VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH ZAVEDENÍ BEZPEČNOSTNÍCH OPATŘENÍ V SOULADU S ISMS PRO OBCHODNÍ SPOLEČNOST

DESIGN OF SECURITY COUNTERMEASURES IMPLEMENTATION IN ACCORDANCE WITH ISMS FOR BUSINESS COMPANY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Petr Dočekal**
AUTHOR

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

BRNO 2018

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Petr Dočekal**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2017/18

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

Návrh zavedení bezpečnostních opatření v souladu s ISMS pro obchodní společnost

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 vytvořit návrh zavedení bezpečnostních opatření v souladu se systémem řízení bezpečnosti informací. Analýza současného stavu sítě, stavu bezpečnosti a analýzy rizik ve společnosti jsou základem pro dosažení zmíněného cíle. Je důležité zdůraznit, že se práce nezabývá návrhem zavedení systému řízení bezpečnosti informací v plném rozsahu, ale návrhem zavedení vybraných částí.
Práce je rozdělena do čtyř hlavních částí a každá část má svůj vlastní cíl. Cílem první části nazvané teoretická východiska je vysvětlit základní pojmy a definice probíraného tématu. Druhou částí je analýza současného stavu a jejím cílem je představit základní informace o společnosti a současný stav síťové infrastruktury a bezpečnosti. Praktickou částí je analýza rizik, návrh vybraných bezpečnostních opatření a ekonomické zhodnocení s časovým plánem. Poslední částí je závěr shrnující diplomovou práci.

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 2017/18

V Brně dne 28.2.2018

L. S.

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

Abstrakt

Diplomová práce se zaměřuje na oblast bezpečnostních opatření v souladu se systémem řízení bezpečnosti informací. Představuje základní teoretická východiska problematiky informační a kybernetické bezpečnosti a popisuje současný stav ve společnosti. Výstupem je návrh zavedení bezpečnostních opatření přispívajících ke zvýšení bezpečnosti informací ve společnosti.

Klíčová slova

informační bezpečnost, kybernetická bezpečnost, systém řízení bezpečnosti informací, ISO/IEC 27000, analýza rizik, opatření

Abstract

The master's thesis focuses on area of security countermeasures in accordance with information security management system. Presents basic theoretical background of information and cyber security and describes a current state in the company. The thesis's output is the design of security countermeasures implementation which contribute to information security in the company.

Key words

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

Bibliografická citace

DOČEKAL, P. *Návrh zavedení bezpečnostních opatření v souladu s ISMS pro obchodní společnost.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2018. 124 s. Vedoucí diplomové práce Ing. 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 11. května 2018 …….....

podpis

Poděkování

Rád bych poděkoval panu Ing. Petru Sedlákovi za vedení a odborné rady při psaní diplomové práci. Dále chci poděkovat společnosti a jejímu vedení za poskytnutí možnosti zpracování práce. V neposlední řadě bych rád poděkoval všem, kteří mě během mého studia podporovali.

OBSAH

ÚVOD **11**
CÍLE PRÁCE **12**
1 TEORETICKÁ VÝCHODISKA **13**
1.1 Definice pojmů 13
1.1.1 Základní pojmy a zkratky 13
1.1.2 Informační bezpečnost 16
1.1.3 Kybernetická bezpečnost 17
1.2 Systém řízení bezpečnosti informací 18
1.2.1 Ustanovení 19
1.2.2 Zavádění a provoz 21
1.2.3 Monitorování a přezkoumání 22
1.2.4 Údržba a zlepšování 22
1.3 Normy vztahující se k informační a kybernetické bezpečnosti 22
1.3.1 Normalizační instituce 23
1.3.2 ISO/IEC 27K 24
1.3.3 Normy NIST 27
1.4 Legislativa vztahující se k informační a kybernetické bezpečnosti 28
1.4.1 Legislativa České republiky 28
1.4.2 Legislativa Evropské unie 31
1.5 Analýza rizik 34
1.5.1 Kvalitativní analýza 34
1.5.2 Kvantitativní analýza 34
1.5.3 Fáze analýzy rizik 35
1.6 Opatření 36
1.6.1 Výběr opatření 37
2 ANALÝZA SOUČASNÉHO STAVU **39**
2.1 Informace o společnosti 39
2.2 Současný stav 39
2.2.1 Serverovna 39
2.2.2 Sídlo 40
2.2.3 Sklad Morava a Čechy 40
2.2.4 Kancelář 40
2.2.5 Pracovní stanice a notebooky 41

2.2.6 Mobilní zařízení 41
2.2.7 Přenos dat 41
2.2.8 Zálohování 42
2.3 Analýza vybraných oblastí 42
2.3.1 ISMS 43
2.3.2 Řízení aktiv 44
2.3.3 Řízení rizik 46
2.3.4 Organizační bezpečnost 48
2.3.5 Řízení dodavatelů 49
2.3.6 Bezpečnost lidských zdrojů 50
2.3.7 Řízení provozu a komunikací 52
2.3.8 Řízení přístupu a bezpečné chování uživatelů 55
2.3.9 Ověřování identity uživatelů 57
2.3.10 Řízení přístupových oprávnění 58
2.3.11 Aplikační bezpečnost 58
2.3.12 Kryptografie 59
2.3.13 Zajištění dostupnosti 60
2.3.14 Fyzická bezpečnost 61
2.3.15 Ochrana integrity komunikačních sítí 62
2.3.16 Ochrana před škodlivým kódem 63
2.3.17 Detekce kybernetických bezpečnostních událostí 64
2.3.18 Řízení kontinuity činností 64
2.3.19 Shrnutí plnění 65
2.4 Souhrn analýzy oblastí k opatřením ISMS 66
2.5 Požadavky společnosti 70
2.6 Důvod zájmu společnosti o bezpečnost 70
3 NÁVRH ŘEŠENÍ 71
3.1 Rozsah a hranice 71
3.2 Analýza rizik 71
3.2.1 Identifikace a hodnocení aktiv 72
3.2.2 Identifikace hrozeb a zranitelnosti 74
3.2.3 Matice zranitelnosti 77
3.2.4 Matice úrovní rizik 79
3.2.5 Zhodnocení 81
3.2.6 Výběr bezpečnostních opatření 83

3.3 Návrh zavedení bezpečnostních opatření ... 84
3.3.1 Politiky bezpečnosti informací – A.5 ... 85
3.3.2 Organizace bezpečnosti informací – A.6 ... 87
3.3.3 Řízení aktiv – A.8 ... 90
3.3.4 Řízení přístupu – A.9 ... 92
3.3.5 Kryptografie – A.10 ... 93
3.3.6 Fyzická bezpečnost a bezpečnost prostředí – A.11 ... 96
3.3.7 Bezpečnost provozu – A.12 ... 99
3.3.8 Bezpečnost komunikací – A.13 ... 103
3.3.9 Aspekty BCM organizace z hlediska bezpečnosti informací – A.17 ... 105
3.3.10 Souhrn vzhledem k rizikům a požadavkům ... 105
3.4 Souhrn vzhledem k GDPR ... 106
3.4.1 Zabezpečení ... 107
3.4.2 Ohlašovací a oznamovací povinnost ... 107
3.4.3 Ochrana „by design“ ... 108
3.5 Fáze implementace ... 108
3.5.1 Plán implementace navržených opatření ... 109
3.6 Ekonomické zhodnocení ... 112
3.7 Přínos práce ... 114
4 ZÁVĚR ... 115
SEZNAM POUŽITÝCH ZDROJŮ ... 116
SEZNAM ZKRATEK ... 120
SEZNAM OBRÁZKŮ ... 122
SEZNAM TABULEK ... 123
SEZNAM PŘÍLOH ... 124

ÚVOD

Dnešní technologická éra nám neustále přináší nové možnosti jak v osobním, tak i profesním životě. S těmito možnostmi však přichází i způsoby, jak je zneužít, a to nejen pouze vůči jejich uživateli či uživatelům. Příkladem mohou být automobily a jejich rostoucí elektronizace, která je vystavuje stále větším hrozbám. Zkušený člověk je schopný u moderního automobilu narušit bezpečnost v řádu několika minut a ovládnout jej. Díky tomu je pak během jízdy schopný bez vědomí řidiče například spustit elektronickou ruční brzdu. Takový počin může vést k velké nehodě a automobilové společnosti si to určitě uvědomují. Koncern Volkswagen před dvěma lety založil společnost za účelem vyvíjení bezpečnostních systémů zaměřující se na kybernetické hrozby. Automobilový průmysl však není jediný s podobným problémem.

Z pohledu zabezpečení nemohou technologie řešit vše a nelze se spoléhat pouze na ně. Důvodem je lidský faktor, který je velmi obtížně předvídatelný. Jako příklad lze uvést nepříliš známou aféru „Stuxnet“. Jednalo se o infikování Íránské jaderné elektrárny Natanz malwarem. Síť elektrárny byla zabezpečena a kompletně oddělená od internetu, a přesto žádná technologie ani kompletní oddělení sítě nezabránily infikování systému. Je tedy důležité zavést bezpečnostní opatření nejen na technologické úrovni, ale také zabezpečit lidský faktor a budovat bezpečnostní povědomí.

25. května tohoto roku vyjde v platnost evropské nařízení GDPR (General Data Protection Regulation - Obecné nařízení o ochraně osobních údajů) s cílem zvýšení ochrany osobních dat občanů. Nařízení bude platit celosvětově pro všechny společnosti zpracovávající údaje Evropanů. Za porušení nařízení může společnostem hrozit pokuta ve výši až 20 miliónů eur nebo pokuta do výše 4% z celkového celosvětového obratu. Nejedná se o žádné zanedbatelné sumy, pro většinu společností by to bylo likvidační a informační bezpečnost by se tedy neměla podcenit.

CÍLE PRÁCE

Hlavním cílem práce je vytvořit návrh zavedení bezpečnostních opatření v souladu se systémem řízení bezpečnosti informací. Analýza současného stavu sítě, stavu bezpečnosti a analýzy rizik ve společnosti jsou základem pro dosažení zmíněného cíle. Je důležité zdůraznit, že se práce nezabývá návrhem zavedení systému řízení bezpečnosti informací v plném rozsahu, ale návrhem zavedení vybraných částí.

Práce je rozdělena do čtyř hlavních částí a každá část má svůj vlastní cíl. Cílem první části nazvané teoretická východiska je vysvětlit základní pojmy a definice probíraného tématu. Druhou částí je analýza současného stavu a jejím cílem je představit základní informace o společnosti a současný stav síťové infrastruktury a bezpečnosti. Praktickou částí je analýza rizik, návrh vybraných bezpečnostních opatření a ekonomické zhodnocení s časovým plánem. Poslední částí je závěr shrnující diplomovou práci.

1 TEORETICKÁ VÝCHODISKA

První kapitola je zaměřena na pochopení základní teorie tématu této práce.

1.1 Definice pojmů

Cílem podkapitoly je vysvětlit základní pojmy důležité pro pochopení tématu nebo pojmy využité v diplomové práci.

1.1.1 Základní pojmy a zkratky

IT – Informační technologie (Information Technology)

ICT – Informační a komunikační technologie (Information and Communication Technology)

IS – Informační systém (Information system)

ISMS – Systém řízení bezpečnosti informací (Information Security Management Systém) [1]

S výše zmíněnými pojmy neoddělitelně souvisí následující pojmy.

Informace – jedná se o poměrně širší pojem charakterizující skutečné prostředí, probíhající procesy a stav ve formě dat [1]. Pro účely této práce je na informace nahlíženo jako na aktiva společnosti důležitá k podnikání, a proto musí být důkladně chráněny. Dále jsou uvažovány tři druhy forem informací: materiální (např. na papíře), digitální (např. elektronický dokument uložený na disku) a informace ve formě znalostí zaměstnanců [2].

Data – lze je považovat jako plnění informace, kterou vytváří [1]. Jinými slovy lze říct, že informace jsou data, kterým byl dán význam. Data lze získat výpočtem, pozorováním, měřením a dalšími způsoby [3].

Aktivum – je vše, co má pro vlastníka určitou hodnotu. Aktiva mohou být hmotná a nehmotná [4].

Informační systém – je definován jako systém procesů, služeb, aplikací, aktiv informačních technologií a dalšími komponenty pracující s informacemi [2].

Síťová infrastruktura – pojem, do kterého spadají síťové prvky a komponenty použité při realizaci ICT prostředí [1].

Kybernetický prostor – globální doména informačního prostředí zahrnující vzájemně závislé sítě infrastruktur informačních systémů jako je internet, počítačové systémy, telekomunikační sítě, ovladače a vestavěné procesy [5].

Útok – pokus o získání neoprávněného přístupu k aktivu nebo pokus o využití, krádež, vyzrazení, zničení či změnu aktiva [2].

Kybernetický útok – útok v rámci kybernetického prostoru za účelem vyřadit, narušit, zničit nebo úmyslně ovládat informační infrastrukturu/prostředí, nebo rozbít integritu dat, anebo ukrást vlastněné informace. Kybernetický útok je cílen na prostor využívaný společnosti v kybernetickém prostoru [5].

Hrozba – potencionální nechtěná událost ohrožující bezpečnost [1].

Opatření – aktivita, proces či procedura snižující efekt hrozby [1].

Zranitelnost – slabé místo aktiva nebo opatření, které může být využito hrozbou [2].

Riziko – obecně je riziko efekt nejistoty na dosažení cílů. Konkrétně se jedná o kombinaci zranitelnosti a hrozby s dopadem na aktivum či aktiva [1].

Dopad – škoda způsobená hrozbou na určité aktivum [1].

Bezpečnostní událost – zjištěný výskyt stavu služby sítě nebo systému indikující možné narušení politiky bezpečnosti informací, selhání opatření nebo dříve neznámá situace závažná pro bezpečnost [2].

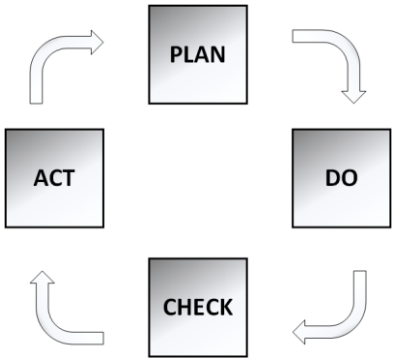
Bezpečnostní incident – jedna nebo série nečekaných nebo nechtěných bezpečnostních událostí, která s velkou pravděpodobností ohrožuje podnikatelské činnosti a informační bezpečnost [2].

Řízení přístupu – úkolem je zajistit omezený a autorizovaný přístup k aktivům na základě bezpečnostních a podnikových požadavků [2].

Audit – je dokumentovaný, systematický a nezávislý proces k zajištění důkazů a jejich objektivní zhodnocení za účelem zjištění, zdali jsou splněna požadovaná kritéria [2]. Existují tři typy auditu – interní, externí a certifikační [1].

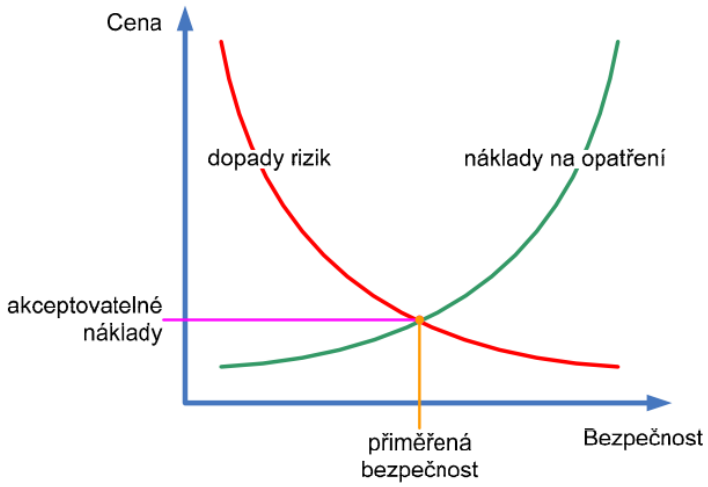
PDCA cyklus – nebo také Demingův cyklus je metoda postupného zlepšování, například v oblasti kvality služeb, procesů, výrobků atd. Zlepšení je docíleno skrze opakované provádění čtyř základních fází: Plan (plánuj), Do (dělej), Check (kontroluj) a Act (jednej) [1].

- **plánuj** – naplánování zamýšleného zlepšení
- **dělej** – provedení plánu
- **kontroluj** – zkontroluj výsledek realizace plánu vzhledem k původnímu plánu
- **jednej** – změna plánu a provedení vzhledem ke třetí kontrolní fázi [1]



Obrázek 1: PDCA cyklus
Zdroj: Vlastní zpracování

Přiměřená bezpečnost – představuje stav, při kterém investice a úsilí do bezpečnosti IS jsou rovny hodnotě aktiva a míře možných rizik. Obrázek 2 zobrazuje zmíněný princip přiměřené bezpečnosti [1].



Obrázek 2: Přiměřená bezpečnost
Zdroj: [1, s. 36]

1.1.2 Informační bezpečnost

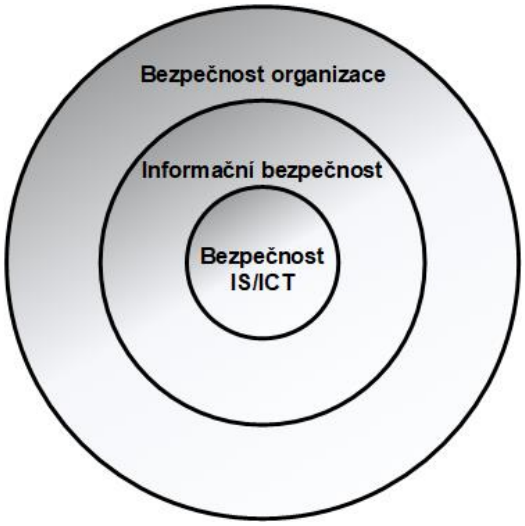
Informační bezpečnost (IB) nebo také bezpečnost informací (BI) má za úkol chránit informace před zničením, poškozením, krádeží či ztrátou [6]. Nejvíce využívanou definicí informační bezpečnosti je ochrana důvěrnosti, integrity a dostupnosti informací. Nicméně, může obsahovat i další kritéria jako odpovědnost, autenticitu, spolehlivost a nepopiratelnost [4]. Informační bezpečnost lze dosáhnout zavedením vhodné sady bezpečnostních opatření, vybraných procesem řízení rizik a spravovaných pomocí systému řízení bezpečnosti informací [2].

Dále je důležité zmínit pojmy ***bezpečnost organizace*** a ***bezpečnost IS/ICT***, se kterými je informační bezpečnost ve vzájemném vztahu [1].

Bezpečnost organizace – úkolem je zabezpečit objekt a majetek organizace [4].

Bezpečnost IS/ICT – zabezpečuje pouze aktiva informačních systémů podporovaných informačními a komunikačními technologiemi [4].

Obrázek 3 zobrazuje vztah mezi zmíněnými pojmy.



Obrázek 3: Vztah bezpečnostních úrovní
Zdroj: Vlastní zpracování dle [4, s. 56]

Definice informační bezpečnosti obsahuje tři kritéria – důvěrnost, integrita a dostupnost – známé také jako **triáda CIA** (Confidentiality, Integrity and Availability). Tyto kritéria jsou základem a zároveň cílem informační bezpečnosti [6].

Důvěrnost – znamená poskytování informací pouze autorizovaným uživatelům, procesům a entitám [4].

Integrita – stav informací zajišťující jejich úplnost a správnost [4].

Dostupnost – kritérium zajišťující dostupnost informací v rámci důvěrnosti v okamžiku požadavku [1].

Bezpečnostní mechanizmus – technika použitá k zavedení bezpečnostní funkce [4].

Bezpečnostní funkce – funkce systému nebo produktu přispívající k jeho bezpečnosti [4].

1.1.3 Kybernetická bezpečnost

Schopnost chránit nebo bránit používaný prostor v kybernetickém prostoru před kybernetickým útokem [5]. Kybernetickou bezpečnost lze definovat také jako soubor technických, vzdělávacích, organizačních a právních prostředků obstarávající ochranu kybernetického prostoru [7].

Ačkoli jsou pojmy kybernetická bezpečnost (KB) a informační bezpečnost (IB) často považovány za stejné pojmy, není tomu tak. Oba typy bezpečnosti se samozřejmě v určitém bodě překrývají, rozdílem je však v jejich perimetru. Informační bezpečnost se týká organizace na úrovni fyzické, organizační, personální a komunikační bezpečnosti, kdežto kybernetická bezpečnost se týká kybernetického prostoru [8]. Existují určité hrozby, které zahrnují pouze informační bezpečnost, ale už ne bezpečnost kybernetickou, jako například krádež papírového dokumentu ze stolu zaměstnance.

Ústředním orgánem pro kybernetickou bezpečnost je v České republice **Národní úřad pro kybernetickou a informační bezpečnost** (NÚKIB) [9]. Už i název tohoto úřadu napovídá, že kybernetická a informační bezpečnost nejsou synonyma.

Kybernetická bezpečnost je v České republice z pohledu kritické infrastruktury řešena zákony a vyhláškami. Zákon i vyhláška vyšly poprvé v roce 2014 jako *zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů* a *vyhláška č. 316 Sb. o kybernetické bezpečnosti,* s účinností od roku 2015. V roce 2017 vešly v platnost dva

zákony, které zákon č. 181 novelizují - *zákon č. 104/2017 Sb*. a *zákon č. 205/2017 Sb*. [9]. Zákony jsou blíže popsány v kapitole o legislativě České republiky.

Kritická infrastruktura (KI) – jsou výrobní a nevýrobní systémy a služby, u kterých by narušení nebo ztráta funkce měly závažný dopad na bezpečnost státu, města, jednotlivce, ekonomiku a další [1].

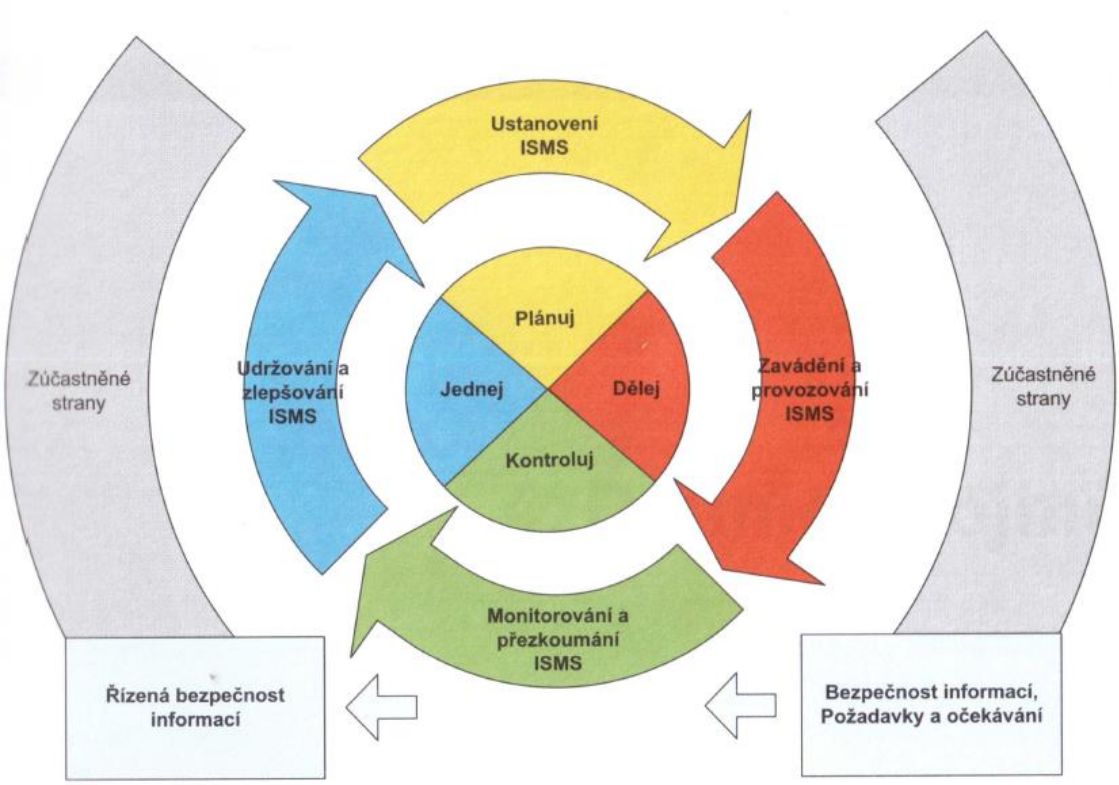
Kritická informační infrastruktura (KII) – prvek nebo systém prvků KI s důrazem na ICT v kybernetické bezpečnosti [9].

1.2 Systém řízení bezpečnosti informací

Systém zkráceně označovaný **ISMS** (z anglického názvu „*Information Security Management System*“) tvoří část celkového systému řízení organizace. Cílem systému je zajistit ochranu aktiv prostřednictvím směrnic, politik, postupů, činností a příslušných zdrojů. ISMS představuje systematický přístup na úrovni ustanovení, implementování, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací. Systém je založen na zhodnocování rizik a přijímání rizik organizace na úrovni, která je navržena na efektivní jednání a správu s riziky. K úspěšnému zavedení ISMS přispívá analýza požadavků na ochranu aktiv a použití adekvátních opatření na jejich ochranu, dle požadavků. Úspěšnému zavedení ISMS také přispívají základní principy jako povědomí o potřebě informační bezpečnosti, aktivní prevence a detekce incidentů, posouzení rizika na základě kterého stanovena příslušná opatření, aby bylo dosaženo přijatelných úrovní rizika a další [2].

Systém funguje na již zmíněném PDCA cyklu a je definován těmito etapami:

- ustanovení ISMS,
- zavádění a provoz ISMS,
- monitorování a přezkoumání ISMS,
- údržba a zlepšování ISMS [1].



Obrázek 4: PDCA cyklus v ISMS
Zdroj: [1, s. 25]

1.2.1 Ustanovení

Při etapě ustanovení se definují správné formy řešení bezpečnosti. Etapa by měla být ukončena souhlasem vedení se zavedením ISMS na základě potřeb organizace, zjištěných při analýze a zvládání rizik ISMS. Činnosti etapy ustanovení lze rozdělit dle následujícího:

- definice rozsahu a hranic ISMS,
- definice a odsouhlasení Prohlášení o politice ISMS,
- analýza rizik a zvládání rizik,
- souhlas vedení organizace s navrhovanými zbytkovými riziky a se zavedením ISMS,
- příprava Prohlášení o aplikovatelnosti [4].

Definice rozsahu a hranic ISMS

Název již napovídá, že se jedná o definování rozsahu a hranic, ve kterých je ISMS uplatňováno. Není pravidlem, že rozsah a hranice musí pokrývat celou organizaci [4]. K definování rozsahu lze využít dva základní způsoby:

- Prvním způsobem je definování rozsahu celé organizace. Tento způsob má své výhody i nevýhody. Výhodou je, že řízení od počátku řeší bezpečnost informací v celé organizaci. Z toho zároveň vyplývá i nevýhoda nemalé investice ve formě spotřeby zdrojů a financí. Další věcí je, že ne vždy dojde k realizaci veškerých plánovaných a očekávaných přínosů řízení bezpečnosti.
- Druhý způsob obnáší omezení rozsahu ISMS již v počátku a zaměření se pouze na zvolenou část organizace jako např. vybranou pobočku, informační systém či organizační celek. Také je vhodné vybrat tu část, která je otevřena a ochotna přistoupit ke smysluplným změnám a zlepšením [4].

Prohlášení o politice ISMS

Jedná se o definování politiky ISMS na základě specifických potřeb organizace. Ačkoli se jedná o rozsahově krátký dokument, významem je velmi důležitý. Politika by měla definovat cíle ISMS, základní směr a rámec pro řízení bezpečnosti informací. Dále by měla zohlednit cíle a požadavky organizace, a také související smluvní požadavky na úrovni regulací a zákonů. Závěrem by měla vytvořit vazby potřebné k vybudování a údržbě ISMS, stanovit kritéria popisu a hodnocení rizik. Po dokončení by měla být schválena vedením [4].

Analýza rizik a zvládání rizik

Analýza a zvládání rizik patří do celku zvaného řízení rizik. Jde o koordinované činnosti, které slouží ke kontrole a řízení organizace s ohledem na rizika. Analýzu rizik lze definovat jako systematickou činnost k odhadu míry rizika určení jeho zdrojů. Zvládáním rizik se rozumí výběr a přijmutí opatření za účelem změny rizika [4].

Tématika analýzy rizik bude více rozebrána v dalších kapitolách.

Souhlas vedení se zavedením a s navrhovanými zbytkovými riziky

V této činnosti je zapotřebí, aby vedení odsouhlasilo návrh bezpečnostních opatření. Navrhovaná opatření jsou nutná ke snížení bezpečnostních rizik. Zároveň by také mělo vedení usnést rozhodnutí o přijatelnosti či nepřijatelnosti existujících zbytkových rizik [4].

Prohlášení o aplikovatelnosti

Jedná se o dokumentované prohlášení udávající cíle opatření a jednotlivá bezpečnostní opatření, která jsou významná a použitelná na ISMS organizace. V případě, že organizace usiluje o shodu svého ISMS s normou ISO/IEC 27001, jedná se o povinný dokument [4]. Dokument musí obsahovat:

- nové cíle opatření, jednotlivá bezpečnostní opatření a důvody jejich výběru,
- stávající cíle opatření, jednotlivá bezpečnostní opatření, která jsou už v organizaci zavedena,
- vyřazené cíle opatření, jednotlivá vyřazená bezpečnostní opatření uvedená v příloze A a odůvodnění pro jejich vyřazení [1].

1.2.2 Zavádění a provoz

V této etapě je snaha prosadit všechna bezpečnostní opatření, tak jak byla navržena v etapě ustanovení. Je zapotřebí, aby byly připraveny jednotlivé plány, upřesňující termíny, odpovědné osoby apod. [4].

Nutné činnosti k provedení:

- sepsat dokument „Plán zvládání rizik a začít se zaváděním“,
- zavést navržená bezpečnostní opatření a sepsat příručku bezpečnosti informací upřesňující pravidla a postupy aplikovaných opatření,
- formulovat program budování bezpečnostního povědomí a přípravu a zaškolení všech z úseku informatiky, a především z řízení bezpečnosti,
- upřesnit způsoby měření účinnosti bezpečnostních opatření a sledovat stanovené ukazatele [4],

- zavést postupy a další opatření pro rychlou detekci a reakci na bezpečnostní incidenty,
- řídit záznamy, zdroje a dokumenty ISMS [4].

1.2.3 Monitorování a přezkoumání

Etapa zahrnuje pravidelná přezkoumávání účinnosti zavedených opatření na základě výsledků auditů, návrhů incidentů, výsledků měření účinnosti opatření všech zainteresovaných stran. Přezkoumávání slouží k definování přiměřenosti, vhodnosti a efektivnosti přezkoumávaného předmětu [1].

Následující činnosti je nutné provést:

- monitorovat a ověřit účinnost prosazení bezpečnostních opatření,
- realizovat interní audity ISMS (náplň pokrývající plný rozsah ISMS),
- vypracovat zprávu o stavu ISMS a podle této zprávy přehodnotit ISMS na úrovni vedení organizace [4].

1.2.4 Údržba a zlepšování

Jedná se o poslední etapu cyklu. Udržování a zlepšování se provádí sběrem podnětů ke zlepšení ISMS a nápravě neshod objevujících se v ISMS. Neshodou je myšleno nesplnění požadavku [4].

Nezbytné činnosti etapy:

- zavést identifikované možnosti zlepšení,
- realizovat odpovídající opatření k nápravě nedostatků a preventivní opatření k jejich odstranění [4].

1.3 Normy vztahující se k informační a kybernetické bezpečnosti

Podkapitola norem představí normalizační instituce, které publikují normy zmíněné v této práci. Dále jsou představeny normy řady 27K a pár zajímavých norem instituce NIST. Nejprve je však důležité vysvětlit rozdíl mezi normou a standardem, neboť se nejedná o dvě slova stejného významu.

Norma – jedná se o doporučení pro dané řešení či standard [1].

Standard – je úmluva v podobě dokumentu, která obsahuje přesně stanovená kritéria nebo technické specifikace používané jako pravidla, směrnice [1].

1.3.1 Normalizační instituce

Normalizační instituce vztahující se k použitým normám v této diplomové práci

ISO – International Organization for Standardization

Je nezávislou a nadnárodní organizací podporující rozvoj standardizační činností. Působí celosvětově se zaměřením na spolupráci na úrovni technologických, ekonomický, vědeckých a intelektuálních aktivit a také na usnadnění mezinárodních směn služeb a zboží [1].

IEC – International Electrotechnical Comission

Organizace s celosvětovou působností, která světu připravuje a publikuje normy pro všechny elektronické, elektrotechnické a na ně vztahující se technologie. Společně s ISO a ITU jsou tři největší globální instituce [1].

ITU - International Telecommunications Union

Celosvětová normalizační instituce, která podpořila růst mnoha technologií, jako mobilní technologie a Internet. Představuje vedoucí roli ve správě spekter rádiové frekvence. Společně s ISO a IEC tvoří trojici největších globálních institucí [1].

NIST – National Institute for Standards and Technology

Americká normalizační organizace s posláním v oblasti vývoje a podpory standardů, technologií a měřících technik za účelem zlepšení života a zvýšení produktivity a usnadnění obchodu [1].

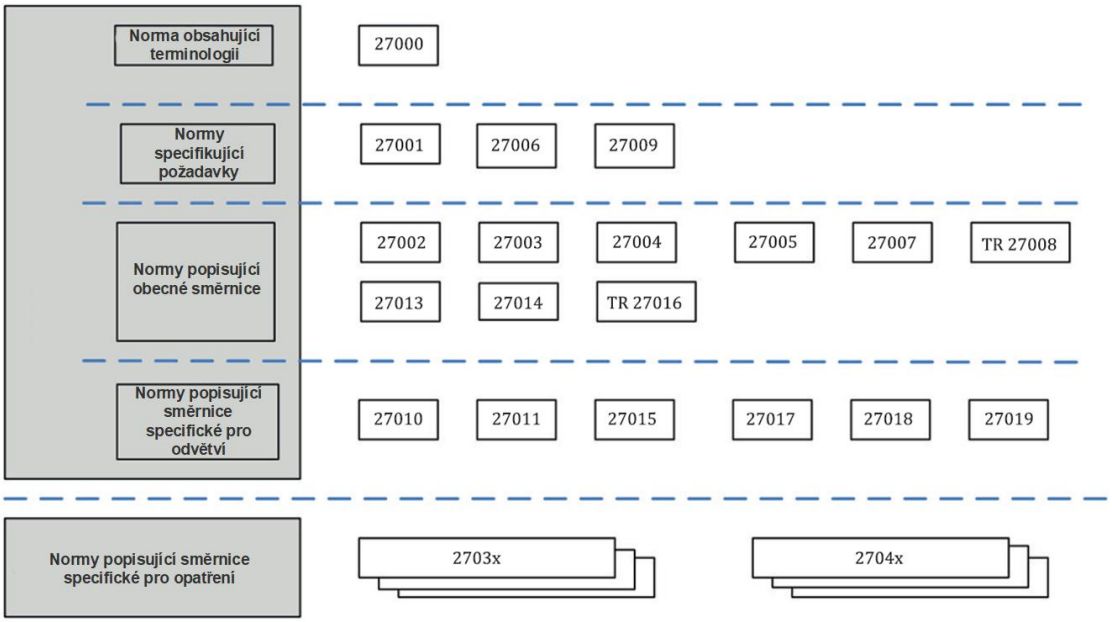
ČAS – Česká agentura pro standardizaci

Byla zřízena jako státní příspěvková organizace Úřadem pro technologickou normalizaci, metrologii a státní zkušebnictví (**ÚNMZ**) a od 1. ledna 2018 je zodpovědná za všechny činnosti v rámci tvorby, vydávání a distribuce technických norem [10].

ČSN je zkratka znamenající „Česká technická norma“, dříve „Česká státní norma“. Její vznik je možný přejímáním evropských a mezinárodní norem nebo tvorbou původních norem vyplývajících z národních potřeb [1].

1.3.2 ISO/IEC 27K

Řada norem ISO/IEC 27000 (nebo také nazývána jako „*řada norem ISMS*“) jsou mezinárodní normy určeny pro systémy řízení, konkrétně pro jejich tvorbu a provozování. Za pomocí této řady norem jsou organizace všech typů a velikostí schopny zavést a provozovat ISMS. Řada zahrnuje čtyři typy norem. Prvním typem jsou normy stanovující požadavky na ISMS a na pracovníky provádějící certifikací těchto systémů. Dalším typem jsou ty normy, které poskytují podrobný návod, přímou podporu a/nebo výklad pro celkový proces ISMS. Třetí typ se zaměřuje na směrnice ISMS pro specifické obory. Poslední typ se zabývá posuzováním shody požadavků ISMS [2].



Obrázek 5: Vztahy norem řady ISO/IEC 27K
Zdroj: Upraveno dle [2, s. 21]

a) Normy obsahující terminologii

ISO/IEC 27000 | *Systémy řízení bezpečnosti informací – Přehled a slovník*

Norma poskytuje slovník použitých termínů a definic v řadě norem ISMS, úvod k systémům řízení bezpečnosti informací a přehled norem. Účelem je popis základů ISMS, které tvoří předmět řady norem ISMS a definuje související termíny [2]. Tato norma prošla v únoru 2018 revizí a oproti původní verzi došlo k následujícím změnám:

- přepsání úvodu,
- odebrání některých pojmů a definic,
- zarovnání úrovně struktury kapitoly „*Termíny a definice*“ pro **MSS*** ,
- aktualizace kapitoly „*Řada norem ISMS*“ na základě změn v dotčených normách,
- odebrání příloh A a B [2].

***MSS** (Management System Standards) – Je systémem řízení norem instituce ISO. Došlo tedy k harmonizaci se systémem řízení norem ISO. Co se zmíněné změny týče, byla přidána kapitola normativních odkazů a kapitola termínů a definic byla posunuta.

b) Normy specifikující požadavky

ISO/IEC 27001 | *Systémy řízení bezpečnosti informací – Požadavky*

Norma specifikuje požadavky na cyklus formalizovaných ISMS v kontextu celkových rizik činností organizace. Cyklem je myšleno ustanovení, zavádění a provoz, monitorování a přezkoumání, a nakonec udržování a zlepšování. Definuje požadavky na bezpečnostní opatření upravených na základě potřeb organizací či jejích částí [2].

ISO/IEC 27006 | *Požadavky na orgány poskytující audit a certifikaci systémů řízení bezpečnosti informací*

Slouží především k podpoře certifikačních orgánů a předmětem normy je specifikace požadavků a poskytnutí návodu pro orgány poskytující audit a certifikaci ISMS na základě ISO/IEC 27001 [2].

ISO/IEC 27009 | *Používání ISO/IEC 27001 pro specifická odvětví - Požadavky*

Definuje požadavky k použití ISO/IEC 27001 pro specifická odvětví (obor, oblast aplikace nebo trh). Účelem je zajistit nekonfliktnost dodatečných nebo upravených

požadavků s požadavky v příloze A normy ISO/IEC 27001 [2]. Norma momentálně prochází revizí.

c) Normy popisující obecné směrnice

ISO/IEC 27002 | *Soubor postupů pro opatření bezpečnosti informací*

Norma poskytuje seznam obecně uznaných cílů opatření a opatření osvědčených postupů, které by měly být použity jako návod k zavedení při výběru a zavedení opatření s cílem dosažení informační bezpečnosti [2].

ISO/IEC 27003 | *Směrnice pro implementaci systému řízení bezpečnosti informací*

Dokument poskytuje vysvětlení a návod k normě ISO/IEC 27001 [2].

ISO/IEC 27004 | *Řízení bezpečnosti informací – Měření*

Účelem normy je poskytnutí rámce pro měření, umožňující posoudit měřenou efektivnost ISMS podle ISO/IEC 27001 [2].

ISO/IEC 27005 | *Řízení rizik bezpečnosti informací*

Poskytuje směrnice pro řízení rizik bezpečnosti informací a pomáhá uspokojivě zavést a splnit požadavky uvedené v ISO/IEC 27001 [2]. Norma momentálně prochází revizí.

ISO/IEC 27007 | *Směrnice pro audit systémů řízení bezpečnosti informací*

Norma poskytuje směrnici k provádění auditů ISMS nebo řízení programu auditu ISMS na základě požadavků ISO/IEC 27001 [2].

ISO/IEC TR 27008 | *Směrnice pro audit opatření ISMS*

Technická zpráva se zaměřuje na směrnici k přezkoumání, zavedení a provozování opatření včetně kontroly technické shody opatření IS dle norem ustanovených danou organizací. TR – Technical Report [2]. Norma momentálně prochází revizí.

ISO/IEC 27013 | *Návod pro integrovanou implementaci ISO/IEC 27001 a ISO/IEC 20000-1*

Norma je zaměřena výhradně na integrovanou implementaci ISMS specifikovaného ISO/IEC 27001 a SMS specifikovaného ISO/IEC 20000-1 [2].

ISO/IEC 27014 | *Správa bezpečnosti informací*

Poskytuje návod s principy a postupy ke správě bezpečnosti informací [2].

ISO/IEC TR 27016 | *Řízení bezpečnosti informací – Organizační ekonomika*

Technická zpráva doplňující řadu norem ISMS metodami, které pokrývají ekonomická hlediska při ochraně organizačních aktiv. Dále poskytuje návod při aplikaci organizační ekonomiky bezpečnosti informací za pomocí příkladů a modelů [2].

d) Normy popisující směrnice specifické pro odvětví

Tyto normy jsou svým obsahem mimo působnost této práce, a proto jsou zmíněny pouze jejich označením a českým názvem.

ISO/IEC 27010 | *Směrnice pro řízení bezpečnosti informací pro meziodvětvové komunikace a komunikace mezi organizacemi*

ISO/IEC 27011 | *Směrnice pro řízení bezpečnosti informací pro telekomunikační organizace na základě ISO/IEC 27002*

ISO/IEC TR 27015 | *Směrnice pro řízení bezpečnosti informací pro finanční služby*

ISO/IEC 27799 | *Řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002*

Pozn. Normy ISO/IEC 27K jsou původně v anglickém znění a do ČSN nejsou všechny přejaty. Z tohoto důvodu jsou výše uvedené normy s originálním označením a českým překladem názvu.

1.3.3 Normy NIST

NIST publikuje dokumenty mnoha témat, od kybernetické bezpečnosti, přes chemii až ke konstrukci budov. Právě v kybernetické a informační bezpečnosti lze najít mnoho užitečných norem:

NISTIR 7298 Glossary of Key Information Security Terms (*Slovník klíčových pojmů informační bezpečnosti)*

Jedná se o dokument poskytující souhrnný přehled důležitých pojmů informační bezpečnosti použitých právě v ostatních publikacích NIST či jiných zdrojích [5].

NIST SP 800-12 An Introduction to Information Security *(Úvod do informační bezpečnosti)*

Publikace poskytuje velký přehled principů informační bezpečnosti představením příbuzných konceptů a řad bezpečnostních opatření, které mohou organizace využít za účelem efektivního zabezpečení jejich systémů a informací. Jedná se o prověřené opatření a koncepty federálních informačních systémů a organizací [11].

NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations *(Bezpečnostní opatření pro federální informační systémy a organizace)*

Obsahuje katalog bezpečnostních opatření a proces výběru bezpečnostních opatření k ochraně provozu, aktiv, jednotlivců organizace a také ostatních organizací a státu před velkou škálou hrozeb, jako kybernetický útok, přírodní pohromy, lidské chyby apod.. Opatření jsou upravitelná a jejich zavedení je částí organizačního procesu zvládání informační bezpečnosti a rizik [12].

1.4 Legislativa vztahující se k informační a kybernetické bezpečnosti

Tato kapitola je zaměřena na seznámení s legislativou, která je spojená s informační a kybernetickou bezpečností. Není-li napsáno jinak, je zmíněná legislativa platná k 20. květnu 2018.

1.4.1 Legislativa České republiky

Zákon č. 181/2014 Sb., *o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*

Zákon o kybernetické bezpečnosti vešel v účinnost 1. ledna 2015. Od té doby byl novelizován třemi zákony, a to v roce 2017. Zákony novelizující zákon č.181/2014 Sb.:

- zákon č. 104/2017 Sb.,
- zákon č. 183/2017 Sb.,
- zákon č. 205/2017 Sb. [9].

Zákon upravuje práva a působnost orgánů veřejné moci a povinnosti a práva osob v oblasti kybernetické bezpečnosti a nevztahuje se na informační nebo komunikační

systémy nakládající s utajovanými informacemi [13]. Zákon zapracovává, na základě novely **č. 205/2017**, *evropskou směrnici NIS* a upravuje zajišťování bezpečnosti sítí elektronických komunikací a infomačních systémů. Tato novela přináší poměrně mnoho změn jako úpravu pokut a přestupků, rozšíření pravomocí národního a vládního CERT a další. Nejvýraznější změnou je však zavedení nových subjektů – *Provozovatel základních služeb* a *Poskytovatel digitálních služeb* [14]. Řeší ochranu kybernetického prostoru z pohledu kritické infrastruktury a ta je určována na základě *nařízení vlády č. 432/2010 Sb.* a jeho novelizací, *nařízením vlády č. 315/2014 Sb.* [9].

Základní služba – služba splňující tři kritéria. První kritériem je závislost poskytované služby na sítích elektronických komunikací nebo informačních systémech. Dále zabezpečuje ekonomické nebo společenské činnosti v odvětví energetiky, dopravy, bankovnictví, infrastruktury finančních trhů, zdravotnictví, vodního hospodářství, digitální infrastruktury a chemického průmyslu. Posledním kritériem narušení sítí elektronických komunikací nebo informačních systémů, které by mohlo mít významný dopad na zabezpečení činností v odvětvích zmíněných v druhém kritériu [14] [15].

Provozovatel základních služeb (PZS) – subjekt poskytující základní službu, který je určen Úřadem pro kybernetickou a informační bezpečnost. Na základě směrnice NIS se považují jako PZS také orgány a osoby spravující či provozující komunikační nebo informační systémy KII. K určení PZS slouží *vyhláška č. 437/2017 Sb.* [14] [15].

Digitální služba – jakákoli elektronicky poskytovaná služba na individuální elektronickou žádost uživatele. Jedná se provoz on-line tržiště, cloud computingu nebo internetového vyhledávače [15].

On-line tržiště – model používání internetových služeb umožňujících poskytovateli nebo spotřebiteli on-line uzavírat kupní smlouvu nebo smlouvu o poskytování služeb a to prostřednictvím internetové stránky prodávajícího, který využívá službu tržiště nebo internetovou stránkou on-line tržiště [14].

Cloud computing – model používání internetových služeb umožňujících přístup k přizpůsobitelnému a rozšiřitelnému výpočetnímu zdroji nebo uložišti, které je možné sdílet [14].

Poskytovatel digitální služby (PDS) – subjekt poskytující digitální službu. Zákon se však vztahuje pouze na ty poskytovatele, kteří mají více jak 50 zaměstnanců nebo roční obrat, popř. bilanci vyšší 10 miliónů eur včetně [15].

Vyhláška č. 316/2014 Sb., *o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)*

Vyhláška stanovuje strukturu a obsah dokumentace pro:

- informační systém KII,
- komunikační systém KII,
- významný informační systém [16].

Dále stanovuje obsah pro:

- bezpečnostní opatření a rozsah jejich zavedení,
- typy a kategorie bezpečnostních incidentů,
- náležitosti a způsob oznamování kybernetického bezpečnostního incidentu,
- náležitosti oznámení a provedení reaktivního opatření a jeho výsledku [16].

Významný informační systém – systém, který není součástí KII a je spravovaný orgány veřejné moci, u kterých by mohlo dojít k omezení či výraznému ohrožení výkonu působnosti orgánu veřejné moci při narušení bezpečnosti informací [7].

Zákon č. 412/2005 Sb., *o ochraně utajovaných informací a o bezpečnostní způsobilosti*

Mnohokrát novelizovaný zákon upravující zásady, které definují informaci jako utajovanou. Dále upravuje podmínky, za kterých je možné k těmto informacím přistupovat a požadavky na jejich ochranu. Jako poslední upravuje podmínky pro jejich výkon a také zásady definování citlivých činností [17].

Utajovaná informace – informace, při jejímž vyzrazení nebo zneužití by mohlo dojít ke způsobení újmy zájmu České republiky nebo způsobení nevýhody pro daný zájem a zároveň je uvedena v seznamu utajovaných informací [17].

Vhodné je zmínit i *Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů*, který je v ČR dlouhou dobu aktivní a byl mnohokrát novelizován, nicméně bude

25. května nahrazen *evropským nařízením GDPR*. Z toho důvodu se aktuálně připravuje „*Návrh zákona o zpracování osobních údajů*“, který má nahradit zákon č. 101/2000 Sb.. Tento návrh má být harmonizován s nařízením GDPR a má z části implementovat směrnici Evropského parlamentu a Rady (EU) 2016/680 [18].

1.4.2 Legislativa Evropské unie

Nejdříve je důležité zmínit rozdíl mezi nařízením a směrnicí. Nařízení je zaváděno, tak jak je předloženo, u směrnice je na každém státu, jak ji uvede do svého právního řádu. Proto nařízení GDPR nahrazuje zákon o ochraně osobních údajů, kdežto směrnice NIS se pouze harmonizuje s kybernetickým zákonem.

SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/1148 *(Směrnice **NIS**), o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii*

Network and Information Security incidents (NIS) je směrnice, jejíž cíl je uveden již v jejím rozšířeném názvu, tedy zajistit vysokou úroveň bezpečnosti sítí a informačních systémů v EU. Směrnice zavádí nutnost zřízení subjektů provozovatele základních služeb a provozovatele digitálních služeb. Nové subjekty mají zároveň povinnost hlásit bezpečnostní incidenty a zavést bezpečnostní opatření. Zvýšení pokut do výše maximálně pěti miliónů korun a zavedení pozice manažera kybernetické bezpečnosti pro povinné subjekty [19]. Jak bylo zmíněno v předchozí podkapitole, český kybernetický zákon byl s touto směrnicí již harmonizován.

NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/679 *(Nařízení **GDPR**), o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů a o zrušení rámcového rozhodnutí Rady 2008/977/SVV*

General Data Protection Regulation (GDPR) je obecné nařízení o ochraně údajů. Přijato bylo v roce 2016, ale v platnost vstoupí až 25. května 2018. GDPR má celosvětový rozsah, týká se všech subjektů, které zpracovávají osobní údaje občanů Evropské unie v rámci členských států. Při porušení ochrany osobních údajů může danému subjektu

hrozit pokuta až v řádu miliónů eur. Směrnice nutí k zavedení bezpečnostních opatření již od začátku příprav technických a organizačních procesů a postupů. V případě narušení bezpečnosti osobních údajů má subjekt nahlašovací povinnost vůči dozorovému orgánu [19].

Osobní údaj – jedná se jakoukoli informaci o osobě, jako je například jméno, datum narození či dokonce IP adresa.

Novinky a změny přicházející s GDPR:

Souhlas – ke zpracování osobních údajů je považován jako projev vůle, který je specifický, svobodný, jednoznačný, informovaný a dán formou prohlášení nebo jiným zjevným potvrzením [20].

Práva jednotlivců – rozšíření práv jednotlivců:

- **právo na informace** – správci dat jsou povinni poskytnout jednotlivcům informace o zpracovávání jejich osobních údajů [20].
- **právo na opravu** – jednotlivec má právo na opravu jeho osobních údajů, v případě že jsou údaje nepřesné [20].
- **právo na výmaz** – nebo také „právo být zapomenut“ je právo jednotlivce, aby správce dat vymazal jeho osobní údaje [20].
- **právo na omezení zpracování** – lze aplikovat v definovaných případech, jako např. protiprávní zpracování údajů, ale jednotlivec odmítá vymazání údajů [20].
- **právo na přenositelnost –** jednotlivec má právo získat své osobní údaje od správce dat a předat je jinému správci dat [20].

Na zmíněná práva se však vztahují i omezení v případě, že se jedná například o zajištění národní bezpečnosti. Celý výčet důvodů omezení se nachází v *článku 23* [20].

Ohlašovací povinnost – správce je povinen ohlásit jakékoli porušení zabezpečení osobních údajů dozorovému orgánu, a to nejlépe do 72 hodin od zjištění. V případě nenahlášení do 72 hodin je nutné uvést důvody, proč nebylo porušení oznámeno v rámci časového rámce [20].

Oznamovací povinnost – správce je povinen jednotlivci oznámit porušení zabezpečení osobních údajů, v případě že porušení vede k velkému riziku pro práva a svobody fyzických osob [20].

Soulad s požadavky – aby byl správce schopen dokázat soulad s požadavky, měl by zavést interní politiky a opatření, která jsou v souladu s ochranou dat „*by design"* a „*by default"*. Příkladem takových opatření může být *pseudonymizace* a *anonymizace* údajů. Dále také zavést pozici *pověřence pro ochranu osobních údajů*. [20].

Ochrana dat:

- **by default –** ve smyslu GDPR byl tento pojem přeložen jako „standardní" ochrana osobních údajů". Správce musí zavést vhodná technická a organizační opatření, aby zpracovával pouze ty údaje, které jsou pro daný účel zpracování nezbytné [20].
- **by design** – přeloženo jako „záměrná ochrana osobních údajů" a to znamená, že správce dat musí zavést vhodná technická a organizační opatření, jak v době určení prostředků pro zpracování, tak i při samotném zpracování [20].
    - ***Pseudonymizace*** – vratný proces skrytí identity, po kterém nelze spojit osobní údaje s jednotlivcem bez použití dodatečných informací, které jsou uchovávány odděleně [21].
    - ***Anonymizace*** – nevratný proces skrytí identity, po kterém již nelze jednotlivce identifikovat [21].

Pověřenec pro ochranu osobních údajů – v případě, že zpracovatel nebo správce zaměstnává více jak 250 zaměstnanců, je povinen zřídit pozici pověřence pro ochranu osobních údajů. Má za úkol informovat správce, zpracovatele, zaměstnance o jejich povinnostech při zpracování dat, spolupracovat s dozorovým orgánem a další dle *článku 39* [20].

PROVÁDĚCÍ NAŘÍZENÍ KOMISE (EU) 2018/151, *kterým se stanoví pravidla pro uplatňování směrnice Evropského parlamentu a Rady (EU) 2016/1148, pokud jde o bližší upřesnění prvků, které musí poskytovatelé digitálních služeb zohledňovat při řízení bezpečnostních rizik, jimiž jsou vystaveny sítě a informační systémy, a parametrů pro posuzování toho, zda je dopad incidentu významný*

Stanovuje pravidla pro uplatňování směrnice NIS. Upřesňuje bezpečnostní opatření pro poskytovatele digitálních služeb, která musí zohledňovat při řízení bezpečnostních rizik [9].

1.5 Analýza rizik

Analýza rizik je proces sloužící k odhadnutí ztrát při působení hrozeb na aktiva. Umožňuje určit hodnotu rizika, nebezpečnost hrozeb a zranitelnost aktiv. Existují dva způsoby analýzy – kvalitativní a kvantitativní. Často se používají oba způsoby, popř. i jejich kombinace [1] [22].

1.5.1 Kvalitativní analýza

Analýza k popisu používá škálu kvalifikačních atributů. Popisuje se velikost potenciálních následků (např. nízké, střední, vysoké, kritické) a pravděpodobnost výskytu následků. Škály a popisy lze nastavit nebo upravit dle okolností. Tuto analýzu lze použít, když je kvalitativní analýza vhodná k rozhodnutí nebo je nevhodné využít číselných údajů nebo zdrojů ke kvantitativní analýze. Dále se také používá jako prověřovací činnost případě, že identifikace rizik vyžaduje podrobnější přístup [22].

Výhoda: snadno pochopitelná pro příslušné pracovníky

Nevýhoda: subjektivnost zvolené škály [22]

Tabulka 1: Klasifikační schéma pro hrozby
Zdroj: Vlastní zpracování [16]

Úroveň	Popis
Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.
Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

1.5.2 Kvantitativní analýza

Kvantitativní analýza používá k určení následků a pravděpodobnosti stupnice s číselným vyjádřením. Využívá data z různých zdrojů a kvalita analýzy spočívá na přesnosti a úplnosti číselných hodnot. V mnoha případě využívá historická data incidentů [22].

Výhoda: použití historických dat incidentů → přímá souvislost se zájmy organizace a cíli bezpečnosti

Nevýhoda: málo dat u nových incidentů nebo zranitelností [22]

Tabulka 2: Klasifikační schéma pro riziko
Zdroj: Vlastní zpracování dle [1]

Klasifikační kritérium	Klasifikační stupeň
Bezvýznamné riziko	**0-10**
Akceptovatelné riziko	**11-20**
Nízké riziko	**21-30**
Nežádoucí riziko	**31-60**
Nepřijatelné riziko	**61-125**

1.5.3 Fáze analýzy rizik

Analýza rizik lze rozdělit do 3 fází.

První fáze

Provedení hodnocení aktiv na základě potencionálního dopadu při narušení důvěrnosti, integrity a dostupnosti [1].

- **Identifikace aktiv** – než je možné aktiva ohodnotit, je zapotřebí je identifikovat. Aktiva lze dělit vícero způsoby. Jedním způsobem je klasické rozdělení na softwarová, hardwarová, informační aktiva a služby [1]. Další možností je rozdělení aktiv na primární a podpůrná. Primárními aktivy jsou obchodní procesy a informace, podpůrnými aktivy jsou pak hardware, software, sítě, pracovníci, lokalita, organizace [22].
- **Ohodnocení aktiv –** k identifikovaným aktivům se přiřadí hodnoty na základě zvoleného schématu. Hodnoty představují význam aktiv pro organizaci. K ohodnocení aktiv je dobré použít dotazník nebo rozhovor s vlastníky a uživateli aktiv. Hodnotu lze určit na základě finančního ohodnocení nebo také vzhledem k dopadu na organizaci při narušení důvěrnosti, integrity a dostupnosti informací [1].

Druhá fáze

Druhou fází je ohodnocení hrozeb a zranitelnost a jejím účelem je zhodnotit hrozby a zranitelnost aktiv a díky tomu stanovit úroveň rizik [1].

- **Hodnocení hrozeb** – zde je také opět důležité identifikovat hrozby. To lze provést pomocí normy ČSN ISO/IEC 27005, kde je v příloze C seznam příkladů hrozeb dle typového rozdělení. Identifikací je zapotřebí provést v kontextu s organizací, protože ne všechny hrozby jsou pro organizaci hrozbou (např. sopečný jev atd.). Ohodnocení hrozeb je pak zapotřebí provést v souvislosti s aktivy organizace [1].
- **Odhad zranitelnosti** – představuje odhad slabého místa či nedostatku aktiva, který může být využit hrozbou [1].
- **Úroveň rizika** – úroveň rizika je vypočtena pro každé aktivum pomocí hodnoty aktiva, hodnoty hrozby a zranitelnosti [1].

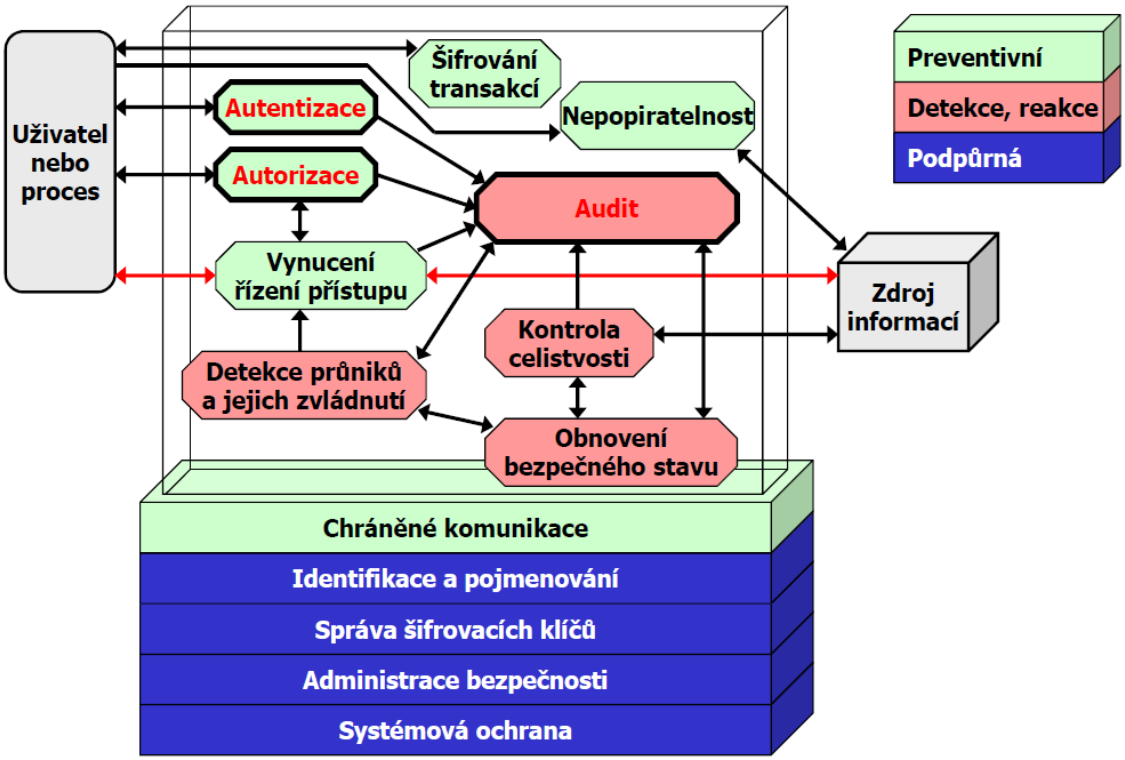
Třetí fáze

Volba vhodných opatření na základě míry rizika. Opatření lze volit například na základě databáze metodiky CRAMM, normy ISO/IEC 27002 a dalších [1].

1.6 Opatření

Jak bylo zmíněno již v definici pojmů, tak opatření je procedura, proces nebo činnost, která vede ke snížení účinku hrozby. Bezpečnostní opatření lze rozdělit do tří typů:

- preventivní,
- detekce a reakce,
- podpůrná.

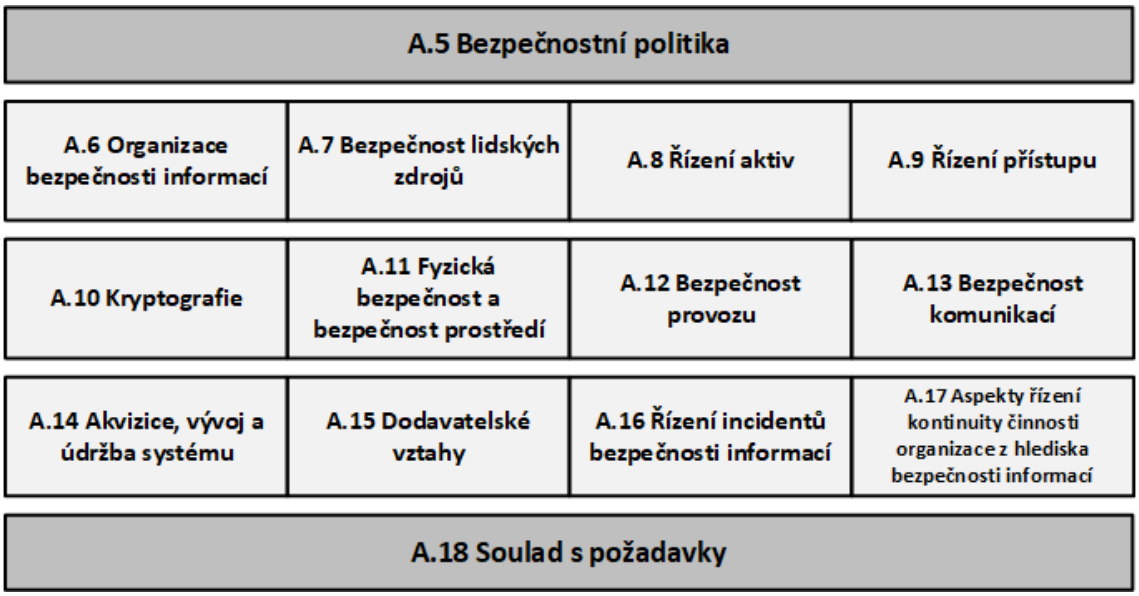


Obrázek 6: Rozlišení bezpečnostních opatření
Zdroj: [1, s. 100]

1.6.1 Výběr opatření

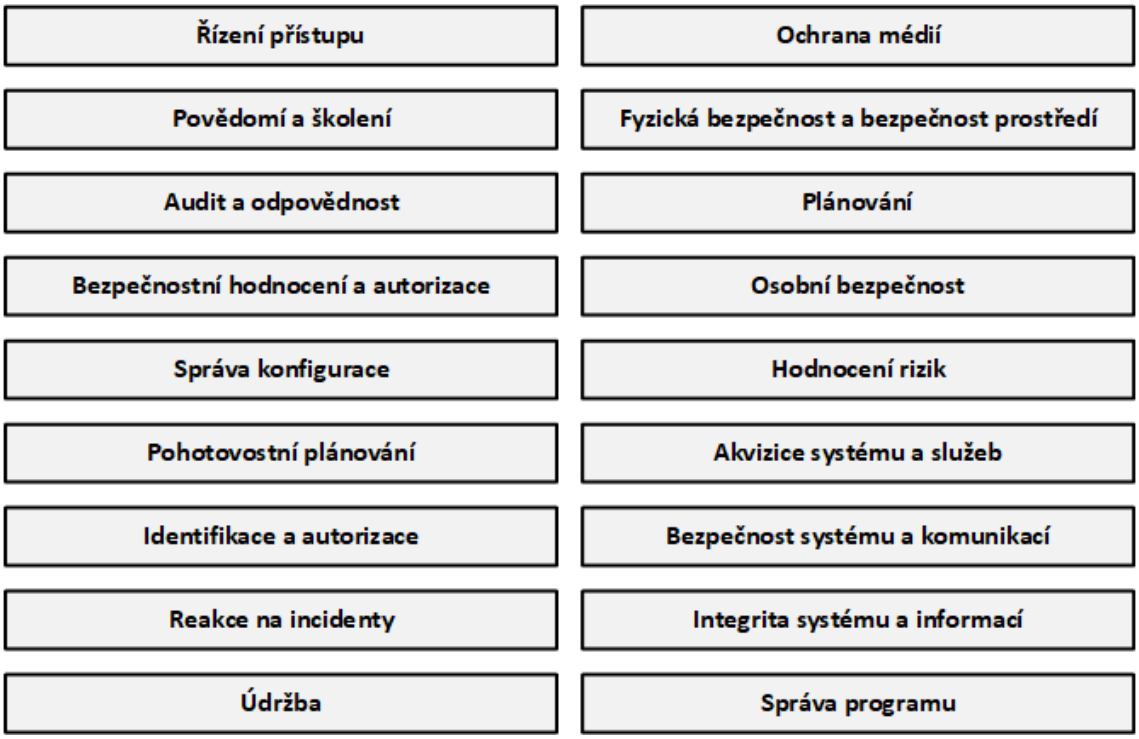
Obecně lze vybírat opatření z norem či metodik k tomu určeným nebo lze také navrhnout nová opatření ke splnění potřeby organizace. Výběr také může podléhat národní či mezinárodní legislativě [23]. Příkladem „katalogů“ opatření jsou normy ISO/IEC 27002, NIST SP 800-53 nebo také metodika CRAMM.

Norma ISO/IEC 27002 obsahuje 114 opatření rozdělených do 14 oblastí. Jednotlivé oblasti jsou vyobrazeny na obrázku 7.



Obrázek 7: Oblasti bezpečnosti informací podle ISO/IEC 27001
Zdroj: Vlastní zpracování [24]

NIST SP 800-53 obsahuje celkem 18 oblastí opatření.



Obrázek 8: Oblasti opatření podle NIST SP 800-53
Zdroj: Vlastní zpracování dle [12, s. 9]

2 ANALÝZA SOUČASNÉHO STAVU

Kapitola analýzy současného stavu má za úkol představit základní informace o společnosti, popis sítě a analýzu vybraných oblastí. V závěru kapitoly budou zmíněny požadavky ze strany společnosti a důvod zájmu o bezpečnost.

2.1 Informace o společnosti

Z důvodu povahy tématu si společnost nepřeje být jmenována ani býti identifikovatelná z informací uvedených v této diplomové práci. Z tohoto důvodu je společnost označována jako „společnost ABC“, popřípadě pouze jako „společnost“. Informace, které by mohly vest k identifikaci společnosti, jsou anonymizované. Stejné pravidlo platí pro informace vedoucí k rozporu s bezpečnostními opatřeními.

Správní forma společnosti je společnost s ručením omezeným a působí v oboru stavebnictví. Poskytuje technické návrhy, provádí technologické zkoušky, servis, školení, konzultace, prodej tmelů a další. Společnost aktuálně vlastní čtyři hlavní prostory. Sídlo společnosti se nachází v Praze a dále bude označována jako „sídlo“. Dalšími prostory jsou dva sklady, první nacházející se na Moravě a druhý v Čechách. Označení použité pro tyto sklady je „sklad Morava“ a „sklad Čechy“. Posledním prostorem je kancelář na území Moravy označená jako „kancelář“.

Společnost také provozuje e-shop, na kterém prodává od výrobců produkty od lepidel po výplňové profily ve stavebnictví, průmyslu atd. E-shop. V krátké době se stal důležitým komunikačním kanálem společnosti pro prodej produktů.

2.2 Současný stav

V této kapitole je popsána síť společnosti a další podstatné prvky.

2.2.1 Serverovna

Server společnosti se nachází mimo její prostory, ačkoliv je vlastníkem serveru, je provozován externě na základě SLA smlouvy společností vlastnící datové centrum. Jedná

se o jeden hardwarový server, na kterém jsou provozovány doménové služby, Microsoft Exchange Server, VPN server, spam filtr a jeden virtuální server obstarávající účetnictví s CRM. Na serveru je nainstalovaný operační systém Microsoft Server 2012. Připojování k serveru z poboček je možný pouze pomocí VPN (IPsec) a to přes stolní počítače či notebooky. Zabezpečení je tedy řešeno jen z pohledu připojení, protože ostatní bezpečnost řeší datové centrum.

2.2.2 Sídlo

Sídlo společnosti je umístěno v záplavové oblasti a pracuje zde několik lidí. Do sítě se připojují pomocí stolních počítačů, notebooků a také mobilními zařízeními. Každý má své přidělené zařízení. Jelikož je server umístěn mimo prostory společnosti, připojení je zprostředkováno pomocí VPN. Připojení k serveru je důležité, protože se na něm nachází účetní a další interní data. Ze sídla zároveň probíhá zálohování dat na cloudové uložiště – Synology cloud – pomocí SSL šifrování. V sídle se také nachází stroj k technologickým zkouškám připojený do sítě a produkuje elektronická data o vykonaných zkouškách, které lze poté v počítači zkoumat. Zabezpečení prostorů je řešeno na dvou úrovních – vchod do budovy a vchod do kanceláří. Ke kontrole vstupu do budovy slouží intercom a kamera. Kanceláře v sídle jsou uzamykatelné. Politika fyzické bezpečnosti není zdokumentována, ale postupy a pravidla mezi zaměstnanci existují. Rozvaděč v sídle je uzamykatelný a je do něj omezen přístup.

2.2.3 Sklad Morava a Čechy

Ve skladu na Moravě pracuje několik lidí a skladník. Jedná se o centrální sklad. Pracovníci mají své počítače, se kterými se připojují pomocí VPN na server. Sklad Čechy má pouze jeden počítač a pracuje zde pouze jeden skladník, který se také připojuje na server prostřednictvím VPN.

2.2.4 Kancelář

Z kanceláře se pracovníci na server připojují pomocí VPN převážně za účelem zpracování účetnictví a k dalším občasným pracím.

2.2.5 Pracovní stanice a notebooky

Pracovní stanice a notebooky slouží k práci zaměstnanců. Notebooky jsou příležitostně brány na výjezdy za zákazníky. Ve všech zařízeních je nainstalován operační systém Windows 10. Na pracovních stanicích i noteboocích je nainstalovaná nejnovější verze antivirového programu AVG.

2.2.6 Mobilní zařízení

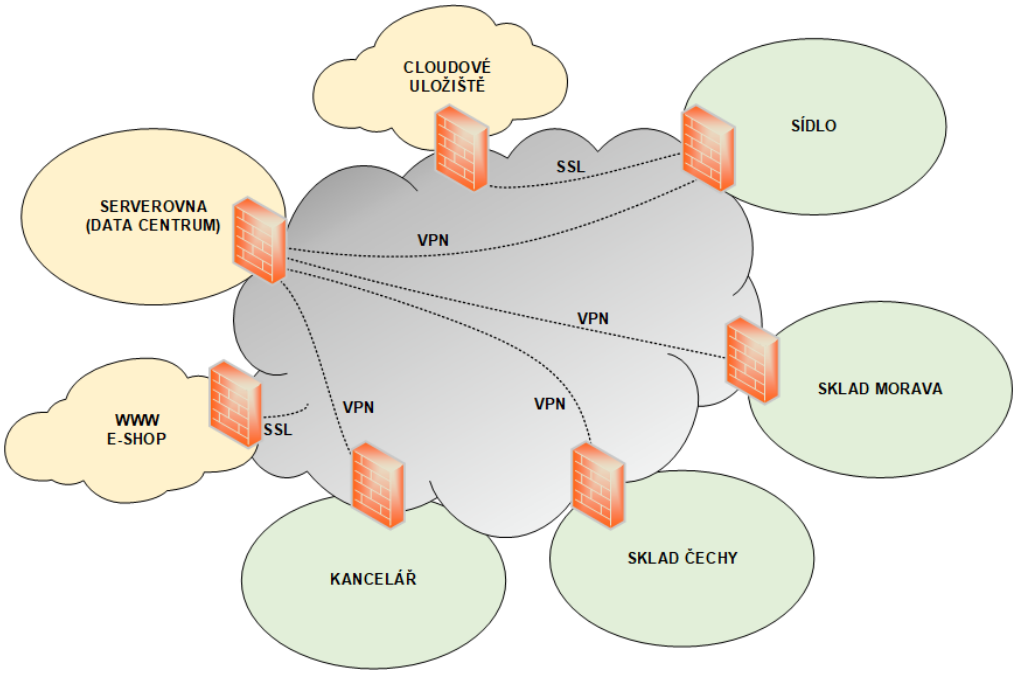
Mobilní telefony používané k práci jsou vlastněny společností a slouží ke komunikaci mezi pracovníky a ke komunikaci se zákazníky. Všechny mobilní telefony jsou pro emailovou komunikaci a synchronizaci kalendáře propojeny pomocí Microsoft Exchange. Při ukončení pracovního poměru se zaměstnancem je mu zařízení odebráno. Nicméně, momentálně neexistuje bezpečnostní opatření na zabezpečení dat v případě, že by se zaměstnanec dozvěděl o výpovědi dříve než oficiální cestou. Dále také neexistuje bezpečnostní opatření při jejich ztrátě či odcizení, kromě klasického zámku displeje a pinu, který není politikou vyžadován a závisí na osobním rozhodnutí zaměstnance. Zabezpečení mobilních zařízení je tedy klasické, tzv. „z výroby“. Společnost nemá zavedenou politiku mobilních zařízení.

2.2.7 Přenos dat

Přenos dat ve společnosti probíhá především po síti. Zaměstnanci nejvíce přenášejí data mezi sídlem a datovým centrem. Kromě komunikace mezi sebou komunikují často i se zákazníky. K zabezpečení komunikace mezi serverem a pracovní stanicí či notebookem je použito VPN na protokolu IPsec. Připojení z mobilního zařízení není zabezpečeno. Pro komunikaci a odesílání dokumentů se používána zejména emailová komunikace. Flash disky, CD ani DVD již dnes společnost nevyužívá. Přenos dat z části řeší firemní politika pravidly a postupy, nicméně pro řízení a komunikaci politika neexistuje. V případě potíží s přenosem dat, řízením a komunikací existují dvě spojení na kontaktní osoby. První spojení je na osobu řešící potíže v rámci společnosti a druhá kontaktní osoba řeší potíže z pohledu data centra.

2.2.8 Zálohování

Provádějí se dvě hlavní zálohy, záloha serveru a záloha pracovních stanic. Záloha pracovních stanic probíhá v sídle společnosti a ukládá se na Cloudové uložiště – Synology cloud. Komunikace je šifrovaná (SSL) a autentizace probíhá dvou-faktorově – heslo a generovaný kód na mobilním telefonu. Záloha serveru představuje zálohu dat na serveru, kdy tato záloha je zároveň uložena na serveru. Politika záloh však není definována, zálohy jsou prováděny systémově automaticky a kontrola záloh je prováděna nahodile. V podstatě existuje ještě třetí záloha dat a to je záznam z IP kamer. Záznam lze normálně sledovat přes aplikaci tzv. „live“ a záloha tohoto záznamu se pak ukládá na paměťovou kartu IP kamery.



Obrázek 9: Propojení sítí
Zdroj: Vlastní zpracování

2.3 Analýza vybraných oblastí

Tato analýza slouží k poskytnutí přehledu bezpečnostních opatření ve společnosti. Analýza je provedena na základě pomůcky k auditu bezpečnostních opatření poskytované úřadem NÚKIB [25], vyhlášky č. 316/2014 Sb. [16] a nařízení GDPR [20]. Některé nerelevantní oblasti jsou vynechány, protože se na společnost nevztahují, jako například zaznamenávání činnosti KII a VIS. V příloze lze nalézt i analýzu k nařízení GDPR, avšak

je zde brána spíše jako vodítko pro společnost, protože se jedná, vzhledem k této práci, o vedlejší téma. Ke každé oblasti je uvedeno shrnutí. Šablona, podle které je analýza provedena:

Název oblasti	Požadavek/otázka
stav	Popis

Stav má definovány čtyři možnosti – **aplikováno**, **částečně aplikováno**, **neaplikováno** a **nerelevantní**.

2.3.1 ISMS

ISMS	Stanoven rozsah a hranice ISMS.
neaplikováno	

ISMS	Stanovena bezpečnostní politika ISMS.
neaplikováno	

ISMS	Zaveden proces: - monitorování účinnosti bezpečnostních opatření - vyhodnocování vhodnosti a účinnosti bezpečnostní politiky - vyhodnocení účinnosti ISMS, které obsahuje hodnocení stavu ISMS včetně revize hodnocení rizik
neaplikováno	

ISMS	Jsou posouzeny výsledky provedených kontrol a auditů kybernetické bezpečnosti a dopadů kybernetických bezpečnostních incidentů na systém řízení bezpečnosti informací, a to nejméně 1x ročně.
neaplikováno	

ISMS	Je prováděna aktualizace ISMS a související dokumentace na základě zjištění auditů/penetračních testů, výsledků hodnocení účinnosti ISMS a v souvislosti s prováděnými změnami.
neaplikováno	

ISMS	Řízen provoz a zdroje ISMS, zaznamenávány činnosti spojené s ISMS a souvisejícím řízením rizik.
neaplikováno	

Společnost nemá zavedenou žádnou část systému řízení bezpečnosti informací a z výše uvedených požadavků nesplňuje žádný. Nemonitoruje účinnost bezpečnostních opatření, nevyhodnocuje vhodnost ani účinnost bezpečnostních politik.

2.3.2 Řízení aktiv

Řízení aktiv	Jsou identifikována a evidována aktiva.
aplikováno	Ano, identifikovány i evidovány.

Řízení aktiv	Stanovena bezpečnostní politika pro klasifikaci aktiv.
neaplikováno	

Řízení aktiv	Určena bezpečnostní role: garant aktiva.
částečně aplikováno	Používá se, ale nejsou dokumentovány práva, povinnosti a kompetence.

Řízení aktiv	Jsou určeni jednotliví garanti aktiv, kteří jsou odpovědní za aktiva.
částečně aplikováno	U soupisu aktiv uveden vlastník (garant). Nejsou práva, povinnosti ani kompetence.

Řízení aktiv	Je hodnocena důležitost aktiv z hlediska důvěrnosti, integrity a dostupnosti.
neaplikováno	

Řízení aktiv	Při hodnocení důležitosti aktiv je posouzeno především: a) Rozsah a důležitost osobních údajů nebo obchodního tajemství. b) Rozsah dotčených právních povinností nebo jiných závazků. c) Rozsah narušení vnitřních řídících a kontrolních činností. d) Poškození veřejných, obchodních nebo ekonomických zájmů. e) Možné finanční ztráty. f) Rozsah narušení běžných činností orgánu a osoby. g) Dopady spojené s narušením důvěrnosti, integrity a dostupnosti. h) Dopady na zachování dobrého jména nebo ochranu dobré pověsti.
neaplikováno	

Řízení aktiv	Jsou stanovena pravidla ochrany, nutná pro zabezpečení jednotlivých úrovní aktiv tím, že: - jsou určeny způsoby rozlišování jednotlivých úrovní aktiv, - jsou stanovena pravidla pro manipulaci a evidenci s aktivy podle úrovní aktiv, včetně pravidel pro bezpečné elektronické sdílení a fyzické přenášení aktiv, - jsou stanoveny přípustné způsoby používání aktiv.
částečně aplikováno	Pravidla ochrany jsou řešena pouze na úrovni směrnice bezpečného chování uživatelů.

Řízení aktiv	Jsou stanovena pravidla ochrany, nutná pro zabezpečení jednotlivých úrovní aktiv tím, že: - jsou zavedena pravidla ochrany odpovídající úrovni aktiv - jsou určeny způsoby pro spolehlivé smazání nebo ničení technických nosičů dat s ohledem na úroveň aktiv
neaplikováno	

V oblasti řízení aktiv nemá společnost zavedenou žádnou politiku. Aktiva i vlastníky aktiv identifikované i evidované má, nicméně nejsou zavedeny povinnosti, práva ani kompetence vlastníků. Je zavedena pouze jedna povinnost vlastníků, a to navrácení aktiv v případě ukončení pracovního poměru. Jedná se tedy pouze o zdokumentovaný seznam. Hodnocení aktiv zavedené není a tím pádem ani řízení rizik. Ochranu aktiv řeší z menší části směrnice o bezpečném chování uživatelů, nicméně se jedná pouze o malou část problematiky ochrany. Částečně tedy ochrana aktiv existuje, ale nejedná se o

systematické řízení ochrany. Jeden požadavek je plněn, tři požadavky jsou plněny částečně a čtyři požadavky plněny nejsou.

2.3.3 Řízení rizik

Řízení rizik	Je zaveden proces řízení rizik.
neaplikováno	

Řízení rizik	Jsou stanoveny metodiky pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik včetně stanovení kritérií pro přijatelnost rizik.
neaplikováno	

Řízení rizik	Prováděna identifikace a hodnocení důležitosti VŠECH aktiv, které patří do rozsahu ISMS, Výstupy jsou zapracovány do zprávy o hodnocení aktiv a rizik.
neaplikováno	

Řízení rizik	Prováděna identifikace rizik, kdy jsou zohledňovány hrozby a zranitelnosti a jsou posuzovány možné dopady na aktiva.
neaplikováno	

Řízení rizik	Jsou určena a schválena přijatelná rizika a je zpracována zpráva o hodnocení aktiv a rizik.
neaplikováno	

Řízení rizik	Na základě bezpečnostních potřeb a výsledků hodnocení rizik je zpracováváno prohlášení o aplikovatelnosti.
neaplikováno	

Řízení rizik	Je zpracovaný a zavedený plán zvládání rizik (RTP), který obsahuje: cíle a přínosy bezpečnostních opatření, určení osoby odpovědné za prosazování bezpečnostních opatření, potřebné finanční, technické, lidské a informační zdroje, termín jejich zavedení a popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními.
neaplikováno	

Řízení rizik	Prováděna aktualizace zprávy o hodnocení aktiv a rizik, bezpečnostní politiky, plánu zvládání rizik a plánu rozvoje bezpečnostního povědomí.
neaplikováno	

Řízení rizik	Při hodnocení rizik jsou zváženy hrozby, související s: a) porušením bezpečnostní politiky, provedením neoprávněných činností, zneužitím oprávnění ze strany uživatelů a administrátorů b poškozením nebo selháním technického anebo programového vybavení c) zneužitím identity fyzické osoby d) užíváním programového vybavení v rozporu s licenčními podmínkami e) kybernetickým útokem z komunikační sítě f) škodlivým kódem (například viry, spyware, trojské koně) g) nedostatky při poskytování služeb IS/KS KII nebo VIS h) narušením fyzické bezpečnosti i) přerušením poskytování služeb elektronických komunikací nebo dodávek elektrické energie j) zneužitím nebo neoprávněnou modifikací údajů k) trvale působícími hrozbami l) s odcizením nebo poškozením aktiva
neaplikováno	

Řízení rizik	Při hodnocení rizik jsou zváženy hrozby, související s: a) porušením bezpečnostní politiky, provedením neoprávněných činností, zneužitím oprávnění ze strany administrátorů KII b) pochybením ze strany zaměstnanců c) zneužitím vnitřních prostředků, sabotáží d) dlouhodobým přerušením poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb e) nedostatkem zaměstnanců s potřebnou odbornou úrovní f) cíleným kybernetickým útokem pomocí sociálního inženýrství, použitím špionážních technik g) zneužitím vyměnitelných technických nosičů dat
Neaplikováno	

Řízení rizik	Zváženy zranitelnosti, související s: - nedostatečnou ochranou ICT - nevhodnou bezpečnostní architekturou - nedostatečnou mírou nezávislé kontroly - neschopností včasného odhalení pochybení ze strany zaměstnanců
neaplikováno	

Řízení rizik	Zváženy zranitelnosti, související s: a) nedostatečnou ochranou vnějšího perimetru b) nedostatečným bezpečnostním povědomí uživatelů a administrátorů c) nedostatečnou údržbou IS/KS KII nebo VIS d) nevhodným nastavením přístupových oprávnění e) nedostatečnými postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů f) nedostatečným monitorováním činností uživatelů a administrátorů a neschopností odhalit jejich nevhodné nebo závadné způsoby chování g) s nedostatečným stanovením bezpečnostních pravidel, nepřesným nebo nejednoznačným vymezením práv a povinností uživatelů, administrátorů a bezpečnostních rolí
neaplikováno	

Řízení rizik není ve společnosti zavedeno, rizika jsou řešena nesystematicky a individuálně.

Žádný z požadavků není splněn.

2.3.4 Organizační bezpečnost

Organizační bezpečnost	Bezpečnostní politika: Organizační bezpečnost
neaplikováno	

Organizační bezpečnost	Určena bezpečnostní role: manažer kybernetické bezpečnosti.
nerelevantní	

Organizační bezpečnost	Určena bezpečnostní role: architekt kybernetické bezpečnosti.
nerelevantní	

Organizační bezpečnost	Určena bezpečnostní role: auditor kybernetické bezpečnosti.
nerelevantní	

Organizační bezpečnost	Bezpečnostní role jsou určeny přiměřeně.
neaplikováno	

Uvedené bezpečnostní role jsou pro společnost nerelevantní, protože se na ně ze zákona nevztahují a z pohledu velikosti organizace by neměly smysl, alespoň co se pozice na plný úvazek týče. Nicméně, důvod uvedení této oblasti je ten, že společnost má v plánu do budoucna rozšířit působnost i do oboru energetiky.

Tři požadavky jsou pro společnost nerelevantní a dva požadavky plněny nejsou.

2.3.5 Řízení dodavatelů

Řízení dodavatelů	Jsou stanovena pravidla pro dodavatele, která zohledňují potřeby řízení bezpečnosti informací, a řídí své dodavatele nebo jiné externí subjekty, které se podílejí na rozvoji, provozu nebo zajištění bezpečnosti ICT.
neaplikováno	

Řízení dodavatelů	Rozsah zapojení dodavatelů na rozvoji, provozu nebo zajištění bezpečnosti ICT dokumentuje písemnou smlouvou, jejíž součástí je ustanovení o bezpečnosti informací.
neaplikováno	

Řízení dodavatelů	Bezpečnostní politika: Řízení vztahů s dodavateli.
neaplikováno	

Řízení dodavatelů	Bezpečnostní politika: Řízení dodavatelů
neaplikováno	

Řízení dodavatelů	U dodavatelů je před uzavřením smlouvy prováděno hodnocení rizik, která jsou spojena s podstatnými dodávkami.
neaplikováno	

Řízení dodavatelů	S dodavateli se uzavírá dohoda o úrovni poskytovaných služeb (SLA), která stanoví způsoby a úrovně realizace bezpečnostních opatření a určí vztah vzájemné smluvní odpovědnosti za zavedení a kontrolu bezpečnostních opatření.
aplikováno	

Řízení dodavatelů	U dodavatelů se provádí pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření u poskytovaných služeb a zjištěné nedostatky odstraňuje nebo po dohodě s dodavatelem zajistí jejich odstranění.
neaplikováno	

Řízení dodavatelů je řešeno pouze z pohledu smlouvy mezi společností a poskytovatelem služeb. Jako příklad lze uvést smlouvu s data centrem – data centrum spravuje server společnosti.

Plněn je pouze jeden požadavek a zbylých šest požadavků plněno není.

2.3.6 Bezpečnost lidských zdrojů

Bezpečnost lidských zdrojů	Bezpečnostní politika: Bezpečnost lidských zdrojů.
neaplikováno	

Bezpečnost lidských zdrojů	Bezpečnostní politika: Bezpečné chování uživatelů.
aplikováno	Ano, existuje dokument.
Bezpečnost lidských zdrojů	Je stanoven plán rozvoje bezpečnostního povědomí, který obsahuje formu, obsah a rozsah potřebných školení a jsou určeny osoby provádějící realizaci jednotlivých činností, které jsou v plánu uvedeny.
neaplikováno	

Bezpečnost lidských zdrojů	V souladu s plánem rozvoje bezpečnostního povědomí je zajištěno poučení uživatelů, administrátorů a osob zastávajících bezpečnostní role o jejich povinnostech a o bezpečnostní politice formou vstupních a pravidelných školení.
neaplikováno	

Bezpečnost lidských zdrojů	Je zajištěno odborné školení bezpečnostních rolí v souladu s plánem rozvoje bezpečnostního povědomí.
neaplikováno	

Bezpečnost lidských zdrojů	Je zajištěna kontrola dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role.
částečně aplikováno	Ano, kontrola dodržování bezpečnostní politiky existuje, ale provádí se náhodně.

Bezpečnost lidských zdrojů	Je zajištěno vrácení svěřených aktiv a odebrání přístupových oprávnění při ukončení smluvního vztahu s uživateli, administrátory nebo osobami zastávajícími bezpečnostní role.
aplikováno	Ano, na základě smlouvy.

Bezpečnost lidských zdrojů	O školení jsou vedeny přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.
aplikováno	Ano, školení jsou dokumentována.

Bezpečnost lidských zdrojů	Jsou stanovena pravidla pro určení osob, které budou zastávat bezpečnostní role, role administrátorů nebo uživatelů.
částečně aplikováno	Ano, ale nejsou sepsána.

Bezpečnost lidských zdrojů	Je hodnocena účinnost plánu rozvoje bezpečnostního povědomí, provedených školení a dalších činností spojených s prohlubováním bezpečnostního povědomí.
neaplikováno	

Bezpečnost lidských zdrojů	Jsou určena pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role (disciplinární řízení).
částečně aplikováno	Ano existují, ale nejsou sepsána. Dochází například ke snížení odměn.

Bezpečnost lidských zdrojů	Zajištěna změna přístupových oprávnění při změně postavení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role.
částečně aplikováno	Ano, při změně postavení dochází ke změně přístupových oprávnění. Nicméně nejsou stanovena pravidla.

Bezpečnost lidských zdrojů má společnost řešenu směrnicí a je i kontrolováno její dodržování. Nicméně kontrola je prováděna nahodile, takže nejsou stanoveny pravidelné intervaly. Společnost posílá své zaměstnance na školení, ale nejedná se školení bezpečnostních rolí a neexistuje žádný plán rozvoje bezpečnostního povědomí. Podstoupená školení jsou dokumentována, tedy o jaké školení se jednalo, a kdo se ho účastnil. Navrácení svěřených aktiv při ukončení pracovního vztahu je řešena ve smlouvě. Pravidla pro určování bezpečnostních rolí jsou využívána, ale nejsou sepsána, pravidla existují pouze v hlavě odpovědné osoby. Disciplinární řízení jsou ve společnosti využívány, nicméně nejsou sepsány. Jedná se například o snížení odměn daného zaměstnance. Tři požadavky splněny, čtyři splněny částečně a pět jich je nesplněno.

2.3.7 Řízení provozu a komunikací

Řízení provozu a komunikací	Bezpečnostní politika: Řízení provozu a komunikací.
neaplikováno	

Řízení provozu a komunikací	Pomocí technických nástrojů (uvedených ve VKB v § 21 až 23 ZKB) jsou detekovány kybernetické bezpečnostní události, pravidelně vyhodnocovány získané informace a na zjištěné nedostatky je reagováno v souladu se zvládáním kybernetických bezpečnostních událostí a incidentů.
neaplikováno	

Řízení provozu a komunikací	Bezpečnostní politika: Bezpečnost komunikační sítě.
částečně aplikováno	

Řízení provozu a komunikací	Bezpečnostní politika: Zálohování a obnova.
neaplikováno	

Řízení provozu a komunikací	Je prováděno pravidelné zálohování a prověřování použitelnosti provedených záloh.
aplikováno	Ano, zálohování je automatizováno a kontrola probíhá nahodile.

Řízení provozu a komunikací	Provozní pravidla a postupy orgánu a osoby obsahují: - Práva a povinnosti osob zastávajících bezpečnostní role, administrátorů a uživatelů.
neaplikováno	

Řízení provozu a komunikací	Provozní pravidla a postupy orgánu a osoby obsahují: - Postupy pro spuštění a ukončení chodu systému, pro restart nebo obnovení chodu systému po selhání a pro ošetření chybových stavů nebo mimořádných jevů
neaplikováno	

Řízení provozu a komunikací	Provozní pravidla a postupy orgánu a osoby obsahují: - Postupy pro sledování kybernetických bezpečnostních událostí a pro ochranu přístupu k záznamům o těchto činnostech
neaplikováno	

Řízení provozu a komunikací	Provozní pravidla a postupy orgánu a osoby obsahují: - Spojení na kontaktní osoby, které jsou určeny jako podpora při řešení neočekávaných systémových nebo technických potíží.
aplikováno	Ano, existuje spojení na osobu k řešení potíží (jedna na řešení potíží ve společnosti a druhá na řešení potíží se serverem).

Řízení provozu a komunikací	Provozní pravidla a postupy orgánu a osoby obsahují: - Postupy řízení a schvalování provozních změn.
částečně aplikováno	Ano, ale není zdokumentováno.

Řízení provozu a komunikací	Provozní pravidla a postupy orgánu a osoby obsahují: - Postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů.
částečně aplikováno	Ano, má na starosti personalista.

Řízení provozu a komunikací	Je zajištěno oddělení vývojového, testovacího a produkčního prostředí.
neaplikováno	

Řízení provozu a komunikací	Bezpečnostní politika: Řízení technických zranitelností.
neaplikováno	

Řízení provozu a komunikací	Jsou určena pravidla a postupy pro ochranu informací, které jsou přenášeny komunikačními sítěmi.
aplikováno	Ano, existuje dokument (směrnice) určující pravidla a postupy.

Řízení provozu a komunikací	Bezpečnostní politika: Bezpečné předávání a výměna informací.
neaplikováno	

Řízení provozu a komunikací	Výměna a předávání informací je prováděna na základě pravidel stanovených právními předpisy za současného zajištění bezpečnosti informací a tato pravidla jsou dokumentována.
neaplikováno	

Řízení provozu a komunikací	S ohledem na klasifikaci aktiv je prováděna výměna a předávání informací na základě písemných smluv, jejichž součástí je ustanovení o bezpečnosti informací.
neaplikováno	

Řízení provozu a komunikací	Bezpečnostní politika: Poskytování a nabývání licencí programového vybavení a informací.
aplikováno	Ano, dokument zahrnující správu licencí (seznam, nabývání, kontrola).

Řízení provozu a komunikací	Bezpečnostní politika: Dlouhodobé ukládání a archivace informací.
částečně aplikováno	Ano, dlouhodobé ukládání a archivace se provádí, nicméně neexistují pravidla ani postupy.

Společnost nemá politiku řízení provozu a komunikací, ale má částečně politiku bezpečnosti komunikační sítě. Zálohování probíhá na serveru a v sídle, na serveru se zálohují serverová data, ke kterým zaměstnanci přistupují a v sídle se zálohují pracovní stanice. Politika zálohy je automatizovaná a kontrola je prováděna nahodile. Podpora při neočekávaných potížích je řešena z pohledu serveru a společnosti. Podporu serveru má na starosti datové centrum na základě SLA smlouvy a podporu ve společnosti má na starost jiná kontraktovaná osoba. Řízení lidských a technických zdrojů má ve společnosti na starosti personalista. Správa licencí je řešena dokumentem. Archivace a ukládání dat se ve společnosti provádí, ale nejsou žádné postupy ani pravidla.

Čtyři požadavky splněny, další čtyři jsou plněny částečně a jedenáct jich plněno není.

2.3.8 Řízení přístupu a bezpečné chování uživatelů

Řízení přístupu a bezpečné chování uživatelů	Řízen přístup k systémům a informacím.
částečně aplikováno	

Řízení přístupu a bezpečné chování uživatelů	Každému uživateli je přiřazen jednoznačný identifikátor (každý uživatel má své vlastní autentizační údaje).
aplikováno	
Řízení přístupu a bezpečné chování uživatelů	Bezpečnostní politika: Řízení přístupu.
částečně aplikováno	Ano, princip minimálního oprávnění, přezkoumání přístupových oprávnění, nicméně není pravidelné.

Řízení přístupu a bezpečné chování uživatelů	Používán nástroj pro ověřování identity uživatelů (autentizační server).
částečně aplikováno	Ano, používán autentizační certifikát (ale pouze na Microsoft zařízeních).

Řízení přístupu a bezpečné chování uživatelů	Používán nástroj pro řízení přístupových oprávnění.
neaplikováno	

Řízení přístupu a bezpečné chování uživatelů	Přistupujícím aplikacím je přidělen samostatný identifikátor.
aplikováno	
Řízení přístupu a bezpečné chování uživatelů	Je omezeno přidělování administrátorských oprávnění.
aplikováno	Ano, admin. Oprávnění přiděluje odpovědná osoba. Role adminů jsou odebírány, když již nejsou zapotřebí. Role superadmina existuje.

Řízení přístupu a bezpečné chování uživatelů	Přidělování a odebírání přístupových oprávnění je prováděno v souladu s politikou řízení přístupu.
neaplikováno	Není na to dokument.

Řízení přístupu a bezpečné chování uživatelů	Je prováděno pravidelné přezkoumání nastavení přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách nebo rolích.
neaplikováno	

Řízení přístupu a bezpečné chování uživatelů	Bezpečnostní politika: Bezpečné používání mobilních zařízení.
neaplikováno	

Řízení přístupu a bezpečné chování uživatelů	Jsou zavedena bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení, případně i bezpečnostní opatření spojená s využitím technických zařízení, kterými povinná osoba nedisponuje.
částečně aplikováno	Politika neexistuje, bezpečné používání pouze z hlediska systémového řešení iOs/Android.

Přístup k systémům a informacím je řízen pouze částečně, na Microsoft zařízeních je k ověřování identity využíván autentizační certifikát, nicméně se jedná pouze o notebooky a pracovní stanice. Princip minimálního oprávnění i přezkoumávání oprávnění jsou ve společnosti prováděny, ale přezkoumání není pravidelné. Přidělování administrátorský práv má na starost odpovědná osoba, která zároveň role odebírá, když

již nejsou nadále zapotřebí, pravidla odebírání ale neexistují. Bezpečnostní opatření z pohledu mobilních zařízení jsou řešena pouze systémovým řešením.

Tři požadavky jsou plněny, čtyři jsou plněny částečně a čtyři nejsou plněny.

2.3.9 Ověřování identity uživatelů

Ověřování identity uživatelů	Síla hesla v příp. autentizace pouze heslem, zajišťuje: - Minimální délku hesla 8 znaků. - Minimální složitost hesla tak, že heslo bude obsahovat alespoň 3 z následujících čtyř požadavků: 1. nejméně jedno velké písmeno, 2. nejméně jedno malé písmeno, 3. nejméně jednu číslici nebo 4. nejméně jeden speciální znak, který není uveden v bodech 1 až 3. - Maximální dobu pro povinnou výměnu hesla nepřesahující 100 dnů; tento požadavek není vyžadován pro samostatné identifikátory aplikací.
částečně aplikováno	Ano, min. délka 8 znaků i různorodost hesla je používána. Maximální doba pro výměnu je však 12 měsíců.

Ověřování identity uživatelů	Délka hesla u administrátorů min. 15 znaků (za uplatnění ostatních předchozích pravidel).
částečně aplikováno	Není vyžadováno min., ale heslo bývá vždy nastaveno jako velmi dlouhý řetězec. Žádná politika neexistuje.

Ověřování identity uživatelů	Použita více-faktorová autentizace.
neaplikováno	

Ověřování identity uživatelů	Je zamezeno opětovnému používání dříve používaných hesel; není umožněno více změn hesla jednoho uživatele během stanoveného období, které musí být nejméně 24 hodin.
částečně aplikováno	Neřeší dokument.

Ověřování identity uživatelů	Automatické odhlášení při nečinnosti (Je používán nástroj pro ověřování identity, který provádí opětovné ověření identity po určené době nečinnosti).
aplikováno	Ano, řeší i dokument.

Nástroj pro ověřování identity má nastavenou minimální délku hesla osm znaků a zmíněné požadavky. Nicméně, povinná výměna hesla je nastavena na dvanáct měsíců. V případě administrátorských hesel je využíváno supersilné heslo přesahující patnáct znaků, ale neexistuje politika. Nástroj znemožňuje použití dříve použitých hesel, ale vícerá změna hesel během jednoho dne není zamezena a ani není řešena dokumentem. Automatické odhlášení při nečinnosti je nastaveno a je i řešeno dokumentem.

Jeden požadavek je plněn, tři jsou plněny částečně a jeden plněn není.

2.3.10 Řízení přístupových oprávnění

Řízení přístupových oprávnění	Je používán nástroj pro řízení přístupových oprávnění, kterým zajišťuje řízení oprávnění: Pro přístup k jednotlivým aplikacím a datům.
neaplikováno	

Řízení přístupových oprávnění	Je používán nástroj pro řízení přístupových oprávnění, kterým zajišťuje řízení oprávnění: Pro čtení dat, pro zápis dat a pro změnu oprávnění.
neaplikováno	

Řízení přístupových oprávnění	Logování přístupů (Je používán nástroj pro řízení přístupových oprávnění, který zaznamenává použití přístupových oprávnění v souladu s bezpečnostními potřebami a výsledky hodnocení rizik).
aplikováno	Ano, systémové řešení MS.

Logování přístupu je řešeno pouze systémovým řešením Microsoft.

Jeden požadavek je plněn a dva nikoli.

2.3.11 Aplikační bezpečnost

Aplikační bezpečnost	Jsou prováděny bezpečnostní testy zranitelnosti aplikací, které jsou přístupné z vnější sítě, a to před jejich uvedením do provozu a po každé zásadní změně bezpečnostních mechanismů.
neaplikováno	

Aplikační bezpečnost	Je zajištěna trvalá ochrana aplikací a informací dostupných z vnější sítě před neoprávněnou činností, popřením provedených činností, kompromitací nebo neautorizovanou změnou.
aplikováno	Ano, firewall, spam filtr a omezení přístupu a oprávnění.

Aplikační bezpečnost	Je zajištěna trvalá ochrana transakcí před jejich nedokončením, nesprávným směrováním, neautorizovanou změnou předávaného datového obsahu, kompromitací, neautorizovaným duplikováním nebo opakováním.
neaplikováno	

Ochrana aplikací a informací je řešena na úrovni firewallu, spam filtru a omezení oprávnění a přístupu. Testy zranitelnosti však prováděny nejsou a ani není zajištěna trvalá ochrana transakcí.

Jeden požadavek splněn a dva nesplněny.

2.3.12 Kryptografie

Kryptografie	Bezpečnostní politika: Používání kryptografické ochrany.
neaplikováno	

Kryptografie	Pro používání kryptografické ochrany je stanovena úroveň ochrany s ohledem na typ a sílu kryptografického algoritmu.
neaplikováno	

Kryptografie	Pro používání kryptografické ochrany jsou stanovena pravidla kryptografické ochrany informací při přenosu po komunikačních sítích nebo při uložení na mobilní zařízení nebo vyměnitelné technické nosiče dat.
neaplikováno	

Kryptografie	V souladu s bezpečnostními potřebami a výsledky hodnocení rizik jsou používány kryptografické prostředky, které zajistí ochranu důvěrnosti a integrity předávaných nebo ukládaných dat a prokázání odpovědnosti za provedené činnosti.
neaplikováno	

Kryptografie	Pro používání kryptografických prostředků je stanoven systém správy klíčů, který zajistí generování, distribuci, ukládání, archivaci, změny, ničení, kontrolu a audit klíčů.
neaplikováno	

Kryptografie	Jsou používány odolné kryptografické algoritmy a kryptografické klíče.
částečně aplikováno	Používá se autentizační certifikát, VPN.

Při přihlašování na server je totožnost ověřována pomocí autentizačního certifikátu. Toto však lze provádět pouze na zařízeních Microsoft, nicméně na mobilních zařízeních se ověřování certifikátem nedělá. Dále se používá VPN na protokolu IPsec k připojování na server. Tento protokol využívá kryptografické algoritmy i klíče.

Jeden požadavek částečně plněn a zbylých pět neplněno.

2.3.13 Zajištění dostupnosti

Zajištění dostupnosti	V souladu s bezpečnostními potřebami a výsledky hodnocení rizik je zajištěna potřebná úroveň dostupnosti informací.
částečně aplikováno	Zálohy i redundance disků, ale ne na základě hodnocení rizik.

Zajištění dostupnosti	Zajištěna dostupnost systémů pro účely splnění cílů řízení kontinuity činností.
neaplikováno	

Zajištění dostupnosti	Zajištěna odolnost systémů vůči kybernetickým bezpečnostním incidentům, které by mohly snížit dostupnost.
částečně aplikováno	Spam filtr, firewall, antivir, VPN router.

Zajištění dostupnosti	Zálohování důležitých technických aktiv je řešeno využitím redundance v návrhu řešení.
neaplikováno	

Zajištění dostupnosti	Zálohování důležitých technických aktiv je řešeno i zajištěním náhradních technických aktiv v určeném čase.
neaplikováno	

Dostupnost informací je řešena obecně nikoliv však na základě hodnocení rizik. Důležitá data jsou zálohována a disky zapojené do RAID. Zajištění dostupnosti před kybernetickými útoky má za úkol firewall, spam filtr, antivir a VPN router.

Dva požadavky jsou částečně plněny a tři neplněny.

2.3.14 Fyzická bezpečnost

Fyzická bezpečnost	Bezpečnostní politika: Fyzická bezpečnost.
částečně aplikováno	Existuje, ale není žádná dokumentace.

Fyzická bezpečnost	Jsou přijata nezbytná opatření k zamezení neoprávněnému vstupu do vymezených prostor, kde jsou zpracovávány informace a umístěna technická aktiva.
aplikováno	Omezen přístup do prostorů společnosti, kanceláří i rozvaděče v sídle.

Fyzická bezpečnost	Jsou přijata nezbytná opatření k zamezení poškození a zásahům do vymezených prostor, kde jsou uchovány informace a umístěna technická aktiva.
aplikováno	

Fyzická bezpečnost	Je předcházeno poškození, krádeži nebo kompromitaci aktiv nebo přerušení poskytování služeb.
částečně aplikováno	

Fyzická bezpečnost	Jsou uplatněny prostředky fyzické bezpečnosti pro zajištění ochrany na úrovni objektů.
aplikováno	

Fyzická bezpečnost	Jsou uplatněny prostředky fyzické bezpečnosti pro zajištění ochrany v rámci objektů zajištěním zvýšené bezpečnosti vymezených prostor, ve kterých jsou umístěna technická aktiva.
aplikováno	

Fyzická bezpečnost je ve společnosti řešena, ale není zdokumentovaná. Je tedy obecný rámec, jak postupovat při odemykání a zamykání prostor, ale není sepsán. Přístup do

prostor s aktivy a informacemi je omezen. Do budovy společnosti je zapotřebí klíč a vchod je snímán kamerou. Kanceláře a rozvaděč jsou také uzamykatelné klíčem.

Čtyři požadavky splněny a dva požadavky splněny částečně.

2.3.15 Ochrana integrity komunikačních sítí

Ochrana integrity komunikačních sítí	Pro ochranu integrity rozhraní vnější komunikační sítě je zavedeno: Řízení bezpečného přístupu mezi vnější a vnitřní sítí
aplikováno	Firewall

Ochrana integrity komunikačních sítí	Pro ochranu integrity rozhraní vnější komunikační sítě je zavedeno: Segmentace zejména použitím demilitarizovaných zón jako speciálního typu sítě používaného ke zvýšení bezpečnosti aplikací dostupných z vnější sítě a k zamezení přímé komunikace vnitřní sítě s vnější sítí.
neaplikováno	

Ochrana integrity komunikačních sítí	Pro ochranu integrity rozhraní vnější komunikační sítě je zavedeno: Použití kryptografických prostředků pro vzdálený přístup, vzdálenou správu nebo pro přístup pomocí bezdrátových technologií.
částečně aplikováno	Ano, VPN.

Ochrana integrity komunikačních sítí	Pro ochranu integrity rozhraní vnější komunikační sítě je zavedeno: Opatření pro odstranění nebo blokování přenášených dat, které neodpovídají požadavkům na ochranu integrity komunikační sítě.
částečně aplikováno	Ano, firewall a antivir.

Ochrana integrity komunikačních sítí	Pro ochranu integrity rozhraní vnější komunikační sítě je zavedeno: Jsou využívány nástroje pro ochranu integrity vnitřní komunikační sítě, které zajistí její segmentaci.
částečně aplikováno	Ano, firewall a VLAN.

Řízení přístupu mezi vnitřní a vnější sítí je řešeno pomocí firewallu a pro vzdálený přístup je využíváno VPN připojení. Pro blokování neodpovídajících dat slouží firewall, a nakonec antivir na koncovém zařízení. Vnitřní síť je segmentovaná do virtuálních lokálních sítí (VLAN). Jeden požadavek splněn, tři částečně a jeden nesplněn.

2.3.16 Ochrana před škodlivým kódem

Ochrana před škodlivým kódem	Bezpečnostní politika: Ochrana před škodlivým kódem.
neaplikováno	

Ochrana před škodlivým kódem	Je používán nástroj pro ochranu před škodlivým kódem, který zajistí ověření a stálou kontrolu: Komunikace mezi vnitřní sítí a vnější sítí.
aplikováno	Ano, antivir, firewall, spam filtr.

Ochrana před škodlivým kódem	Je používán nástroj pro ochranu před škodlivým kódem, který zajistí ověření a stálou kontrolu: Serverů a sdílených datových úložišť.
aplikováno	Ano, ale řeší data centrum.

Ochrana před škodlivým kódem	Je používán nástroj pro ochranu před škodlivým kódem, který zajistí ověření a stálou kontrolu: Pracovních stanic.
aplikováno	Ano, antivir.

Ochrana před škodlivým kódem	Jsou prováděny pravidelné aktualizace nástrojů pro ochranu před škodlivým kódem, jejich definic a signatur.
aplikováno	

Politika na ochranu před škodlivým kódem neexistuje. Ochrana komunikace před škodlivým kódem mezi vnitřní a vnější sítí je řešena firewallem, spam filtrem a antivirem. Ochranu serveru řeší data centrum, tudíž server je lépe zabezpečen, než kdyby byl ve správě společnosti. Ochrana pracovních stanic je řešena pouze na úrovni antiviru.

Čtyři požadavky splněny a jeden nesplněn.

2.3.17 Detekce kybernetických bezpečnostních událostí

Detekce kybernetických bezpečnostních událostí	Bezpečnostní politika: Nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí
neaplikováno	

Detekce kybernetických bezpečnostních událostí	Je používán nástroj pro detekci kybernetických bezpečnostních událostí, který vychází ze stanovených bezpečnostních potřeb a výsledků hodnocení rizik a který zajistí ověření, kontrolu a případné zablokování komunikace mezi vnitřní komunikační sítí a vnější sítí.
neaplikováno	

Detekce kybernetických bezpečnostních událostí	Je používán nástroj pro detekci kybernetických bezpečnostních událostí, který zajistí ověření, kontrolu a případně zablokování komunikace v rámci vnitřní komunikační sítě.
částečně aplikováno	

Detekce kybernetických bezpečnostních událostí	Je používán nástroj pro detekci kybernetických bezpečnostních událostí, který zajistí ověření, kontrolu a případně zablokování komunikace serverů.
aplikováno	Ano, řeší datové centrum.

Detekce řešení kybernetických bezpečnostních událostí je plně řešena pouze ze strany datové centra.

2.3.18 Řízení kontinuity činností

BCM	Je stanovena strategie BCM
neaplikováno	

BCM	Jsou stanoveny cíle BCM formou určení: Minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu ICT (Minimum Business Continuity Objective (MBCO)).
neaplikováno	

BCM	Jsou stanoveny cíle BCM formou určení: Doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných klíčových služeb (závislých na ICT) (RTO).
neaplikováno	

BCM	Jsou stanoveny cíle BCM formou určení: Doby obnovení dat jako termínu, ke kterému budou obnovena data po kybernetickém bezpečnostním incidentu (RPO).
neaplikováno	

BCM	Jsou v rámci řízení kontinuity činností stanoveny práva a povinnosti garantů aktiv, administrátorů a osob zastávajících bezpečnostní role.
neaplikováno	

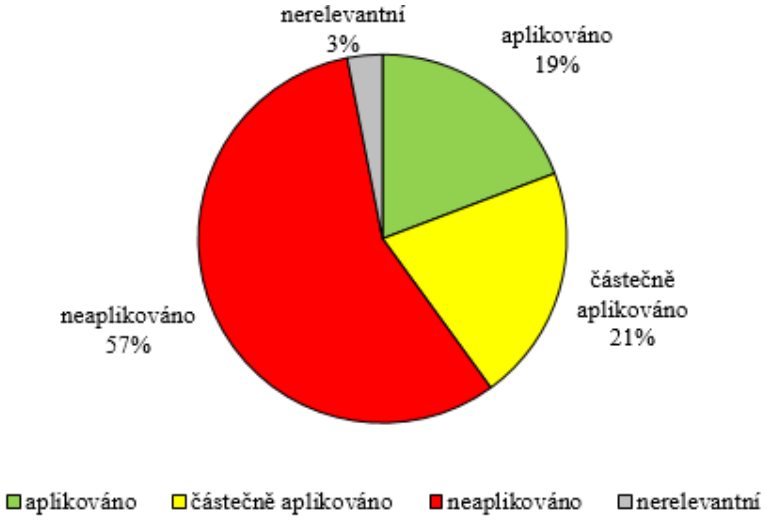
BCM	Jsou vyhodnocovány a dokumentovány možné dopady kybernetických bezpečnostních incidentů a posouzena možná rizika související s ohrožením kontinuity činností.
neaplikováno	

BCM	Jsou stanoveny, aktualizovány a pravidelně testovány plány kontinuity činností (BCP).
neaplikováno	

Kontinuita činnosti není společností nijak provozována, a proto nesplňuje žádný z požadavků.

2.3.19 Shrnutí plnění

Z analýzy vybraných oblastí vyplynulo, že celkově společnost splňuje 25 požadavků (19%), částečně splňuje 27 požadavků (21%), nesplňuje 74 požadavků (57%) a 4 požadavky (3%) jsou pro ni nerelevantní. Obrázek 10 zobrazuje zmíněné plnění požadavků koláčovým grafem.



Obrázek 10: Koláčový graf procentuálního plnění požadavků
Zdroj: Vlastní zpracování

2.4 Souhrn analýzy oblastí k opatřením ISMS

Na základě analýzy vybraných oblastí je sestavena tabulka plnění jednotlivých opatření ISMS. Tato tabulka představuje souhrn opatření, které společnost splňuje či nikoli. Jednotlivá opatření jsou převzata z přílohy normy ČSN ISO/IEC 27001 a k nim je následně přiřazeno jejich plnění na základě předchozí analýzy. Stavy opatření jsou definovány stejně jako u předchozí analýzy – neaplikováno, aplikováno, částečně aplikováno a nerelevantní.

Tabulka 3: Analýza oblastí převedená na opatření ISMS
Zdroj: Vlastní zpracování

A.5 Politiky bezpečnosti informací	
A.5.1 Směřování bezpečnosti informací vedením organizace	
A.5.1.1 Politiky pro bezpečnost informací	**Částečně**
A.5.1.2 Přezkoumání politik pro bezpečnost informací	**Neaplikováno**
A.6 Organizace bezpečnosti informací	
A.6.1 Interní organizace	
A.6.1.1 Role a odpovědnosti bezpečnosti informací	**Neaplikováno**
A.6.1.2 Princip oddělení povinností	**Neaplikováno**
A.6.1.3 Kontakt s příslušnými orgány a autoritami	**Neaplikováno**
A.6.1.4 Kontakt se zájmovými skupinami	**Neaplikováno**
A.6.1.5 Bezpečnost informací v řízení projektů	**Neaplikováno**
A.6.2 Mobilní zařízení a práce na dálku	
A.6.2.1 Politika mobilních zařízení	**Neaplikováno**
A.6.2.2 Práce na dálku	**Neaplikováno**

A.7 Bezpečnost lidských zdrojů	
A.7.1 Před vznikem pracovního vztahu	
A.7.1.1 Prověřování	**Neaplikováno**
A.7.1.2 Podmínky pracovního vztahu	**Zavedeno**
A.7.2 Během pracovního vztahu	
A.7.2.1 Odpovědnosti vedení organizace	**Částečně**
A.7.2.2 Povědomí, vzdělávání a školení bezpečnosti informací	**Neaplikováno**
A.7.2.3 Disciplinární řízení	**Částečně**
A.7.3 Ukončení a změna pracovního vztahu	
A.7.3.1 Odpovědnosti při ukončení nebo změně pracovního vztahu	**Aplikováno**
A.8 Řízení aktiv	
A.8.1 Odpovědnost za aktiva	
A.8.1.1 Seznam aktiv	**Částečně**
A.8.1.2 Vlastnictví aktiv	**Aplikováno**
A.8.1.3 Přípustné použití aktiv	**Neaplikováno**
A.8.1.4 Navrácení aktiv	**Aplikováno**
A.8.2 Klasifikace informací	
A.8.2.1 Klasifikace informací	**Neaplikováno**
A.8.2.2 Označování informací	**Neaplikováno**
A.8.2.3 Manipulace s aktivy	**Neaplikováno**
A.8.3 Manipulace s médii	
A.8.3.1 Správa výměnných médií	**Neaplikováno**
A.8.3.2 Likvidace médií	**Neaplikováno**
A.8.3.3 Přeprava fyzických médií	**Neaplikováno**
A.9 Řízení přístupu	
A.9.1 Požadavky organizace na řízení přístupu	
A.9.1.1 Politika řízení přístupu	**Částečně**
A.9.1.2 Přístup k sítím a síťovým službám	**Částečně**
A.9.2 Řízení přístupu uživatelů	
A.9.2.1 Registrace a zrušení registrace uživatele	**Částečně**
A.9.2.2 Správa uživatelských přístupů	**Částečně**
A.9.2.3 Správa privilegovaných přístupových práv	**Částečně**
A.9.2.4 Správa tajných autentizačních informací uživatelů	**Částečně**
A.9.2.5 Přezkoumání přístupových práv uživatelů	**Aplikováno**
A.9.2.6 Odebrání nebo úprava přístupových práv	**Částečně**
A.9.3 Odpovědnosti uživatelů	
A.9.3.1 Používání tajných autentizačních informací	**Částečně**
A.9.4 Řízení přístupu k systémům a aplikacím	
A.9.4.1 Omezení přístupu k informacím	**Částečně**
A.9.4.2 Bezpečné postupy přihlášení	**Částečně**
A.9.4.3 Systém správy hesel	**Aplikováno**
A.9.4.4 Použití privilegovaných programových nástrojů	**Neaplikováno**
A.9.4.5 Řízení přístupu ke zdrojovým kódům programů	**Částečně**

A.10 Kryptografie	
A.10.1 Kryptografická opatření	
A.10.1.1 Politika pro použití kryptografických opatření	**Neaplikováno**
A.10.1.2 Správa klíčů	**Neaplikováno**
A.11 Fyzická bezpečnost a bezpečnost prostředí	
A.11.1 Bezpečné oblasti	
A.11.1.1 Fyzický bezpečnostní perimetr	**Neaplikováno**
A.11.1.2 Fyzické kontroly vstupu	**Částečně**
A.11.1.3 Zabezpečení kanceláří, místností a vybavení	**Aplikováno**
A.11.1.4 Ochrana před vnějšími hrozbami a hrozbami prostředí	**Neaplikováno**
A.11.1.5 Práce v bezpečných oblastech	**Neaplikováno**
A.11.1.6 Oblasti pro nakládku a vykládku	**Nerelevantní**
A.11.2 Zařízeni	
A.11.2.1 Umístění zařízení a jeho ochrana	**Částečně**
A.11.2.2 Podpůrné služby	**Neaplikováno**
A.11.2.3 Bezpečnost kabelových rozvodů	**Částečně**
A.11.2.4 Údržba zařízení	**Neaplikováno**
A.11.2.5 Přemístění aktiv	**Neaplikováno**
A.11.2.6 Bezpečnost zařízení a aktiv mimo prostory organizace	**Neaplikováno**
A.11.2.7 Bezpečná likvidace nebo opakované použití zařízení	**Částečně**
A.11.2.8 Uživatelská zařízení bez obsluhy	**Neaplikováno**
A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru	**Neaplikováno**
A.12 Bezpečnost provozu	
A.12.1 Provozní postupy a odpovědnosti	
A.12.1.1 Dokumentované provozní postupy	**Částečně**
A.12.1.2 Řízení změn	**Částečně**
A.12.1.3 Řízení kapacit	**Neaplikováno**
A.12.1.4 Princip oddělení prostředí vývoje, testování a provozu	**Neaplikováno**
A.12.2 Ochrana proti malwaru	
A.12.2.1 Opatření proti malwaru	**Částečně**
A.12.3 Zálohování	
A.12.3.1 Zálohování informací	**Částečně**
A.12.4 Zaznamenávání formou logů a monitorování	
A.12.4.1 Zaznamenávání událostí formou logů	**Částečně**
A.12.4.2 Ochrana logů	**Částečně**
A.12.4.3 Logy o činnosti administrátorů a operátorů	**Částečně**
A.12.4.4 Synchronizace hodin	**Neaplikováno**
A.12.5 Správa provozního softwaru	
A.12.5.1 Instalace softwaru na provozní systémy	**Aplikováno**
A.12.6 Řízení technických zranitelností	
A.12.6.1 Řízení technických zranitelností	**Neaplikováno**
A.12.6.2 Omezení instalace softwaru	**Aplikováno**
A.12.7 Hlediska auditu informačních systémů	

A.12.7.1 Opatřeni k auditu informačních systémů	**Neaplikováno**
A.13 Bezpečnost komunikací	
A.13.1 Správa bezpečnosti sítě	
A.13.1.1 Opatření v sítích	**Částečně**
A.13.1.2 Bezpečnost síťových služeb	**Částečně**
A.13.1.3 Princip oddělení v sítích	**Aplikováno**
A.13.2 Přenos informací	
A.13.2.1 Politiky a postupy při přenosu informací	**Aplikováno**
A.13.2.2 Dohody o přenosu informací	**Neaplikováno**
A.13.2.3 Elektronické předávání zpráv	**Částečně**
A.13.2.4 Dohody o utajení nebo o mlčenlivosti	**Neaplikováno**
A.14 Akvizice, vývoj a údržba systémů	
	Nerelevantní
A.15 Dodavatelské vztahy	
A.15.1 Bezpečnost informací v dodavatelských vztazích	
A.15.1.1 Politika bezpečnosti informaci pro dodavatelské vztahy	**Neaplikováno**
A.15.1.2 Bezpečnostní požadavky v dohodách s dodavateli	**Částečně**
A.15.1.3 Dodavatelský řetězec informačních a komunikačních technologií	**Neaplikováno**
A.15.2 Řízení dodávek služeb dodavatelů	
A,15.2.1 Monitorování a přezkoumávání služeb dodavatelů	**Neaplikováno**
A.15.2.2 Řízení změn ve službách dodavatelů	**Neaplikováno**
A.16 Řízení incidentů bezpečnosti informací	
A.16.1 Řízení incidentů bezpečnosti informací a zlepšování	
A.16.1.1 Odpovědnosti a postupy	**Neaplikováno**
A.16.1.2 Hlášení událostí bezpečnosti informací	**Částečně**
A.16.1.3 Hlášení slabých míst bezpečnosti informací	**Neaplikováno**
A.16.1.4 Posouzení a rozhodnutí o událostech bezpečnosti informací	**Neaplikováno**
A.16.1.5 Reakce na incidenty bezpečnosti informací	**Neaplikováno**
A.16.1.6 Ponaučeni z incidentů bezpečnosti informací	**Částečně**
A.16.1.7 Shromažďování důkazů	**Neaplikováno**
A.17 Aspekty řízení kontinuity činností organizace z hlediska bezp. informací	
A.17.1 Kontinuita bezpečnosti informací	
A.17.1.1 Plánování kontinuity bezpečnosti informací	**Neaplikováno**
A.17.1.2 Implementace kontinuity bezpečnost informací	**Neaplikováno**
A.17.1.3 Verifikace, přezkoumání a vyhodnocení kontinuity bezpečnosti informací	**Neaplikováno**
A.17.2 Redundance	
A.17.2.1 Dostupnost vybavení pro zpracování informací	**Neaplikováno**
A.18 Soulad s požadavky	
A.18.1 Soulad s právními a smluvními požadavky	
A.18.1.1 Identifikace odpovídající legislativy a smluvních požadavků	**Částečně**
A.18.1.2 Ochrana duševního vlastnictví	**Částečně**

A.18.1.3 Ochrana záznamů	**Částečně**
A.18.1.4 Soukromí a ochrana osobních údajů	**Částečně**
A.18.1.5 Regulace kryptografických opatření	**Částečně**
A.18.2 Přezkoumání bezpečnosti informací	
A.18.2.1 Nezávislá přezkoumání bezpečnosti informací	**Neaplikováno**
A.18.2.2 Shoda s bezpečnostními politikami a normami	**Neaplikováno**
A.18.2.3 Přezkoumání technické shody	**Neaplikováno**

2.5 Požadavky společnosti

Společnost potřebuje zabezpečit mobilní zařízení. To znamená zabezpečení přenášených dat mezi mobilním zařízením a serverem, a také obecné zabezpečení před škodlivým kódem. Zabezpečit mobilní zařízení zablokováním na dálku. Jedná se o případy, kdy se například mobilní zařízení ztratí nebo je ohrožena důvěrnost dat. Dalším požadavkem je zabezpečit pracovní stanice šifrováním, tedy konkrétně stolní počítače a notebooky. Posledním požadavkem je zavedení redundance hardwaru a dat serveru, protože je server kritický pro činnosti společnosti.

Souhrn požadavků:

- zabezpečení mobilních zařízení,
- šifrování pracovních stanic,
- redundance serverových dat a hardwaru.

2.6 Důvod zájmu společnosti o bezpečnost

Důvodem zájmu o bezpečnost je bezpečnostní incident, který se stal v roce 2017. Útočník se dostal díky neadekvátně zabezpečenému starému účtu na server společnosti. Jednalo se o nezrušený účet po bývalém zaměstnanci, který měl nastavené slabé a neadekvátní heslo a díky tomu se útočník dostal na server společnosti. Data na serveru jsou jediná a neexistuje záloha mimo server. Kdyby útočník data zničil, tak by dnes společnost pravděpodobně neexistovala. Společnost si díky tomuto incidentu uvědomila roli, jakou hraje bezpečnost v podnikání a sama podnikla kroky ke zlepšení bezpečnosti.

3 NÁVRH ŘEŠENÍ

Kapitola návrhu řešení je koncipována do několika podkapitol. První podkapitola řeší rozsah a hranice, které jsou vysvětleny v teoretických východiskách. Podkapitola analýzy rizik má v práci dva účely, analyzovat rizika a zároveň působit jako návrh pro společnost. Z podkapitoly analýzy rizik a požadavků společnosti pak vychází podkapitola návrhu bezpečnostních opatření. Další podkapitola s názvem „souhrn vzhledem k GDPR“ představuje dodatečné téma, které v této práci nelze, vzhledem k obsáhlosti, uskutečnit v plném rozsahu, ale stojí za základní zmínku. Poslední tři podkapitoly obsahují fáze implementace, ekonomické zhodnocení a přínos diplomové práce.

3.1 Rozsah a hranice

Na začátek je potřeba uvést fakt, který je zmíněn již v cílech diplomové práce. Rozsahem uplatňování ISMS v této práci není plný záběr. Z hlediska diplomové práce není možné pokrýt veškeré aspekty.

Jak již bylo uvedeno v teoretických východiscích, k rozsahu se lze stavět dvěma způsoby. Společnost nemá v nejbližší době v plánu zavedení v plném rozsahu ani certifikaci ISMS, proto je zvolen druhý způsob, při kterém je rozsah omezený na definované části. V případě této práce to jsou vybraná bezpečnostní opatření na zvládání zjištěných rizik a požadavků společnosti.

3.2 Analýza rizik

Důležité je zmínit, že analýza rizik zde působí zároveň jako návrh k politice řízení rizik, která je řešena v kategorii opatření A.5.1.1 kapitoly 3.3. Z toho důvodu je analýza rizik umístěna v návrhové části práce.

Jako první v pořadí je v analýze rizik identifikace aktiv a hodnocení aktiv. Dále jsou identifikovány hrozby a zranitelnost. Nakonec je vypracována matice úrovní rizik a zhodnocení analýzy rizik.

3.2.1 Identifikace a hodnocení aktiv

Nejprve je zapotřebí identifikovat aktiva. Aktiva lze dělit podle několika způsobů a pro účely této práce je zvoleno klasické dělení do čtyř skupin – informační, hardwarová (HW), softwarová (SW) aktiva a služby. Běžně se u identifikace aktiv provádí i identifikace vlastníka aktiv, nicméně vzhledem k veřejné povaze diplomové práce tyto informace zveřejněny nebudou.

K ohodnocení aktiv je využito klasifikační schéma upravené dle [1]. Jednotlivá aktiva jsou hodnocena dle nákladů vzniklých v důsledku porušení atributů důvěrnosti, integrity a dostupnosti (CIA).

Tabulka 4: Klasifikační schéma pro aktiva
Zdroj: Vlastní zpracování dle [1]

Klasifikační kritérium pro aktiva	Klasifikační stupeň
Žádný dopad	1
Zanedbatelný dopad	2
Potíže a finanční ztráty	3
Vážné potíže a velké ztráty	4
Existenční potíže	5

K výpočtu hodnoty aktiva je použit součtový algoritmus:

$$Hodnota\ aktiva = \frac{(\text{Důvěrnost} + \text{Integrita} + \text{Dostupnost})}{3} \quad [1]$$

Hodnotící škála jednotlivých atributů (důvěrnost, integrita, dostupnost) je stejná jako v tabulce 4, tedy 1 až 5.

Tabulka 5: Identifikovaná a ohodnocená aktiva
Zdroj: Vlastní zpracování

Typ	Aktivum (A)	Zdroj	C	I	A	H
INFORMAČNÍ AKTIVA	Data o zákaznících	*e-shop, CRM*	5	5	5	5
	Data o zaměstnancích	*server*	5	4	3	4
	Interní data	*server, exchange server*	5	5	5	5
	Zálohy dat	*server*	5	5	5	5
		cloud	5	5	3	4
		IP kamera	3	2	1	2
HARDWAROVÁ AKTIVA	Server		5	5	5	5
	Pracovní stanice		3	2	3	3
	Notebooky		3	2	3	3
	Mobilní zařízení		3	3	3	3
	Pasivní síťové prvky	*kabeláž, zásuvky, ...*	5	5	5	5
	Aktivní síťové prvky	*switch, router*	5	5	5	5
	Firewall		5	5	5	5
SOFTWAROVÁ AKTIVA	Operační systémy	*server*	5	5	5	5
		prac. stanice, noteboky	3	3	3	3
	Exchange server		5	5	5	5
	Software měřícího zařízení		4	4	1	3
	Účetní software +CRM		5	5	5	5
	Software IP kamer		3	3	1	2
	VPN klient		4	4	4	4
	Antivirový software		5	5	5	5
	Spam filter	*server*	2	3	1	2
SLUŽBY	Internetové připojení	*sídlo*	4	4	4	4
		sklad Morava	4	4	4	4
		sklad Čechy	4	3	3	3
		kancelář	4	4	4	4
		mobilní zařízení	4	4	4	4
	Elektrická energie	*Sídlo*	4	4	5	4
		Sklad Morava	4	4	3	4
		Sklad Čechy	4	4	3	4
		Kancelář	4	4	3	4
	Doménové služby	*server*	5	1	1	2
	E-shop	*poskytovatel*	4	4	4	4
	WWW	*poskytovatel*	2	1	2	2
	Dohled výměníkové stanice	*software*	3	3	3	3
	Služba záloh	*synology*	5	4	4	4
	VPN připojení	*VPN klient*	4	4	4	4
	Služba IP kamer		3	2	1	2

Vzhledem k velikosti tabulky byly upraveny názvy atributů na anglické zkratky C – důvěrnost, I – integrita, A – dostupnost, aby bylo možné tabulku prezentovat v plném rozsahu. H – hodnota aktiva na základě klasifikačního stupně tabulky 4.

Z identifikace a ohodnocení aktiv vyplývá, že nejhodnotnější aktiva se pohybují okolo serveru. Data o zákaznících a zaměstnancích a interní data se nachází na serveru, pasivní a aktivní síťové prvky umožňují provoz dat mezi zařízením a serverem (spravován externě) a stejně tak Microsoft Exchange Server je nainstalován na serveru. Účetní program s CRM taktéž, konkrétněji tedy na virtuálním serveru.

Identifikace a ohodnocení aktiv byla provedena s příslušnou osobou ze společnosti.

3.2.2 Identifikace hrozeb a zranitelnosti

Jako první jsou identifikovány hrozby, které mají potenciál poškození aktiv společnosti. Dále je hrozbám přiřazena pravděpodobnost výskytu s příkladem zranitelnosti. Ke snadnějšímu pochopení a přehlednosti je zařazen i o jaký typ hrozby se jedná. Výstupem identifikace je seznam hrozeb s pravděpodobností výskytu a příkladem zranitelnosti.

Pravděpodobnost vzniku hrozby je hodnocena dle následujícího schématu:

Tabulka 6: Klasifikační schéma pravděpodobnosti vzniku hrozeb
Zdroj: Vlastní zpracování dle [1]

Klasifikační kritérium pravděpodobnosti	Klasifikační stupeň
Nahodilá	1
Nepravděpodobná	2
Pravděpodobná	3
Velmi pravděpodobná	4
Trvalá	5

Na základě normy ČSN ISO/IEC 27005 [22] jsou identifikovány následující hrozby:

Tabulka 7: Identifikované hrozby
Zdroj: Vlastní zpracování

Typ	Hrozba (T)
FYZICKÉ POŠKOZENÍ	Požár
	Poškození vodou
	Zničení zařízení nebo médií
PŘÍRODNÍ UDÁLOST	Povodeň
ZTRÁTA ZÁKL. SLUŽEB	Přerušení dodávky elektřiny
	Selhání telekomunikačních zařízení
OHROŽENÍ INFORMACÍ	Vzdálená špionáž
	Odposlech
	Krádež médií nebo dokumentů
	Krádež zařízení
	Vyzrazení
	Falšování pomocí aplikačního programového vybavení
	Odhalení pozice
TECHNICKÉ SELHÁNÍ	Selhání zařízení
	Chybné fungování zařízení
	Chybné fungování aplikačního programového vybavení
	Chyba údržby
NEOPRÁVNĚNÉ ČINNOSTI	Neoprávněné použití zařízení
	Podvodné kopírování aplikačního programového zařízení
	Použití padělaného nebo zkopírovaného prog. vybavení
	Poškození dat
	Nezákonné zpracování dat
OHROŽENÍ FUNKČNOSTI	Chyba používání
	Zneužití oprávnění
	Odepření činnosti
	Nedostatek personálu

Tabulka 8: Identifikované hrozby s pravděpodobností a příkladem zranitelnosti
Zdroj: Vlastní zpracování

Hrozba (T)	P	Příklad zranitelnosti
Požár	2	Zacházení s hořlavinami
Poškození vodou	1	Zacházení s vodou
Zničení zařízení nebo médií	3	Nedodržení pravidelné výměny
Povodeň	1	Poloha v zátopové oblasti
Přerušení dodávky elektřiny	3	Citlivost na změny napětí
Selhání telekomunikačních zařízení	4	Komunikace prováděna výhradně online
Vzdálená špionáž	1	Nedostatečně bezpečná síťová infrastruktura
Odposlech	1	Nechráněné komunikační linky
Krádež médií nebo dokumentů	3	Nedostatečná fyzická ochrana budov, dveří atd.
Krádež zařízení	4	Nedostatečná ochrana zařízení mimo pracoviště
Vyzrazení	5	Nedostatečné postupy pro nábor pracovníků
Falšování pomocí aplikačního programového vybavení	4	Nekontrolované stahování a užívání programů
Odhalení pozice	3	Nedostatečná ochrana mobilních telefonů
Selhání zařízení	3	Nedostatky v plánech kontinuity
Chybné fungování zařízení	3	Nedostatečná údržba zařízení
Chybné fungování aplikačního programového vybavení	3	Neodladěný nebo nový program
Chyba údržby	3	Nedostatečná údržba
Neoprávněné použití zařízení	3	Nechráněné připojení do veřejné sítě
Podvodné kopírování aplikačního programového zařízení	1	Nedostatečný log management
Použití padělaného nebo zkopírovaného prog. vybavení	1	Nedostatečné postupy pro zajištění souladu se zákony na ochranu duševního vlastnictví
Poškození dat	2	Široce rozšířené programy
Nezákonné zpracování dat	1	Spuštění nepotřebných služeb
Chyba používání	3	Nedostatek povědomí o bezpečnosti
Zneužití oprávnění	4	Neodhlášení se při opuštění pracovní stanice
Odepření činnosti	3	Nedostatky ve vhodném přidělení odpovědnosti za bezpečnost informací
Nedostatek personálu	4	Nepřiměřená nebo nedbalá kontrola fyzického přístupu do budov, místností a kanceláří

Sloupec **P** v tabulce 8 představuje pravděpodobnost vzniku hrozby.

3.2.3 Matice zranitelnosti

Matice zranitelnosti představuje pravděpodobnost hrozby v závislosti na hodnotě aktiva. Zranitelnost se volí na základě odhadu slabého místa, stavu analyzované entity, v tomto případě tedy aktiva. Odhad je založen na následujícím klasifikačním schématu:

Tabulka 9: Klasifikační schéma pro zranitelnost
Zdroj: Vlastní zpracování dle [16]

Klasifikační kritérium pro zranitelnost	Klasifikační stupeň
Velmi nízká	1
Nízká	2
Střední	3
Vysoká	4
Kritická	5

Vzhledem k velikosti celé matice zranitelnosti je v textu práce uvedena pouze její část s informačními aktivy. Celá matice v plném rozsahu je k dispozici v příloze.

Tabulka 10: Matice zranitelnosti
Zdroj: Vlastní zpracování

Zranitelnost [V]		INFORMAČNÍ					
	Zdroj	*server*			*server*	*cloud*	*IP kamera*
	Aktivum	Data o zákaznících	Data o zaměstnancích	Interní data	Zálohy dat		
	A	5	4	5	5	4	2
Hrozba	**T**						
Požár	2						
Poškození vodou	1						
Zničení zařízení nebo médií	3						
Povodeň	1						
Přerušení dodávky elektřiny	3	4	4	4	2	3	2
Selhání telekomunikačních zařízení	4	4	4	4	4	3	
Vzdálená špionáž	1	4	4	4	4	4	1
Odposlech	1						
Krádež médií nebo dokumentů	3	4	2	4	1	2	1
Krádež zařízení	4						
Vyzrazení	5	3	3	4	3		
Falšování pomocí aplikačního programového vybavení	4				1	1	1
Odhalení pozice	3						
Selhání zařízení	3						
Chybné fungování zařízení	3						
Chybné fungování aplikačního programového vybavení	3						
Chyba údržby	3						
Neoprávněné použití zařízení	3						
Podvodné kopírování aplikačního programového zařízení	1						
Použití padělaného nebo zkopírovaného prog. vybavení	1						
Poškození dat	2	3	3	3	3	3	3
Nezákonné zpracování dat	1	3	3	3	3	3	3
Chyba používání	3	3	3	3	3	3	2
Zneužití oprávnění	4	3	3	3	3	3	2
Odepření činnosti	3						
Nedostatek personálu	4						

3.2.4 Matice úrovní rizik

K výpočtu úrovně rizika **R** zvolena tří parametrová metoda. Tato metoda se skládá ze tří parametrů, **A** – hodnota aktiva, **T** – pravděpodobnost hrozby a **V** – zranitelnosti aktiva. Vynásobením zmíněných parametrů vyjde úroveň rizika. Vzhledem k tomu, že všechny tři parametry mají maximální hodnotu 5, tak úroveň rizika se může pohybovat v rozmezí 0 až 125. Výpočet úrovně rizika **R**:

$$R = A \cdot T \cdot V \qquad [1]$$

Úroveň rizika se klasifikuje dle následujícího klasifikačního schématu:

Tabulka 11: Klasifikační schéma pro úroveň rizika
Zdroj: Vlastní zpracování dle [1]

Klasifikační kritérium pro úroveň rizika	Klasifikační stupeň
Bezvýznamné riziko	0-10
Akceptovatelné riziko	11-20
Nízké riziko	21-30
Nežádoucí riziko	31-60
Nepřijatelné riziko	61-125

Příklad výpočtu úrovně rizika:

Hodnota aktiva **A**:	Interní data	Hodnota 5
Pravděpodobnost hrozby **T**:	Přerušení dodávky elektřiny	Hodnota 3
Zranitelnost aktiva **V**:	Citlivost na změny napětí	Hodnota 4
Úroveň rizika **R**:	$5 \cdot 3 \cdot 4 =$ 60	

Vzhledem k velikosti celé matice úrovní rizik je v textu práce uvedena pouze její část s informačními aktivy. Celá matice v plném rozsahu je k dispozici v příloze.

Tabulka 12: Matice úrovní rizik
Zdroj: Vlastní zpracování

Úroveň rizika [R]		Zdroj	INFORMAČNÍ					
			server			*server*	*cloud*	*IP kamera*
		Aktivum	Data o zákaznících	Data o zaměstnancích	Interní data	Zálohy dat		
		A	5	4	5	5	4	2
Hrozba	**T**							
Požár	2							
Poškození vodou	1							
Zničení zařízení nebo médií	3							
Povodeň	1							
Přerušení dodávky elektřiny	3		60	48	60	30	36	12
Selhání telekomunikačních zařízení	4		80	64	80	80	48	
Vzdálená špionáž	1		20	16	20	20	16	2
Odposlech	1							
Krádež médií nebo dokumentů	3		60	24	60	15	24	6
Krádež zařízení	4							
Vyzrazení	5		75	60	100	75		
Falšování pomocí aplikačního programového vybavení	4					20	16	8
Odhalení pozice	3							
Selhání zařízení	3							
Chybné fungování zařízení	3							
Chybné fungování aplikačního programového vybavení	3							
Chyba údržby	3							
Neoprávněné použití zařízení	3							
Podvodné kopírování aplikačního programového zařízení	1							
Použití padělaného nebo zkopírovaného prog. vybavení	1							
Poškození dat	2		30	24	30	30	24	12
Nezákonné zpracování dat	1		15	12	15	15	12	6
Chyba používání	3		45	36	45	45	36	12
Zneužití oprávnění	4		60	48	60	60	48	16
Odepření činnosti	3							
Nedostatek personálu	4							

3.2.5 Zhodnocení

Následující tabulka představuje výpis všech nepřijatelných rizik:

Tabulka 13: Výpis nepřijatelných rizik
Zdroj: Vlastní zpracování

Hrozba	Úroveň rizika	Aktivum	Zdroj
Selhání telekomunikačních zařízení	80	Data o zákaznících	*server*
	64	Data o zaměstnancích	*server*
	80	Interní data	*server*
	80	Zálohy dat	*server*
	80	Internetové připojení	*sídlo*
	80		*kancelář*
	64	VPN připojení	
Odposlech	96	Internetové připojení	*sídlo*
Vyzrazení	75	Data o zákaznících	*server*
	100	Interní data	*server*
	75	Zálohy dat	*server*
Zneužití oprávnění	80	Server	
	80	Účetní software	

Na základě analýzy představuje největší riziko vyzrazení interních dat, jako třeba know-how. Jedná se o lidský faktor, který se nachází všude a nelze se mu zcela vyhnout. Je zapotřebí toto riziko snížit a kontrolovat. Obecně jsou ve společnosti data velmi cenná, což lze z analýzy dobře vidět. Data jsou převážně uložena na serveru, z čehož vyplývá, že je zapotřebí mít důkladně zabezpečený server. Jelikož je server spravován externě data centrem, lze konstatovat, že jeho zabezpečení je mnohem lepší, než kdyby server společnost spravovala sama. Z toho důvodu je důležité se zaměřit především na koncové zařízení a komunikaci mezi serverem a koncovým zařízením.

Z pohledu internetového připojení jsou data náchylná z toho důvodu, že se nachází mimo prostory společnosti a musí se k nim vzdáleně připojovat. Bez internetového připojení toho tedy společnost příliš neudělá. Z toho důvodu je dále důležité VPN připojení, které zajišťuje bezpečnější komunikaci se serverem a bez internetového připojení či elektrické energie nebude fungovat.

Zneužití oprávnění může vzniknout náhodně nebo úmyslně, a to i na serveru u data centra. Dále je poměrně vysoké riziko při zneužití oprávnění u účetního softwaru, ve kterém se také může napáchat velmi škod.

Vzhledem k velkému množství rizik s hodnotou 60 a faktu, že je dělí pouhý jeden „bod“ od kategorie nepřijatelná rizika, je důležité uvést i tato nežádoucí rizika.

Tabulka 14: Výpis nežádoucích rizik
Zdroj: Vlastní zpracování

Hrozba	Úroveň rizika	Aktivum	Zdroj
Přerušení dodávky elektřiny	60	Elektrická energie	*sídlo*
	60	Data o zákaznících	*server*
	60	Interní data	*server*
	60	Pasivní síťové prvky	
	60	Aktivní síťové prvky	
	60	Firewall	
Krádež médií nebo dokumentů	60	Data o zákaznících	*server*
	60	Interní data	*server*
Krádež zařízení	60	Mobilní zařízení	
	60	Aktivní síťové prvky	
	60	Firewall	
Vyzrazení	60	Data o zaměstnancích	*server*
Chybné fungování aplikačního programového vybavení	60	Účetní software	
Chyba používání	60	Pasivní síťové prvky	
	60	Účetní program	
	60	Antivirový software	
Zneužití oprávnění	60	Data o zákaznících	*server*
	60	Interní data	*server*
	60	Zálohy dat	*server*
	60	Aktivní síťové prvky	
	60	Firewall	
	60	Exchange server	
	60	Antivirový program	
Odepření činnosti	60	VPN klient	
	60	Antivirový program	
	60	VPN připojení	
Nedostatek personálu	60	Účetní software	

Při zaměření na nežádoucí rizika lze pozorovat, že nejvíce vysokých hodnot se pohybuje u hrozeb přerušení dodávky elektřiny, selhání telekomunikačního zařízení, krádež zařízení, chyba používání, zneužití zařízení a odepření činnosti. Z toho tři hrozby se zároveň objevují u rizik nepřijatelných. Hrozeb s velkou hodnotou je samozřejmě více, ale nejedná se o příliš velké zastoupení. Jednotlivé hrozby s menším zastoupením aktiv jsou pak tedy například krádež zařízení nebo nedostatek personálu obsluhující účetní software, protože práce s takovýmto softwarem vyžaduje od uživatele konkrétní znalosti, které ne každý má.

3.2.6 Výběr bezpečnostních opatření

Na základě požadavků společnosti a provedené analýze rizik je z normy ISO/IEC 27001 vybráno 25 bezpečnostních opatření, které mají zacílit na požadavky a rizika zmíněná v předešlé kapitole. Vzhledem k většímu počtu a přehlednosti jsou opatření uvedena tabulkově.

Tabulka 15: Vybraná bezpečnostní opatření
Zdroj: Vlastní zpracování

A.5 Politiky bezpečnosti informací
A.5.1 Směřování bezpečnosti informací vedením organizace
A.5.1.1 Politiky pro bezpečnost informací
A.5.1.2 Přezkoumání politik pro bezpečnost informací
A.6 Organizace bezpečnosti informací
A.6.1 Interní organizace
A.6.1.1 Role a odpovědnosti bezpečnosti informací
A.6.1.3 Kontakt s autoritami
A.6.1.4 Kontakt se zvláštními zájmovými skupinami
A.6.2 Mobilní zařízení a práce na dálku
A.6.2.1 Politika mobilních zařízení
A.6.2.2 Práce na dálku
A.8 Řízení aktiv
A.8.1 Odpovědnost za aktiva
A.8.1.1 Seznam aktiv
A.8.1.2 Vlastnictví aktiv
A.8.1.3 Přípustné použití aktiv
A.8.2 Klasifikace informací
A.8.2.1 Klasifikace informací
A.8.2.2 Označování informací
A.9 Řízení přístupu

A.9.1 Požadavky organizace na řízení přístupu
A.9.1.1 Politika řízení přístupu
A.9.1.2 Přístup k sítím a síťovým službám
A.9.2 Řízení přístupu uživatelů
A.9.2.1 Registrace a zrušení registrace uživatele
A.10 Kryptografie
A.10.1 Kryptografická opatření
A.10.1.1 Politika pro použití kryptografických opatření
A.10.1.2 Správa klíčů
A.11 Fyzická bezpečnost a bezpečnost prostředí
A.11.2 Zařízeni
A.11.2.2 Podpůrné služby
A.11.2.4 Údržba zařízení
A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru
A.12 Bezpečnost provozu
A.12.2 Ochrana proti malwaru
A.12.2.1 Opatření proti malwaru
A.12.3 Zálohování
A.12.3.1 Zálohování informací
A.13 Bezpečnost komunikací
A.13.1 Správa bezpečnosti sítě
A.13.1.1 Opatření v sítích
A.13.2 Přenos informací
A.13.2.1 Politiky a postupy při přenosu informací
A.17 Aspekty řízení kontinuity činností organizace z hlediska bezp. informací
A.17.2 Redundance
A.17.2.1 Dostupnost vybavení pro zpracování informací

3.3 Návrh zavedení bezpečnostních opatření

Kapitola řeší návrhy bezpečnostních opatření, které jsou zmíněny v kapitole 3.2.6. Jako poslední je uveden souhrn mapující jednotlivá opatření k rizikům z analýzy rizik. U každé kategorie opatření je uveden cíl dle normy ISO/IEC 27002, kterého má být dosaženo. Pro jednotlivá opatření je pak uvedeno specifické prohlášení o opatření, které má plnit cíle. Kvůli odlišení kapitol diplomové práce od kategorií opatření, je u nadpisů opatření použito proložení.

3.3.1 Politiky bezpečnosti informací – A.5

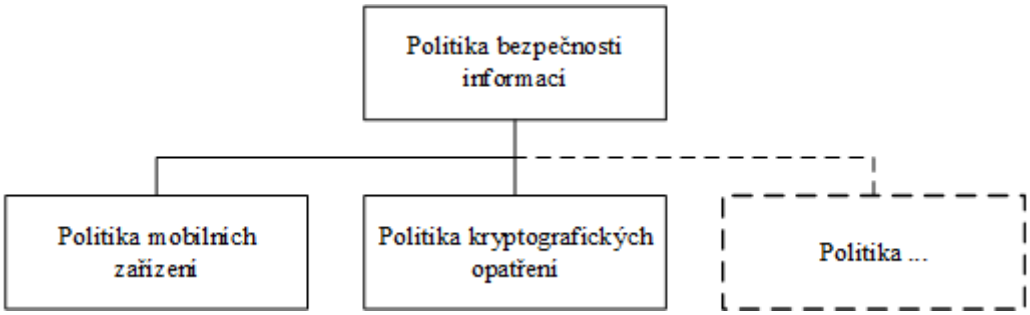
Podkapitola věnující se vybraným opatřením kategorie A.5 z norem řady ISO/IEC 27000.

A.5.1 Pokyny managementu organizace k bezpečnosti informací

***Cíl*: „Poskytnout pokyny a podporu ze strany managementu pro bezpečnost informací v souladu s požadavky podnikatelské činnosti organizace a příslušnými zákony a předpisy“ [23, s. 10].**

A.5.1.1 Politiky pro bezpečnost informací

Ve společnosti již politika bezpečnosti informací existuje, ale musí projít revizi. Politiku je potřeba rozšířit o oblasti působnosti jako řízení rizik, mobilní zařízení apod., které aktuální politika neřeší. Prvním návrhem je tedy vytvořit novou organizační strukturu politik, viz obrázek 11. Hlavní politikou bude politika bezpečnosti informací, která bude nejvyšší úrovní a bude zahrnovat smluvní a legislativní požadavky, způsob řešení a organizace podřízených politik, definování bezpečnosti informací, postupů a cílů. Poté přiřadit odpovědnosti k řízení bezpečnosti informací vztahující se k definovaným cílům. Vodítkem pro rozšíření oblastí politik může být analýza oblastí z analytické části práce, která udává konkrétní přehled o tom, co lze nově zahrnout a co již ve společnosti existuje. Oblasti, které politika již řeší jako například přenos informací je zapotřebí rozšířit a transformovat do nové podoby samostatné politiky. Zrevidovanou politiku je poté zapotřebí zveřejnit pro všechny zaměstnance a zainteresované strany.



Obrázek 11: Návrh organizace politik
Zdroj: Vlastní zpracování

Návrh samostatných oblastí politik:

- Mobilní zařízení
- Klasifikace informací
- Řízení rizik
- Řízení přístupu
- Kryptografická opatření
- Zálohování
- Ochrana proti malwaru
- Přenos informací

Politika řízení rizik

K řízení rizik je zapotřebí přistupovat jako k nikdy nekončícímu cyklu. Politika tedy musí definovat všechny jeho procesy:

- Stanovení kontextu
- Analýza rizik
- Vyhodnocení rizik
- Zvládání rizik [1]

V kontextu musí politika definovat role a odpovědnosti v rámci procesu, a kritéria pro analýzu, vyhodnocení a zvládání rizik. Analýzu rizik řeší tato práce a slouží zároveň jako podpora pro vytvoření politiky řízení rizik. V rámci analýzy rizik jsou již tedy vypracována následující kritéria:

- *Identifikace aktiv* – informační, softwarová, hardwarová a služby
- *Ohodnocení aktiv* – důvěrnost, integrita a dostupnost
- *Identifikace hrozeb a zranitelností* – příloha C a D ISO/IEC 27005
- *Ohodnocení hrozeb* – stupnice pravděpodobnosti vzniku hrozby
- *Ohodnocení zranitelnosti* – stupnice zranitelnosti aktiv

A.5.1.2 Přezkoumání politik pro bezpečnost informací

Politiky budou přezkoumávány jednou ročně odpovědnou osobou definovanou na základě hlavní politiky bezpečnosti informací. Cílem přezkoumání je posoudit aktuálnost, vhodnost a efektivnost politiky. Zrevidované politiky je zapotřebí schválit vedením.

3.3.2 Organizace bezpečnosti informací – A.6

Podkapitola organizace bezpečnosti informací se věnuje opatřením z kategorie A.6.

A.6.1 Interní organizace

***Cíl*:** „Ustanovit řídící rámec pro zahájení a řízení implementace a provozu bezpečnosti informací v rámci organizace“ [23, s. 11].

A.6.1.1 Role a odpovědnosti bezpečnosti informací

Zavést role a odpovědnosti bezpečnosti v souladu s pokyny politiky bezpečností informací.

- Ustanovit roli tzv. manažera bezpečnosti s úkolem celkové odpovědnosti za implementaci a rozvoj bezpečnosti informací.
    - Tato role je odpovědná za formulace politik, jejich přezkoumání, proces řízení rizik a ohlašovací i oznamovací povinnost v případě narušení bezpečnosti osobních údajů.
- Určit vlastníky aktiv na základě identifikovaných aktiv z analýzy rizik, kteří jsou zodpovědní za dodržování bezpečnosti v rámci svěřených aktiv a jejich odpovědnosti
- Ustanovit úrovně oprávnění

Jednotlivé role s odpovědností za bezpečnost informací mohou delegovat úkoly s bezpečnostním zaměřením na jiné osoby, nicméně jejich odpovědnost za daný úkol jim zůstává.

A.6.1.3 Kontakt s autoritami

Zavést formát a postup, kterými se manažer bezpečnosti bude řídit při ohlašovací činnosti v případě narušení bezpečnosti osobních údajů. Vzhledem k nařízení GDPR bude od 25. května ohlášení povinnou činností.

Ohlašovací povinnost - GDPR

Kdy: Při narušení bezpečnosti osobních údajů.

Kdo: Manažer bezpečnosti.

Komu: Dozorovému orgánu České republiky.

Limit: Bez zbytečných odkladů, nejlépe do 72 hodin od narušení.

Poznámka: V případě nedodržení limitu 72 hodin je nutné k ohlášení uvést důvod.

Minimální obsah hlášení:

- Popis povahy narušení bezpečnosti osobních údajů.
- Přibližný počet dotčených subjektů a přibližný počet dotčených osobních údajů.
- Kontaktní údaje na odpovědnou osobu v případě nutnosti dalších informací.
- Popis možných důsledků.
- Popis opatření, která byla zavedena či navržena za účelem vyřešení daného narušení bezpečnosti osobních údajů a případně popis případných opatření ke zmírnění dopadu narušení [20].

A.6.1.4 Kontakt se zvláštními zájmovými skupinami

Zavést formát a postup, kterými se manažer bezpečnosti bude řídit při oznamovací činnosti v případě narušení bezpečnosti osobních údajů. Vzhledem k nařízení GDPR bude od 25. května oznámení povinnou činností.

Oznamovací povinnost - GDPR

Kdy: Při narušení bezpečnosti osobních údajů (vyjma případů uvedených ve 3. odstavci článku 34 nařízení Evropského parlamentu a Rady (EU) 2016/679).

Kdo: Manažer bezpečnosti.

Komu: Dotčený subjekt údajů.

Limit: Bez zbytečných odkladů.

Minimální obsah oznámení:

- Popis povahy narušení bezpečnosti osobních údajů (za pomocí jasných a jednoduchých jazykových prostředků).
- Kontaktní údaje na odpovědnou osobu v případě nutnosti dalších informací.
- Popis možných důsledků.
- Popis opatření, která byla zavedena či navržena za účelem vyřešení daného narušení bezpečnosti osobních údajů a případně popis případných opatření ke zmírnění dopadu narušení [20].

A.6.2 Mobilní zařízení

Cíl: „Zajistit bezpečnost práce na dálku a bezpečnost použití mobilních zařízení“ [23, s. 13].

A.6.2.1 Politika mobilních zařízení

Společnost využívá dva typy mobilních zařízení - telefony a tablety.

Registrace: Všechna mobilní zařízení společnosti musí být zaregistrována mezi aktiva společnosti a musí mít přiřazeného vlastníka.

Používání mobilních zařízení: Všechna zařízení používaná k práci musí být vlastněna společností. Do sítě společnosti se nesmí zaměstnanci připojovat z vlastních zařízení používaných pro osobní účely a stejně tak s takovými zařízeními provozovat pracovní úkony. Je zakázáno připojování do sítí na veřejných místech. Zaměstnanci nesmí sami od sebe odinstalovat aplikace, upravovat vnitřní nastavení ani oprávnění v mobilních zařízeních.

Fyzická ochrana: Zařízení by nikdy nemělo zůstat bez dozoru, a to ani v prostorách společnosti. V případech, kdy je to možné, by měla být zařízení uzamčena.

Omezení instalace aplikací: Je nutné v mobilních zařízeních omezit instalaci aplikací, protože libovolná instalace aplikací může vést k narušení bezpečnosti. Instalace dodatečných aplikací musí být prověřena a schválena manažerem bezpečnosti.

Zabezpečení: Zabezpečení formou PIN kódu – samotné zařízení a zámek obrazovky. Nesmí však být oba PIN kódy shodné a musí být měněny na základě zvoleného intervalu. Pevně nastavený interval pro uzamčení obrazovky při nečinnosti. Zařízení musí být šifrováno a musí na něm fungovat aktuální antivirový program. Musí existovat možnost zablokování zařízení a výmazu dat zařízení v případě, že dojde ke ztrátě či odcizení.

Konkrétní opatření k zabezpečení mobilních zařízení je řešeno v kategorii A.12.2 ochrana proti malwaru.

A.6.2.2 Práce na dálku

Práce na dálku je v kontextu společnosti brána jako její běžné fungování, protože se musí připojovat na vzdálený server. K připojení na server je nutné využívat vždy zabezpečené

připojení VPN, s platností na pracovní stanice, notebooky i mobilní zařízení. Je zakázáno se připojovat na VPN mimo prostory společnosti, výjimku tvoří pouze nutné činnosti prováděné z mobilních zařízení mimo společnost.

3.3.3 Řízení aktiv – A.8

Podkapitola řeší opatření z kategorie A.8, odpovědnost za aktiva a klasifikace informací.

A.8.1 Odpovědnost za aktiva

Cíl: „Identifikovat aktiva organizace a definovat odpovědnosti za přiměřenou ochranu“ [23, s. 19].

A.8.1.1 Seznam aktiv

Na základě politiky řízení rizik mají být aktiva identifikována podle následující kategorizace a identifikace:

- Informační aktiva – IA00
- Hardwarová aktiva – HA00
- Softwarová aktiva – SA00
- Služby – SL00

Ke každému aktivu přiřadit identifikátor a datum zařazení do seznamu. Pravidelný interval kontroly seznamu aktiv stanoven na půl rok, nicméně aktuální změny by se měli aktualizovat bez zbytečných odkladů. Každé aktivum musí mít identifikovaného vlastníka viz A.8.1.2. Vést dodatečný seznam vyřazených aktiv s datem vyřazení, kde záznam vyřazeného aktiva udržovat minimálně po dobu dvou let.

A.8.1.2 Vlastnictví aktiv

Všechna identifikovaná aktiva musí mít přiřazeného vlastníka, který je odpovědná za správu a řízení. K přiřazení vlastníka musí dojít při vytváření aktiva nebo při převedení do organizace. Povinnosti vlastníků aktiv je zajistit:

- Inventarizaci a klasifikaci aktiv
- Správu a řízení aktiv
- Změny v seznamu při změně, výmazu či zničení aktiva

- U informačních aktiv: klasifikace a označení

Následující tabulka představuje návrh seznamu aktiv s vlastníky.

Tabulka 16: Návrh seznamu aktiv a vlastníků
Zdroj: Vlastní zpracování

ID	Aktivum	Zdroj	Datum zařazení	Vlastník
SL06	Dohled výměníkové stanice	Software	27.11.17	XY
SL07	….	..	..	..

A.8.1.3 Přípustné použití aktiv

Je nutné vést identifikovaná a dokumentovaná pravidla k přípustnému využívání aktiv. Tato pravidla musí platit jak pro zaměstnance, tak i na zainteresované strany, které mají určitý přístup k aktivům. Používání aktiv je řešeno politikami společnosti, a proto musí být všem zainteresovaným stranám zveřejněny, alespoň v dostatečné formě zajišťující bezpečnost informací společností a aktiv.

A.8.2 Klasifikace informací

Cíl: „Zajistit, aby informace získala odpovídající úroveň ochrany v souladu s jejím významem pro organizaci“ [23, s. 21].

A.8.2.1 Klasifikace informací

Klasifikace informací je navržena na základě běžného schématu pro komerční sféru. Vzhledem k nařízení GDPR je však kategorie „citlivé“ přejmenována na „interní“. Za klasifikaci aktiv jsou odpovědni vlastníci.

Klasifikační schéma informací:

Tabulka 17: Klasifikace informací
Zdroj: Vlastní zpracování dle [1]

Klasifikace	Dopad	Příklad
Důvěrné	Zničující dopad na společnost	Know-how
Soukromé	Negativní dopad na společnost	Osobní údaje
Interní	Negativní dopad na společnost	Dokumentace
Veřejné	Žádný	Poskytované služby

A.8.2.2 Označování informací

Papírové i digitální dokumenty je nutné označovat dle klasifikace a odpovědni jsou za to vlastníci aktiv. Označování na přední straně dokumentu v pravém horním rohu. Informace citlivé a důvěrné se značit musí, veřejné nikoliv. Klasifikaci i způsob označování uveřejnit zaměstnancům i zainteresovaným stranám.

3.3.4 Řízení přístupu – A.9

Kategorie opatření A.9 řeší opatření v rámci řízení přístupu.

A.9.1 Požadavky organizace na řízení přístupu

Cíl: „Omezit přístup k informacím a k vybavení pro zpracování informací“ [23, s. 24].

A.9.1.1 Politika řízení přístupu

Společnost má dobře navrženou strukturu skupin a přidělených oprávnění k informacím v rámci Active Directory na základě minimálního oprávnění. Nicméně je nutné vzít v úvahu klasifikaci informací z A.8.2.1 srovnat, zdali bude vyhovovat nadále. Pro fyzický přístup platí to stejné, společnost funguje na určitém řízení přístupů, ale nemá dokumentovány pokyny ani postupy. Tyto existující pokyny a postupy je nutné sepsat do politiky. Zároveň je třeba zavést pravidlo: „Co není povoleno, je zakázáno“. Definovat postupy při registraci a zrušení uživatele a definovat interval přezkoumávání přístupových práv, doporučeno jednou za čtvrt roku.

A.9.1.2 Přístup k sítím a síťovým službám

Přístup do sítě umožnit pouze autorizovaným osobám s autorizovaným zařízením. Jak bylo zmíněno v politice mobilních zařízení, do sítě společnosti se nesmí připojovat zařízení, které není ve společnosti registrováno.

Řízení přístupu na server je aktuálně bezpečně řešeno pouze na pracovních stanicích a noteboocích pomocí autentizačního certifikátu. Tento certifikát funguje pouze na zařízeních s operačním systémem Windows. Na server je tedy doporučeno implementovat řešení RADIUS server, který je schopen řešit přístup na server i z pohledu mobilních zařízení.

A.9.2 Řízení přístupu uživatelů

Cíl: „Zajistit oprávněný přístup uživatelů a zabránit neoprávněnému přístupu k systémům a službám“ [23, s. 25].

A.9.2.1 Registrace a zrušení registrace uživatele

Přidělování jedinečného identifikátoru uživatelům a aplikacím existuje. Nové uživatele registrovat při nástupu do práce a zrušení uživatelů provádět bez zbytečných odkladů při ukončení pracovního poměru. Přístupová práva novým uživatelům nastavit dle jejich pozice ve fungující struktuře AD. Přístupová práva rušit bez zbytečných odkladů, když dojde k ukončení důvodu, pro který byly přiděleny. Nepovolovat sdílené identifikátory. V případě, že by společnost v budoucnu potřebovala použít sdílené identifikátory kvůli provozním či organizačním důvodům, je nutné jejich použití schválit manažerem bezpečnosti a dokumentovat.

3.3.5 Kryptografie – A.10

Podkapitola řeší kategorii kryptografických opatření A.10 z norem řady 27000.

A.10.1 Kryptografická opatření

Cíl: „Zajistit správné a efektivní využití kryptografie na ochranu důvěrnosti, autenticity a/nebo integrity informací“ [23, s. 31].

A.10.1.1 Politika použití kryptografických opatření

Jedním z požadavků společnosti je šifrování pracovních stanic. Společnost by tedy měla zároveň vypracovat politiku použití kryptografických opatření. Vzhledem k analýze rizik je třeba se rozhodnout o požadované úrovni ochrany s ohledem na typ, sílu a kvalitu algoritmu. Je nutné kryptografická opatření zahrnout jak na pracovní stanice, notebooky tak i mobilní zařízení. Za politiku a správu klíčů musí být odpovědný manažer bezpečnosti.

A.10.1.2 Správa klíčů

Jako kryptografické opatření na úrovni pracovních stanic, notebooků a mobilních zařízení je zvoleno následující řešení - **ESET Endpoint Encryption – Pro Edition**

Řešení nabízí následující:

Tabulka 18: Vlastnosti ESET Endpoint Security - Pro Edition
Zdroj: Vlastní zpracování dle [26]

Pracovní stanice, notebooky		Mobilní zařízení	
Šifrování disku	✓	Šifrování souborů	✓
Šifrování výměnných médií	✓	Šifrování e-mailů	✓
„Go“ přenosné šifrování	✓	Šifrování textu a schránek	✓
Šifrování souborů a složek	✓	Šifrování pomocí hesel	✓
Šifrování e-mailu	✓	Šifrování pomocí šifrovacích klíčů	✓
Šifrování textu a schránek	✓		
Virtuální disky a archiv	✓		
Kompatibilita s centrální správou	✓		

Šifrování disku

- Umožňuje zašifrovat definované disky a oddíly.
- Zašifrování i správa na dálku.
- Transparentní zabezpečení za použití AES 256 šifrování.
- Obnovení uživatelského hesla na dálku.
- Kontrola kompatibility před zašifrováním.

Šifrování výměnných médií

- Kompatibilní se všemi flash disky, CD i DVD.

Šifrování souborů a složek

- Zašifruje vybrané soubory a složky.
- Okamžité zašifrování.

Šifrování e-mailů

- Mail může přečíst pouze příjemce se stejným klíčem.
- Podpora všech e-mailových klientů
- Transparentní šifrování zpráv.

Vzdálená správa:

- Nezávislé na Active Directory [26].

- Spravuje všechny uživatele a stanice se standardním připojením.
- Na úrovni správy, vytvoření a odstranění uživatelů.

Správa šifrovacích klíčů:

- Umožňuje přidat nebo odstranit jeden nebo všechny šifrovacích klíčů.

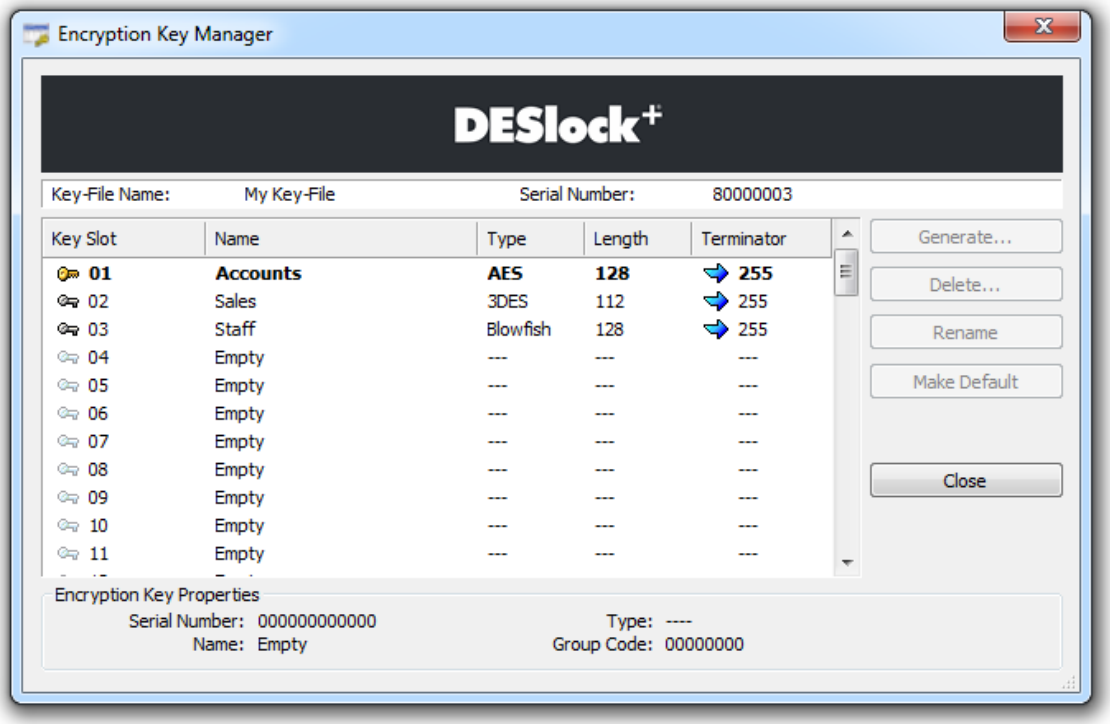
Algoritmy:

- AES 256b, 128b
- SHA 256b, SHA1 160b
- RSA 1024b
- Triple DES 112b
- Blowfish 128b

Kompatibilní systémy:

- Windows 10, 8, 8.1, 7, Vista, XP (SP3), Server 2003-2012
- iOs [26]

Obrázek 12 vyobrazuje manažera (správu) šifrovacích klíčů řešení Endpoint Encryption.



Obrázek 12: Správa šifrovacích klíčů
Zdroj: [26]

Společnost si však nepřeje šifrovat svá zařízení 256 bitovým algoritmem kvůli zpomalení, a proto bude šifrování nastaveno na 128 bitů. V případě budoucí změny lze v rámci řešení přejít na silnější algoritmus.

Jelikož řešení nepodporuje mobilní zařízení s operačním systémem Android, je nutné šifrovat zařízení skrze systémové nastavení, které využívá AES algoritmus. Před tímto šifrováním je však nutné, aby uživatel zálohoval data v mobilním zařízení. Před šifrováním musí být baterie zařízení v úrovni 80% a víc, jinak může hrozit ztráta dat v případě vybití v průběhu šifrování. Postup šifrování mobilních zařízení se systémem Android je zapotřebí uvést do politiky kryptografických opatření.

3.3.6 Fyzická bezpečnost a bezpečnost prostředí – A.11

Podkapitola řeší kategorii opatření A.11 zahrnující fyzickou bezpečnost a bezpečnost prostředí.

A.11.2 Zařízení

Cíl: „Zabránit ztrátě, poškození, odcizení nebo kompromitace aktiv a přerušení provozu organizace“ [23, s. 36].

A.11.2.2 Podpůrné služby

Vzhledem k analýze rizik je nutné vyřešit podpůrné služby na úrovni elektrické energie a internetového připojení, protože jsou pro chod společnosti zásadní.

Redundance internetového připojení

Aktuálně se nejvhodněji nabízí řešení redundantního bezdrátového připojení. Z aktuální nabídky se jako nejlepší redundantního připojení jeví „Připojení bez kabelu“ od mobilního operátora Vodafone. Datový strop by měl v případě výpadku vystačit, to stejné platí i pro limit připojených zařízení. Limit připojených zařízení je 32+1.

Tabulka 19: Parametry nabídky Připojení bez kabelu
Zdroj Vlastní zpracování dle [27]

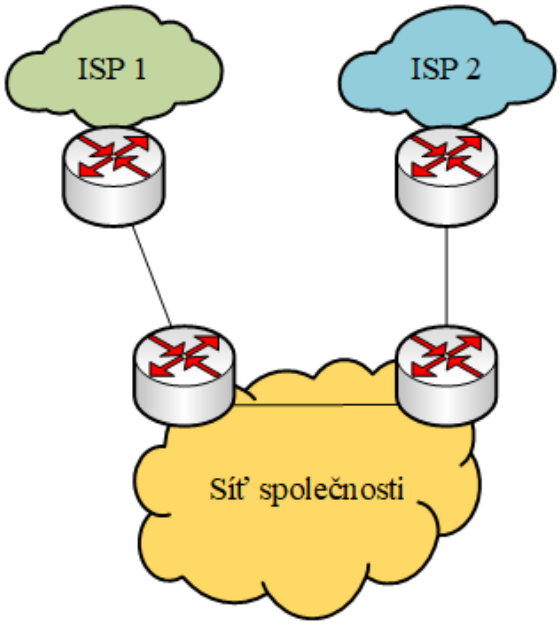
Objem dat	60 GB
Rychlost stahování	8 Mbit/s
Rychlost nahrávání	4 Mbit/s
Cena	**449 Kč/měs**

Důležité je však dodržovat všechny bezpečnostní politiky, postupy a pokyny i v případě nouzového připojení.

Případná varianta:

V případě že bude navržené řešení v budoucnu nedostatečné, lze v sídle společnosti přistoupit k redundanci na úrovni dvou přívodů od dvou poskytovatelů připojení. Role dvou poskytovatelů je v tomto řešení důležitá, protože redundance dvou přívodů od jednoho poskytovatele ztrácí při výpadku smysl.

Jedná se o tzv. „Dual Multihoming“, kdy existují dva přívody internetového připojení do sítě společnosti. U tohoto řešení je však nutné, aby směrovače společnosti podporovaly směrovací protokol BGP. V případě výpadku primárního přívodu dojde k přesměrování na sekundární (redundantní) přívod. ISP v obrázku 13 je anglická zkratka pro „Internet Service Provider“, tedy poskytovatel připojení.



Obrázek 13: Logické schéma Dual Multihoming
Zdroj: Vlastní zpracování

Zajištění elektrické energie

K zajištění elektrické energie a tím zachování provozu společnosti je vhodné použít záložní zdroje napájení UPS a vytvoření dvou UPS obvodů. Využít lze například záložní

zdroje CyberPower 1500EPFCLCD. Výstupní výkon zdroje je 900 W a při plném zatížení jsou schopny udržet připojená zařízení v chodu po dobu 3 minut. V případě 50% zatížení se doba chodu zvýší na 10 minut [28]. Vzhledem k práci přes VPN je nutné zajistit chod nejen pracovních stanic a notebooků, ale také přepínačů a směrovače a dalších zařízení, které zprostředkovávají komunikaci se serverem.

A.11.2.4 Údržba zařízení

Aby nedocházelo k selhání zařízení je zapotřebí je řádně udržovat. Je nutné vytvořit seznam zařízení s rozdělením podle hodnoty aktiva a k jednotlivým zařízením definovat jejich servisní intervaly na základě dodavatelských specifikací. Dle těchto doporučených intervalů by měla být zařízení udržována. Vést záznamy o provedených údržbách, kde by byly uvedeny případné chyby či preventivní údržby apod. Po provedení údržby je nutná kontrola funkčnosti zařízení. Za údržbu je odpovědný vlastník aktiva.

A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru

Součástí politiky bezpečnosti informací musí být i zásada prázdného stolu a prázdné obrazovky. Tyto zásady snižují riziko ztráty a vyzrazení informací a riziko neoprávněného přístupu.

Zásada prázdného stolu: Na základě klasifikace informací z kategorie opatření A.8.2.1 o Klasifikaci informací, musí být informace, jak v papírové, tak v digitální formě, zabezpečeny, resp. uzamčeny když nejsou využívány. Nesmí docházet k situacím, že dokumenty zůstanou položené na pracovním stole bez dohledu v opuštěné kanceláři. Na informace veřejné, volně dostupné se tato zásada nevztahuje.

Zásada prázdné obrazovky: V případě ponechání pracovní stanice, notebooku a mobilního zařízení bez obsluhy musí být odhlášeny a zabezpečeny před přihlášením bez autentizace uživatele. Zařízení by tedy měly mít minimálně uzamykací mechanismus obrazovky.

3.3.7 Bezpečnost provozu – A.12

Ke zvýšení zabezpečení je pro společnost zvolen set ochranných softwarových opatření od společnosti ESET. Vzhledem k rozsahu celého setu zde bude uveden pouze obsah balíku.

ESET Secure Business

Řešení obsahuje tyto oblasti ochrany:

Ochrana pracovních stanic: Antivirová a antispywarová ochrana počítačů a notebooků.

- ESET Endpoint Anivirus pro Windows

Ochrana mobilních zařízení: Komplexní zabezpečení mobilních zařízení.

- ESET Endpoint Security pro Android
- ESET Mobile Device Management pro Apple iOs

Ochrana virtualizovaného prostředí: Ochrana virtuálního stroje.

- ESET Virtualization Security pro VMware vShield

Ochrana file serverů: Antivirová a antispywarová ochrana serverových operačních systémů.

- ESET File Security pro Microsoft Windows Server

Firewall a antispam: Ochrana koncových zařízení a sítě.

- ESET Endpoint Security pro Windows

Ochrana mail serverů: Ochrana před nevyžádanou poštou a malwarem.

- ESET Mail Security pro Microsoft Exchange Server

Vzdálená správa: Nástroj pro správu stanic, serverů, mobilních zařízení.

- ESET Remote Administrator

V případě budoucích změn operačních systémů by neměl být problém, protože licence zahrnují i produkty kompatibilní s operačním systémem OS X a Linux. Uvedeny jsou pouze relevantní produkty [29].

A.12 2 Ochrana proti malwaru

Cíl: „Zajistit, že informace a vybavení pro zpracování informací jsou před malwarem chráněny“ [23, s. 42].

A.12.2.1 Opatření proti malwaru

Opatření proti škodlivému kódu jsou řešeny pro pracovní stanice, notebooky, mobilní zařízení, server i mailový server.

Ochrana pracovních stanic a notebooků

- ESET Endpoint Anivirus pro Windows

Instalace na všechny pracovní stanice a notebooky v sídle, obou skladech a kanceláři.

Ochrana koncových zařízení

- ***Antivirus a antispyware*** – Odstranění všech typů hrozeb, rootkitů, červů a spyware.
- ***Podpora virtualizace*** – Ukládání metadat kontrolovaných souborů → urychlení skenování.
- ***HIPS*** – Systém prevence průniku v rámci daného zařízení.
- ***Exploit blocker*** – Ochrana často zneužívaných aplikací (prohlížeč, MS Office, PDF čtečky atd.)
- ***Kontrola paměti*** – Monitoring škodlivých procesů.
- ***Podpora různých platforem*** – Zabránění šíření malwaru cílených na jiné systémy.

Ochrana přístupu k datům

- ***Anti-Phishing*** – Ochrana před pokusy získat citlivá data (bankovní data, hesla, údaje kreditních karet).
- ***Kontrola zařízení*** – Správa vyměnitelných médií (blokace, povolení). Tvorba pravidel podle bezpečnostní politiky.

Vzdálená správa

- Webová správa ESET Remote Administrator [29]

Ochrana mobilních zařízení

- ESET Endpoint Security pro Android
- ESET Mobile Device Management pro Apple iOs

Instalace na všechna mobilní zařízení s operačním systémem Android a iOs.

Ochrana mobilních zařízení Android

- ***Ochrana v reálném čase*** – Kontrola aplikací a komunikace kvůli malwaru.
- ***Kontrola při nabíjení*** – Možnost provedení kontroly při nabíjení nebo zamčené obrazovce.
- ***Anti-Phising*** – Ochrana před pokusy získat citlivá data (bankovní data, hesla, údaje kreditních karet).
- ***Ochrana před odinstalací*** – Odinstalace možná po zadání administrátorského hesla.
- ***Filtr volání*** – Lze nastavit osoby, které se mohou na jako jediné dané zařízení dovolat.

Bezpečnost

- Lze zablokovat integrovanou kameru.
- Určit interval výměny hesla.
- Nastavit požadavky na heslo.
- Maximální počet pokusů pro odemčení zařízení.
- Nastavit interval pro uzamčení obrazovky zařízení.

Díky nastavení politik lze monitorovat, zdali jsou zařízení stále v požadovaném stavu.

Anti-Theft

- ***Vzdálená lokalizace*** – Lokalizace telefonu, získaní GPS souřadnic.
- ***Vzdálené vymazání*** – Výmaz dat telefonu na dálku, data nelze obnovit, ale ESET zůstane.
- ***Vzdálené uzamčení*** – Vzdálené uzamčení i odemčení ztraceného telefonu.
- ***Tovární nastavení*** – Vymazání dat a převedení zařízení do továrního nastavení [29].

Obsahuje další funkce, ale zmíněné jsou nejrelevantnější.

Kontrola aplikací

Umožňuje správu a blokování nainstalovaných aplikací na daném zařízení. Možnost nastavení kontroly dle kategorií, přístupových práv a zdrojů instalace.

Správa

- ***Nastavení*** – Import/export nastavení napříč firemními zařízeními.
- ***Lokální administrace*** – Možná lokální administrace zařízení za použití administrátorského hesla.
- ***Vzdálená správa*** - Webová správa ESET Remote Administrator [29].

Ochrana serveru

- ESET File Security pro Microsoft Windows Server

Instalace na server společnosti v datovém centru. V podstatě se jedná o Endpoint Antivirus rozšířený o funkce zamřené konkrétně na zabezpečení serverů.

A.12.3 Zálohování

Cíl: „Ochrana před ztrátou dat“ [23, s. 43].

A.12.3.1 Zálohování informací

Ve společnosti se zálohují data na serveru a data na pracovních stanicích. Se zálohou serveru souvisí opatření A.17.2.1, protože v současnosti společnost zálohuje data serveru přímo na serveru. Tuto zálohu je nutné oddělit od jejího zdroje a zálohovat i na jiné místo.

Záloha pracovních stanic

Způsob zálohy je popsán v kapitole 2.2.8. Co se způsobu zálohy týče, není nutné zavádět nový způsob zálohy. Nutné jsou dva požadavky, prvním je zabudovat do smlouvy s poskytovatelem služby, aby společnost věděla, kde jsou její data na cloudu uložena. Druhým požadavkem je sepsání postupů a pokynů k zálohování.

Záloha serveru

Zálohu serveru je nutné provádět mimo hardware a prostor zdroje dat. Sepsat postupy a pokyny k zálohování. Pro zálohu serveru je doporučen open-source program Bacula. Přenos zálohy provádět skrze šifrovaný SSH tunel.

Politika

Ponechat stávající frekvenci záloh, ale definovat interval pro jejich testování. Politika by měla řešit minimálně následující:

- Jaká data a odkud se zálohují.
- Interval provádění záloh a interval testování záloh.
- Odpovědnost za zálohy a kontrolu.
- Kde se zálohy nachází.
- Zabezpečení záloh.
- Postup obnovy dat po havárii.

3.3.8 Bezpečnost komunikací – A.13

Podkapitola zaměřená na kategorii A.13 z norem řady ISO/IEC 27000.

A.13.1 Správa bezpečnosti sítě

Cíl: „Zajistit ochranu informací v sítích a jejich podpůrných prostředcích pro zpracování informací“ [24, s. 20].

A.13.1.1 Opatření v sítích

Jelikož má v místě sídla datové centrum vlastní optickou síť, je doporučeno si nechat od datového centra přivést optický přívod, například nechat si vyhradit jedno optické vlákno – jednalo by se o paralelní přenos vícero optických signálů o různých vlnových délkách po jediném vlákně. Pro takový přenos se využívá například technologie vlnový multiplex (WDM). Vzhledem k vyhrazené lince se tedy jedná o velmi bezpečnou formu přenosu.

Zavést vybrané prvky prvních dvou bezpečnostních stupňů řešení NISS.

Stupeň 0: Usnadňuje správu systému a pomáhá ke správnému způsobu zapojení [30].

- Aplikovat popisky na panely a PatchCordy.

Stupeň 1: Smyslem je zavést prostředky, které ochrání nebo blokují prvky kabeláže a konektivity [30].

- Aplikovat blokující prvky do nevyužívaných metalických a USB portů.

Obrázek 14: Blokovací prvek portu RJ45 firmy Panduit
Zdroj: [30]

- K vybraným PatchCordům aplikovat ochranu proti vytažení.

Obrázek 15: Zámek PatchCordu od firmy Panduit
Zdroj: [30]

A.13.2 Přenos informací

Cíl: „Zachovat bezpečnost informací přenášených v rámci organizace a s jakýmkoli externím subjektem“ [23, s. 50].

A.13.2.1 Politiky a postupy při přenosu informací

Společnost již politiku přenosu informací vypracovanou má, je tedy zapotřebí ji oddělit od hlavní politiky do vlastní politiky a rozšířit o nové postupy. Politika by se měla rozšířit minimálně o následující:

- Zakomponovat do stávající politiky klasifikaci informací.
- Rozšíření o přenos informací skrze mobilní zařízení.
- Použití kryptografických opatření.
- Zákaz důvěrných diskuzí na nezabezpečených komunikačních kanálech a veřejných místech.

- Pokyny a postupy k uchovávání korespondence.

3.3.9 Aspekty BCM organizace z hlediska bezpečnosti informací – A.17

Podkapitola řeší opatření ke splnění požadavku společnosti a analýzy rizik.

A.17.2 Redundance

Cíl: „Zajistit dostupnost vybavení pro zpracování informací“ [23, s. 68].

A.17.2.1 Dostupnost vybavení pro zpracování informací

Vzhledem ke kritičnosti serveru je nutné vytvořit redundanci, která bude zároveň sloužit k zálohování. Jelikož společnost nechce aktuálně pořizovat další server, tak se nabízí pronajmutí dedikovaného serveru u datového centra, pouze se musí jednat o jiné datové centrum než to, ve kterém se nachází současný server. Jednou z možností se naskýtá společnost Master Internet. Z jejich nabídky se naskýtá sestava Dell EMC PowerEdge T20 T1. Sestava obsahuje procesor Intel E3-1225v3 se čtyřmi jádry a základní frekvencí 3.2 GHZ, paměť RAM 16 GB a 2x 1Terrabytový pevný disk s rozhraním SATA za 1363 Kč. Konektivita dedikovaného serveru Blue Line 1 Gbps, která má vyhrazený 1 Gbps port a šířku pásma v České republice 1000 Mbps za 100 Kč. Operační systém Windows Server 2012 je za příplatek 560 Kč. Dohromady pronájem serveru stojí 2 023 Kč/měs.

3.3.10 Souhrn vzhledem k rizikům a požadavkům

Navržená bezpečnostní opatření dle normy ISO/IEC 27002 byla navržena na základě zhodnocení analýzy rizik a požadavků společnosti. Následující tabulky zobrazují cílení navržených opatření ke kritickým rizikům a požadavkům společnosti.

Některá opatření nejsou v tabulce uvedena, protože nejsou zvolena přímo na daná rizika, ale obecně přispívají k bezpečnosti informací ve společnosti a zároveň působí na vícero rizik, jako například politika řízení rizik.

Tabulka 20: Souhrn opatření vzhledem k vybraným rizikům
Zdroj: Vlastní zpracování

Hrozba	Aktivum	Opatření
Přerušení dodávky elektřiny	Elektrická energie	A.11.2.2
Selhání telekomunikačních zařízení	Data o zákaznících	A.11.2.2, A.11.2.4
	Data o zaměstnancích	A.11.2.2, A.11.2.4
	Interní data	A.11.2.2, A.11.2.4
	Zálohy dat	A.11.2.2, A.11.2.4
	Internetové připojení	A.11.2.2, A.11.2.4
	VPN připojení	A.11.2.2, A.11.2.4
Odposlech	Internetové připojení	A.6.2.2, A.10.1.2, A.13.1.1, A.13.2.1
Vyzrazení	Data o zákaznících	A.6.2.1, A.8.2.1, A.8.2.2, A.10.1.1, A.10.1.2, A.11.2.9 A.12.2.1, A.13.1.1, A.13.2.1
	Interní data	A.6.2.1, A.8.2.1, A.8.2.2, A.10.1.1, A.10.1.2, A.11.2.9 A.12.2.1, A.13.1.1, A.13.2.1
	Zálohy dat	A.12.3.1, A.10.1.2, A.13.2.1
Zneužití oprávnění	Server	A.9.1.1, A.9.1.2, A.9.2.1
	Účetní software	A.9.1.1, A.9.2.1

Tabulka 21: Souhrn opatření vzhledem k požadavkům
Zdroj: Vlastní zpracování

Požadavek	Opatření
Zabezpečení mobilních zařízení	A.6.2.1, A.12.2.1
Šifrování pracovních stanic	A.10.1.2
Redundance serverových dat a HW	A.12.3.1, A.17.2.1

3.4 Souhrn vzhledem k GDPR

Nařízení GDPR je obsahově velmi rozsáhlé a v kontextu této práce jej nelze zcela podchytit. Nicméně, určitá navržená opatření podporují požadavky nařízení, a proto se tato kapitola zaměřuje na pět vybraných oblastí nařízení, ve kterých se překrývají s opatřeními z normy ISO/IEC 27001 – zabezpečení, ohlašovací a oznamovací povinnost, ochrana „by design“. Pro účely kapitoly 3.5 je nadále nařízení GDPR uváděno u pouze jako „nařízení“ a norma ISO/IEC 27001 jako „norma“.

3.4.1 Zabezpečení

Nařízení řeší zabezpečení dat v článku 5 odstavci 1. bodu f) a článku 32. Stejně jako normy se i nařízení zaměřuje na rizika působící na data z pohledu důvěrnosti, integrity a dostupnosti - článek 32, odstavec 1., bod b). Z normy pokrývá oblast zabezpečení organizační opatření A.5.1.1 a to konkrétně politikou řízení rizik, s touto politikou zároveň souvisí i seznam aktiv A.8.1.1 a definovaní vlastníci aktiv A.8.1.2. Technická opatření spadající do zabezpečení nařízení jsou opatření z kategorie A.10, která zavádí politiku kryptografických opatření a zavedení samotných kryptografických opatření.

Tabulka 22: Souhrn GDPR – Zabezpečení
Zdroj: Vlastní zpracování

GDPR	ISO/IEC 27001
Článek 5, odstavec 1., bod f)	**A.5.1.1, A.8.1.1**, **A.8.1.2**, **A.10**
Článek 32, odstavec 1., body a), b), c), d)	

3.4.2 Ohlašovací a oznamovací povinnost

Z pohledu nařízení se ohlašovací a oznamovací povinnost stává povinnou a řeší jej článek 33 a 34. Z návrhů opatření k nim patří kategorie A.6.1.3 - Kontakt s autoritami a A.6.1.4 - Kontakt se zvláštními zájmovými skupinami, které byly uzpůsobeny pro nařízení. Obě opatření definují odpovědnost za danou činnost a postupy a pokyny, které musí odpovědná osoba provést za účelem splnění ohlašovací a oznamovací povinnosti v případě narušení bezpečnosti osobních údajů.

Tabulka 23: Souhrn GDPR - Ohlašovací a oznamovací povinnost
Zdroj: Vlastní zpracování

GDPR	ISO/IEC 27001
Článek 33, odstavec 1. - odstavec 3., body a), b), c), d)	**A.6.1.3**
Článek 34, odstavec 1. - odstavec 2.	**A.6.1.4**.

3.4.3 Ochrana „by design“

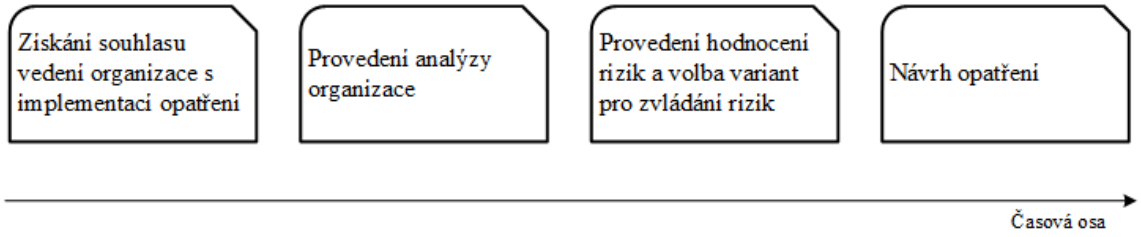
V tomto případě se u zmíněných opatření jedná spíše o podporu než o přímé splnění. Pseudonymizace nebo anonymizace stále není plněna. Jsou tedy přípravou pro určení technických opatření, které budou zcela splňovat požadavky.

Tabulka 24: Souhrn GDPR – Ochrana dat „by design“
Zdroj: Vlastní zpracování

GDPR	ISO/IEC 27001
Článek 25, odstavec 1. - odstavec 2.	**A.5.1.1, A.8.1.1**, **A.8.1.2**, **A.10**

3.5 Fáze implementace

Implementace bezpečnostních opatření byla a bude prováděna na základě doporučení zavádění ISMS z normy ISO/IEC 27003. Většina činností z fází již byla provedena a zbývá pouze činnost vytvoření finálního plánu implementace, který řeší kapitola 3.6.1. Následující obrázek představuje čtyři hlavní fáze zavádění navržených opatření z této práce. Poslední fází je pak již samotná implementace.



Obrázek 16: Fáze zavádění
Zdroj: Vlastní zpracování dle [31]

Některé činnosti chronologicky nesedí na kapitoly v této práci, protože rozložení kapitol je voleno kvůli lepšímu pochopení, a aby vyhovovalo směrnici pro vypracování prací.

Tabulka 25: Fáze a činnosti zavádění
Zdroj: Vlastní zpracování

Fáze implementace	Krok	Činnost	Dokumentovaný výstup	Součástí práce
Získání souhlasu vedení organizace s implementací opatření	1	Shromáždění cílů týkajících se činností organizace	Seznam cílů týkajících se činnosti organizace	Ne
	2	Definování rozsahu	Popis rozsahu	Kapitola 3.1
	3	Získání souhlasu a závazku vedení organizace k zahájení projektu implementace		Ne
Provedení analýzy organizace	4	Definování požadavků bezpečnosti informací	Požadavky organizace týkajících se důvěrnosti, integrity a dostupnosti.	Kapitola 2.5
	5	Identifikace aktiv	Identifikace aktiv společnosti	Kapitola 3.2.1
	6	Vytvoření hodnocení bezpečnosti informací	Záznam o současném stavu.	Kapitola 2.3
Provedení hodnocení rizik a volba variant pro zvládání rizik	7	Provedení hodnocení rizik	Analýza rizik, schválená metodika	Kapitola 3.2
	8	Výběr jednotlivých bezpečnostních opatření	Dokumentované hodnocení rizik, volba opatření	Kapitola 3.2.5, 3.2.6
	9	Získání souhlasu vedení organizace s implementací		Ne
Návrh	10	Návrh organizace bezpečnosti	Politika, role a odpovědnosti	Kapitola 3.3
	11	Návrh bezpečnosti ICT a fyzické bezpečnosti	Vybraná bezpečnostní opatření	Kapitola 3.3
	12	Vytvoření finálního plánu projektu	Vedením organizace schválený plán implementace projektu	Kapitola 3.5.1

3.5.1 Plán implementace navržených opatření

Plán zavedení bezpečnostních opatření je navržen na základě logičnosti jdoucích opatření. Politika pro bezpečnost informací je hlavní politikou a vychází z ní ostatní politiky, implementace kryptografických opatření až po zavedení kryptografické politiky a další.

Opatření A.8.1.1 Seznam aktiv a A.8.1.2 Vlastníci aktiv nejsou zahrnuty, protože jsou již zpracovány.

Tabulka 26: Plán implementace navržených opatření
Zdroj: Vlastní zpracování

Opatření	Časová náročnost [hodina]
A.5.1.1 Politiky pro bezpečnost informací	12
A.6.1.1 Role a odpovědnosti bezpečnosti informací	4
A.8.1.3 Přípustné použití aktiv	3
A.8.2.1 Klasifikace informací	2
A.8.2.2 Označování informací	1
A.12.3.1 Zálohování informací	6
A.6.2.1 Politika mobilních zařízení	8
A.6.2.2 Práce na dálku	3
A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru	1
A.9.1.1 Politika řízení přístupu	6
A.9.1.2 Přístup k sítím a síťovým službám	3
A.9.2.1 Registrace a zrušení registrace uživatele	4
A.11.2.4 Údržba zařízení	7
A.11.2.2 Podpůrné služby	12
A.17.2.1 Dostupnost vybavení pro zpracování informací	12
A.12.2.1 Opatření proti malwaru	24
A.10.1.1 Politika pro použití kryptografických opatření	5
A.10.1.2 Správa klíčů	28
A.13.1.1 Opatření v sítích	10
A.13.2.1 Politiky a postupy při přenosu informací	3
A.6.1.3 Kontakt s autoritami	2
A.6.1.4 Kontakt se zvláštními zájmovými skupinami	2
A.5.1.2 Přezkoumání politik pro bezpečnost informací	5

Tabulka na další straně představuje odhad časového plánu implementace bezpečnostních opatření. Práce na implementaci si vyhrazuje pondělí až pátek s osmi hodinovou pracovní dobou. Dle časového odhadu započne implementace v pondělí 18. června a skončí v pondělí 9. července, jedná se o rozpětí 25. a 29. týdne. V 27. týdnu jsou dva státní svátky ve čtvrtek 5. července a v pátek 6. července, kdy je implementace na tyto dny pozastavena. Je doporučeno si vyhradit zbytek 29. týdne a 30. týden pro případnou časovou rezervu.

Tabulka 27: Časový plán
Zdroj: Vlastní zpracování

Opatření	Časová náročnost	25. týden					26. týden					27. týden					28. týden					29. týden				
		Po	Út	St	Čt	Pá	Po	Út	St	Čt	Pá	Po	Út	St	Čt	Pá	Po	Út	St	Čt	Pá	Po	Út	St	Čt	Pá
A.5.1.1	12	8	4																							
A.6.1.1	4		4																							
A.8.1.3	3			3																						
A.8.2.1	2			2																						
A.8.2.2	1			1																						
A.12.3.1	6			2	4																					
A.6.2.1	8				4	4																				
A.6.2.2	3					3																				
A.11.2.9	1					1																				
A.9.1.1	6						6																			
A.9.1.2	3						2	1																		
A.9.2.1	4							4																		
A.11.2.4	7							3	4																	
A.11.2.2	12								4	8																
A.17.2.1	12										8	4														
A.12.2.1	24											4	8	8			4									
A.10.1.1	5												4				4	1								
A.10.1.2	28																	7	8	8	5					
A.13.1.1	10																				3					
A.13.2.1	3																					1	2			
A.6.1.3	2																						2			
A.6.1.4	2																						2			
A.5.1.2	5																						2	3		

3.6 Ekonomické zhodnocení

Zhodnocení bere v úvahu náklady pořizovací, které se týkají nového majetku, nových služeb a náklady implementace, které berou v úvahu práci potřebnou k zavedení daných opatření. S pořizovacími náklady jsou spojené i náklady, které se vynakládají v pravidelných intervalech. Jelikož nejsou intervaly jednotné, je zvolen interval jeden rok.

Tabulka 28: Pořizovací náklady
Zdroj: Vlastní zpracování

Opatření	Název	Množství	Pořizovací náklady	Roční náklady
A.11.2.2	CyberPower 1500EPFCLCD	7 kusů	42 000 Kč	-
	Vodafone Připojení bez kabelu	1 služba	449 Kč	5 388 Kč
A.17.2.1	Dedikovaný server od Master Internet	1 služba	2 023 Kč	24 276 Kč
A.10.1.2	ESET Secure Bussines	35 licencí	37 734 Kč	26 390 Kč
A.12.2.1	ESET Endpoint Encryption	35 licencí	43 832 Kč	43 832 Kč
A.13.1.1	Panduit PSL-USBA USB type "A" block-out device	30 kusů (6x5 kusů)	3 699,8 Kč	-
	Panduit PSL-DCJB-VL Jack Module Block-out Device	50 kusů (5x10 kusů)	2 418,6 Kč	-
	Panduit PSL-DCPLX-BL RJ45 Plug Lock-In Device	20 kusů (2*10 kusů)	1 822,96 Kč	-
	Panduit S100X150VBC Popiska na kabely	100 kusů (1 balení)	1 027,7 Kč	-
	Panduit C061X030FJJ Popiska na panely	5000 kusů (1balení)	1 065,2 Kč	-
			136 072 Kč	**99 886 Kč**

Ceny v Kč s DPH.

Roční náklad 24 276 Kč na dedikovaný server od společnosti Master Internet je uvažován při měsíční frekvenci platby. V případě, kdyby společnost zvolila roční frekvenci platby, celkový ročník náklad by se snížil na výši 23 064 Kč.

Důvodem rozdílu mezi pořizovacím a ročním nákladem u ESET Secure Bussines je sleva, kterou poskytuje společnost ESET při prodloužení licencí o jeden rok. Společnost ABC má však při prodloužení licencí další dvě možnosti, a to prodloužení o dva nebo tři roky. Při prodloužení licencí o dva roky by celkový náklad byl ve výši 47 320 Kč, tzn. roční náklad vycházející na 23 660 Kč. Třetí možností je prodloužení licencí na tři roky s nákladem 64 120 Kč a ročním nákladem 21 373 Kč. Výběr možnosti prodloužení bude tedy záležet na společnosti ABC. V případě produktu ESET Endpoint Encryption

společnost ESET aktuálně neposkytuje slevu na prodloužení licence, proto se počítá s ročním nákladem jako pořizovacím. Náklady na produkty Panduit jsou převzaty z [32] a jsou přibližné, protože jsou přepočítány z amerických dolarů na české koruny. Aktuální kurz k 5.5.2018 1 $ = 21,31 Kč [33].

Tabulka 29: Náklady na implementaci
Zdroj: Vlastní zpracování

Opatření	Náklady implementace	Pořizovací náklady	Celkové náklady implementace opatření
A.5.1.1	6 000 Kč	-	6 000 Kč
A.6.1.1	2 000 Kč	-	2 000 Kč
A.8.1.3	1 500 Kč	-	1 500 Kč
A.8.2.1	1 000 Kč	-	1 000 Kč
A.8.2.2	500 Kč	-	500 Kč
A.12.3.1	3 000 Kč	-	3 000 Kč
A.6.2.1	4 000 Kč	-	4 000 Kč
A.6.2.2	1 500 Kč	-	1 500 Kč
A.11.2.9	500 Kč	-	500 Kč
A.9.1.1	3 000 Kč	-	3 000 Kč
A.9.1.2	1 500 Kč	-	1 500 Kč
A.9.2.1	2 000 Kč	-	2 000 Kč
A.11.2.4	3 500 Kč	-	3 500 Kč
A.11.2.2	6 000 Kč	42 449 Kč	48 449 Kč
A.17.2.1	6 000 Kč	2 023 Kč	8 023 Kč
A.12.2.1	12 000 Kč	37 734 Kč	49 734 Kč
A.10.1.1	2 500 Kč	-	2 500 Kč
A.10.1.2	14 000 Kč	43 832 Kč	57 832 Kč
A.13.1.1	5 000 Kč	10 034 Kč	15 034 Kč
A.13.2.1	1 500 Kč	-	1 500 Kč
A.6.1.3	1 000 Kč	-	1 000 Kč
A.6.1.4	1 000 Kč	-	1 000 Kč
A.5.1.2	2 500 Kč	-	2 500 Kč
	81 500 Kč	**136 072 Kč**	**217 572 Kč**

Náklady na implementaci jsou počítány při sazbě 500 Kč/h. Práce na zavedení všech opatření celkově vyjde na 81 500 Kč. Pořizovací náklady na všechny služby a produkty jsou vypočítány na výši 136 072 Kč. Finální suma, kterou společnost ABC zaplatí za implementaci všech bezpečnostních opatření je 217 572 Kč.

3.7 Přínos práce

Obecným přínosem práce je zvýšení bezpečnosti informací ve společnosti ABC. Navržená bezpečnostní opatření zvyšují bezpečnost v daných oblastech snížením rizik. Zároveň práce představuje základ pro řízení rizik, který by společnost měla správně uchopit a dále provozovat, aby předešla naplnění rizik.

Dalším přínosem je samozřejmě splnění požadavků, které společnost ABC zvolila. Zabezpečení mobilních zařízení je řešeno politikou mobilních zařízení a konkrétním opatření v podobě produktů ESET pro mobilní zařízení. Produkty pokrývají zabezpečení od ochrany v reálném čase po kontrolu aplikací, zároveň řeší i konkrétní požadavek společnosti o zablokování a vymazání dat na dálku. Ke splnění požadavku šifrování zařízení je zvolen opět produkt od společnosti ESET, který nabízí široké možnosti v šifrování pracovních stanic, notebooků i mobilních zařízení. Poslední požadavek o redundanci serverových dat a serveru samotného je splněn pronajmutím dedikovaného serveru, na který bude zároveň probíhat záloha dat ze zdrojového serveru.

Práce zároveň napomáhá společnosti jít naproti evropskému nařízení o ochraně údajů, které vejde v platnost 25. května 2018. Celá problematika nařízení řešena není, ale podporuje určité požadavky, které se nově stanou pro společnosti povinností. Přínosem pro společnost je i analýza udávající přehled plnění vzhledem k nařízení, která není součástí hlavního textu práce, ale je umístěna v příloze a společnost ji může použít jako pomůcku k dalším krokům vedoucím k harmonizaci s nařízením.

Přínosem je také díky jednotnosti a kompatibilitě produktů společnosti ESET centralizace správy zabezpečení. Správce dokáže spravovat zařízení napříč operačními systémy, má centralizované upozornění ze všech zařízení, dokáže vynucovat nastavené bezpečnostní politiky a mnoho dalšího.

Vzhledem k faktu, že chod serveru a důvěrnost, integrita a dostupnost jeho dat jsou pro společnost kritickými prvky, lze říci, že navržená opatření chrání společnost před velkými ztrátami až případnými existenčními potíži. Celkové náklady na implementaci jsou tedy podstatně nižší než případné ztráty při naplnění rizika.

4 ZÁVĚR

Hlavním cílem práce bylo vytvořit návrh bezpečnostních opatření, která jsou v souladu se systémem řízení bezpečnosti informací. Návrh bezpečnostních opatření byl proveden na základě analýzy současného stavu, analýzy stavu bezpečnosti ve vybraných oblastech, požadavků společnosti a analýzy rizik, která slouží zároveň jako součást návrhu politiky řízení rizik ve společnosti.

Práce zároveň definovala cíle jednotlivých hlavních kapitol. První kapitolou jsou teoretická východiska sloužící k vysvětlení základních pojmů a definic tématu práce. Vysvětleny a rozvedeny jsou hlavní pojmy, jako informační a kybernetická bezpečnost, systém řízení bezpečnosti informací, normy řady ISO/IEC 27000 a další související normy a legislativa, analýza rizik a opatření, které jsou základem tématu a následujících kapitol.

Druhá kapitola je zaměřena na analýzu současného stavu ve společnosti. Kapitola představuje základní informace o společnosti ABC a popisuje její současný stav. Dále je provedena analýza vybraných oblastí, která udává přehled bezpečnosti ve zvolených oblastech na základě pomůcky k auditu bezpečnostních opatření. Na základě této analýzy je zároveň provedeno přemostění k opatřením z normy ISO/IEC 27001, které slouží k přehledu o již aplikovaných, částečně aplikovaných nebo neaplikovaných opatřeních ze zmíněné normy. Poslední podkapitolami jsou požadavky definované společností ABC a důvod, který vedl společnost k zaměření pozornosti na bezpečnost informací.

Návrh řešení je třetí kapitolou, která začíná definováním rozsahu a hranic a následuje analýzou rizik, ze které z velké části vychází návrh bezpečnostních opatření. Bezpečnostní opatření jsou navržena dle normy ISO/IEC 27001 a pokynů z normy ISO/IEC 27002. Součástí návrhů je i souhrn srovnávající, jaká bezpečnostní opatření jsou navržena, na jaká rizika a požadavky. Následuje souhrn, který zahrnuje i evropské nařízení o ochraně dat a dává přehled o navržených bezpečnostních opatřeních. Ta napomáhají s danými požadavky ve vybraných oblastech nařízení. Součástí kapitoly jsou následně ještě fáze implementace zpřehledňující provedené činnosti a plán implementace navržených opatření. Kapitola obsahuje i ekonomické zhodnocení uvádějící náklady na pořízení nových služeb a produktů a náklady na práci potřebnou k implementaci navržených opatření. Nakonec je popsán přínos této diplomové práce společnosti.

SEZNAM POUŽITÝCH ZDROJŮ

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

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

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

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

[5] NISTIR 7298. *Glossary of Key Information Security Terms*. 2. revize. Gaithersburg: National Institute of Standards and Technology, 2013.

[6] ONDRÁK, Viktor. *Management informační bezpečnosti*. Brno, 2014.

[7] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník Kybernetické bezpečnosti - Cyber Security Glossary*. 3. aktualizované vydání. Praha: Policejní akademie ČR v Praze a Česká pobočka AFCEA pod záštitou Národního centra kybernetické bezpečnosti České republiky, Národního bezpečnostního úřadu České republiky., 2015. Dostupné také z: https://www.govcert.cz/download/aktuality/container-nodeid-665/slovnikkb-cz-en-1505.pdf

[8] SEDLÁK, Petr. *Kybernetická bezpečnost: Obecně*. Brno, 2017.

[9] NÚKIB. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. 2017 [cit. 2018-02-14]. Dostupné z: https://www.govcert.cz/

[10] *Česká agentura pro standardizaci* [online]. 2017 [cit. 2018-02-18]. Dostupné z: http://www.agentura-cas.cz/

[11] NIST SP 800-12. *An Introduction to Information Security*. 1. revize. Gaithersburg: National Institute of Standards and Technology, 2017.

[12] NIST SPECIAL PUBLICATION 800-53. *Security and Privacy Controls for Federal Information Systems and Organizations*. 4. revize. Gaithersburg: National Institute of Standards and Technology, 2013.

[13] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: *Sbírka zákonů*. 2014, částka 74. Dostupné také z: https://portal.gov.cz/app/zakony/zakon?q=181/2014

[14] Zákon č. 205/2017 Sb., 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: *Sbírka zákonů*. 2017, částka 74. Dostupné také z: https://portal.gov.cz/app/zakony/zakon?q=205/2017

[15] *Informace o změnách zákona č. 181/2014 Sb., o kybernetické bezpečnosti účinných od 1. srpna 2017*. Verze 1.0. Národní bezpečnostní úřad - Národní centrum kybernetické bezpečnosti, 2017. Dostupné také z: https://www.govcert.cz/download/legislativa/2017/Zm%C4%9Bna_z%C3%A1kona_o_kybernetick%C3%A9_bezpe%C4%8Dnosti_velk%C3%A1_novela_v4.pdf

[16] Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). In: *Sbírka zákonů*. 2014, částka 127. Dostupné také z: https://www.govcert.cz/download/kii-vis/vkb_uz.pdf

[17] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. In: *Sbírka zákonů*. 2005. Dostupné také z: https://www.nbu.cz/cs/pravni-predpisy/1089-zakon-c-4122005/

[18] *Ministerstvo průmyslu a obchodu* [online]. ©2005-2018 [cit. 2018-02-22]. Dostupné z: https://www.mpo.cz/

[19] SEDLÁK, Petr. *GDPR: v praxi*. Brno, 2017.

[20] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 ,o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů). In: *Úřední věstník*. b.r., L 119, 4.5.2016, s. 1—88. Dostupné také z: http://eur-lex.europa.eu/legal-content/cs/TXT/?uri=CELEX%3A32016R0679

[21] *GDPR recitals and articles* [online]. 2017 [cit. 2018-02-24]. Dostupné z: https://ico.org.uk/media/about-the-ico/disclosure-log/2014536/irq0680151-disclosure.pdf

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

[23] 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.

[24] 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.

[25] *POMŮCKA K AUDITU BEZPEČNOSTNÍCH OPATŘENÍ PODLE ZÁKONA O KYBERNETICKÉ BEZPEČNOSTI*. Verze 2.1. Národní centrum kybernetické bezpečnosti, 2015, 32 s. Dostupné také z: https://www.govcert.cz/download/kii-vis/container-nodeid-580/vkbchecklistfinalv21rev.pdf

[26] Šifrování od mistra: ESET Endpoint Encryption. *ESET* [online]. [cit. 2018-04-29]. Dostupné z: https://www.eset.com/cz/firmy/enterprise-sluzby/sifrovani/#c47524

[27] Připojení bez kabelu pro podnikatele - Vodafone.cz. *Vodafone.cz* [online]. [cit. 2018-04-30]. Dostupné z: https://www.vodafone.cz/podnikatele/internet/pripojeni-bez-kabelu/

[28] CyberPower. *CyberPower* [online]. [cit. 2018-04-30]. Dostupné z: https://www.cyberpower.com/mm/en/product/sku/CP1500EPFCLCD

[29] Rozšířený balíček ochrany pro firemní počítače a servery. *ESET* [online]. [cit. 2018-04-30]. Dostupné z: https://www.eset.com/cz/firmy/firemni-reseni/secure-business/

[30] JORDÁN, Vilém a Viktor ONDRÁK. *Infrastruktura komunikačních systémů II: kritické aplikace*. Vydání první. Brno: CERM, Akademické nakladatelství, 2015. ISBN 978-80-214-5240-4.

[31] ISO/IEC 27003. *Information technology - Security techniques - Information security management systems - Guidance*. 2. vydání. Švýcarsko: Mezinárodní organizace pro normalizaci, 2017.

[32] *Rexel USA: Electrical Supplies for Commercial* [online]. [cit. 2018-05-05]. Dostupné z: https://www.rexelusa.com/usr/

[33] *Kurzy.cz: Dolar, Americký dolar USD, kurzy měn* [online]. [cit. 2018-05-05]. Dostupné z: https://www.kurzy.cz/kurzy-men/nejlepsi-kurzy/USD-americky-dolar/

SEZNAM ZKRATEK

27K	Označení pro 27000 (u norem řady ISO/IEC 27000)
A	Asset, Aktivum
ABC	Fiktivní název firmy
BCM	Business Continuity Management
BI	Bezpečnost informací
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CIA	Confidentiality, Integrity, Availability
CRAMM	CCTA Risk Analysis and Management Method
CRM	Customer Relationship Management
ČAS	Česká agentura pro standardizaci
ČSN	České technické normy (původně: „Československé státní normy“)
GDPR	General Data Protection Regulation
HIPS	Host-based Intrusion Prevention System
HW	Hardware
IB	Informační bezpečnost
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IPsec	Internet Protocol Security
IS	Information System
ISMS	Information Security Management System
ISO	International Organization for Stardardization
ISP	Internet Service Provider
IT	Information Technology
ITU	International Telecommunication Union
KB	Kybernetická bezpečnost
KI	Kritická infrastruktura
LAN	Local Area Network
MSS	Management System Standards
NIS	Network and Information Security incidents
NISS	Network Infrastructure Security Solution
NIST	National Institute of Standards and Technology

NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PDCA	Plan, Do, Check, Act
PDS	Poskytovatel digitálních služeb
PZS	Provozovatel základních služeb
R	Risk, Riziko
RAID	Redundant Array of Independent Disks
SLA	Service Level Agreement
SMS	Service Management System
SW	Software
T	Threat, Hrozba
TR	Technical Report
UPS	Uninterruptible Power Supply/Source
ÚNMZ	Úřad pro technologickou normalizaci, metrologii a státní zkušebnictví
V	Vulnerability, Zranitelnost
VIS	Významný informační systém
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WDM	Wavelength-Division Multiplexing

SEZNAM OBRÁZKŮ

Obrázek 1: PDCA cyklus 15
Obrázek 2: Přiměřená bezpečnost 15
Obrázek 3: Vztah bezpečnostních úrovní 16
Obrázek 4: PDCA cyklus v ISMS 19
Obrázek 5: Vztahy norem řady ISO/IEC 27K 24
Obrázek 6: Rozlišení bezpečnostních opatření 37
Obrázek 7: Oblasti bezpečnosti informací podle ISO/IEC 27001 38
Obrázek 8: Oblasti opatření podle NIST SP 800-53 38
Obrázek 9: Propojení sítí 42
Obrázek 10: Koláčový graf procentuálního plnění požadavků 66
Obrázek 11: Návrh organizace politik 85
Obrázek 12: Správa šifrovacích klíčů 95
Obrázek 13: Logické schéma Dual Multihoming 97
Obrázek 14: Blokovací prvek portu RJ45 firmy Panduit 104
Obrázek 15: Zámek PatchCordu od firmy Panduit 104
Obrázek 16: Fáze zavádění 108

SEZNAM TABULEK

Tabulka 1: Klasifikační schéma pro hrozby....34
Tabulka 2: Klasifikační schéma pro riziko....35
Tabulka 3: Analýza oblastí převedená na opatření ISMS....66
Tabulka 4: Klasifikační schéma pro aktiva....72
Tabulka 5: Identifikovaná a ohodnocená aktiva....73
Tabulka 6: Klasifikační schéma pravděpodobnosti vzniku hrozeb....74
Tabulka 7: Identifikované hrozby....75
Tabulka 8: Identifikované hrozby s pravděpodobností a příkladem zranitelnosti....76
Tabulka 9: Klasifikační schéma pro zranitelnost....77
Tabulka 10: Matice zranitelnosti....78
Tabulka 11: Klasifikační schéma pro úroveň rizika....79
Tabulka 12: Matice úrovní rizik....80
Tabulka 13: Výpis nepřijatelných rizik....81
Tabulka 14: Výpis nežádoucích rizik....82
Tabulka 15: Vybraná bezpečnostní opatření....83
Tabulka 16: Návrh seznamu aktiv a vlastníků....91
Tabulka 17: Klasifikace informací....91
Tabulka 18: Vlastnosti ESET Endpoint Security - Pro Edition....94
Tabulka 19: Parametry nabídky Připojení bez kabelu....96
Tabulka 20: Souhrn opatření vzhledem k vybraným rizikům....106
Tabulka 21: Souhrn opatření vzhledem k požadavkům....106
Tabulka 22: Souhrn GDPR – Zabezpečení....107
Tabulka 23: Souhrn GDPR - Ohlašovací a oznamovací povinnost....107
Tabulka 24: Souhrn GDPR – Ochrana dat „by design“....108
Tabulka 25: Fáze a činnosti zavádění....109
Tabulka 26: Plán implementace navržených opatření....110
Tabulka 27: Časový plán....111
Tabulka 28: Pořizovací náklady....112
Tabulka 29: Náklady na implementaci....113

SEZNAM PŘÍLOH

Příloha 1: Analýza oblasti GDPR I
Příloha 2: Matice zranitelnosti XIII
Příloha 3: Matice rizik XIV