Vývoj informačního managementu v průmyslu komerční bezpečnosti

Bc. Adam Březík

Diplomová práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Adam Březík**
Osobní číslo:	**A16259**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Vývoj informačního managementu v průmyslu komerční bezpečnosti**
Téma anglicky:	**Developments in Information Management in the Commercial Security Industry**

Zásady pro vypracování:

1. **Zpracujte rešerši literatury a pramenů, které se vztahují ke zpracovávanému tématu.**
2. **Vymezte fenomenologické a etiologické otázky spojené s informačním managementem v privátním bezpečnostním sektoru.**
3. **Zpracujte metodiku výzkumné části kvalifikační práce.**
4. **Analyzujte současný stav informačního managementu v komerční bezpečnosti.**
5. **Výstupy z praktické části kvalifikační práce aplikujte ve vlastních návrzích a závěrech, získaná data vyhodnoťte a zpracujte do grafů a tabulek.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **BRABEC, František, DOUCEK, Petr, ed. Informační management: soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur. Praha: Professional Publishing, 2010. ISBN 978-80-7431-010-2.**
2. **KAMENÍK, Jiří a František BRABEC. Komerční bezpečnost: soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur. Praha: ASPI, 2007. ISBN 978-80-7357-309-6.**
3. **LAUCKÝ, Vladimír a František BRABEC. Technologie komerční bezpečnosti I.: soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004. ISBN 80-731-8194-0.**
4. **VODÁČEK, Leo a Oľga VODÁČKOVÁ. Moderní management v teorii a praxi: soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur. Praha: Management Press, 2006. ISBN 80-726-1143-7.**
5. **VYMĚTAL, Jan, Anna DIAČIKOVÁ a Miriam VÁCHOVÁ. Informační a znalostní management v praxi: soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur. Praha: LexisNexis CZ, 2005. ISBN 80-869-2001-1.**

Vedoucí diplomové práce: **PhDr. Mgr. Stanislav Zelinka**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **8. prosince 2017**

Termín odevzdání diplomové práce: **28. května 2018**

Ve Zlíně dne 8. prosince 2017

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 10.5.2018

.....
podpis diplomanta

ABSTRAKT

Cílem diplomové práce je analýza vývoje manažerských postupů, integračního propojení souboru poznatků, metod, doporučení a systémových přístupů v oblasti bezpečnostní informatiky. Teoretická část práce se zabývá literární rešerší v oblasti informačního managementu, popisem nástrojů a metod a informační bezpečností.

Praktická část popisuje současný stav informačního managementu a zajištění informační bezpečnosti ve vybraném podniku. Ze získaných dat a informací společnosti je vypracována analýza a předloženy návrhy na opatření ke zlepšení současného stavu. V poslední kapitole diplomové práce je popsán způsob implementace nařízení o ochraně osobní údajů - GDPR.

Klíčová slova: informace, informační management, informační systém, informační manažer, informační bezpečnost

ABSTRACT

The aim of the diploma thesis is to analyze the development of managerial procedures, integration of the set of knowledge, methods, recommendations and system approaches in the field of security informatics The theoretical part of the thesis is focused on research of literature in field of information management, description of tools, methods and information security.

The practical part of the thesis describes the current state of information management and information security in selected company. The company’s data and information are analyzed and proposals are made for measures to improve the current situation. The last chapter of the diploma thesis descibes the way of implementation of the regulation on presonal data protection - GDPR.

Keywords: information, information management, information system, information manager, information security

Děkuji panu PhDr. Mgr. Stanislavu Zelinkovi za odborné vedení mé diplomové práce, cenné rady, ochotu a trpělivost. Dále bych chtěl poděkovat společnosti Cross Zlín, a.s. za poskytnuté informace, které jsem využil v praktické části diplomové práce. Poděkování také patří mé rodině za podporu a pomoc během celého studia.

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

OBSAH

ÚVOD

Informační management prochází od 60. let minulého století neustálým vývojem. Během těchto období se postupně měnilo i chápání toho, co pojem informační management vlastně znamená. V současnosti se objem informací na celém světě zvyšuje a dostupnost těchto informací je zejména díky internetu mnohem jednodušší. Tomuto trendu napomáhá i rychlý rozvoj informačních a komunikačních technologií, jejichž prostřednictví se lze k těmto informacím dostat. Informační management představuje nástroj, který pomáhá podniku určit relevantní informace a způsob, jak je správně využít pro ekonomický úspěch.

Informace jsou pro podnik velmi cenné, a proto je třeba věnovat patřičnou pozornost i jejich bezpečnosti. Poškození, zničení nebo ztráta důležitých informací, může pro podnik znamenat značné finanční náklady. Proto je lepší takovým situacím předcházet vhodným zabezpečením. V dnešní době existuje řada nástrojů, kterými se dá dosáhnout dobré úrovně informační bezpečnosti. Jedním z hlavních témat současnosti, které souvisí s ochranou dat, je nové evropské nařízení o ochraně osobních údajů, tzv. GDPR.

Cílem diplomové práce je analýza vývoje manažerských postupů, integračního propojení souboru poznatků, metod, doporučení a systémových přístupů v oblasti bezpečnostní informatiky.

Diplomová práce je rozdělena na dvě hlavní části, tedy na teoretickou a praktickou část. Teoretická část se skládá z popisu vývoje informačního managementu a jeho současných trendů, popisem nástrojů, metod a základních dokumentů. Dále se zabývá pojmy informační systém a informační bezpečnost.

Praktická část je zaměřena na popis současného stavu informačního managementu a úrovně informační bezpečnosti ve vybraném podniku. V této části práce jsou aplikovány metody analýzy rizik pro zjištění nedostatků. Na základě výstupů z těchto analýz jsou navržena nápravná opatření a doporučení pro zlepšení současné situace.

I. TEORETICKÁ ČÁST

1 INFORMAČNÍ MANAGEMENT

Pojem informační management nemá v současnosti jasně vymezený význam a lze ho tak chápat v několika různých souvislostech. Informační management se může například chápat jako skupina osob, která nese zodpovědnost za informační systém organizace. Jedním z dalších významů je proces výstavby a provozu informačních systémů organizace. [1]

1.1 Vývoj pojetí informačního managementu

Informační management si prošel od svého počátku několika vývojovými etapami. Během tohoto vývoje se postupně měnil pohled na něj i celé jeho chápání. Tento vývoj je podrobně rozebrán v následujících podkapitolách.

1.1.1 1. etapa

Podle Vymětala, Diačíkové a Váchové [1] sahají počátky informačního managementu do 60. let minulého století. Tento pojem byl poprvé použit v roce 1966, na konferenci systémového pojetí a zpracování inženýrských informací a výuky, americkým knihovním a informačním vědcem Robertem S. Taylorem a jeho kolegy. V tomto období se na informační management nahlíželo hlavně jako na prostředek pro ekonomické řešení technických úloh.

Informační management se počátkem 70. let rozšířil i do netechnických oblastí lidské práce, především z hlediska aplikace výpočetní techniky, jež měla pomoct k ekonomičtějšímu zvládání těchto prací. [1,2]

1.1.2 2. etapa

Na přelomu 70. a 80. let 20. století byla zaměřena pozornost na postupy ekonomicky hospodárné realizace projektů tvorby a fungování informačních systémů. Informační management byl v této době chápán jako management, který využívá prostředky informačních technologií. Nastala změna v pohledu na tvorbu a použití IS. Místo původního čistě technického pohledu se začínalo věnovat více pozornosti pohledu ekonomickému. [1,2]

Informačními manažery je možné nazývat projektanty IS. Ti měli za úkol najít postupy, jak efektivně zvládnout tvorbu a zavedení daných IS podle specifických požadavků. Problémem ale byly časté rozpory v názorech projektantů a zadavatelů zakázky. [1,2]

1.1.3 3. etapa

Začátkem 90. let dochází k většímu průniku informačního managementu do manažerské literatury. Informační technologie jsou stále více považovány za nástroje pro podporu a zajištění dosahování poslání a cílů organizace. Taktéž se začínají objevovat názory, že informační technologie představují nezbytně důležitý nástroj manažerské práce a slouží k jejímu účinnému a účelnému zabezpečení. [3]

V tomto období přestává být informační management zaměřený jen na ekonomické využití IS, jako tomu bylo v předchozích etapách a mnohem více se začíná soustředit pozornost na „celkový obraz“ podniku a jeho cílů, které by měl kvalitně zavedený informační management pomoct splnit. [2]

1.2 Současné pojetí informačního managementu

Počátek 21. století představuje zatím poslední etapu ve vývoji informačního managementu. Charakteristickým znakem této doby je rychlejší vznik a rozvoj nových technologií, jež jsou mnohem více dostupnější a používanější běžnými uživateli a pro udržení konkurenceschopnosti musí na tyto změny reagovat i podnikový management. Důsledkem stále novějších technologií je zvyšování nároků na informační manažery. Informační manažeři jsou vedoucí pracovníci, kteří by měli být hnací silou organizace v oblasti informatizace, vytváření a provozování jejich informačních systémů. [2,4]

Podle Lukáše, Hrůzy a Kného [4] se informační management skládá z těchto tří hlavních oborových zdrojů:

- management,
- informační systémy a technologie,
- systémový přístup.

Z oblasti managementu využívá poznatků především z hlediska formulace cílů, funkcí, procesů a metod. Systémový přístup znamená způsob, jakým by mělo být na informační management nahlíženo, tedy jako na soustavu. Ta je složena ze sjednocených prvků k uplatnění cílové funkce. Posledním oborem, na jehož základech je informační management postaven, je informatika. Odborné znalosti z oblasti informačních technologií jsou klíčovým faktorem pro naplnění cílů informačního managementu. Informační technologie představují nástroj informačního managementu, a také potenciál pro vytvoření informačního systému. [4]

1.3 Trendy v současném informačním managementu

Trendy informačního managementu, které budou popsány v následující kapitole, lze rozdělit do dvou kategorií. Jedná se o generické ICT trendy a specifické trendy pro informační management. Do kategorie generických ICT trendů ovlivňující i informační management patří hlavně mobilita a všudypřítomné připojení, Big data, sociální média a Cloud computing. Z kategorie specifických trendů pro informační management stojí za to, zmínit například nové případy užití informací, dostupnost nových druhů informací nebo rostoucí počet zdrojů informací. [5,6]

1.3.1 Mobilita a připojení

Rozvoj v oblasti informačních technologií znamená zvýšení mobility pracovníků, ať už se jedná o mobilitu geografickou, tak i možnost pracovat třeba z domova. Informační management by tedy měl být schopen zajistit, aby měl každý pracovník náležité informace dostupné kdekoliv. S tímto trendem je spojený i přesun práce na mobilní zařízení, a proto je potřeba zobrazované informace tomuto trendu přizpůsobit. Samozřejmě, že přesun práce na tyto typy zařízení s sebou nese i spoustu bezpečnostních rizik. Zejména se jedná o zabezpečení koncových zařízení a rizika spojená s přenosem dat do koncového mobilního zařízení. Dalším trendem v oblasti informačního managementu je bezesporu změna v rychlosti rozhodování. V dnešní době je především na vedoucí pracovníky vyvíjen stále větší tlak na rychlost rozhodnutí, a i zvětšující se počet rozhodnutí. Pro každé rozhodnutí potřebují manažeři správné a relevantní informace, a úkolem informačního managementu je jim je poskytnout. Pro informační management to znamená rozvoj služeb datové logistiky. Ačkoliv mohou být tyto změny pro organizace prospěšné, tak mají bohužel i vliv na osobní život zaměstnanců. Neustálé připojení pracovníků k firemní síti může mít za následek i komunikaci s kolegy mimo pracovní dobu. To může mít v dlouhém časovém horizontu za následek zvyšování stresu pracovníka a jeho sníženou výkonnost. [5,6]

1.3.2 Big data

Pojem Big Data je poměrně nový, ale i tak je již velmi populární a zabývá se jím hodně institucí a firem. Tento pojem je možné definovat jako množiny dat, které se dají charakterizovat velkým objemem, velkou komplexitou, různorodostí a rychlostí změny. Z hlediska významu jsou Big Data pro informační management velmi důležitá, poněvadž velmi podstatně zvyšují kvantitu dostupných dat. Nárůst objemu dat představuje významný faktor pro

zavedení pojmu Big Data. Tento nárůst je způsoben několika vlivy. Prvním z nich je rostoucí dostupnost úložných zařízení, jež přímo souvisí s neustálým rozvojem technických prostředků. V souvislosti s technickým rozvojem totiž dochází k neustálému nárůstu uložených dat. Dalším důležitým faktorem je rostoucí potřeba dat. S dostupností dat je spojena nová potřeba dat v pracovních postupech a věcných oblastech, kde buď dříve nebyla data dostupná anebo nebyla zapotřebí. Dále zde patří vznik nových datových formátů pro uložení, jelikož dochází ke stále většímu používání multimédií a rozšiřování počítačových čipů do více oblastí našeho života. S tím souvisí i nárůst zdrojů dat, které jsou dostupné pro jejich ukládání. [5]

Nárůst objemu dat s sebou nese samozřejmě spoustu výhod, ale i nákladů, a proto je důležité o něm správně přemýšlet. Zvyšování objemu ukládaných dat je sice možné, ale znamená to i zvyšování nákladů. Protože data často obsahují velké množství informací, kterým je potřeba porozumět, je nutné používat různé nástroje pro jejich zobrazování. V současnosti je moderní, data zobrazovat pomocí nejrůznějších grafických ukazatelů, dashboardů a interaktivních nástrojů. [5]

1.3.3 Sociální média

Fenoménem dnešní doby jsou bezesporu sociální média, která lze podle Doucka [5] charakterizovat jako skupinu internetově orientovaných aplikací, založených na ideových a technických základech platformy Web 2.0. Tato platforma umožňuje tvorbu a výměnu obsahu generovaného uživateli. Typickým příkladem sociálních médií současnosti mohou být např.: Facebook, Twitter, Skype, Whatsapp, YouTube a mnohé další.

Sociální média mají hned několik dopadů na oblast informačního managementu. Jedním z nich je vnitrofiremní komunikace. Většina komunikace probíhá prostřednictvím mobilních telefonů nebo emailů. V mnoha organizacích dochází, kromě zavádění intranetových stránek nebo diskuzních skupin, i k zavádění zcela nových technologií, jako jsou vnitrofiremní sociální sítě, které je možné napojit i na Facebook nebo Linked-In. Rozvoj sociálních sítí s sebou nese i nové komunikační kanály, které mohou být využívány ke komunikaci s klienty, i se širokým okolím. Patří mezi ně například blogy, přítomnost na sociální síti či sdílená videa. Využívání sociálních sítí nemusí být zaměřeno jen na komunikaci se zákazníky, ale třeba na získávání a vyhledávání informací o svých klientech. Informace tohoto typu mohou být dostupné přímo z konkrétní vazby na sítích ovládaných klienty, anebo také z elektronických

stop, jež za sebou zanechávají klienti v programech a aplikacích třetích stran. Na základě těchto získaných dat poté firmy mohou upravovat komunikaci s klientem. [5,6]

Informační management se vzhledem k rozvoji sociálních sítí bude muset vypořádat s několika novými oblastmi. Jednou z nich jsou nové datové formáty. Doposud totiž informační management zpracovával v podstatě jen čísla, předem strukturované texty a nějaké číselníky. V současnosti si ovšem bude muset poradit i s nestrukturovaným textem, audio a video nahrávkami, geografickými nebo behaviorálními daty. Další problém pro informační management představuje analýza nestrukturovaných dat ze sociálních sítí. V tomto případě bude zapotřebí vymyslet nové analytické postupy, které budou zaměřeny i na vyhledávání nových a zatím zcela netušených skutečností. Vzhledem k velkému množství ukládaných osobních dat, je nezbytné připravit speciální politiku pro nakládání s těmito daty uvnitř i vně organizace, a promyslet možnosti jejich případného ekonomického využití, archivace a jejich mazání. [5]

1.3.4 Cloud computing

„*Cloud computing je nový způsob využívání zdrojů (zejména hardware, software) v IT, vycházející z možnosti jejich sdílení mezi aplikacemi a odstranění přímé vazby aplikační logiky na fyzické komponenty (virtualizace)“.* [7]

Ve spojitosti s informačním managementem existuje několik důležitých aspektů, poněvadž v mnoha případech data fyzicky opouštějí hranice organizace. Z tohoto důvodu je důležité upravit směrnice o nakládání s daty a nastavení metodiky uložení dat a jejich fyzickou kontrolu na místě uložení. Klíčové pro využívání cloud computingu je správně nastavit dostupnost služby, což se projeví na její ceně. Využívání služeb cloud computingu znamená také nárůst potřeb internetového připojení. Data v rámci této služby jsou dostupná v podstatě odkudkoliv. Proto je třeba myslet i na architekturu řešení, jelikož nejde jen o zajištění dostupnosti dat, ale také jejich ukládání a zálohování v jiných lokalitách cloudu. Dostupnost dat kromě úpravy architektury řešení znamená i úpravu jejich zabezpečení, aby nedošlo k datovému úniku. Nicméně je nutné zabezpečit i přenos dat mezi datovým úložištěm a místem pro využití dat, ať už jsou umístěna kdekoliv. [5,7]

Cloud computing znamená zásadní změnu podnikových ICT a velmi výrazně zasahuje i do informačního management. Hlavně v oblastech poskytování dat uživatelům. [5]

1.4 Zásady, metody a nástroje informačního managementu

V této podkapitole jsou vypsány vybrané zásady, metody a nástroje, které se využívají v rámci informačního managementu.

1.4.1 Zásady

Podle Tvrdíkové [8] je během realizace procesů informačního managementu vhodné dodržovat jisté zásady. Za zásadu lze považovat určitý princip, myšlenku nebo nepochybné východisko, které je ověřeno v praxi a jeho použitím je možné docílit efektivního a optimálního výsledku. Základními zásadami informačního managementu jsou **komplexnost, efektivnost, trvalost a přiměřenost**.

- zásada komplexnosti napomáhá vidět organizaci komplexně,
- zásada efektivnosti zabezpečuje, aby náklady na informační systém odpovídaly následné informační podpoře,
- zásada trvalosti představuje trvalý zájem o zlepšení činnosti informačního systému,
- zásada přiměřenosti pomáhá zajistit přiměřenou informační podporu v organizaci. [8]

1.4.2 Metody

Řídící pracovníci používají pro dosažení cílů během životního cyklu informačních systémů určité metody práce, jež napomáhají efektivnímu vykonávání činnosti. V této podkapitole jsou dále popisovány metody, které patří mezi hlavní metody informačního managementu. Za základní metody informačního managementu můžeme považovat **analýzu, syntézu, metodu systémového přístupu, metodu projektového řízení, optimalizace, audit a metodu operativního řízení**:

- **metoda analýzy** je chápána jako myšlenkový postup, který rozkládá vymezený celek na jeho menší části,
- **metoda syntézy** je opakem analýzy, jelikož tato metoda spočívá ve skládání, spojování a slučování menších částí do jednoho celku,
- **metoda systémového přístupu** umožňuje vidět výsledný systém jako jednotu prvků a vazby mezi nimi,
- **metoda projektového přístupu** přistupuje k přípravě a návrhu IS jako k projektu,

- **metoda optimalizace** slouží pro hledání nejlepšího postupu s ohledem na zadaná kritéria,
- **audit** je metoda**,** která slouží ke zhodnocení stavu a porovnání s požadovaným stavem,
- **metoda optimálního řízení** je postavena na trvalém monitorování informačního systému a následném odstranění nedostatků jeho činnosti. [8]

1.4.3 Nástroje

V následující podkapitole jsou popsány důležité nástroje informačního managementu. Zde je možné zařadit například:

- **systém řízení informačního systému** představuje základní nástroj informačního managementu. Stanovuje systém, kompetence, odpovědnosti, činnosti orgánů informačního managementu v oblasti zabezpečení výstavby a provozu informačního systému,
- **systém řízení bezpečnostních informací** obsahuje organizační strukturu, plánovací činnosti, odpovědnosti, praktiky, postupy, procesy a zdroje.
- **informační strategie** je koncepční dokument pro provoz a využití IS dané organizace,
- **předpis** znamená vymezení pravidel, která jsou obecným návodem pro řešení problému,
- **směrnice** jsou dokument, který upřesňuje na základě předpisů a platné legislativy způsob, jak realizovat danou činnost v určité oblasti,
- **provozní dokumenty** obsahují údaje důležité pro zajištění informační podpory,
- **zpráva auditu** představuje dokument, ve kterém je popsáno zhodnocení současného stavu dané oblasti informačního systému,
- **softwarové produkty** jsou nástroje, které pomáhají realizovat informačnímu managementu podporu jejích činností,
- **školení zaměstnanců** slouží pro získání informací a znalostí způsobů, jakým lze využít informační systém. [8]

1.5 Informační manažer – CIO

Informační manažer je vedoucí pracovník, který je zodpovědný za strategický rozvoj a bezpečnost informačních systémů. Jelikož jde o velmi odpovědnou manažerskou pozici, bývá

obvykle součástí top managementu organizace. Hlavním úkolem informačního manažera, je řízení provozu a rozvoje informatiky v organizaci, a optimalizování cílů organizace pomocí informačních a komunikačních technologií. Informační manažer má možnost delegovat část svých pravomocí a odpovědností na jiné vrcholové manažery nebo manažery nižších úrovní. Podobně jako každý manažer musí i ten informační splňovat náležitou úroveň manažerských dovedností. [8,9]

Podle Vágnerové [9] se pro popis rozsahu a kompetencí informačního manažera používá model **CIO Wheel**. Tento model popisuje kompetence informačního manažera v těchto deseti oblastech:

- Policy – politika, pravidla,
- Strategic planning – strategické plánování,
- Performance & Result based – výkonnost a orientace na výsledky,
- Process Improvement – zlepšování procesů,
- Capital Planning & Investment – investiční plánování,
- Leadership management – vedení lidí,
- Technology Assesment – hodnocení technologií (ICT),
- Security – bezpečnost,
- Architectures – architektura,
- Acquisition – nákup a získávání zdrojů.

Častým problémem, jenž informačnímu manažerovi brání v naplňování jeho povinností, je nedostatečný soulad mezi oddělením IT a danou organizací. [9]

2 ZÁKLADNÍ DOKUMENTY INFORMAČNÍHO MANAGEMENTU

Tato kapitola pojednává o základních dokumentech, které jsou důležitým nástrojem informačního managementu. Mezi tyto dokumenty patří **informační strategie, informační politika a bezpečnostní politika organizace**. Popis jednotlivých typů těchto dokumentů je uvedený v následujících podkapitolách.

2.1 Informační strategie

Informační strategie představuje základní dokument informačního managementu. Obsahem tohoto dokumentu je soubor doporučení, která v dané organizaci vymezují informační potřeby a způsob jejich zabezpečení, v souladu s celkovou podnikatelskou strategií firmy. Jedná se o jednu z dílčích strategií a navazuje na globální strategii organizace. Informační strategie je taktéž základním nástrojem systémové integrace. Vytvoření informační strategie je možné svěřit externí organizaci, je však nutné, aby obě organizace při tom vzájemně spolupracovaly. Není totiž možné, aby externí organizace byla schopna bez pomoci zadavatele sama tuto strategii vytvořit. Řada firem se může vypracováním informační strategie zbavit mnoha svých problémů a snížit rizika ze zavádění a inovací IS/ICT. Zodpovědnost za informační strategie organizace má většinou informační manažer firmy. [10,11]

Informační strategie podle Kocha a Ondráka [10] obsahuje tyto hlavní body:

- určení vazeb mezi celkovou strategií firmy a informační strategií,
- analýza dosavadního vývoje informačních technologií v organizaci,
- analýza a prognóza obecného vývoje informačních technologií,
- určení informačních zdrojů pro informační podporu systému řízení firmy,
- plán rozvoje informačního systému ve střednědobém a dlouhodobém horizontu,
- objem finančních a nefinančních zdrojů pro zajištění realizace strategie,
- přehled standardů, které budou při realizaci uplatňovány,
- návrh organizačních změn a metrik dosažení cílů,
- návrh kvalifikačních a rekvalifikačních programů,
- zásady pro vyhodnocování účinnosti realizace strategie.

S informační strategií jsou spjaty i taktické a strategické plány, které představují detailní popis a harmonogram jednotlivých projektů realizovaných v oblasti informatiky ve firmě. Kromě těchto plánů může být součástí informační strategie i aplikační, funkční, datová a technická architektura, sloužící pro další rozvoj a budování IS/IT. [10]

2.2 Informační politika

Pojmem informační politika se rozumí dlouhodobá koncepce rozvoje informačních a komunikačních technologií. Způsob budování a provozování informačního systému organizace je klíčovým kritériem pro dělení jednotlivých informačních politik. Správné nastavení a uplatnění informační politiky je ukázkou kvality informačního manažera. Soustavné pěstování a prosazování informační politiky zlepšuje informační podporu řízení a napomáhá vzniku informačně založené organizace. Informační politika se podle Lukáše, Hrůzy a Kného [4] dělí takto:

- technokratický utopismus,
- anarchie,
- feudalismus,
- monarchie,
- federalismus.

2.2.1 Technokratický utopismus

Tento typ informační politiky staví do popředí především využívání nejnovějších informačních technologií v rámci informačního systému organizace. Cílem této politiky je zajištění bezchybnosti a spolehlivosti informačního systému. V rámci politiky se příliš nezohledňuje využití jednotlivých aplikací uživateli nebo efektivnost vynaložených prostředků. Technicky a informaticky založený manažer spoléhá hlavně na sílu technologií. [4]

2.2.2 Anarchie

Je typem politiky, které schází jakýkoliv řád při budování informačního systému organizace. Při pořizování a provozování technických prostředků informačního systému se vychází z aktuálních potřeb a spoléhá se na individuální znalosti a nápady jednotlivých pracovníků organizace. Vzhledem k tomu, že nedochází k jednotnému vybavování organizace informačními systémy, nejsou tyto samostatné systémy schopné vzájemné spolupráce. Typickým příkladem jsou často jednotlivé osobní počítače s individuálními aplikacemi a databázemi. K nakupování nových prostředků dochází nárazově a ve většině případů za peněžní prostředky, které organizaci v rozpočtu zbyly. [4]

2.2.3 Feudalismus

V rámci tohoto druhu politiky si jednotlivé prvky organizace vytváří a budují vlastní informační systémy. Takový informační systém podává vrcholnému managementu pouze vymezené informace a pracovníkům z jiných prvků organizace je neposkytuje vůbec. Všechny informační systémy se skládají z managementu, technologií, standardů a rozpočtu. Globální a kooperativní řízení není možné vzhledem k uplatňování této informační politiky. Pozice informačního manažera na centrální úrovni organizace většinou neexistuje anebo nemá potřebné pravomoci, aby mohl prosadit budování informačního systému jako celku. Informační management je v takové organizaci zpravidla na nízké úrovni. [4]

2.2.4 Monarchie

Jedná se o typ informační politiky, jenž podporuje a zajišťuje centralizované řízení budování informačního systému organizace. Informační manažer disponuje rozsáhlými kompetencemi pro realizování informační politiky. Celkovou koncepci informačního systému určuje centrum a jednotlivé prvky organizace tudíž nemají šanci ovlivnit, jaký informační systém mohou mít k podpoře své činnosti. Mimo jiné centrum také určuje možnosti přístupu k informacím, kvalitu aplikací a způsob sdílení dat. Aktivní role jednotlivých uživatelů, prvků a složek je tímto druhem politiky potlačována a nedochází k uspokojení informačních potřeb, jelikož zde chybí zpětná vazba od uživatele k řídícím orgánům. [4]

2.2.5 Federalismus

Toto pojetí informační politiky podporuje optimální vztah mezi centralizací a autonomností informačních systémů jednotlivých prvků organizace. Vytvořený informační systém je složený z jednotlivých subsystémů a umožňuje sdílení dat. Neexistují žádné technologické překážky pro spolupráci jednotlivých aplikací. Takový informační systém podporuje cílovou funkci organizace komplexně a zaměřuje se na podporu hlavní činnosti organizace. [4]

2.3 Bezpečnostní politika

Bezpečnostní politika je základním dokumentem informační bezpečnosti. Po přijetí a schválení managementem organizace je tento dokument závazný pro celou společnost a určuje východiska pro veškeré další aktivity společnosti v informační bezpečnosti. Bezpečnostní politika má za cíl:

- definovat hlavní cíle při ochraně informací,

- stanovit způsob jak bezpečnost řešit,
- určit pravomoci a zodpovědnost. [11,12]

Po zpracování bezpečnostní politiky je důležité s tímto dokumentem seznámit také všechny zaměstnance podniku. Seznámení zaměstnanců s celým obsahem není nutné, podstatné jsou ty části, které přímo souvisí s výkonem jejich pracovní funkce. Pokud je politika rozsáhlejší, je vhodné připravit tabulku pracovní funkce bezpečnostní politiky informačního systému. V této tabulce se pak zaznamená, jestli je určitá oblast pro danou funkci potřebná. Takovou tabulku je poté možné využít například pro přípravu školení či extraktů z bezpečnostní politiky. [11,12]

Principy informační bezpečnosti, které jsou definovány v bezpečnostní politice informačního systému, se pomocí bezpečnostních standardů zpracovávají do detailní podoby. Tyto standardy jsou ve shodě s bezpečnostní politikou a předpokládá se častější frekvence jejich úprav. [13]

3 INFORMAČNÍ SYSTÉMY

Pro pojem informační systém existuje řada různých definic. Obecně lze říci, že informační systém je možné chápat jako systém, který vzájemně propojuje informace a procesy, jež s těmito informacemi pracují. Procesy tedy znamenají funkce zabezpečující sběr, přenos, uložení, zpracování a distribuci informací. [14]

Podle Lukáše, Hrůzy a Kného [4] jsou informační systémy předmětem informačního managementu.

3.1 Architektura informačních systémů

Architekturu informačních systémů je možné definovat jako koncepční rámec řešení informačního systému. Architektura představuje jeden z nástrojů systémové integrace a měla by respektovat strategii podniku. Absence architektury způsobuje nepokryté požadavky a funkce, draze nakoupený hardware a software, který není možné využít aj. Dělí se na globální a dílčí architekturu. [15]

3.1.1 Globální architektura

Globální architektura představuje základní schéma informačního systému a tvoří ji jednotlivé stavební bloky. [10]

3.1.2 Dílčí architektura

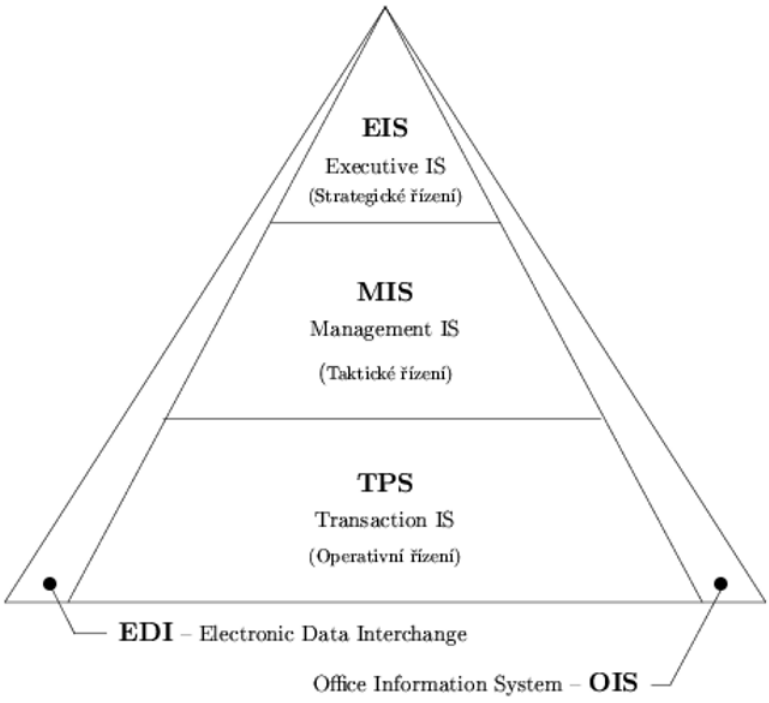
Dílčí architektura, se na rozdíl od architektury globální, zabývá podrobnějšími návrhy informačních systémů podle různých hledisek. Do této kategorie patří tyto architektury:

- **funkční architektura** – rozděluje informační systém na subsystémy pomocí dekompozice globální architektury,
- **procesní architektura** – zaměřuje se na popis budoucího stavu procesů v podniku. Cílem této architektury je připravit co nejefektivnější reakce podniku na externí události,
- **technická architektura** – stanovuje typy a rozmístění prostředků informačních technologií. Tento druh architektury je zobrazován schématem a specifikací počítačových sítí, serverů, koncových uživatelských počítačů a jiných zařízení,

- **technologická architektura** – definuje způsoby, jakými jsou zpracovávány jednotlivé aplikace v těsné návaznosti na určenou technickou, datovou a programovou architekturu,
- **datová architektura** – je návrh datové základny organizace a jejím výsledkem je schéma všech databází a jejich vět,
- **softwarová architektura** – vymezuje programy a programové komponenty, ze kterých se bude daný informační systém skládat a jaké vazby mezi nimi budou existovat,
- **komunikační architektura** - stanovuje jakým způsobem bude informační systém komunikovat se svým okolím,
- **řídící architektura** – určuje pravidla pro fungování systému, standardy a organizaci služeb uživatelům. Součástí této architektury může být i orgware, což je organizační struktura a pravidla fungování systému. [10]

3.2 Rozdělení informačních systémů

Informační systémy lze rozdělit do kategorií podle několika různých hledisek. Může to být například podle účelu, obsahu, velikosti, strukturální složitosti, počtu a typu uživatelů apod. S ohledem na postavení informačního systému v systému řízení, se dá rozlišit zejména jeho úroveň na stupni informační pyramidy. Informační pyramida je znázorněna na následujícím obrázku. [16]



Obr. 1. Druhy informačních systémů [16]

V této podkapitole jsou podrobněji popsány vybrané druhy informačních systémů.

3.2.1 TPS

Transakční informační systémy podporují hlavní činnosti podniku na operativní úrovni a jsou nástupci klasických dávkových systémů. V minulosti byla vedlejším produktem těchto systémů kategorie pracovníků, jež byli specializovaní, pouze na vstup dat do těchto systémů. S nástupem on-line systémů se tato situace změnila a uživatelé transakčních systémů jsou v současnosti velmi kvalifikovaní pracovníci, kteří jsou schopni provádět samostatná rozhodnutí v zájmu podnikových cílů. Specifikace těchto systémů závisí na zaměření podniku a jeho konkrétní činnosti. Jedná se tedy o provozní informační systémy, které zajišťují základní funkce organizace. [16]

3.2.2 MIS

Systémy MIS zajišťují hlavně taktickou a částečně i operativní úroveň řízení. Jedná se o nástroj pro střední řídící vrstvu. Charakteristickým znakem pro tuto úroveň je skutečnost, že značné množství úloh na této úrovni je standardizováno a jsou velmi podobné pro organizace různého typu. Manažerské informační systémy zabezpečují především informační podporu pro řešení částečně nebo špatně strukturovaných problémů s menší možností algoritmizace a s větší mírou potřebné aplikace heuristických a znalostních postupů. [4,14]

3.2.3 EIS

Systémy EIS jsou zaměřeny na podporu vrcholového řízení organizace pro podporu globálních a strategických rozhodnutí. Tyto systémy zajišťují výběr a zpracování nejdůležitějších dat ze všech důležitých oblastí v organizaci. Dále využívají vlastní prostředky pro modelování analytických a rozhodovacích procesů s pomocí statistických metod. Systémy EIS nabízí stálou aktualizaci svých modelů z dostupných datových zdrojů a umožňují uživateli velmi kvalitní formu výstupů. [4,14]

3.2.4 DSS

Systémy DSS podporují většinou taktické rozhodování a využívají přitom optimalizační a simulační programy. Vstupními daty jsou obvykle jednorázové úlohy a výsledek je požadován v krátkém čase. Pro zvýšení vypovídající hodnoty jsou výstupní data doplňována grafickým znázorněním. Tento efekt však umožňují pouze počítače, které jsou zapojeny do hierarchických sítí pro možnost přenosu potřebných dat. [14]

3.2.5 Expertní systémy

Tyto informační systémy jsou postaveny na pravidlech, pomocí kterých i méně zkušení pracovníci dokáží řešit úlohy diagnostického charakteru. V tomto systému jsou soustředěny znalosti unikátních expertů a využívá se zde technologie umělé inteligence. [14]

3.2.6 OIS

Systémy OIS zabezpečují automatizační podporu typických kancelářských činností. Z hlediska náplně systémů OIS došlo v posledních letech k prudkému vývoji. Jedná se o skupinu úloh, které mají sloužit pro podporu individuální práce uživatele, a to pro podporu zejména rutinních kancelářských prací. Mezi ně patří psaní textů, kreslení obrázků, příprava prezentací, správa dokumentů, elektronická pošta apod. Mimo to existují ještě tzv. malé manažerské informační systémy, do kterých patří např. interní telefonní seznamy, kartotéky zákazníků, manuály osvědčených firemních postupů apod. Podstatou těchto systémů je fakt, že se s nimi pracuje s malým lidským úsilím, jelikož se snadno zavádějí a přitom poskytují uživatelům velmi cenné služby. Obvykle je uživatelé zpracovávají jen pro svou osobní potřebu, ale mohou mít i charakter, kdy slouží více osobám nebo i celé organizaci. [14]

3.3 Informační systémy v bezpečnostních službách

Informační systémy v bezpečnostních službách musí splňovat specifické požadavky. K vymezení těchto potřeb docházelo postupně. Začátek používání informačních systémů vedl k objektivnímu posuzování výkonů jednotlivých pracovníků, při určování mzdových nároků. Další problematikou byla personalistika a hned poté logistická podpora pracovní činnosti (evidence a správa pracovních pomůcek, výstroje, výzbroje a evidence jízd motorových vozidel). První informační systémy vznikaly během roku 2000 a dodávaly se průřezově pro všechna odvětví. K rozlišování specifických potřeb bezpečnostních služeb začalo docházet až v dalších letech. Průkopníkem v této oblasti lze nazvat programový produkt Helios. Zde jsou uvedeny požadavky bezpečnostních služeb, ze kterých tento program vychází:

- autofakturace,
- Controlling Business Intelligence,
- dokumentace pro management,
- evidence a správa vozového parku,
- evidence a správa pracovních pomůcek, výstroje a výzbroje,
- mzdy a personalistika,

- připojení na specializované softwarové a hardwarové vybavení,
- Workflow. [11]

Pro vytváření softwarových produktů byl dalším významným zdrojem seznam aktivit bezpečnostních agentur. Mezi hlavní oblasti zájmů těchto organizací patří především systémy zabezpečení osob, majetku a informací. Na základě těchto skutečností byly určeny klíčové oblasti a jejich podoblasti:

- **Fyzická ostraha**
  - FO objektů, majetku a osob,
  - střediska pro monitorování a dispečinky,
  - kontrola vozidel a osob,
  - recepční služby,
  - pořadatelské služby. [11]
- **Vzdálený dohled a mobilní hlídky**
  - výjezd na signál PCO,
  - pravidelná kontrola objektů a určitých lokalit,
  - vzdálený dohled před vniknutím, požárem, zaplavením nebo jinou živelnou či zaviněnou katastrofou. [11]
- **Cashové služby**
  - přeprava finančních hotovostí a cenných zásilek,
  - další služby spojené s hotovostí. [11]
- **Instalace bezpečnostních technologií**
  - návrh, projektování a realizace komplexního řešení technického zabezpečení,
  - bezpečnostní analýza zabezpečovaného objektu,
  - poradenská a projekční činnost,
  - realizace technického zabezpečení a napojení na PCO. [11]
- **Facility management**
  - správa a údržba nemovitostí a zařízení,
  - revize a odborné technické prohlídky,
  - havarijní služba, opravy,
  - úklidové služby. [11]

4 INFORMAČNÍ BEZPEČNOST

Pojem informační bezpečnost podle Jaška [13] představuje zodpovědnost za ochranu informací během jejich vzniku, zpracování, ukládání přenosů a likvidace využitím logických, technických, fyzických a organizačních opatření, která musí působit proti ztrátě důvěrnosti, integrity a dostupnosti těchto hodnot.

Zajištění bezpečnosti informačních systémů je jednou z klíčových oblastí, které je třeba věnovat patřičnou pozornost. Jestliže by došlo ke zničení nebo zneužití dat, může to pro firmu znamenat mnohem větší problém, než nahradit zničenou techniku či přeinstalovat poškozené programy. Kromě zabezpečení informačního systému ochrannými prvky proti vnějším hrozbám, je stejně tak důležité zabezpečení systému proti napadnutí zevnitř organizace. [13]

Koch [10] ve své knize uvádí, že podle výsledků několika statistik vyplývá, že největší procento zneužití dat mají na svědomí pracovníci vlastní organizace.

Bezpečnost informačních systémů je nutno chápat i jako součást bezpečnosti celé organizace, jenž obsahuje velké množství další aspektů, jakými jsou třeba personální bezpečnost, zabezpečení objektu proti neoprávněnému vniknutí apod. [10,13]

4.1 Bezpečnostní hrozby a rizika

Hrozba představuje jakoukoliv událost, která využívá zranitelnosti aktiva a může způsobit na aktivu potenciální škodu. Hrozby se dělí především na **objektivní** a **subjektivní**. Mezi objektivní hrozby patří **přírodní** hrozby, jejichž prevence je obtížná a obvykle se v tomto případě provádí opatření pro minimalizaci dopadů škod. Dalšími objektivními hrozbami jsou hrozby **fyzikální, technické** nebo **logické**. Na rozdíl od objektivních hrozeb ty subjektivní plynou především z lidského faktoru. Mohou to být hrozby **neúmyslné**, které jsou většinou způsobeny neproškoleným uživatelem, anebo hrozby **úmyslné**. [13,17]

Typickými hrozbami pro informační technologie jsou např. **modifikace informací, informačních zdrojů a služeb, agregace citlivých informací, krádeže hardwarových a softwarových komponent** atd. Riziko představuje určitou pravděpodobnost, že nastane škodlivá událost. Vhodným nástrojem pro odhalení možných hrozeb je analýza rizik. Ta kromě určení hrozeb stanoví i pravděpodobnost, s jakou může daná hrozba nastat a způsobit škody. Při ochraně aktiva vždy záleží na jeho ceně a nákladech na jeho ochranu. [17]

4.2 Bezpečnostní incidenty

Bezpečnostní incident je událost, která je vždy doprovázena informačními ztrátami. Za bezpečnostní incidenty lze považovat např. **poškození nebo ztrátu datových souborů, delší vyřazení systému z provozu, rozšíření počítačových virů v síti** apod. Jakmile dojde ke zjištění bezpečnostního incidentu, je nutné, aby došlo k vyšetření jeho příčiny a k podrobnému analyzování situace. Po odstranění důsledků je důležité realizovat taková opatření, která zamezí opakování incidentu. Zde je uveden obvyklý postup šetření bezpečnostního incidentu:

- zjištění zdroje napadení systému,
- zajištění důkazů podrobným šetřením a změna přístupových hesel diskriminovaných účtů,
- zjištění možnosti fyzického přístupu ke zdroji,
- zpracování protokolu s osobami, které byly, mohly nebo neměly být účastníky incidentu,
- vyvození disciplinárních nebo kázeňských opatření s viníky na základě výsledků z důkladného šetření,
- přijetí technických, režimových a jiných preventivních opatření v informačním systému a na příslušných pracovištích. [17]

4.2.1 Minimalizace bezpečnostních incidentů

Informační systémy organizace obsahují velké množství citlivých a utajovaných dat, jejichž únik by mohl danou organizaci i finančně poškodit. Organizace jsou povinny data chránit a ve většině případů i ze zákona. Jedná se zejména o soubory osobních dat zaměstnanců, mzdové soubory, údaje spořitelny, akcionářů atp. K úniku těchto dat může dojít hned několika možnými způsoby. Jedním z možných způsobů obrany proti úniku dat je identifikace, při které se posuzuje prokazatelnost konkrétního zdroje informace a kteréhokoli prvku informačního systému, jenž přišel s informací do styku. Pro minimalizaci bezpečnostních incidentů existují tyto tři způsoby:

- **minimalizace pravděpodobnosti** vzniku kalamitní situace,
- **minimalizace škod** v případě, že kalamitní situace už nastala,
- **návrh a použití vhodné metody obnovy** po odeznění kalamitní situace. [17]

4.2.2 Prevence bezpečnostních incidentů

Hlavním cílem prevence je předejít vzniku jakýkoliv příčin a podmínek zločinnosti a kriminality. Případně zabránit tomuto nebezpečí, jestliže vznikají náznaky ohrožení a zabránit procesům, jež mají nežádoucí a kriminogenní účinky. Volba nástrojů a prostředků prevence je závislá na příčinách a podmínkách stávajícího ohrožení a zpracování prognózy případného ohrožení informací a jejich systému. Prevence je možné dělit na **obecnou, zvláštní a situační**. [17]

- **obecná prevence** je taková, kdy její opatření působí celkově na všechny objekty a subjekty pracující s informacemi, bez ohledu na to, jestli nebezpečí už vzniklo,
- **zvláštní** nebo také **individuální** prevence představuje opatření, která se zaměřují na vybrané jevy a procesy v běžných pracovních procesech,
- **situační prevence** provádí rychlá operativní opatření na základě momentální situace s cílem zabránit, odvrátit a překazit vznik dalších škod anebo zmírnit následky působení některých příčin. [17]

4.2.3 Hrozby sociálních sítí

Sociální sítě jsou v dnešní době stále více populární. Existuje mnoho aplikací, které využívají miliony uživatelů. Stránky sociálních sítí jsou aplikace, které sami o sobě pro organizaci nepředstavují významný problém. Hrozby pro podniky představují spíše zaměstnanci, kteří využívají sociální sítě. Mohou to být např. **problémy v oblastech produktivity, internetové konektivity, virů a malwaru, sociálního inženýrství, reputace a právní odpovědnosti**:

- **produktivita** představuje jeden z hlavních důvodů, proč organizace zakazují přístup k sociálním sítím. Používání sociálních sítí v pracovní době může do značné míry snížit produktivitu zaměstnanců, kteří se tak více věnují svému profilu než pracovním povinnostem. Účinným nástrojem pro řešení tohoto problému je vypracování komplexní bezpečnostní strategie filtrování webového přístupu. Aby společnosti byly včas varovány a připraveny na možná rizika, potřebují softwarové nástroje pro komplexní zabezpečení, monitoring a řízení přístupu zaměstnanců na internet,
- **internetová konektivita** může být ohrožena v případě, že je internetové připojení zatěžováno využíváním sociálních sítí a může tím pádem dojít ke zpomalení práce nebo vyšším nákladům na internetové připojení,

- **viry a malware** představují velká rizika, poněvadž v nich hackeři vidí značný potenciál k provedení spamových útoků nebo k distribuci škodlivého kódu. V současnosti existuje i řada aplikací třetích stran pro různé sociální sítě, jejichž zabezpečení nemusí být na dokonalé úrovni. Některé z těchto aplikací mohou dokonce nakazit počítače škodlivým kódem, který následně může shromažďovat citlivá data ze sociální sítě či provádět jiné škodlivé aktivity,
- **sociální inženýrství** může vést ke ztrátě dat nebo odcizení identity. Jde o problém, který se pořád rozšiřuje a má stále více obětí. Uživatelé sociálních sítí mohou být nabádáni k poskytnutí svých **identifikačních údajů, rodných čísel, detailů o zaměstnání** apod. Přestože většina lidí by tyto údaje možná neposlala ani e-mailem, tak na sociálních sítích tito uživatelé citlivé informace v rámci svého profilu sdílejí. Tato data mohou být poté zneužita hackery. Například v březnu 2018 vyšlo najevo, že ze sociální sítě Facebook unikly osobní data více než 87 miliónů uživatelů,
- **reputace a právní odpovědnost** představuje problém v případě, že např. zaměstnanec veřejně komentuje kroky svého zaměstnavatele na sociální síti, což může být příčinou snížení reputace celé firmy. Společnost může být za své zaměstnance také právně odpovědná v případě, že se zaměstnanci z pracovního počítače připojují ke stránkám s citlivým nebo nelegálním obsahem. [18]

Velké množství společností v současnosti řeší dilema, jestli povolit nebo zakázat přístup zaměstnanců k sociálním sítím. Neexistuje pro to žádné univerzální doporučení. Společnosti vědí, že se musí přizpůsobovat nejnovějším trendům, ale zároveň mají obavy ze zmíněných problémů, které považují za vážné. Pro podniky tak existují **tři možnosti**, jak s přístupem k sociálním sítím naložit. Mezi tyto možnosti patří **úplný zákaz**, nastavení **omezeného přístupu** anebo **neomezený přístup**. [18]

Úplný zákaz sociálních sítí je nutný zejména u některých typů organizací, jako jsou např. banky nebo státní podniky. Varianta neomezeného přístupu je pro většinu podniků nemyslitelná, a tak se jako nejvíce reálnou variantou jeví možnost omezeného přístupu.

Každá společnost by měla mít v dnešní době patřičná zabezpečení, která obsahují aktualizovaný software, software pro monitoring využívání internetu a sociálních stránek v podniku. V případě, že se společnost rozhodne svým zaměstnancům povolit přístup k sociálním sítím, měla by brát v úvahu několik doporučení. Prvním z nich je zavedení omezeného přístupu. Podnik tak poskytne zaměstnancům určitou volnost a může přístup k sociálním sítím povolit

např. během obědové pauzy, před anebo po pracovní době. Pomocí softwaru pro filtrování webového přístupu mohou administrátoři zavést časově omezený přístup k těmto nebo jiným stránkám. [18]

Druhým doporučením je vzdělávání a školení zaměstnanců, jelikož mnozí zaměstnanci si možná ani nejsou vědomi toho, jaké bezpečnostní hrozby mohou způsobit svými aktivitami během používání sociálních sítí. Z těchto důvodů je vhodné zaměstnancům srozumitelně vysvětlit, co se může stát, jestliže svůj počítač a celou podnikovou síť nechají napadnout škodlivým kódem. [18]

Posledním doporučením je definovat politiku bezpečnosti při využívání internetu, se kterou by se měli všichni zaměstnanci společnosti seznámit. Jedná se o politiku, která se týká využívání internetu, přístupu k sociálním sítím a aktivit povolených v průběhu pracovní doby. Monitorování veškerých webových aktivit je velmi důležité a zaměstnanci by měli být informováni, že všechny jejich aktivity jsou zaznamenávány, a že nerespektování předepsaných pokynů může v kritických případech znamenat i propuštění ze zaměstnání. [18]

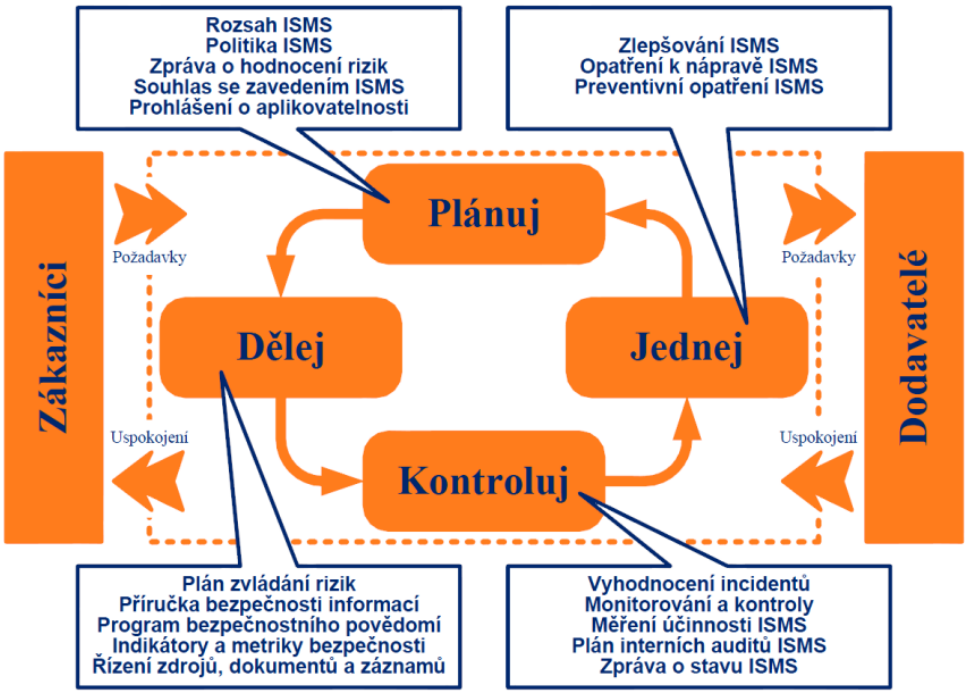
4.3 Systémy řízení bezpečnosti informací

Bezpečnost informací je v dnešní době důležitou součástí každodenního řízení a vnitřní kultury jakékoliv organizace. Pro cílené a účelné rozvíjení řízení bezpečnosti informací je nutné tento prvek řízení vnímat jako **systém řízení bezpečnosti informací**. Bezpečnost informačního systému představuje soubor opatření k zabezpečení provozu informačního systému dle stanovených zásad a pravidel k ochraně jejich dat. [11,17]

„*Systém řízení bezpečnosti informací lze charakterizovat jako procesní přístup pro vybudování, zavedení provozování, monitorování, udržování a zlepšování efektivnosti a bezpečnosti v organizaci*.“ [11]

4.3.1 Model PDCA

Model PDCA (Plánuj, Dělej, Kontroluj, Jednej) na jehož základě je založen systém řízení bezpečnosti informací. Může být aplikován na všechny procesy ISMS a znázorňuje veškeré principy pro řízení bezpečnosti informačních systémů a sítí. Jeho ilustrace je uvedena na následujícím obrázku. [11]



Obr. 2. Model PDCA [19]

Zjednodušeně by se dalo říci, že v první etapě je důležité daný systém správně naplánovat, druhá fáze představuje prosazení naplánovaného, ve třetí etapě je nutné dělat pravidelné kontroly a vyhodnocovat je. V poslední čtvrté fázi je potřeba celý systém zlepšovat a zkvalitňovat. [11]

4.4 Bezpečnost počítačových systémů

Počítačový systém je soubor **hardwaru, softwaru, záznamových médií, dat a personálu**, který organizace využívá ke správě svých informací.

4.4.1 Principy bezpečnosti počítačových systémů

Podle Požára [17] je základním principem informační bezpečnosti a ochrany informačních systémů skutečnost, že jakákoli informace a její ochrana má svou cenu.

Důležitý je **princip nejsnazšího průniku**, který vyjadřuje jednání a myšlení útočníka. Pachatel využívá nejjednodušší způsob průniku pro dosažení výhody a zisku, proto by s tím měl každý odborník na informační bezpečnost počítat. Ve většině případů útočník hledá nejslabší místo a čas pro napadení informačního systému, aby mohl získat citlivá data a informace. Používá k tomu různé metody a postupy, které se snaží maskovat tak, aby nedošlo k jeho odhalení dřív, než stačí informace získat. [17]

Mezi další princip bezpečnosti počítačových systémů patří **princip časové závislosti**. Z kterého vyplývá, že ochrana a zabezpečení objektů by měla trvat pouze do doby, než ztratí svoji hodnotu. [17]

4.4.2 Hrozby v počítačových systémech

Podle Požára [17] jsou chyby informačních systémů obvykle způsobeny nerespektováním základních pravidel při práci s daty a informacemi. To může být zdrojem hrozeb a nebezpečí. Mezi tyto hrozby patří zejména **přerušení, zachycení, modifikace a fabrikace**:

- **přerušením** se má na mysli, že dojde ke ztrátě části systému nebo je tato část nedosažitelná,
- **zachycení** představuje situaci, kdy neoprávněný subjekt získá přístup k určitému objektu daného systému a pachatel tak zachytí a získá citlivé informace,
- **modifikace** naopak znamená, že neoprávněný subjekt s úmyslem pozmění nějaká data a informace nebo rovnou i celé části systému,
- **fabrikace** je neoprávněné vytvoření nového falešného objektu, o kterém uživatel neví, že existuje a útočník pak může narušovat bezpečnost informačního systému. [17]

S takovými hrozbami souvisí i místa zranitelnosti počítačových systémů. Především se jedná o místa zranitelnosti jako je **utajení, integrita a dosažitelnost**:

- **utajení** představuje vybrané objekty v počítačovém systému, které jsou zpřístupněny pouze určitým oprávněným subjektům. Utajená místa patří mezi nejčastější objekty, na které útočníci zaměřují svoji pozornost,
- **integrita** znamená, že jedině autorizované subjekty mohou provádět modifikaci vybraných objektů,
- **dosažitelnost** v počítačových systémech znamená, že určené objekty jsou přístupné oprávněným subjektům a uživatelům. [17]

4.4.3 Objekty bezpečnosti počítačových systémů

Objekty informační bezpečnosti je možné klasifikovat a dělit podle různých charakteristických znaků. Tyto znaky používané různými autory jsou však nejednotné, a proto je v této kapitole rozebráno jen obecné dělení. Mezi objekty informační bezpečnosti lze především zařadit **technické zařízení, programy, data, záznamová média, sítě a klíčové osoby**:

- **technická zařízení** mohou být odcizena, porušena, záměrně poškozena, zničena katastrofou apod.,
- **programy** představují pro útočníky častý terč. Přístup k různým typům programů by měl být jasně vymezen, aby se dalo předejít modifikaci programů nebo jejich odcizení,
- **data a informace o činnosti organizace** mají těžko vyčíslitelnou a obvykle i velmi vysokou hodnotu. Udržení citlivých dat v utajení je proto životně důležité,
- **záznamová média** představují především zálohu systému. Zálohovaný systém může být totiž obnoven během relativně krátké doby po bezpečnostním incidentu. Záznamová média mohou být i využívána k archivaci, kdy jsou data uložená na bezpečném místě po dobu **několika desítek let**. Tato data jsou obvykle určena pro pozdější využití,
- **sítě** jsou páteří celého informačního systému během přenosu, ukládání a výměny dat mezi danými subjekty a okolím. Zajišťují v podstatě přenos dat od zdroje k příjemci, a proto je velmi důležité zabezpečit jejich ochranu před nejrůznějšími typy útoků. K tomuto účelu se nejčastěji používá šifrování,
- **klíčoví lidé** jsou pro provoz celého systému nepostradatelní a obvykle mají rozsáhlé pravomoci. I když je počet těchto lidí v organizaci poměrně malý, dokáží systém velmi dobře udržovat. Vzhledem na rozsah pravomocí těchto osob je velmi důležitý jejich správný výběr, jelikož by mohlo dojít k vyzrazení informací o informačním systému organizace. [17]

4.4.4 Vybrané metody počítačové bezpečnosti

V této podkapitole jsou zmíněny vybrané metody počítačové bezpečnosti. Níže jsou popsány metody šifrování, softwarové kontroly, kontroly hardwaru, bezpečnostní politika, fyzická kontrola a efektivita informační bezpečnosti. [13,17]

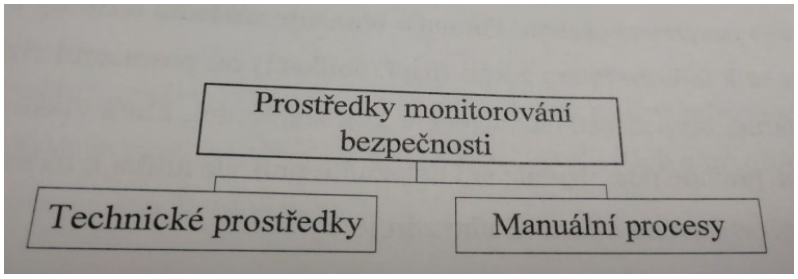
- **šifrováním** jsou data zakódována tak, aby je nebylo možné přečíst běžnými prostředky. Jestliže by došlo k odcizení takto zabezpečených dat, nedojde k jejich zneužití. Avšak neustálým šifrováním při zápisu a dešifrováním při čtení dochází ke snižování výkonu systému. Šifrování je možné využít i pro zajištění integrity dat nebo k vytvoření speciálních protokolů pro výměnu informací,
- **softwarové kontroly** přímo ovlivňují přístup uživatele k systému a je tedy nezbytně nutné, aby neznemožňovaly práci. Nástroje kontroly jsou např. **kryptografie** nebo

hardwarové součástky atp. Tyto kontroly dále zahrnují kontroly vývoje, operačního systému a interní programové kontroly,

- **kontroly hardwaru** zkoumají, zda technická zařízení, která jsou používána pro zpracování utajovaných informací či dat, vyhovují specifickým normám. Velmi důležité je jejich zabezpečení proti útokům a také zabezpečení samotného přístupu k nim,
- **bezpečnostní politika** je základním a nejjednodušším bezpečnostním opatřením. Je vhodným nástrojem pro seznámení uživatelů s postupy, které vedou k zajištění bezpečnosti ve vztahu k počítačům,
- **fyzická kontrola** zahrnuje zámky, stráže, záložní kopie dat a programů, náhradní technické vybavení i např. plánování umístění jednotlivých komponent systému. Fyzické kontroly jsou zpravidla velmi účinným, avšak často přehlíženým nástrojem bezpečnosti,
- **efektivita informační bezpečnosti** úzce souvisí s dodržováním a chápáním nastavených pravidel bezpečnosti. Velmi důležité je, aby tato pravidla byla jasná a srozumitelná pro všechny uživatele, což by mělo zamezit jejich případnému obcházení. Dále je třeba soustavně ověřovat, zda přijatá bezpečnostní opatření nejsou zastaralá a případně je aktualizovat. Způsoby ochrany musí být efektivní, výkonné, přiměřené a hlavně nesmí uživatelům překážet. [13,17]

4.5 Monitoring a audit informačního systému

Monitoring a audit informační bezpečnosti patří mezi důležité součásti procesu řízení informační bezpečnosti. Aby bylo možné provádět monitoring informačního systému, je nutné nadefinovat celkový rozsah monitoringu. Dále je potřeba stanovit a rozdělit odpovědnosti za monitoring. Prostředků pro monitorování bezpečnosti existuje velké množství a dělí se na dvě kategorie, které jsou uvedeny na následujícím obrázku.



Obr. 3. Rozdělení prostředků monitoringu bezpečnosti [13]

4.5.1 Technické prostředky

Technické prostředky jsou z velké části obsaženy již v operačním systému, pro jiné je nutný speciální nástroj. Do kategorie technických prostředků podle Jaška [13] patří:

- přihlášení a odhlášení uživatele,
- neautorizované pokusy o přihlášení do systému,
- záznam události, při které byla provedena specifická aktivita,
- záznam události, při které byl využit specifický datový zdroj,
- využití výkonných nástrojů operačního systému,
- záznam rizikových událostí, které jsou specifické pro daný systém,
- pokus o neautorizované využití služby systému.

4.5.2 Manuální prostředky

Kategorie manuálních prostředků zahrnuje procesy vyhodnocování záznamů z auditů včetně vyhodnocování bezpečnostních incidentů. Zde patří:

- **Balanced scorecad** je nepřímá metoda monitorování bezpečnosti, která je využívána některými organizacemi. Její základ tvoří dobře navržený formulář, jenž je pravidelně vyplňován vlastníkem informačního zdroje či prověřenou osobou,
- **penetrační testy** slouží k odhalování bezpečnostních slabin. Prostřednictvím těchto testů, je simulován přístup neoprávněného uživatele zvenku nebo zevnitř organizace. [13]

4.5.3 Informační audit

Prostřednictvím informačního auditu jsou identifikovány informace, které jsou nezbytné pro řízení organizace. Dále je prověřováno, zda nedochází k duplicitě zdrojů v poskytování informací nebo jejich absenci. V současnosti není určený žádný standard, podle kterého by měl být informační audit prováděn. Avšak existují doporučené postupy a metody, na které je při jeho realizaci brát zřetel. Obsahem informačního auditu je:

- **vymezení** zejména kritických informačních potřeb a stanovení jejich důležitosti,
- **identifikace** zdrojů a služeb, jaké potřeby uspokojují a kdo je využívá,
- **mapování** informačních toků uvnitř organizace,
- **analýza** duplicity a absence informačních zdrojů,
- **vymezení oblastí**, které potřebují změny informační podpory. [4]

Výstupy z informačního auditu mohou pomoci lépe pochopit, jak je v dané organizaci s informacemi nakládáno a upozornit na případné nedostatky. Součástí výsledků auditu jsou i návrhy a doporučení ke zlepšení. Implementace těchto poznatků by měla zlepšit celkovou informační podporu v organizaci i efektivnost vynaložených finančních prostředků na tuto podporu. [4]

4.5.4 Audit informačního systému

Cílem auditu informačního systému je zhodnotit, jestli je systém ve shodě se stanovenými požadavky. Audit informačního systému, lze chápat jako analýzu informačního systému, kterou provádí nezávislá autorizovaná osoba nebo instituce, jež nemá přímou odpovědnost za funkce prověřovaného systému. Audit je možné si představit taktéž jako záznam událostí a činností důležitých z hlediska bezpečnosti informačního systému. Kromě státních a národních standardizačních institutů se problematice norem auditu věnuje Mezinárodní organizace pro standardizaci (ISO) a další profesně zaměřené organizace jako například ISACA. [11]

4.5.5 Bezpečnostní audit

Bezpečnostní audit slouží pro zjištění aktuálního stavu bezpečnosti informačního systému. Cílem auditu je upozornit na zranitelnosti systému, které by ho mohly ohrozit, na nedodržování bezpečnostních opatření a na nedostatečnost zabezpečení informačního systému. [12,20]

Bezpečnostní audit se skládá ze **dvou částí**. **První část** je zaměřena na formální posouzení veškerých materiálů bezpečnostní politiky organizace. V této části se prověřuje, zda jsou nastaveny definice hrozeb a cíle politiky správně, a jestli navrhovaná bezpečnostní opatření dostatečně pokrývají všechny části informačního systému. [12,20]

Druhá část bezpečnostního auditu zahrnuje kontrolu správnosti implementace stanovené bezpečnostní politiky. Ověřuje se, zda jsou všechny části systému správným způsobem nastaveny a jestli jsou aplikovány odpovídající bezpečnostní záplaty, aktuální verze produktů apod. Na základě výstupů z auditu pak mohou být realizována opatření pro zlepšení stavu auditovaného systému. [12,20]

5 METODY PRO VÝZKUM

V následující kapitole jsou popsány vybrané metody pro výzkum, realizovaný v praktické části diplomové práce.

5.1 SWOT analýza

SWOT analýza je univerzální metoda pro zhodnocení vnitřních a vnějších faktorů, které ovlivňují úspěšnost organizace nebo určitého záměru. Nejčastěji se SWOT analýza využívá v rámci strategického řízení. SWOT analýzu jsem v praktické části aplikoval pro zhodnocení současného stavu informačního managementu podniku. [21]

5.2 Analýza

Analýza je proces, během kterého dochází k dekompozici poznávaného objektu na jeho jednotlivé části a zjišťují se vzájemné souvislosti mezi nimi. Tato metoda umožňuje poznání důležitých znaků zkoumaného jevu a odkrytí jeho struktury a vztahů. Analýzu jsem použil v praktické části práce pro posouzení rizik z hlediska informační bezpečnosti podniku. [22]

5.3 Syntéza

Syntéza představuje opak analýzy, to znamená, že se jedná o sjednocování nějakého předmětu, jevu nebo procesu z jeho základních prvků na nějaký celek. Syntéza většinou doplňuje analýzu a umožňuje tím poznání předmětu v jeho úplnosti. Syntéza představuje proces, při kterém se hledá spojováním částí v celek taková struktura, která by měla předem požadované chování. Syntéza může být tedy i hledáním nejvhodnější varianty, které lze dosáhnout kombinací jednotlivých prvků a jejich vlastností. Metodu syntézy jsem použil v teoretické části práce na propojení literatury s informacemi. [23]

5.4 Brainstorming

Brainstorming je skupinovou kreativní technikou, jejímž cílem je generovat co nejvíce nápadů na dané téma. Oblasti využití této metody jsou v podstatě neomezené. Metodu brainstormingu jsem použil při tvorbě analýz v praktické části práce. [24]

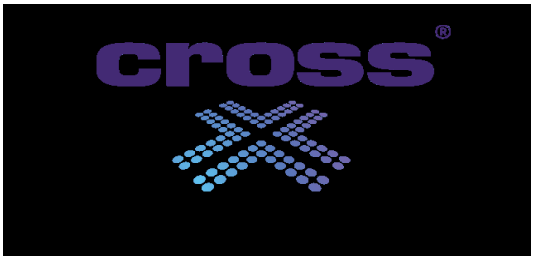
II. PRAKTICKÁ ČÁST

6 INFORMAČNÍ MANAGEMENT VE VYBRANÉ SPOLEČNOSTI

V následující části diplomové práce je detailně rozebrán současný stav informačního managementu ve vybrané společnosti a s pomocí SWOT analýzy jsou vyhodnoceny silné a slabé stránky, hrozby a příležitosti v oblasti informačního managementu.

6.1 Představení vybrané společnosti – Cross Zlín, a.s.

Společnost Cross Zlín, a.s. (dále jen Cross Zlín) byla založena v roce 1994 ve Zlíně. Vyrábí a dodává dopravní technologie do celého světa a podílí se na technologických projektech pro chytrá města. Hlavní sídlo společnosti je ve Zlíně, kde probíhá i veškerá výroba a technologický vývoj. V České republice má firma ještě dvě pobočky, které jsou zaměřeny na servis dopravních technologií. Jedna z těchto poboček je ve Velkém Meziříčí a druhá v Praze. Kromě poboček v České republice má společnost tři pobočky i v zahraničí. Jsou to pobočky v Rusku, Brazílii a Chorvatsku. Firma se neustále rozrůstá a v současnosti má přes 120 zaměstnanců. Na prestižním veletrhu dopravních technologií v Amsterdamu získala společnost v roce 2016 a 2018 významná ocenění. Logo společnosti je představeno na následujícím obrázku.

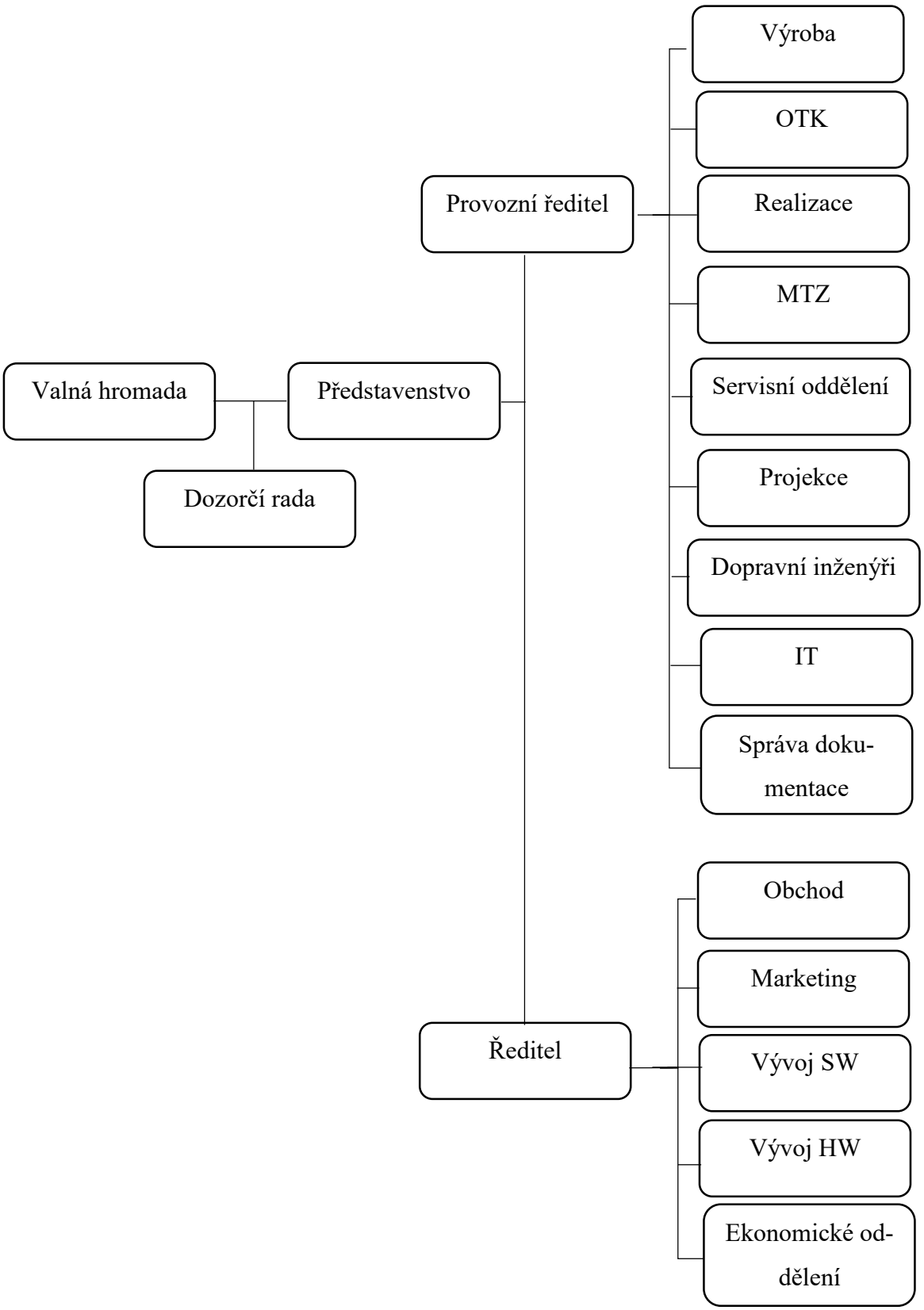


Obr. 4. Logo společnosti [25]

Produktové portfolio společnosti:

- systémy řízení dopravy,
- sčítání a klasifikace dopravy,
- dojezdové časy,
- vážení za jízdy,
- silniční meteorologie,
- parkovací systémy,
- detekce dopravních přestupků,
- Invipo platforma.

6.1.1 Organizační struktura společnosti



Obr. 5. Organizační struktura společnosti [vlastní zpracování]

7 SOUČASNÝ STAV INFORMAČNÍHO MANAGEMENTU VE SPOLEČNOSTI CROSS ZLÍN

Tato kapitola popisuje současný stav informačního managementu společnosti. Na základě těchto informací je dále provedena SWOT analýza informačního managementu. Z výsledků analýzy jsou navržena patřičná nápravná opatření a doporučení pro zlepšení fungování informačního managementu společnosti.

7.1 Informační manažer podniku

Ve společnosti Cross Zlín je vytvořena pozice informačního manažera, což je z hlediska fungování informačního managementu jeden z klíčových faktorů. Informační manažer má v podniku rozsáhlé pravomoci, které jsou uvedeny zde:

- zajišťuje provoz sítě, tj. propojení jednotlivých stanic,
- schvaluje připojení každého nového zařízení do sítě a schvaluje změny v konfiguraci či umístění koncových zařízení nebo podřízených sítí,
- zodpovídá za konfiguraci síťových prvků, má právo určovat minimální parametry připojovaného zařízení,
- má právo, za účelem optimalizace chodu, monitorovat provoz koncových zařízení připojených k síti a podřízeným sítím a v případě porušování zásad ze strany uživatele je povinen tomu zabránit a vyvodit z toho důsledky,
- má právo stanovit harmonogram pravidelných výluk sítě. S tímto harmonogramem je povinen seznámit uživatele sítě, výluky sítě probíhají přednostně mimo pracovní dobu tak, aby byl minimalizován jejich vliv na práci uživatelů,
- má právo rozesílat zprávy všem uživatelům sítě pro mimořádně důležitá a neodkladná sdělení,
- má odpovědnost za vypracování informační strategie podniku a povinnost ji pravidelně aktualizovat,
- má povinnost provádět informační audit společnosti. [25]

7.2 Dokumenty informačního managementu

Tato podkapitola se věnuje vypracovaným dokumentům v oblasti informačního managementu společnosti Cross Zlín. V rámci hodnocení současného stavu bylo zjištěno, že podnik má vypracovanou bezpečnostní politiku a informační strategii. Dále existují směrnice v oblasti ICT, které definují povinnosti správců a uživatelů informačních technologií pro zajištění dostatečné informační a datové bezpečnosti.

7.2.1 Bezpečnostní politika

Cílem je určit směr a vyjádřit podporu bezpečnosti informací ze strany vedení v souladu s požadavky organizace, příslušnými zákony a směrnicemi. Firma má vypracovaný dokument bezpečnostní politiky informací. Přezkoumávání bezpečnostní politiky probíhá z hlediska aplikovatelnosti a kontinuity. Lhůta pro přezkoumání nepřesahuje 12 měsíců. [25]

7.2.2 Informační strategie

Jak již bylo zmíněno výše, odpovědnost za vypracování informační strategie nese informační manažer společnosti. Informační strategie představuje dlouhodobý plán vytvořený za účelem dosažení cílů podniku v oblasti nakládání s informacemi a daty. Společnost Cross Zlín si je vědoma, že informační strategie je jedním ze základních dokumentů informačního managementu, a proto tento dokument vypracovaný má. Poslední aktualizace proběhla v polovině roku 2017. [25]

7.2.3 Směrnice ICT

Směrnice ICT jsou vypracovány pro správu a používání informačních a komunikačních technologií v podniku. Z pohledu správy směrnice definují povinnosti všech pracovníků, kteří provádí správu IT. Pro uživatele směrnice stanovují podmínky pro provoz a obsluhu všech zařízení, která mají nebo mohou mít vliv na bezpečnost informací důležitých pro činnost společnosti. Mezi tato zařízení patří počítače a jejich příslušenství, podpůrná zařízení (sítě, záložní zdroje, apod.), zařízení a vybavení pracovišť, technická i organizační zařízení omezující přístup osob na jednotlivá pracoviště, přístup do prostor využívaných společnosti a přístup k informacím, které se ve společnosti vyskytují. Směrnice jsou uloženy v intranetu společnosti, kam mají přístup všichni zaměstnanci a mohou se tak s nimi seznámit. [25]

7.3 Sdílení firemních informací

Pro sdílení firemních informací existují sdílená úložiště, která mají určené své správce. Zodpovědnou osobu za dodržování pravidel pro tyto sdílená úložiště představuje hlavní správce.

Sdílené úložiště je společný diskový prostor, ke kterému mají v různých úrovních přístup všichni zaměstnanci. Tento prostor je rozdělen na více sdílených disků.

- sdílený disk je část sdíleného úložiště, které je označováno jedním písmenem (např. Z:) a které je uživateli zpřístupněno po přihlášení do operačního systému ve firemní síti.

Správce sdíleného disku je osoba jmenovaná hlavním správcem, která zodpovídá za dohlížení a plnění pravidel pro společný diskový prostor. Správce je jmenován v rámci každého oddělení.

Hlavní správce je osoba jmenovaná vedením společnosti, která zodpovídá za celkové dodržování pravidel pro sdílené úložiště a zároveň koordinuje jednotlivé správce. [25]

7.3.1 Sdílené disky

Sdílené disky vytváří hlavní správce a ve spolupráci s příslušným správce sdíleného disku nastavuje oprávnění pro přístup vybraných zaměstnanců. Zaměstnanci mají přístup k jednotlivým sdíleným diskům na základě pracovního zařazení nebo aktuální pracovní role. Informace o zpřístupnění disků a pokyny související s obsahem zveřejní příslušným zaměstnancům jejich nadřízený nebo správce sdíleného disku.

Pokud zaměstnanec zjistí, že na svém počítači z nějakého důvodu nemá dostupný sdílený disk, který potřebuje pro ukládání dat v rámci svého pracovního zařazení, je povinen tuto situaci řešit se svým nadřízeným nebo správcem sdíleného disku. Na sdílené disky je zakázáno ukládat soukromá data zaměstnanců, která nesouvisejí s výkonem pracovní činnosti. [25]

Povinnosti správce sdíleného disku:

- dohlížet na ukládání a sdílení souborů na přidělených discích,
- odstraňovat duplicity a zamezovat sdílení nepodstatných či nekompletních dat,
- být příkladem pro své kolegy a vést je k pořádku a důslednosti,
- sdílení informací o zakázkách a produktech. [25]

7.3.2 Zákaznický disk Z

Disk Z slouží pro ukládání společných dat k zakázkám. Předepsaná adresářová struktura disku je popsána v metodickém pokynu pro práci s diskem Z, který je uvedený v příloze P II.

Každý zaměstnanec společnosti má povinnost:

- **ukládat** veškeré soubory k zakázkám na sdílený disk Z. Soubory se hlavně rozumí projektové či vývojové dokumenty, podklady k zadání zakázky od zákazníka, fotografie, výrobní dokumenty, dokumenty z instalace a všechna další data, která vzniknou v rámci realizace zakázky,
- **aktualizovat** veškeré soubory k zakázkám na sdíleném disku Z, pokud zaměstnanec provedl změnu těchto souborů mimo disk Z,
- **dodržovat** základní adresářovou strukturu popsanou v souboru,
- **konzultovat** v případě potřeby sdílení informací se správcem sdílených disků. [25]

7.3.3 Produktový disk P

Disk P slouží pro ukládání společných dat k produktům. Předepsaná adresářová struktura disku je popsána v metodickém pokynu pro práci s diskem P, který je popsán v příloze P I.

Každý zaměstnanec společnosti má povinnost:

- **ukládat** veškeré soubory k produktům na sdílený disk P. Soubory se hlavně rozumí technická a obchodní dokumentace, SW ke stažení, materiály od konkurence, fotodokumentace a popis standardů,
- **aktualizovat** veškeré soubory k zakázkám na sdíleném disku P, pokud zaměstnanec provedl změnu těchto souborů mimo disk P,
- **dodržovat** základní adresářovou strukturu popsanou v souboru,
- **konzultovat** v případě potřeby sdílení informací se správcem sdílených disků. [25]

7.3.4 Ostatní disky

Kromě výše uvedených sdílených disků Z: a P: existují další sdílené disky, které jsou určeny pro sdílení dat v rámci jednotlivých organizačních složek firmy nebo pro sdílení dat vybraných skupin zaměstnanců. Přesná struktura složek a ukládaných dat u těchto disků není předepsána a zodpovídá za ni vybraný zaměstnanec (např. vedoucí oddělení) ve spolupráci s

příslušným správcem sdílených disků, který odpovídajícím způsobem informuje uživatele daného sdíleného disku. [25]

Každý zaměstnanec společnosti má povinnost:

- **ukládat** data na ostatní sdílené disky dle pokynů svého nadřízeného nebo správce sdíleného disku,
- **aktualizovat** soubory v případě, kdy zaměstnanec provedl změnu souborů mimo příslušný sdílený disk,
- **konzultovat** v případě potřeby sdílení informací se správcem sdíleného disku. [25]

7.4 Zásady práce s daty na elektronických nosičích

Ve společnosti Cross Zlín jsou jednotlivé počítače a jejich příslušenství propojeny v síti. Tato síť umožňuje jednoduchou komunikaci mezi zaměstnanci a usnadňuje sdílení společných záznamů.

7.4.1 Správce sítě

Odpovědnost za provoz počítačové sítě nese jmenovaný pracovník - správce sítě (vedoucí oddělení IT). Správce sítě na pravidelných schůzkách informuje o změnách ostatní uživatele sítě. Odpovědnost za přidělení práv uživatelům má správce sítě, který odpovídá za funkčnost počítačové sítě, samostatných počítačů a dále za archivaci a ochranu dat. Se správcem sítě v této problematice spolupracují ostatní úseky, které jsou uživateli sítě. [25]

7.4.2 Přístupová práva

Přístupová práva jednotlivých uživatelů jsou zdrojem jednoznačné identifikace autora záznamů a změn uložených dat. Práva přístupu jsou přidělována na základě příslušnosti uživatele k úseku a jeho požadavkům na využití výpočetní techniky. Obsahem přístupových práv je uživatelské jméno, které je jedinečné v rámci organizace a příslušné heslo uživatele. Hesla je oprávněn měnit pouze správce sítě. Aktuální hesla jsou uložena u správce sítě a u ředitele. Zaměstnanci jsou při obdržení hesla formou ústního sdělení upozorněni na zásady bezpečného nakládání s heslem. [25]

7.4.3 Zálohování a ochrana dat

Každý pracovník je zodpovědný za pravidelné zálohování svých pracovních dat. Pracovními daty se rozumí všechny informace vytvořené pracovníkem, nutné k uchování do budoucnosti, zejména zdrojové kódy všech programů, texty smluv, dopisů a záznamů o jednáních, rozpočty a jiné obchodní dokumenty, dokumentované informace k výrobkům, technické i obchodní atd. Není nutno zálohovat programy, jež lze kdykoliv obnovit z instalačních medií.

Každý pracovník zálohuje v daném časovém intervalu nově vytvořené nebo pozměněné dokumenty na server SBSCROSS. Tento interval je pro pracovníky vývoje **1 x denně**, pro ostatní pracovníky **2x týdně**.

Server je automaticky zálohován **2x týdně** na záložní server (každé úterý a čtvrtek pošta, každou středu a pátek soubory. Předepsaný způsob a intervaly zálohování jsou minimální, každý pracovník může provádět zálohy častěji podle vlastního uvážení. Vedoucí vývoje provede **2x ročně** kontrolu zálohování dat, výsledek vyhodnotí a předá řediteli.

Každý pracovník má instalován antivirový program ESET neustále ve stavu rezidentní ochrany. Pravidelné aktualizace zajišťuje správce počítačové sítě. Správce počítačové sítě zajišťuje antivirovou ochranu serverů s automatickým stahováním nejnovějších antivirových informací od externího poskytovatele.

Správce sítě zabezpečí při každé změně konfigurace serveru zálohování aktuální konfigurace na magnetický pásek a uložení do trezoru společnosti. Správce sítě vede v elektronické podobě seznam PC a jejich TCP IP adres. [25]

7.4.4 Obnova dat

Při poruše, ztrátě nebo zavirování dat uživatelé neprodleně informují správce sítě. Správce sítě nejprve prověří, zda síť nebyla napadena viry a poté přistoupí k obnově dat. Data jsou přednostně obnovována ze serveru SBSCROSS, poté z nejnovější zálohy ze záložního serveru a jen v případě nemožnosti použití nejnovějších záloh se použije starší záloha ze záložního serveru. [25]

7.5 Správa ICT společnosti

Systém IT se skládá z HW, SW a dat uložených na diskových polích, pevných discích serverů, pracovních stanic a zálohovacích médiích. Umístění výpočetní infrastruktury je na

dvou místech. Prvním z nich je serverovna firmy Cross Zlín (v sídle firmy) a druhým místem je datacentrum, které je umístěno mimo budovu společnosti. [25]

Tab. 1. Složení systému IT [vlastní zpracování]

Hardware systému	Software systému	Data
servery	virtualizační software	data informačních systémů
aktivní prvky sítě	databázové servery	data sdílených disků
záložní zdroje napájení - UPS	aplikační software	data jednotlivých uživatelů
strukturovaná kabeláž		
pracovní stanice		
periferní zařízení		
mobilní zařízení		

7.5.1 Administrace serverů

Správce výpočetní techniky provádí v průběhu pracovního týdne denně kontrolu virtuální infrastruktury a serverů jak umístěných v serverovně firmy, tak v datacentru. Ve výjimečných případech musí být infrastruktura nebo server zkontrolována minimálně **1x za týden.**

Všechny důležité servery, služby a další hardware (např. tiskárny), připojené do sítě, jsou nepřetržitě monitorované ze dvou nezávislých míst (serverovna a datacentrum). Informace o výpadcích služeb jsou zasílány jak na obecnou e-mailovou adresu, tak v podobě SMS na telefony správců. Monitoring využívá záložní připojení k internetu, takže je schopen detekovat i výpadky primárního internetového připojení. [25]

7.5.2 Virtualizační software

Správce provádí kontrolu a analýzu stavu virtualizační infrastruktury (jak přímo uložené v serverovně firmy, tak ve vzdáleném datacentru), zejména pak funkcí pro zajištění vysoké dostupnosti, propojení fyzických serverů s diskovými poli. Virtualizační software automaticky zasílá vybrané informace o chybových stavech na vybrané uživatele v podobě e-mailových zpráv. V případě zjištění problémů správce provádí jejich neprodlené odstranění. O provedených akcích provede zápis do administrátorského deníku. [25]

7.5.3 Servery na platformě Microsoft

Správce provádí analýzu veškerých nestandardních procesů, které na serverech nastanou. Pokud k nestandardnímu procesu dojde (chybová zpráva v protokolu událostí) musí být odstraněna jeho příčina v co nejkratším termínu. Po odstranění příčin je nutné provést kontrolu

funkčnosti v součinnosti s uživateli. Správce provede zápis do administrátorského deníku. [25]

7.5.4 Aktualizace systému

Aktualizaci systému smí provádět pouze vybraný správce. Kontroluje pravidelně dostupnost aktualizací a provádí jejich instalaci. U vybraných serverů, které musejí běžet v režimu 24x7 se aktualizace aplikují ručně v dohodnutých intervalech. U ostatních infrastrukturních serverů je nastavena automatická instalace aktualizací tak, aby nekolidovala s běžným denním využíváním serverů. [25]

7.5.5 Přístupová práva

Přístupová práva jsou řízena v rámci domény Active Directory. Správce přiděluje práva na základě požadavku uživatele po vyhodnocení oprávněnosti (schválení nadřízeného pracovníka uživatele, který o přístupová práva požádal). Vkládat nové uživatele má právo pouze správce, popřípadě osoba k tomu pověřená. Autorizace je daná nastavenými pravidly. Správce při zakládání účtu vygeneruje heslo, které je sděleno uživateli s tím, že uživatel musí toto heslo při prvním přihlášení změnit. Přístupová práva mohou být přidělována k tomuto uživatelskému účtu, popřípadě udělována počítači. V případě požadavku na zablokování účtu, musí správce neprodleně tento účet zablokovat. Využít práva podat požadavek na zablokování účtu mají také členové bezpečnostního fóra, nadřízený uživatele i uživatel. [24]

7.5.6 Certifikáty

V případě, kdy uživatel pro práci potřebuje vzdálený přístup do firmy, je mu vygenerován uživatelský certifikát, který se používá pro ověřování přístupu při připojení do VPN. V případě požadavku na odvolání certifikátu (například v případě krádeže firemního počítače) správce neprodleně provede odvolání certifikátu a další nutné akce. Uživatel pak dostává pro obnovení přístupu nově vygenerovaný certifikát. [25]

7.5.7 Zálohování dat

V rámci firmy probíhá několik procesů zálohování dat. Tyto procesy jsou popsány v následujících podkapitolách

7.5.7.1 Zálohování uživatelských dat

Zálohování dat přímo na počítačích uživatelů se neprovádí. Uživatelé mají k dispozici vlastní sdílený disk, který je pravidelně zálohován **1x týdně** v rámci zálohování dat sdílených disků serverů. [25]

7.5.7.2 Zálohování dat sdílených disků serverů

Zálohování dat sdílených disků serverů se provádí denně a provádí se na vyhrazený zálohovací server v podobě archivů chráněných heslem. Jednou týdně jsou data ze zálohovacího serveru replikována na externí disk. Externí disky jsou k dispozici dva, vyměňují se každý týden a nepoužitý disk je uložen v trezoru. [25]

7.5.7.3 Zálohování na úrovni serverů

Zálohování na úrovni serverů probíhá denně. Vytváří se diskový obraz celého serveru, který je uložen na vyhrazeném zálohovacím serveru. Tyto zálohy jsou denně replikovány na vyhrazený zálohovací server v datacentru. [25]

7.5.7.4 Zálohování na úrovni virtuálních serverů

Zálohování na úrovni virtuálních serverů probíhá průběžně před každou změnou konfigurace serveru tak, aby bylo možné v případě potřeby přejít zpět k původnímu nastavení serveru. Zálohování probíhá na vyhrazený zálohovací server v rámci firmy. [25]

7.5.7.5 Zálohování produkčních dat v datacentru

Zálohování produkčních dat v datacentru probíhá dle požadavků zákazníků, kterým se data poskytují, buď na vyhrazený zálohovací server přímo v datacentru, nebo na vyhrazený zálohovací server v rámci firmy. [25]

7.5.8 Elektronická pošta

Firemní elektronická pošta je řešena interním Exchange serverem ve verzi 2010, k jehož nastavení má přístup pouze správce. Součástí Exchange serveru je antivirový modul, který provádí automaticky kontrolu veškeré příchozí pošty a současně i kontrolu již uložených zpráv. Součástí Exchange serveru je také antispamové řešení, které provádí filtrování příchozích nevyžádaných zpráv. Nevyžádané zprávy jsou ukládány do vybrané veřejné složky a uživatelé mají možnost ovlivnit klasifikaci špatně zařazených zpráv. [25]

7.5.9 Firewall

V rámci firemní infrastruktury existují dva firewally. Jeden je umístěn v sídle firmy a zajišťuje síťové funkce a přístup pro firemní uživatele, druhý je umístěn v datacentru a zajišťuje síťové funkce a přístup pro zákazníky. [25]

7.5.9.1 Firewall v rámci firmy

Za firewall je považován router, který je umístěn v uzamčené serverovně. Povolení přístupu pro příchozí a odchozí provoz provádí pouze správce na základě požadavku uživatele se schválením nadřízeného pracovníka uživatele. V odůvodněných případech povolení přístupu schvaluje bezpečnostní fórum.

Firewall složí k řízení přístupu mezi jednotlivými podsítěmi, mezi kterými jsou definované pravidla pro přístup, a k řízení přístupu uživatelů a serverů do a z internetu. Správce provádí denní kontrolu pravidel firewallu a kontrolu logů se zřetelem na nepovolený provoz jak v rámci internetu, tak v rámci místních podsítí. [25]

7.5.9.2 Firewall v datacentru

Za firewall v datacentru je považován router, který je umístěn v zabezpečeném racku v datacentru. Povolení přístupu pro příchozí a odchozí provoz provádí pouze správce na základě požadavku zákazníků. V odůvodněných případech povolení přístupu schvaluje bezpečnostní fórum. Správce provádí denní kontrolu pravidel firewallu a kontrolu logů se zřetelem na nepovolený provoz jak v rámci internetu, tak v rámci místních podsítí. [25]

7.5.10 Administrace pracovních stanic

Uživatelé mají přidělena administrátorská práva ke své pracovní stanici, za kterou jsou plně odpovědní. Administrátorská oprávnění jsou přidělena všem uživatelům, kteří s danou pracovní stanicí pracují v případě, kdy se jedná o pracovní stanici, sdílenou mezi uživateli. HW konfiguraci pracovní stanice a její vybavení typem OS a aplikačního SW vybírá správce společně s uživatelem. Instalaci systému a aplikací provádí správce. Při likvidaci, prodeji či jiného umístění správce odstraní veškerá data z paměťových zařízení u pracovních stanic, na kterých by mohla být důvěrná data, a následně provede formátování HDD.

Aktualizace pracovních stanic se provádí automaticky a její nastavení je vnuceno počítačům v rámci zásad skupin domény Active Directory. [25]

7.5.11 Antivirová ochrana

Antivirová ochrana počítačová sítě je realizovaná systémem ESET včetně centrální konzole, kam jednotlivé počítače pravidelně předávají informace o aktuálním stavu antivirového softwaru. Správce provádí pravidelnou kontrolu událostí získaných od pracovních stanic uživatelů. V případě potřeby je možné spouštět vzdálenou automatickou kontrolu vybrané pracovní stanice případně změnu konfigurace antivirového softwaru na pracovní stanici. Uživatelé nemají přístup do konfigurace antivirového programu, která je chráněná heslem. [25]

7.5.12 Kontrola pasivních a aktivních prvků LAN

Fyzická kontrola aktivních a pasivních prvků není prováděna, pouze v případě nefunkčnosti daného zařízení správce zařídí opravu či výměnu zařízení. [25]

7.5.13 Správa vyměnitelných médií

Uživatelé mohou užívat vyměnitelná média (USB disk, DVD, CD, apod.). Jsou plně odpovědní za jejich obsah. Při likvidaci vyměnitelných médií je nutno toto zařízení fyzicky znehodnotit (mechanické poškození). [25]

7.5.14 Bezpečnostní incidenty v LAN

Provozní události jsou monitorovány jak monitorovacím systémem, tak správcem událostí OS Windows případně protokolem událostí systému Linux. Tyto události mohou být příčinou bezpečnostního incidentu. Poté tyto záznamy slouží jako zdroje pro specifikaci příčiny incidentu. Dalším zdrojem jsou informace od uživatelů.

Správce má za povinnost v případě incidentu provést záznam do administrátorského deníku. Následné řešení bezpečnostního incidentu probíhá dle směrnice Řízení neshod, nápravná a preventivní opatření. [25]

7.5.15 Automatická inventarizace hardwaru a softwaru

V rámci firmy a domény probíhá automatická inventarizace hardwaru a softwaru serverů a pracovních stanic. Inventarizace probíhá automaticky vždy při přihlášení uživatele. Výstupem inventarizace je kompletní seznam hardwarových komponent a softwaru, který je v okamžiku přihlášení na počítači k dispozici. Seznam je uchováván pro všechny servery i pracovní stanice v centrální databázi, která umožňuje vyhledávání a filtraci tak, aby bylo možné jednoduše hledat jak hardwarové komponenty, tak instalovaný software. Správce provádí

namátkové kontroly instalovaného softwaru na pracovních stanicích s ohledem na instalaci nelicencovaných verzí aplikací uživateli. [25]

7.5.16 Rozšiřování IT systému

Rozšiřování IT systému o nové technologie pro zpracování dat, jejich upgrade, navrhuje správce, zaměstnanci do jejichž kompetence spadá nakládání s těmito daty a členové bezpečnostního fóra s ohledem na bezpečnost a kapacitu zpracování dat. Správce zpracuje tyto návrhy, rozpracuje z hlediska požadavků na HW a bezpečnost dat.

Nároky na HW vybavenost musí odpovídat stavu systému, v případě požadavku na větší výkon HW zpracuje správce podklady pro bezpečnostní fórum a ředitele společnosti na uvolnění finančních zdrojů. Ředitel společnosti schvaluje uvolnění těchto zdrojů. [25]

Bezpečnost dat musí být u nových technologií na vyšší, nebo alespoň stejné úrovni jako je stávající stav:

- každý uživatel musí mít svůj přístupový účet s heslem, správce může řídit politiku bezpečnosti hesla,
- účet generuje správce, definuje práva a oprávnění přístupu, v případě potřeby zablokuje účet. [25]

7.5.16.1 Schválení rozšíření a změn systému IT

Bezpečnostní fórum projedná návrh nových technologií z hlediska bezpečnosti informací, požadavku na zdroje a schvaluje rozšíření systému. [25]

7.6 Intranet společnosti

Kromě sdílených disků využívá společnost Cross Zlín intranet, tzv. Sharepoint. Na tomto místě jsou ukládány firemní dokumenty, ke kterým by měli mít přístup všichni zaměstnanci společnosti a seznámit se s jejich obsahem. Přihlášení do intranetu provede uživatel zadáním svého přístupového hesla. Kromě ukládání společných dokumentů tento intranet slouží i k evidenci služebních odchodů a cest a také k evidenci dovolené. Veškerý obsah tohoto webu je uveden na následujícím obrázku.

Obr. 6. Obsah intranetu společnosti [25]

Jak už bylo zmíněno výše intranet společnosti, slouží i pro ukládání firemních dokumentů. Seznam těchto dokumentů je uvedený na obrázku níže.

Obr. 7. Seznam dokumentů v intranetu [25]

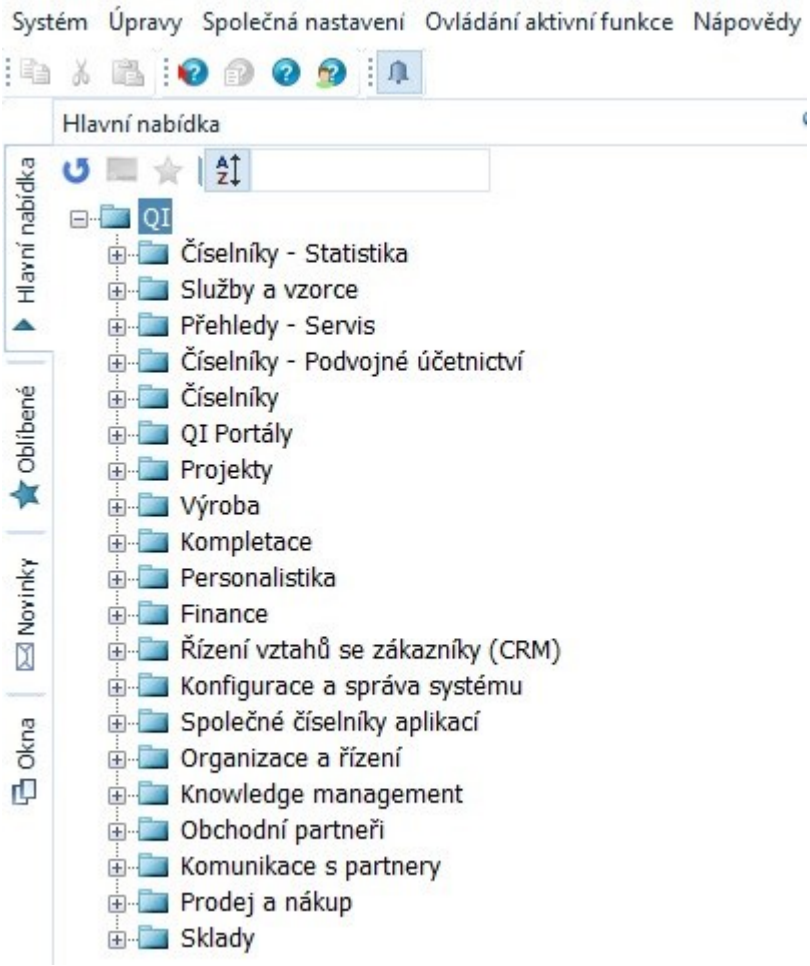
7.7 Informační systém QI

Společnost Cross Zlín používá informační systém QI od roku 2015. Tento nový informační systém spravuje externí společnost. Firma fungovala téměř 20 let bez podnikového informačního systému. Zavedení informačního systému mělo za cíle:

- nahradit co největší množství nesourodých a neprovázaných aplikací,
- zajistit provázanost dat mezi jednotlivými uživateli,

- provázat ekonomická data s klíčovými firemními procesy,
- potlačit komunikační problémy a problémy se sdílením informací na všech úrovních organizační struktury,
- odstranit paralelní a duplicitní aktivity napříč celou firmou,
- zavést centrální sklad a následně centrální nákup,
- poskytnout on-line přehled o firmě. [25]

Hlavní nabídka informačního systému s jednotlivými moduly je vidět na následujícím obrázku.



Obr. 8. Hlavní nabídka IS společnosti [25]

8 ZABEZPEČENÍ BUDOVY SPOLEČNOSTI

Budova společnosti Cross Zlín, a.s. je zabezpečena pomocí EZS a sestává se z jednotlivých čidel narušení prostoru, panelů pro ovládání uživateli a ostatních technických zařízení, nutných pro správnou činnost systému. Systém EZS slouží k ochraně bezpečnosti budovy mimo pracovní dobu a k detekci narušení budovy společnosti, a je napojen na pult centrální ochrany. Systém EZS mohou obsluhovat pouze oprávnění uživatelé, kteří mají přidělen kód pro přístup do budovy centrály a absolvovali školení o obsluze EZS. [25]

8.1.1 Zóny EZS

Systém EZS je rozdělen do 4 zón označených čísly 1-4. Zóny zahrnují následující prostory:

1. Celé první nadzemní podlaží budovy společnosti, příruční sklad v druhém nadzemním podlaží budovy společnosti s výjimkou společných prostor schodiště.

2. Celé druhé nadzemní podlaží budovy společnosti s výjimkou příručního skladu a společných prostor schodiště.

3. Celé třetí nadzemní podlaží budovy společnosti s výjimkou společných prostor schodiště.

4. Společné prostory schodiště, hlavní vchod a zádveří hlavního vchodu. [25]

V jednotlivých zónách jsou umístěny detektory pro snímání pohybu. Typ detektoru je uvedený na obrázku níže.

Obr. 9. Detektor pro snímání pohybu [25]

8.1.2 Přístupová oprávnění do zón EZS

Jednotliví uživatelé EZS mají oprávnění do všech zón EZS bez omezení, takže mohou provádět kódování a odkódování všech zón bez výjimek. Uživatel si tedy může dle potřeby odkódovat všechny zóny s ohledem na umístění technických prostředků, které bude při práci využívat (kávovar, tiskárny…). [25]

8.1.3 Příchod do budovy

Při příchodu uživatele do budovy společnosti je stav zakódování zón indikován LED diodami na panelech ovládání EZS. Uživatel zadá svůj kód a stiskne tlačítko A. Pokud uživatel přišel do budovy hlavním vchodem, automaticky se odkóduje zóna č. 4. Při příchodu do budovy vchodem z haly se zóna č. 4 automaticky neodkóduje. Pak uživatel pomocí tlačítek vybere zónu nebo zóny pro odkódování a výběr potvrdí tlačítkem enter. Systém EZS provede vypnutí příslušných zón, které je indikováno zvukově a zhasnutím příslušných LED diod na panelu.

Další příchozí uživatelé jsou povinni při příchodu do budovy společnosti ověřit, že zóna, ve které mají pracoviště, je odkódovaná, protože první příchozí pracovník nemusel provést odkódování celé budovy. Na obrázku níže je zachycen přístupový panel pro odkódování budovy. [25]

Obr. 10. Přístupový panel pro odkódování budovy [25]

8.1.4 Odchod z budovy

Poslední uživatel, který z budovy odchází, je povinen důkladně zkontrolovat uzavření oken, uzamčení dveří, které vedou ze společných prostor do jednotlivých částí firmy a provést zakódování tak, aby byly zakódované všechny zóny. Zakódování se provede stejným postupem, tj. zadáním kódu, stisknutím tlačítka A, výběrem zón pro zakódování a stisknutím tlačítka enter. Po odchodu a zamčení stupních dveří je možné stav zakódování ověřit na LED diodách u hlavního vchodu do budovy společnosti. [25]

Uživatelé, kteří odcházejí z budovy na konci pracovní doby a jsou například poslední na daném patře, jsou povinni domluvit se s ostatními uživateli, kteří ještě v budově pracují, na postupu případného zakódování jednotlivých zón. Informaci o uživatelích, kteří se ještě v budově nacházejí, je možné najít například v docházkovém systému. Uživatelé jsou povinni při odchodu kontrolovat uzavření oken v prostorech svého pracoviště a případně uzamknout při odchodu vstupní dveře do společných prostor. Cílem domluvy s ostatními uživateli je omezit riziko odchodu uživatelů bez zakódování budovy. V takových případech je pak následně možné jak z docházky uživatelů, tak ze záznamů systému EZS, dohledat příslušné informace o odchodech jednotlivých uživatelů. [25]

8.1.5 Povinnosti uživatele systému EZS

Každý uživatel EZS je povinen se seznámit s těmito zásadami. Ukončením pracovního poměru, či smluvního ujednání automaticky zaniká i možnost používat EZS budovy centrály společnosti Cross Zlín. [25]

8.1.6 Zabezpečení serverovy

Serverovna v hlavní budově společnosti se nachází za dveřmi bez zvýšené odolnosti. Jedná se o standardní dveře, které mají místo kliky tzv. „kouli“. V okolí vstupu do serverovny se vyskytuje pouze detektor pro snímání pohybu, který je součástí EZS. Popsané skutečnosti je možné vidět na následujícím obrázku.

Obr. 11. Vstupní dveře do serverovny [25]

Obr. 12. Klika a zámek dveří serverovny [25]

9 SWOT ANALÝZA INFORMAČNÍHO MANAGEMENTU

Tato kapitola je zaměřena na SWOT analýzu informačního managementu firmy Cross Zlín. Analýza vychází z informací, které byly zmíněny již v předchozích kapitolách, a byla vypracována s pomocí informačního manažera společnosti. Výsledky analýzy jsou popsány v následujících podkapitolách. Z dosažených výsledků analýzy budou navržena nápravná opatření a doporučení ke zlepšení současného stavu IM.

9.1 SWOT analýza informačního managementu společnosti

Na základě získaných informací z podniku byla sestavena následující tabulka. SWOT analýza je rozdělena na **interní** a **externí** část. Interní část zahrnuje silné a slabé stránky. Jedná se o klasický soupis kladů a záporů. Pro bodování silných stránek byla zvolena kladná stupnice 1-5 s tím, že 5 znamená nejvyšší spokojenost a 1 nejnižší spokojenost. Pro slabé stránky byla zvolena záporná stupnice -1 až -5. Hodnota -5 znamená nejvyšší nespokojenost a -1 nejnižší nespokojenost.

Externí část analýzy obsahuje **vnější faktory**, kterými jsou příležitosti a hrozby. Pro příležitosti byla zvolena stejná kladná stupnice jako pro silné stránky. Pro hrozby byla použita stejná záporná stupnice, jako pro slabé stránky.

Každé položce v tabulce byla přiřazena váha, která představuje její důležitost. Váha jednotlivých položek v dané kategorii musí v součtu být 1. Čím je číslo jednotlivé položky větší, tím větší je i její důležitost v její kategorii a naopak.

Výše zmíněné informace jsou přeneseny do následující tabulky, která je uvedena na další straně.

Tab. 2. SWOT analýza IM podniku [vlastní zpracování]

	Váha	Hodnocení	Výsledek
SILNÉ STRÁNKY			
kvalita IT zázemí	0,1	3	0,3
zálohování dat	0,15	4	0,6
moderní IS	0,15	3	0,45
zabezpečení budovy EZS	0,1	4	0,4
dokumenty IM	0,1	4	0,4
pozice informačního manažera	0,15	4	0,6
omezená práva pro změnu dat	0,1	4	0,4
sdílené disky	0,15	4	0,6
součet	**1**		**3,75**
SLABÉ STRÁNKY			
závislost na dodavateli IS	0,3	-3	-0,9
kvalifikace zaměstnanců	0,25	-2	-0,5
nevyužití potenciálu IS	0,35	-4	-1,4
nejednotná verze OS uživatelů	0,1	-2	-0,2
součet	**1**		**-3**
PŘÍLEŽITOSTI			
úprava IS pro využití firmy	0,35	3	1,05
školení zaměstnanců	0,35	4	1,4
sjednocení OS uživatelů	0,1	3	0,3
nové informační technologie	0,2	3	0,6
součet	**1**		**3,35**
HROZBY			
výpadek serveru s IS	0,3	-4	-1,2
únik informací	0,2	-4	-0,8
přístup zaměstnanců ke změnám	0,1	-2	-0,2
krach firmy poskytující IS	0,15	-4	-0,6
finanční nároky IS	0,15	-2	-0,3
legislativa, platnost GDPR	0,1	-2	-0,2
součet	**1**		**-3,3**
interní faktory			0,75
externí faktory			0,05
výsledná bilance			**0,8**

Z výsledné bilance analýzy interních a externích faktorů vyplývá, že tyto faktory vykazují **kladnou bilanci hodnocení**. Z toho je patrné, že v tomto případě převažují silné stránky a příležitosti.

9.1.1 Silné stránky

Jednou ze silných stránek informačního managementu podniku je považováno kvalitní zázemí v oblasti IT. To umožňuje zaměstnancům efektivně provádět potřebné pracovní úkony.

S kvalitou IT zázemí souvisí další silné stránky. Jedná se především o zálohování dat a možnost využívání sdílených disků. Zálohování probíhá pravidelně na dva servery, což už bylo popsáno výše. Sdílené disky slouží pro ukládání a sdílení firemních dat. Společnost jich má několik a každý má své specifické využití. Pro každý sdílený disk existuje metodický pokyn, jak s ním pracovat. Metodický pokyn pro disk Z a P je uvedený v příloze.

Další silnou stránkou je, že společnost má informačního manažera, který se stará o rozvoj informačních systémů a informačních technologií v podniku, aby bylo dosaženo co nejvyšší efektivity. S tím souvisí i to, že společnost má moderní informační systém, který podniku poskytuje nadstandardní podporu v efektivním podnikání.

Kromě informačního manažera jsou v podniku vypracovány základní dokumenty informačního managementu. Mezi tyto dokumenty patří bezpečnostní politika, informační strategie a informační politika. V rámci bezpečnostní politiky firma používá různá přístupová práva podle pracovního zařazení, aby se k potřebným informacím dostali jen ti uživatelé, pro které jsou tyto informace určené. S informační bezpečností souvisí i poslední silná stránka podniku, kterou představují EZS budovy. Informační bezpečnost je tak zajišťována zevnitř i zvenku podniku.

9.1.2 Slabé stránky

Jednou ze slabých stránek firmy je závislost na dodavateli IS. Podnik vlastní licenci na používání IS, avšak o aktualizaci a správu systému se stará dodavatel. Stalo se, že aktualizace systému neproběhla v pořádku nebo systém nepracoval správně. V takovém případě nemohou zaměstnanci vykonávat svoji činnost a čekají, až bude systém opět v provozu.

Další slabou stránkou je nedostatečná kvalifikace zaměstnanců pro práci s IS. Správně pracovat s IS dokáže v podniku jen málo pracovníků, kteří pak mnohdy musí opravovat špatně zadané vstupní informace. Slabou stránkou firmy je i to, že nevyužívá plný potenciál svého informačního systému. I když je IS QI vytvořený pro podnik na míru, podle jeho zadaných

požadavků, není využíván na sto procent. Příčinou jsou nedostatečně proškolení zaměstnanci a nesprávné nadefinování některých procesů.

Poslední slabou stránkou je to, že informační technologie podniku, které využívají zaměstnanci pro svoji práci, nemají jednotnou verzi OS Windows. To může způsobovat problémy s kompatibilitou některých programových nástrojů používaných ve firmě.

9.1.3 Příležitosti

Úprava stávajícího IS pro potřeby firmy je jednou z možných příležitostí. I když byl IS navržen na míru podle firemních požadavků, nebyly všechny procesy nastaveny správně. Podnik by však musel znova nadefinovat přesné požadavky, aby bylo dosaženo požadovaného efektu IS.

Druhou příležitostí je školení zaměstnanců, kteří pracují s IS. Školením by došlo ke zmírnění případných problémů při práci s IS. Další příležitostí je sjednotit používanou verzi OS pro všechny zaměstnance. Dosáhlo by se tak lepší kompatibility, jelikož by všichni používali stejný systém. Poslední příležitostí jsou nové informační technologie, čímž by došlo ke zlepšení kvality IT. Používání aktuálních technologií napomáhá zaměstnancům pracovat efektivněji.

9.1.4 Hrozby

Výpadek serveru s IS představuje pro podnik hrozbu, jelikož tento systém pro svoji práci využívá hodně zaměstnanců. Výpadkem serveru by došlo k výraznému omezení činnosti podniku.

Druhou hrozbu představuje únik firemních informací, ať už napadením např. hackerským útokem nebo nespokojeným zaměstnancem. Můžou to být informace o zakázce, firemních postupech, strategii, o dodavatelích či zákaznících. Únik informací by mohl narušit důvěru v podnik ze strany zákazníků.

V návaznosti na provedené změny se mohou vyskytnout problémy se zaměstnanci. Může se stát, že někteří zaměstnanci nebudou ochotni se daným změnám přizpůsobit a bude docházet k nerespektování těchto změn. Management by tuto hrozbu měl podchytit již na počátku celého procesu, tak aby k ní vůbec nedošlo.

Zánik firmy poskytující IS představuje další hrozbu pro podnik. Zkrachování dodavatele IS může reálně nastat. To by pro podnik znamenalo problémy, jelikož by nebylo možné IS

pravidelně aktualizovat a museli by se vynaložit značné finanční prostředky pro zavedení nového IS. Dalšími hrozbami podniku jsou zvyšující se finanční náklady na provoz a aktualizace IS.

Poslední hrozbou současného informačního managementu podniku, je platnost nového nařízení o ochraně osobních údajů – GDPR. Nedodržení nebo zanedbání tohoto nařízení bude trestáno vysokými finančními postihy. V současnosti probíhá v podniku analýza zpracování osobních údajů pro jednotlivá oddělení. Z výsledků těchto analýz budou navržena nápravná opatření v souladu s GDPR.

10 ANALÝZA RIZIK ISMS

V této kapitole je vypracována analýza rizik informační bezpečnosti společnosti Cross Zlín. Tato analýza byla vypracována s pomocí informačního manažera společnosti a zahrnuje informační aktiva, programová aktiva, fyzická aktiva, služby a lidi.

10.1 Metodika analýzy rizik

Při analýze rizik se využívá matice aktiv, hrozeb a zranitelnosti. Prvním krokem je identifikace a ohodnocení aktiv. K ohodnocení je využita stupnice 1 - 5 (**parametr A**). Druhým krokem je stanovení pravděpodobnosti vzniku hrozby (**parametr T**). Pravděpodobnost je stanovena stupnicí 1 – 5. Následuje doplnění zranitelnosti jednotlivých aktiv konkrétními hrozbami (**parametr V**) do tabulky. Zranitelnost je stanovena stupnicí 1 – 5.

10.2 Klasifikace míry rizika

V následujícím kroku dojde k samotnému výpočtu míry rizika. Poslouží k tomu vzorec:

$$\boldsymbol{R = T\,x\,A\,x\,V}$$

Kde R je míra rizika, T je pravděpodobnost vzniku hrozby, A je hodnota aktiva a V je zranitelnost daného aktiva. Následující tabulka zobrazuje přehled stanovených hodnot pro klasifikaci míry rizika.

Tab. 3. Klasifikace míry rizika [vlastní zpracování]

Rozmezí hodnoty R	Slovní popis míry rizika	Zkratka
0-25	nízké riziko	NR
26-50	střední riziko	SR
51 a více	vysoké riziko	VR

I. Nízké riziko (bezvýznamné riziko) – akceptovatelné (přijatelné) riziko, riziko přijatelné se souhlasem vedení. Zpravidla není vyžadováno žádné zvláštní opatření. Nejedná se však o 100 % bezpečnost, proto je nutno existující riziko evidovat, případně také uvést např. jaká organizační opatření je třeba realizovat.

II. Střední riziko – je zpravidla nutno realizovat bezpečnostní opatření dle zpracovaného plánu podle rozhodnutí BF. Prostředky na snížení rizika musí být implementovány ve stanoveném časovém období.

III. Vysoké riziko – nežádoucí riziko, vyžadující urychlené provedení odpovídajících bezpečnostních opatření snižujících riziko na přijatelnější úroveň, na snížení rizika se musí přidělit potřebné zdroje. Je-li toto riziko spojeno se značnými nebezpečnými dopady, musí se provést jeho další vyhodnocení, aby se přesněji stanovila pravděpodobnost vzniku incidentu, jako podklad pro stanovení potřeby dosažení zlepšení a snížení rizika. O akceptovatelnosti rizik rozhoduje vedení společnosti.

10.3 Informační aktiva

Informační aktiva jsou pro firmu velmi důležitá, jelikož mají významný vliv na její fungování. Ve spolupráci s informačním manažerem byla vybrána důležitá informační aktiva. Ztráta nebo poškození těchto dat by pro firmu znamenalo značné komplikace a případně také ekonomické ztráty. Stejný případ by mohl nastat, pokud by došlo k jejich zneužití. V tabulce níže jsou vypsána důležitá informační aktiva a určena jejich hodnota pro podnik.

Tab. 4. Informační aktiva [vlastní zpracování]

Identifikovaná aktiva	Hodnota aktiva
Databáze serveru	5
Databáze IS	5
Databáze sdílené disky	4
Databáze Sharepoint	3
Zdrojové kódy a související soubory	2

Pro vybraná informační aktiva, bylo identifikováno několik hrozeb a byla určena pravděpodobnost jejich uskutečnění s ohledem na současný stav bezpečnostních opatření v podniku. Mezi identifikované hrozby patří požár, povodeň, krádež, neúmyslná modifikace a zlomyslné kódy. Tyto identifikované hrozby a pravděpodobnost jejich naplnění, jsou uvedeny v následující tabulce 5.

Tab. 5. Identifikované hrozby [vlastní zpracování]

Identifikovaná hrozba	Pravděpodobnost hrozby
Požár	2
Povodeň	2
Krádež	3
Neúmyslná modifikace	4
Zlomyslné kódy	4

Aktiva a hrozby byly identifikovány v tabulkách výše. Pro analýzu rizik je velmi důležité stanovit míru zranitelnosti jednotlivých aktiv. Na základě určené míry zranitelnosti se poté vypočítá hodnota rizik ohrožených aktiv. Míra zranitelnosti identifikovaných aktiv je uvedena v následující tabulce 6.

Tab. 6. Matice zranitelnosti – informační aktiva [vlastní zpracování]

	Popis aktiva	Databáze serveru	Databáze IS	Databáze SD	Databáze Sharepoint	Zdrojové kódy
	Hodnota aktiva (A)	5	5	4	3	2
Popis hrozby	**Pravděpodobnost hrozby (T)**					
Požár	2	2	2	2	2	2
Povodeň	2	1	1	1	1	1
Krádež	3	2	2	2	1	2
Neúmyslná modifikace	4	2	2	4	1	2
Viry a malware	4	2	2	2	2	3

Matice zranitelnosti představuje základ pro vypočítání míry rizik pro jednotlivá aktiva. Z hodnot uvedených v tabulce 6 se vypočítá matice rizik. Výsledné hodnoty jsou dosazeny do tabulky 7, která je uvedena níže.

Tab. 7. Matice rizik – informační aktiva [vlastní zpracování]

	Popis aktiva	Databáze serveru	Databáze IS	Databáze SD	Databáze Sharepoint	Zdrojové kódy
	Hodnota aktiva (A)	5	5	4	3	2
Popis hrozby	**Pravděpodobnost hrozby (T)**					
Požár	2	20	20	16	12	8
Povodeň	2	10	10	8	6	4
Krádež	3	30	30	24	9	12
Neúmyslná modifikace	4	40	40	64	12	16
Viry a malware	4	40	40	32	24	24

Z výsledné matice rizik informačních aktiv vyplývá, že největším rizikem je neúmyslná modifikace dat na sdílených discích. Hodnota rizika pro toto aktivum je **64**, což znamená vysoké riziko. Druhá nejvyšší dosažená hodnota rizika je **40**, tedy střední riziko. Tímto rizikem je neúmyslná modifikace databáze serveru a IS. Kromě toho stejným rizikem jsou pro databáze serveru a IS viry a malware. Viry a malware představují střední riziko i pro data na sdílených discích. Posledním středním rizikem je krádež dat ze serveru a IS, hodnota tohoto rizika vyšla shodně **30**. Všechny ostatní vypočítané hodnoty v matici rizik patří do kategorie nízkých rizik.

10.4 Programová aktiva

Pro zajištění informační bezpečnosti je důležité, aby byla dostatečně zabezpečena i programová aktiva společnosti. Mezi tyto aktiva patří **instalační média** a **licence**. Instalačními médii jsou myšlena veškerá instalační média na software, který je používaný v rámci firmy buď v podobě médií, nebo v podobě ISO obrazů a partnerském webu Microsoft. Licencemi se rozumí všechny softwarové licence uložené buď v papírové podobě, anebo elektronicky. Hodnota identifikovaných aktiv je uvedena v tabulce 8.

Tab. 8. Identifikovaná programová aktiva [vlastní zpracování]

Identifikovaná aktiva	Hodnota aktiva
Instalační média	3
Licence	4

Pro tyto vybraná aktiva byly identifikovány hrozby, které by mohly nastat. Na základě současného stavu zabezpečení těchto aktiv, byla určena jejich pravděpodobnost, která je uvedena v tabulce 9. :

Tab. 9. Identifikované hrozby programových aktiv [vlastní zpracování]

Identifikovaná hrozba	Pravděpodobnost hrozby
Výpadek internetového připojení	2
Selhání SW	3
Zlomyslné kódy	3
Požár	2

Určení míry zranitelnosti jednotlivých aktiv vůči identifikovaným hrozbám je jedním z důležitých kroků analýzy rizik. Na základě údajů uvedených v tabulce výše byla vytvořena matice zranitelnosti programových aktiv společnosti. Tato matice je v tabulce 10.

Tab. 10. Matice zranitelnosti – programová aktiva [vlastní zpracování]

	Popis aktiva	Instalační média	Licence
	Hodnota aktiva (A)	3	4
Popis hrozby	**Pravděpodobnost hrozby (T)**		
Výpadek internetového připojení	2	3	3
Selhání SW	3	2	2
Zlomyslné kódy	3	4	4
Požár	2	2	2

Z údajů uvedených v matici zranitelnosti se vypočítá míra rizika pro jednotlivá aktiva a hrozby. Výsledné hodnoty jsou dosazeny do tabulky 11, která je uvedena níže.

Tab. 11. Matice rizik – programová aktiva [vlastní zpracování]

	Popis aktiva	Instalační mé-dia	Licence
	Hodnota aktiva (A)	3	4
Popis hrozby	**Pravděpodobnost hrozby (T)**		
Výpadek internetového připojení	2	18	24
Selhání SW	3	18	24
Zlomyslné kódy	3	36	48
Požár	2	12	16

Z výsledků uvedených v tabulce výše vyplývá, že největším rizikem jsou zlomyslné kódy pro instalační média a licence. Dosažené hodnoty **48** a **36** znamenají, že se jedná o střední

riziko pro programová aktiva společnosti. Všechny ostatní hodnoty v matici rizik patří do nízkých rizik.

10.5 Fyzická aktiva

Do informačního managementu firmy patří i fyzická aktiva. Jedná se o serverovou infrastrukturu, která je umístěná v zabezpečené serverovně. Kromě ní existuje ještě serverová infrastruktura v datacentru. Dalším fyzickým aktivem je síťová infrastruktura, která je umístěna v serverovně a rozvaděčích po celé firmě. Fyzickými aktivy jsou i stolní PC a notebooky zaměstnanců, a také sdílená zařízení uživatelů, což mohou být např. tiskárny. Hodnota těchto aktiv pro podnik je uvedena v tabulce 12.

Tab. 12. Identifikovaná fyzická aktiva [vlastní zpracování]

Identifikace aktiva	Hodnota aktiva
Servery - serverovna	5
Servery – datacentrum	5
Síťové prvky	4
Stolní PC	3
Notebooky	3
Sdílená zařízení	2

K vybraným fyzickým aktivům byly určeny hrozby. Mezi tyto hrozby patří havárie klimatizace, chyba obsluhy, narušení prostoru, povodeň a požár. Tyto identifikované hrozby jsou uvedeny v následující tabulce 13. V tabulce je kromě zmíněných hrozeb vypsána i pravděpodobnost, s jakou by mohly jednotlivé hrozby nastat.

Tab. 13. Identifikované hrozby fyzických aktiv [vlastní zpracování]

Identifikovaná hrozba	Pravděpodobnost hrozby
Havárie klimatizace	3
Chyba obsluhy	2
Narušení prostoru	2
Povodeň	1
Požár	1

Data z tabulek 12 a 13 jsou přenesena do matice zranitelnosti. V této matici jsou určeny hodnoty zranitelnosti jednotlivých aktiv vůči daným hrozbám. Vše je uvedeno v následující tabulce 14.

Tab. 14. Matice zranitelnosti – fyzická aktiva [vlastní zpracování]

	Popis aktiva	Servery - serverovna	Servery - datacentrum	Síťové prvky	Počítače	Notebooky	Sdílená zařízení
	Hodnota aktiva (A)	5	5	4	3	3	2
Popis hrozby	**Pravděpodobnost hrozby (T)**						
Havárie klimatizace	3	3	3	2			
Chyba obsluhy	2	3	3	2	5	5	3
Narušení prostoru	2	5	5	4	3	4	2
Povodeň	1	2	2	1	2	2	1
Požár	1	2	2	1	2	2	1

Dosazením hodnot do tabulky 14 vznikla matice zranitelnosti. Z této matice je vypočítána míra rizik pro vybraná fyzická aktiva. Výsledné hodnoty rizik jsou vypsány v tabulce 15 a tvoří tak matici rizik fyzických aktiv podniku.

Tab. 15. Matice rizik – fyzická aktiva [vlastní zpracování]

	Popis aktiva	Servery - serverovna	Servery - datacentrum	Síťové prvky	Počítače	Notebooky	Sdílená zařízení
	Hodnota aktiva (A)	5	5	4	3	3	2
Popis hrozby	**Pravděpodobnost hrozby (T)**						
Havárie klimatizace	3	45	45	24			
Chyba obsluhy	2	30	30	16	30	30	12
Narušení prostoru	2	50	50	32	18	24	8
Povodeň	1	10	10	4	6	6	2
Požár	1	10	10	4	6	6	2

Nejvyšší hodnota rizik fyzických aktiv, která byla v matici rizik vypočítána, je **50**. To znamená, že se jedná o střední riziko. Tímto rizikem je narušení prostoru serverovny v hlavní budově společnosti i v datacentru. Druhá nejvyšší vypočítaná hodnota rizik je **45**. Tímto rizikem je havárie klimatizací v obou serverovnách. Zjištěným středním rizikem je pak ještě narušení prostoru síťových prvků a chyba obsluhy obou serveroven, počítačů a notebooků. Všechny ostatní hrozby představují pro společnost nízké riziko.

10.6 Služby

V analýze ISMS jsou zahrnuty i služby, které společnost využívá Cross Zlín, a mohly by mít vliv na bezpečnost dat. Do těchto služeb patří dodávka elektřiny do serverovny v budově společnosti a také do serverovny v datacentru. Další důležitou službou je EZS budovy napojený na PCO. Dále zde patří také konektivita obou serveroven a konektivita s informačním systémem. Hodnota všech výše popsaných aktiv je v tabulce 16.

Tab. 16. Identifikovaná aktiva – služby [vlastní zpracování]

Identifikace aktiva	Hodnota aktiva
Dodávka elektřiny - serverovna	3
Dodávka elektřiny - datacentrum	4
EZS	2
Konektivita - serverovna	3
Konektivita - datacentrum	4
Konektivita IS	4

Kromě hodnoty jednotlivých aktiv pro podnik, je důležité vymezit hrozby, které by mohly nastat. V případě poskytovaných služeb se jedná o výpadek elektrické energie, výpadek internetové připojení, narušení komunikačních kanálů nebo problém na straně dodavatele datacentra. Pravděpodobnost, že zmíněné hrozby nastanou, je vyjádřena v tabulce 17.

Tab. 17. Identifikované hrozby – služby [vlastní zpracování]

Identifikovaná hrozba	Pravděpodobnost hrozby
Výpadek elektrické energie	2
Výpadek internetového připojení	2
Narušení komunikačních kanálů	3
Problém na straně dodavatele služeb datacentra	4

Identifikovaná aktiva a hrozby jsou společně s mírou zranitelnosti aktiv uvedeny v následující tabulce 18. V matici zranitelnosti se jednotlivým aktivů přiřazuje míra zranitelnosti pro identifikované hrozby. Následně se z matice zranitelnosti vypočítá míra rizik pro všechna identifikovaná aktiva a výsledné hodnoty se zaznamenají do matice rizik.

Tab. 18. Matice zranitelnosti – služby [vlastní zpracování]

	Popis aktiva	Dodávka elektřiny - serverovna	Dodávka elektřiny - datacentrum	EZS	Konektivita - serverovna	Konektivita - datacentrum	Konektivita IS
	Hodnota aktiva (A)	3	4	2	3	4	4
Popis hrozby	**Pravděpodobnost hrozby (T)**						
Výpadek elektrické energie	2	3	2	2	2	2	2
Výpadek internetového připojení	2			2	2	3	3
Narušení komunikačních kanálů	3				2	4	4
Problém na straně dodavatele služeb datacentra	4					3	

Hodnoty, které jsou zapsány v tabulce 18, se použijí pro sestavení matice rizik. Jestliže se na identifikované aktivum daná hrozba nevztahuje, není v buňce uvedena žádná hodnota. V tomto okamžiku jsou tedy známé všechny hodnoty, ze kterých lze vypočítat míru rizik pro jednotlivá aktiva, vzhledem k uvedeným hrozbám. K tomuto výpočtu se použije vzorec, který byl definován již na začátku této kapitoly.

$$\boldsymbol{R = T\,x\,A\,x\,V}$$

Dosazením hodnot z tabulky 18 do tohoto vzorce dojde k výpočtu míry rizik. Vypočtené hodnoty jsou uvedeny v tabulce 19, která tvoří matici rizik.

Tab. 19. Matice rizik – služby [vlastní zpracování]

	Popis aktiva	Dodávka elektřiny - serverovna	Dodávka elektřiny - datacen-	EZS	Konektivita - serve- rovna	Konektivita - datacen- trum	Konektivita IS
	Hodnota aktiva (A)	3	4	2	3	4	4
Popis hrozby	**Pravděpodobnost hrozby (T)**						
Výpadek elektrické energie	2	18	16	8	12	16	16
Výpadek internetového připojení	2			8	12	24	24
Narušení komunikačních kanálů	3				18	48	48
Problém na straně dodavatele služeb datacentra	4					48	

Z uvedených dat v tabulce 19 vyplývá, že výpadek některé z poskytovaných služeb nemá zásadní vliv na informační bezpečnost firmy. Po vypočítání matice rizik je nejvyšší výsledná hodnota **48**, což znamená střední riziko. Z tohoto pohledu je tedy patrné, že současný systém využívání je nastavený a zabezpečený správně a není třeba ho nějak podstatně zlepšovat.

10.7 Lidé

Informační bezpečnost je závislá i na jednotlivcích a jejich dodržování stanovených pravidel bezpečnosti. Z tohoto pohledu je pro firmu důležitá hlavně kvalifikace zaměstnance a úroveň jeho zaškolení z hlediska dodržování interních pravidel. Zmíněným aktivům byla v následující tabulce 20 přidělena jejich hodnota pro firmu.

Tab. 20. Identifikovaná aktiva – lidé

[vlastní zpracování]

Identifikovaná aktiva	**Hodnota aktiva**
Kvalifikace	5
Úroveň zaškolení	5

Pro tyto aktiva byly vymezeny hrozby, které by mohly daná aktiva ohrozit. Mezi tyto hrozby rozhodně patří ztráta kvalifikace zaměstnance, riziko související s neznalostí interních předpisů a také záměrné porušení interních předpisů, které by mohlo znamenat poškození nebo ztrátu důležitých firemních dat. Tyto hrozby jsou vypsány v tabulce 21 i s pravděpodobností jejich naplnění.

Tab. 21. Identifikované hrozby – lidé [vlastní zpracování]

Identifikovaná hrozba	Pravděpodobnost hrozby
Ztráta kvalifikace	2
Riziko související s neznalostí interních předpisů	4
Záměrné porušení interních přepisů	3

Tabulka 22 představuje matici zranitelnosti. V této tabulce jsou vypsány zranitelnosti jednotlivých aktiv vůči identifikovaným hrozbám. Na základě těchto dat je pak vypočítána míra rizik.

Tab. 22. Matice zranitelnosti – lidé [vlastní zpracování]

	Popis aktiva	Kvalifikace	Úroveň zaškolení
	Hodnota aktiva (A)	5	5
Popis hrozby	**Pravděpodobnost hrozby (T)**		
Ztráta kvalifikace,certifikace	2	2	2
Riziko související s neznalostí interních předpisů	4	3	4
Záměrné porušení interních předpisů	3	3	3

Hodnoty uvedené v tabulce 22 slouží pro výpočet matice rizik. Tuto matici představuje tabulka 23, ve které jsou vypočítány hodnoty rizik pro jednotlivá aktiva.

Tab. 23. Matice rizik – lidé [vlastní zpracování]

	Popis aktiva	Kvalifikace	Úroveň zaškolení
	Hodnota aktiva (A)	5	5
Popis hrozby	**Pravděpodobnost hrozby (T)**		
Ztráta kvalifikace,certifikace	2	20	20
Riziko související s neznalostí interních předpisů	4	60	80
Záměrné porušení interních předpisů	3	45	45

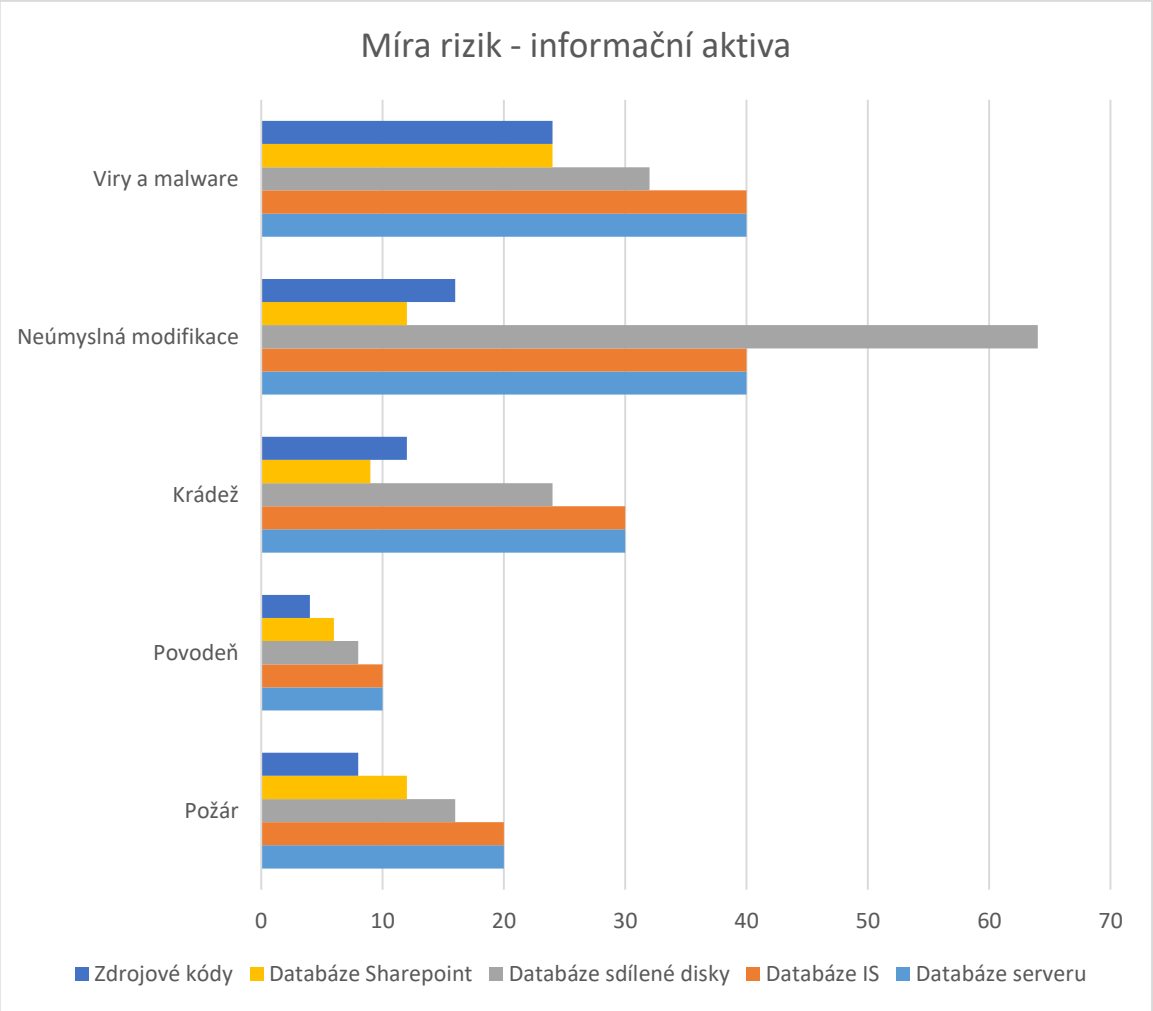
Z výsledných hodnot v matici rizik vyplývá, že největším rizikem je neznalost interních předpisů z důvodu neodpovídající úrovně zaškolení. Hodnota tohoto rizika je **80**, což představuje vysoké riziko. Druhou nejvyšší dosaženou hodnotou (**60**) je stejné riziko vzhledem k úrovni kvalifikace zaměstnance. Kromě toho je z matice patrné, že záměrné porušení interních předpisů představuje pro podnik střední riziko. Další údaje z matice pak patří do kategorie nízkých rizik.

10.8 Shrnutí výsledků analýzy ISMS

V této kapitole bylo provedeno několik analýz z pohledu informační bezpečnosti podniku. Analýzy se týkaly informačních aktiv, programových aktiv, fyzických aktiv, služeb a lidí. Tato aktiva mají pro firmu velký význam z hlediska zajištění informační bezpečnosti, a proto je důležité, aby byla dostatečně chráněna. Z výsledků analýz vyplývá, že existují nějaká rizika, která by mohla tato aktiva ohrozit a způsobit tak podniku škody. Tato podkapitola je tedy zaměřená na shrnutí dosažených výsledků z předchozích analýz, na základě kterých budou navržena nápravná opatření.

10.8.1 Informační aktiva

Zajištění bezpečnosti informačních aktiv je pro podnik velmi důležité, neboť jejich poškození, ztráta nebo zneužití by pro firmu představovalo značný problém. Analýzou informačních aktiv vyšlo najevo, že z pohledu bezpečnosti existuje jedno vysoké riziko a pár středních rizik. Výsledky z analýzy byly přeneseny do grafu, který je vidět na obrázku 13.

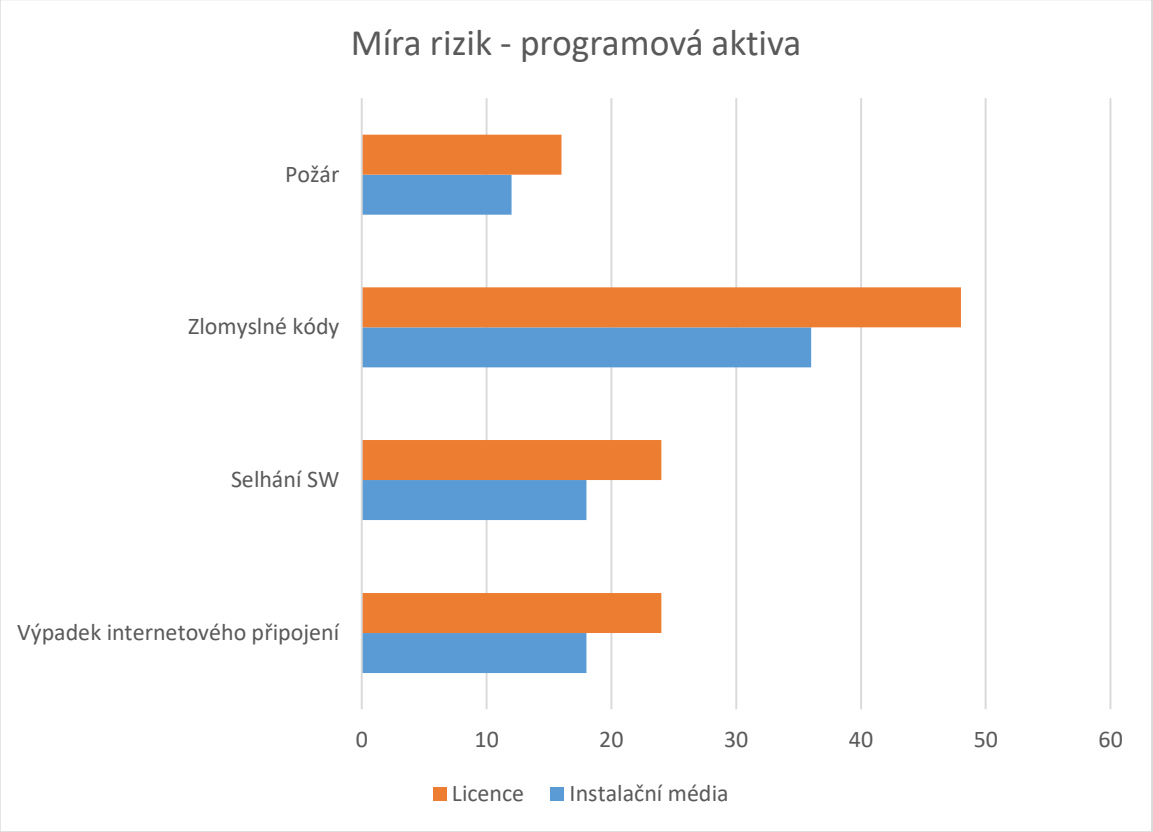


Obr. 13. Graf – rizika informačních aktiv [vlastní zpracování]

Z grafu je zřejmé, že vysoké riziko představuje neúmyslná modifikace dat, která jsou uložena na sdílených discích společnosti. Jak již bylo zmíněno společnost má sdílených disků několik a každý má jiné využití. Slouží pro ukládání a sdílení důležitých firemních informací. Jestliže by došlo k jejich neúmyslné modifikaci, byl by to pro firmu značný problém. Proto je nutné, aby došlo k vypracování nápravného opatření, které by přispělo ke snížení tohoto rizika. Dále byla zjištěna střední rizika, která nevyžadují tak rychlou realizaci nápravných opatření, avšak bez povšimnutí zůstat nemůžou.

10.8.2 Programová aktiva

Důležitým prvkem informačního managementu společnosti jsou i programová aktiva. Aby byla zajištěna vysoká úroveň informační bezpečnosti, je potřeba zabezpečit dostatečnou ochranu i těmto aktivům. Analýza ukázala, že v oblasti programových aktiv v současnosti neexistují vysoká rizika. Zjistilo se, že existuje pár středních rizik, která by mohla mít na informační bezpečnost vliv. Výsledky z provedené analýzy jsou uvedeny v grafu, který je na obrázku 14.

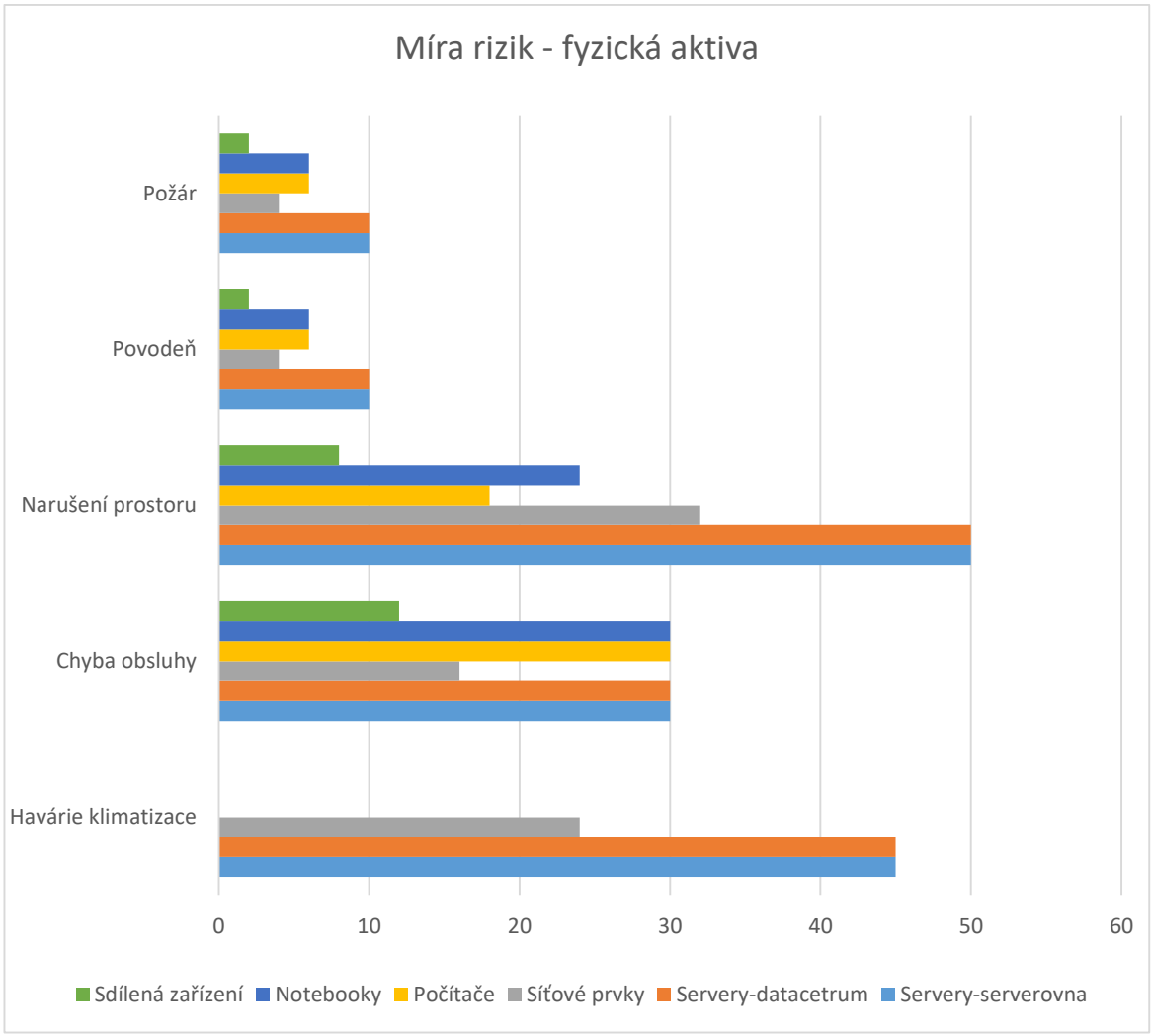


Obr. 14. Graf – rizika programových aktiv [vlastní zpracování]

Z grafu lze vyčíst, že středním rizikem jsou zlomyslné kódy pro instalační média a licence. Všechna ostatní zjištěná rizika patří do kategorie nízkých rizik a nevyžadují tedy nápravná opatření.

10.8.3 Fyzická aktiva

Kromě informačních a programových aktiv je z hlediska informační bezpečnosti nutné zajistit odpovídající ochranu fyzických aktiv. Analýza těchto aktiv odhalila, že existuje několik středních rizik, která je mohou ohrozit a způsobit tak narušení informační bezpečnosti podniku. Dosažené hodnoty z analýzy byly převedeny do grafu, který je na obrázku 15.

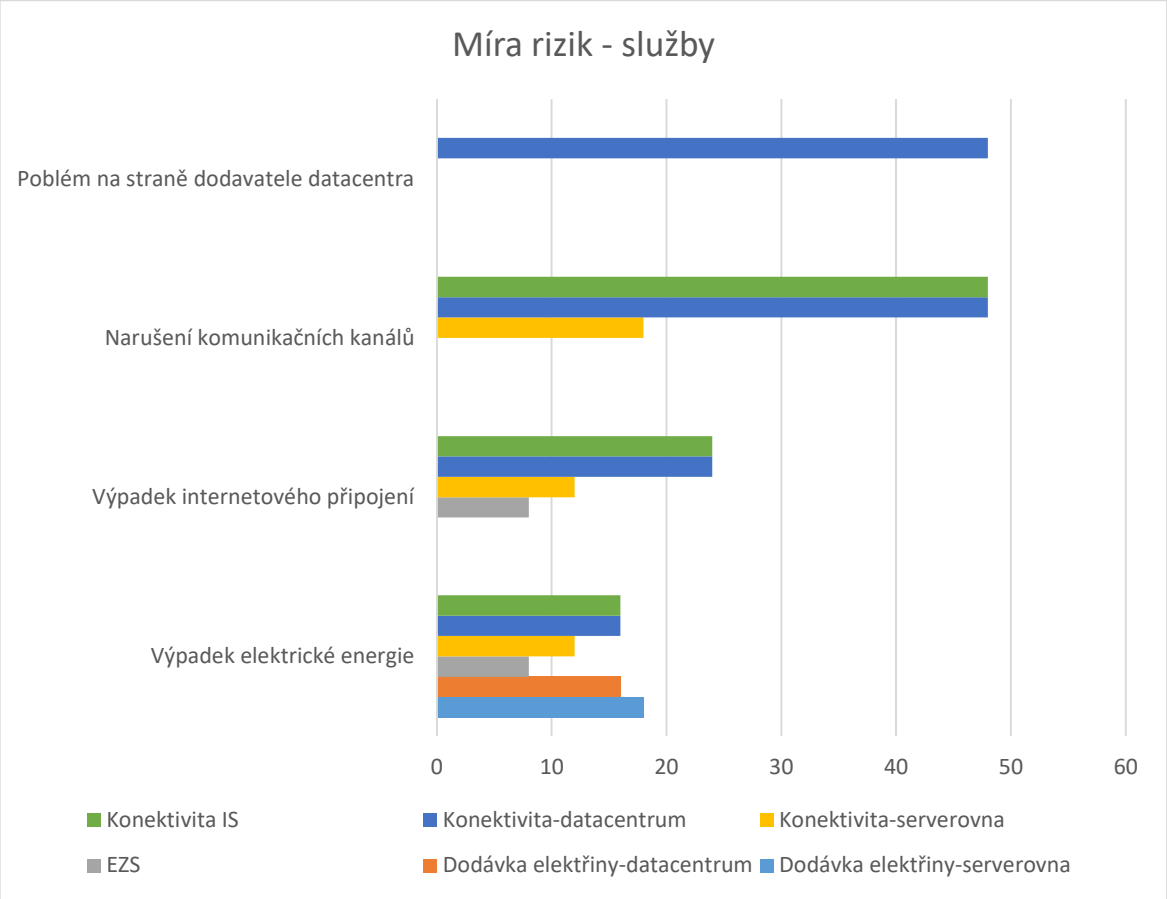


Obr. 15. Graf – rizika fyzických aktiv [vlastní zpracování]

Z grafu je patrné, že středním rizikem je narušení prostoru serverovny v hlavní budově společnosti, a také narušení prostoru serverovny umístěné v datacentru. V případě, že by se do serveroven dostala nepovolaná osoba, mohlo by např. neznalostí dojít k poškození důležitých částí a ztrátě dat nebo dokonce k ochromení činnosti podniku. Další riziko představuje havárie klimatizace v obou serverovnách. Závada klimatizace by mohla způsobit přehřívání serveru, což by mohlo mít za následek ztrátu dat nebo poškození serveru. Posledním rizikem je chyba obsluhy v případě obou serveroven, stolních počítačů a notebooků. Všechna tato zmíněná rizika jsou zařazena do kategorie středních rizik. Nevyžadují tedy okamžitou nápravu, ale je nutné, aby se o nich vědělo a v budoucnosti se podnikly kroky, které povedou k jejich eliminaci.

10.8.4 Služby

Poskytované služby představují aktiva, jejichž dodávka se nedá z velké části ovlivnit, avšak jejich kvalita má vliv na informační bezpečnost podniku. V případě, že nastane výpadek nějaké z poskytovaných služeb, mělo by být zajištěno náhradní řešení pro tuto situaci. Analýzou služeb bylo zjištěno, že v oblasti poskytovaných služeb existuje několik středních rizik. Výsledné hodnoty z analýzy jsou vidět na grafu, který je na obrázku 16.

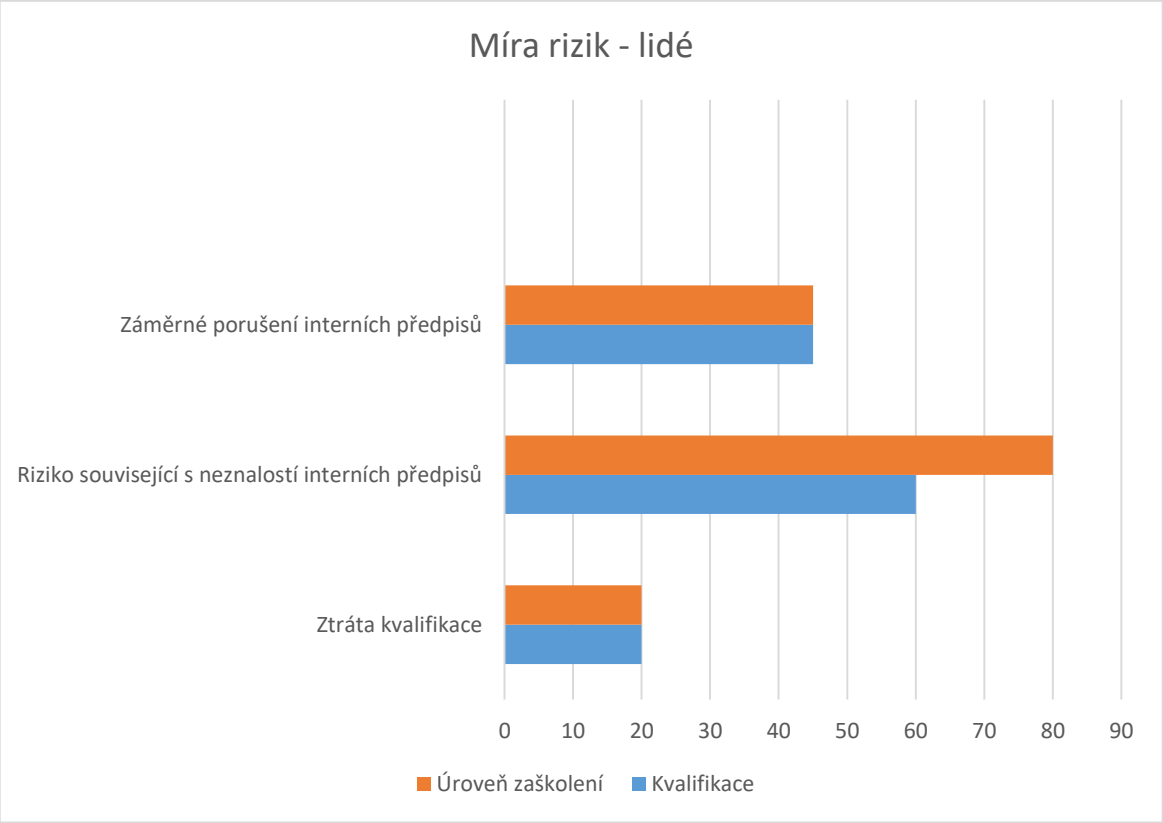


Obr. 16. Graf – rizika poskytovaných služeb [vlastní zpracování]

Z grafu lze vyčíst, že střední riziko v oblasti poskytovaných služeb představuje narušení komunikačních kanálů. Tím by došlo ke ztrátě konektivity obou serveroven. Dalším středním rizikem je možnost, že by mohl vzniknout problém na straně dodavatele služeb pro datacentrum.

10.8.5 Lidé

Informační bezpečnost podniku je závislá i na lidech a jejich dodržování nastavených pravidel v oblasti bezpečnosti. Z tohoto důvodu je nezbytné, aby byly vypracovány potřebné dokumenty, se kterými by se zaměstnanci mohli seznámit. Výsledné údaje z analýzy jsou zobrazeny v grafu, který je na obrázku 17.



Obr. 17. Graf – rizika lidského faktoru [vlastní zpracování]

Z tohoto grafu vyplývá, že vysoké riziko představuje neznalost interních předpisů, která souvisí s úrovní zaškolení zaměstnanců. Všichni zaměstnanci by měli být řádně proškoleni o tom, jak dodržovat pravidla informační bezpečnosti. Důležitou roli v tomto směru hraje i kvalifikace zaměstnanců. Dalším rizikem je záměrné porušení interních předpisů. To se může stát z mnoha důvodů. Jedním z nich může být např. frustrovaný zaměstnanec společnosti, který se chce tímto činem pomstít podniku.

11 NÁVRH NÁPRAVNÝCH OPATŘENÍ A DOPORUČENÍ

Na základě výsledků provedených analýz jsou v této kapitole popsány návrhy nápravných opatření ke zlepšení současné situace. Nejprve byla v kapitole 9 vypracována SWOT analýza současného stavu informačního managementu společnosti Cross Zlín. Kapitola 10 zahrnuje analýzu z pohledu informační bezpečnosti společnosti.

11.1 Návrhy na základě výsledků SWOT analýzy

Celková bilance SWOT analýzy informačního managementu dopadla pro podnik příznivě, neboť výsledná hodnota součtu interních a externích faktorů je +0,8. I když je výsledek kladný, tak dosažená hodnota není moc vysoká. Proto by bylo vhodné aplikovat určitá nápravná opatření, což by zlepšilo úroveň informačního managementu firmy Cross Zlín.

11.1.1 Opatření pro slabé stránky

Výsledky analýzy ukázaly, že slabými stránkami informačního managementu je závislost na dodavateli IS, úroveň kvalifikace zaměstnanců pro práci s IS, nevyužití potenciálu IS a nejednotná verze OS na počítačích zaměstnanců společnosti. Z tohoto důvodu byla navržena tato doporučení:

- **kvalifikace zaměstnanců pro práci s IS** se dá zlepšit aplikováním školení požadované úrovně, dle zařazení zaměstnance. V současné době firma zajišťuje zaměstnancům školení při jejich nástupu na pracovní pozici. Avšak je nezbytné, aby v případě, že nastane u zaměstnance změna jeho pracovního zařazení, zajistit řádné školení pro práci s IS, které odpovídá jeho nové pracovní pozici a byla mu nastavena odpovídající přístupová práva v systému,
- **nevyužití potenciálu IS** je způsobeno několika faktory. Prvním z nich je ten, že firma poskytující IS neměla při jeho implementaci dostatečné zkušenosti s takovým podnikem jako je Cross Zlín. Druhým faktorem je to, že firma Cross Zlín během svého dvacetiletého fungování nevyužívala žádný IS. Z těchto důvodů neproběhl proces implementace nejlépe a zejména v začátcích se firma potýkala se značnými problémy funkčnosti IS. Nyní je to tři roky co je IS ve firmě používán a i v současnosti se stále vyskytují problémy. Pro odstranění přetrvávajících problémů by bylo vhodné, aby celý proces implementace proběhl od začátku s lépe definovanými požadavky. Toto řešení ovšem bude vyžadovat další výdaje na fungování IS,

- **nejednotná verze OS** na počítačích zaměstnanců způsobuje občas problémy s kompatibilitou některých důležitých programů. Některým uživatelům funguje vše bez problému a jiní nemohou vykonávat svou činnost, protože májí odlišnou verzi OS a musí tak kontaktovat IT oddělení. I když v rámci organizace Cross Zlín jsou využívány informační technologie pro všechny zaměstnance od stejného výrobce, tak verze OS může být odlišná. Ideálním případem by bylo, aby všichni používali identickou verzi, což ale vzhledem k omezenému počtu licencí není možné. Firma by tak musela nakoupit nové licence. V tomto případě je ovšem nutné zjistit, zda by nákup nových licencí byl pro podnik rentabilní.

11.1.2 Opatření pro hrozby

Z dosažených výsledků analýzy je patrné, že pro informační management existuje několik hrozeb, které by se měly minimalizovat. Zjištěnými hrozbami jsou výpadek serveru IS, únik informací, přístup zaměstnanců ke změnám, krach firmy poskytující IS, finanční nároky IS a legislativa. Z tohoto důvodu byla navržena tato doporučení:

- **výpadek serveru IS** by znamenal značné omezení činnosti organizace. Řešení tohoto problému je spíše na dodavateli poskytovaných služeb, a tak společnost Cross Zlín v takové situaci moc možností nemá. Poskytovatel by mohl využít např. záložní server a tím by nedošlo k takovému výpadku činnosti podniku,
- **krach firmy poskytující IS** by pro společnost Cross Zlín znamenal zásadní problém. V informačním systému jsou totiž uložena data o zakázkách, ekonomické agendě společnosti, data o zákaznících a dodavatelích a také IS slouží pro evidenci docházky. Všechna tato data by musela být přenesena do nového systému, což by pro podnik představovalo velkou finanční zátěž. Řešením takové situace by bylo vypracování interního dokumentu pro podobné situace. Tento dokument by obsahoval metodické pokyny, jak v takové situaci postupovat a měl by být aktualizován jedenkrát za rok,
- z pohledu informačního managementu **v oblasti legislativy** představuje nyní největší hrozbu platnost GDPR. Jestliže by společnost zanedbala přípravu a nezajistila dostatečnou ochranu osobních dat, hrozily by jí vysoké sankce. Nyní proto probíhá v rámci organizace analýza využívání osobních dat a na základě výsledků budou navržena vhodná nápravná opatření,

- **finanční nároky IS** se z velké části ovlivnit nedají a záleží na poskytovateli služeb. Může ovšem nastat situace, že nabízené ceny za služby nebudou zcela odpovídat běžným cenám na trhu. Management společnosti by na to měl myslet a v takovém případě si nechat vypracovat analýzu, zda se mu stávající IS za takových podmínek vyplatí.

11.2 Návrhy pro zlepšení informační bezpečnosti

V kapitole 10 byla provedena analýza rizik ISMS, která odhalila, že v oblasti informační bezpečnosti společnosti Cross Zlín, je několik rizik, která je potřeba eliminovat. Náplní této kapitoly je vypracování návrhů opatření pro zlepšení informační bezpečnosti podniku.

11.2.1 Opatření pro vysoká rizika

Z provedených analýz vyšlo najevo, že je třeba se vypořádat se dvěma vysokými riziky. První z těchto rizik je neúmyslná modifikace dat na sdílených discích, které slouží pro ukládání a sdílení důležitých firemních dat a informací. Z tohoto důvodu byly vypracovány návrhy nápravných opatření při práci se sdílenými disky.

Z pohledu prevence se doporučuje:

- **pravidelný audit** oprávnění ke složkám sdíleného disku s cílem minimalizovat počet osob, které mohou provádět odstranění dat,
- **pravidelná školení** pracovníků, kteří jsou zodpovědní za dozor nad obsahem sdílených složek a kteří mohou provádět hromadné kopírování a přesuny dat,
- nutnost upozornit zodpovědné pracovníky, aby v případě neúmyslného odstranění dat neprodleně informovali správce IT.

Jestliže už k neúmyslnému odstranění dat ze sdílených disků dojde, je třeba mít vypracován plán pro obnovu těchto dat.

V rámci obnovy dat ze sdílených disků se doporučuje:

- provádět **pravidelnou kontrolu zálohování** sdílených disků tak, aby byly v libovolném okamžiku k dispozici co možná nejaktuálnější zálohy dat, ze kterých by se dala chybějící data obnovit,
- **postupné zvětšování zálohovacího prostoru** pro možnost uchovávat větší počet záloh tak, aby byla v případě potřeby dostupná i historická data, ze kterých by bylo možné chybějící data obnovit.

Druhým vysokým rizikem pro společnost Cross Zlín, které bylo odhaleno analýzou, je neznalost interních předpisů.

Z tohoto důvodu se doporučuje:

- seznámit každého nového zaměstnance během vstupního školení s firemními předpisy v oblasti informační bezpečnosti společnosti. V současné době probíhá vstupní školení jen v rámci BOZP a PO.

11.2.2 Opatření pro střední rizika

Kromě vysokých rizik byla analýzou odhalena i rizika střední. Tato rizika nevyžadují okamžitou realizaci nápravných opatření, avšak je nutné se jimi zabývat a co nejvíce je eliminovat ve stanoveném časovém horizontu. V rámci této práce byla proto navržena nápravná opatření i pro tuto skupinu rizik.

Rizika, která souvisí se zabezpečením serverovny je několik. Jedná se o narušení prostoru serverovny neoprávněnou osobou, krádež dat, neúmyslnou modifikací a narušení komunikačních kanálů. S těmito riziky souvisí, jakým způsobem je zabezpečený vstup do prostoru serverovny. V hlavní budově podniku je vstup do serverovny zabezpečen obyčejnými dveřmi bez bezpečnostního zámku. Z tohoto důvodu jsou doporučována následující opatření:

- výměna standardních dveří do serverovny za dveře se zvýšenou odolností a bezpečnostním zámkem,
- použití systémů pro kontrolu vstupu do serverovny, jako jsou např. RFID čipy, karty, hesla nebo i biometrické údaje. Výběrem správného systému kontroly může dojít k výraznému zlepšení zabezpečení serverovny podniku.

Dalším zjištěným rizikem v této kategorii je havárie klimatizace v serverovně. V případě, že by k takové události došlo, mohlo by vlivem nedostatečného chlazení dojít k přehřívání serveru a jeho poškození. Z tohoto důvodu bylo navrženo, aby pro tyto případy měla firma pořízenou **náhradní klimatizaci**, kterou by mohla případně využít a předejít tak případné ztrátě nebo poškození dat.

12 IMPLEMENTACE GDPR

Nařízení o ochraně osobních údajů vstoupí v platnost dne 25. května 2018. Tato kapitola popisuje proces implementace tohoto nařízení do podnikového procesu firmy Cross Zlín.

12.1 Plán implementace

Plán implementace sestavoval provozní ředitel společnosti Cross Zlín. Implementace GDPR byla rozdělena do tří hlavních etap.

I. etapa

V první fázi bylo nutné vytvořit pracovní skupinu, která bude odpovědná za implementaci nového nařízení. Tým byl složený z osmi členů a bylo potřeba je s problematikou GDPR seznámit. Absolvovali tedy důležitá školení, aby získali potřebné znalosti k procesu implementace.

Dalším krokem v této etapě byla inventura dat. Pracovní tým vytvořil dokument pro realizaci analýzy zpracovávaných osobních údajů ve firmě pro potřeby GDPR. Tento dokument obsahoval otázky, které se týkaly zpracování osobních údajů (jaké údaje, o kom, k čemu, odkud, komu se předávají, jaké dokumenty, atd) a byl předán všem vedoucím jednotlivých oddělení k vyplnění.

Vyplněné dokumenty byly pracovní skupinou analyzovány. Na základě zjištěných informací bylo vyhodnoceno, ve kterých oblastech zpracovávání osobních údajů, je třeba provést nápravná opatření tak, aby nedošlo k porušení nařízení GDPR. Všechny osobní údaje, které jsou zpracovávány nad rámec potřeb podniku, musejí být zlikvidovány ze všech nosičů a záloh.

II. etapa

Druhá etapa implementace se zabývá nastavením vnitřních procesů, a to včetně metodiky:

- co firma zpracovává,
- v jakém rozsahu,
- s jakou dobou platnosti,
- jak jsou údaje zabezpečeny,
- kdo a k čemu má přístup,
- kdo a jak řeší případný únik.

Dalším krokem této etapy je revidování všech směrnic, smluv a dokumentů z pohledu GDPR pro každé oddělení a nastavení zpracovatelských smluv. Dalším důležitým krokem je kontrola poskytnutých souhlasů se zpracováním.

III. etapa

Třetí etapa je zaměřena na použití vhodného technického řešení pro zajištění dostatečné bezpečnosti osobních údajů. Jedná se především o nastavení a přidělení přístupů oprávněných osob, pořízení samostatných disků pro práci s osobními údaji, atd.

Dále se tato etapa zabývá správou dat a nastavením mechanismů pro případné porušení.

12.2 Platnost nařízení

Jak už bylo zmíněno výše, platnost tohoto nařízení je od 25. května 2018. Během psaní této práce probíhala ve firmě Cross Zlín I. etapa implementace nařízení. Dále byl stanoven harmonogram dokončení jednotlivých fází tak, aby byla firma na platnost nařízení včas připravena. Z poskytnutých informací o implementaci GDPR vedením společnosti Cross Zlín je zřejmé, že příprava na toto opatření nebyla podceněna, avšak účinnost podniknutých kroků se projeví až později.

ZÁVĚR

Cílem této práce bylo zhodnocení současného stavu informačního managementu z hlediska informační bezpečnosti ve vybraném podniku. Výzkum se týkal společnosti Cross Zlín, která patří k předním světovým výrobcům dopravních technologií. Popis a hodnocení současného stavu informačního managementu vychází z interních materiálů společnosti a přímého dotazování informačního manažera. Z výsledků hodnocení bylo zjištěno, že podnik má informačního manažera a jsou vypracovány základní dokumenty informačního managementu. Dále bylo zjištěno, že má firma velmi kvalitní IT zázemí a od roku 2015 využívá moderní informační systém, který je spravován externí společností s pravidelnými aktualizacemi.

Pro hodnocení současného stavu informačního managementu byla vypracována SWOT analýza, čímž byly odhaleny silné a slabé stránky, hrozby a příležitosti v oblasti informačního managementu společnosti. Výsledek celkové bilance provedené analýzy je +0,8 což je kladný výsledek. Avšak identifikovaným slabým stránkám a potenciálním hrozbám je třeba věnovat pozornost. Proto byly vypracovány návrhy nápravných opatření, jež povedou ke zlepšení stávající situace. Navržená opatření se týkají především zlepšení kvalifikace zaměstnanců, kteří s informačním systémem pracují a zlepšení efektivity v jeho využívání. Proškolení pracovníků a implementování lépe nadefinovaných modulů je jedním z prvních kroků pro zlepšení současného stavu informačního managementu.

Pro zajištění co největší informační bezpečnosti má firma vypracovány směrnice ICT, které definují povinnosti správců a uživatelů informačních a komunikačních technologií v podniku. V diplomové práci byl pro potřeby analýzy popsán EZS podniku, který se podílí na zajištění informační bezpečnosti podniku. Analýzou byla zjištěna dvě vysoká rizika, která vyžadují aplikaci nápravných opatření. Jedním z těchto rizik je neúmyslná modifikace dat na sdílených discích. Tyto disky využívá společnost Cross Zlín pro ukládání a sdílení důležitých interních informací. Druhým z těchto rizik je neznalost interních předpisů, což může způsobit řadu problémů. Pro zjištěná rizika byla navrhnuta patřičná nápravná opatření. Tato opatření se týkají především lepší informovanosti zaměstnanců se stanovenými předpisy v oblasti IT, jelikož při nástupu do zaměstnání nejsou probírány. Je tak povinností každého zaměstnance se s těmito dokumenty seznámit samostatně, což nemusí každý ze zaměstnanců dodržovat.

V závěru práce je ještě uveden popis implementace nařízení o ochraně osobních údajů, tzv. GDPR ve firmě, který vzhledem k datu platnosti není nijak analyzován.

SEZNAM POUŽITÉ LITERATURY

[1] VYMĚTAL, Jan, Anna DIAČIKOVÁ a Miriam VÁCHOVÁ. Informační a znalostní management v praxi. 1. vyd. Praha: LexisNexis CZ, 2005, 399 s. Studijní texty. ISBN 80-86920-01-1.

[2] VODÁČEK, Leo a Antonín ROSICKÝ. Informační management: pojetí, poslání a aplikace. Vyd. 1. Praha: Management Press, 1997, 146 s. ISBN 80-85943-35-2.

[3] DOUCEK, Petr. Informační management. 1. vyd. Praha: Professional Publishing, 2010, 251 s. ISBN 978-80-7431-010-2.

[4] LUKÁŠ, Luděk, Petr HRŮZA a Milan KNÝ. Informační management v bezpečnostních složkách. 1. vyd. Praha: Ministerstvo obrany České republiky, 2008, 214 s. ISBN 978-80-7278-460-8.

[5] DOUCEK, Petr, Miloš MARYŠKA a Lea NEDOMOVÁ. Informační management v informační společnosti. 1. vyd. Praha: Professional Publishing, 2013, 264 s. ISBN 978-80-7431-097-3.

[6] BASL, Josef a Roman BLAŽÍČEK. Podnikové informační systémy: podnik v informační společnosti. 3., aktualiz. a dopl. vyd. Praha: Grada, 2012, 323 s. Management v informační společnosti. ISBN 978-80-247-4307-3.

[7] Co je to cloud. IGNUM s.r.o. [online]. [cit. 2018-04-03]. Dostupné z: https://www.webcloud.cz/cz/o-cloudu/co-je-to-cloud

[8] TVRDÍKOVÁ, Milena. Zavádění a inovace informačních systémů ve firmách. 1. Praha: Grada, 2000.

[9] VÁGNEROVÁ, Daniela. Příručka manažera XII - Supertipy CIO = CIO super tips: manage´s handbook. 1. Praha: TATE International, 2009. ISBN 978-80-86813-18-9.

[10] KOCH, Miloš a Viktor ONDRÁK. Informační systémy a technologie. Vyd. 3. Brno: Akademické nakladatelství CERM, 2008, 166 s. Učební texty vysokých škol. ISBN 978-80-214-3732-6.

[11] LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management. Zlín: Radim Bačuvčík - VeRBuM, 2015. ISBN 9788087500194.

[12] KAMENÍK, Jiří a František BRABEC. Komerční bezpečnost: soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur. Vyd. 1. Praha: ASPI, 2007, 338 s. ISBN 978-80-7357-309-6.

[13] JAŠEK, Roman. Informační a datová bezpečnost. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006, 140 s. ISBN 80-7318-456-7.

[14] POŽÁR, Josef. Manažerská informatika. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010, 357 s. ISBN 978-80-7380-276-9.

[15] ŽÁČEK, Jaroslav. Architektury informačních systémů. Ostravská univerzita [online]. [cit. 2018-04-08]. Dostupné z: http://www1.osu.cz/~zacek/sweng/2013/06.pdf

[16] DANIEL, Roman. Architektura IS: Klasifikace IS: TPS, MIS, EIS. Vysoká škola báňská - Technická univerzita Ostrava [online]. [cit. 2018-04-08]. Dostupné z: https://www.google.cz/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0ahUKEwiKjdCy8J7aAhXCJJoKHa7LDsIQFggguMAE&url=http%3A%2F%2Fhomel.vsb.cz%2F~dan11%2Fis2011%2F3%2520Informacni%2520systemy%2520-%2520architektura%2520IS.ppt&usg=AOvVaw2fyDth1rCWTxcmn0_qh7Rx

[17] POŽÁR, Josef. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005, 309 s. Vysokoškolské učebnice. ISBN 80-86898-38-5.

[18] ŘÍHA, Martin. Sociální sítě na pracovišti: Skvělý nástroj, ale i bezpečnostní hrozby. *System online* [online]. [cit. 2018-04-10]. Dostupné z: https://www.systemonline.cz/it-security/socialni-site-na-pracovisti-1.htm

[19] ŠUMBERA, Adam. Zavedení bezpečnosti informací v podniku dle ISO 27001. DOCPLAYER [online]. [cit. 2018-04-14]. Dostupné z: http://docplayer.cz/44519275-Zavedeni-managementu-bezpecnosti-informaci-v-podniku-dle-iso-27001.html

[20] Audit v oblasti bezpečnosti IS/IT. ITIL [online]. [cit. 2018-04-14]. Dostupné z: http://www.itil.cz/index.php?id=1037

[21] SWOT analýza. *Management Mania* [online]. 2017, 22.1.2017 [cit. 2018-05-04]. Dostupné z: https://managementmania.com/cs/swot-analyza

[22] PALÁN, Zdeněk. Analýza. *Andromeda* [online]. [cit. 2018-05-05]. Dostupné z: http://www.andromedia.cz/andragogicky-slovnik/analyza

[23] Brainstorming. *Management Mania* [online]. 2016, 9.12.2016 [cit. 2018-05-06]. Dostupné z: https://managementmania.com/cs/brainstorming

[24] Analýza a syntéza. VŠE [online]. [cit. 2018-05-06]. Dostupné z: https://nb.vse.cz/kfil/win/atlas1/analyza.htm

[25] Téma: *Interní data společnosti Cross Zlín, a.s.* Informace poskytl informační manažer společnosti, Zlín, od 1.2.2018 do 10.5.2018

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BF	Bezpečnostní fórum
CIO	Informační manažer
DSS	Systémy pro podporu taktického rozhodování
EIS	Systémy pro podporu vrcholového rozhodování
EZS	Elektronický zabezpečovací systém
FO	Fyzická ostraha
GDPR	Nařízení o ochraně osobních údajů
HDD	Pevný disk
HW	Hardware
ICT	Informační a komunikační technologie
IM	Informační management
IS	Informační systém
ISMS	Systém řízení bezpečnosti informací
LAN	Lokální síť
MIS	Manažerské informační systémy
MTZ	Materiálně technické zabezpečení
OIS	Systémy automatizační podpory
OTK	Oddělení testování a kvality
PC	Osobní počítač
PCO	Pult centrální ochrany
SW	Software
TCP/IP	Sada protokolů k počítačové komunikaci
TPS	Transakční informační systémy

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH