VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

NÁVRH ZAVEDENÍ ŘÍZENÍ BEZPEČNOSTI INFORMACÍ S DŮRAZEM NA BUDOVÁNÍ BEZPEČNOSTNÍHO POVĚDOMÍ V PŘÍSPĚVKOVÉ ORGANIZACI

PROPOSAL TO INTRODUCE INFORMATION SECURITY MANAGEMENT WITH EMPHASIS ON BUILDING SECURITY AWARENESS IN A CONTRIBUTORY ORGANISATION

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTORPRÁCE — Bc. David Chudoba

AUTHOR

VEDOUCÍ PRÁCE — Ing. Petr Sedlák

SUPERVISOR

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

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

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

Návrh zavedení řízení bezpečnosti informací s důrazem na budování bezpečnostního povědomí v příspěvkové organizaci

Charakteristika problematiky úkolu:

Úvod
Cíle práce
Teoretická východiska
Analýza současného stavu
Návrh řešení
Závěr
Seznam použitých zdrojů
Přílohy

Cíle, kterých má být dosaženo:

Hlavním cílem práce je na základě analytické části vypracovat návrh na zavedení systému řízení bezpečnosti informací a vypracování programu budování bezpečnostního povědomí. Návrh bude vypracováván s ohledem na obecné nařízení Evropské unie o ochraně osobních údajů. Tato práce se nebude zabývat systémem řízení bezpečnosti informací v celém jeho rozsahu, ale budou vybrány pouze části na míru organizaci.
Dílčími cíli jsou vypracování teoretické základny řešeného problému, vytvoření nezbytných analýz stávajícího stavu a vlastního návrhu řešení.

Základní literární prameny:

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

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

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

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

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

V Brně, dne 28. 2. 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ
L.S.

doc. RNDr. Bedřich Půža, CSc.
ředitel

doc. Ing. et Ing. Stanislav Škapa, Ph.D.
děkan

Abstrakt

Diplomová práce se zabývá systémem řízení bezpečnosti informací v organizaci společně s budováním bezpečnostního povědomí u zaměstnanců. Téma je zaměřeno na zpracování konkrétního návrhu šitého na míru příspěvkové organizaci, ve které se zpracovávají osobní a citlivé údaje. V procesu řízené změny budou jednotlivé kroky návrhu postupně implementovány za účelem zvýšení bezpečnosti a uvedení probíhajících procesů v organizaci do souladu s požadavky vyplývajícími z nařízení GDPR.

Klíčová slova

bezpečnost, systém řízení bezpečnosti informací, analýza rizik, ISO/IEC 27k

Abstract

The thesis deals with the information security management system in the organization together with building of security awareness among employees. The theme is focused on the custom made proposal for a contributory organization in which personal and sensitive data are being processed. In the process of controlled change, the individual steps of the design will be gradually implemented in order to increase the security and bring the ongoing processes in the organization into line with the requirements of the GDPR.

Key words

security, Information Security Management System, risk analysis, ISO/IEC 27k

Bibliografická citace

CHUDOBA, David. Návrh zavedení řízení bezpečnosti informací s důrazem na budování bezpečnostního povědomí v příspěvkové organizaci. Brno, 2019. Dostupné také z: https://www.vutbr.cz/studenti/zav-prace/detail/119861. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 10. května 2019 ……...…

podpis studenta

Poděkování

Děkuji vedoucímu diplomové práce Ing. Petrovi Sedlákovi za odbornou pomoc a cenné rady při zpracování této diplomové práce.

OBSAH

ÚVOD

Bezpečné používání výpočetní techniky se dnes skloňuje nejen v oblasti našeho školního, či pracovního života, ale zasahuje i do našeho soukromí. Nejslabším článkem počítačové bezpečnosti je zpravidla koncový uživatel. Organizace zaměstnávající osoby, které nemají dostatečné povědomí o bezpečném užívání této techniky, stojí před nelehkým úkolem. V první řadě musí zajistit bezpečnost celé sítě i jednotlivých prvků a dále pak musí zajistit průběžné vzdělávání svých zaměstnanců, aby předešla rizikům spojeným s narušením bezpečnosti celého systému. Každý z koncových uživatelů si musí uvědomit, že je nedílnou součástí širší počítačové bezpečnosti.

Společně s postupným rozšiřováním užívání ICT i v příspěvkových organizacích a v souvislosti s novou legislativou vyvstala potřeba intenzívně se zabývat systémem řízené bezpečnosti informací. Vzhledem k faktu, že organizace tohoto typu zpracovávají osobní údaje a v některých případech i údaje citlivé, je tedy na místě, že berou rizika s tímto spojená velmi vážně a jsou připraveni systém bezpečnostních opatření a doporučení postupně implementovat do praxe.

Systém řízení bezpečnosti informací je základním prvkem pro soulad činnosti organizace s opatřeními vyplývajícími z opatření obecného nařízení EU 2016/679 ze dne 27. dubna 2016 známého pod zkratkou GDPR. Aby organizace naplnila tyto požadavky, je nezbytné zavedení systému řízení bezpečnosti informací, při jehož implementaci je nutné brát zřetel na rozdíly v požadavcích ISMS a GDPR.

Tato diplomová práce je zaměřena na zpracování návrhu pro zavedení systému řízení bezpečnosti informací ve vybrané příspěvkové organizaci poskytující pobytové sociální služby seniorům. Z důvodu zpracovávání osobních i citlivých údajů je nezbytné u všech jejích zaměstnanců vybudovat kvalitní bezpečnostní povědomí, zkráceně SAE. Jak již bylo zmíněno, zavedení ISMS by mělo být prvním krokem organizace k souladu s nařízením GDPR. Souladu by mělo napomoci i vzdělávání všech osob v organizaci, které je zmiňováno a požadováno jak v ISMS tak v GDPR. Vzdělávání bude součástí programu budování bezpečnostního povědomí, které by chtěla organizace postupně implementovat. Cílem této diplomové práce je tedy navrhnout taková opatření, která pomohou konkrétní příspěvkové organizaci zavést systém řízení bezpečnosti informací na míru jejím potřebám a v souladu s GDPR.

1 TEORETICKÁ VÝCHODISKA PRÁCE

V teoretické části práce se zaměřím na vymezení základních pojmů, o které se budu v dalších kapitolách opírat a jejichž znalost je pro pochopení celého tématu nezbytná. Dále popíšu problematiku systému řízení bezpečnosti informací a obecného nařízení EU, známého pod zkratkou GDPR. V navazující kapitole objasním jednotlivé části modelu 7S. Poté navážu problematikou programu na budování bezpečnosti povědomí s problematikou komunikačních sítí.

1.1 Základní pojmy

Na začátku teoretické části diplomové práce považuji za nezbytné vymezit terminologii a základní pojmy, které budou dále v textu používány. Jejich přesné vymezení je nutné pro správné pochopení celé popisované problematiky.

1.1.1 Významná změna

Jedná se o změnu s potenciálem mít významný vliv na kybernetickou bezpečnost v současnosti nebo budoucnosti. Současně by tato změna představovala vysoké riziko (3).

1.1.2 Osobní údaje

Jako osobní údaj je označovaná informace o identifikované nebo identifikovatelné fyzické osobě, a to jejím přímým nebo nepřímým označením za pomoci určitého identifikátoru. Tím může být její jméno, číslo, síťový identifikátor. Dále to mohou být zvláštní prvky identity, kterých může být více nebo pouze jeden. Tyto prvky mohou být fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské (8, 16).

1.1.3 Anonymní údaje

U těchto údajů nelze ani správcem a ani nikým jiným opět navázat pouto s osobou, které patřily. Anonymní údaje jsou proto takové údaje, se kterými není možné spojit jakoukoliv identifikovatelnou nebo identifikovanou osobu (9).

1.1.4 Pseudonymizované údaje

U těchto údajů, na rozdíl od těch anonymních, existuje stále možnost přiřadit je k identifikované nebo identifikovatelné osobě. Proto hovoříme o zdánlivé anonymizaci a je třeba na tyto údaje stále nutné nahlížet jako na osobní údaje. Zpětné přiřazení se děje za pomoci dodatečných informací. Proto tyto informace je třeba uchovávat odděleně a musí na ně být vztažena technická a organizační opatření (9).

1.1.5 Správce

Správcem je ten, kdo určuje za jakým účelem a jakými prostředky jsou zpracovávány osobní údaje. Rovněž je tím, kdo primárně za zpracování osobních údajů zodpovídá bez ohledu na právní formu správce (16).

1.1.6 Zpracovatel

Zpracovatelem je subjekt zpracovávající osobní údaje za správce. Ani u zpracovatele není rozhodující jeho právní forma. Rozdíl mezi správcem a zpracovatelem je vztah podřízenosti. Správce zpracovateli určuje, jaké operace mohou být prováděny u osobních údajů. Případně může zpracovatel provádět pouze ty operace, které vyplývají z činnosti poskytované správci (9).

1.1.7 Profylaxe

Profylaxí se rozumí činnosti a opatření, která jsou prevencí proti vzniku poruch. V době, kdy je dané zařízení, služba nebo infrastruktura v provozu, provádí se pouze

operační diagnostika, která by měla odhalit případné odchylky od normálního či běžného stavu. V době mimo rutinní provoz probíhá komplexní testování všech funkcí, aby byla ověřena správná funkčnost zařízení. Dále jsou prováděny preventivní prohlídky všech částí mající za úkol včas odhalit částečně poškozené nebo opotřebené části zařízení, které by zapříčinily v brzké době jeho poruchu. Výměna komponent spadá do oblasti údržby. Mimo to je třeba provést předepsanou údržbu. U zařízení se jedná většinou o jeho vyčištění nebo seřízení. Údržbu můžeme provádět i u služeb, které jsou poskytovány online (10).

1.1.8 Aktivum

Jako aktivum lze označit vše, co má pro danou organizaci hodnotu, která je základní charakteristikou a může být při zapůsobení hrozby změněna. Aktiva můžeme rozdělit na hmotná a nehmotná (7, 11, 17).

Aktivem může být pro organizaci i vlastnost. Příkladem může být dostupnost dat nebo funkčnost systému. Dále to může být dobré jméno či reputace organizace. Z pohledu kybernetické bezpečnosti můžeme označit aktivem i konkrétní osoby. V tomto případě se však jedná o jejich znalosti a zkušenosti (17).

1.1.9 Riziko

Obecně lze konstatovat, že riziko znamená vystavení nepříznivým okolnostem. Jedná se o odhad pravděpodobnosti výskytu nebezpečí nebo události s nežádoucími následky. V tomto kontextu pak lze říci, že existuje potenciál zapůsobení konkrétní hrozby na konkrétní zranitelnost služby, aktiva a tak dále. Přesná definice rizika neexistuje (11, 17).

1.1.10 Zranitelnost

Pokud hovoříme o zranitelnosti, jedná se většinou o nějaký nedostatek nebo slabinu aktiva podrobovaného analýze (11).

Z hlediska bezpečnosti můžeme zranitelnost rozdělit na dva typy. Prvním typem je zranitelnost neznámá, které nám je skryta, nebo ještě nebyla objevena. Druhým typem

zranitelnosti je zranitelnost známá. Tuto známou zranitelnost dále můžeme dělit na opravenou, kdy například u softwaru byla vydána aktualizace, a na zranitelnost neopravenou, o které výrobce ví, ale ještě nebyla sjednána její náprava (17).

1.1.10.1 Integrita

Pod pojmem integrita se skrývá ochrana proti neautorizované změně informací (7).

Integritu můžeme popsat jako vlastnost úplnosti a přesnosti. Pro zjištění integrity používáme kontrolní součty, hashovací funkce nebo redundanci. V zabezpečení informací hovoříme o platnosti daných dat. Tyto chyby se většinou objevují při nastavování oprávnění, kterých následně útočník využije právě k provedení změn v datech uložených v databázích. Případně může útočník nalézt chybu v samotné databázi (17).

1.1.11 Důvěrnost

S pojmem důvěrnosti se setkáváme při zajišťování informací proti jejich neoprávněnému odhalení. Říkáme tedy, že k daným datům přistupují pouze ty osoby, které k nim přistupovat smí. Při zpracovávání většího množství informací je vhodné data začít klasifikovat (7, 17).

1.1.12 Dostupnost

Pod tímto pojmem se skrývá spolehlivé poskytování informací konkrétním a oprávněným subjektům v takovém čase, v jakém jej požadují. V případě, kdy budeme mít bezvadný systém z hlediska důvěrnosti a integrity, ale nebude zajištěn spolehlivý přístup podle potřeb uživatele, bude daný systém nevyužitelný (7, 17).

1.1.13 Bezpečnostní incident

Pokud hovoříme o bezpečnostním incidentu, znamená to, že selhala bezpečnost. Pro tyto případy by měly být stanoveny formální procesy, jak bezpečnostní incident řešit (7).

1.1.14 Data

Obecně lze konstatovat, že data chápeme jako fakta a poznatky vhodné pro další zpracování. Tedy daty zkráceně označujeme veškerá čísla, zvuk, text, obraz a další smyslové vjemy (15).

1.1.15 Informace

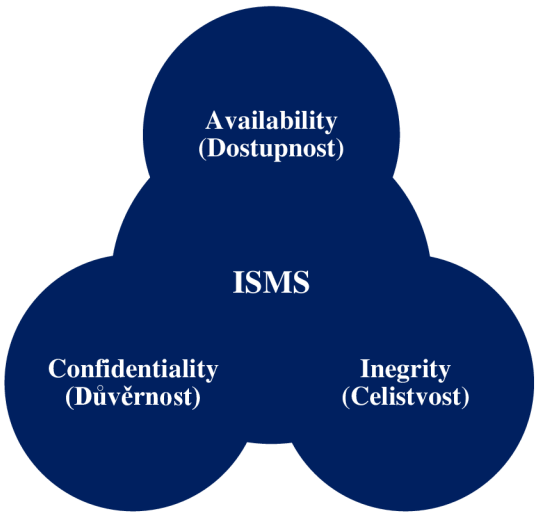
Pojem informace chápeme jako význam, který pro nás mají data. Kupříkladu data, která dokáže vnímat každý, má informace určitý význam a vztah pouze k jejímu příjemci (15, 18).

1.1.16 Speciální publikace NIST řady 800

Speciální publikace řady osm set vydávané americkým Národním institutem standardů a technologií byly vyvinuty pro účely podpory bezpečnosti a ochrany osobních údajů (3).

1.2 ISMS

Zkratka ISMS značí systém řízení bezpečnosti informací. Jak již ze samotného názvu vyplývá, jedná se o bezpečnost informací, kterou bude třeba řídit. V rámci tohoto procesu se bude třeba vypořádat se všemi pozitivními i negativními vlastnostmi dané změny, která v organizaci díky ISMS nastane (7).



Obrázek 1 Vztah triády CIA k ISMS (Zdroj: 17)

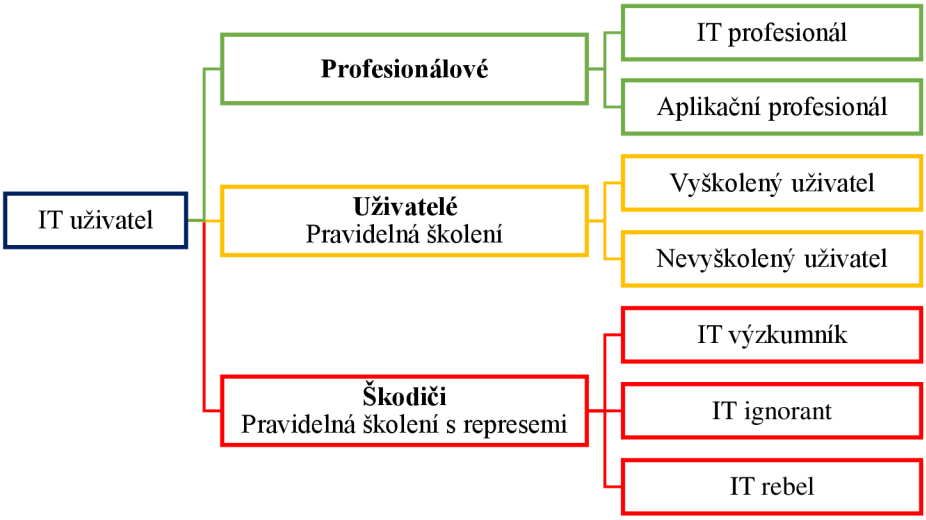
ISMS můžeme označit jako soubor pravidel, která se snaží zachovat důvěrnost, integritu i dostupnost také označovanou jako triáda CIA za pomoci procesu řízení rizik. Jistotou pro všechny zainteresované strany díky ISMS je, že řízení rizik je přiměřené. Kromě samotného řízení rizik jsou v rámci ISMS také chráněna aktiva a již zavedená opatření jsou kontrolována. Celý tento systém se promítá do všech procesů a do celého systému řízení organizace. Zároveň je jeho obrovskou výhodou, že jej lze aplikovat pouze na organizační jednotku, specifický informační nebo komunikační systém nebo jejich části (17).

ISMS vyžaduje komplexní a systémový přístup, který respektuje principy a prvky celého životního cyklu kybernetické bezpečnosti, a proto je založen na Demingově modelu PDCA. Princip tohoto modelu je zaměřen na postupné zvyšování kvality. Demingův model je rozdělen, stejně jako tento model, do následujících čtyř etap: plánuj, dělej, kontroluj, jednej (7).

1.2.1.1 Uživatelé jako zdroj rizik

Jako nejslabší článek bezpečnosti všech systémů je označován člověk. Zavedením ISMS v organizaci pouze výrazně snižujeme dopad rizik na aktiva na přijatelnou úroveň (17).

Technické zabezpečení je ve většině případů relativně snadné, jelikož jej lze vyřešit tím, že je včas implementován vhodný produkt. Tímto krokem vznikne řetěz s velmi silnými články. Následně do něj musíme zapojit poslední článek, kterým je uživatel. Jeho vstupem do každého informačního systémů přichází i největší zdroj bezpečnostních rizik. Z tohoto důvodu lze uživatele rozdělit do následujících tří skupin (7).



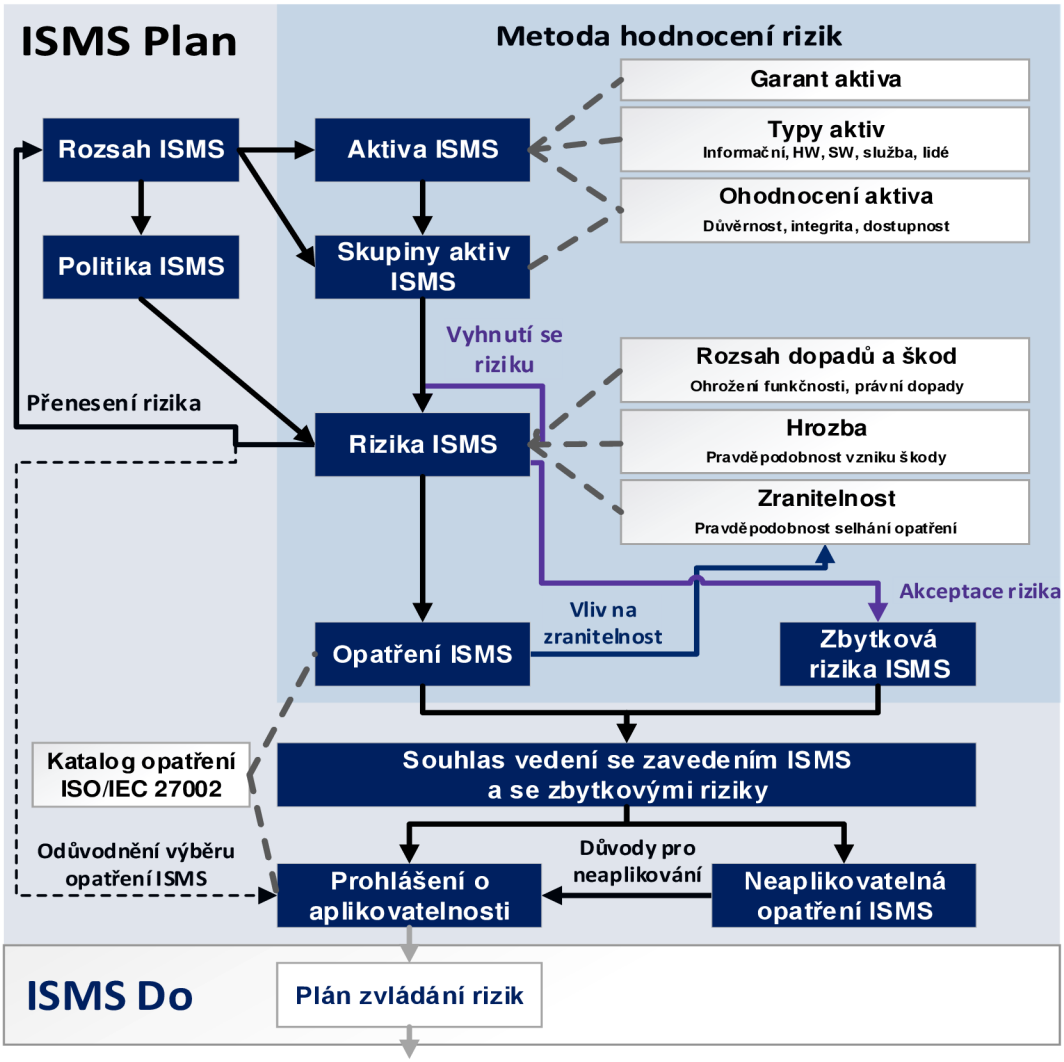
Obrázek 2 Schéma dělení uživatelů (Zdroj: 7)

1.2.2 Ustanovení ISMS

Prvním krokem zavedení systému řízení bezpečnosti informací je jeho ustanovení. To znamená, že je třeba stanovit jeho rozsah a hranice na míru konkrétní organizaci.

Rozsah a hranice systému se budou výrazně lišit dle rozsahu systému, počtu uživatelů, způsobu zpracovávání dat a jejich hodnoty. Nejdůležitějším faktorem, který systém ovlivní, jsou rizika, která mohou být reálně způsobena. Za jediný a správný systém řízení bezpečnosti informací považujeme ten, který je popsaný v normě ISO/EIC 27001 (21).

Bude tedy nutné zpracovat samotné politiky, metodiky hodnocení rizik a určit kritéria pro akceptaci rizik. V dalším kroku je třeba identifikovat informační aktiva a na ně působící rizika, u kterých je třeba určit jejich hodnotu. Závěrem je třeba zpracovat prohlášení o akceptovatelnosti opatření (7).



Obrázek 3 Řízení rizik v procesu ISMS (Zdroj: 22)

1.2.2.1 Řízení rizik

Problematika řízení rizik (risk management) se liší podle oblasti, ve které je řešena. Obecně je pod pojmem řízení rizik označován proces, při kterém se snažíme zamezit působení všech současných i budoucích vlivů na daný subjekt. Jeho součástí je rozhodovací proces, který navazuje na analýzu rizik. Lze také uvažovat o tom, že tyto faktory mohou působit pozitivně a mohou být organizací chápany jako příležitost. Konečným řešením každého řízení rizika je rozhodnutí, jenž může nabývat různých podob. Je-li úroveň rizik nepřijatelná, potom je třeba přijmout taková opatření, která daná rizika sníží. V případě přijatelných rizik, která jsou pro organizaci nějakým způsobem významná a byla by zdrojem výrazné ztráty, je třeba i na ně vytvořit plán preventivních opatření, aby byla redukována. Na ostatní rizika je třeba vypracovat

krizový plán. Je však třeba tato rizika znovu přezkoumat, zda je nelze ještě nějakým způsobem redukovat nebo eliminovat (11).

Z hlediska bezpečnosti se tento pohled výrazně neliší. Pouze se zde již konkrétně hovoří o činnostech spojených s riziky, jako například jejich hodnocení, výběr a zavedení opatření, která organizaci pomohou tato rizika zvládat. Dále je třeba sdílet informace o rizicích, ale též je sledovat a přezkoumávat (17).

1.2.2.2 Analýza rizik

K analýze rizik lze přistoupit dvěma způsoby. Prvním způsobem je kvalitativní metoda. U této metody je využito hodnocení rizik za pomoci určitého rozsahu. Tento rozsah může být pro příklad pravděpodobnostní, tedy hodnoty budou nabývat hodnot nula až jedna. Dále můžou být rizika ohodnocena slovně, nebo za pomoci rozsahu bodů. Jejich hodnota je většinou určena kvalifikovaným odhadem. Nevýhodou této metody při posuzování nákladů opatření je chybějící vyjádření hodnoty rizika (11).

Druhým způsobem jsou kvantitativní metody, které jsou založeny na matematickém výpočtu rizika za pomoci frekvence jeho výskytu a dopadu. Dopad rizika je finančně vyjádřen. Nevýhodou těchto metod je jejich výpočetní náročnost a riziko zahlcení vedení organizace množstvím strukturovaných dat, na které nebude schopno reagovat v dostatečně krátkém čase (11).

1.2.2.3 Vyhodnocení rizik

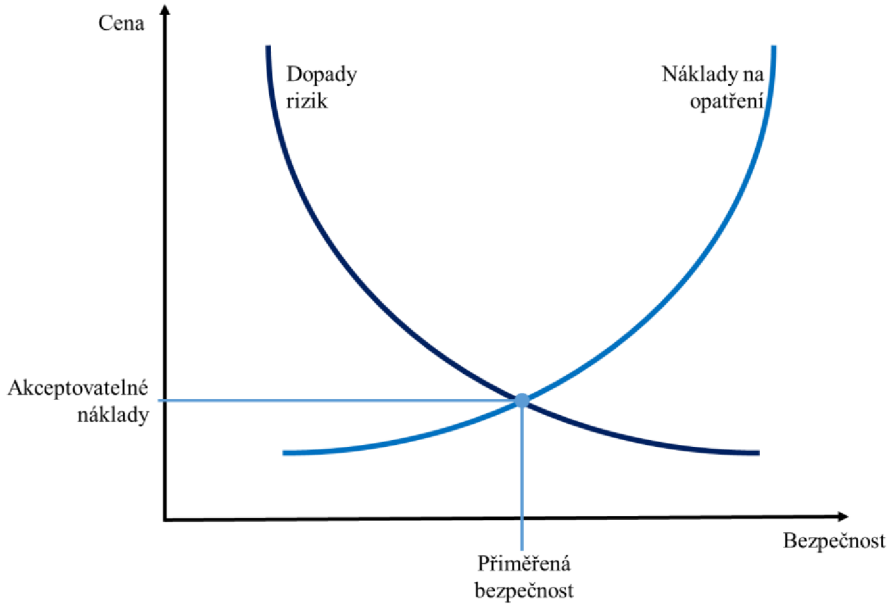
Vyhodnocením rizik určujeme jejich význam pro danou organizaci. Tento význam získáme porovnáním rizik vypočítaných nebo odhadnutých s kritérii ustanovenými v politikách ISMS (7).

1.2.2.4 Zvládání rizik

Při zavádění ISMS do organizace je třeba, aby hodnota vynaloženého úsilí a finančních prostředků odpovídala hodnotě aktiva a s ním souvisejícím množství rizik, která přináší. V praxi to znamená, že ať se zabýváme kterýmkoliv požadavkem na ustanovení,

implementování, udržování nebo na neustálé zlepšování systému řízení bezpečnosti informací, musíme mít neustále na mysli fakt, že jakýkoliv požadavek s sebou nese určité náklady. Tyto náklady bude muset daná organizace zaplatit, vyčlenit produktivní čas svých zaměstnanců a případně vynaložit další náklady spojené s konkrétním požadavkem (7, 13).

Daným požadavkem může být některé z opatření mířící k omezení nebo eliminaci hrozby směřující na vybraná aktiva organizace. Bylo by tedy velmi neefektivní, kdyby náklady byly vyšší nebo se rovnaly ceně samotného aktiva (7).



Graf 1 Přiměřená bezpečnost za akceptovatelné náklady. (Zdroj: 7)

1.2.2.5 Akceptace rizika

Riziko můžeme akceptovat vědomě či nevědomě. Akceptaci rizika můžeme označit jako retenci rizika. K vědomé retenci dochází, je-li riziko rozpoznáno, ale není proti němu vytvořeno nebo uplatněno žádné opatření. V opačném případě není riziko rozpoznáno a je tedy zadrženo nevědomě. Dále můžeme riziko akceptovat dobrovolně. V tomto případě souhlasíme s případnou ztrátou, které s sebou riziko nese. Většinou je k dobrovolné retenci přistupováno, protože veškerá aplikovatelná opatření by

převyšovala svými náklady hodnotu rizika. Neplatilo by zde pravidlo bezpečnosti za přijatelné náklady (7, 11).

1.2.2.6 Prohlášení o aplikovatelnosti

Prohlášení o aplikovatelnosti ukončuje fázi ustanovení ISMS. Jedná se o dokument, který shrnuje a popisuje vybraná opatření aplikovaná v ISMS organizace. Nebude se jednat pouze o nově navržená opatření, ale taktéž o opatření, která již jsou v organizaci zavedena. U nově vybraných opatření budou v tomto dokumentu vytyčeny cíle včetně důvodu, proč byla vybrána. Za zpětnou kontrolu považujeme poslední část dokumentu, ve které popisujeme důvody, proč nejsou vybrána konkrétní opatření z přílohy A normy ISO/EIC 27001 (7).

1.2.3 Zavádění a provoz ISMS

Tento úsek životního cyklu ISMS se specializuje na uplatnění veškerých bezpečnostních opatření stejným způsobem, jako byla navržena v předchozím úseku při ustanovení ISMS. Příprava dílčích plánů, ve kterých jsou zmíněny přesné termíny, odpovědné osoby a podobně, je nejdůležitější. Dokumentace by měla obsahovat veškerá bezpečnostní opatření v Příručce bezpečnosti informací. Zároveň je nezbytné, aby u všech manažerů a uživatelů došlo k vysvětlení bezpečnostních principů (17).

V procesu implementace ISMS je nutné formulování plánu zvládání rizik a zahájení jeho implementace. Dále je nutné uvedení plánovaných bezpečnostních opatření a formulace Příručky bezpečnosti informací upřesňující předpisy a cestu použitých opatření v určených oblastech bezpečnosti informací. Nutností je také upřesnění stylu měření působení bezpečnostních opatření, sledování určených ukazatelů, zavedení kroků a dalších opatření pro bleskové odhalení a reakci na bezpečnostní události, řízení dokumentů, zdrojů a záznamů ISMS (21).

1.2.4 Monitorování a přezkoumání ISMS

Zajištění funkční zpětné vazby je hlavní povinností tohoto úseku nastolení ISMS. Ve spojitosti s tímto nárokem by proto mělo dojít k přešetření veškerých použitých bezpečnostních opatření a jejich implikací na ISMS. Samotné prověření začíná dozorem nad osobami odpovědnými za práci ze strany jejich nadřízených či bezpečnostním manažerem. Důležitým článkem je také nezávislé odhadnutí fungování a účinnost ISMS za pomoci interních auditů ISMS. Celkově je nedůležitější příprava dostatku podkladů o opravdovém fungování ISMS. Tyto podklady jsou důležité pro přezkoumání, zda je uskutečnění ISMS podle obecných potřeb organizace. Nutností pro nastolení ISMS je sledování a prověření funkčnosti uplatněných bezpečnostních opatření uskutečněnými interními audity ISMS a zda jejich záběr pokryje celý rozsah ISMS v organizaci. Nezbytná je také příprava zprávy o stavu ISMS na jejímž základě může dojít k přehodnocení ISMS na stupni vedení organizace (21).

1.2.5 Údržba a zlepšování ISMS

Údržba a zlepšování je poslední úsek celé implementace ISMS v organizaci. V této fázi by mělo docházet ke sběru podnětů k vylepšení ISMS a k nápravě všech nedostatků – takzvaných neshod, které ISMS obsahuje. Nezbytností je nastolení identifikované varianty vylepšení ISMS, zejména podle přehodnocení vedení a uskutečnění odpovídajícího opatření k nápravě a preventivní opatření pro odstranění nedostatků (21).

Údržba a zlepšování ISMS pojednává také o neshodě, pod kterou si lze představit nesplněný požadavek. Dále pojednává o nápravě, což je postup pro odstranění zjištěné neshody. Pod opatřením k nápravě si můžeme představit postup k odstranění příčiny zjištěné neshody nebo jiného nežádoucího stavu. Postup k odstranění příčiny případné neshody nebo jiného případně nežádoucího stavu se nazývá preventivní opatření (7).

1.3 GDPR

V této podkapitole bude porovnáno obecné nařízení Evropské unie o ochraně osobních údajů se systémem řízení bezpečnosti informací.

1.3.1 Obecně o GDPR

Toto nařízení nahrazuje dříve platnou směrnici 95/46/ES, která se také zabývala ochranou zpracování osobních údajů fyzických osob a volném pohybu daných údajů. Nutnost změny vyplynula ze zastarání této směrnice především v oblastech automatizovaného zpracování, profilování a podobně, které je v současné době mnohem komplexnější. V České republice toto nařízení zohledňuje Zákon o zpracování osobních údajů č. 110/2019 Sb. (8, 23).

1.3.2 Vztah GDPR s normami ISO 27000

Porovnáním GDPR s normou ISO/IEC 27001 zjistíme, že GDPR více podporuje práva majitelů dat, kteří mají možnost svá data přenést, vymazat a také má právo být informován. V případě, že normu ISO 27001 doplníme doporučeními normy ISO 27018, splníme tím většinu z požadavků GDPR (8).

Motivací organizace k posouzení rizik vyplývajících ze zpracování osobních údajů jsou vysoké pokuty plynoucích z nedodržení nařízení GDPR. Pro nalezení souladu GDPR a normy ISO 27001 podle opatření A.8.2.1. říkající, že informace musí být ohodnoceny s ohledem na zákonné požadavky. Z tohoto důvodu je třeba zpracování osobních údajů při analýze rizik ohodnotit jako vysoce kritické (8, 12).

Povinností organizace dle GDPR je oznámit incident porušení integrity dat do dva a sedmdesáti hodin jak na Úřad na ochranu osobních údajů, tak osobám, pro které by tento incident mohl znamenat vysoké riziko pro jejich práva a svobodu. K tomu napomáhá zavedení opatření A16.1, které klade organizaci za úkol, aby zajistila odpovídající a efektivní postoj ke zvládání incidentů bezpečnosti informací (8, 12).

Opatření A.8 normy ISO 27001 pomáhá organizaci do informační bezpečnosti zařadit i osobní údaje u nichž je třeba provést identifikaci. Dále je třeba dle GDPR u všech údajů uvést, po jakou dobu jsou uchovávány, kde jsou uchovávány a kdo má k daným údajům přístup. (8) Řízení přístupu k informacím je v ISMS zajištěno opatřením A.9.1, které klade organizaci za cíl omezení přístupu pouze k takovým informacím, které jsou potřebné k výkonu v rámci organizace (12).

Dle opatření A.7.2.2 je povinností organizace zajistit odpovídající vzdělání a školení pro zvyšování bezpečnostního povědomí všem svým zaměstnancům případně i smluvním stranám, je-li to potřeba (8).

1.4 Mc Kinley model 7 faktorů

V zájmu organizace je rovnoměrně rozvíjet sedm vzájemně závislých faktorů působících uvnitř organizace, které jsou velmi důležité pro její úspěch (11, 20).

1.4.1 Strategie

První z těchto faktorů je strategie organizace, která by měla vycházet z představ jejího zřizovatele a jejího konkrétního poslání. Většinou bývá strategie ukryta v písemnostech dané organizace nebo ji lze vysledovat ze směru, kterým se organizace ubírá. Většinou se setkáme s volně formulovanými myšlenkami a činnostmi, kterým jsou podřizovány veškeré aktivity v organizaci, a které by organizaci měly přinést konkurenční výhodu. Výhoda bude o to větší, pokud dvě konkurenční organizace využívají stejné a momentálně nejlepší dostupné technologie, které již nelze nijak vylepšit. Ta bude spočívat v podobě efektivnějšího využití vnitřních, v tomto případě lidských zdrojů tak, aby byl co nejlépe a nejefektivněji uspokojen trh a zájem zřizovatele organizace. Pro optimalizaci uvedeného rozhodovacího operativního problému může být aplikována teorie front. Odlišení organizace od její konkurence může mít dvě podoby. Jednak se může chtít odlišit od ostatních, nebo s nimi bojovat snížením svých cen díky zacílení na minimalizaci nákladů (11, 20).

1.4.2 Struktura

Druhým faktorem je organizační struktura mající za úkol optimální rozdělení pravomocí, kompetencí a úkolů mezi jednotlivé zaměstnance. Organizační struktury se vyvíjely od těch jednodušších, liniových, po ty složitější, maticové, co nejvíce využívající výhod svých předchůdců, čímž by měly odstranit jejich nevýhody při zachování maximální jednoduchosti. Teprve na základě strategie organizace by měla být vytvořena organizační struktura, která by ji měla co nejvíce podporovat (11, 20).

1.4.3 Systémy

Informační systémy napomáhají zpracovávat informace, které jsou na nižších stupních organizační struktury masově zpracovávány a zachycovány nejpřesněji, jak je to jen možné. Při postupu organizační strukturou jsou data zobecňována pro co nejjednodušší řízení organizace. Na nejvyšší úrovni se jedná o tvorbu firemní strategie (11, 20).

1.4.4 Styl řízení

Organizaci lze řídit za pomoci tří stylů. Prvním z nich je autoritativní, který nedává zaměstnancům žádnou možnost podílet se na řízení. Ti slouží pouze jako zdroj informací pro rozhodování vedoucích pracovníků. V druhém, demokratickém stylu jsou jednotlivá rozhodnutí vedoucích pracovníků diskutována s jejich podřízenými. Odpovědnost však stále zůstává na vedoucím pracovníkovi. Poslední styl zvaný laissez-faire nechává volný průběh, s minimálními zásahy vedoucího v procesu rozdělení a postupů prací (11, 20).

1.4.5 Spolupracovníci

Spolupracovníci jsou nejpodstatnějším a zároveň nerizikovějším faktorem na cestě úspěchu organizace. Těmi nejvíce rizikovými jsou zaměstnanci, kteří přicházejí do přímého kontaktu se zákazníky. Organizace by měla vytvářet u svých zaměstnanců pocit ztotožnění se s firmou, její strategií a jejím kolektivem, což by mělo vést k dlouhodobé spolupráci a spokojenosti obou stran. S tím souvisí fakt, že zaměstnanci budou efektivnější a loajálnější, pokud budou moci pracovat v atraktivním prostředí a budou-li správně motivováni (11, 20).

1.4.6 Schopnosti

I schopnosti personálu jsou důležité pro úspěch firmy a měly by být rozvíjeny napříč celou organizační strukturou. Pro úspěch tohoto faktoru je třeba nezaměřovat se pouze na technické a výrobní schopnosti, ale i u nižších vrstev organizace zvyšovat schopnosti v oblastech práva, ekonomie a infomačních technologií. Podle aktuálních požadavků

a změn v organizaci by měl být úspěšný manažer schopen rychlé reakce. Takové manažery můžeme označit za mistry změny. Stejně jako u ostatních faktorů není vhodné pro úspěch organizace některý z faktorů protěžovat (11, 20).

1.4.7 Sdílené hodnoty

Posledním faktorem jsou sdílené hodnoty označované též jako firemní kultura. Ta je tvořena souhrnem názorů a hodnot, jež jsou běžně a nenuceně dodržovány uvnitř organizace všemi zaměstnanci, aniž by musely být formálně vyjádřeny. Díky jejich působení je vnitřní prostředí organizace vnímáno personálem pozitivně. Je tedy nutné si uvědomit, že firemní kultura je neodmyslitelně spjata s dříve popsaným faktorem, kterým jsou spolupracovníci (11, 20).

1.5 Program budování bezpečnostního povědomí – SAE

V této kapitole budou popsány nejlepší způsoby pro budování bezpečnostního povědomí v organizaci. Bude popsáno vytvoření programu budování bezpečnostního povědomí (dále označován jen jako program), jeho rozvoj, implementace a jak se o program starat během jeho užívání v organizaci. Touto problematikou se zabývají speciální publikace NIST SP 800-50. Publikace slouží jako návod a soubor nejlepších praktik pro zavedení programu pro budování bezpečnostního povědomí v organizaci.

1.5.1 Budování bezpečnostního povědomí jako spojité prostředí

Tato kapitola popisuje budování bezpečnostního povědomí jako jednoho uceleného navzájem propojeného celku. Ten je možné chápat jako prostředí, které je prostředkem pro šíření potřebných informací pro vykonávání práce všech uživatelů napříč organizací (1).

Toto prostředí je rozděleno do čtyř oblastí podle úrovně vzdělání uživatelů v organizaci. Do první oblasti jsou zařazeni v první fázi všichni uživatelé a je třeba u nich provést zvýšení bezpečnostního povědomí. Úsilí pro zvýšení bezpečnostního povědomí by mělo vést ke změně chování uživatelů nebo jim pomoci s osvojením bezpečnostních postupů,

které jsou osvědčeny a jsou účinné pro zachování bezpečnosti organizace. Zvyšování bezpečnostního povědomí není bráno jako výcvik. Má za cíl umožnit jednotlivým uživatelům získat schopnost rozpoznat bezpečnostní událost a jak na ni zareagovat. Způsob, jak je možné atraktivně u uživatelů bezpečnostní povědomí budovat, je vytvořit informační materiál nebo setkání uživatelů a deklarovat tyto prostředky pro konkrétní téma. Pro lepší pochopení můžeme použít příklad ochrany před viry. Seznámíme uživatele s tím, co vlastně virus je, scénář při infikaci ICT systémů virem a co může uživatel udělat, když se virus objeví (2).

Po prvním procesu je předpokládáno, že uživatelé získali základní bezpečnostní povědomí a vzdělání. Mělo by se jednat o všechny uživatele, kteří mají přístup do některého z informačních systémů uvnitř organizace. Podstatným rozdílem od předchozího kroku je učení uživatelů relevantních a potřebných bezpečnostních dovedností k vykonávání své náplně práce v organizaci. Při procesu učení je předpokládáno, že již uživatel má základy bezpečnostního povědomí a je základně bezpečnostně vzdělán. Proces učení nemusí být formálně zaštiťován vzdělávací organizací například vysokou školou, ale je možné využít jejich materiálů pro vzdělávání. Příkladem může být kurz bezpečnosti pro správce ICT systému detailně řešící řízení v oblastech technologie, provozu a správy, které by měly být zavedeny (1).

Ve třetí fázi procesu vzdělávání jsou integrovány do jednoho společného souboru vědomostí veškeré dovednosti a kompetence z různorodých specializací. V této úrovni by se již mělo jednat o uživatele, specialisty na bezpečnost informačních technologií, kteří jsou schopni předvídat a aplikovat dříve získané zkušenosti na nové události. Narozdíl od výuky se v této oblasti hovoří o školení (2).

Oblast profesního rozvoje je zacílena od začátečníků po profesionály, kteří by měli mít dostatečnou úroveň znalostí a kompetencí pro výkon své práce. Uživatelé této úrovně potvrzují své znalosti a dovednosti za pomoci certifikace. Pokud je certifikace úspěšná, můžeme to označit termínem profesionalizace. Certifikáty existují jako obecné a technické. Obecná certifikace potvrzuje spíše znalosti ze základů bezpečnosti ICT. Technická certifikace se již zaměřuje na konkrétní technické bezpečnostní oblasti, jako jsou například bezpečnostní chyby u jednotlivých platforem a operačních systémů. Tyto

certifikace pak slouží jak zaměstnancům při vyjednávání o svém finančním ohodnocení, tak i zaměstnavatelům při rozhodování u pracovních pohovorů (1).

1.5.2 Jak vytvořit program bezpečnostního povědomí

Nyní bude popsán způsob hodnocení potřeb organizace a jak na jejich základě vypracovat a schválit strategii pro vybudování bezpečnostního povědomí na míru pro danou organizaci (1).

Při vytváření programu budování bezpečnostního povědomí je třeba myslet na fakt, že uživatelé jsou tou největší skupinou pracující s ICT aktivy a jsou také hlavní skupinou vytvářející nejvíce neúmyslných chyb a bezpečnostních incidentů v systémech informačních technologií. Pokud chceme ve své organizaci budovat bezpečnostní povědomí je zapotřebí, aby uživatelé:

- chápali svoje postavení uvnitř organizace a zodpovědnosti z něj vyplývající vůči organizaci a její bezpečnostní misi,
- chápali bezpečnostní politiky, procesy a postupy nastavené společností,
- měli dostatečnou a aktuální úroveň bezpečnostních znalostí, které jsou potřebné a dostupné pro řízení rozmanitých činností v oblastech technologických, managementu nebo provozu a byli tak schopni chránit aktiva, za která jsou zodpovědní (2).

Na výše zmíněné požadavky musíme klást o to větší důraz a požadavky u organizací, kde jsou lidé, na rozdíl od technologie, tím klíčovým aktivem pro chod společnosti (1).

Při vytváření programu si může organizace volit mezi třemi modely. První model je plně centralizovaný. Odpovědnost a náklady na provoz připadají pouze na jeden centralizovaný prvek, který je zodpovědný za veškeré bezpečnostní politiky, strategie a jejich implementaci pro celou organizaci (2).

Druhý model je částečně decentralizovaný. Posouzení potřeb a určení strategie programu zůstává stále na centrálním prvku. Konkrétní strategie, politiky a rozpočet si však již určují samotné organizační jednotky. Tento model je určený pro větší organizace s rozsáhlejším geografickým rozložením (1).

Třetí model je plně decentralizovaný. V tomto modelu jsou převedeny veškerá posouzení potřeb, sestavování rozpočtů, vytváření politik a tvorba materiálů pro program na jednotlivé organizační jednotky. Pro kontrolování správnosti tohoto programu centrálním prvkem vzniká spousta výkazů ze strany organizačních jednotek. Tento model je vhodný pro obrovské nadnárodní organizace, u kterých může vzniknout potřeba mít různé programy pro různé organizační jednotky v návaznosti na jejich geografické umístění (1).

1.5.3 Rozvoj bezpečnostního povědomí

Tato část programu SAE je zaměřena na rozvoj již dostupných materiálů pro školení. Bude zkoumán rozsah jejich obsahu a jak dané materiály v případě potřeby rozšířit, aby co nejlépe pokrývaly současné potřeby organizace. Taktéž jak je třeba se zachovat v případech, kdy je nutná pomoc třetí strany (2).

1.5.4 Jak implementovat program budování bezpečnostního povědomí

Jak účinně komunikovat při zavádění programu pro budování bezpečnostního povědomí, je třeba se naučit v této části programu SAE. Dále je třeba se věnovat problému distribuce s poskytováním informačních nebo vzdělávacích materiálů během samotné implementace, ale i během chodu programu v organizaci (1).

1.5.5 Jak o program pečovat po implementaci

Dalším potřebným krokem v životním cyklu programu SAE je jeho udržování v co nejaktuálnější podobě. Dále je třeba určit způsob zjišťování, nakolik je program stále účinný. Taktéž je třeba určit, jak nejúčinněji a nejefektněji získat zpětnou vazbu od účastníků programu (1).

1.6 Infrastruktura komunikačních systémů

Aby byla komunikační infrastruktura spolehlivá, je nutné začít od kvalitního projektování sítě. Zpracovaný projekt by měl zajistit jak dostatečnou kvalitu sítě, tak její spolehlivost. Tyto požadavky by měly být splněny tím, že bude dodrženo několik nezbytných základních pravidel. Tato pravidla budou sloužit jako návod, jak udělat kvalitní návrh komunikačních systémů. Pro ucelenost informací budou v dalších podkapitolách tato pravidla rozčleněna, doplněna a diskutována.

1.6.1.1 Proč nepodceňovat návrh infrastruktury komunikačního systému

Pro návrh a realizaci spolehlivé a finančně příznivé infrastruktury komunikačního systému je nutné se zabývat problematikou jejího návrhu s dostatečnou pozorností, pečlivostí a dodržovat při tom dále popsaná fakta. Kromě spolehlivosti a finanční stránky by nás také mohla motivovat dlouhodobými statistikami z praxe prokázaná následující fakta:

- kabelážní systém představuje 3-5 % z celkové investice do komplexního komunikačního systému,
- selhání komunikačního systému je ze 70 % zapříčiněno kabelážním systémem (10).

1.6.1.2 Základní pojmy

Pro snadnější orientaci v řešené problematice samotného návrhu je nutné si vymezit několik základních pojmů, jejichž pochopení zajistí kvalitní základ pro samotný návrh. Podstatné je pochopit co vlastně samotná komunikační infrastruktura je. Je to soubor technických prostředků, které nám zajišťují možnost komunikovat. Můžeme zde najít analogii se silniční dopravou (10).

Vzhledem k faktu, že komunikační infrastruktura dokáže splnit požadavky pro několik specializovaných komunikačních aplikací, můžeme u nich hovořit o tak zvané konvergenci. Ta může být pasivní a aktivní (10).

Pasivní konvergenci můžeme chápat tak, že po stejném fyzickém přenosovém kanále posíláme jinou službu nebo data, než pro která byl komunikační kanál vyvinut. Příkladem mohou být hlasové služby posílané po stejné strukturované kabeláži, která byla původně navržena pro internet (7, 10, 14).

Aktivní konvergencí chápeme přenos služeb a dat za pomoci IP protokolu, který byl původně vyvíjen pouze pro přenos dat mezi PC. Proto u aktivní konvergence je nutno využít aktivních prvků umožňující ve stejný okamžik přenos několika různých služeb nebo dat po jednom přenosovém médiu (7, 10, 14).

Při použití kombinace konvergencí můžeme danou síť označit jako Next Generation Networks (NGN), tedy jako sítě následující generace. Takové sítě jsou dnes běžně používané v telekomunikacích, firmách i domácnostech. Využíváme tedy aktivní konvergence pro data, vysílání a telekomunikace do jednoho komunikačního protokolu, který je přenášen po datovém přenosovém médiu (7).

Komunikační síť je třeba rozčlenit na páteřní sekci a horizontální sekci. Páteřní sekce je vždy topologií hvězdy. Pokud v dané síti chceme využít redundance, změní se nám topologie na neúplný polynom. Tato sekce nám propojuje datové rozvaděče. Dle ČSN EN 50173 ji realizujeme pouze optickým vedením. Horizontální sekce dle dříve uvedené normy bývá realizována metalickým vedením, ale může zde být i vedení optické a její topologie je vždy hvězda. Tato sekce propojuje datový rozvaděč se zásuvkou na pracovišti, kde potom bude umístěno koncové zařízení s komunikačním rozhraním. Tomuto propojení mezi koncovým zařízením a zásuvkou říkáme pracovní sekce. Datovým rozvaděčem označujeme místo, kde jsou umístěny přepojovací panely, organizéry kabeláže, aktivní prvky a případně další zařízení (10).

1.6.1.3 Vstupní analýzy

První potřebnou analýzu pro návrh infrastruktury komunikačních systémů je ta, která nám popisuje současný stav. Měl by z ní vyjít verdikt a tom, jestli budeme schopni použít celou současnou infrastrukturu nebo jsme schopni použít pouze její část anebo za třetí, zdali nebude výhodnější současnou infrastrukturu zrušit a začít budovat infrastrukturu komunikačních systémů úplně od začátku (10).

Dalším krokem je pak analýza požadavků investora. Zde je třeba si uvědomit, že se od investora spíše očekává vyjádření požadavků na současné i budoucí využití sítě než na technické řešení dané sítě. Měli bychom dostat základní vstupní informace o tom, kolik pracovních stanic bude síť obsluhovat, jaká je požadovaná šířka pásma. Další otázkou je jakou očekává životnost a náklady spojené se sítí. Dále bychom se měli od investora dozvědět, v jakém prostředí bude infrastruktura provozována a jaká jsou případná fyzická omezení (19).

1.6.1.4 Návrh obecného schématu sítě

Po všech nezbytných předchozích analýzách nyní přejdeme na další část, kterou je návrh obecného schématu sítě. Ten představuje první pracovní verzi, kde se umístí jednotlivé uzly sítě. Zde je nutností uzly popsat a stanovit počet portů, které budou z daného uzlu obsluhovány. V dalším kroku je třeba vypočítat šířku pásma pro jednotlivé pracovní stanice. Po všech potřebných výpočtech je třeba ověřit, zda je stále dostačující šířka pásma, aby někde nevzniklo úzké hrdlo (10).

1.6.1.5 Návrh technických prostředků

V této poslední fázi je zapotřebí vybrat správné technické prostředky případně řešení. Tedy je zapotřebí se rozhodnout jakou chceme použít hustotu řešení, což znamená, kolik bude nutné nainstalovat techniky do jednotlivých rozvaděčů. Poté je třeba vybrat takovou techniku, která splní naše požadavky na rychlost a zátěž sítě. Následně je nutné ošetřit podle politik dané organizace bezpečnost dané sítě. Závěrečným krokem je určení garance komunikačního systému, neboť ta se bude lišit podle prostředí a účelu, pro který je daná síť realizována (10).

2 ANALÝZA PROBLÉMU A SOUČASNÉ SITUACE

V této kapitole bude představena samotná organizace, se kterou jsem v rámci své diplomové práce spolupracoval. Bude popsán současný stav jejích informačních technologií, datových toků, ale také způsob řízení a vedení organizace. Bude provedena analýza rizik a vlivů působících jak z okolního, tak z vnitřního prostředí organizace.

2.1 Představení organizace

Příspěvková organizace, kterou jsem si vybral, a se kterou jsem navázal úzkou spolupráci, se nachází ve městě se čtyřiceti tisíci obyvatel. Jedná se o registrovaného poskytovatele pobytových sociálních služeb, který se řídí ustanovením zákona č. 108/2006 Sb. o sociálních službách. Z hlediska právní formy se jedná o příspěvkovou organizaci zřízenou územním samosprávním celkem – krajem, zapsanou v obchodním rejstříku.

Tato konkrétní organizace poskytuje dvě pobytové sociální služby na základě zákona č. 108/2006 sb. o sociálních službách, které jsou zacíleny na seniory. Z důvodu zachování anonymity, což bylo předem dohodnutou podmínkou, uvádím, že v organizaci je pečováno maximálně o 200 klientů. Pobytovou službu zajišťuje celkově asi 110 pracovníků zaměstnaných na hlavní pracovní poměr v nepřetržitém provozu. Taktéž organizace zaměstnává osoby na dohody o provedení práce a dohody o pracovní činnosti. Celkový finanční rozpočet, se kterým daná organizace hospodaří, je v současnosti cca 70 milionů Kč.

2.2 Motivace společnosti pro zvýšení bezpečnosti

Již řadu let se organizace snaží udržet bezpečnost na takové úrovni, aby chránila samu sebe před okolím, ale i naopak. Přes veškerou snahu však lze nalézt oblasti, které byly v minulosti zanedbávány, nebo jim nebyl přidělován takový důraz a byly řešeny pouze v případech, kdy si pozornost vyžádaly okolnosti. Tato částečná řešení mnohdy přinášela náklady bez návaznosti na komplexní řešení problematiky. Aby organizace těmto negativním vlastnostem současného řízení bezpečnosti v budoucnu předešla, chce

tomuto řízení dát přesný řád. To zajistí, že do procesů výběru, rozhodování a řešení vzniklých situací nebude vnášen chaos a nahodilost, ale bude vše řízeno v symbióze se strategií a střednědobým plánem rozvoje organizace.

Vzhledem k faktu, že organizace v rámci provozu své činnosti nutně musí zpracovávat osobní a citlivé údaje, jsou nutné změny v řízení bezpečnosti informací. To by mělo do organizace zavést jasný řád, jak s informacemi bezpečně nakládat, aby nemohly být ukradeny, nebo zneužity. Bezpečnostní incident tohoto charakteru by byl pro organizaci velmi ohrožující, proto je v této oblasti vysoce motivována.

Z důvodu zpracovávání citlivých údajů je organizace motivována k tomu mít řádně proškolený personál v oblasti bezpečnosti. Je to jeden z nejdůležitějších kroků pro potlačení bezpečnostních incidentů a neúmyslných chyb, které nejvíce vznikají z důvodu nevědomosti personálu.

V organizaci neexistuje samostatná organizační jednotka starající se o ICT a jeho bezpečnost. ICT je tedy řízeno jedním z vedoucích pracovníků, který je vytížen jinými pracovními činnostmi natolik, že péči o ICT byla zajištěna jako služba od externí firmy. Jelikož není vypracován mezi organizací a externí firmou žádný SLA dokument, je sice péče o ICT poskytována na vysoké úrovni, ale veškerá zodpovědnost zůstává stále na interním zaměstnanci a v konečném důsledku na řediteli celé organizace. Toto jsou hlavní důvody vysoké motivace pro vytvoření a zavedení směrnic a provozních řádů pro užívání ICT včetně jasně definované zodpovědnosti jednotlivých uživatelů.

2.3 Současný stav

V této kapitole bude popsán současný stav, ve kterém se spolupracující organizace nachází. Pozornost bude zaměřena na oblasti zahrnující serverovnu, počítačovou síť, zálohování dat a aktuální stav výpočetní techniky v organizaci. V těchto jednotlivých oblastech budou identifikovány i nedostatky, které by mohly ohrozit bezpečnost v organizaci a na které se bude třeba zaměřit v rámci vlastního návrhu řešení.

2.3.1 Serverovna

V současném stavu nelze označit žádnou z místností uvnitř budovy za serverovnu. Důvodem je fakt, že se současný hlavní datový uzel nachází ve volně přístupné místnosti nad dveřmi. Zabezpečení je pouze standardním zámkem určeným pro systém typu RACK, který je určen především pro ochranu proti nahodilému přístupu neoprávněné osoby do dané skříně. Z umístění též vyplývá, že tento centrální přístupový bod není opatřen systémem fyzického zabezpečení, tedy zamezení přístupu neoprávněných osob. Dalším problémem je chlazení aktivních prvků uvnitř skříně, které nyní spoléhá na přirozený průtok chladnějšího vzduchu dovnitř skříně z budovy nasávaného aktivním chlazením uvnitř umístěných aktivních prvků. Tento aktuální stav je proto vysoce nevyhovující pro oblast bezpečnosti i spolehlivosti a je třeba se jím zabývat.

2.3.2 Počítačová síť

Technologie počítačové sítě využívá kabeláž kategorie 5. Tato kabeláž je používaná i pro páteřní vedení. Vycházíme-li z požadavků kapitoly 1.10 je tento stav nevyhovující a je třeba jej ošetřit v budoucnu při budování nové informačně-komunikační infrastruktury. Jelikož současné aktivní prvky, které jsou použity, neumí pracovat s optickou sítí, je třeba je vyměnit.

2.3.3 Zálohování

Nyní probíhá zálohování pouze uvnitř perimetru organizace. Tyto zálohy nejsou šifrovány a jsou uloženy na více místech v organizaci. Zařízení, na která se zálohy ukládají, jsou neustále online, proto je zde vysoké riziko, že by mohly být smazány nebo znehodnoceny útočníkem za pomoci ransomware. Proto je současný stav nevyhovující a vyžaduje provedení změny.

2.3.4 Výpočetní technika

Současně nainstalovaná výpočetní technika odpovídá dnešním standardům. Organizace je již z předchozích let od firmy spravující informační techniku navyklá na profylaxe techniky, které probíhají v letních měsících a zajišťují tedy bezproblémový chod ICT technologie. Pro uživatele výpočetní techniky v současné době není zpracována aktuální směrnice, která by jasně vymezovala povinnosti při užívání výpočetní techniky. Z tohoto důvodu i zde existuje možnost jejího zneužití případně riziko neúmyslného vzniku bezpečnostního incidentu.

2.4 Rozbor „7 S Faktorů“

V návaznosti na předchozí popis současného stavu organizace bude v této kapitole provedena analýza mířící na faktory působící uvnitř organizace, které podmiňují její úspěšnost.

Jedná se o těchto sedm faktorů:

- Strategie
- Struktura
- Systémy
- Styl řízení
- Systémy
- Spolupracovníci
- Schopnosti

2.4.1 Strategie organizace

V rámci strategického plánování je vymezeno poslání a cíl organizace, které jasně ukazuje směr, kterým se bude nadále ubírat. Poslání i cíle organizace byly stanoveny v rámci týmové spolupráce všech pracovních úseků tak, aby precizně formulovaly to, oč je v hlavní činnosti organizace usilováno.

Organizace zaměřuje svoji pozornost na proces neustálého zvyšování kvality poskytovaných služeb. K tomuto účelu je zde implementován systém řízení

kvality E-qalin, který je založený na sebehodnocení organizace v jednotlivých procesech. Ve srovnání s konkurencí se tato organizace specializuje na implementaci moderních metod péče o seniory a zejména pak o seniory s demencí. Cílem je nabídnout klientům bezpečnou péči na vysoké profesionální úrovni.

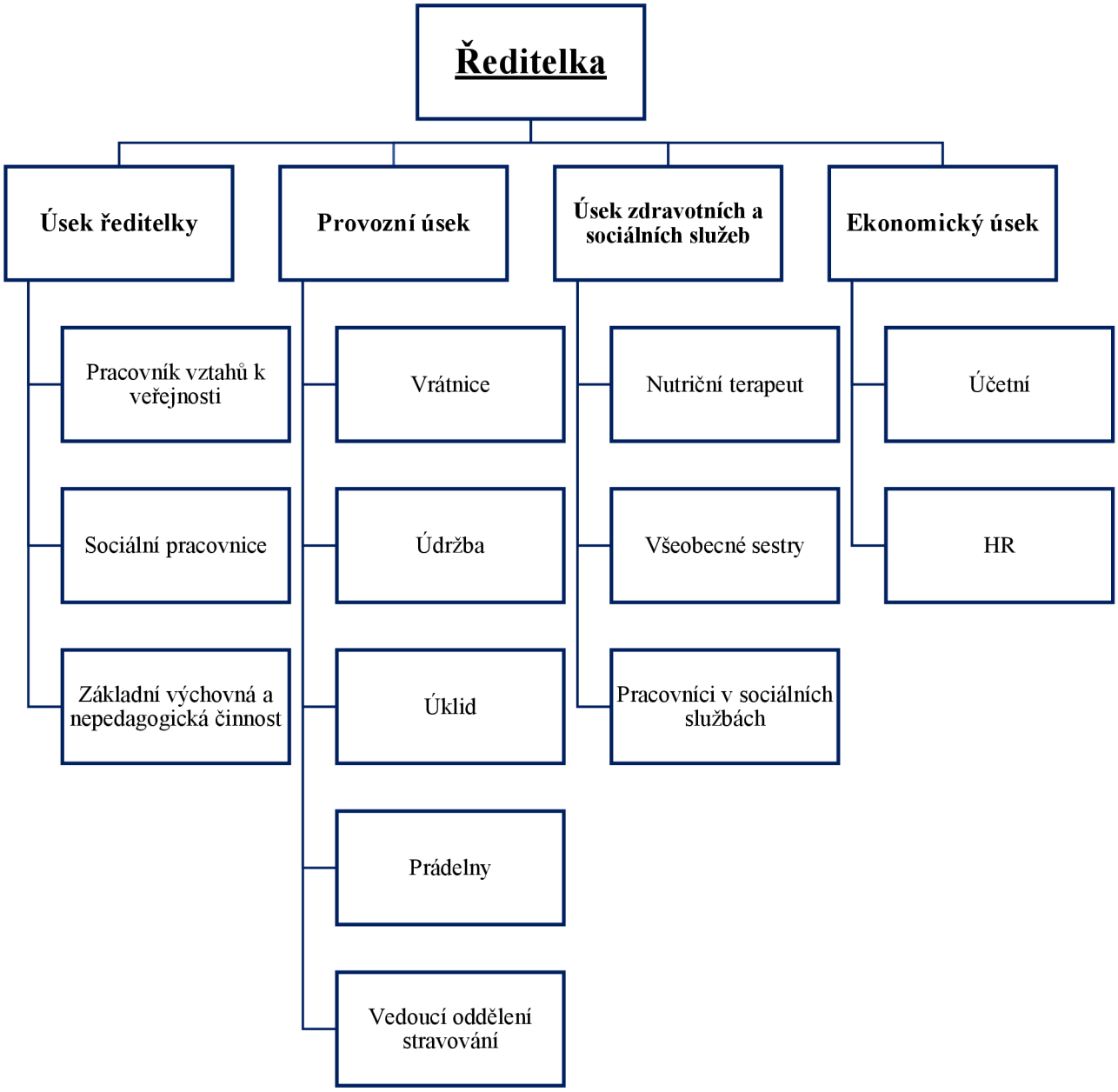
2.4.2 Organizační struktura domova pro seniory

Organizační struktura je navrhována ředitelkou, která je zároveň statutárním zástupcem organizace. Tato organizační struktura je schvalována zřizovatelem. Z organizační struktury jasně vyplývají kompetence jednotlivých pracovních pozic včetně vztahů nadřízenosti a podřízenosti. Nejvyšším článkem organizační struktury je ředitelka. Nižšími řídícími články jsou vedoucí jednotlivých úseků – ekonomického, zdravotního a provozního (střední management). Zdravotní a provozní úseky jsou pak dále členěny na další nižší články. Úsek zaměřený na sociální péči je řízen přímo ředitelkou.

Zdravotní úsek poskytující seniorům zdravotní služby je řízen vrchní sestrou, která přímo řídí staniční a všeobecné sestry. Staniční sestry dále řídí nejnižší články organizační struktury, což jsou pracovníci v sociálních službách.

Provozní úsek je řízen vedoucí provozu, které přímo podléhají pracovníci úklidu, údržby a prádelny. Vedoucí provozu je taktéž podřízena vedoucí stravovacího úseku, která řídí pracovníky kuchyně.

Z hlediska širokých povinností, které musí daná organizace zajišťovat, jsou některé typy služeb, pořizovány outsourcingem. Jedná se zejména o oblasti jako je BOZP, PO, ICT služby, ale taktéž veškeré povinné revize a opravy prováděné v daném objektu.



Obrázek 4 Organizační struktura (Zdroj: Vlastní zpracování)

2.4.3 Informační systémy

V organizaci je používán informační systém Cygnus firmy Iresoft. Cygnus je souborem jednotlivých modulů, které byly speciálně vyvinuty pro prostředí pobytových sociálních služeb. Zahrnuje všechny nástroje pro komplexní správu žadatelů, klientů a zaměstnanců. Všechny pracovní pozice mají k dispozici nástroje, pomocí kterých mohou spravovat data potřebná k plynulému chodu celé služby. Pro evidenci zaměstnanců, plánování směn a docházkové výkazy slouží modul zaměřený na

zaměstnance. Pro efektivní sledování docházky zaměstnanců organizace využívá docházkové čtečky na otisky prstů nebo čipy. Modul Klienti umožňuje sociálním pracovníkům vést přehledně komplexní evidenci žadatelů o pobytovou službu i aktuální klienty daného domova. Funkčnost je zaměřena na výpočet úhrad za pobyt včetně sledování nepřítomnosti klienta, vedení stavu jeho depozit a generování potřebných dokumentů. V rámci sociální a ošetřovatelské dokumentace s vyúčtováním provedených zdravotních výkonů pro zdravotní pojišťovny je umožněno všeobecným sestrám a pečujícímu personálu sestavovat plány péče, vést záznamy o poskytnuté péči s možností ji vyhodnocovat. Pro sledování skutečného objemu poskytnuté péče organizace používá přenosné terminály na čárové kódy. Z důvodu omezení papírového zpracování dokumentace organizace upřednostnila vedení ošetřovatelské dokumentace pouze v elektronické podobě a integrovala elektronické podpisy jako plnohodnotné náhrady ručního podpisu. Pro zabezpečení elektronických podpisů proti neoprávněnému zneužití zajišťuje podpisovými tokeny s osobním certifikátem každé všeobecné sestry. Nedílnou součástí celého informačního systému je i nástroj pro stravovací provoz, který umožňuje sestavování jídelních lístků, normování jídel, příjemky a výdejky navázané na sklad potravin. V rámci provázanosti modulů je možné objednávat stravu a zpětně kontrolovat odběr stravy v návaznosti na docházku zaměstnanců nebo nepřítomnost klienta. Pro profesní rozvoj všech zaměstnanců slouží nástroj k hodnocení zaměstnanců, včetně stanovení potřeb dalšího vzdělávání. V daném informačním systému jsou nastavena přístupová práva tak, aby se zamezilo neoprávněnému zneužití osobních či citlivých dat. Tento informační systém využívá cloudové úložiště. Organizace za užívání systému hradí měsíčně paušální částku.

Dalším informačním systémem používaným v organizaci, je ekonomický systém, kde je zpracováváno komplexní účetnictví s vytvářením výkazů a sestav v provázanosti na elektronický bankovní systém. Organizace má pro tento ekonomický systém zakoupenou licenci s úhradou ročního udržovacího poplatku.

Pro řešení mzdové a personální problematiky organizace využívá program od společnosti Kvasar. Tento systém umožňuje zpracovat mzdy, komunikovat on-line s portály veřejné správy včetně tvorby formulářů pro komunikaci s úřady. Také pro tento program má organizace zakoupenou licenci s ročním udržovacím poplatkem.

Správa majetku je řešena pomocí programu EMA od společnosti Gordic, který poskytuje možnost vedení operativní i účetní evidence spojenou se sledování pohybu majetku od jeho pořízení až po jeho vyřazení.

2.4.4 Styl řízení

Ředitelka organizace je zároveň statutárním orgánem právnické osoby zajišťující pobytové služby. Ředitelka má svůj poradní orgán, který je složen z vedoucích jednotlivých úseků dané organizace. Ředitelka organizace dává velký prostor podřízeným vedoucím jednotlivých úseků k projevení názorů a připomínek a zároveň jim významně nezasahuje do práce, dbá o jejich odborný růst. V rámci hodnocení pak se svými podřízenými zhodnotí výsledky jejich práce. Tím jim poskytne zpětnou vazbu, co udělali dobře a kde je naopak třeba se zlepšit. V rámci řízení je kladen velký důraz na týmovou spolupráci mezi jednotlivými úseky organizace.

2.4.5 Spolupracovníci

Vzhledem k faktu, že se jedná o poměrně velkou organizaci zaměstnávající cca 110 zaměstnanců, je v organizaci vytvořena pracovní pozice, která se zabývá lidskými zdroji. Personalistka zároveň kompetenčně zastává i mzdovou účetní. Jako nástroj řízení kvality v organizaci slouží Standardy kvality sociálních služeb, které jsou obsaženy v příloze č. 2 Vyhlášky Ministerstva práce a sociálních věcí č. 505/2006 Sb. (prováděcí vyhláška k zákonu o sociálních službách (zákon č. 108/2006 Sb. o sociálních službách). Části těchto Standardů kvality – č. 9 a 10 jsou zaměřeny právě na zaměstnance. Organizace má jasně stanovenou organizační strukturu, ze které vyplývají vztahy nadřízenosti a podřízenosti. Zároveň je stanoven počet zaměstnanců zastávající jednotlivé pracovní pozice organizační struktury. Jsou stanoveny komunikační kanály a způsoby předávání informací na pravidelných schůzkách jednotlivých úseků i mezi úseky navzájem. Vedení organizace má velký zájem na profesním a osobním růstu zaměstnanců na každé pracovní pozici, proto je vždy na následující rok vytvořen vzdělávací plán, který reflektuje nejen vzdělávací potřeby jednotlivých zaměstnanců, ale zároveň je zacílen na naplňování vize organizace v oblasti moderních trendů v péči o seniory. Formy školení jsou voleny s ohledem na velikost organizace a počet

pracovníků, kteří se školí. Osvědčenou formou se tedy stávají školení a semináře šité na míru organizaci a zároveň pořádané v místě sídla organizace, čímž se eliminují náklady na cestovní náhrady. Z důvodu péče o zaměstnance a duševní hygienu je do organizace pravidelně přizván supervizor. Zaměstnanci tak mohou v bezpečném prostředí řešit problémy vyplývající z každodenní praxe.

2.4.6 Sdílené hodnoty firmy

Při budování firemní kultury bylo přihlédnuto na definici hodnot, které jsou v organizaci všeobecně sdíleny. U nově nastupujících zaměstnanců je dbáno na to, aby si brzy tyto hodnoty osvojili a implementovali je do každodenní praxe. Kultura organizace je tvořena ředitelkou organizace a vedoucími jednotlivých úseků (střední management), kteří určují cíle, principy a poslání, které jsou poté vlastní činností naplňovány. Velký důraz je kladen na vztahy na pracovišti, neboť tyto se následně velkou měrou odrážejí na poskytované péči. Pracovní vztahy ovlivňují prakticky všechny probíhající procesy v organizaci, proto je maximální snaha směrována na kvalitní komunikaci jako prevenci konfliktů v oblasti pracovních vztahů.

2.4.7 Schopnosti

Mezi nejsilnější vlastnosti organizace patří tradice a dobré jméno, které byly vybudovány v průběhu času a jsou v povědomí obyvatel města. K výhodám též lze zařadit dobrou dostupnost a geografickou polohu, materiálně technické vybavení, bezbariérovost a moderní zázemí. Organizace je vyhledávaným a atraktivním zaměstnavatelem, který velmi dbá na profesní rozvoj a stabilitu svých zaměstnanců. Vedení organizace v co možná nejvyšší míře motivuje zaměstnance k dalšímu vzdělávání, je neustále podněcován osobní potenciál a aktivita každého jednotlivce v týmu.

2.5 Stanovení rozsahu ISMS

V této kapitole bude stanoven rozsah ISMS na základě vyhodnocení současného stavu za pomoci metody Asistovaného zhodnocení

2.5.1 Asistované zhodnocení – Organizační opatření

Asistované zhodnocení (4) bylo vytvořeno Národním úřadem pro kybernetickou a informační bezpečnost, vystupující pod zkratkou NÚKIB, jako analytická pomůcka pro bezpečnostní auditory. Okruhy otázek jsou cíleny na opatření požadovaná zákonem č. 205 ze dne 7. června 2017 (5) a jsou definované vyhláškou č. 82/2018 Sb. (6).

Kompletně vyplněná tabulka asistovaného zhodnocení je vložena jako příloha číslo jedna.

Některé oblasti asistovaného zhodnocení jsou vynechány z důvodu nevhodnosti pro vybranou organizaci. Jedná se o oblasti hodnotící činnosti kritické komunikační infrastruktura KII a významných informačních systémů VIS.

2.5.1.1 ISMS

V současné době se organizace připravuje na proces zavádění sytému řízení bezpečnosti, proto žádná z položek z této podkapitoly není v dané organizaci aplikována.

2.5.1.2 Řízení rizik

Organizace doposud nestanovila metodiku, jakou hodnotí rizika, a za jakých podmínek je ochotna rizika akceptovat. Současná rizika nejsou přehodnocována v případě významných změn. Není zpracovaný a zavedený plán zvládání rizik.

2.5.1.3 Bezpečnostní politika

V rámci bezpečnostní politiky by si měla daná organizace stanovit cíle, principy a potřeby řízení bezpečnosti informací. V dané organizaci zatím nezavedeno.

2.5.1.4 Organizační bezpečnost

V rámci organizační bezpečnosti nejsou zavedeny bezpečnostní role manažera kybernetické bezpečnosti a architekta kybernetické bezpečnosti. Tyto role organizace řeší outsourcingem. Role garantů jednotlivých aktiv jsou v dané organizaci stanoveny.

2.5.1.5 Stanovení bezpečnostních požadavků pro dodavatele

Z hlediska řízení bezpečnostních informací organizace v současné době vede evidenci dodavatelů, ale nemá definovány významné dodavatele dle Přílohy č. 7 k vyhlášce č. 82/2018 Sb.

2.5.1.6 Řízení aktiv

Organizace již nyní zná a eviduje svá primární aktiva, kterým určila jejich garanty, jenž za ně jsou zodpovědní. Hodnotí-li se důležitost aktiv, jsou organizací posuzována již v současné době dle jejich rozsahu a významnosti.

2.5.1.7 Bezpečnost lidských zdrojů

Dle § 9 vyhlášky č. 82/2018 je povinná osoba v rámci řízení bezpečnosti lidských zdrojů zajistit poučení uživatelů, administrátorů, dodavatelů o jejich povinnostech a o bezpečnostní politice. V praxi to tedy znamená, že daná organizace má ve vzdělávacím plánu zaměstnanců zahrnutou i oblast týkající se budování bezpečnostního povědomí spojenou s užíváním ICT techniky. Při analýze výchozího stavu (asistované zhodnocení) bylo zjištěno, že v dané organizaci není tato oblast systematicky zpracovaná, řídící dokument týkající se ICT techniky není aktuální. V rámci návrhů a

praktických výstupů z této práce bude dílčím cílem zpracovat program budování bezpečnostního povědomí v dané organizaci a taktéž zpracovat návrh aktualizace řídícího dokumentu o užívání ICT techniky.

2.5.1.8 Řízení provozu a komunikace

Daná organizace v současné době bezpečně provozuje komunikační systém. Práva a povinnosti administrátorů a uživatelů jsou stanovena. Pravidelné zálohování sice prováděno je, nikoliv však následné prověřování použitelnosti provedených záloh.

2.5.1.9 Řízení přístupu a bezpečné chování uživatelů

Řízení přístupu je v organizaci v současné době nastaveno, jelikož jsou řízeny přístupy k informačním a komunikačním systémům. Jsou přijata opatření sloužící k zajištění ochrany údajů používaných pro přihlášení do obou těchto systémů a bránící ve zneužití údajů neoprávněnou osobu. Řízení přístupu probíhá na základě stanovení skupin a rolí podle organizační struktury a náplně práce jednotlivých uživatelů. Jedinečným identifikátorem každého uživatele je jeho přihlašovací jméno. Organizace neřeší používání technických zařízení mimo svoji správu, jelikož k výkonu práce není třeba takových zařízení. V současnosti již jsou přidělována privilegovaná opatření pouze na takovou úroveň, která je nezbytná pro výkon dle náplně práce. V případě personální změny jsou přidělována a odebírána přístupová oprávnění v souladu se současnou politikou řízení přístupů. Nastavení jednotlivých pracovních stanic omezuje možnost instalace, čímž je zamezeno užívání programových prostředků se schopností překonávat systémové nebo aplikační kontroly.

2.5.1.10 Akvizice, vývoj a údržba

Organizace aktuálně při plánování akvizice, vývoje nebo údržby informačních či komunikačních systémů nemá nastaveny postupy zahrnující řízení rizik a významných změn. Nemá tedy písemně stanoveny bezpečnostní požadavky a ve většině případů nejsou zahrnovány bezpečnostní požadavky do projektů.

2.5.1.11 Zvládání kybernetických bezpečnostních událostí a incidentů

Organizace má zavedeny procesy detekce, avšak dále nejsou zpracována data pro vyhodnocování kybernetických bezpečnostních událostí.

2.5.1.12 Řízení kontinuity činností

Řízení kontinuity činností není aktuálně řešeno. V případě výpadku systémů není kriticky ohrožen chod organizace.

2.5.2 Asistované zhodnocení – Technická opatření

V této podkapitole budou popsány dílčí analýzy z metodiky asistovaného zhodnocení, které nyní budou zaměřeny na technická opatření.

2.5.2.1 Fyzická bezpečnost

V rámci fyzické bezpečnosti je předcházeno poškození, krádeži či zneužití aktiv nebo přerušení poskytování služeb informačního systému tím, že jsou umístěna do RACKu. Není však stanoven fyzicky bezpečnostní perimetr, který by ohraničoval oblast, kde jsou zpracovávány a uchovávány informace a umístěna technická aktiva informačního a komunikačního systému.

2.5.2.2 Nástroj pro ochranu integrity komunikačních sítí

Nástroje zajišťující ochranu integrity sítě jsou již v současné době používány. Pro řízení bezpečného přístupu mezi vnitřní a vnější sítí je použit softwarový firewall. Pro skrytí zařízení uvnitř organizace je při překladu adres zapnuta funkce maškarády.

Demilitarizované zóny v současném využívání sítě nejsou nutné, jelikož ze strany organizace nevznikla potřeba přístupu k žádné ze svých aplikací z vnější sítě, jelikož veškerá činnost vyžívající ICT služeb probíhá ve vnitřním perimetru organizace.

Pro segmentaci a tím udržení integrity vnitřní sítě je využíváno její logické rozdělení do několika na sobě nezávislých sítí včetně nezávislosti na fyzické síti. Toho je dosaženo za pomoci VLAN. Díky jejich využití se zjednodušila správa sítě a zvýšila se její bezpečnost.

2.5.2.3 Nástroj pro ověření identity uživatelů

Organizace v současné době nevyužívá jednotného nástroje, který by umožňoval správu a ověřování identity uživatelů, ale využívá ověřování identity uživatelů za pomoci vnitřních mechanismů jednotlivých aplikací nebo služeb. V tomto případě se organizace spoléhá na to, že každá z aplikací ověří identitu uživatele před zahájením jakýkoliv aktivit. S tím souvisí řízení počtu neúspěšných přihlášení, přenos autentizačních údajů, jejich offline uložení v dostatečně odolné podobě a případné automatické vyžádání si znovu přihlášení uživatele po nějaké době jeho nečinnosti. Žádná z těchto aplikací nebo služeb nepodporuje vícefaktorovou autentizaci. Současně nejsou vynucována pravidla pro hesla jako je jejich délka, obsah, časové omezení nebo změnu výchozích hesel.

2.5.2.4 Nástroj pro řízení přístupových oprávnění

Organizace v současné době nepoužívá centralizovaný nástroj, který zajišťuje přístupy k jednotlivým aktivům a zároveň by zajišťoval řízení oprávnění pro čtení, zápis dat a změnu oprávnění. Jsou používány decentralizované nástroje, tedy nástroje jednotlivých služeb, které právě umožňují řídit změny v oprávněních pro čtení, zápis dat. Díky tomu, že neexistuje jeden centralizovaný nástroj, je správa těchto oprávnění časově náročnější a ne tak komfortní jako v případě centralizovaného řešení.

2.5.2.5 Nástroj pro ochranu před škodlivým kódem

Ochrana před škodlivým kódem je v současnosti řešena nástrojem, který provádí nepřetržitou automatickou ochranu, a to jak koncových stanic, tak serverů. Z důvodu využití komerčního nástroje je zajištěna jeho pravidelná aktualizace. I při využití placeného komerčního nástroje je jeho cena adekvátní vůči ceně aktiv, která chrání.

2.5.2.6 Nástroj pro detekci kybernetických bezpečnostních událostí

V současné době není využíván nástroj, který by byl schopen zajistit detekci kybernetických bezpečnostních událostí a dokázal by zablokovat komunikaci mezi vnitřní komunikační sítí a internetem (vnější komunikační sítí) nebo v rámci samotné vnitřní sítě.

2.5.2.7 Aplikační bezpečnost

Používáním krabicových řešení jednotlivých informačních systémů a služeb organizace předpokládá, že penetrační testování prováděl výrobce daného řešení. Organizace zajišťuje trvalou ochranu aplikací, informací a transakcí před neoprávněnou činností nebo jejich popření tím, že veškeré tyto činnosti probíhají pouze uvnitř perimetru organizace.

2.5.2.8 Kryptografické prostředky

Aktuálně nejsou v organizaci stanovena pravidla, která by stanovovala typ a sílu kryptografického algoritmu, jeho užívání při přenosu informací na přenosných mediích nebo jejich použití pro zajištění důvěrnosti a integrity předávaných dat. Dále není stanoven systém správy klíčů používaných u kryptografických prostředků.

2.5.2.9 Nástroj pro zajišťování úrovně dostupnosti

Současný chod organizace není ze sta procent závislý na komunikačních systémech. Ty jsou pro ni pouze nástrojem, který ulehčuje její každodenní činnosti spojené s vedením agendy jejích klientů a zaměstnanců. Z toho důvodu nenarušuje výpadek komunikační infrastruktury kontinuitu činnosti organizace.

3 VLASTNÍ NÁVRH ŘEŠENÍ

Po předchozí kapitole, kde jsem popsal získané informace o aktuálním stavu zvolené spolupracující organizace včetně identifikace rizikových míst, nyní navážu vlastním návrhem pro zavedení systému řízení bezpečnosti informací pro zvolenou organizaci.

3.1 Řízení změny

Jelikož je zavedení ISMS pro organizaci významnou a náročnou změnou, je třeba, aby tato změna byla systematicky řízena. Pro návrh řízení změn bude využito Lewinova modelu řízené změny, který se jeví jako nejvhodnější k zavádění zamýšlené změny tohoto typu v organizaci.

3.1.1 Síly inicializující proces změny

Dne 25. května 2018 vstoupilo v platnost obecné nařízení GDPR. Od tohoto dne je třeba, aby se veškeré subjekty zpracovávající osobní údaje tímto nařízením řídily. Tlaky působící na potřebu zavedení změny v organizaci jsou naléhavější z důvodu zpracovávání citlivých osobních údajů. Jelikož tyto údaje mohou poškodit konkrétní fyzickou osobu v rámci jejího běžného života, podléhají mnohem přísnějšímu režimu.

Na základě toho, že se v průběhu času legislativa zpřísňovala, vyhodnotilo vedení organizace potřebu přistupovat ke zpracovávání osobních údajů, a zejména těch citlivých, s velkou mírou zodpovědnosti dle požadavků nařízení GDPR a tím přijmout potřebná opatření. Jedním ze základních opatření je zavedení systému řízení bezpečnosti informací. Tento systém pokrývá svými řešeními většinu z požadavků obecného nařízení EU 2016/679, známého jako GDPR.

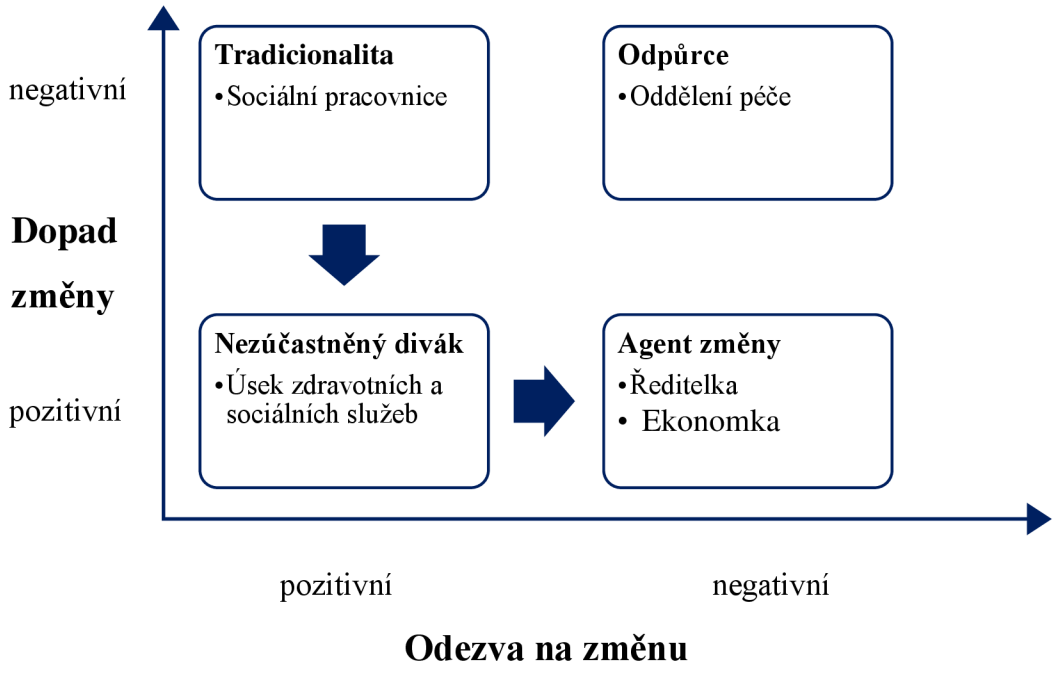
3.1.2 Síly působící pro a proti plánované změně

Systém řízení bezpečnosti informací v organizaci byl iniciován několika nařízeními vlády a zákonů reflektujících na obecné nařízení Evropské unie GDPR.

Taktéž ze strany zřizovatele bylo doporučeno se touto problematikou důsledně zabývat a přijmout taková pravidla a opatření v organizaci, která budou v souladu s platnou legislativou. Na základě těchto popsaných událostí bylo vyhodnoceno jako nezbytné zabývat se zvyšování bezpečnosti organizace, které z hlediska metrik pro audit systému řízení bezpečnosti informací začíná školením. A právě do této skupiny spadá program pro budování bezpečnostního povědomí.

Hlavními opoziční silou jsou uživatelé, kteří jsou obecně proti ICT technologiím, nebo se je dokonce bojí používat. Dalšími odpůrci změny budou uživatelé, kteří jsou zaměřeni spíše na výkon u klienta než na administrativní práci a práci s PC. Dalším důvodem je mnohdy i věk uživatelů, jejich mizivé zkušenosti s používáním PC, kteří odmítají novinky a modernizace způsobů péče.

Nyní bude shrnuta ochota zaměstnanců akceptovat proces změny ve čtyřech kategoriích pracovníků organizace:



Graf 2 Základní kategorizace pracovníků firmy (Zdroj: Vlastní zpracování, 20)

3.1.3 Identifikace agenta změny

Agentem změny je v případě této organizace vedoucí pracovnice, která je služebně nejstarší a zná velmi dobře většinu procesů v organizaci. Zároveň zastává několik agregovaných funkcí, jako je například hlavní účetní, garant aktiva ICT a další.

Sponzorem změny bude ředitelka organizace, která bude pomáhat prosazovat ISMS svojí politickou silou uvnitř organizace.

3.1.4 Intervence v organizaci

Pro nastolení procesu řízení změn je třeba nejdříve popsat veškeré změny, které v organizaci následně nastanou. Proto budou v následující kapitole tyto změny popsány. Jedná se zejména o změny, které zasáhnou do oblasti lidských zdrojů, organizační struktury a technologií.

3.1.4.1 Intervence lidských zdrojů

Připravovaná změna v organizaci nejvíce ovlivní lidské zdroje zejména v oblasti osobního rozvoje a vzdělávání. U určených skupin zaměstnanců bude požadováno absolvování všech pro ně vybraných školení a programů sebevzdělávání. Ty budou specifikovány podle náplně práce a zpracovány takovým způsobem, aby byl co nejvíce omezen vzdor jednotlivých uživatelů. Vzdor vůči zaváděným změnám by měl být snížen tím, že se zaměstnanci na systému budou moci podílet a participovat s týmem, který jej bude vytvářet. Cílem bude snížit odpor podporou k tomu, aby byli zaměstnanci schopni požadavky ISMS lehce začlenit k běžné pracovní náplni a zároveň časovému harmonogramu pracovní doby. Vytvoření návrhů a veškeré plány ISMS budou konzultovány s vedením organizace tak, aby ISMS vyhovovalo co nejpřesněji a nejlépe potřebám organizace, jinými slovy vytvořit jej na míru organizaci.

3.1.4.2 Intervence v organizační struktuře

V organizační struktuře v současné době ke změně nedojde. Ideálním stavem by bylo, kdyby v organizační struktuře byla vytvořena pozice pro zaměstnance, jehož hlavní

pracovní náplň by obsahovala správu programu řízení bezpečnosti informací a zároveň by měl zodpovědnost nad celým systémem ICT v organizaci. Tato osoba by v organizační struktuře byla podřízena přímo ředitelce.

3.1.4.3 Intervence v technologii

Připravovanou změnou budou také ovlivněny technologie využívané organizací. Tyto změny se budou týkat jak softwaru, tak i hardwaru. V této řízené změně užívaného softwaru bude změněna internetová ochrana a antivir. Tímto krokem bude organizaci zajištěna možnost šifrovat svá data a spravovat svá hesla. Změna hardwaru bude výraznější, jelikož se předpokládá výměna celého komunikačního systému a změna umístění serverovny. Tato změna ve svém důsledku povede ke zvýšení bezpečnosti

3.1.5 Verifikace dosažených výsledků

Veškerá navržená opatření organizaci nepřinesou žádný zisk. Tato opatření kryjí organizaci proti případným ztrátám na jejich aktivech, ať už hovoříme o těch hmotných nebo nehmotných. Proto nelze zjednodušeně říci, zdali jsou dosažené výsledky optimální či nikoliv bez provedení vlastních ověření o tom, že navržená pravidla jsou dodržována a jsou stále platná. Dále bude třeba zkoumat, zdali jsou v dané době ještě stále platná a v jakém rozsahu. Předpokladem je, že by po aplikaci systémů řízení bezpečnosti informací nemělo docházet k takovým bezpečnostním incidentům, které byly systémem ošetřeny. Pokud by přesto takový bezpečnostní incident nastal, není to známkou nefunkčnosti systému, ale bude se jednat o pochybení některého článku v celém systému, který přestal být v čase tak účinný, jako při jeho inicializaci.

3.2 Riziková politika

V této podkapitole bude popsána riziková politika organizace, ve které je zahrnuta identifikace a ohodnocení aktiv. Dále budou identifikovány hrozby, které by na tyto aktiva mohly působit. U hrozeb je nutné určitě jejich pravděpodobnost, se kterou by mohly nastat, což umožní sestavit matici zranitelnosti. Po zpracování matice zranitelností je zpracována matice rizik, která na ni navazuje.

3.2.1 Identifikace a ohodnocení aktiv

Nyní bude provedena identifikace a ohodnocení aktiv na základě hodnotící tabulky, která je uvedena pod tímto textem. Vložená tabulka je rozdělena hodnotící škálou 1 až 5 a každý stupeň škály je doplněn o slovní vyjádření dopadu na organizaci. Podle této tabulky byla ohodnocena aktiva, která jsou uvedena v následující tabulce. Váha aktiva se vypočítá za pomoci rovnice číslo jedna.

Tabulka 1 Stupnice a hodnocení kritérií (Zdroj: 7)

Míra rizika	Dopad rizika	Váha aktiva
bezvýznamné	žádný	1
akceptovatelné	zanedbatelný	2
nízké	potíže a finanční ztráty	3
nežádoucí	vážné potíže a velké finanční ztráty	4
nepřijatelné	ohrožující existenci	5

Váha pro jednotlivá aktiva byla vypočítána na základě rovnice níže.

$$Váha = \frac{Dostupnost + Důvěrnost + Integrita}{3}$$

V níže uvedené tabulce jsou uvedena aktiva, která byla identifikována při konzultacích s vedením organizace. Při identifikaci aktiv bylo přihlíženo na jejich vtah k bezpečnosti informací. Pro každé aktivum byla stanovena hodnota dostupnosti říkající, jak je

zajištěna dostupnost informace pro oprávněného uživatele v okamžiku jeho potřeby. Dále je uvedena důvěrnost, kterou vyjadřujeme, jak jsou informace zajištěny, zdali jsou přístupny nebo sděleny pouze oprávněným osobám. Integritou je myšlena správnost a úplnost informace. Tyto tři hodnoty jsou doplněny o následně vypočítanou hodnotu váhy aktiva.

Tabulka 2 Identifikace a ohodnocení aktiv (Zdroj: Vlastní zpracování)

Typ		Aktivum	Dostupnost	Důvěrnost	Integrita	Váha
Data	1.	Data o klientech	5	5	5	5
	2.	Data o účetnictví	5	5	5	5
	3.	Data o zaměstnancích	5	5	5	5
	4.	Zálohy dat	5	5	5	5
HW	5.	Routery	4	3	5	4
	6.	Řízené switche	5	2	3	3
	7.	Servery	4	4	4	4
	8.	Pasivní síťové prvky	5	1	1	2
	9.	Pracovní stanice	4	4	4	4
	10.	Tiskárny	1	5	1	3
	11.	EZS	2	4	2	2
Služby	12.	Elektronická pošta	3	5	5	4
	13.	Internetové připojení	5	2	2	3
SW	14.	Antivirus	3	5	5	4

3.2.2 Identifikace hrozeb a jejich pravděpodobnosti

Možné hrozby byly vytypovány při setkání s vedením organizace. Dále bylo třeba stanovit pravděpodobnosti hrozeb, se kterými mohou tyto hrozby působit. I u hrozeb bylo použito pěti stupňové škály, u které číslo jedna znamená, že působení této hrozby je vyloučeno.

Tabulka 3 Hodnocení hrozeb (Zdroj: 17)

Pravděpodobnost	Hodnota
Vyloučená	1
Nepravděpodobná	2
Možná	3
Pravděpodobná	4
Jistá	5

Tabulka 4 Identifikace hrozeb a jejich pravděpodobnosti (Zdroj: Vlastní zpracování)

Hrozba	Pravděpodobnost
Krádež aktiva	1
Krádež dat	1
Narušen důvěrnosti aktiva	3
Narušení integrity aktiva	3
Nedostupnost aktiva	1
Nefunkční zařízení	1
Neoprávněné nakládání s aktivy	2
Neoprávněné vniknutí do perimetru	2
Neoprávněné vniknutí do zabezpečené oblasti	2
Neúmyslná změna aktiva	3
Nevhodné nakládání s aktivy	4
Odpor zaměstnanců vůči změně	5
Online útok	1
Pochybení zaměstnance	4
Poškození vodou	2
Požár	1
Přepětí v elektrické síti	1
Špatné provedení údržby	2
Špionáž	1
Úmyslné poškození aktiva	1
Únik informací	2
Zneužití aktiva	4
Zničení zařízení	2

3.2.3 Matice zranitelnosti a matice rizik

Matice zranitelnosti vyjadřuje zranitelnost aktiva při působení jednotlivých identifikovaných hrozeb. V hodnotě zranitelnosti je promítnuta jak hodnota daného aktiva, tak pravděpodobnost s jakou daná hrozba může nastat. Sumou všech těchto úvah je hodnota zranitelnosti, jenž může nabývat hodnoty jedna až pět. Stejně jako v přechozích případech vyšší číslo znamená vyšší zranitelnost a naopak. Veškeré hodnoty byly opět konzultovány s vedením organizace.

Po vypracování matice zranitelností bylo nutné vypočítat matici rizik. Jednotlivé hodnoty byly vypočítány za pomoci vzorce:

$$\boldsymbol{R = T \times A \times V}$$

Kde:

- **R** je vypočítaná hodnota rizika,
- **T** je pravděpodobnost hrozby,
- **A** je hodnota aktiva,
- **V** je zranitelnost.

Pro různé stupně rizik je nutné stanovit hodnotu jejich hranic a tyto stupně vyjádřit i slovně. Pro přehlednost jsou jednotlivé stupně v matici rizik rozlišeny barevně. Prvním stupněm rizik označené bílou barvou a nabývající hodnoty nula až třicet jsou rizika s nízkou mírou. Na druhém stupni, který je označen žlutě a nabývá hodnot třicet jedna až šedesát jsou rizika se střední mírou. Na posledním stupni označeným červeně a nabývajícím hodnoty šedesát jedna a více jsou rizika s vysokou mírou. Obecně je zapotřebí navrhovat opatření od rizik s nejvyšší hodnotou, přes střední, až u rizik s velmi nízkou hodnotou můžeme uvažovat o jejich akceptaci.

Tabulka 5 Matice zranitelnosti (Zdroj: Vlastní zpracování)

Zranitelnost (V)	Aktiva	Data				HW						Služby		SW
		Data o klientech	Data o účetnictví	Data o zaměstnancích	Zálohy dat	Routery	Řízené switche	Servery	Pasivní síťové prvky	Pracovní stanice	Tiskárny	EZS	Elektronická pošta	Internetové připojení	Antivirus
	A	**5**	**5**	**5**	**5**	**4**	**3**	**4**	**2**	**4**	**3**	**2**	**4**	**3**	**4**
Hrozba	**T**														
Krádež aktiva	**1**	5	5	5	5	1	1	1	0	1	1	0	0	0	0
Krádež dat	**1**	5	5	5	5	0	0	0	0	0	0	0	0	0	0
Narušení důvěrnosti aktiva	**3**	5	5	5	5	5	0	5	0	4	0	0	1	0	0
Narušení integrity aktiva	**3**	5	5	5	5	5	0	5	0	4	0	0	1	0	0
Nedostupnost aktiva	**1**	5	5	5	5	5	5	5	3	3	1	1	1	5	3
Nefunkční zařízení	**1**	0	0	0	0	3	3	3	1	3	1	2	1	3	1
Neoprávněné nakládání s aktivy	**2**	5	5	5	5	0	0	0	1	2	2	0	0	0	0
Neoprávněné vniknutí do perimetru	**2**	0	0	0	0	0	0	0	0	0	0	3	0	0	0
Neoprávněné vniknutí do zabezpečené oblasti	**2**	4	4	4	4	0	0	0	0	0	0	3	0	0	0
Neúmyslná změna aktiva	**3**	5	5	5	5	0	0	0	0	0	0	0	0	0	0
Nevhodné nakládání s aktivy	**4**	5	5	5	5	0	0	0	0	3	1	0	1	0	0
Online útok	**1**	5	5	5	5	4	4	4	2	4	4	0	2	4	5
Pochybení zaměstnance	**4**	5	5	5	5	0	0	0	0	3	0	0	0	0	0
Poškození vodou	**2**	1	1	1	1	3	3	3	0	3	3	3	0	1	0
Požár	**1**	1	1	1	1	2	2	2	3	3	3	3	0	1	0
Přepětí v elektrické síti	**1**	1	1	1	0	4	4	4	4	4	4	4	0	1	0
Špatné provedení údržby	**2**	3	3	3	3	4	4	4	3	3	2	1	0	1	0
Špionáž	**1**	5	5	5	5	3	2	2	1	4	4	0	2	5	5
Úmyslné poškození aktiva	**1**	4	3	3	4	3	3	3	3	3	2	1	0	0	0
Únik informací	**2**	5	5	5	5	0	0	3	0	0	3	0	2	0	0
Zneužití aktiva	**4**	5	5	5	5	0	0	0	2	2	2	0	1	0	0
Zničení zařízení	**2**	0	0	0	3	5	5	5	3	1	1	1	0	1	0

Tabulka 6 Matice rizik (Zdroj: Vlastní zpracování)

Míra rizika ®		Data				HW							Služby		SW
	Aktiva	Data o klientech	Data o účetnictví	Data o zaměstnancích	Zálohy dat	Routery	Řízené switche	Servery	Pasivní síťové prvky	Pracovní stanice	Tiskárny	EZS	Elektronická pošta	Internetové připojení	Antivirus
	A	**5**	**5**	**5**	**5**	**4**	**3**	**4**	**2**	**4**	**3**	**2**	**4**	**3**	**4**
Hrozba	**T**														
Krádež aktiva	**1**	25	25	25	25	4	3	4	0	4	3	0	0	0	0
Krádež dat	**1**	25	25	25	25	0	0	0	0	0	0	0	0	0	0
Narušení důvěrnosti aktiva	**3**	75	75	75	75	60	0	60	0	48	0	0	12	0	0
Narušení integrity aktiva	**3**	75	75	75	75	60	0	60	0	48	0	0	12	0	0
Nedostupnost aktiva	**1**	25	25	25	25	20	15	20	6	12	3	2	4	15	12
Nefunkční zařízení	**1**	0	0	0	0	12	9	12	2	12	3	4	4	9	4
Neoprávněné nakládání s aktivy	**2**	50	50	50	50	0	0	0	4	16	12	0	0	0	0
Neoprávněné vniknutí do perimetru	**2**	0	0	0	0	0	0	0	0	0	0	12	0	0	0
Neoprávněné vniknutí do zabezpečené oblasti	**2**	40	40	40	40	0	0	0	0	0	0	12	0	0	0
Neúmyslná změna aktiva	**3**	75	75	75	75	0	0	0	0	0	0	0	0	0	0
Nevhodné nakládání s aktivy	**4**	100	100	100	100	0	0	0	0	48	12	0	16	0	0
Online útok	**1**	25	25	25	25	16	12	16	4	16	12	0	8	12	20
Pochybení zaměstnance	**4**	100	100	100	100	0	0	0	0	48	0	0	0	0	0
Poškození vodou	**2**	10	10	10	10	24	18	24	0	24	18	12	0	6	0
Požár	**1**	5	5	5	5	8	6	8	6	12	9	6	0	3	0
Přepětí v elektrické síti	**1**	5	5	5	0	16	12	16	8	16	12	8	0	3	0
Špatné provedení údržby	**2**	30	30	30	30	32	24	32	12	24	12	4	0	6	0
Špionáž	**1**	25	25	25	25	12	6	8	2	16	12	0	8	15	20
Úmyslné poškození aktiva	**1**	20	15	15	20	12	9	12	6	12	6	2	0	0	0
Únik informací	**2**	50	50	50	50	0	0	24	0	0	18	0	16	0	0
Zneužití aktiva	**4**	100	100	100	100	0	0	0	16	32	24	0	16	0	0
Zničení zařízení	**2**	0	0	0	30	40	30	40	12	8	6	4	0	6	0

Organizace by měla co nejdříve vyřešit rizika s nejvyšší hodnotou (označená červeně), která můžeme vidět v matici rizik. Ve všech třech případech se jedná o data kvalifikována podle požadavků GDPR jako kritická, jelikož obsahující osobní údaje. Proto je třeba zajisti soulad opatření ISMS a požadavky GDPR, jejichž spojením by se hodnota rizika měla rapidně snížit. Následně organizace může řešit zabezpečení zařízení pro zpracování dat.

3.3 GDPR

Vstupem v platnost obecného nařízení EU známého jako GDPR, je třeba doplnit ISMS o několik specifických požadavků. Sjednocení nařízení s touto normou je motivováno především vysokými pokutami, které z nedodržení tohoto nařízení vyplývají.

3.3.1 Posouzení rizik

Prvním nutným souladem, který byl již v této diplomové práci aplikován, je označení všech dat obsahujících osobní údaje jako kritické. Toto lze ověřit ve vypracované tabulce s názvem Identifikace a ohodnocení aktiv. Veškerá tato data jsou označena tím nejvyšším stupněm pro hodnocení aktiv, tedy jako aktiva ohrožující existenci organizace.

Pro organizaci z toho vyplývá povinnost při klasifikování informací v opatření A.8, že veškeré informace musí být ohodnoceny s ohledem na právní požadavky. V této skupině opatření je též důležité, aby u klasifikovaných dat obsahujících osobní údaje, bylo ještě navíc určeno: o jaký typ osobních údajů se jedná, kde jsou tyto informace uchovávány (nejlépe zabezpečený perimetr), jak dlouho tyto údaje budou uchovány, jejich původ a kdo má k daným údajům přístup.

3.3.2 Soulad

Aby bylo dosaženo souladu s požadavky opatření A.18 ISMS, je nezbytné, aby organizace do svého seznamu legislativních požadavků zahrnula i nařízení GDPR.

Tento soulad by mělo vyřešit i druhé opatření ze stejné skupiny opatření, které má za úkol zajistit soukromí a ochranu osobních údajů.

3.4 Program budování bezpečnostního povědomí

Stejně jako v ISMS ve skupině opatření A.7, tak i v nařízeních GDPR, je dbáno na vzdělávání jednotlivců v organizacích. Pro jejich soulad je vhodné zavést v organizaci program budování bezpečnostního povědomí.

Program budování bezpečnostního povědomí byl na přání organizace vytvořen pouze ve zkušebním režimu, neboť počet zaměstnanců, které je nutné proškolit je vysoký. Z tohoto důvodu bylo nutné nejdříve vytvořit „zkušební vzorek“. Organizace chtěla v tomto malém měřítku nejdříve ověřit proveditelnost tohoto programu před tím, než do něj bude investovat více úsilí a peněz. Dalším důvodem je vyzkoušení nastavení různých režimů pro tento program.

Některé z oblastí programu budou pouze doporučeními pro samotnou organizaci a dále již bude pouze v jejich silách, aby tyto oblasti dále rozvíjela. Vybudováním těchto základních principů a návrh postupů pro program SAE a jejich následným postupným implementováním samotnou organizací, by mělo mít za následek postupné zvyšování bezpečnostního povědomí na všech úrovních organizace.

3.4.1 Návrh programu

Prvním krokem pro vybudování programu SAE je vytvoření jeho návrhu. V tomto návrhu je zohledněno zúžení na dvě skupiny dobrovolníků. První skupinou byli ti, kteří se chtějí vzdělávat i pro své osobní potřeby bezpečnosti mimo organizaci. Druhou skupinou byli zaměstnanci obecně odmítající ICT techniku. Pro každou z nich byl vytyčen jeden cíl. Prvním cílem je poučení, jak se chovat bezpečněji v prostředí internetu. Druhým cílem je vyvést dobrovolníky z digitální propasti.

V případě následného zavádění programu doporučuji, aby byl budován na centralizovaném modelu řízení programu. V organizaci tedy bude vyčleněna pracovní skupina, která bude mít na starosti stanovení rozsahu, cíle, rozdělení uživatelů

a vypracování programu. Tedy jedna skupina v organizaci bude plně zodpovědná za celý program.

3.4.2 Vytvoření programu

Pro potřeby dvou vybraných skupin byly vytvořeny školicí prezentace. Pro skupinu vyváděnou z digitální propasti byla vytvořena prezentace ukazující základy práce s počítačem a základní úkony pro práci v organizaci. Jelikož prezentace obsahovala prvky, podle kterých bylo možné organizací identifikovat, bylo zveřejnění této prezentace organizací zamítnuto. V druhé prezentaci nejsou obsaženy žádné prvky, které by odkazovaly na spolupracující organizaci, proto bylo možné tuto prezentaci vložit jako přílohu č.2.

3.4.3 Uskutečnění programu

Jelikož je náš program vytvořen pouze pro malou skupinu lidí není třeba pro ně stanovovat časový harmonogram. Ten bude třeba navrhnout až pracovní skupinou při zavádění plnohodnotného programu na budování bezpečnostního povědomí.

3.4.4 Udržování programu

Po zavedení programu do organizace je třeba dbát na aktualizaci výukových materiálů, aby byly aktuální vůči novým požadavkům na bezpečnost. Tyto aktualizace musí probíhat v nastaveném intervalu nebo při výrazné změně v bezpečnosti informací.

3.4.5 Doporučení pro organizaci

Přihlédnu-li k vytížení pracovníků organizace a časové náročnosti tvorby vzdělávacích materiálů, hrozí zde neuskutečnění programu SAE v dostatečně brzké době a potřebném rozsahu pro organizaci. Je tedy dobré zvážit vhodnost různých alternativ. Jednou z možných alternativ je outsourcing tohoto programu. Je to jistá finanční zátěž pro organizaci, ale má i své výhody. Uživatelé, kteří tento program absolvují mimo

organizaci, obdrží certifikát. V případně vhodné motivace těchto uživatelů se z nich mohou stát interní školitelé na budování bezpečnostního povědomí pro organizaci.

3.5 Návrh bezpečnostních opatření

V této kapitole budou navržena opatření na míru vybrané organizaci. Tato opatření budou vycházet z nejlepších praktik, které se nacházejí v příloze A normy ISO/IEC 27001. Tím bude ošetřeno případné riziko, že by byla nějaká nezbytná opatření opomenuta.

3.5.1 A.5 Politiky bezpečnosti informací

Prvním krokem při vytváření politiky bezpečnosti je získání souhlasu vedení organizace se zavedením ISMS. Důvodem jsou předpokládané finanční náklady, ale i zatížení lidských zdrojů. Proto je třeba vytvořit takové politiky ISMS, které budou definovány a schváleny vedením organizace. Po vypracování politik, kterými vedení organizace určí směr její informační bezpečnosti, je nutné tyto politiky vydat a seznámit s nimi všechny zaměstnance a relevantní externí strany.

Pro politiky je třeba vytvořit časový plán, který určí jejich pravidelné přezkoumávání včetně mimořádného přezkoumání v případě významné změny, která by mohla mít dopad na politiku bezpečnosti.

3.5.2 A.6 Organizace bezpečnosti informací

Tato skupina opatření klade organizaci za cíl vytvořit politiky ošetřující řízení bezpečnosti informací při jejím zahájení přes implementaci po její rutinní provoz. Veškerá tato opatření je nutné sladit s nastaveným směrem bezpečnosti informací organizace v oblasti A.5.

V této fázi opatření je nutné stanovit odpovědné osoby za ochranu jednotlivých aktiv případně za provádění specifických činností.

Je nutné jasně definovat role a přidělit odpovědnosti za aktiva případně za specifické procesy v rámci řízení bezpečnosti informací. Tyto odpovědnosti je třeba vztáhnout k jednotlivým aktivům, které zaměstnanec užívá, případně s nimi svázat konkrétní postupy podporující bezpečnost.

Také je třeba přezkoumat, zda u některého z odpovědných zaměstnanců nedochází ke střetu zájmů různých oblastí, ve kterých zaměstnanec působí. Díky nim by mohlo dojít k neoprávněným nebo neúmyslným změnám potažmo zneužití aktiv. Toto je nutné zvažovat při návrhu veškerých opatření.

Vzhledem k faktu, že i zřizovatel příspěvkové organizace zaměřuje svoji pozornost na politiku bezpečnosti informací, doporučuji, aby v případě zřízení pracovní skupiny zabývající se touto problematikou v příspěvkových organizacích byl vyslán zástupce takové organizace. Člen takové skupiny by následně mohl vnést do organizace nové znalosti, postupy, informace, varování a doporučení, jenž jsou aktuálně uplatňovány nebo objeveny v jiných organizacích a mohou sloužit k dalšímu zlepšování.

Jelikož organizace u většiny ze svých nerutinních činností využívá metod projektového řízení, doporučuji do všech těchto metod implementovat zásady a cíle z bezpečnosti informací. Díky tomu budou v každém projektu řešena bezpečnostní rizika.

Ve vybrané organizaci není podporována práce na dálku včetně mobilních zařízení. Proto v současnosti není třeba v rámci návrhu opatření s nimi spojená řešit. Práce na dálku nebo s mobilními zařízeními může být brána jako významná změna, se kterou budou pro ně vytvořeny politiky souběžně s přezkoumáním těch současných.

3.5.3 A.7 Bezpečnost lidských zdrojů

U skupiny těchto opatření jsou řešeny povinnosti zaměstnanců a smluvních stran vycházející z jejich začlenění v organizaci. I když jsou již některá z opatření aktuálně v organizaci zavedena, je nutné jejich přezkoumání dle požadavků ISMS.

3.5.3.1 Před vznikem pracovního poměru

Než je se zaměstnancem uzavřena pracovní smlouva je prověřena jeho vhodnost na vypsanou pozici. Tato vhodnost je krom dalších osobnostních požadavků již v současnosti posuzována na základě dokladu o dosažení vzdělání doloženém vysokoškolským diplomem, maturitním vysvědčením nebo výučním listem. U pozic, které vykonávají vysoce kvalifikovanou činnost spojenou s důvěrností nebo financemi, je prověřován profesní životopis žadatele u jeho předchozích zaměstnavatelů. Vzhledem k faktu, že v organizaci tohoto typu nemohou pracovat osoby se záznamem v rejstříku trestů, je po žadateli požadován aktuální výpis. Všichni zaměstnanci včetně externistů s umožněným přístupem k osobním údajům podepisují dohodu o zachování mlčenlivosti. Všechny tyto požadavky jsou v souladu se systémem řízení bezpečnosti informací a není nutné je tedy měnit.

3.5.3.2 Během pracovního poměru

Během pracovního poměru je zapotřebí zaměstnancům neustále připomínat jejich povinnosti a zajistit jejich plnění.

Odpovědností managementu organizace je vyžadování respektu k bezpečnostním politikám organizace ze strany zaměstnanců. Tento respekt může podpořit vhodná motivace zaměstnanců.

Vzdělávání a školení o bezpečnosti informací je vhodnou formou, kterou lze dále rozvíjet své zaměstnance v případě potřeby i pomocí externistů. Tento program by měl být realizován v souladu s politikami organizace. Program je třeba tvořit na míru činnostem, které jsou vykonávány zaměstnanci. Program by měl být aktualizován a měly by do něj být zahrnovány poučení z bezpečnostních incidentů. Toto by mělo zajistit, že se již nebudou opakovat. V případě změny pozice je třeba, aby tento nebo tito zaměstnanci absolvovali školení relevantní k nové pozici.

3.5.3.3 Ukončení pracovního poměru

V současné době organizace nemá zpracovaný formální postup, který by byl uplatňován v případech ukončení pracovního poměru. Proto navrhuji tento postup formálně zdokumentovat včetně činností, které jsou třeba vykonat, než bude pracovní poměr s definitivní platností ukončen. V tomto postupu je třeba dbát na to, aby byly na prvním místě chráněny zájmy organizace, a to především ty zájmy týkající se bezpečnosti informací. Tedy měla by být se zaměstnancem uzavřena dohoda, které stanoví dobu po ukončení pracovního poměru, po kterou není možné sdělovat postupy nebo důvěrné informace z prostředí současné organizace.

3.5.4 A.8 Řízení aktiv

Pro usnadnění a efektivnější ochranu aktiv je nutné v organizaci vytvořit seznam aktiv. Seznam bude usnadňovat práci s aktivy i mimo řízení bezpečnosti informací. Příkladem může být případ, když se organizace bude rozhodovat o pojištění svých aktiv. V tomto seznamu by měla být uvedena veškerá aktiva včetně jejich významu pro organizaci. Tento seznam je třeba udržovat neustále aktualizovaný. Data v něm musí být přesná. V případě informací by měl být ještě zdokumentován jejich celý životní cyklus. Tedy jak a kým byly informace vytvořeny, jak a kým jsou zpracovávány, kde jsou tyto informace uloženy, kdo a kdy data vymazal, případně zničil. Pokud jsou přenášena mimo organizaci, mělo by dojít k zdokumentování, jak s nimi v tomto průběhu bylo nakládáno. Všem aktivům je třeba určit vlastníka, který za ně bude nést zodpovědnost. Tuto zodpovědnost je vhodné určit již při nabývání daného aktiva. Vlastníkem nemusí být pouze jednotlivec, ale případně i skupina osob. Veškeré osoby využívající aktiva organizace musí vědět, jak s konkrétním aktivem mohou nakládat.

3.5.4.1 Při ukončení spolupráce s organizací

K ukončení spolupráce s organizací je nutné vytvořit jeho oficiální postup. Nutností je vytvořit pro každého zaměstnance seznam aktiv se kterými disponuje a při každém přidělení aktiv je třeba tento seznam aktualizovat. Tento seznam bude sloužit při ukončení pracovního vztahu jako seznam aktiv, které bude jejich uživatel vracet.

Dle požadavků GDPR je třeba informace obsahující osobní údaje klasifikovat jako kritická. Tedy doporučuji zavést smysluplné označení těchto dokumentů, aby bylo ihned patrné, jestli obsahují osobní údaje, či nikoliv. V případě, že daný dokument, přenosné uložiště nebo elektronický dokument obsahuje osobní údaje bude označen. Pro aktiva je důležité zpracovat pokyny pro nakládání s nimi. Tyto postupy by měly obsáhnout omezení přístupu k aktivům podle organizační úrovně. Tato povolení k přístupu musí organizace evidovat.

3.5.4.2 Manipulace s výměnnými médii

Je třeba stanovit povolené manipulace s výměnnými médii. Pokud toto médium je vyřazeno z oběhu organizace je třeba z tohoto média odstranit veškerý obsah takovým způsobem, který znemožní obnovení obsahu. Tato média je třeba skladovat v bezpečném prostředí, které vyhoví specifikacím výrobce na prostředí, kde lze tato média uchovat. Jelikož organizace na média klade důraz na důvěrnost a integritu, je třeba veškeré informace na těchto médiích šifrovat. Data slouží pouze k dočasnému přenosu informací, proto je nutné, aby organizace stanovila takový typ média, na kterém budou tyto informace čitelné po požadovanou dobu.

3.5.4.3 Likvidace médií

Jediným spolehlivým a bezpečným zlikvidováním, které neumožní případný únik důvěrných informací, je fyzická likvidace daného média. Proto již v současné době organizace disponuje skartovacím zařízením pro papírovou formu informací. Ovšem je třeba vyřešit zbylá média jako jsou flashdisky nebo jiná elektronická úložiště dat. Mým návrhem organizaci je, aby tato elektronická média shromažďovala na bezpečném místě uvnitř své organizace a byla pro tato média sjednána služba, která provede jejich fyzickou likvidaci. Samozřejmostí je, že tato firma musí vystavit organizaci protokol o tom, jak bylo médium zlikvidováno a jak byl dále zlikvidován tento odpad.

3.5.5 A.9 Řízení přístupu

Omezení přístupu k jednotlivým informacím a vybavení pro zpracování informací je řešeno již v současnosti. Je jen nutné k těmto přístupům zřídit politiky, podle kterých se budou řídit a budou v nich zdokumentovány. Toto řízení přístupu bude nutné řešit i v případě, že organizace zřídí nové bezpečnostní perimetry pro ukládání dat. V těchto politikách je také třeba uvést, jak a kým budou přístupy přidělovány a také odebírány. Veškerá tato práva je třeba uvést pro přehlednost do seznamů, které budou uloženy na bezpečném místě a ty v pravidelných intervalech přezkoumávat. Tyto intervaly je třeba nastavit tak, aby seznamy přístupových práv byly stále aktuální.

3.5.5.1 Systém správy hesel

Oblast, která není v organizaci aktuálně řešena, je správa hesel. Tuto oblast je třeba ošetřit pomocí politik pro správu hesel. Politiky by měly obsahovat postupy nutné při změně hesel nebo při vynucení jejich změny. Tyto změny mohou být vynuceny například při prvním přihlášení uživatele do daného systému, kdy mu bylo implicitně vygenerováno heslo pouze pro první přihlášení.

3.5.5.2 Řízení přístupu k systémům a aplikacím

Každý užívaný informační systém v organizaci má v sobě již tento systém zabudován. Daná politika by tedy měla stanovit, jak daný systém nastavit, pokud je to možné. Pokud informační systém neumožňuje tento systém individuálně nastavit a má již přednastavené postupy mimo soulad s politikou organizace, je k těmto postupům třeba určit politiku, která případné nedostatky daného systému ošetří na straně uživatelů. Aplikace by měly být nastaveny takovým způsobem, aby při zadávání hesel nebyla hesla čitelná. Musí být vytyčeny body které musí heslo splňovat, aby bylo považováno za bezpečné a dostatečně kvalitní.

3.5.6 A.10 Kryptografie

Pro bezpečnost organizace je třeba přijmout opatření využívající kryptografie, která zajistí ochranu autenticity, důvěrnosti a taktéž integrity.

Tyto prostředky je třeba využívat v případech, kdy je nakládáno s citlivými osobními daty, pokud u nich nelze provést anonymizaci. Jelikož organizace zpracovává citlivé osobní údaje, je nutné využívat kryptografických prostředků v co největší možné míře. Vzhledem k faktu, že organizace využívá programové vybavení od společnosti ESET, je vhodné využít kryptografických prostředků z jejich portfolia. To pro organizaci bude znamenat provedení upgradu současných licencí pro ESET Internet Security na nové licence pro ESET Smart Security Premium, které umožňují šifrování souborů a výměnných médií. Tato úroveň šifrování je dostatečná pro tuto organizaci.

3.5.6.1 Správa klíčů

Protože je u kryptografických prostředků třeba využívat klíčů, je nutné pro ně vypracovat a realizovat politiku jejich životního cyklu a ochrany. V rámci této politiky musí být řešeno, jak a jaké klíče budou generovány pro konkrétní kryptografické systémy nebo aplikace. Dále by měla aplikace podporovat ukládání, archivaci, znovuzískání, distribuci, vyřazení a zničení klíče. Modul pro správu hesel obsahuje řešení pomocí ESET Smart Security Premium, který by tyto podmínky pro zvolenou organizaci plně pokrýval bez nutnosti další nákladů. Vniknou pouze náklady na proškolení uživatelů, nebo vypracování materiálů pro sebevzdělávání uživatelů včetně následného testování nabytých znalostí.

3.5.7 A.11 Fyzická bezpečnost a bezpečnost prostředí

Fyzická bezpečnost je v současnosti již řešena na takové úrovni, kde jsou uvažovány oblasti, kde jsou zpracovávány citlivé nebo kritické informace, nebo je zde umístěno vybavení zpracovávají dané informace.

Pro zvýšení bezpečnosti perimetru organizace je již v současné době zřízena vrátnice s obsluhou, u které se musí ohlásit veškeré osoby vstupující do fyzického perimetru

organizace. Tím, že je vyžadováno ohlášení osoby, za kterou osoba vyžaduje přístup, se předpokládá zvýšení bezpečnosti perimetru. Tímto opatřením by mělo být zamezeno vstupu neoprávněných osob do perimetru, nebo jejich počet minimalizovat. Mělo by to omezit především osoby mající za cíl neblahé zapůsobení na některé ze zabezpečení.

Pro ještě vyšší bezpečnost uvnitř perimetru navrhuji organizaci zřízení fyzických bezpečnostních perimetrů, které budou rozčleněny podle aktiv, která zde budou uloženy. Prvním z těchto perimetrů by měla být samostatná místnost, serverovna, v níž budou uloženy veškeré centrální síťové prvky, které budou chráněny elektronickým zabezpečovacím systémem napojeným na pult centrální ochrany. Tím bude ošetřen neoprávněný fyzický přístup k síťovým prvkům.

Druhým navrhovaným bezpečnostním perimetrem je místnost, do které budou ukládány veškeré fyzické dokumenty a média, která již nejsou třeba pro aktuální chod organizace. Uvnitř perimetru budou umístěny uzamykatelné skříně. K jednotlivým skříním budou mít přístup pouze osoby oprávněné k přístupu. I zde bude řízena kontrola fyzického vstupu za pomoci EZS, který již nebude napojen na pult centrální ochrany. Bude však spuštěn lokální hlasitý alarm a bude upozorněna bezpečnostní služba nacházející se v organizaci.

Pro zvýšení zabezpečení proti neoprávněného vstupu do kanceláří, místností s daty a zařízením s nimi pracujícími navrhuji opatření ve formě odstranění klik z vnějšku dveří. Přístup budou mít pouze osoby oprávněné ke vstupu vlastnictvím fyzického klíče od dveří. Ta pracoviště, kde neprobíhá nepřetržitý provoz, je třeba též opatřit elektronickým zabezpečovacím systémem s napojením na pult centrální ochrany.

Všechny osoby s přístupem a odpovědností za celou, nebo pouze za část některé z bezpečnostního perimetru, budou seznámeni s postupy, které je třeba pro dodržení úrovně zabezpečení dodržovat.

Z oblasti pro nakládku a vykládku je přístup do perimetru organizace zabezpečený bezpečnostními dveřmi, které jsou vždy zamčené. V této oblasti se nenachází žádné vybavení pro zpracování dat a nenachází se zde osobní údaje. Pro zvýšení bezpečnosti navrhuji, aby byl zakázán vstup do prostor s dveřmi oddělující tuto oblast a vnitřní perimetr organizace neoprávněnou osobou.

Pro ochranu zařízení proti vlivu okolí navrhuji jejich umístění do rozvaděčů. Pro všechny rozvaděče jsou, nebo budou vybrána taková místa, která většinu z vlivů prostředí eliminují nebo je minimalizují. Omezení přístupu k zařízením umístěným v serverovně bylo řešeno v předchozí podkapitole. U ostatních prvků navrhuji při realizaci nové sítě umisťovat podružné rozvaděče do míst s omezeným přístupem, jako jsou třeba jednotlivé kanceláře.

Ve všech rozvaděčích navrhuji aplikovat záložní zdroje elektrické energie, které zajistí chod těch zařízení, po kterých by bylo nutné komunikovat i v případech výpadku elektrické energie.

Nové kabelové rozvody je třeba umístit do míst, která zajistí jejich ochranu proti poškození, odposlechem a rušením. Jedním z mnou navrhovaných míst je umístění těchto rozvodů do bezpečnostních kabelových žlabů umístěných do rozebíratelných stropních podhledů. Již toto samotné umístění zajistí jejich ochranu proti jejich náhodnému poškození. Ve spojení s bezpečnostními žlaby je zajištěno opatření proti odposlechu a jejich úmyslnému poškození bez použití řezné techniky. Aby nebyla komunikace rušena, je třeba ji umístit co nejdále od rozvodů silové energie. Další umístění jsou již proprietární a musí být řešeny v rámci projektu. Pro kontrolu správnosti projektu navrhuji organizaci konzultace s odborným technikem, případně provést kontrolu svépomocí podle literatury uvedené pod číslem deset v seznamu literatury této diplomové práce.

Dále navrhuji organizaci zavedení řízení aktiv při jejich přesunech nebo údržbě. V případě přemisťování aktiva mimo organizaci je třeba zajistit souhlasy garanta aktiva a osoby odpovědné za bezpečnost. Dále navrhuji organizaci, aby vyžadovala protokoly v případě údržby nebo opravy aktiv, že nebyla narušena jeho integrita, důvěrnost nebo dostupnost. V protokolu by měla být uvedena identita všech osob, kdo s aktivy zacházel.

Dalším opatřením, které navrhuji do organizace zavést, jsou zásady prázdné obrazovky a prázdného stolu. Tyto zásady snižují riziko zneužití, ztráty nebo poškození aktiv v době, kdy jsou mimo dohled odpovědné osoby, a to jak v pracovní době, tak i mimo ni. Je tedy nutná vyměnitelná media nebo informace v papírové podobě pokud již nejsou užívána, uchovávat v uzamčeném prostoru.

3.5.8 A.12 Bezpečnost provozu

Tato opatření cílí na bezpečnost při běžném provozu organizace. Je třeba, aby byly zdokumentovány veškeré postupy a odpovědnosti spojené s vybavením pro zpracování informací.

V organizaci je třeba zpracovat dokumentaci k ošetření rutinních procesů a postupů v případě zpracování informací o nakládání s aktivy organizace. Pro jednotnou bezpečnost v celé organizaci je zapotřebí, aby byly ve spolupráci s odborníky vypracovány provozní pokyny pro instalaci a konfiguraci použitých systémů. Bez těchto zpracovaných pokynů může být v některém ze systémů (kupříkladu z důvodu jiné konfigurace) vynecháno některé důležité bezpečnostní nastavení.

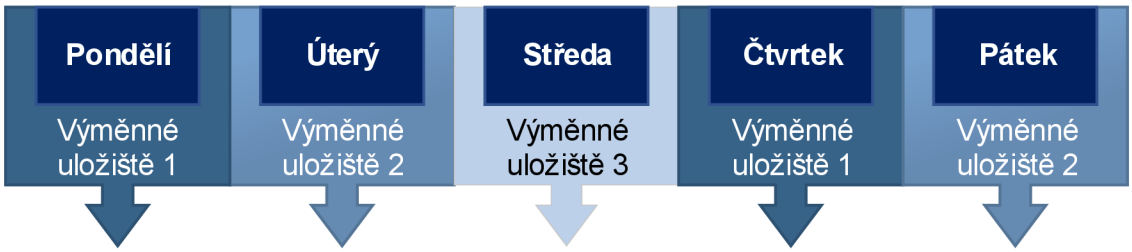
V případě, že při zpracování některé z úloh vnikne neočekávaná chyba nebo jiné výjimečné podmínky, je pro ně stanoveno telefonní číslo technické podpory, která danou situaci pomůže ošetřit, případně zajistí vyslání technika na místo, pokud to situace vyžaduje. Výjimečnou podmínkou je selhání systému. V těchto případech je uživatelům zakázáno do systému jakkoliv zasahovat a okamžitě musí zavolat na technickou podporu.

Veškeré významné změny v organizaci je třeba řídit a kontrolovat. Tyto změny mohou být řízeny za pomoci Lewinova modelu řízení změny. Pokud změny chceme řídit, je zapotřebí tyto změny detailně popsat a zaznamenat je. Následuje plánování změny, pokud je to třeba, může být změna vyzkoušena, zdali je pro organizaci vyhovující. I na tuto významnou změnu může být aplikováno projektové řízení. Proto je třeba posoudit, jaký dopad bude mít tato změna na bezpečnost v organizaci. Pokud změna zatím všem podmínkám vyhověla, je třeba v organizaci stanovit formální postup pro schvalování těchto změn. Po schválení změny je zapotřebí ověřit splnění požadavků bezpečnosti informací. Dále je nutné s touto změnou podrobně seznámit všechny zaměstnance, kterých se tato změna dotkne. Je nutné zpracovat postupy v případě, že by nebylo možné změnu korektně dokončit.

Ochrana před malwarem je v organizaci řešena za pomoci automatizované pokročilé internetové ochrany od firmy ESET, kterou jsou opatřeny všechny pracovní stanice. Tyto stanice se tedy chrání před ostatními, ale chrání i ostatní samy před sebou. Tento

software se automaticky aktualizuje, a to včetně své databáze obsahující potřebné informace k udržení dostatečné bezpečnosti systému klientských stanic.

Pro zálohování v organizaci je třeba zřídit samostatnou politiku. Je to jedno z nejúčinnějších bezpečnostních opatření, které může organizaci zachránit před nemalými finančními ztrátami. Do této politiky je třeba zpracovat postup záloh pro jednotlivé informační systémy. Je třeba v ní uvést místo, nebo více míst, kam budou tyto zálohy ukládány. Nejvhodnější místa pro uložení těchto záloh jsou ta, která nejsou běžně dostupná, když je zařízení spuštěné nebo přístupné ze sítě. Prvním navrženým místem jsou výměnná uložiště, na kterých budou zálohy šifrovány. Tyto fyzické nosiče budou následně uloženy na vyhrazeném místě, které bude uzamykatelné. Pro ještě vyšší bezpečnost navrhuji organizaci používání více takových výměnných uložišť a střídat je v intervalu jeden den – pro názornost jsem vytvořil grafické znázornění (viz. obrázek 5). Kupříkladu budou použita tři výměnná uložiště, kde na každé z nich budou uloženy zálohy v pro ně určený den po ukončení práce. Tato uložiště budou střídána, tedy daný odpovědný subjekt bude mít pro případ nouze zálohy z předešlých dvou dnů.



Obrázek 5 Proces správy výměnných uložišť při zálohování (Zdroj: Vlastní zpracování)

Dále je navrhnuto organizaci zajištění úložného prostoru mimo její perimetr, kam budou zašifrované zálohy přenášeny. Jelikož budou zálohy mimo perimetr, nevztahují se na ně rizika organizace. Jako výhodu můžeme zmínit například ochranu před malwarem. Rozhodujícím faktorem je špičková úroveň vybavení a zabezpečení datových center a cena dané outsourcované služby. V této oblasti již připravuje zřizovatel datové úložiště, které bude k dispozici pro své zřizované organizace zdarma.

3.5.9 A.13 Bezpečnost komunikací

Při přenosech citlivých informací je třeba tuto komunikaci chránit před odposlechem, kopírováním, pozměněním nebo chybným směrováním. K tomuto cíli je třeba směrovat veškeré související činnosti a vypracovávané politiky.

Správa bezpečnosti sítě již aplikována v organizaci je. Síť je řízena za pomoci routerů a řízených switchů umožňující logické oddělení sítě za pomoci VLAN. Síť je dělena i fyzicky, kde je oddělena síť pro klienty a síť pro potřeby organizace. Veškerá opatření správy, řízení i kontroly sítě jsou outsourcována, proto je třeba smluvně ošetřit, aby vybraná firma plnila bezpečnostní opatření obsažená v politikách organizace.

3.5.10 A.14 Akvizice, vývoj a údržba systémů

Tato oblast opatření není pro organizaci aplikovatelná. Jelikož je pouhým uživatelem těchto systému, které kupuje jako krabicové řešení, nebo si je najímá jakou službu.

3.5.11 A.15 Dodavatelské vztahy

Organizace musí vytvořit ve spolupráci s dodavateli politiky pro přístup k jejím aktivům. Tyto politiky mají za úkol snížit rizika, která s tímto přístupem mohou vzniknout. Tyto politiky musí být diskutovány s každým z dodavatelů, kteří je musí odsouhlasit. Pro každého dodavatele s přístupem k aktivům je třeba tyto dohodnuté podmínky zdokumentovat smlouvou.

3.5.12 A.16 Řízení incidentů bezpečnosti informací

Organizace musí stanovit dostatečně jasné a přesné postupy pro potřeby zvládnutí události bezpečnosti informací. Tyto postupy musí obsahovat kontakt na odpovědnou osobu. Dále musí uvést, jak se zachovat v případech, když odpovědná osoba není k dispozici a na danou událost nemůže zareagovat osobně. Odpovědná osoba v době přítomnosti v organizaci tuto událost prošetří a zhodnotí, zdali se jednalo o událost, nebo se stala již incidentem, vše zdokumentuje a zvolí další postup.

3.5.12.1 Hlášení slabých míst

V organizaci mohou nastat případy, kdy některý ze zaměstnanců nebo externistů při přístupech k informačním systémům nebo některým přidruženým službám může v některém z těchto aktiv, najít slabé místo zabezpečení. Toto slabé místo by mohlo vést k ohrožení dostupnosti, integrity nebo důvěrnosti daného aktiva. Je důležité, aby slabé místo bylo nahlášeno odpovědné osobě za toto aktivum. Je nutno veškeré tyto osoby upozornit, aby se tuto slabinu nepokoušeli sami prokazovat. Mohlo by tím totiž dojít k poškození aktiva nebo ztrátě osobních údajů z něj.

3.5.13 A.17 Aspekty řízení kontinuity činností organizace z hlediska bezpečnosti informací

Během nepříznivých situací v organizaci je třeba zajistit, aby zabezpečené perimetry byly uzamknuté a tím bylo zamezeno přístupu k informacím organizace. Toto uzamknutí je třeba v těchto případech pouze zkontrolovat. Tyto zóny nikdy nesmí zůstat odemknuté i při běžné činnosti v organizaci. Jelikož většina z tištěné dokumentace má svůj původ v elektronické podobě, není nutné většinu z těchto dokumentů chránit. Je třeba chránit pouze ty dokumenty, které jsou opatřeny podpisy a jsou nezbytné pro chod organizace. Pro tyto dokumenty je třeba zřídit vzduchotěsný a žáruvzdorný trezor, který dokáže zabezpečit tyto dokumenty před zničením v případě, kdy nastane nepříznivá situace v organizaci.

3.5.13.1 Redundance

V současné době není v organizaci zjištěna potřeba vyžadující nutnost redundance pro žádné z opatření nebo zařízení. Přesto navrhuji organizaci provést redundanci na páteřních vedeních komunikačního systému. Ty pomohou zajistit organizaci v dostatečné míře její požadavky na dostupnost. Toto opatření bylo vybráno z historických událostí, kdy v případě rekonstrukce části budovy, kterou právě procházelo páteřní vedení bylo nutné toto vedení na několik dnů odstranit kvůli potřebám rekonstrukce. V tu chvíli by se ocitlo celé oddělení organizace bez přístupu

k potřebným informacím uložených na serveru. Tím vnikly náklady na vytvoření provizorního redundantního páteřního vedení mimo tuto rekonstruovanou část.

3.5.14 A.18 Soulad s požadavky

Pro soulad se všemi zákonnými a smluvními požadavky je třeba, aby organizace vytvořila seznam všech legislativních a smluvních požadavků, které musí plnit.

Organizace již v současnosti disponuje a klade důraz pouze na využívání takového software, aby nebylo porušováno duševní vlastnictví. Tedy za všechno svoje softwarové vybavení řádně platí buď pořizovací anebo udržovací poplatky. V celé organizaci je zakázáno instalovat jakýkoliv software. Instalace je možná pouze ICT technikem. Tento technik ručí organizaci, že je instalován pouze software, kterým organizace disponuje, anebo může případně disponovat bez porušení duševního vlastnictví.

Dle klasifikačního schématu pro informace jsou vybrány ty záznamy, které je třeba ochránit a po jakou dobu. Podle této doby musí organizace vybrat vhodná média, která musí vybranou dobu informace udržet. Jelikož každé médium v čase informaci ztratí s tím, že tento čas je jiný pro různá média. Je třeba, aby se organizace řídila doporučeními výrobce daného média.

3.5.14.1 Přezkoumání ISMS

Po zavedení systému bezpečnosti řízení je nutné, aby organizace zhodnotila, zda tento systém byl implementován a je provozován tak, jak byly navrženy jednotlivé politiky a postupy v nich. Přezkoumání by mělo probíhat v naplánovaných intervalech a mimo plánované intervaly v těch případech, kdy nastane významná změna. Toto přezkoumání by mělo proběhnout nejlépe subjektem nezávislým k organizaci.

Osoba zodpovědná za systém řízení bezpečnosti informací by měla zajistit, že tento systém bude pravidelně přezkoumáván, jestli je stále ve shodě se zákony, normami, nařízeními a podobně, které jsou relevantní k bezpečnosti informací. Do tohoto přezkoumávání by měly být zahrnuty také informační systémy, neboť musí být v souladu s politikami nastavenými organizací.

3.6 Serverovna

Jelikož je současné řešení serverovny nevyhovující, bylo rozhodnuto o nutnosti v co nejbližším termínu zřídit novou serverovnu. V tomto nově zvoleném prostoru pro umístění serverovny je třeba zajistit několik základních pravidel.

3.6.1 Umístění serverovny

Jelikož se vybraný prostor nachází v přízemí, není třeba se zabývat nosností stropů a podlah. Dalším faktorem je umístěni organizace mimo vodní zdroje, které by serverovnu mohly v případě záplav zatopit.

3.6.2 Technické vybavení

Pro nové umístění centrálního uzlu komunikační infrastruktury (serverovny) je nutné zvážit několik technických opatření. Některá z nich zajistí spolehlivý chod zařízení, jiná cílí na bezpečnost daných zařízení. Tato opatření budou pouze doporučující. Je následně na rozhodnutí organizace, které z nich převede do praxe.

V případě serverovny je třeba zajistit dostatečně silný záložní zdroj elektrické energie, který bude schopný udržet v chodu k němu připojené techniky po takovou dobu, po kterou je nutný provoz daného zařízení. U serverů a síťových uložišť je nutné prodloužení doby napájení k tomu, aby stihly tyto prvky korektně ukončit svoji činnost a bezpečně se vypnout.

Jelikož aktivní prvky vytvářejí při své činnosti spousty odpadního tepla, je třeba především v letních měsících zajistit, aby ve spojení s vysokou teplotou prostředí a vytvořeným teplem nedošlo k omezení činnosti nebo poškození zařízení umístěných v serverovně. Udržování nízké teploty má na starost jednotka klimatizace, kterou je zde třeba umístit. Tím, že budou zařízení pracovat v kontrolovaném, pokud možno neměnném a pro ně vhodném prostředí, prodlouží se jejich životnost.

Pro případ vznícení některého z aktivních prvků je vhodné skříň typu RACK opatřit kapslí naplněnou látkou pohlcující kyslík potřebný k hoření. Hašení jakýmkoliv jiným způsobem vede ke zničení ostatních prvků ve skříni a vznikne tak vyšší škoda, než je hodnota dané kapsle.

Další vybavení této místnosti, jako jsou na příklad kabelové žlaby, je nutné řešit v projektu pro celou komunikační síť.

3.7 Komunikační síť

Zřizovatel organizace má v plánu zřízení nové ICT sítě z důvodu zastarání té současné. Proto je zapotřebí dostatečně kvalitně stanovit podobu nové ICT sítě. Tato síť by měla dbát nejen na bezpečnost, ale především na její spolehlivost a dostupnost. Proto v této podkapitole budou stručně navrženy základní obecné požadavky, postupy a návrhy sítě pro tuto konkrétní příspěvkovou organizaci.

3.7.1 Motivace kvalitního zpracování komunikační sítě

Jak již bylo zmíněno v teoretických východiscích práce, kabelážní systém zapříčinil 70 % selhání komunikačního systému. Je třeba vzít v úvahu cenu kabelážního systému vůči celkovým nákladům na investici. Pro tento nepoměr navrhuji organizaci věnovat kabelážnímu systému náležitou pozornost a nezanedbat žádný detail v návrhu, jelikož i u kabelážního systému platí princip nejslabšího článku.

3.7.2 Analýzy

Při zpracování návrhu komunikační sítě je třeba začít analýzou současného stavu, která již byla popsána. Z té vyplývá, že současná síť je nevyhovující v celém jejím rozsahu. Důvodem je zhotovení současné sítě z nekvalitní kabeláže a obecně nedostatečného provedení sítě. Proto je třeba udělat celou ICT síť kompletně znovu. K tomu bude třeba vytvořit obecný návrh sítě. Na kvalitě jeho zpracování závisí kvalita celé budoucí počítačové sítě.

Nejdůležitějším krokem v tomto procesu je nutnost, aby organizace do co největších detailů popsala své požadavky na budoucí komunikační infrastrukturu. Pokud tyto požadavky nebudou dostatečně detailně definovány a popsány, nemůže v žádném případě vzniknout kvalitní realizace komunikační infrastruktury.

Další organizací vypracovanou analýzou je ta popisující osazení místností a tím počty portů v jednotlivých místnostech. Vzhledem k rostoucím nárokům na ICT síť doporučuji organizaci nepodcenit počty portů v jednotlivých místnostech.

Jelikož by se mohly v organizaci v budoucnu objevit prvky zkvalitňující péči o klienty požadující konektivitu na internet, bylo by vhodné udělat analýzu požadavků těchto prvků dostupných již dnes. Zaměřit se na to, zdali tyto prvky nemají speciální požadavek na přenos. K přihlídnutí vytížení a předmětu podnikání organizace doporučuji konzultaci všech těchto analýz s odborníkem nebo odborníky na ICT.

3.7.3 Dosah komunikačních kanálů

Při kontrole vypracovaného projektu je důležitá kontrola dosahu komunikačních kanálů. U metalického vedení je nutné, aby délka kanálu nepřesáhla sto metrů. U optického vedení nelze univerzálně určit jeho maximální délku, proto zde též doporučuji konzultaci s odborníkem.

3.7.4 Další doporučení

Jelikož další řešení v rámci komunikační sítě vyžadují odborné znalosti, není v silách organizace další postupy problematiky řešit vlastními silami. Proto je třeba konzultací s nezávislým oborníkem, který organizaci pomůže s korekcí projektu na jeho špičkovou úroveň, případně zajistí odborný dohled nad celou realizací komunikační infrastruktury.

3.8 Ekonomické zhodnocení

V této kapitole budou shrnuty veškeré náklady spojené s navrženými opatřeními. Tato opatření nepřinesou organizaci žádný ekonomický zisk. Ve spojení s těmito opatřeními vzniknou organizaci pouze náklady, které však budou vyváženy zvýšením bezpečnosti v organizaci. Díky popisu postupů a jejich sjednocení v celé organizaci by měly přinést

zrychlení a usnadnění práce. Po jejich zavedení by také mělo klesnout riziko vystavení organizace nějaké sankci.

Pro vyjádření nákladů na celou navrhovanou změnu v organizaci bylo zapotřebí ve spolupráci s odborníkem na bezpečnost informací odhadnout časy potřebné pro realizaci opatření z jednotlivých oblastí.

Tabulka 7 Časový plán pro zavedení opatření (Zdroj: Vlastní zpracování)

	Název	Doba pro zavedení [h]
A.5	Politiky bezpečnosti informací	3
A.6	Organizace bezpečnosti informací	8
A.7	Bezpečnost lidských zdrojů	6
A.8	Řízení aktiv	16
A.9	Řízení přístupu	5
A.10	Kryptografie	8
A.11	Fyzická bezpečnost a bezpečnost prostředí	32
A.12	Bezpečnost provozu	5
A.13	Bezpečnost komunikací	3
A.14	Akvizice, vývoj a údržba systémů	---
A.15	Dodavatelské vztahy	10
A.16	Řízení incidentů bezpečnosti informací	5
A.17	Aspekty řízení kontinuity činnosti organizace z hlediska bezpečnosti informací	2
A.18	Soulad s požadavky	12
	Hodin celkem:	115

Na základě odhadů z časového plánu pro zavedení opatření byly vypočítány finanční náklady na tato opatření. Vybraný odborník pro konzultace časové náročnosti měl stanovenou hodinovou sazbu 900 Kč. Na základě této ceny byly provedeny výpočty veškerých nákladů na práci. V tabulce finančního vyjádření pro jednotlivá opatření jsou shrnuty náklady jak na práci, tak na nákup potřebných technických prostředků. Celkové náklady činní 186 500 Kč. Tato suma je pouze odhadem a je závislá na hodinové sazbě konzultanta vybraného organizací. V této sumě nejsou zahrnuty slevy a jedná se o koncové ceny včetně DPH.

Náklady na technické vybavení skupiny opatření A.10 jsou složeny z nákupu nových programových licenci programu pro internetové zabezpečení ESET. Pro oblast A.11 je stanoven pouhý odhad ceny potřebného řešení na základě konzultace s odborníkem přes elektronická zabezpečovací zařízení. Pro oblast A.12 je tato suma vyčíslena jako nákup výměnných médií pro potřeby záloh. Ekonomické vyjádření není řešeno pro změnu v komunikační infrastruktuře, jelikož je v předprojektové fázi.

Tabulka 8 Finanční vyjádření pro jednotlivá opatření (Zdroj: Vlastní zpracování)

	Výpočet nákladů práce [h, Kč]	Celkem za práci [Kč]	Výpočet nákladů na technické vybavení [h, Kč]	Celkem za náklady na technické vybavení [Kč]	Celkem [Kč]
A.5	3 × 900	2 700	0	0	2 700
A.6	8 × 900	7 200	0	0	7 200
A.7	6 × 900	5 400	0	0	5 400
A.8	16 × 900	14 400	0	0	14 400
A.9	5 × 900	4 500	0	0	4 500
A.10	8 × 900	7 200	30 × 400	12 000	19 200
A.11	32 × 900	28 800	1 × 65 000	65 000	93 800
A.12	5 × 900	4 500	15 × 400	6 000	10 500
A.13	3 × 900	2 700	0	0	2 700
A.14	---	---	---	---	---
A.15	10 × 900	9 000	0	0	9 000
A.16	5 × 900	4 500	0	0	4 500
A.17	2 × 900	1 800	0	0	1 800
A.18	12 × 900	10 800	0	0	10 800
		∑ = 103 500		∑ = 83 000	
				Celkem za všechna opatření:	186 500

4 ZHODNOCENÍ A PŘÍNOSY PRÁCE

V rámci zhodnocení této diplomové práce lze konstatovat, že byl zpracován podrobný návrh na zavedení systému řízení bezpečnosti informací pro organizaci, se kterou jsem navázal úzkou spolupráci. Spolupracující organizace se nacházela v situaci, kdy si vedení organizace velmi dobře uvědomovalo naléhavost potřeby vnesení určitých pravidel pro uživatele ICT v organizaci a zároveň významným způsobem posunout bezpečnostní povědomí svých zaměstnanců.

Výstupem této oboustranně výhodné spolupráce je zpracovaný návrh na zavedení systému řízení bezpečnosti informací, který je dané organizaci šitý na míru a lze jej tedy bez větších problémů postupně implementovat do každodenní praxe.

Další nespornou výhodou je fakt, že se podařilo skloubit požadavky systému řízení bezpečnosti informací s požadavky kladenými nařízením GDPR.

K přínosům této práce lze také přiřadit vyhodnocení současného stavu organizace za pomoci asistovaného zhodnocení, což umožnilo poukázat na silné i slabé stránky a nastavit správný směr, kterým je třeba se v rámci vnitřní bezpečnostní politiky ubírat. Tato vhodně nastavená vnitřní bezpečnostní politika má dopady i na finanční stránku, neboť by následně neměly vznikat organizaci zbytečné náklady na nesystémová opatření.

Tím, že byl vypracován program budování bezpečnostního povědomí pouze ve zkušebním režimu a odzkoušen na malém vzorku zaměstnanců, umožnil odladit a doplnit požadavky organizace na ucelené vzdělávání v této oblasti bez zbytečných vícenákladů.

Při konzultacích s vedením organizace byly vzneseny požadavky z více oblastí, přesto se je podařilo dobře propojit a popsat v návrzích opatření. Tím, že celá práce byla konzultována s hlavní ekonomkou organizace lze veškeré opatření a návrhy zavést bez větších problému do praxe, což znamená, že návrhy jsou reálné a realizovatelné. Hlavní ekonomka chápala důvody a potřebu zavedení řízení bezpečnosti informací a stejně tak vnímala významnou potřebu ochránit osobní a citlivé údaje, které se v organizaci zpracovávají. V rámci jednotlivých konzultací tak vlastně absolvovala školení v rámci budování bezpečnostního povědomí na míru jejího začlenění do organizací struktury.

Veškerá vybraná a navržená opatření mají za úkol co nejvíce snížit pravděpodobnost vzniku hrozby nebo jejímu vzniku úplně zabránit.

ZÁVĚR

Hlavním cílem stanoveným na začátku diplomové práce bylo zpracování návrhu pro zavedení systému řízení bezpečnosti informací a vypracování programu budování bezpečnostního povědomí pro vybranou příspěvkovou organizaci. Pro splnění vytyčeného hlavního cíle této diplomové práce bylo nutné splnit všechny dílčí cíle s ohledem na požadavky vybrané příspěvkové organizace.

Prvním dílčím cílem bylo vypracování teoretické základny řešeného problému. Zde bylo nezbytné vymezit terminologii tak, aby byla srozumitelná i pro osoby, které se v dané problematice nepohybují a neznají odborné pojmy.

V rámci druhého dílčího cíle byly provedeny všechny potřebné analýzy, na základě kterých byl podrobně popsán aktuální stav organizace nejen z pohledu řízení lidských zdrojů, ale zejména byla pozornost zaměřena na to, v jakém stavu se nachází oblast zpracování osobních a citlivých údajů, jak jsou tato data chráněna před možnými hrozbami, v jakém stavu se nachází systém ICT v organizaci a jaké jsou stávající politiky řízení bezpečnosti.

Zjištění a utřídění všech informací o aktuálním stavu v organizaci bylo podkladem pro naplnění třetího dílčího cíle, což bylo vytvoření vlastního návrhu řešení šitého na míru spolupracující příspěvkové organizace a jeho implementace do běžné praxe. Převedením všech zpracovaných návrhů do praxe dosáhne organizace souladu s požadavky GDPR a zároveň zvýšení své bezpečnosti.

Domnívám se, že vlastní návrh, který byl zpracován na míru konkrétní organizace je bez větších problémů aplikovatelný i pro jinou organizaci podobného typu. Může se tedy stát jakýmsi vodítkem či návodem pro manažery při zavádění systému řízení bezpečnosti informací v organizaci.

Závěrem tedy lze konstatovat, že hlavní cíl diplomové práce včetně všech dílčích cílů byl splněn.

SEZNAM POUŽITÉ LITERATURY

(1) NIST SPECIAL PUBLICATION 800-50. Building an Information Technology Security Awareness and Training Program: Computer Security. 1. Gaithersburg: National Institute of Standards and Technology, 2003.

(2) NIST SPECIAL PUBLICATION 800-16. Information Technology Security Training Requirements: a Role- and Performance-Based Model: Computer Security. 1. Gaithersburg: National Institute of Standards and Technology, 1998.

(3) NIST Special Publication 800-series General Information. NIST Special Publication 800-series General Information [online]. Gaithersburg: The National Institute of Standards and Technology, 2018 [cit. 2019-03-24]. Dostupné z: https://www.nist.gov/itl/nist-special-publication-800-series-general-information

(4) Pomůcka k auditu bezpečnostních opatření podle vyhlášky o kybernetické bezpečnosti č. 316/2014 Sb. In: PODPŮRNÉ MATERIÁLY [online]. Brno: Národní úřad pro kybernetickou bezpečnost, 2016 [cit. 2019-03-16]. Dostupné z: https://www.govcert.cz/download/kii-vis/container-nodeid580/vkbchecklistfinalv21rev.pdf

(5) 205 ZÁKON ze dne 7. června 2017, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění zákona č. 104/2017 Sb., a některé další zákony.
In: . Praha: Česká republika, 2017, ročník 2018, číslo 205. Dostupné také z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=z&id=62038

(6) Sbírka zákonů Česká republika. Břeclav: Moraviapress, 2018, 2018(82). ISSN 1211-1244.

(7) ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-807-2048-724.

(8) NEZMAR, Luděk. GDPR: praktický průvodce implementací. Praha: Grada Publishing, 2017. Právo pro praxi. ISBN 978-802-7106-684.

(9) ŽŮREK, Jiří. Praktický průvodce GDPR: včetně úplného znění GDPR. 2. aktualizované vydání. Olomouc: ANAG, 2018. Právo (ANAG). ISBN 978-807-5541-529.

(10) JORDÁN, Vilém a Viktor ONDRÁK. Infrastruktura komunikačních systémů I: univerzální kabelážní systémy. Druhé, rozšířené vydání. Brno: CERM, Akademické nakladatelství, 2015. ISBN 978-802-1451-155.

(11) RAIS, Karel a Radek DOSKOČIL. Risk management: studijní text pro kombinovanou formu studia. Brno: Akademické nakladatelství CERM, 2007. ISBN 978-802-1435-100.

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

(13) ČSN ISO/IEC 27002. Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací. 2. vydání. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

(14) KŘÍŽ, Jiří a Petr SEDLÁK. Audiovizuální a datové konvergence. Brno: CERM, 2012. ISBN 978-807-2047-840.

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

(16) SMEJKAL, Vladimír. Kybernetická kriminalita. 2. rozšířené a aktualizované vydání. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-807-3807-207.

(17) KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-808-8168-317.

(18) POŽÁR, Josef. Manažerská informatika. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 978-807-3802-769

(19) JORDÁN, Vilém a Viktor ONDRÁK. Infrastruktura komunikačních systémů II: kritické aplikace. Brno: CERM, Akademické nakladatelství, 2015. ISBN 978-802-1452-404.

(20) SMEJKAL, Vladimír a Karel RAIS. Řízení rizik ve firmách a jiných organizacích. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. Expert (Grada). ISBN 978-802-4746-449.

(21) NOVÁK, Luděk a Josef POŽÁR. Systém řízení informační bezpečnosti. In: Systém řízení informační bezpečnosti: Information security management systém [online]. [cit. 2019-05-05]. Dostupné z: https://www.cybersecurity.cz/data/srib.pdf

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

(23) Zákon č. 110/2019 Sb. Zákon č. 110/2019 Sb. [online]. Zlín: AION CS, c2010-2019 [cit. 2019-05-06]. Dostupné z: https://www.zakonyprolidi.cz/cs/2019-110/zneni-20190424#p67_p67-1-1

SEZNAM ZKRATEK

27k	Označení norem ISO/IEC 27000
BOZP	Bezpečnost a ochrana zdraví při práci
CIA	Confidentiality, integrity, availability
GDPR	General Data Protection Regulation
HR	Human Resources
HW	Hardware
ICT	Information and Communication Technologies
ISMS	Information Security Management System
ISO/IEC	International Organization for Standardization and the International Electrotechnical Commission
KII	Kritická informační infrastruktura
NGN	Next generation network
PDCA	Plan, do, check, act
PO	Požární ochrana
SAE	Security Awareness Education
SLA	Service Level Agreement
SP	Special Publication
SW	Software
VIS	Významné informační systémy
VLAN	Virtual local area network

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH