vlastněné fyzickou nebo právnickou osobou a schopné generovat zisk a zvyšovat jí příjmy.

Do informačních aktiv patří veškeré informace, které mají hodnotu pro osobu či organizaci. Zahrnují informace vytištěné nebo napsané na papíře, zasílané poštou nebo elektronicky uložené na serverech, webových stránkách, mobilních zařízeních, magnetických a optických nosičích, a také informace zpracované v podnikových informačních systémech a přenášené prostřednictvím komunikačních kanálů.

Bezpečnost informací (Information security) spolu s bezpečností IS/ICT, která řeší pouze ochranu aktiv informačního systému, tvoří bezpečnost organizace. Úkolem bezpečnosti informací je zajištění ochrany veškerých informačních aktiv podniku a jejich dostupnosti, a na rozdíl od bezpečnosti IS/ICT zahrnuje práci s informacemi v nedigitální formě (Ondrák a kol., 2013).

Základní cíle informační bezpečnosti dle normy ISO/IEC 27001 se dělí na:

- **Důvěrnost** – přístup k informacím není oprávněn osobám nebo organizacím, které nemají povolení k jejich zhlednutí. Důvěrnost je nezbytnou součástí interního prostředí společnosti, slouží pro zabezpečení určitých informací, které jsou zpřístupněny pouze autorizovaným osobám. K zachování důvěrnosti dat se nejčastěji používají klasifikace informačních aktiv, šifrování a likvidace zařízení.
- **Dostupnost** – zajištění přístupnosti k informacím oprávněnému uživateli v požadovaný okamžik. K zachovaní dostupnosti se používají taková opatření, jako antivirová ochrana, refundace kritických systémů a preventivní ochrana proti DOS a DDOS útokům.

- **Integrita** – mechanismus, který zajišťuje přesnost a úplnost informací odhalením změny dat jak autorizovaným, tak neautorizovaným způsobem.

Tato trojice je také známá pod zkratkou CIA (Confidentiality, Integrity, Availibility) a vytváří užitečný bezpečnostní model pro posouzení úrovně zabezpečení podnikových informačních aktiv.

Po mnoho letech se většina výzkumných prací o informační bezpečnosti se zabývala důvěrností a zbytek se týkal autenticity a integrity, dostupnost byla zanedbána. Avšak v současné době, výdaje typické banky jsou rozděleny jinak. Asi třetina všech nákladů na IT se týká mechanismů dostupnosti a restartování systému, jako jsou náhradní servery a mnohonásobně redundantní sítě; několik procent je investováno do mechanismů integrity, jako je interní audit; a téměř bezvýznamná částka se utratí za mechanismy důvěrnosti, jako jsou šifrovací schránky. Mnoho dalších činnosti, od poplachů proti vloupání přes elektronické válčení až po ochranu společnosti před denial-of-service (DoS) útoky, je v zásadě o dostupnosti. Překonáni poruch a obnovení po selhání jsou obrovskou součástí práce systémového administrátora. (Anderson, 2008)

Hrozba (Threat). Hrozbou se rozumí potenciálně možná událost, proces nebo jev, který ohrožuje bezpečnost informací zneužitím existující zranitelnosti programu.

Zranitelnost (Vulnerability). V oblasti informační bezpečnosti pojem se používá k označení chyby v programu, pomocí čeho lze úmyslně narušit integritu dat a způsobit poruchu. Obvykle část aktiv podniku je citlivá na konkrétní hrozbu, takový jev se povazuje za zranitelnost aktiva.

Opatření (Countremeasure) – je aktivita, která snižuje hrozbu tím, že ji eliminuje nebo předchází, minimalizuje potenciální škodu, nebo detekuje a nahlásí hrozbu, aby bylo možno provést nápravné opatření.

Riziko (Risk) – je definováno panem doktorem Ondrákém a kol. (2013) jako „kombinace hrozby a zranitelnosti s dopadem na aktivum“. Jinak řečeno existuje nebezpečí, že hrozba využije zranitelnost informačních aktiv a tím způsobí škodu organizaci. Riziko se měří podle pravděpodobnosti výskytu událostí a jich důsledků.

Analýza rizik (Risk analysis) – je proces pochopení povahy rizik a určení úrovně rizik pomocí identifikace potenciálních hrozeb, které mohou mít negativní dopad na informační aktiva

společnosti nebo kritické projekty, aby umožnit organizacím těmto rizikům zabránit nebo je zmírnit.

Proces řízení rizik (Risk management process) – systematické uplatňování strategií řízení, postupů a stávajících pravidel při výměně informací, konzultacích, jakož i identifikaci, analýze, posuzování, zpracování, průběžném sledování a přezkumu rizik.

Bezpečnostní incident (Security incident). Za bezpečnostní incident je třeba považovat poškození či ztrátu datových souborů, delší vyřazení systému z provozu, rozšíření počítačových virů v síti nebo průnik do informačního systému. (Požár, 2005).

Bezpečnostní audit (Security audit) – pravidelná, nezávislá a dokumentovaná kontrola a analýza záznamů v systému zpracování dat, kontrola shody s akceptovanou bezpečnostní politikou a provozními postupy, odhalování bezpečnostních hrozeb, doporučení a postupy dodržování bezpečnostní politiky. Nezávislé testování činnosti informačního systému a jeho záznamů, které má za cíl zjistit, zda jsou kontroly náležitě prováděny, a jsou v souladu s bezpečnostní politikou, a poskytnout doporučení případných změn v systému protiopatření. Provádí se to zpravidla pomocí externího nebo interního auditora.

Politika bezpečnosti informací (IT security policy) – požadavky a postupy odvozené ze zákonů a bezpečnostních norem, v dokumentované podobě, které směrují management společnosti v procesech spravování a chránění informačních aktiv pro zajištění jejich důvěrnosti, dostupnosti a integrity. Popisují, jak probíhá komunikace a výměna dat uvnitř systému a mimo něj, kladou požadavky na prostředí, ve kterém systém působí.

Autorizace (Authorization) – poskytnutí uživateli přístupových práv do systému ve formě údajů, které ověřují prohlašované identity daného subjektu. Pravá se přidělují pro vykonávání určených aktivit v informačním systému.

3.2 Zákony a normy v oblasti bezpečnosti IT

V této kapitole budou popsány normy řady ISO/IEC 27000, které obsahují doporučení pro zavedení systému řízení bezpečnosti informací, přínosy dané certifikace a právní předpisy České

republiky a EU, které upravují legislativní rámec v oblasti informační a komunikační bezpečnosti.

3.2.1 Normy řady ČSN ISO/IEC 27000

Řada norem ISO/IEC 27000 má souhrnný název „Informační technologie – Bezpečnostní techniky“ a představuje podrobný návod pro různé aspekty implementace ISMS, čímž poskytuje organizacím všech typů a velikostí možnost zavést a provozovat ISMS. Níže jsou uvedeny nejzásadnější normy pro regulaci systému řízení bezpečnosti informací.

ISO je zkratka pro Mezinárodní organizace pro normalizaci (Internation Organization for Standardization), která se zabývá tvorbou mezinárodních norem. Ve spolupráci s mezinárodní elektrotechnickou komisí (International Electrotechnical Commission) v roce 2005 ISO vydala normy řady ISO/IEC 27000, které se věnují problematice řízení bezpečnosti informací a prohlubují a vymezují vztahy a hranice mezi již existujícími bezpečnostními normami (Doucek, 2011). Úřad pro technickou normalizaci, metrologii a státní zkušebnictví se stara o překlad a zajišťuje proces integrace právního řadu a technických předpisů z norem mezi Českou republikou a Evropskou unií. Dále budou podrobně popsány jen ty nejpodstatnější pro tuto práci normy řady ISO/IEC 27000.

ČSN ISO/IEC 27000:2018 – „Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník“. Tato norma poskytuje přehled systému řízení bezpečnosti informaci, popisuje základní terminy a definice související se s ISMS a sloužící jako podklad pro jeho zavedení a provozování. Poprvé publikováno v roce 2009. Aktuální páté vydání je z roku 2018.

ČSN ISO/IEC 27001:2013 – „Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky“. Klíčovým prvkem je tato norma, která stanoví, jak zavést, řídit, kontrolovat a monitorovat systém řízení bezpečnosti informací v organizacích odlišného typu, velikosti a působnosti, jež jsou nezbytné pro úspěšnou certifikaci norem řady ČSN ISO/IEC 27000. Popisuje oblasti, na které by organizace neměla zapomenout při ochraně informační bezpečnosti, a to zejména na politiku organizace bezpečnosti informací, řízení aktiv, bezpečnosti lidských zdrojů, bezpečnosti prostředí, provozu a komunikací, údržbu systému, řízení incidentu bezpečnosti informací a na soulad s požadavky.

ČSN ISO/IEC 27002:2013 – „Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací“. Druhá nejdůležitější norma obsahuje podrobný výklad vhodných bezpečnostních opatření, takzvané „best-practice“, která zajišťují nejvyšší bezpečnost při práci s daty a tím podporují dosahování podnikatelských cílů. Vhodná opatření jsou vybírána na základě hodnocení rizik a jej implementace je závislá na konkrétní situaci. Ale některá opatření v této normě mohou být považována za hlavní zásady pro řízení bezpečnosti informací použitelné pro většinu organizací. Bezpečnostní opatření organizací lze rozdělit do třech oblastí: řízení a správa bezpečnosti, technologická bezpečnost a bezpečnost provozního prostředí.

ČSN ISO/IEC 27003:2017 – „Informační technologie – Bezpečnostní techniky – Směrnice pro zavádění systému řízení bezpečnosti informací“. Tato norma poskytuje praktické pokyny pro zřízení a implementace a další návody na provozování, monitorování, revizi, údržbu a zlepšování ISMS v souladu s ISO/IEC 27001. Dle této normy implementace je rozdělena do pěti etap:

- získání souhlasu vedení organizace se zahájením projektu ISMS;
- definice rozsahu, hranic a politik ISMS;
- provedení analýzy;
- hodnocení rizik a plán zvládání rizik;
- finální návrh ISMS.

ČSN ISO/IEC 27005:2018 – „Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací“. „Tato mezinárodní norma poskytuje doporučení pro řízení rizik bezpečnosti informací v rámci organizace, podporuje obecný koncept specifikovaný v ISO/IEC 27001 a je strukturována tak, aby dostatečně podporovala implementaci informační bezpečnosti založené na přístupu řízení rizik.“ (Ondrák a kol, 2013). Norma se skládá ze šesti základních částí:

- První část je stanovení kontextu – vymezuje základní aspekty a kritérií řízení rizik, dopadu a přijatelnosti rizika, definuje rozsah a hranice.
- Druhá část se zabývá posouzením rizik z pohledu identifikace hrozeb, aktiv, opatření, zranitelnosti a následků. Dále je zde popsána analýza rizik, její metody, formy posuzování a určování pravděpodobnosti výskytu incidentu.
- Následující třetí část normy řeší zaopatření – výběr protiopatření k redukci, podstoupení, vyvarování se nebo přenosu rizik a definice plánu zvládání rizik.
- Navazující čtvrtá část vysvětluje akceptaci rizik bezpečnosti informací.
- Předposlední část popisuje proces sdílení informace o rizicích.

- Závěrečná část je věnována monitorování a přezkoumávání rizik a jej faktorů (ČSN ISO/IEC 27005, 2018).

Metodiky řízení rizik uvedené v této normě mají pouze ilustrativní charakter a slouží pro nabytí povědomí o možnostech přístupu k řízení rizik bezpečnosti informací. Norma nestanoví přesný postup, který musí striktně dodržovat všechny organizace, pokud chtějí úspěšně implementovat ISMS. Jinými slovy, norma nabízí pouze určitá doporučení a upozornění, jak postupovat a jaké skutečnosti při jednotlivých krocích či etapách implementace nepřehlížet. S ohledem na tento fakt, norma je aplikovatelná na organizace různého typu, jejich rozdílnými strategiemi, vizemi a cíli. V následujících kapitolách jsou popsány a použity jednotlivé kroky procesu řízení rizik bezpečnosti informací, které jsou v této normě uvedeny.

Některé další ISO normy z rodiny 27000:

ČSN ISO/IEC 27004:2016 – „Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Měření“.

ČSN ISO/IEC 27006:2015 – „Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací“.

ČSN ISO/IEC 27007:2017 – „Informační technologie – Bezpečnostní techniky – Směrnice pro auditování systému řízení bezpečnosti informací“.

ČSN ISO/IEC 27008:2011 – „Informační technologie – Bezpečnostní techniky – Směrnice pro auditory o opatřeních systémů řízení bezpečnosti informací“.

Další skupiny norem řady ISO/IEC 27000 obsahuji požadavky a doporučení základních norem, které jsou rozlišovány podle potřeb a specifických podmínek řízení bezpečnosti informací v různých odvětvích lidské činností.

3.2.1.1 Přínosy certifikace dle ČSN ISO/IEC 27001

Snahou zavedení standardů je zvýšit produktivitu práce organizace a přinést jí tím prospěch. V současné době počet ISO certifikovaných společností roste z čehož plyne, že standardizace přináší řadu výhod. Nicméně certifikace je doprovázena finančními výdaji a řadou potenciálních rizik.

Výhody standardizace budou primárně vyplývat ze snížení rizik bezpečnosti informací (tj. snížení pravděpodobnosti výskytu událostí anebo dopadů způsobených incidenty informační bezpečnosti). Konkrétně výhody realizované pro organizaci k dosažení udržitelného úspěchu od zavedení standardů jsou následující:

- Zabezpečení informací. Identifikace a zvládnutí hrozeb, ohrožující aktiva společnosti, ošetření identifikovaných slabých míst v informační bezpečnosti. Zpřehlednění v řízení SW a HW, minimalizace výpadků a zlepšení dostupnosti IT služeb. Snížení rizika ztráty informací, finančních dopadů při znehodnocení nebo ztrátě citlivých informací, při jejich úniku/vyzrazení či dokonce jejich zneužití konkurencí.
- Vedení společnosti je dobře informováno o kvalitě vnitřních procesů podniku, má přístup k řízení informační bezpečnosti v rámci řízení a správy podnikových rizik, včetně školení svých zaměstnanců. Zaměstnanci se zase snaží kvalitně plnit předepsané úkoly, zvyšují se jejich povědomí a odpovědnost při nakládání s citlivými informacemi v organizaci.
- Standardizace procesů a racionalizace činností, zejména díky zavedení komplexní dokumentace. Slouží k zaznamenávání a uchovávání důležitých skutečností a informací pro současné i budoucí zaměstnance.
- Prosazování v podniku globálně uznávaných správných postupů v oblasti bezpečnosti informací, které vyhovují jejich specifickým okolnostem. Připravenost na legislativní požadavky a požadavky auditů.
- Zvýšení prestiže. Jedná z konkurenčních výhod je pořízení certifikací. Připravenost na plnění požadavků zákona o kybernetické bezpečnosti zvyšuje důvěryhodnost a prestiže pro spolupracující organizace, které se mohou spolehnout na certifikovaného partnera.
- Efektivnější ekonomické řízení investic do informační bezpečnosti.

3.2.2 Legislativní a právní předpisy České republiky a EU

Legislativní orgány musí včas reagovat na změny ve světě, spojené s rozvojem informačních technologií, a umožnit využití jejich potenciálu ve prospěch hospodářského růstu. V České republice právní rámce, které se týkají informační bezpečnosti a bezpečnosti informačních systémů, jsou upraveny zejména těmito zákony:

- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím. Zákon zavazuje organizace i orgány poskytovat informace o veškeré své činnosti. Také zákon upravuje pravidla pro poskytování informací, podávaní a vyřizování žádostí a stanovení lhůt (Doucek, 2011).
- Zákon č. 29/2000 Sb., o poštovních službách.

- Zákon č. 121/2000 Sb., autorský zákon.
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy (ISVS).
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě.
- Zákon č. 127/2005 Sb., o elektronických komunikacích.
- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Tento zákon upravuje zásady pro odhalení utajované informace, stanoví podmínky pro přístup k takovým informacím a požadavky na jejich ochranu. Zákon také definuje zásady pro stanovení citlivých činností, podmínky pro jejich výkon a vymezuje činnost Národního bezpečnostního úřadu (NBÚ) (Doucek, 2011).
- Zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů.
- Zákon č. 111/2009 Sb., o základních registrech.
- Vyhláška č. 432/2011 Sb., o zajištění kryptografické ochrany utajovaných informací.
- Zákon č. 181/2014 Sb., o kybernetické bezpečnosti. Zákon upravuje práva a povinnosti osob, působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti a má za cíl nastavit mechanismus aktivní spolupráce mezi soukromým sektorem a veřejnou správou za účelem vyšší efektivity řešení kybernetických bezpečnostních incidentů.
- Zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce.
- Zákon č. 110/2019 Sb., o zpracování osobních údajů. Zákon navazuje na přímo použitelný předpis Evropské unie č. 2016/679/ES o ochraně osobních údajů.

Kromě tuzemských zákonů je oblast řízení informační bezpečnosti výrazně ovlivněna právními předpisy vydávanými Evropskou unií. V souladu s následujícími směrnicemi Evropského společenství zákon upravuje právní rámec v oblasti ICT na území celé EU:

- směrnice č. 96/9/ES, o právní ochraně databází;
- směrnice č. 2002/19/ES o přístupu k sítím elektronických komunikací a přiřazeným zařízením a o jejich vzájemném propojení;
- směrnice č. 2002/58/ES, o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací;
- směrnice č. 2004/48/ES, o dodržování práv duševního vlastnictví;
- směrnice č. 2009/24/ES, o právní ochraně počítačových programů;
- směrnice č. 2013/37/EU o opakovaném použití informací veřejného sektoru;
- nařízení č. 2014/910/ES, o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu;

- nařízení č. 2016/679/ES, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů;
- směrnice č. (EU) 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.

Jednou z nejdůležitějších a nejznámějších mezinárodních norem v současné době je nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES označované termínem „General Data Protection Regulation“ neboli široko známou zkratkou **GDPR**. Nařízení nahrazuje stávající směrnici 1995/46/ES o ochraně osobních údajů, začala platit od 25. května 2018 v celé EU a týká se všech firem a institucí, jednotlivců a online služeb, které zpracovávají data uživatelů. Pro firmy GDPR zavadí hned několik nových povinností. Správce musí vypracovávat takzvané záznamy o činnostech zpracování, které budou obsahovat jméno a kontaktní údaje správce, účely zpracování, popis kategorií subjektů údajů a kategorií zpracovávaných osobních údajů, informací o případném předávání osobních údajů do zahraničí apod. Další novinkou je zřízení pozice tzv. pověřence pro ochranu osobních údajů pro dohled nad dodržováním GDPR během firemních aktivit a pro případnou komunikaci s Úřadem pro ochranu osobních údajů. Mezi dalšími povinností patří nutnost získat souhlas od zákazníka k použití osobních údajů a seznámit ho se způsoby zpracování údajů; nutnost provést analýzu rizik vztahující se k ochraně osobních údajů; nutnost bezodkladně ohlašovat veškeré případy porušení zabezpečení osobních údajů úřadu pro ochranu osobních údajů a v případě velmi rizikových incidentů i samotným subjektům údajů; nutnost umožnit klientovi či zaměstnanci smazání všech jeho osobních údajů (Matzner, 2017). Nařízení GDPR výrazně ovlivňuje chod ISMS, vznikají nové požadavky na zajištění informační bezpečnosti a posílení bezpečnostních opatření u procesů, během kterých se zpracovávají osobní údaje.

3.3 Řízení rizik informační bezpečnosti

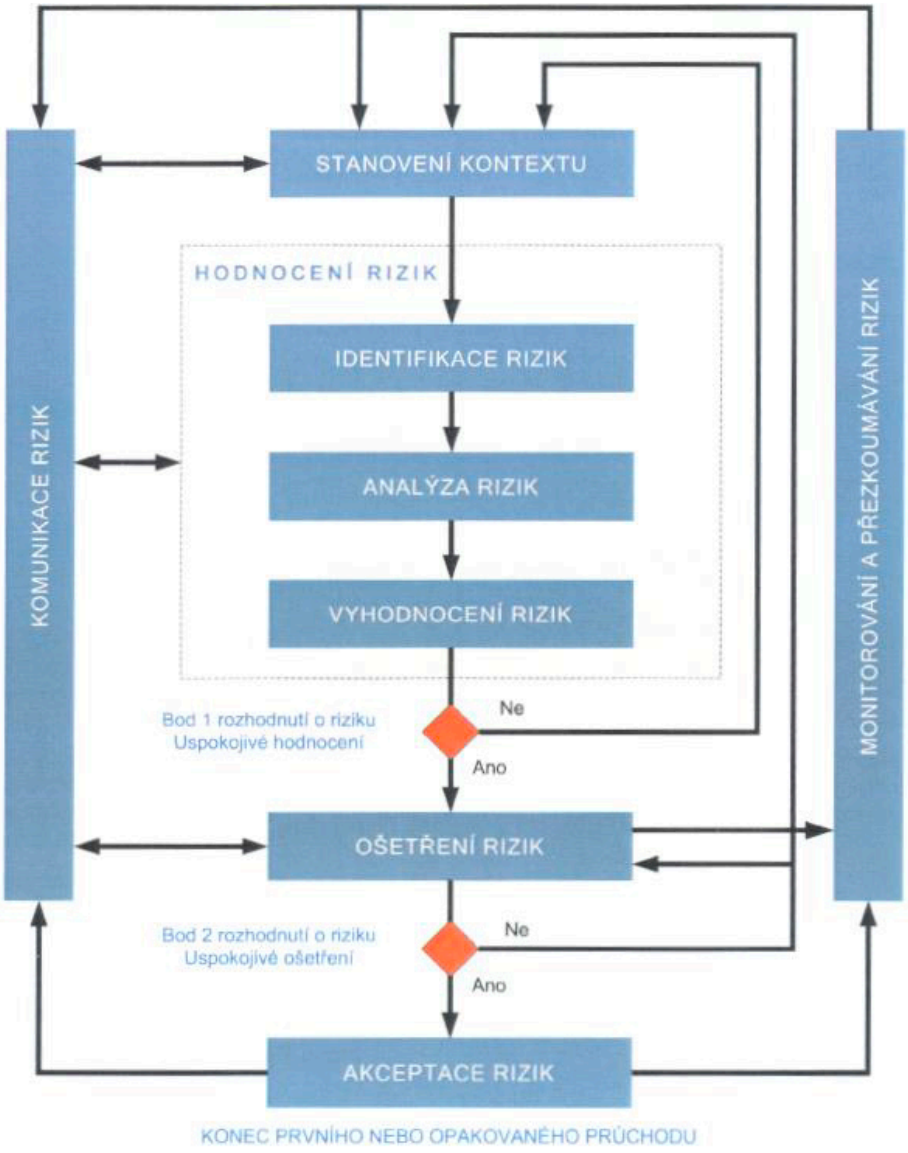
Proces řízení rizik je klíčovým nástrojem pro systematické řízení bezpečnosti informací a skládá se z několika navazujících fází. Pro zajištění bezpečnosti informací je nezbytně nést nepřetržitý dohled nad rizikovými situacemi, které mohou nastat při práci s daty. Z toho důvodu tyto situace je potřeba okamžitě detektovat, zjišťovat příčiny jejich výskytu spolu s jejich důsledky a vyhledávat nápravná opatření. Stejně jako se řídí většina klíčových procesů podniku pro správu rizik je nutné nejdříve zvolit metodologii – zde přichází mezinárodní standard ISO/IEC 27005,

který definuje proces řízení rizik informační bezpečnosti. Daný proces je velmi důležitý pro tuto práci, protože její praktická část se zaměřuje právě na analýzu a hodnocení rizik podniku a z tohoto důvodu bude zde detailně probrán.

„Řízení rizik musí pokračovat i po zavedení systému. Je těžké říci, k čemu bude nový vynález užitečný, útoky jsou stejně obtížné předvídat. Nelze očekávat, že ochranná opatření budou fungovat správně hned na začátku používání systému. Ve mnoha případech bezpečnostní politika se zavádí současně s implementaci systému, a následně se porušují v důsledku vývoje prostředí nebo produktu. Musí existovat mechanismus pro monitorování a řízení změn požadavků na ochranu.“ (Anderson, 2008).

Proces řízení rizik je znázorněn na obrázku č. 1 a představuje cyklické opakování jednotlivých činností, které jsou popsány v této podkapitole. Proces je aplikovatelný na libovolnou část podniku nebo jeho celek. Je ale nezbytně, aby všechna data bez výjimky byla zahrnuta do procesu řízení rizik bezpečnosti informací (ČSN ISO/IEC 27005, 2018).

Obrázek č. 1: Proces řízení rizik informační bezpečnosti



Zdroj: (ČSN ISO/IEC 27005, 2018)

3.3.1 Stanovení kontextu

První krok procesu řízení bezpečnosti informací je stanovení kontextu. Kontextem v daném případě je oblast pro řízení rizik. Stanovením kontextu se tak rozumí určení rolí a odpovědností v rámci procesu řízení rizik, metodiky analýzy rizik, kritéria a způsoby hodnocení a zvládání rizik.

Proces stanovení kontextu se skládá z třech etap. První etapou je **základní kritéria**. V této etapě se určují přístupy, kterými se riziko bude řídit. Když vhodný přístup k řízení rizik je zvolen, budou se řešit základní kritéria, jako jsou:

- kritéria pro hodnocení rizik – při výběru kritéria je potřeba si dávat pozor na strategickou hodnotu informačních aktiv podniku, právní a legislativní požadavky, dostupnost, integritu a důvěrnost firemních činností, očekávaní zúčastněných stran a reputaci;
- kritéria dopadu – měla by být vypracovány pro případ bezpečnostního incidentu a zařazovat závažnost poškozeného informačního aktiva, rozsah a důsledky incidentu;
- kritéria akceptace rizik – během výběru daných kritérií je nutno brát v úvahu, že:
    - kritéria mohou kolísat i za hranici přijatelného rizika, určené pro vyšší manažery, s tím, že budou zacházet s těmito riziky za definovaných okolností;
    - kritéria mohou být vyjádřena jako poměr odhadovaného zisku (nebo jiného obchodního prospěchu) k odhadovanému riziku;
    - na různé třídy rizik se mohou vztahovat různá kritéria přijatelnosti, např. rizika, která by mohla mít za následek nedodržení právních předpisů, nesmí být přijata, zatímco akceptování vysokých rizik může být povoleno, pokud je to uvedeno jako smluvní požadavek (ČSN ISO/IEC 27005, 2018).

Druhá etapa stanovení kontextu se zabývá **určením rozsahu a hranic**. Cílem této fáze je zajistit, aby při posuzování rizik byly brány v úvahu všechna relevantní aktiva. Určení hranic vyžaduje od společnosti co největší množství informací popisující prostředí, ve kterém se ona působí. Během této fáze zkoumá se strategie a politika organizace, obchodní procesy, legislativa a smluvní požadavky vztahující se na organizaci, informační aktiva, politické, geografické a sociálně-kulturní umístění organizace. Příklady rozsahu řízení rizik mohou být aplikace, infrastruktura IT, obchodní proces nebo definovaná část organizace.

Poslední třetí etapa je věnovaná **organizaci řízení rizik bezpečnosti informací**. Měla by být stanovena a udržována struktura a odpovědnost za proces řízení rizik. Hlavní role a odpovědnosti organizace jsou: vývoj procesu řízení, definice zúčastněných stran, jak interních, tak i externích, a jejich odpovědností, specifikace nezbytných záznamů. Definovaný postup by měl být schválen vedením firmy.

3.3.2 Posouzení rizik informační bezpečnosti

Druhou fází procesu řízení rizik je posouzení samotných rizik bezpečnosti informací. Riziko představuje kombinaci pravděpodobnosti výskytu události a jí důsledků. Hodnocení rizik kvantifikuje nebo kvalitativně popisuje riziko a umožňuje manažerům upřednostňovat rizika podle jejich vnímání závažnosti nebo jiných stanovených kritérií. Proces se skládá z identifikaci,

analýzy a vyhodnocení rizik. Posouzení rizik určuje hodnotu informačních aktiv, identifikuje hrozby a zranitelnosti, které existují nebo by mohly existovat, určuje možné důsledky a řádí odvozená rizika dle kritérií pro hodnocení rizik, stanovených v souladu s předchozí podkapitolou „Stanovení kontextu“. Výstupem posouzení rizik je seznam hodnocených rizik s určenou prioritou dle kritérií hodnocení rizika.

Identifikace rizik (risk identification) – proces hledání, rozpoznávání a popisu rizika. Následující kroky shromažďují vstupní data pro činnost analýzy rizik:

- identifikace aktiv firmy (např. HW, SW, etický kodex pracovníků, business procesy, sdílené „know-how“ atd.);
- identifikace hrozeb (např. neoprávněná akce, fyzické zničení, technické poruchy atd.);
- identifikace stávajících opatření (např. plány ošetření rizik, kontrol osob odpovědných za informační bezpečnost, fyzických opatření a auditů);
- identifikace zranitelných míst (např. organizace, procesy a postupy, provozní řízení, zaměstnance, fyzické prostředí, konfigurace informačního systému, HW, SW, komunikační zařízení atd.);
- identifikace důsledků (např. ztráta času, ztráta příležitosti, poškození zdraví a bezpečnosti, finanční náklady na specifické dovednosti nutné pro nápravu škody atd.).

Analýza rizik (risk analysis) – proces chápání povahy rizika pomocí posouzení pravděpodobnosti incidentu, jeho důsledků a určení úrovně rizika. Dělí se na:

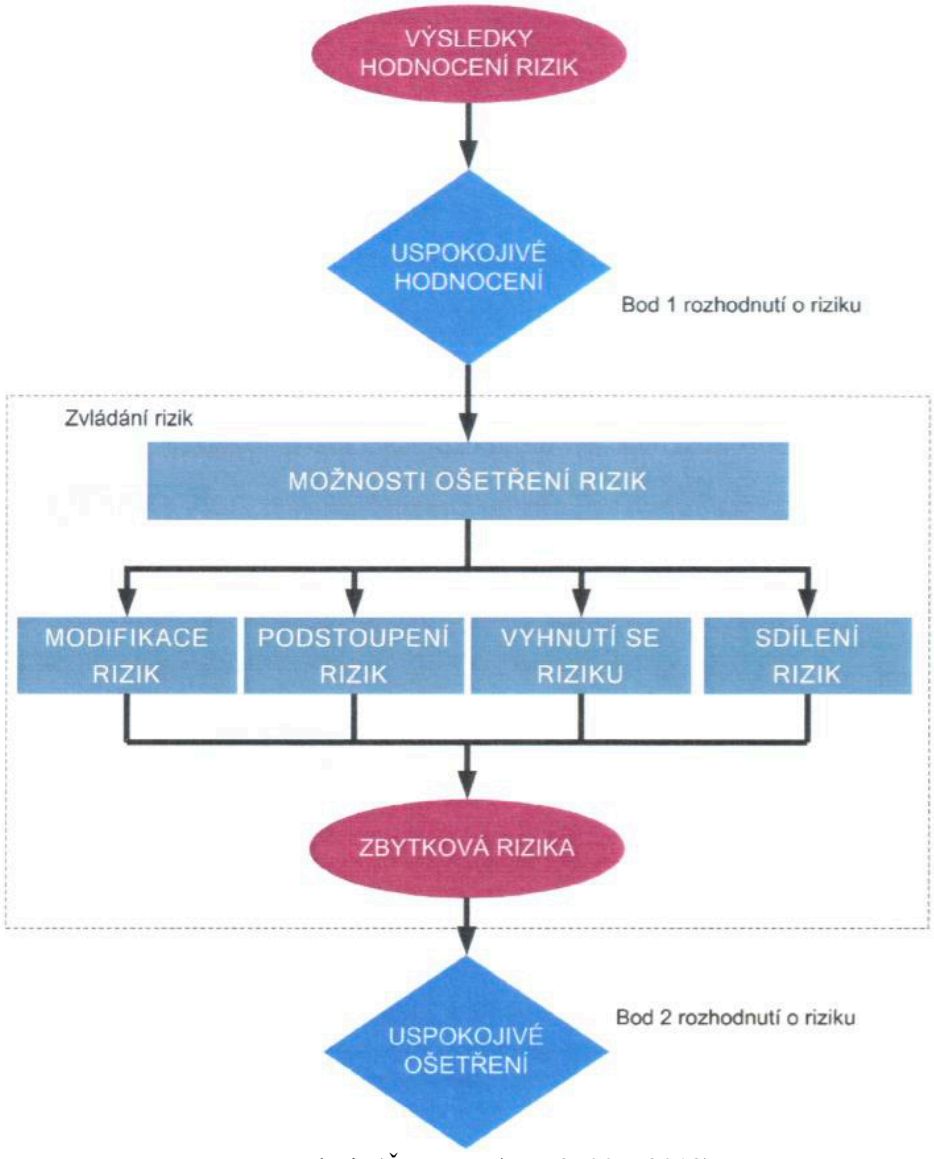
- kvalitativní analýzu rizik – řádí jednotlivá rizika dle pravděpodobnosti a rozsahu důsledků na nízká, střední a vysoká;
- kvantitativní analýzu rizik – využívá škálu s číselnými hodnoty pro hodnocení možných důsledků rizik.

Vyhodnocení rizik (risk evaluation) – proces porovnání výsledků analýzy rizik s kritérii rizika, vymezenými ve fáze stanovení kontextu, aby bylo možné určit, zda je riziko akceptovatelné nebo ne. Vyhodnocení rizik je hlavně založeno na akceptovatelném úrovně rizika. Agregace více nízkých nebo středních rizik může vést k mnohem vyšším celkovým rizikům a musí být odpovídajícím způsobem řešena. Výstupem činnosti hodnocení rizik je seznam rizik upřednostňovaných podle kritérií hodnocení rizika ve vztahu k scénářům incidentů, které k těmto rizikům vedou. (ČSN ISO/IEC 27005, 2018).

3.3.3 Zaopatření rizik informační bezpečnosti

Zaopatření rizik je třetí etapou procesu řízení rizik informační bezpečnosti. Cílem této etapy je vybrat nejvhodnější nástroje pro modifikace, postoupení, vyhnutí nebo sdílení rizika a definovat plán zaopatření těchto rizik. Proces zaopatření rizik je znázorněn na obrázku č. 2.

Obrázek č. 2: Proces zaopatření rizika



Zdroj: (ČSN ISO/IEC 27005, 2018)

Instrumenty zaopatření rizik se vybírají na základě výsledků posouzení rizika, očekávaných nákladů na implementaci těchto instrumentů a očekávaných z nich přínosů. Máme čtyři možnosti ošetření rizik, které se vzájemně nevylučují a jejich vzájemnou kombinací lze účinněji eliminovat riziko. Některá opatření mohou řešit více než jedno riziko (např. školení a povědomí

o bezpečnosti informací). Ve výstupu by měl být definován plán zaopatření rizik, který jasně určuje pořadí priorit a jejich časové rámce.

Modifikace rizik spočívá v zacházení s rizikem pomocí zavedení, odstranění nebo změny ovládání tak, aby došlo k přehodnocení rizika jako přijatelného. Náklady na vlastnictví systému je možné snížit pomocí správně vybraných ovládacích prvků zabezpečení informací. Ovládání může poskytovat jeden nebo více z následujících typů ochrany: korekce, eliminace, prevence, minimalizace dopadu, detekce, monitorování a informovanost. Při výběru kontrol je důležité zvážit náklady na pořízení ovládacích nástrojů s hodnotou chráněných aktiv.

Postoupení rizik – rozhodnutí o zachování rizika bez dalších opatření. Používá se při úrovních rizik, které dosáhli kritéria akceptace.

Vyhnutí se riziku je založeno na principu vyvarování činnosti, které způsobují zvláštní riziko. V případech, kdy riziko je považováno za příliš vysoké nebo náklady na zaopatření převyšují přínosy, nezbývá nic jiného, než se riziku vyhnout a odstoupit od plánované nebo stávající činnosti s tímto rizikem spojené. Například pro rizika způsobená přírodními a klimatickými podmínkami může být nákladově adekvátnější alternativou fyzicky přemístit ohrožený objekt na místo, kde riziko neexistuje nebo je pod kontrolou.

Sdílení rizik. Proces sdílení rizik může být efektivním způsobem ošetření rizik tím, že poskytuje možnost účinněji řídit konkrétní riziko. Sdílení může být zajištěno například prostřednictvím pojištění nebo outsourcingu rizikové oblasti. Ale je nutno dávat pozor na to, že odpovědnost za řízení rizika je možné sdílet, ale za normálních okolností nelze sdílet odpovědnost za dopad.

3.3.4 Akceptace rizik informační bezpečnosti

Po sestavení planu ošetření rizik následující etapou je akceptace rizik na základě daného planu. Během této fáze je potřeba řešit otázku akceptovaní rizik, stanovit odpovědnosti za tyto rozhodnutí, a to celé úředně zaznamenat. Ve finále procesu se zpracovává seznam akceptovaných rizik s odůvodněním pro ty, které nesplňují obvyklá kritéria přijatelnosti rizik organizace.

3.3.5 Sdělování a konzultování rizik informační bezpečnosti

Pátá etapa procesu řízení rizik – sdělování a konzultování rizik je nepřetržitým procesem, který organizace provádí za účelem poskytování, sdílení nebo získávání informací, a také pro budování dialogu se zúčastněnými stranami ohledně řízení rizik. Komunikace mezi zúčastněnými stranami je důležitá z toho důvodu, že může mít významný dopad na objektivitu rozhodnutí, které se tyká všech zúčastněných stran. Mezi hlavními cíli sdělování rizik jsou shromážděny informace o riziku, omezení výskytu bezpečnostních incidentů v důsledku vzájemného neporozumění mezi osobami s rozhodovací pravomoci a zúčastněnými stranami, podpora rozhodování, lepší koordinace činnosti, zlepšení povědomí.

3.3.6 Monitorování a přezkoumání rizik informační bezpečnosti

Finální etapou procesu řízení rizik je monitorování a přezkoumání rizik. Tato činnost spočívá v kontinuálním sledování a přezkoumávaní rizik a jejich faktorů (např. hodnota aktiv, dopady, hrozby, zranitelnosti, pravděpodobnost výskytu atd.). Úkolem procesu je včas identifikovat změny v kontextu organizace, které se mohou probíhat bez jakýchkoliv příznaků, aby nedošlo k ohrožení aktiv a zájmů firmy. Proces se rozděluje do dvou fází: sledování a přezkum rizikových faktorů a monitorování, kontrola a zdokonalení procesu řízení rizik.

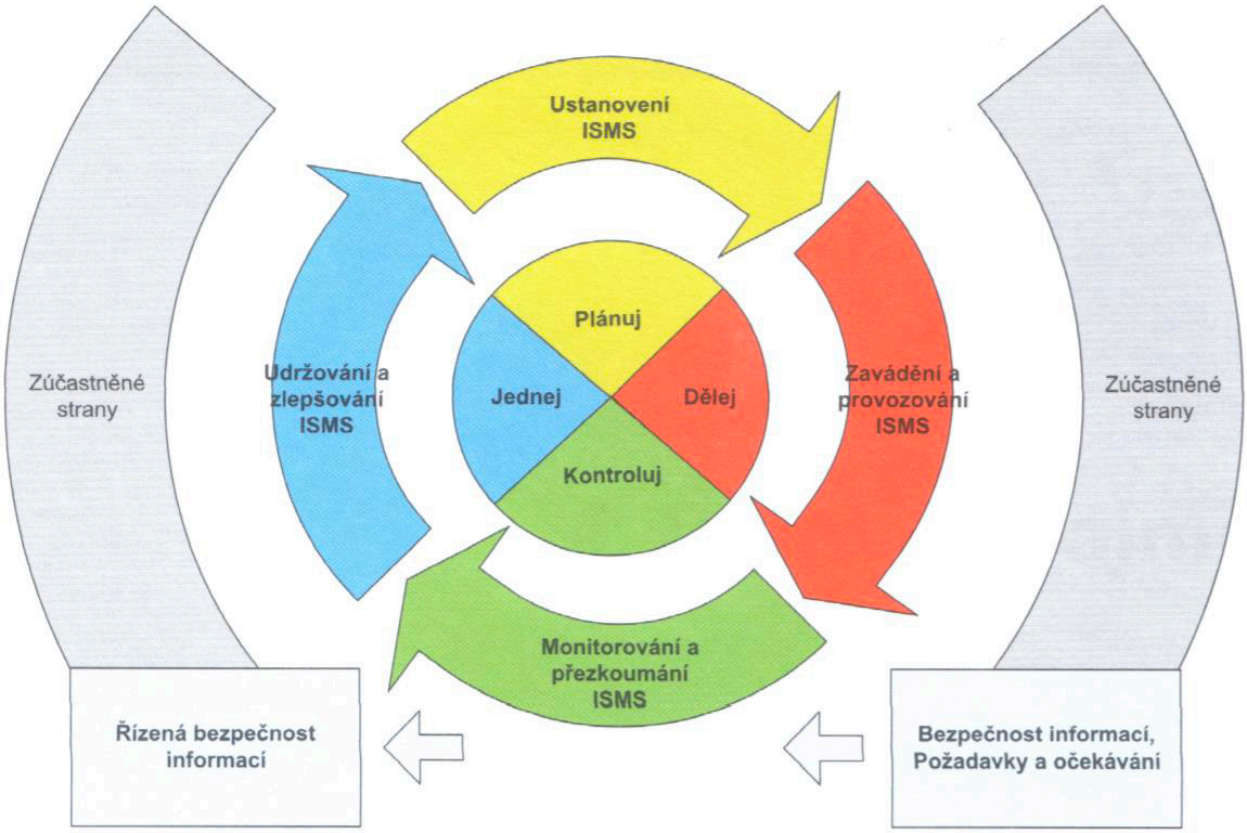
3.4 ISMS

ISMS (Information Security Management System) neboli Systém řízení informační bezpečnosti. Za ISMS se považuje soubor zásad a postupů pro systematické řízení citlivých dat organizace. Cílem systému ISMS je minimalizovat riziko a zajistit nepřetržitou činnost tím, že aktivně omezuje dopad narušení bezpečnosti. Daný systém chrání kritická podniková informační aktiva a důležitá data proti narušení důvěrnosti, integrity a dostupnosti. ISMS není dočasným řešením, které se zavede a tím skončí. Jedná se o kontinuální proces, který je neustále monitorován, aktualizován a zdokonalován.

ISMS je založen na principu **PDCA (Demingův model)**, což je iterativní čtyřstupňovou metodou, která se používá v podnikání pro řízení a neustálé zlepšování procesů a produktů. Norma ISO/IEC 27001 rozdělují procesní postup na ustavení, zavedení, provozování, monitorování, udržování a zlepšování efektivnosti ISMS v organizaci. Z obrázku č.3 je patrné, že ISMS přijímá na vstupu požadavky na bezpečnost informací a očekávání zainteresovaných stran. Též je lze vidět vzájemné propojení jednotlivých ISMS procesů, které jsou aplikovány na čtyři dané činnosti:

- **Plan** – stanovení ISMS politiky, určeni její rozsahu a odpovědnosti, které souvisejí s řízením rizik a posílením bezpečnosti informací ve společnosti tak, aby poskytovaly výsledky v souladu se stanovenými cíli organizace.
- **Do** – zavádění a provoz ISMS, řízení její procesů a postupů.
- **Check** – monitorování ISMS pomocí zajištění zpětné vazby a měření výkonu s ohledem na stanovenou politiku ISMS, cíle a praktické zkušenosti.
- **Act** – udržování a zlepšování efektivnosti ISMS; nápravná a preventivní opatření, založené na výsledcích interního auditu pro dosažení trvalého zkvalitňování ISMS.

Obrázek č. 3: Životní cyklus ISMS



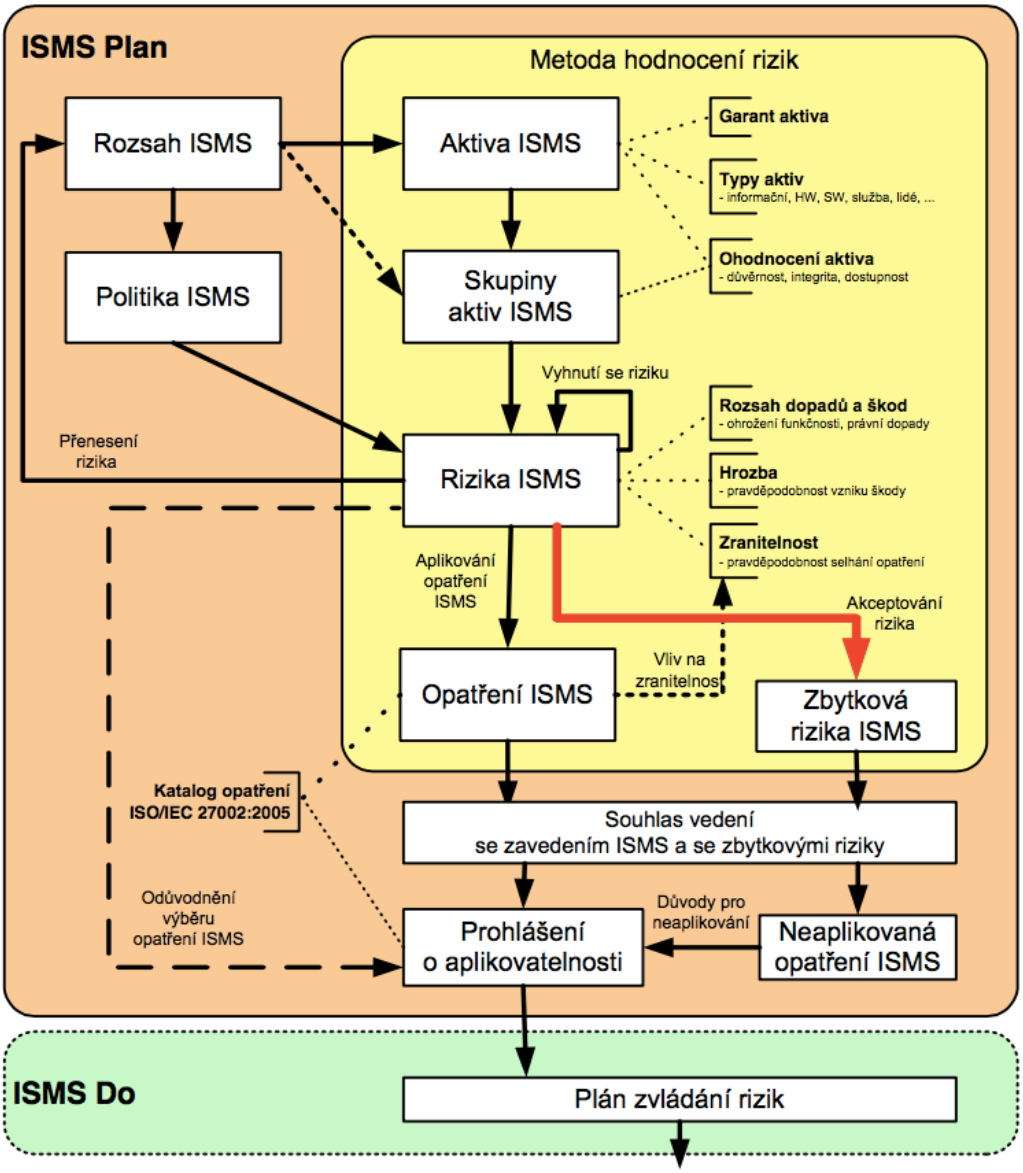
Zdroj: (Ondrák a kol, 2013)

3.4.1 Ustanovení ISMS politiky

První etapa budování ISMS je ustanovení jeho politiky a má za cíl určit rozsah a hranice, ve kterých ISMS bude provozován. V podstatě politiky nejen definuje základ celého systému řízení bezpečnosti informací, ale zahrnuje i kritické činnosti týkající se provedení analýzy rizik a výběru vhodných bezpečnostních opatření pro odstranění nebo zmírnění dopadů existujících rizik. Výsledky této etapy se využívají v dalších etapách ISMS, kde mají dlouhodobý vliv,

z tohoto důvodu je velice důležité zvážit veškeré souvislosti již v této první etapě – pozdější úpravy jsou velmi náročné a vyžadují vysoké finanční náklady.

Obrázek č. 4: Proces ustavení ISMS



Zdroj: (Doucek, 2011)

Na obrázku č. 4 lze vidět postup činností a zásadní vazby mezi nimi v etapě ustanovení ISMS. Prvním krokem je stanovení rozsahu ISMS, který má působení na politiku ISMS a aktiva, ze kterých se vytvářejí skupiny aktiv. Aktiva a skupiny aktiv mají takové vlastnosti, jako jsou garant aktiva, typy aktiv a ohodnocení aktiv. Tohle vše představuje potřeby ISMS, od čehož se pustí jeho návrh.

Druhý krok etapy ustanovení ISMS je prohlášení o politice ISMS, která je definována na základě současných a budoucích potřeb společnosti. Dokument politiky ISMS určuje podmínky pro

analýzu rizik a jeví sebou zájem vedení firmy o systém řízení bezpečnosti informací. Prohlášení o politice ISMS mimo jiného zahrnuje cíle ISMS, legislativu, kritéria hodnocení rizik a potvrzení o schválení vedením organizace (Doucek, 2011).

Další činnosti ustanovení ISMS je definice pravidel a postupů řízení rizik. Podrobné určení a pochopení rizik je jedním z nejpodstatnějších faktorů pro účinné fungování ISMS. Řízení rizik informační bezpečnosti dle normy ČSN ISO/IEC 27005 je detailně popsáno v kapitole 3.3.

Předposlední etapou je zaručení souhlasu vedení se zavedením ISMS a se zbytkovými riziky. Implementace ISMS je náročným procesem a vyžaduje jak úsilí zaměstnanců, kteří budou na projektu pracovat, tak i zvýšení nákladů. Z toho se pak vychází poslední krok budování ISMS – zpracování prohlášení o aplikovatelnosti a celkového planu zvládání rizik. Proces ustanovení má podstatný vliv na provozování ISMS během dalších etap jeho životního cyklu.

3.4.2 Zavádění a provoz ISMS

Tato část životního cyklu ISMS se zaměřuje na implementaci všech bezpečnostních opatření, které byly nadefinovány v etapě ustanovení ISMS. Tyto opatření by měli být řádně zdokumentovány v tzv. příručce bezpečnostních informací a vysvětleny všem uživatelům systému. Každá změna je zpravidla těžko přijímána a je nutné se postarat, aby lidé chápali důvody, kvůli kterým ke změnám dochází. V rámci zavádění a provozování organizace musí provést:

- formulace dokumentu Plán zvládání rizik, vymezení odpovídající řídící činnosti a odpovědnosti;
- zavedení plánovaných bezpečnostních opatření a formulace příručky bezpečnosti informací, která upřesní pravidla a postupy těchto opatření;
- definice programu budování bezpečnostního povědomí a programu školení;
- stanovení způsobů měření účinnosti vybraných opatření a určeni způsobů vyhodnocení těchto měření pro porovnání výstupů hodnocení;
- určení postupu pro detekci a reakci na bezpečnostní incidenty;
- řízení zdrojů, dokumentů a záznamů ISMS (Doucek, 2011).

Postupem času opatření se zapojí do každodenní činnosti lidí ve společnosti, a to od vedení po koncové zaměstnance. ISMS přináší řadu každodenních povinností: pro vybrané činnosti se tvoří záznamy o jejich provozu, kontrolují se aktiva, v pravidelných intervalech se aktualizují

bezpečnostní politiky a další. Sbírané záznamy o provádění klíčových činností v podniku jsou nezbytné jak pro interní zkoumání, tak pro audit, který díky nim může kontrolovat dodržování bezpečnostních opatření.

3.4.3 Monitorování a přezkoumávání ISMS

Následující etapa monitorování a přezkoumávání ISMS je nezbytná pro získání zpětné vazby na zavedená opatření. Kontroly se provádí pověřenými bezpečnostními experty či interními auditory a mají za cíl zjistit skutečný stav bezpečnosti a činnosti ISMS v podniku a porovnat ho se stavem, který podnik očekává.

V této části zavádění ISMS je nutné provést následující činnosti:

- provádění kontrol ze strany všech osob, které mají za fungování ISMS odpovědnost na všech manažerských úrovních. Součástí kontrol by mělo být i včasné zvládání bezpečnostních incidentů;
- provádění interních auditů ISMS, které by měly prověřovat dva aspekty ISMS – dodržování procesních pravidel a fungování jednotlivých bezpečnostních opatření. Norma ISO/IEC 21002 zde vystupuje jako hlavní kritérium auditu, podle kterého kontrolují se způsob, vhodnost a míra prosazení aplikovaných opatření;
- přezkoumání ISMS vedením organizace je činnost prováděna k určení vhodnosti, přiměřenosti a efektivnosti zavedených bezpečnostních opatření pro dosažení požadovaného stavu, která by měla probíhat pravidelně, zpravidla jednou za rok.

3.4.4 Údržba a zlepšování ISMS

Poslední etapou cyklu prosazování ISMS je údržba a zlepšování. Během této etapy se vyhledávají a sbírají návrhy na zlepšení fungování ISMS a provádí se následující činností:

- Zlepšování ISMS na základě zpětné vazby a zkušeností aktivních účastníků procesu.
- Odstraňování nedostatků ISMS, které zahrnuje dvě formy opatření. Opatření k nápravě odstraňují příčiny skutečně zajištěné neshody, naproti tomu preventivní opatření odstraňují příčiny neshody, která se ještě neprojevila, ale odklad může vést k tomu, že v budoucnu nějaká negativní událost se objeví.

4 Analytická část

4.1 Analýza současného stavu

Následující část práce je praktická a odráží faktický stav zajištění bezpečnosti informací v organizaci Milá papírna s.r.o., která z důvodu citlivosti informací uvedených v práci jmenována vymyšleným názvem. Analýza zároveň slouží jako podklad k návrhu bezpečnostních opatření pro zkoumanou organizace.

Řízení bezpečnosti informací, podnikových aktiv a řízení bezpečnostních rizik v dnešní době jsou jedněmi z nedůležitějších otázek při podnikání. Vzhledem k vysokým postihům za nedodržení směrnice GDPR, ochrana a zabezpečení zpracovávaných údajů by měli být jednou z prioritních činnosti podniku. Z těchto důvodů bylo rozhodnuto v rámci reálné organizace podnikající na internetu provést základní analýzu bezpečnosti a navrhnout řešení systému řízení rizik.

4.1.1 Popis firmy

Společnost s ručením omezeným „Milá papírna“ byla založena v březnu roku 2018 v Praze. Hlavní činností je maloobchod – firma se zabývá provozováním e-shopu papírenského zboží a designerských doplňků. Společnost vytváří návrhy designových kancelářských potřeb pomocí nezávislých designérů a objednává jejich výrobu od továren, většinou se importují ze třetích zemí. Po dodání je zboží naskladňováno v prostorách společnosti a je realizováno prostřednictvím internetového obchodu za pomocí externích doručovacích služeb. Organizaci celého procesu má na starosti ředitelka firmy, hotový e-shop dodává a udržuje třetí strana, veškerou administrativní práci vykonává sekretářka společnosti.

Organizace Milá papírna je mladá a rozvíjející, využívá externí „krabičkové“ e-shopové řešení a nakládá s citlivými daty, aktivně používá sociální medií a outsourcuje několik svých činností. Je totiž důležité zmínit, že technologický pokrok a změna spotřebitelského chování v současné době způsobují strmý růst obratu e-commerce trhu v ČR – meziroční změna na konci roku 2019 je +16 % a podíl e-commerce na celkovém maloobchodním obratu je 10,2 % (Ceska-ecommerce.cz, 2019). Tohle dělá podnik Milá papírna s.r.o. typickým příkladem současného trhu a jednoho z nejpopulárnějších směru podnikání. V souladu se vším výše uvedeným firma jeví sebou výborný objekt zkoumání rizikových oblastí a posouzení jejich závažnosti.

4.1.2 Personální vybavení

Společnost „Milá papírna“ je soustředěná na minimální zaměstnanecké zatížení a outsourcuje značnou část svých činností. Stálých pracovníků v této firmě jsou tři. Největší část práce vykonává ředitelka společnosti: vymýšlí a kompletuje veškerý sortiment zboží, hledá dodavatele a partnery, komunikuje s nimi a rozhoduje o chodu společnosti. Vedoucí jsou přímo řízeny sekretář a PR manažer.

Sekretářka pracuje většinou v provozovně a má na starosti běžnou komunikaci, správu objednávek a skladovou evidenci, dohled za správným provozem webu a dílčí moderace obsahu e-shopu. Má na starosti zákaznickou linku obchodu. Pracuje ve společnosti od začátku její založení, má vysokoškolské vzdělání v ekonomickém oboru a dobře se orientuje v počítače, ale je zkušená zejména v kancelářském SW a otázce bezpečnosti moc nerozumí.

PR manažerka je mobilním pracovníkem – odpovídá za správu sociálních medií (Instagram, Facebook, WhatsApp) a reaguje na komentáře a otázky, které zákazníci posílají prostřednictvím výše uvedených messengerů. Větší část jí prací spočívá ve tvorbě propagačních příspěvků na Facebook Business Manager, což dělá přes osobní účet, kterému byl udělen přístup pouze pro správu reklamních kampaní, takže nemá přístup k nastavením firemní stránky.

Zaměstnanci jsou proškolování na základních věcech, týkajících se informační bezpečnosti. Zároveň jsou též zaškolení o bezpečnosti a ochraně zdraví při práci a o bezpečnosti požární. Školení zatím probíhá jednou, a to při nástupu do práce. Na reálné hrozby z kybernetického prostředí pracovníci připraveny nejsou.

4.1.2.1 Externí subjekty

Nejpodstatnější oblast, která je v tomto podniku svěřena třetí straně, je samotný e-shop, a zejména jeho technická podpora. Vysvětluje se to obrovskými náklady na programování vlastní e-commerce platformy, její náročnou administrací a nutností zajištění nepřetržité podpory. V případě krabicového řešení vše potřebné pro aktualizaci systému, včetně úprav spojených s vývojem účetní a daňové legislativy, jsou automaticky prováděny poskytovatelem. Přítomnost telefonické a e-mailové podpory eliminuje nutnost mít odborníka na plný úvazek.

Druhý závažný úsek podniku je účetnictví, které je svěřeno nezávislému účetnímu, pracujícímu na živnostenský list. Společnost není plátcem DPH a povinností účetního se na dané etapě spočívá ve zpracování generovaných e-shopem faktur a bankovních výpisů, zpracování mezd zaměstnanců včetně všech odvodů a registrací, roční sestavení daňového přiznání a účetní závěrky. Zpracování probíhá v účetním systému Money S3, ale data se do něho zadávají ručně. Sekretářka společnosti nejprve kompletuje soubor faktur a posílá je e-mailovou zprávou účetní pro zaevidování. Firma a účetní komunikují primárně prostřednictvím e-mailových zpráv nebo osobním setkáním pro projednání zvláštních problémů a otázek. Společnost nemá zajištěný přístup pro účetní do administrace e-shopu, ani do datové schránky.

Dopravu zboží zákazníkům společnost zajišťuje pomocí systému Zásilkovna, který poskytuje možnost podávat a odebírat zásilky přes jejich rozsáhlou partnerskou síť výdejních míst. Kromě dopravy a výdeje zásilek na výdejní místa Zásilkovny, společnost využívá také možnosti podání na partnerská výdejní místa společnosti České pošty a kurýrní dopravy DPD. Zásilkovna je napojena přímo na e-shop přes API klíč, pomocí kterého jsou importovány výdejní pobočky do obchodů a zákazník má možnost je snadně vyhledat pomocí interaktivní mapy. V administraci internetové aplikace Zásilkovny se nachází kontrolní nástroje, které umožňují importovat zásilky ve formátu csv nebo xml souborů, získaných formou exportu objednávek z e-shopu. Palubní deska aplikace poskytuje neustálý přehled o odeslaných zásilkách, dobírkách a fakturách. Aplikace splňuje podmínky náležitých norem, tedy že záznamy údajů v informačním systému a v její databáze jsou spolehlivé a jsou chráněny proti změnám.

Firma také nedisponuje IT oddělením. Instalací firemní techniky a síťové infrastruktury se zabývá externí společnost. Většina stížností se týká e-shopu a jeho provozu, které jsou na starosti dodavatelské společnosti. Ostatní problémy se řeší dle úrovně obtížnosti, bud‘ jednatelkou samostatně, nebo pomocí externího technika, který však není v úzkém kontaktu se zaměstnanci a nemá tak ucelený přehled nad aktuálními požadavky na IT ze strany vedení firmy.

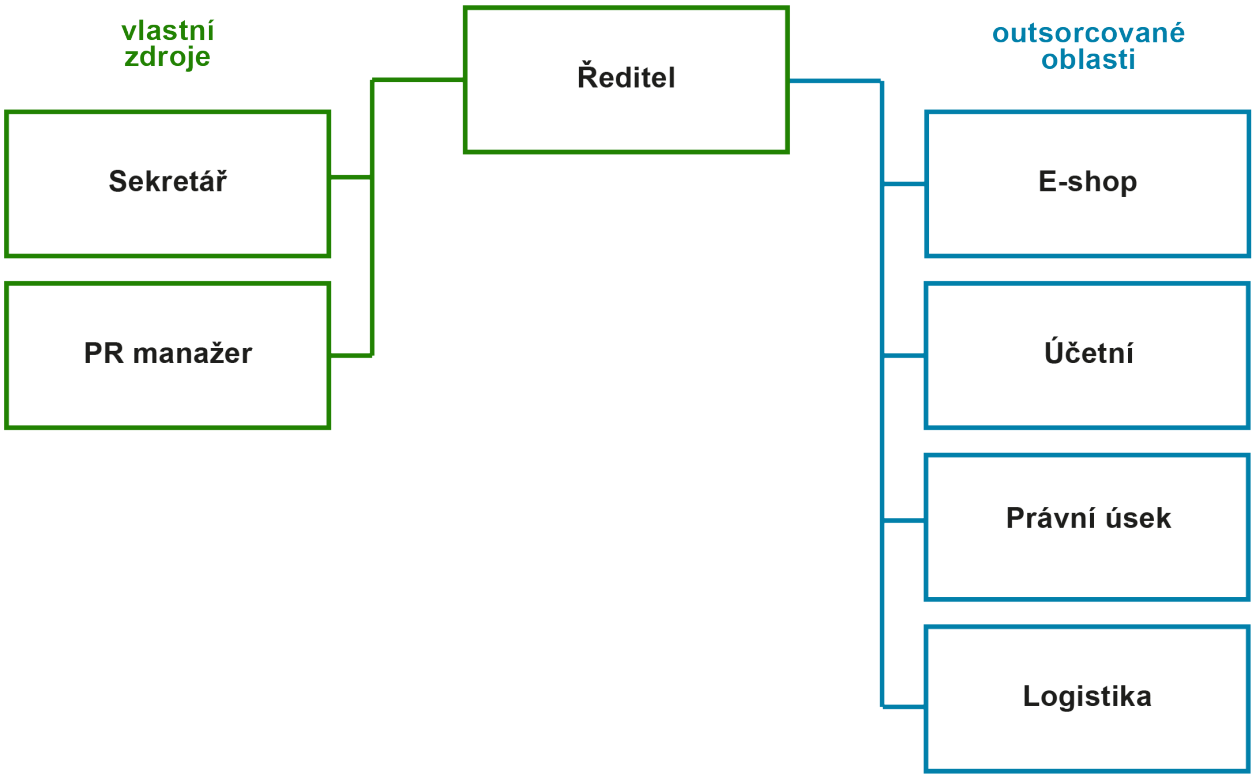
Společnost též má několik uzavřených smluv o dílo s designéři, kteří pomáhají vytvářet návrhy pro výrobu zboží a vzhled webových stránek. Komunikace probíhá e-mailem a na sociálních sítích. Rozpracované a dopracované projekty jsou sdělovány přes Google Disk.

Nakonec firma se občas využívá právní služby na webových stránkách DostupnyAdvokat.cz v případě, když potřebuje sepsat novou smlouvu nebo právní dokumentaci anebo řešit nějakou právní otázku. Konzultace se provádí přes desktopovou aplikaci Skype, bud‘ jednatelkou přes

přenosný počítač, anebo sekretářkou, poté výsledky jednání a další případné dokumenty se zasílají na e-mail jednatelky.

Stručný přehled personálního vybavení společnosti je znázorněn na obrázku č. 5 a je rozdělen do dvou větví – vlastní zdroje a outsourcované oblastí.

Obrázek č. 5: Organizační struktura podniku



Zdroj: Vlastní zpracování pro potřeby DP

4.1.3 Technické vybavení

Tato část je věnována popisu veškerého technického vybavení neboli hardwaru firmy, jeho stavu a provozním aspektům, vztahujícím se k informační bezpečnosti dle výše uvedených norem a pravidel. Dále sleduje záznamy o síťové infrastruktuře a o míře jí zabezpečení.

4.1.3.1 Hardware

Organizace vlastní jeden stolní počítač značky Hewlett-Packard, který se nachází v kanceláři a slouží ke správě obchodu, administraci e-shopu a k další firemní evidenci. Stroj je v provozu od roku 2018 (je stále v záruce do června roku 2021) a je v perfektním stavu. Používá se jediným

administrativním pracovníkem a občas jednatelkou. Také pro firemní potřeby se používá přenosný počítač Apple Macbook Pro 2018, který ředitelka má vždy u sebe v případě naléhavé potřeby. Nejčastěji se však počítač používá pro komunikace s dodavateli a partneři, a také pro rozvoj a grafickou úpravu firemních projektů.

V souvislosti s tím, že samotný e-shop běží na serverech poskytovatele, společnost nepotřebuje mít vlastní server ani serverovou místnost, a zároveň nepotřebuje vlastní databázi. Jako datové uložiště se používají dva externí disky. WD Elements Portable s kapacitou 4TB je trvalým uložištěm, které se vždy nachází v kancelářském trezoru. Pro běžný přenos a ukládání dat se používá WD Elements Portable s kapacitou 1TB. Disky byly pořízeny na začátku roku 2019 a oba jsou v záruce.

Dalšími kancelářskými strojí jsou dvě tiskárny. První je multifunkční laserová tiskárna Samsung SL-C480W (je v záruce do června roku 2020), která je spojena s počítačem přes síť Wi-Fi, a druhou je malá tiskárna dopravních štítků Zebra GK420D, propojená sériovou linkou RS-232. Obě tiskárny byly pořízeny společně s počítačem v roce 2018, tiskárna na štítky Zebra se používá nejčastěji a už je krátce před koncem záruky, proto dostává o bod méně než ostatní hardware.

V následující tabulce č. 1 jsou zaznamenány vše hardwarové prostředky podniku a jejich hodnocení na stupnici od 1 do 5, kde 5 znamená výborný a 1 – nepříjemný stav. Jak už bylo zmíněno výše, všechny stroje jsou nové a jsou ve skoro perfektním stavu – průměrné hodnocení je **4,86**.

Tabulka č. 1: Hardwarové vybavení podniku

	počet	hardware	umístění	rok pořízení	hodnocení
tiskárny	1	Samsung SL-C480W	kancelář	2018	5
	1	Zebra GK420D	kancelář	2018	4
počítače	1	HP ProDesk 400 G4 Micro Tower Intel Core i5 7500 Kaby Lake 3.8 GHz	kancelář	2018	5
	1	MacBook Pro 13" Retina	ředitel	2018	5
externí disk	1	WD 2.5" Elements Portable 4TB	kancelář	2019	5

	1	WD 2.5" Elements Portable 1TB	ředitel	2019	5
router	1	D-LINK DIR-853	kancelář	2018	5

Zdroj: Vlastní zpracování pro potřeby DP

4.1.3.2 Síťová infrastruktura

Síťovou infrastrukturu v první řádě tvoří kabeláž vedena do kancelářské jednotky, která je uložena pod omítku, takže není viditelná. Nová kabeláž budovy byla položena před 4 roky a je v dobrém stavu. Telekomunikační zásuvky v budově nejsou žádným způsobem chráněny, přesto jsou nainstalovány pouze v místech veřejně nepřístupných. V prostředí zkoumané firmy se nachází jedna zásuvka, do které je připojen Wi-Fi router značky D-LINK.

Společnost je připojena do internetové síti prostřednictvím jediného ISP (Internet service provider) – společnosti O2. Tenhle faktor zvyšuje riziko výpadků a jako následku odpojení firmy od internetu a nemožnosti správy e-shopu a celkového chodu společnosti. V názvu Wi-Fi sítě neboli SSID (Service Set Identifier) není žádný odkaz na název společnosti. Přístupové heslo je měněno jednou za rok. Teoretická rychlost připojení je 50Mb/s za download a 5 MB/s za upload. Součástí Wi-Fi routeru je firewall, který monitoruje a filtruje příchozí i odchozí komunikací do vnitřní sítě, a má další pokročilé funkce zvyšující úroveň ochrany, jako je například nastavení bezpečných VPN (Virtual Private Network) tunelů s možností filtrování obsahu, které se však nepoužívají, nebo se používají v omezeném rozsahu.

4.1.4 Aplikační vybavení

Aplikační vybavení tvoří operační systém a aplikace. Na firemní pracovní stanici je nainstalován operační systém Windows 10 Pro, na kterém jsou vytvořeny administrátorský účet pro užívání jednatelkou a zaměstnanecký účet. Zaměstnanecký účet však má povolenou instalaci jakéhokoliv softwaru a přístup k internetu jim není žádným způsobem omezen. Přenosný počítač běží na standartním Mac OS. Má rozdělené účty pro osobní a firemní použití – vše komunikace společnosti probíhají ve firemním účtu. Účty jsou chráněny hesly, která se mění jednou za rok jednatelkou spolu s příslušným zaměstnancem.

Pro zabezpečení pracovní stanice slouží licenční antivirové řešení Avast Business od společnosti Avast Software s.r.o. Ale testování počítače na přítomnost virů je prováděno nepravidelné. Expresní testy se snaží provádět alespoň jednou za týden, ale plný virový test v lepším případě se dělá jednou za půl roku. Stahování virových databází a aktualizace aplikací jsou nastaveny pravidelné. Mezi nejdůležitějšími vestavenými softwary MacOS jsou nástroj pro šifrování disku FileVault a Keychain Access pro ukládání hesel.

Dalšími nejpoužívanějšími licenčními SW jsou balík Microsoft Office, Adobe Photoshop a Adobe Illustrator v návaznosti na časté grafické úpravy a práci s produktovými fotografii, a Adobe Reader kvůli velkému objemu dokumentů a potřeby jejich úprav.

4.1.4.1 E-shop

Společnost Milá papírna využívá přednastavený e-shopový systém UPgates, který vyvinula a spravuje společnost EVici webdesign s.r.o. Společnost poskytuje k dočasnému užívání za úplatu aplikaci – internetový obchod vytvořený pomocí šablony, spolu s technickou podporou.

Na začátku podnikání firma volila mezi open-source řešením (v první řadě Prestashop) a pronájmem „krabicového“ hotového e-shopu. Zřejmými nevýhodami open-source varianty byly zploštělost základních konfigurací a nutnost hledat doplňkové rozšíření (např. napojení na platební bránu, fakturační program atd.), otevřenost zdrojového kódu, což bývá častým lákadlem spamových útoků hackerů, kteří vyvíjí speciální doplňky právě pro tento účel. Zapojená technická podpora a nepřizpůsobivost většiny open-source platform pro český trh a české nákupní zvyklosti se staly rozhodujícími důvody pro zvolení krabicového řešení. Nakonec byl zvolen e-shop od UPgates díky většímu počtu modulů i v základní verzi a možnosti snadně upravovat vzhled stránek pomocí speciálního modulu Designer.

Přístup do administrace e-shopu je realizován prostřednictvím klasického formuláře, kde se zadávají přihlašovací údaje, které jsou třeba vyplnit při instalací. E-shop je po celou dobu trvání smluvního vztahu provozován na vývojářských serverech, které jsou umístěny v Londýně a Frankfurtu u provozovatele serverů společnosti Linode, LLC. Pro komunikaci webového prohlížeče se serverem se používá protokol HTTPS (Hypertext Transfer Protocol Secure). Společnost-odběratel nemá nárok na jakoukoliv manipulace se zdrojovým kódem, za výjimkou individuální úpravy vzhledu webových stránek pomocí vkládání vlastních stylopisů ve formátu css nebo less do speciálního editora kódu, který je součásti administrace e-shopu.

Administrativní část e-commerce stránek je užitečným systémem, v němž uživatelé, resp. administrátor elektronické prodejny přidávají, upravují nebo vymazují produkty, spravují objednávky, provádí komplexní nastavení katalogů a stránek. Systém tedy umožňuje komplexní správu elektronické prodejny, proto musí být přístup k němu vymezen pouze pro oprávnění uživatele.

Po přihlášení se na stránce zobrazí úplný přehled objednávek za týden, měsíc anebo rok, běžný a celkový obrat. Dále jsou upozornění na produkty pod limitem stavu zásob, nové objednávky, kontakty a komunikace. Na konci takzvané nástěnky se nachází přehled o využité produkční a paměťové kapacitě obchodu. Jednotlivé kategorie jsou zobrazeny v rozbalovacím menu v levé části stránky. Kategorií jsou tady docela hodně a snaží se umístit obrovské množství funkcí. Ale jsou v tom i určité nevýhody. Jednotlivé prvky nastavení tak či onak jsou vzájemně propojeny, což ztěžuje jejich zařazení do logických kategorií. Všechny funkční moduly e-shopu od UPgates jsou roztříděny do 9 kategorií, které se rozpadají do dalších podkategorií a to jsou:

- obchod – obsahuje seznam objednávek a příslušných faktur;
- produkty – seznam produktů a jejich klasifikace;
- obsah – slouží pro úpravu samostatných stránek, článků, bannerů atd.;
- zákazníci – seznam zákazníků a jejich osobních údajů;
- statistiky – přehledné grafy se statistickými data obchodu;
- soubory – správce nahráních souborů;
- grafika – modul Designer a editor kódu;
- nastavení – globální nastavení obchodu včetně napojení na dopravce, účetní systémy, EET a další systémy třetích stran, nastavení možností plateb, průvodce importem/exportem;
- můj učet – peněženka, tarifní plán, nastavení profilu a přihlašovacích údajů, formulář technické podpory.

Systém neosahuje bezpečnostní nastavení a lze celkem říci, že řešeni UPgates neposkytuje žádnou možnost zasahování a monitorování interních bezpečnostních procesů. To je plně odůvodněno skutečností, že systém není určen pro pokročilé uživatele.

Data se do e-shopu importují a exportují několika různými způsoby. Všechny grafické prvky a fotografie zboží, které se zobrazují na webu nahrává se rovně z hlavního počítače do modulu spravujícího nahrané soubory v systému e-shopu. Systém přepravce Zásilkovna je napojen přes API klič, ale napojení je jednostranné – Upgates importuje výdejní místa, ale neposílá nazpátek

do Zásilkovny informaci o objednávce. To se musí exportovat ručně v podobě csv nebo xml souborů, které se dočasně ukládají na počítače společnosti. Po zadání objednávek do systému Zásilkovny soubory se vymazují. Dalším napojeným prvkem je platební brána Comgate od společnosti ComGate Payments, a.s. Do e-shopového sytému je také napojena přes API, ale už oboustranně – provádí platbu, ověřuje její stav a pak ho vrací e-shopu. Systém je také napojen na Elektronickou evidenci tržeb (EET) pomocí přístupového hesla a bezpečnostního certifikátu, které podnik obdržel při žádosti o přístupové údaje k EET na portálu daňové správy. E-shop odesílá účtenky, které obsahují náležitosti EET pro evidenci na finanční úřad.

Technickou a zákaznickou podporou e-shopu se rozumí především poskytnutí pomoci při stížnostech v používání systému (např. napojení externích služeb) a nahlášení incidentů včetně incidentů bezpečnosti informací. Podpora má jen omezený přístup do administrace e-shopu, konkrétně nezbytný pro administrace prezentační části aplikace, aktualizace softwaru, opravu vad e-shopu, sledování zatížení prezentace a případných útoků z internetu. Dotazy na technickou podporu a hlášení vad se posílá převážně e-mailem nebo prostřednictvím formuláře technické podpory v administraci e-shopu.

4.1.5 Fyzická bezpečnost

Firma sídlí v kanceláři, kterou pronajímá spolu se skladovou místností v kancelářské budově na okraji Prahy. Budova má čtyři patra a je používána dalšími společnostmi. Pronajatý prostor se nachází v prvním patře a skládá se ze dvou místností o celkové výměře 50 m2. Prostor je uzamykatelný a po čas nepřítomnosti zaměstnanců je uzamčený. Dveře nejsou příliš silné a mohou být snadno vylomeny. Klíče od kanceláře vlastní ředitelka a sekretářka, jedna kopie je uložená ve schránce u ostrahy budovy pro nouzový případ. Tudíž jiné návštěvníky budovy přístup do firemní jednotky nemají. Ale i v době přítomnosti zaměstnanců existuje riziko nepovoleného vstupu třetích stran v zázemí podniku, protože dveře zůstávají otevřené. Kancelář a sklad jsou vybaveny elektrickou požární signalizací a samočinným hasícím zařízením.

Zabezpečení budovy však není příliš silné. Lokalita, ve které se stavba nachází, je průmyslová s přebývajícím množstvím stavebních projektů v okolí, není záplavová ani seismicky aktivní, avšak existuje nebezpečí v podobě lidského faktoru. Bez ohledu na to hlavní vstup do budovy je trvale otevřený, zavírá se jenom v noci po 22. hodině generálním klíčem. Dveře jsou prosklené, žádní turnikety nebo vrata na vstupu nejsou, ostraha eviduje návštěvníky a čas jejich návštěvy, avšak dále osoby se pohybují po areálu budovy bez jakéhokoliv dozoru. Celá recepční zóna je

monitorována kamerovým systémem. Na hlavních dveřích je oznámení, které upozorňuje návštěvníky o užití kamer. Druhý a poslední vstup se nachází v právem křídle budovy a je většinu času zamknutý, přístup k němu má pouze obsluha budovy s generálním klíčem. Dveře jsou kovové, ale nechráněné kamerami. Druhá kamera se nachází na okraje levého křídla budovy, která umožňuje pohled na ulici za budovou, kde se nachází parkoviště a zóna pro nakládku a vykládku. Záznamy z kamer jsou chráněny na pevném disku po dobu 48 hodin, pak data jsou vymazána. Byla jsem přesvědčená správcem budovy, že provoz kamerového systému, a zejména zabíraní dat a nakládaní s nimi se provádí dle jednoznačných pravidel pro zabezpečení zpracovávaných dat, a to včetně pravidelné kontroly funkčnosti kamerového systému.

4.1.6 Bezpečnost informací

Bezpečnost nejzávažnější papírové dokumentace a datových nosičů v organizaci je řešena formou trezoru 1. bezpečnostní třídy dle normy EN 1143-1. Pro ochranu digitálních informací uložených na disku pracovní stanice se používá antivirová aplikace Avast Business s vestaveným firewallem, který slouží jako doplňková ochrana pro vestavený HW firewall.

Externí zálohový disk je trvalým uložištěm a slouží jako opatření proti útokům podnikových informací, zálohy na něm se dělají jednou za 2-3 měsíce a mimo použití je trvalé uložen v trezoru. Na lokálním disku, ze kterého se dělají zálohy, je chráněna historie objednávek a příslušných faktur, dodavatelských smluv, účetních záznamů týkajících se zaměstnanců. Některé z těchto informací tvoří součást obchodního tajemství a know-how. Proto jejich útok ke třetí straně nebo ztráta osobních údajů zákazníků by měly vážné právní následky až existenční potíže pro organizace.

Druhý menší disk se používá pro běžný přenos a ukládání interních podnikových dat, ale většinou obsahuje fotografie zboží, které nemají příliš vysokou povahu.

Bez ohledu na to, že přenosný MacBook obsahuje rozpracované projekty ve velkém rozsahu, drobné smlouvy a další podnikové dokumenty, nemá stanovenou frekvence zálohování a zálohy se dělají na osobní externí disk ředitelky společnosti. Funkčnost těchto záloh není kontrolována.

Stroje jsou v dobrém stavu, ale vždy existuje riziko selhání některé ze stanic, což by znamenalo pro podnik značné finanční náklady na jejich opravu. Nicméně téměř všechna data jsou ukládána

na zálohových discích a závady pracovních stanic by neměly za následek významné potíží pro společnost. Rovněž selhání softwaru by mělo jenom dočasný vliv na činnost společnosti.

Z důvodu toho, že e-shop společnosti běží na serverech dodavatele, firma nesbírá a nechrání osobní data, která on shromažďuje. Skutečnost, že registrace na webových stránkách společnosti není povinná a stejně není podmínkou pro nákup také minimalizuje sběr osobních údajů a citlivých dat.

4.1.7 SWOT analýza

SWOT analýza je založená na hodnocení silných a slabých stránek organizace a jejich okolností, které mohou pozitivně nebo negativně ovlivnit chod společnosti.

Tabulka č. 2: SWOT analýza

Silné stránky (S)	**Slabé stránky (W)**
• originalita • perfektní stav aktiv • dodavatelská kvalita • pozitivní vývoj ukazatelů • aktivní využití sociálních medií	• slabé strukturování a rozdělení odpovědností • malý rozpočet • nedostatek sil, které by se časem nahradily současných zaměstnanců • nízká úroveň připravenosti zaměstnanců na bezpečnostní incidenty
Příležitosti (O)	**Hrozby (T)**
• změna spotřebitelského chování • dynamicky se rozvíjející oblast • outsourcing činností • nízká regionální konkurence	• uživatelské chyby • zneužití zranitelných míst fyzické bezpečnosti • importní podmínky

Zdroj: Vlastní zpracování pro potřeby DP

Ze SWOT analýzy vyplývá, že mezi silné stránky podniku patří zejména jeho neobvyklost a dobrá technická a aplikační vybavenost. K silným stránkám také patří udržování přiměřených vztahu se zákazníky prostřednictvím sociálních sítí, což podporuje oslovení zájmových skupin. Příležitostmi jsou takové okolnosti, jako je změna spotřebitelského chování a soustředění se firmy na své hlavní činnosti. Z hlediska slabých stránek má problémy pocházející z toho, že je mladou firmou. Z důvodu její menší velikosti není stanovena jednoznačná struktura a existuje nedostatek pomocných pracovních sil. Mezi hrozbami jsou případné uživatelské chyby a

zhoršující se importní podmínky z důvodu zesílení podpory českých výrobců – podnik obchoduje s třetími zeměmi.

4.1.8 Shrnutí aktuálního stavu bezpečnosti firmy

Následující část práce jeví sebou shrnutí analýzy současného stavu bezpečnosti informací v podniku pomocí rozdělení do relevantních částí, které jsou definovány normou ISO/IEC 27002 a korelují se s jednotlivými bezpečnostními opatřeními, obsahovanými v kapitolách 5-18 této normy, a to na základě popsané situace v předchozích částech. Na tyto opatření se musí dávat pozor v rámci procesu zavádění ISMS.

A.5 Bezpečnostní politika

Dokument bezpečnostní politiky informací ve firmě není úředně sepsán ani udržován. O bezpečnosti informací se stará jednatelka společnosti, ale většinu provozních činností vykonává sekretářka, která byla před nastoupením do práce informována o bezpečnostních opatřeních a vychází z toho při nakládaní s daty. Avšak žádný jediný dokument není sepsán, jakož i dokumenty o změnách a přezkoumání změn v politice bezpečnosti.

A.6 Organizace bezpečnosti

Odpovědností a role v oblasti bezpečnosti informací nejsou jednoznačně přiřazeny kvůli malému počtu pracovníků a existují většinou v ústní formě. Ale chybějící popis bezpečnostních procesů vyvolává nejasné přiřážení pracovních odpovědností za kontrolu a plánování změn v těchto procesech. Takový přístup má za následek špatné povědomí zaměstnanců a vědění organizace o aktuálním stavu bezpečnosti v podniku, a práce se stává méně efektivní. Činnosti pracovníka ve smlouvě jsou pouze obecně popsány. Kontakty s příslušnými orgány jsou řádně dodržovány. Opatření k ochraně vzdálených pracovních stanic se využívají v minimálním rozsahu a nejsou formálně zdokumentovány.

A.7 Bezpečnost lidských zdrojů

Společnost odpovídá za své zaměstnance po podepsání pracovní smlouvy, která je vytvořena na základě pracovního zákoníku České republiky. Zaměstnanci jsou přijaty do práce po poskytnutí svých identifikačních údajů, životopisu, příp. i dokladu o dosaženém vzdělání a provedení pohovoru. Informace o zaměstnancích existuje jak v papírové podobě, tak i v digitální a jsou nahrány na zabezpečené úložiště. Odpovědnosti za bezpečnost informací ale nejsou žádným způsobem definovány. Školení odpovídajícího pracovníka ohledně bezpečnosti informací bylo

provedeno jen při nástupu do pozice a nebylo formálně ověřeno ani zdokumentováno. Odpovědnosti při ukončení pracovního nebo smluvního vztahu nejsou uvedeny v odpovídajících smlouvách v dostačujícím rozsahu, zaměstnanci však jsou povinni odevzdávat jim svěřené aktivy organizace.

A.8 Řízení aktiv

Ve společnosti existuje jednotný seznam všech firemních zařízení a jiných aktiv, který je řádně aktualizován. Odpovědnosti osob za jednotlivé přístroje a oprávnění je používat však nejsou formálně přiřazeny.

Počítač a zálohový disk jsou trvalé uloženy v prostorách společnosti. Část firemních a externích zařízení se používá pro komunikací a při práci na dálku, pro ně jsou zajištěné jen minimální bezpečnostní opatření.

Klasifikace informací neprobíhá skoro v žádné podobě. Aktiva pracující s informacemi nejsou označena, ani zacházení s takovými aktivy není vymezeno. Ve firmě ale existuje pojetí „citlivá data“, jakož jsou například osobní údaje zákazníků, rozpracované projekty produkce, účetní informace, smlouvy, a které jsou určeny pro vybraný okruh osob a ukládá se v trezoru. Ačkoliv seznam takových údajů se v písemné formě nedodržuje.

A.9 Řízení přístupu

Dokumentace ohledně politiky řízení přístupu, tj. postup pro omezení přístupu k informacím a zařízením pro zpracování informací, není zavedena. Uživatelské účty a přístupové údaje se vytváří jednatelkou, ukládají se v papírové a digitální podobě nešifrování. Hesla na hlavním počítači nejsou chráněna, za výjimkou ukládání hesel v prohlížeči Google Chrome. Macbook ale chrání všechna hesla v aplikaci Keychain Access, některé z nich jsou také duplikovány v prohlížeči. Role a přístupová pravá nejsou rozděleny a popsány kvůli malému počtu zaměstnanců. Zaměstnanecký účet hlavní pracovní stanice nemá omezené pravomoci k instalaci libovolného SW a pohybování se v sítí Internet. Tím vzniká rizika vyvolání poruchy HW a SW nebo zneužití zranitelnosti systému.

Internetové připojení je nezbytné pro všechny zaměstnance dané společnosti. Pokud připojení nefunguje několik hodin, to není tak velký problém, ale při delším výpadku to vede k opoždění plnění důležitých úkolů a termínů. Pevné připojení poskytováno jedním ISP a naštěstí výpadky se stávají zřídka, ale vždy je to velmi nepříjemná situace. Pozastaví se činnosti spojené

s administrací obchodu a správou objednávek. Výpadek připojení rovněž znemožňuje jakoukoliv komunikaci, probíhající zejména prostřednictvím e-mailových zprav.

Mobilní připojení pro vedení společnosti a PR-pracovníka je realizováno přes osobní předplacené SIM-karty a osobní mobilní zařízení. Tato skutečnost komplikuje monitorování činností zaměstnanců na internetu a splnění bezpečnostních požadavků.

A.10 Kryptografie

Firma vlastní elektronický podpis, který se používá při podepsání smluv na dálku a pro komunikaci s úřady. Šifrování disku se vůbec neřeší na stolní stanici. Na přenosném počítači je zapnutý vestavený šifrovací nástroj FileVault. Další metody šifrování a jakékoliv politiky jejich použití nejsou zavedeny.

A.11 Fyzická bezpečnost

Fyzické zabezpečení provozu organizace se nachází na střední úrovni. Střežení areálu je přiměřené, ale však není dostačující. Návštěvníky jsou evidováni, ale osoby mohou po areálu procházet bez dozoru. Nadávková zóna není oddělena od ostatních prostorů budovy a zároveň není neustále sledována uvnitř budovy. Síťová infrastruktura je ale řádně zabezpečená. Kanceláře se po dobu nepřítomnosti pracovníků zamykají. Nejohroženějšími aktivy však zůstávají zařízení a datové nosiče, které se pochybují mimo areál organizace. Problematika fyzické bezpečnosti je také podrobně probrána v kapitole 4.1.5.

A.12 Bezpečnost provozu

Politiky bezpečnosti provozu zatím neexistují. Neevidují se změny v organizaci, jejich obchodních procesech, ani v zařízeních pro zpracování informací, které mají vliv na jejich bezpečnost. Na hlavní počítačové stanici podniku je nainstalován firemní antivirový SW, který se stará o bezpečnostní kontrolu webových stránek a e-mailové korespondence. Nicméně přenosný počítač je chráněn pouze základní verzí antiviru. Virové testy jsou prováděny nepravidelně. Aktualizace všech zařízení a programů však probíhají pravidelně a automaticky. Zálohy se dělají jednou za 2-3 měsíce, což není dostačující frekvence. Kontrola funkčnosti těchto záloh se neprovádí.

A.13 Bezpečnost komunikace

Síťová infrastruktura podniku je v docela dobrém stavu, nicméně zásady, postupy a kontroly k ochraně přenosu informací v objektu nejsou řádně zdokumentovány. Nejsou stanovené

požadavky a postupy komunikací dálkových pracovních stanic, občas se pro připojení využívá veřejné sítí. VPN se nepoužívá. Pro podepsání výhradních e-mailových zprav se používá elektronický podpis.

Kontrolu podezřelých e-mailových zprav zajišťuje antivirový SW, který však není nainstalován na všech používaných v podniku zařízeních, zejména přenosných provádějících většinu komunikací. Pro sdílení rozpracovaných projektu mezí osoby, které se na tvorbě projektu podílejí, a to bud‘ interní nebo externí, se nejčastěji používá Google Disk.

A.14 Akvizice, vývoj a údržba systému

Organizace nemá nainstalovaný ve svém interním prostředí žádný informační systém. E-shopový systém, který společnost využívá, je provozován třetí stranou, stejně jako další systémy logistických a finančních služeb, takže společnost se o jejich provoz nestará. Ve smlouvách s třetími strany nicméně se většinou neobjevují zmínky související se s bezpečností jejich informačních systémů.

A.15 Vztahy s dodavateli

Řízení vztahů s dodavateli není dostatečně zformulováno a bezpečnostní opatření na tenhle řetězec nejsou stanovena a zdokumentována. Z toho důvodu, že většina zboží se objednává u čínských dodavatelů, dodavatelské smlouvy jsou zpravidla v angličtině a neobsahují žádné požadavky na bezpečnost informací, které by snižovaly rizika spojená s přístupem dodavatelů k aktivům organizace, a zejména k jí autorským dílům.

A.16 Řízení incidentů bezpečnosti informací

Ve společnosti není zavedena žádná dokumentace nebo metodika, která by řešila odpovědnosti a postupy pro zvládání bezpečnostních incidentů. Z důvodu minimálního množství incidenty se vždy řeší jednatelka společnosti ve spolupráci s externím technikem. Administrativní pracovník dostává v rámci školení základní znalostí o bezpečnostních incidentech a kam je musí směrovat.

A.17 Řízení kontinuity činností organizace

Firma neřeší zajištění kontinuity provozu systému. Požadavky a postupy k zajištění požadované úrovně informační bezpečnosti a kontinuity procesů správy informační bezpečnosti v nepříznivých situacích nejsou zavedeny. Existuje riziko dočasné nedostupnosti webových služeb – hlavně e-shopu, logistického servisu a e-mailové služby v důsledku přerušení dodávky internetu.

A.18 Soulad s požadavky

Vedení firmy udržuje přehled o dotýkajících se ji změnách v legislativě a zejména následujícím právním předpisům:

- Občanský zákoník č. 89/2012 Sb., v němž jsou obsaženy normy, týkající se elektronického obchodování;
- Zákon o ochraně spotřebitele č. 634/1992 Sb.;
- Zákon o evidenci tržeb č. 112/2016 Sb. (EET);
- Zákon o ochraně osobních údajů č. 101/2000 Sb.;
- Nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR);
- Živnostenský zákon č. 455/1991 Sb.

Společnost pořizuje SW prostředky v souladu s licenčními podmínkami. Důvěrnost a ochrana osobních údajů je zajištěna v rozsahu, požadovaném příslušnými právními předpisy. Neprovádí se ale přezkoumání přístupu organizace k řízení bezpečnosti informací v plánovaných intervalech ani v případě významných změn.

4.2 Analýza rizik

Proces hodnocení rizik je jedním ze základních kroků ustavení ISMS. V rámci dané práce je provedena identifikace a hodnocení aktiv organizace dle opatření A.8 „Řízení aktiv“ normy ISO/IEC 27002, a jsou definovány rizika a hrozby, které jsou s těmito aktivy spojeny. Dle metod, popsaných v normě ISO/IEC 27005, jsou následně sestaveny matice zranitelnosti a rizik, které finalizují obraz stavu zabezpečení podnikových aktiv a slouží pro návrh opatření doporučených ke zlepšení tohoto stavu.

Analýzu rizik lze provést z hlediska několika různých přístupů. V případě zkoumané společnosti a vzhledem k její velikosti analýza se provádí na základní úrovni. Nejprve se provede identifikace aktiv a hrozeb, jim jsou přiřazeny číselné hodnoty, které slouží pro sestavení matice zranitelnosti a následně i matice rizik. Výsledky této analýzy rizik slouží jako východisko pro výběr vhodných bezpečnostních opatření z normy ISO/IEC 27002.

4.2.1 Identifikace aktiv

V této části budou tedy identifikována aktiva, která mají podstatný význam pro společnost a k nim bude přiřazena hodnota, určující závažnost daného aktiva. Pro stanovení číselné hodnoty aktiv je využito nejprve slovní ohodnocení v rozsahu od 3 (střední) do 5 (závažná). Aktiva, která by se nabývala číselných hodnot 1 až 2, nepoužívají se pro danou analýzu a následný vypočet matic zranitelnosti a rizik, protože jejich dopad na provoz podniku je skoro zanedbatelný nebo nejsou objekty rizik informační bezpečnosti.

Tabulka č. 3: Stupnice hodnocení aktiv

Hodnota aktiva	Označení	Popis
střední	3	Nezanedbatelný vliv. Při poškození/ztrátě hrozí potíže či finanční újmy.
vysoká	4	Významný vliv. Při poškození/ztrátě hrozí vážné potíže či finanční újmy.
závažná	5	Existenční vliv. Při poškození/ztrátě hrozí existenční potíže.

Zdroj: Vlastní zpracování pro potřeby DP

Na základě výše uvedené klasifikační stupnice jsou dále vyhodnocena aktiva organizace pomocí přirážení jim hodnot, představujících obchodní dopad při porušení integrity, důvěrnosti anebo dostupnosti daného aktiva.

Tabulka č. 4: Váha aktiv

Název aktiva	Váha aktiva
hlavní firemní počítač	4
přenosný počítač	5
zálohový disk	5
tiskárny	3
router	3
licenční SW	4
rozpracované projekty	4
dopracované projekty	3
smlouvy a dokumentace	4
účetní informace	4
zboží	5

Zdroj: Vlastní zpracování pro potřeby DP

Z toho vyplývá, že nejohroženějšími aktivy společnosti jsou v první řadě přenosné zařízení. Zároveň vidíme, že silný význam mají zásoby zboží, ale z důvodu jejich papírové povahy skoro nejsou vystaveny rizikům informační bezpečnosti.

4.2.2 Identifikace hrozeb

Identifikace a hodnocení hrozeb proběhlo na základě vlastního pozorování a analýzy firemního prostředí, popsané v předchozích kapitolách. Pro hodnocení hrozeb byla použita stupnice od 1 do 4, aby následná matice rizik pak byla v rozmezí od 0 do 100. Nejpodstatnější hrozby budou označený číslem 4 a nejméně ohrožující číslem 1.

Tabulka č. 5: Hodnocení hrozeb

Pravděpodobnost výskytu	Označení
nepodstatná	1
malá	2
střední	3
velká	4

Zdroj: Vlastní zpracování pro potřeby DP

Z přílohy C normy ISO/IEC 27005 byly vybrány hrozby, u kterých budou následně definovány pravděpodobnosti výskytu. Z tabulky se dá vidět, že největší pravděpodobnost výskytu jsou u takových hrozeb, jako jsou lidské chyby při používání systému a krádež nebo zničení HW.

Tabulka č. 6: Pravděpodobnost výskytu hrozeb

Hrozba	Pravděpodobnost
požár	1
selhání hardwaru	3
krádež nebo zničení hardwaru	4
znečištění hardwaru	2
selhání telekomunikačního zařízení	3
selhání softwaru	2
krádež nebo zničení softwaru	2
krádež nebo zničení dat	3
neoprávněné získání administrátorského nebo uživatelského přístupu	3

chyba při používání	4

Zdroj: Vlastní zpracování pro potřeby DP

4.2.3 Matice zranitelnosti

V této části je představena matice zranitelnosti, která slouží k posouzení zranitelnosti jednotlivých aktiv jednotlivými hrozbami. Matice byla sestavena dle technik, popsaných v příloze E normy ISO/IEC 27005 na základě váhy aktiva (tabulka č. 4), pravděpodobnosti hrozby (tabulka č. 6) a snadnosti využití zranitelnosti. Snadnost využití zranitelnosti posuzuje případnou míru poškození pro každou kombinace aktiva a hrozby a ukazuje úroveň ohrožení daného aktiva danou hrozbou. Nabývá se hodnot: N – nízká, S – střední a V – vysoká. Pomocí níže uvedené tabulky se získává hodnota zranitelnosti. Pokud daná hrozba se nedotýká daného aktiva, hodnota zranitelnosti je nulová, bez ohledu na pravděpodobnost výskytu této hrozby.

Tabulka č. 7: Stupnice hodnocení zranitelnosti

Pravděpodobnost výskytu hrozby	1			2			3			4		
Snadnosti využití zranitelnosti	N	S	V	N	S	V	N	S	V	N	S	V
Hodnota zranitelnosti	**0**	**1**	**2**	**1**	**2**	**3**	**2**	**3**	**4**	**3**	**4**	**5**

Zdroj: Vlastní zpracování pro potřeby DP

Výsledky posouzení jsou pak doplněny do tabulky č. 8 a slouží jako podklad pro následné vyplnění matice rizik.

Tabulka č. 8: Matice zranitelnosti

P	**A**	4	5	5	3	3	4	4	3	4	4	5
	hrozba\aktiv	hlavní firemní počítač	přenosný počítač	zálohový disk	tiskárny	router	licenční SW	rozpracované projekty	dopracované projekty	smlouvy a dokumentace	účetní informace	zboží
1	požár	2	0	1	2	2	0	1	0	2	1	2
3	selhání hardwaru	3	4	3	3	3	0	3	2	3	3	0
4	krádež nebo zničení hardwaru	4	5	4	3	4	3	4	0	4	4	0
2	znečištění hardwaru	2	1	1	2	2	0	0	0	0	0	0
3	selhání telekom. zařízení	3	3	2	2	4	0	2	0	0	2	0
2	selhání softwaru	2	3	1	1	1	3	2	1	2	2	0
2	krádež nebo zničení softwaru	2	3	2	1	1	3	2	1	1	1	0
3	krádež nebo zničení dat	3	4	3	2	2	4	4	3	3	3	0
3	neoprávněné získání admin. nebo uživ. přístupu	4	4	2	2	2	3	3	2	3	4	0
4	chyba při používání	5	4	4	3	3	4	3	0	3	4	3

Zdroj: Vlastní zpracování pro potřeby DP

4.2.4 Matice rizik

Závěrečnou fází analýzy rizik je posouzení míry rizika. Prvním krokem je určení jednotlivých úrovní rizik. Výsledná míra rizika je přiřazena k intervalům, rozděleným do třech skupin:

- Malé riziko – vliv je skoro zanedbatelný, nevyžadují se další protiopatření, ale je potřeba pravidelně monitorovat a přezkoumávat tato rizika.
- Střední riziko – významná rizika vyžadující odpovídající nápravní činností, které musí být provedeny dle stanoveného plánu.
- Velké riziko – vyžadující vyhrazené finanční zdroje a bezprostřední bezpečnostní opatření, která musí riziko snížit na přijatelnou úroveň.

Zvolené intervaly jsou znázorněny v následující tabulce č. 9.

Tabulka č. 9: Klasifikace rizik

Interval	Riziko
0–33	Malé
34–67	Střední
68–100	Velké

Zdroj: Vlastní zpracování pro potřeby DP

Dalším krokem analýzy rizik je vypočtení samotné míry rizika pomocí kvalitativní metody maticové analýzy rizik tří faktorů. Výsledek k jednotlivým buňkám matice získáme vynásobením hodnoty aktiva (A), pravděpodobnosti hrozby (P) a hodnoty z matice zranitelnosti (Z) dle vzorců R=P*A*Z, kde R je hledaná míra rizika. Vypracovaná matice rizik pro všechna identifikovaná aktiva a hrozby je zobrazena v tabulce č. 10.

Tabulka č. 10: Matice zranitelnosti

hrozba\aktiv	hlavní firemní počítač	přenosný počítač	zálohový disk	tiskárny	router	licenční SW	rozpracované projekty	dopracované projekty	smlouvy a dokumentace	účetní informace	zboží
požár	8	0	5	6	6	0	4	0	8	4	10
selhání hardwaru	36	60	45	27	27	0	36	18	36	36	0
krádež nebo zničení hardwaru	64	100	80	36	48	48	64	0	64	64	0
znečištění hardwaru	16	10	10	12	12	0	0	0	0	0	0
selhání telekom. zařízení	36	45	30	18	36	0	24	0	0	24	0
selhání softwaru	16	30	10	6	6	24	16	6	16	16	0
krádež nebo zničení softwaru	16	30	20	6	6	24	16	6	8	8	0
krádež nebo zničení dat	36	60	45	18	18	48	48	27	36	36	0
neoprávněné získání admin. nebo uživ. přístupu	48	60	30	18	18	36	36	18	36	48	0
chyba při používání	80	80	80	36	36	64	48	0	48	64	60

Zdroj: Vlastní zpracování pro potřeby DP

4.2.5 Zhodnocení analýzy rizik

Z výsledků analýzy vyplývá, jaké oblasti jsou nejvíce postižené a které představují nejvyšší míru rizika pro společnost. Jedna se o:

- Krádež nebo zničení podnikového hardwaru. Nejvyšší rizikové položky se vztahují k přenosným zařízením – notebooku a zálohovému disku. Další hardware a papírová dokumentace mají střední úroveň rizikovosti, vyžaduje zavedení systematických opatření.
- Uživatelské chyby při používání obou pracovních stanic a při tvorbě zálohových kopií disku v důsledku nedostatku bezpečnostního povědomí a příslušné dokumentace. Ostatní aktiva převážně mají střední míru rizika a také vyžadují určitá protiopatření.

K dalším středně významným rizikům patří hrozby, které plynou ze selhání hardwaru, krádeží nebo zničení dat a neoprávněného získání administrátorského nebo uživatelského přístupu k podnikovým interním systémům. Nejohroženějšími aktivy se stávají stacionární a mobilní pracovní stanice, zálohový disk. Střední úrovně rizika mají rozpracované projekty a účetní dokumentace.

Všechny této oblasti by měly být odraženy v návrhu opatření. Nezbytné je se v první radě zaměřit na zabezpečení použití přenosných zařízení, sestavení postupu řízení bezpečnosti informací, přirazení odpovědností a školení uživatelů.

4.3 Návrh opatření

Následující kapitola definuje požadavky na zavedení a údržbu ISMS v kontextu zkoumané organizace dle normy ISO/IEC 27001. Dále definuje postup řízení rizik bezpečnosti informací, přizpůsobený potřebám organizace, poskytuje opatření, schopné tyto rizika zpříjemnit, a rovněž uvádí plánované náklady na zavedení těchto opatření. Při návrhu jsou využívány podklady z norem ISO/IEC 27001 a ISO/IEC 27002.

4.3.1 Požadavky na ISMS

4.3.1.1 Kontext organizace

Porozumění organizaci a jejímu kontextu je nejdůležitějším faktorem úspěchu této organizaci. Společnost musí identifikovat kontext a stanovit si cíle, kterých by chtěla dosáhnout při zavedení

systému řízení informační bezpečnosti. Je to nezbytné pro vyjádření stanov a politik bezpečnosti, které musí dodržovat zaměstnanci společnosti. Externí správce IT vstupující do prostředí organizace a technická podpora externích systémů potřebují alespoň částečně vědět požadavky společnosti na ISMS při projednání závad a technických otázek.

Porozumění potřebám a očekáváním zainteresovaných stran je dalším úkolem společnosti. Do zainteresovaných stran v první řade patří vedení vybrané společnosti v osobách jednatelky a majitele firmy, které mají nejvyšší zájem o utajení jejich účetních a dalších informací a know-how. Důležitým požadavkem je tedy zabezpečení podnikových dat proti potenciálním útokům. Mezi zainteresovanými strany můžeme zároveň přiřadit i zákazníky obchodu, jejichž osobní údaje má k dispozici vybraná společnost.

Rozsah ISMS byl vedením stanoven na všechna fyzická a informační aktiva, zaměstnance a třetí strany (dodavatele, externí správce IT, účetní apod.), kteří uskutečňují jakékoliv činnost pro danou společnost. Jedná se většinou o společnosti s ručením omezeným nebo osoby samostatně výdělečně činné, které se často nakládají s daty nebo zařízením, souvisejícím se s činností společnosti.

4.3.1.2 Vůdčí role

Vedení organizace by mělo prokázat svůj závazek vůči systému řízení informační bezpečnosti a dodržovat jeho požadavky. Proto je potřeba sestavit a podepsat dokument v následujícím znění:
„Vedení společnosti se zavazuje podporovat zavedení systému pro řízení bezpečnosti informací z hlediska organizačních změn a poskytovat finanční podporu nezbytnou pro zavedení opatření dle požadavků normy ISO/IEC 27001. Vedení stanoví role a odpovědnosti za bezpečnost informací a bude zajišťovat pravidelné školení zaměstnanců. Vedení společnosti bude dbát na neustálou kontrolu a zlepšování úrovně zabezpečení všech informací, které zpracovává, aby byla zajištěna jejich důvěrnost, dostupnost a integrita.“

Zavedení bezpečnostní dokumentace má za cíl zvýšit bezpečnostní povědomí firmy a všech jejích zaměstnanců a jako následek snížit míru rizika jejich chyb při používání systémů. Politika by měla odrážet cíle a úkoly společnosti v oblasti informační bezpečnosti, respektovat její finanční schopnosti a sloužit jako základ pro stanovení současných a všech následujících úkolů. Bezpečnostní politiky musí být vydávány jako dokumentované informace, musí být sdělovány zaměstnancům a musí být k dispozici zúčastněným stranám stanoveným způsobem.

4.3.1.3 Plánování

Základním bodem plánovacího procesu je posuzování rizik bezpečnosti informací. Analýza rizik včetně jejich klasifikace je uvedena v kapitole 4.2 dané práci. Zároveň v následujících částech práce budou navrhnuta opatření, která sníží pravděpodobnost těchto rizik nebo jejich dopad na zkoumanou organizaci.

Společnost si dále potřebuje jasně určit cíle bezpečnosti informací pro všechny své činnosti a postupy jejich dosažení. Při plánování, jak dosáhnout svých cílů v oblasti informační bezpečnosti, organizace musí stanovit postup, vyžadované zdroje, odpovědného za tuto činnost a za bezpečnost jí provádění, očekáváný termín dosažení cílů a postup zkoumání výsledků.

4.3.1.4 Zajištění provozu

V této fázi společnost by měla mít úplnou představu o tom, jak ISMS bude fungovat a jakých výsledků se od toho očekává. Má zajištěné finanční prostředky pro celý proces vývoje, implementace, údržby a zlepšování systému.

Nebytně je také dodržovat kompetenci svých zaměstnanců prostřednictvím školení stálých pracovníků nebo přijímání nových odborníků. Zaměstnanci musí být informováni o zásadách bezpečnosti informací, jejich rolích v provozu ISMS a důsledcích nedodržení požadavků.

Vše interní a externí komunikace nezbytné pro chod společnosti musí být přezkoumány a zmapovány, zejména tyto údaje:

- kdo vyměňuje informace;
- kdy si vyměňují informace;
- s kým si vyměňují informace;
- jaké informace se vyměňují;
- prostřednictvím jakého HW a SW se vyměňují informace;
- kdo by si měl vyměňovat informace;
- postupy, kterými by měla být komunikace prováděna.

Posledním krokem pro zajištění činnosti systému řízení bezpečnosti informací je mít zpracovanou dokumentaci, která odpovídá požadavkům normy. To znamená, že hotové politiky budou:

- přístupné dle přidělených oprávnění;
- náležitě chráněna;
- udržované v přijatelném stavu a dle platné legislativy;
- mít stanovenou dobu platnosti a metody likvidace.

Bezpečnostní dokumentace při vytvoření a po každé aktualizaci se musí zahrnovat tyto údaje:

- identifikační údaje – název, autor, datum vytvoření anebo aktualizaci;
- formát – papírové nebo digitální, a také jazyk, verze použitého softwaru atd.;
- přezkoumání změn a schválení věděním za účelem zachování souladu s cílí podniku.

4.3.1.5 Provoz ISMS

Po zavedení všech opatření organizace potřebuje provoz ISMS rozběhnout. Proto je nezbytné se řídit úkolům a stanoveným cílům organizace dle předchozí podkapitoly 4.3.1.1 a provádět činnosti dle určených politik pro dosazení těchto cílů. Dále je potřeba pravidelně provádět přezkoumání rizik bezpečnosti informací dle postupu kapitoly číslo 4.2, zaznamenávat zjištěné odchylky, připravovat aktuální protiopatření a je bezodkladně aplikovat.

4.3.1.6 Hodnocení účinnosti ISMS

Tato fáze odpovídá etapě Check v modelu PDCA a spočívá ve vyhodnocení provozu a účinností ISMS. Společnost by měla předem přemyslet o tom, co potřebuje sledovat a jakým způsobem provádět měření výsledků. Zvolené metody by měly poskytovat srovnatelné a reprodukovatelné výsledky. Výsledky monitorování a měření se musí uschovávat ve formální podobě po dobu její platnosti.

Vrcholový management by měl v plánovaných intervalech, doporučovalo by se jednou ročně, uskutečňovat interní audit společnosti a přezkoumávat vlastní práce v oblasti řízení bezpečnosti informací, aby to odpovídalo přijatým politikám a bezpečnostním normám.

4.3.1.7 Zlepšování účinnosti ISMS

V případě zajištěných odchylek od stanovených cílů organizace by měla bezprostředně reagovat na nesoulad a pokud je závažný:

- přijmout nápravná opatření;
- přijmout opatření týkající se důsledků nesouladu;
- posoudit příčiny nedodržení předpisů tak, aby nedošlo k jeho opakovanému vzniku.

Frekvence zlepšovaní účinnosti a vhodnosti používaných nástrojů ISMS by se měla shodovat s frekvencí monitorování této účinnosti stanovenou na 1 rok.

4.3.2 Bezpečnostní opatření

V této části práce jsou vypsány bezpečnostní opatření dle normy ISO/IEC 27002, která jsou vhodná pro zavedení do prostředí zkoumané společnosti. Vybraná opatření by měla zohledňovat omezené finanční zdroje podniku a pokrývat alespoň ty nejzávažnější slabá místa, které vyplývají z výsledků analýzy prostředí a analýzy rizik.

A.5 Bezpečnostní politika

Společnost by měla sepsat, zavést a dodržovat jediný dokument, kde jsou definovány požadavky na bezpečnost informací, aby byla zaručena jejich důvěrnost, dostupnost a integrita, a kde je stanovena odpovědná za to osoba. Tento úkol spadá do kompetence vedení organizace. Spolu s tím musí existovat procesy přezkoumání změn v politice bezpečnosti a záznamy o těchto změnách v dokumentované podobě.

A.6 Organizace bezpečnosti

Ve firme je potřeba formálně zaznamenat role zodpovídající za bezpečnost informací a za jejich platnou dokumentaci. V případě dané společnosti bych doporučovala alespoň zavést jednotný seznam odpovědností za:

- bezpečnost informací;
- vytvoření a správu bezpečnostní dokumentace;
- zajištění pravidelného školení zaměstnanců;
- správu bezpečnostních události a hlášení incidentů;
- kontrolu stavu zabezpečení fyzických a informačních aktiv společnosti;
- kontrolu stavu zabezpečení síťové infrastruktury.

Část těchto úkolů je stále možné řešit prostřednictvím externích specialistů, ale odpovědnosti třetích stran rovněž musí být důkladně zdokumentovány a postupy jednotlivých činností náležitě popsány.

V podniku musí být zavedeny bezpečnostní opatření hrozeb, spojených s používáním mobilních zařízení a vzdálených pracovních stanic, na kterých jsou zpracovány nebo uloženy podnikové informace. Ve společnosti se používají přenosný počítač a osobní mobilní zařízení, pro které je potřeba zavést odpovídající bezpečnostní opatření a zejména:

- požadavky na fyzickou zabezpečenost místa pro práci na dálku;
- zabezpečení komunikace, používání virtuálních privátních sítí, výhradní použití známých sítí a omezení konfigurace bezdrátových síťových služeb;
- poskytování technické podpory a údržby hardwaru a softwaru;
- dohled na neoprávněný přístup k informacím od jiných spolubydlících osob, např. rodina a přátelé;
- ochrana před malwarem a využití firewallu;
- postupy pro zálohování a kontinuitu podnikání.

A.7 Bezpečnost lidských zdrojů

Mělo by být ve firme sledováno dodržování požadavků na bezpečnost informací v souladu se zavedenými zásadami a postupy u všech pracovníků. Jejich povinnosti v oblasti bezpečnosti informací během vzniku a zániku pracovního vztahu by měly být detailně popsány. Zaměstnanci musí mít zajištěné pravidelní školení ohledně bezpečnosti informací a nakládání s firemními daty alespoň jednou ročně od specializované firmy, poskytující dané služby. Všechny školení jsou potřeba řádně evidovat a opatřit příslušnými osvědčeními. V současnosti ale školení probíhá pouze na začátku pracovního poměru a nesplňuje vše požadavky normy ISO/IEC 27001, což vede ke zvýšení rizika zneužití zranitelností systému.

A.8 Řízení aktiv

Ve společnosti by měly být nastaveny přípustné způsoby použití a ochrany firemních aktiv včetně přirazení odpovědných za tyto aktiva osob.

Je nezbytné provést klasifikace informací podle stupně jejich utajení. Informace ve firmě je potřeba rozdělit minimálně na tří skupiny: veřejné, interní a chráněné. Do kategorie veřejných informací by měly spadat ty, které jsou dostupné na webových stránkách obchodu, určené k prezentaci firmy a zboží. Interní informace zůstávají v perimetru firmy a jsou určeny pro

zaměstnance a další třetí strany, kteří tyto informace potřebují ke splnění svých dodavatelských závazků. Všechny tyto vztahy musí být chráněny příslušnými smlouvami o mlčelivosti. Do skupiny chráněných informací patří citlivá data, jako jsou účetní informace a osobní údaje zákazníků, které by měly být chráněny pomocí šifrovacích metod, i když zálohový disk se chrání v trezoru.

A.9 Řízení přístupu

Politika řízení přístupu a další dokumentace ohledně přidělení a odebrání uživatelských práv by měli být sepsány, dodržovány a řádně aktualizovány. Musí se rovněž dodržovat soulad mezí přístupovými právy a politikou klasifikace informací. Doporučuje se omezit uživatelská práva kancelářských strojů a sledovat skutečnost, že zaměstnanci a třetí strany mají přístup pouze k těm informacím, které potřebují k plnění svých úkolů.

Je potřeba zavést systém správy hesel. Nejlepší možnost je ukládání hesel pomocí Avast Passwords, která je umožněna na obou počítačích. Zároveň se doporučuje vymazat již uložená hesla v prohlížečích.

V případě zkoumané společnosti připojení dalšího ISP k zajištění nepřetržitého provozu v případě poruchy u prvního poskytovatele je nerentabilní. Problém lze řešit nastavením osobního hotspotu na mobilní stanici, která bude sdělovat mobilní datové připojení přes Wi-Fi anebo USB kabel pro naléhavou potřebu. Pořízení jediného firemního mobilního tarifu a mobilních zařízení pro všechny zaměstnance nebylo by zatím možné a spojené s tím rizika lze ignorovat.

A.10 Kryptografie

Zaprvé se doporučuje na hlavní pracovní stanici používat vestavený šifrovací nástroj BitLocker. Tato aplikace je založena na šifrování celého disku pomocí algoritmu AES (Advanced Encryption Standard). Šifrovací klíče musí být bezpečně uloženy. Nejjednodušší, ale i nejnebezpečnější metodou je použití hesla. Pro vyšší zabezpečení lze také využít kryptografický token nebo čipovou kartu. Doporučuje se zavést politiky správy kryptografických opatření a použití kryptografických klíčů.

A.11 Fyzická bezpečnost

Ochranné opatření budovy, kancelářských prostorů a vybavení by měly být rozvíjena a uplatňována. Dveře do kanceláře se doporučuje nechávat zavřené i po dobu přítomnosti zaměstnanců. Návštěvy budovy by měly být důkladněji sledovány, oblasti pro nakládku a

vykládku musí být odděleny od ostatních částí budovy a rovněž lépe hlídány. Pokud alespoň některé z těchto podmínek nejsou realizovatelné, doporučuje se vyhledat jiné místo na pronájem kanceláře. Nejdůležitějším bodem je ale zajištění pravidel pro přesouvání zařízení, obsahujících firemní informace mimo areál podniku. Neměli by být ponechané bez dozoru ani v místě bydlení, pokud je sdělováno s dalšími osoby.

A.12 Bezpečnost provozu

Ochrana hlavního firemního počítače je dostatečná s placeným antivirem Avast Business a zabudovaným HW firewallem. Pro přenosný počítač společnosti však musí být použity zvýšené metody zabezpečení, zejména zachránění placenou verzí antiviru přes navýšení počtu uživatelů stávajícího podnikového řešení. Důležité je dodržovat ochranná opatření proti malwaru a dávat pozornost na detekci a prevenci podezřelých webových stránek.

Vlastní datové nosiče při připojení k firemním počítačům před otevřením musí být otestoáany antivirem, to slouží jako prevence před možnými škodlivými soubory na přenosném zařízení a následném možném poškození počítače.

Jako další opatření lze použit nástroje pro sledování protokolu událostí, například Netwrix Event Log Manager nebo Splunk, které provádějí analýzu sítě a vytváří log soubory, zaznamenávají vytížení sítě, tvoří pravidelné reporty. Tyhle řešení nejsou placené a mají přívětivě uživatelské rozhraní.

Podstatným bodem je zavedení schématu frekventovaného zálohování disku: doporučuje se dělat zálohy alespoň jednou měsíčně, pro některá důležitá data by se měla dělat i každodenní záloha. Nejprve je potřeba rozhodnout, jaká data se musí zálohovat, určit přístupová pravá k pořízeným zálohám a způsoby jich ochrany. Zároveň je nezbytná kontrola použitelností pořízených zálohových kopií a testování obnovy systému dle stanoveného harmonogramu.

Kompletní pravidla a pracovní postupy spolu s nově nasázenými opatření mají být sepsány a zároveň musí být stanoveny osoby zodpovědné za každý konkrétní software nebo činnost.

A.13 Bezpečnost komunikace

V organizaci chybí zavedené zásady, postupy a kontroly k ochraně přenosu informací prostřednictvím jakéhokoli typu komunikačního zařízení, zejména provazovaného na dálku přes

nedůvěryhodné telekomunikační kanály. Také se doporučuje použití VPN a dvoufázového ověření pro vstup do všech komunikačních systémů a aplikaci, které to podporují.

A.14 Akvizice, vývoj a údržba systému

O provoz a vývoj informačních systémů používaných podnikem se starají třetí strany, které jsou dodavateli těchto systémů. Organizace by měla však řádně kontrolovat a sledovat proces vývoje outsourcovaného systému, smlouvy sjednávané s poskytovateli takových systémů by měly obsahovat zmínky ohledně bezpečnosti informací.

A.15 Vztahy s dodavateli

V první řade se doporučuje volit jen takové zahraniční dodavatelé, kteří mohou poskytnout smysluplnou smlouvu obsahující ustanovení, která se budou týkat bezpečnosti informací a autorského pravá. Také je potřeba zavést rozdělení na typy dodavatelů podle jejich činností a propojit se seznamem definovaných skupin informací, dle kterého se dá stanovit, jaká data je možné sdílet s dodavateli, a jak s nimi dodavatel může manipulovat.

A.16 Řízení incidentů bezpečnosti informací

Navrhuje se vytvořit dokumentaci nebo metodiku, která by řešila odpovědnosti a postupy pro zvládání bezpečnostních incidentů, spolu s tím je nezbytné si stanovit jednotné místo pro sběr záznamů o bezpečnostních incidentech, klasifikovat tyhle incidenty podle závažnosti jejich dopadů a důkladně nahlašovat nově nalezená zranitelná místa v systému a kybernetické bezpečnostní incidenty Národnímu centru kybernetické bezpečnosti (NCKB) přes elektronický formulář, který lze stáhnout z jejich webových stránek.

A.17 Řízení kontinuity činností organizace

Řízení bezpečnosti informací by mělo předpokládat, že požadavky na zabezpečení informací v nepříznivých situacích zůstanou stejné ve srovnání s běžnými provozními podmínkami.

A.18 Soulad s požadavky

Společnost splňuje všechny náležité legislativní požadavky. Doporučuje se založit postupy přezkoumání stavu bezpečnosti informací, rovněž kontrolovat soulad zpracování dat a technický soulad s vytvořenou politikou informační bezpečnosti.

4.3.3 Opatření zaměřená na snížení rizik

V následující tabulce číslo 11 je představen zebříček hrozeb uspořádaný dle výší míry rizika, které mají přirazené odpovídající protiopatření. Poslední čtyři řádky této tabulky znázorňují střední a vysoká bezpečnostní rizika, na která je potřeba si dávat největší pozornost a znamená to, že posloupnost implementace je zdola nahoru dané tabulky.

Tabulka č. 11: Hrozby a navrhovaná protiopatření

Míra rizika	Hrozba	Protiopatření
4,6	požár	Míra rizika je přiměřená. Nevyžadují se žádná další protiopatření.
5,5	znečištění hardwaru	Zajištění pravidelného úklidu a servisu.
12,7	krádež nebo zničení softwaru	Dodržovat politiku řízení přístupu, jinak je míra rizika docela nízká, další opatření se doporučují dle potřeby.
13,3	selhání softwaru	Navýšení kvalifikace zaměstnanců. Další protiopatření jsou možná dle potřeby.
19,4	selhání telekomunikačního zařízení	Zpracování plánu kontinuity činnosti v případě selhání telekomunikačního zařízení, zajištění spojení na kontaktní osoby v případě potíží.
29,2	selhání hardwaru	Zajištění pravidelného servisu u pozáručních zařízení, frekventovaná tvorba záloh disku a kontrola jejich funkčnosti, zpracování plánu kontinuity činnosti v případě selhání hardwaru.
31,6	neoprávněné získání administrátorského nebo uživatelského přístupu	Zpracování interní politiky řízení přístupu, vytvoření systému spravování hesel, systému pravidelné kontroly nasazeného SW, použití VPN a dvoufaktorové autentizace.
33,8	krádež nebo zničení dat	Zavést a dodržovat opatření pro použití přenosných zařízení a politiky řízení přístupu. Přezkoumat a zmapovat vše interní a externí komunikací ve společnosti a mít nad nimi dohled.
51,6	krádež nebo zničení hardwaru	Posílení ochranných opatření budovy a kanceláře, dodržování pravidel pro přesouvání mobilních zařízení mimo areál společnosti. Pravidelné zálohování dat.
54,2	chyba při používání	Vytvoření a správa bezpečnostní dokumentace, uplatnění bezpečnostního povědomí v procesech podniku. Zajištění pravidelného školení zaměstnanců.

Zdroj: Vlastní zpracování pro potřeby DP

4.3.4 Doporučený obsah nových interních dokumentů

Z důvodu menší velikosti organizace by se doporučovalo zavedení jediného dokumentu pod obecným názvem „Bezpečnostní politika“, který bude rozdělen do kapitol odpovídající určitým odvětvím bezpečnosti informací. Níže je uveden doporučený obsah dané politiky.

Bezpečnostní politika

- definice bezpečnosti informací, její cíle rozsah a význam pro organizace;
- požadavek na dodržování zákonných norem, ustanovení a pravidel;
- popis systému řízení informační bezpečnosti;
- stanovení obecných a konkrétních odpovědností pro oblast řízení bezpečnosti informací;
- evidence školení pracovníků ohledně bezpečnosti informací;
- stanovení odpovědností za bezpečnost v pracovních smlouvách;
- odkazy na další interní dokumenty organizace zasahující do oblasti bezpečnosti informací;
- klasifikace informací;
- postupy tvorby a kontrol zálohových kopií dat;
- zajištění bezpečnosti provozu;
- systém hlášení a zvládání bezpečnostních incidentů a technických zranitelností;
- spojení na kontaktní osoby v případě systémových nebo technických potíží;
- postupy pro sledování protokolu událostí;
- schéma aktualizace antivirového a ostatního SW.

Dalším vyhrazeným dokumentem by mohl být souhrn z politiky bezpečnosti mobilních zařízení a politiky řízení přístupu, který bude sloužit jako zaopatření rizik spojených s používáním přenosných zařízení.

Politiky bezpečnosti mobilních zařízení a řízení přístupů

- postupy použití mobilních zařízení;
- nastavení VPN a dvoufaktorové autentizace;
- postupy dálkové práce;
- pravidla přístupu uživatele do uživatelských účtů (registrace, přidělování přístupových údajů, odebrání údajů po skončení pracovního poměru);

- odpovědnosti uživatelů;
- řízení přístupu k síti a postup využívání síťových služeb;
- autentizační metody a bezpečné postupy přihlášení uživatelů;
- systém tvorby, ukládání a chránění hesel;
- řízení přístupu k informacím;
- politika použití šifrovacích metod;
- povinností dodržení platné legislativy.

Pro kompletní zabezpečení podnikových dat je nezbytné řídit vztahy z třetími strany. Politika řízení těchto vztahů by měla obsahovat následující ustanovení.

Politika řízení vztahu s třetími strany

- klasifikace třetích stran;
- seznam zajištěných přístupů třetích stran k aktivům organizace;
- postup sdílení informací s třetími strany;
- kontrola činností informačních systémů třetích stran;
- podmínky a vzory smluv s dodavateli.

4.3.5 Náklady na navržená bezpečnostní opatření

Odhad nákladů na navržená bezpečnostní opatření je členěn do bodů A.5-A.16, odpovídajících normě ISO/IEC 27002. V případě zkoumané společnosti pořízení interního správce IT se na dané etapě nevyplatí. Takže část z těchto opatření mohou být provedena vlastními sílami jednatelky a relevantních zaměstnanců a část – extérním správcem, popřípadě i na dálku. Pro výpočet částky nutné k zavedení opatření je kalkulovaná průměrná hodinová sazba všech pracovníků, kteří se na tom podílí, a odhadnuta na 500,- Kč/hod.

Tabulka č. 12: Časová náročností pro zavedení opatření

Číslo opatření	Činnost	Nasazení (hod.)	Roční (hod.)
A.5.1.1	Politika bezpečnosti informací	5	
A.5.1.2	Přezkoumávání politiky		2
A.6.1.1	Identifikace odpovědností	1	
A.6.2.1	Politika bezpečnosti mobilních zařízení	3	
A.6.2.2	Politika dálkové práce	2	

A.7.1.2	Stanovení odpovědností za bezpečnost v pracovních smlouvách	1	
A.7.2.2	Školení zaměstnanců		8
A.8.2.1	Klasifikace informací	2	
A.8.3.3	Postupy fyzického pohybu paměťových médií	1	
A.9.1.1	Politika řízení přístupu	3	
A.9.2.5	Přezkoumání přístupových práv		2
A.9.4.2	Postupy bezpečného přihlášení	2	
A.9.4.3	Systém správy hesel	2	
A.10.1	Politika používání kryptografických metod	1	
A.11.2.6	Ochrana aktiv mimo areál podniku	3	
A.12.1.1	Politika bezpečnosti provozu	3	
A.12.1.2	Mechanizmy pro řízení změn	1	
A.12.3.1	Politika zálohování	2	
	Testovaní záloh		2
A.12.6.1	Řízení technických zranitelností	2	2
A.13.2.1	Politika přenosu informací	4	
A.13.2.3	Zabezpečení elektronické zasílání zpráv	2	
A.14.2.7	Monitoring činností externích IS		3
A.15.1.1	Řízení bezpečnosti v rámci dodavatelských smluv	2	
A.16.1.1	Odpovědnosti a postupy řízení incidentů bezpečnosti informací	3	
A.16.1.2	Systém hlášení bezpečnostních událostí	2	
Celkem (hod.)		**47**	**19**

Zdroj: Vlastní zpracování pro potřeby DP

Ve výše uvedené tabulce je představen seznam opatření, o kterých je nezbytně uvazovat, pokud zkoumaná organizace rozhoduje o zavedení ISMS. Jednotlivým činnostem je přiřazen časový odhad nutný pro zavedení opatření.

Dále je potřeba započíst částku na pořízení dodatečné licence placeného antivirového SW pro přenosnou pracovní stanici, která činí **1 200 Kč/rok**. Z výše uvedeného vyplývá následující odhadovaná cena pořízení:

Prvotní nasazení činností: **23 500,-Kč**
Roční odhadovaná náročnost činností: **10 700,-Kč**

Tyto částky se mohou lišit v závislosti na časové zatížeností stálých zaměstnanců a ředitelky společnosti a jejich ochotě měnit již zažité procesy. Jinak vypočítaná suma je přiměřená pro daný podnik a výhodou tohoto procesu je to, že může být realizován postupně, čímž dovoluje rovnoměrnější rozdělení nákladů. Společnost není nucena získat certifikát dle řady norem ISO/IEC 27000 v brzké době, naopak cílem vedení je pečlivé zavést doporučená opatření a přednostně řešit ty nejkritičtější oblastí, jejichž opomenutí by mohlo mít vážné potíží v podobě ohrožení bezpečnosti společnosti.

5 Zhodnocení výsledků a doporučení

Rekomendace, které jsou uvedené v dané práci, jsou vhodné pro zavedení bázových ustanovení ISMS a základní řízení bezpečnosti informací. V důsledku zavedení zmíněných opatření a snížení míry rizik společnost může značné posílit zabezpečení svých aktiv včetně chráněných informací a autorských děl, osobních údajů zákazníků a fyzickou bezpečnost areálu, čím získá hodně příležitostí v oblasti informační bezpečnosti a větší důvěru jak zákazníků, tak i partnerů. Některá z opatření se začali zavádět ještě během napsání této diplomové práci a situace v podniku už se začala zlepšovat.

Pokud ale společnost dojde k závěru, že chtěla by pořídit certifikace dle řady norem ISO/IEC 27000, pak by měla zajistit interního IT specialista, alespoň na částečný úvazek, který by převzal odpovědnost za provoz a kontrolu systémů bezpečnosti informací a disponoval celkovým přehledem na stav informačního zabezpečení v daném podniku. Potom je potřeba provést opakovanou analýzu stavu a mělo by dojít k nápravě nalezených nedostatků.

Závěr

Jednou z nejdůležitých strategických otázek managementu společnosti v současném světě je rozhodnutí o způsobu řízení bezpečnosti informačních aktiv a řízení bezpečnostních rizik. Data, která se uschovávají na firemních zařízeních a pochybují se mimo ně, často se stávají terčem útočníků. Vzhledem k posílení kontroly procesu zpracování osobních údajů fyzických osob, zkoumaná společnost rozhodla věnovat zvýšenou pozornost ochraně svých informací. Hlavním cílem této diplomové práce bylo zhodnotit stav zabezpečení informací dle řady norem ISO/IEC 27000, identifikovat rizikové oblasti a navrhnout způsoby ochrany dat.

První část práce jeví sebou teoretickou základnu v oblasti bezpečnosti informací, definuje relevantní pojetí a terminy, vysvětluje koncepci ISMS a určuje právní a normativní požadavky.

Analytická část práce byla zaměřena na analýzu rizikových oblasti organizace. Nejprve byla popsána její činnost, hlavní procesy a organizační struktura. Dále byli uvedeny technické a aplikační prostředky firmy, které jsou relevantní k informační bezpečnosti, její fyzické prostředí a současný stav zabezpečení aktiv.

V podkapitole 4.1.8 Shrnutí aktuálního stavu bezpečnosti firmy jsou znázorněny zásadní odchylky od normy ISO/IEC 27002. Pomocí identifikace aktiv a hrozeb a následné analýzy zranitelnosti a rizik bylo zjištěno, že zkoumané společnosti se nejvíc hrozí ztráta dat v důsledku neoprávněného používání anebo krádeží přenosných zařízení, a také v důsledku uživatelských chyb při zacházení s informačními systémy a zařízením. Na základě shromážděných poznatků a výsledků analýz je proveden návrh opatření, vhodných pro zavedení do prostředí dané společnosti.

Prvořadným úkolem organizace by mělo být stanovení bezpečnostních politik a dohled nad jejich dodržováním. Kapitola číslo 4.3 seznamuje s navrženými protiopatřeními, která jsou rozdělena dle míst jejich aplikací. Dále je představen odhad nákladů, které je potřeba vynaložit na zavedení navržených bezpečnostních opatření. Kalkulována částka činí 23 500 Kč za prvotní nasazení a 10 700 Kč jsou roční výdaje na údržbu systému.

Realizace opatření pokrývá identifikované hrozby firmy a spolu s tím zakládá ISMS, který chrání společnost od pravděpodobných budoucích ztrát v případě neočekáváných incidentů, a tím kompenzuje vynaloženou investice a posiluje konkurenceschopnost společnosti.

Tím pádem stanovené cíle diplomové práce byly dosaženy, i když organizace prozatím neuvažuje o certifikaci. Navrhované změny už mají pozitivní vliv na chod podnikání – zkoumání slabých míst a strukturace získaných informací dle kategorií zvyšují bezpečnostní povědomí všech zaměstnanců, kteří se zúčastnili v provedení této analýzy.

Tato diplomová práce je určena malým firmám a podnikatelům, které se zajímají o bezpečnosti svých informačních, a nejen aktivů, a může sloužit ukázkou návrhu opatření a zavedení ISMS v rámci jejich podnikání.

Seznam použitých zdrojů

ANDERSON, R. Security engineering. Indianapolis: Wiley Publishing, 2008. ISBN 978-04-7006-852-6.

Ceska-ecommerce.cz. Stav e-commerce v ČR v roce 2019 [online] [cit. 05. prosinec 2019]. Dostupné z: https://www.ceska-ecommerce.cz/

ČSN ISO/IEC 27000. Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Přehled a slovník informací. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2018.

ČSN ISO/IEC 27001. Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

ČSN ISO/IEC 27002. Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

ČSN ISO/IEC 27005. Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2018.

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

MATZNER, Jiří, 2017. GDPR: Nový strašák pro firmy. Nařízení shrnuje právník. Podnikatel.cz [online] [cit. 20. říjen 2019]. Dostupné z: https://www.podnikatel.cz/clanky/gdpr-novy-strasak-pro-firmy-narizeni-shrnuje-pravnik/

ONDRÁK, V. -- SEDLÁK P. -- MAZÁLEK V. Problematika ISMS v manažerské informatice. Vyd. 1. Brno: CERM, 2013. ISBN 978-80-7204-872-4.

POŽÁR, J. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

Přílohy

Příloha 1: Seznam použitých zkratek

API	Application Programming Interface
CIA	Confidentiality Integrity Availability
DOS	Denial of Service
EET	Elektronická evidence tržeb
EU	European Union
GDPR	General Data Protection Regulation
HW	Hardware
ICT/IT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IS	Information System
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISP	Internet Service Provider
OS	Operating System
PR	Public Relations
SW	Software
VPN	Virtual Private Network