VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

GAP ANALÝZA SYSTÉMU ŘÍZENÍ BEZPEČNOSTI INFORMACÍ

GAP ANALYSIS OF INFORMATION SECURITY MANAGEMENT SYSTEM

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. Martin Konečný

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. Petr Sedlák

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

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

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

GAP analýza systému řízení bezpečnosti informací

Charakteristika problematiky úkolu:

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

Cíle, kterých má být dosaženo:

Cílem diplomové práce je vytvořit GAP analýzu a návrh provedení nezbytných kroků vedoucích k zavedení systému řízení bezpečnosti informací. Předpokladem pro dosažení cíle bude analýza současného stavu ISMS společnosti. Práce nebude vytvářet návrh zavedení systému bezpečnosti informací v plném rozsahu, ale zaměřuje se pouze na návrh zavedení dílčích částí.

Základní literární prameny:

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

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

DOUCEK P., L. NOVÁK, L. NEDOMOVÁ a V. SVATÁ. Řízení bezpečnosti informací. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

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

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

V Brně dne 28.2.2019

L. S.

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

Abstrakt

Diplomová práce se zaměřuje na GAP analýzu systému řízení bezpečnosti informací. Práce se skládá z teoretické, analytické a praktické části. První část pojednává o teoretických východiscích problematiky informační a kybernetické bezpečnosti. Analytická část popisuje současný stav ve zkoumané společnosti. Výstupem práce je návrh registru rizik a návrh zavedení bezpečnostních opatření. Návrh cílí na opatření vedoucí k zvýšení bezpečnosti informací ve společnosti.

Abstract

The master's thesis focuses on GAP analysis of information security management system. The thesis consists of theoretical, analytical and practical part. The first part discusses the theoretical background of the issue of information and cyber security. The analytical part describes the current condition of the researched company. The thesis's output is the draft of risk register and draft of security countermeasures implementation. The draft targets on countermeasures leading to increase information security in company.

Klíčová slova

informační bezpečnost, kybernetická bezpečnost, GAP analýza, systém řízení bezpečnosti informací, ISO/IEC 27000, analýza rizik, opatření, bezpečnostní politiky, registr rizik

Key words

Information security, cyber security, GAP analysis, information security management system, ISO/IEC 27000, risk analysis, countermeasures, security policy, risk register

Bibliografická citace

KONEČNÝ, Martin. GAP analýza systému řízení bezpečnosti informací [online]. Brno, 2019 [cit. 2019-05-09]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/119877. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Petr Sedlák.

Čestné prohlášení

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

V Brně dne 9. května 2019 .....

podpis autora

Poděkování

Tímto bych rád poděkoval vedoucímu práce Ing. Petr Sedlákovi a Ing. Martinu Konečnému za odborné vedení, vynaložený čas a cenné rady, které mi velmi pomohly při tvorbě této diplomové práce. Poděkování patří také společnosti za spolupráci a poskytnutí potřebných dat k vypracování této diplomové práce. V neposlední řadě patří poděkování všem, kteří mi byli oporou během mého studia a při vypracovávání diplomové práce.

OBSAH

ÚVOD

Téma diplomové práce se zabývá systémem řízení bezpečnosti informací, který je nedílnou součástí společností, pro které je správa informačních aktiv klíčová. Z tohoto důvodu jsou identifikována aktiva a určena rizika bezpečnosti informací, která se budou řídit. Součástí tohoto systému řízení je zavedení opatření pro jednotlivá rizika.

Vzhledem k možnostem současné doby se četnost způsobů zneužití informací a aktiv zvyšuje. Kybernetický prostor se stal novodobým bojištěm a o kybernetických hrozbách se pojednává, čím dál více. Útoky z kybernetického prostoru míří například na prvky infrastruktury (elektrárny, řídící centra, rozvodné soustavy). Cílem těchto útoků je, buď ovládnout danou infrastrukturu, nebo do nich nahrát škodlivý kód. Motivace pro útočníky jsou různé. Může jít o osobní zisk, zničení vybraného cíle, vyvolání paniky a napáchání dodatečných škod nebo prostě „jen“ chuť ukázat, že mají takové schopnosti.

Konkrétním příkladem je kybernetický útok na jadernou elektrárnu v Iránu, kdy červ „Stuxnet“ způsobil zpoždění zprovoznění elektrárny a velké finanční ztráty. Mezi další případy spadá výpadek elektrického proudu na Ukrajině, kdy skupina hackerů umístila trojského koně do jednotlivých komponent distribuční sítě a následně způsobili její poškození či ochromení – tzv. sabotáž v průmyslovém systému. S nástupem tzv. „chytrých domácností“ hrozí tyto útoky také v našich končinách. Útočník zvládne zapnout v domácnosti spotřebič, tak aby uměle navýšil spotřebu energií. Celosvětově se rozmáhají také hackerské útoky na automobily, kdy dochází ke krádeži nebo získání kontroly nad vozidlem. Vzhledem k vážnosti problematiky je třeba ji řešit. V ČR probíhají každoročně pravidelná kybernetická cvičení pod záštitou Národního centra kybernetické bezpečnosti. Tato cvičení se věnují útoku na infrastrukturu státu a stojí proti sobě tým „útočníků“ a „obránců“. Tým reprezentující ČR, patří každoročně k nejúspěšnějším na cvičením pořádaném organizací NATO – Locked Shields.

Bezpečnostní opatření na úrovni technologického zabezpečení, ale nikdy nemůže vyřešit všechna rizika. Proto je důležité dbát i na zabezpečení lidského faktoru, budování bezpečnostního povědomí a pravidelná školení.

CÍLE PRÁCE

Cílem diplomové práce je vytvořit GAP analýzu a návrh provedení nezbytných kroků vedoucích k zavedení systému řízení bezpečnosti informací. Předpokladem pro dosažení cíle bude analýza současného stavu ISMS společnosti. Práce nebude vytvářet návrh zavedení systému bezpečnosti informací v plném rozsahu, ale zaměřuje se pouze na návrh zavedení dílčích částí.

První část pojednává o teoretických východiscích práce. Tato část je zaměřena na osvětlení základních pojmů a názvosloví, nutných pro pochopení významu problematiky. Druhá část informuje o společnosti a analyzuje její současný stav z hlediska infrastruktury a bezpečnosti. Návrhová část se věnuje analýze rizik a výběru bezpečnostních opatření, přičemž vychází z informací v analytické části práce. Poslední část obsahuje závěr, ve kterém bude shrnuta diplomová práce jako celek.

1 TEORETICKÁ VÝCHODISKÁ PRÁCE

Teoretická část diplomové práce pojednává o názvoslovích a pojmech, které jsou důležité, pro pochopení problematiky. Následuje část věnována teoretickému podkladu pro oblast ISMS. Nedílnou součástí této části jsou také normy ISO/IEC 27000 a jejich následný popis. V neposlední řadě se teoretická část věnuje analýze rizik, jejich řízení a opatřením. První část je zakončena legislativou a evropským nařízením GDPR.

1.1 Názvosloví

Z hlediska četnosti výskytu odborných pojmů a názvosloví v diplomové práci, je součástí této kapitoly přehledné vysvětlení základních pojmů a definic.

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

IS – (Information System) – Informační systém

ISMS – (Information Security Management System) – Systém řízení informační bezpečnosti

IT – (Information Technology) – Informační technologie [1].

Základní pojmy

Aktivum – (Asset) – mezi aktiva řadíme všechny nehmotné a hmotné statky, které mají pro společnost hodnotu [1].

Audit – nezávislý, systematický a dokumentovaný proces pro objektivní hodnocení za pomoci předem stanovených kritérií [1].

Bezpečnostní incident – může jít o jednu nebo několik po sobě jdoucích nečekaných a nechtěných bezpečnostních událostí, které nejčastěji cílí a ohrožují informační bezpečnost a podnikatelskou činnost v organizaci [3].

Bezpečností událost – zjištění výskytu systému, služby sítě značící možné porušení zásad bezpečnosti informací, politik či selhání opatření. Může jít o doposud nezaznamenanou situaci, která může být bezpečnostně důležitá [3].

Data – slouží k naplnění informace, kterou vytváří [1]. Informace jsou uložené jako statické záznamy, odkazují na stav reality v určitém časovém okamžiku při jejich zápisu [2].

Dopad – (Impact) – škoda vzniklá v důsledku vlivu hrozby [1].

Hrozba – (Threat) – jde o událost, která narušuje bezpečnost [1].

Informace – rozsáhlý pojem, který popisuje reálné prostředí, procesy v něm probíhající a stav. Entropie (neurčitost) je rozdílem v množství informace před a po zprávě [1]. Informace je z pohledu práce považována za aktivum, které je pro společnost nezbytné k podnikání, proto musí být vhodně chráněny. Informace mohou existovat v mnoha formách: digitální (datové soubory uložené na elektronickém nebo optickém médiu), materiální (zpravidla na papíře) a v neposlední řadě také ve znalosti samotných zaměstnanců podniku [3].

Informační management – obsahuje veškeré činnosti managementu, které pojednávají o procesech zajištění, zpracování, přenosu a uložení informací [2].

Informační systém – je možno chápat jako systém s vzájemně propojenými informacemi a procesy, které pracují právě s informacemi [1]. Jedná se o metodu získávání, přenosu, uchovávání a zpracování dat od technických a lidských zdrojů společnosti, za účelem využití výstupů těchto zpracovaných dat pro uživatele informačního systému [2].

Kybernetický prostor – Vzájemně závislé sítě infrastruktur informačních systémů v globální doméně informačního prostředí. Řadíme sem například: počítačové systémy, internet, telekomunikační sítě a procesy. Účelem je vytvářet, ukládat, upravovat, vyměňovat, sdílet a extrahovat či používat a odstraňovat informace nebo je narušování fyzických zdrojů [5].

Kybernetický útok – je operací v kyberprostoru, ať už ofenzivní, nebo defenzivní, v jejímž důsledku je třeba očekávat způsobení zranění či smrti osobám, nebo poškození či zničení věcí. Například: Útok na infrastrukturu, integritu dat, krádež informací [6].

Opatření – (Countermeasure) – aktivita nebo proces, sloužící k snížení hrozeb [1].

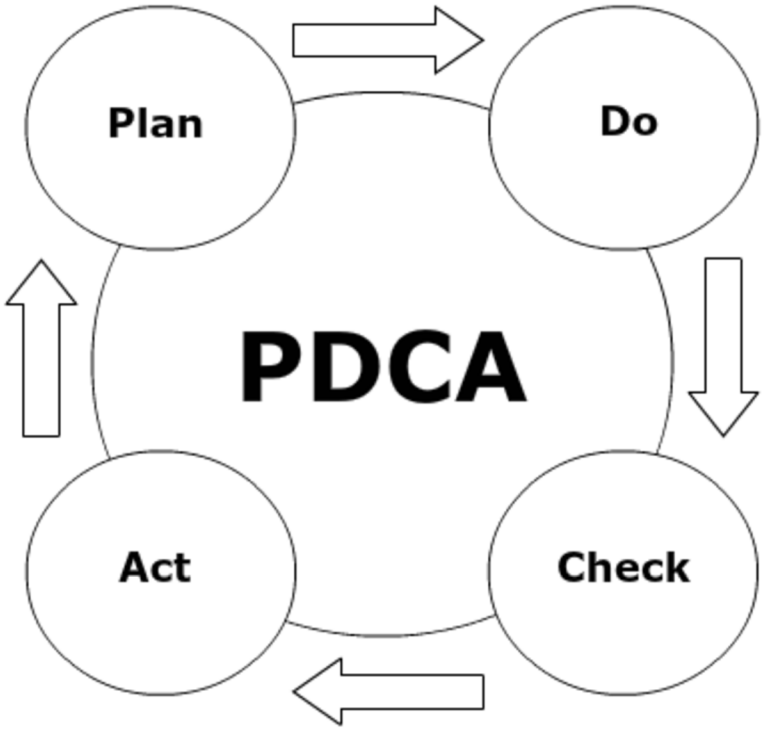
PDCA cyklus

Někdy také označován jako Demingův cyklus či životní cyklus ISMS. PDCA cyklus je manažerská metoda používaná především v managementu a to ve velkém množství oborů [4].

Slouží jako metoda zlepšování například kvality služeb, procesů, výrobků, aplikací nebo dat. Realizace spočívá v opakujícím se vykonávání čtyř základních činností, mezi které se řadí [1]:

- **Plánuj** – (Plan) – je záměrem pro uvažované zlepšení
- **Dělej** – (Do) – v tomto kroku se realizuje plán
- **Kontroluj** – (Check) – srovnání výsledné realizace a původního plánu
- **Jednej** – (Act) – po poznatcích z předchozích kroků, je třeba upravit plán i samotné vlastní provedení na základě ověření a následně plošně implementovat zlepšení do praxe[1].

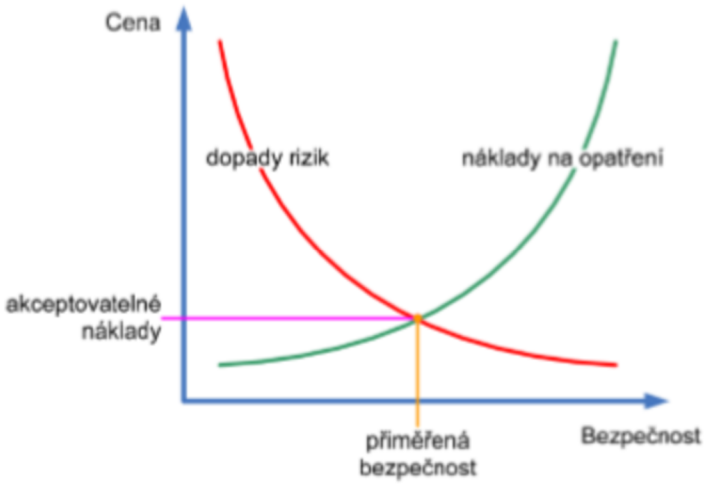
Důležitou součástí modelu je dokumentace. Zaznamenává se každá etapa cyklu. Vzniklé procesy je potřeba identifikovat, popsat a zavést do dokumentace. Také je třeba procesy správně řídit na základě dokumentace a v neposlední řadě optimalizovat [1].



Obrázek 1: PDCA cyklus (Zdroj: vlastní zpracování)

Počítačová síť – slouží jako součást síťové infrastruktury, kdy vzniká komunikační prostředí pro uživatele sítě [1].

Přiměřená bezpečnost – graf pojednává o rovnosti úsilí a investic vložených do bezpečnosti IS se musí přibližně rovnat hodnotám aktiv a míře možných rizik. Bezpečnostní politika organizace stanovuje přiměřenou bezpečnost. Křivky náklady na opatření a dopady rizik, se střetávají právě v bodě, ze kterého vedou kolmice akceptovatelných nákladů a přiměřené bezpečnosti [1].



Obrázek 2: Graf přiměřené bezpečnosti (Zdroj: [1])

Riziko – (Risk) – vzniká propojením hrozby a zranitelnosti. Má dopad na aktiva. [1].

Řízení přístupu – slouží k zajištění autorizovaného a omezeného přístupu k aktivům. Vychází z podnikových a bezpečnostních požadavků [3].

Síťová infrastruktura – je pojmem pro všechny síťové prvky a zařízení používané k realizaci ICT prostředí. V některých případech se jedná o aktiva v oblasti informačních a komunikačních technologií, používaná k vytváření a podpoře informačního systému [1].

Zranitelnost – (Vulnerability) – je slabým místem daného aktiva. Na tuto slabinu cílí hrozby [1].

Útok – snaha o zisk aktiva bez oprávněného přístupu. Ve zkratce je útok často pokusem o krádež, zneužití, vyzrazení, zničení nebo změnu daného aktiva [3].

1.2 Informační a Kybernetická bezpečnost

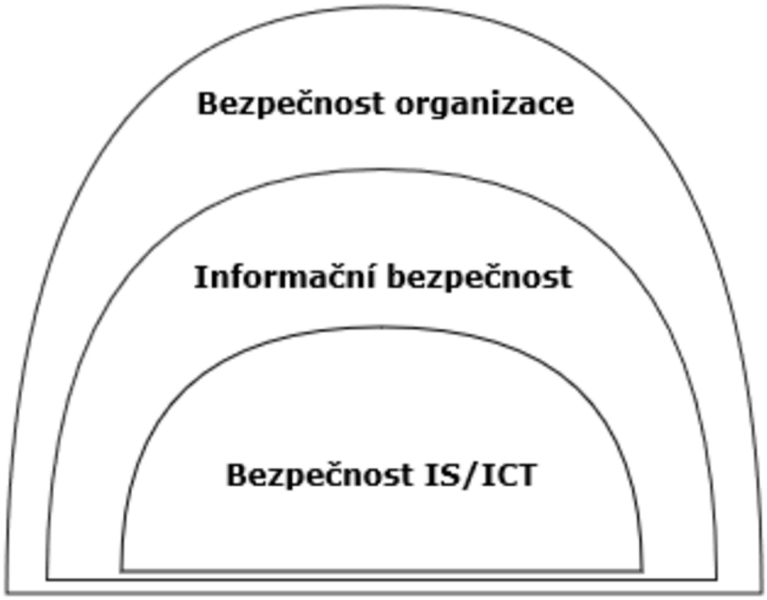
Informační bezpečnost

Informační bezpečnost (IB) či někdy také bezpečnost informací (BI) se týká ochrany dostupnosti, důvěrnosti a integrity informací. Svou roli zde, ale můžou hrát i jiná kritéria spolehlivost, autenticita, nepopiratelnost a odpovědnost [4]. Informace je všeobecně brána jako aktivum, které má hodnotu a vyžaduje specifickou ochranu. Včasným poskytováním přesných a kompletních informací těm, kdo na ně mají oprávnění je hnacím motorem pro efektivitu podnikání [3].

Bezpečnost IS/ICT – zajišťuje ochranu informačního systému, který je podporován informačními a komunikačními technologiemi a obsahuje aktiva organizace [4].

Bezpečnost Organizace – cílem je zabezpečení majetku a objektu organizace a to s ohledem na vnější a vnitřní prostředí [4].

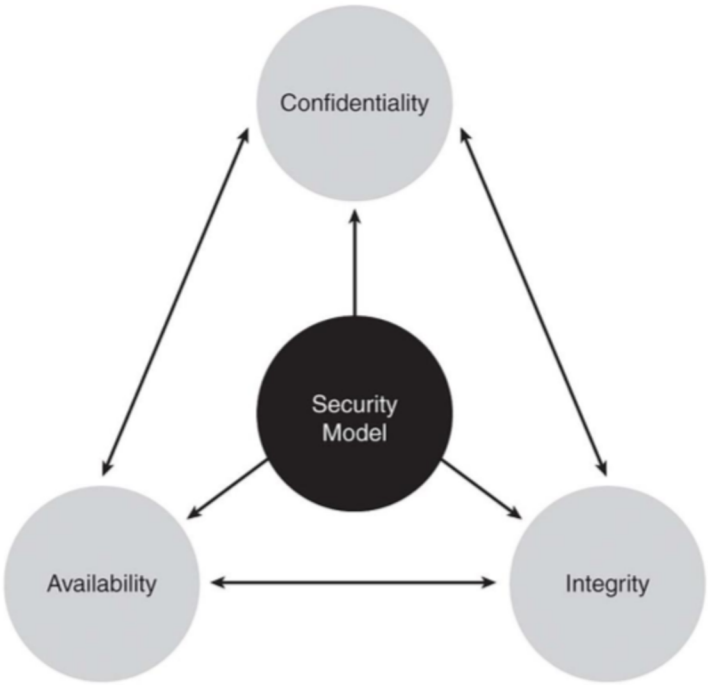
Nutno dodat, že pojmy Bezpečnost IS/ICT, Informační bezpečnost a Bezpečnost organizace jsou ve vzájemném vztahu. Tento vztah je zobrazený na Obrázku č. 3 [1].



Obrázek 3: Schéma úrovní bezpečnosti **(Zdroj: vlastní zpracování)**

Kritéria informační bezpečnosti, nazývána též jako **triáda CIA**[8]., do které řadíme:

- **Důvěrnost –** (Confidentiality) – kritérium zajišťující, že informace nejsou zpřístupněny nebo zveřejněny neoprávněným uživatelům, entitám nebo procesům[3].
- **Integrita –** (Integrity) – informace musí plnit kritérium úplnosti a přesnosti (správnosti) [3].
- **Dostupnost –** (Availability) – tento typ kritéria se týká dostupnosti informací, které jsou přístupné a použitelné na požádání oprávněným uživatelem v příslušném momentu požadavku [3].



Obrázek 4: Kritéria informační bezpečnosti (Zdroj: [14])

Kybernetická bezpečnost

Kybernetická bezpečnost (KB) je množinou vzdělávacích, organizačních, technických a právních prostředků, zajišťujících ochranu kyberprostoru [7]. Kybernetická a Informační jsou někdy chybně považovány za totožné. Určité podobnosti je spojují, zásadní je však rozdíl v perimetru těchto pojmů. Kybernetická bezpečnost se týká kybernetického prostoru, kdežto v případě informační bezpečnosti jde o bezpečnost fyzickou, komunikační, organizační, personální [9].

Ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany

v České Republice je **Národní úřad pro kybernetickou a informační bezpečnost** (NÚKIB). Tento úřad vznikl 1. srpna 2017 na základě zákona číslo 205/2017 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). O Kybernetické bezpečnosti pro kritickou infrastrukturu pojednávají zákony a vyhlášky. Poprvé byli vydané roku 2014, přičemž v roce 2017 vyšla jejich novelizace, *zákon č. 104/2017 Sb. a zákon č. 205/2017 Sb.* [10].

Kybernetická bezpečnost popisuje pojmy **Kritická infrastruktura** a **Kritická informační infrastruktura** [10].

Kritická infrastruktura – je zastoupena ve výrobních i nevýrobních systémech a službách, kde vážné narušení či ztráta správné funkce může způsobit dopad na bezpečnosti stát, zabezpečení základních životních potřeb obyvatelstva, ekonomiku atp. [1]. Typickým příkladem může být zařízení, stavba, veřejná infrastruktura. Kritéria pro výběr KI jsou obsažena v *nařízení vlády č. 432/2010 Sb.*, o kritériích pro určení prvku kritické infrastruktury [11].

Kritická informační infrastruktura – obsahuje prvky či soubor prvků KI a to ve vztahu k ICT v Kybernetické bezpečnosti. Proces určování probíhá dle *zákona č. 240/2000 Sb.*, o krizovém řízení a o změně některých zákonů jinak nazýváno jako krizový zákon a *nařízení vlády č. 432/2010 Sb.*, o kritériích pro určení prvku kritické infrastruktury ve znění *novely č. 315/2014 Sb.* [10].

1.3 Systém řízení bezpečnosti informací (ISMS)

Systém řízení bezpečnosti informací, také popisován názvem v anglickém jazyce (*Information Security Management System*) či zkratkou ISMS.

Definice ISMS

ISMS se skládá z politik, postupů, pokynů, souvisejících zdrojů a činností kolektivně řízených společností ve snaze o ochranu jejich informačních aktiv. Slouží k systematickému přístupu k ustanovení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování organizační informační bezpečnosti k dosažení podnikatelských cílů. Vychází z posouzení rizika a úrovní akceptovatelnosti rizika organizace, které jsou navrženy tak, aby účinně ošetřovaly a řídily rizika. K zajištění

ochrany těchto informačních aktiv, v závislosti na požadavcích, přispívá analýza požadavků na ochranu informačních aktiv a vhodné kontroly [3].

Pro úspěšnou implementaci ISMS přispívají i tyto základní principy:

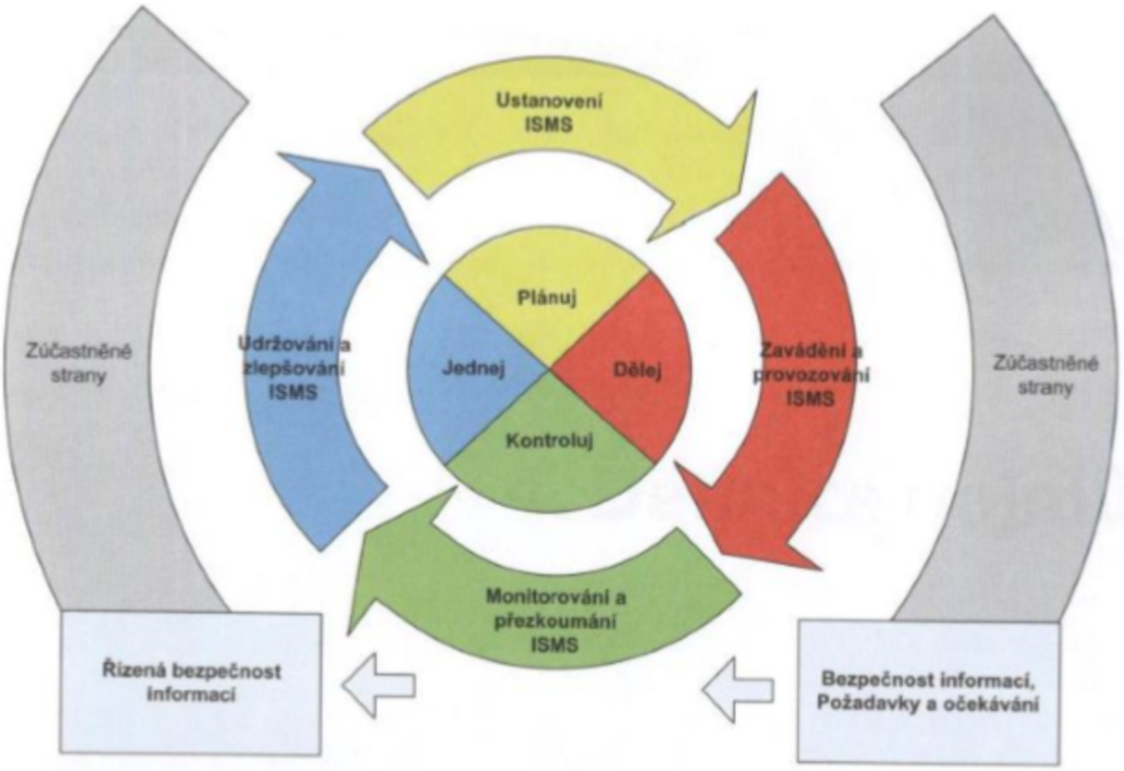
- přidělení odpovědnosti za bezpečnost informací,
- povědomí o potřebě pro informační bezpečnost,
- začlenění závazků vedení a zájmů zúčastněných stran,
- posouzení rizik určující vhodné kontroly pro dosažení přijatelné úrovně rizika,
- bezpečnost začleněná jako základní prvek informačních sítí a systémů,
- aktivní prevenci a odhalování incidentů bezpečnosti informací,
- neustálé přehodnocování bezpečnosti informací a případné úpravy,
- zajištění komplexního přístupu k řízení informační bezpečnosti [3].

Systém řízení bezpečnosti informací je možno zavést pro organizační složku společnosti, informační systém či jeho část, ale lze zavádět i pro celou organizaci. Rozhodnutí o zavedení ISMS je tedy strategickým rozhodnutím vedení společnosti [1].

ISMS je také napojeno na výše popisovaný PDCA cyklus a skládá se ze čtyř etap. Chce-li společnost zavést ISMS, pak by cílem mělo být zavedení zvolených bezpečnostních opatření a to efektivně a systematicky [1].

Mezi etapy cyklu ISMS řadíme:

- Ustanovení ISMS,
- Zavádění a provozování ISMS,
- Monitorování a přezkoumání ISMS,
- Udržování a zlepšování ISMS [1].



Obrázek 5: PDCA cyklus pro ISMS (Zdroj: [1])

Ustanovení ISMS (Plánuj)

Úvodní etapa ustanovení ISMS je většinou tou nejnáročnější. V této etapě je třeba vymezit hranice a samotný rozsah ISMS. Vedení musí tuto část odsouhlasit zejména ve smyslu požadavků společnosti, které vyplynuli z analýzy rizik ISMS [2]. Mezi hlavní činnosti této etapy řadíme:

- vymezení rozsahu a hranic ISMS,
- odsouhlasené Prohlášení o politice ISMS,
- vypracování analýzy rizik
- přijmutí zbytkových rizik vedením organizace a zavedení ISMS
- vytvoření Prohlášení o aplikovatelnosti [4].

Vymezení rozsahu a hranic ISMS

Hranice ISMS mohou být nastaveny různě, není nutné ISMS aplikovat na celou organizaci [4] Při vymezení lze vychází ze dvou způsobů.

Možnost první vymezuje rozsah pro celou organizaci. Výhodou tohoto způsobu je především ve vytvoření informační bezpečnosti v celé organizaci. Řešení tohoto typu s sebou však nese i nevýhody především v podobě nutných investic, kdy je třeba vynaložit zdroje a peněžní prostředky [4].

Další způsob pojednává o omezení rozsahu ISMS, kdy můžeme zavádět jen na vybranou část organizace, např. informační systém. Lépe je zvolit tu část organizace, kde jsou ochotni se přizpůsobit efektivním změnám a vylepšením [4].

Prohlášení o politice ISMS

Jedná se o dokument sloužící k definování politiky ISMS vytvořený na základě potřeb dané organizace. Ačkoliv se jedná o krátký dokument, jeho důležitost je značná. Slouží k výběru směru, definování cíle ISMS a vymezení rámce řízení bezpečnosti informací. Prohlášení zohledňuje i cíle organizace a požadavky, včetně smluvních na úrovni zákonu a regulace. V neposlední řadě je součástí stanovení kritérií popsání a hodnocení rizik, ale i údržby ISMS. Tento dokument musí být taktéž schválen vedením organizace [4].

Analýza rizik (řízení rizik)

Analýza rizik je dle definice systematická činnost, sloužící pro odhad míry rizika a stanovení jeho zdroje. Tyto koordinované aktivity slouží pro řízení organizace se zřetelem na rizika a kontrolu [4].

V další části práce se k analýze rizik ještě vztahuje důkladnější popis.

Přijmutí zbytkových rizik vedením organizace a zavedení ISMS

Vedení musí přijmout návrh bezpečnostních opatření. Opatření jsou navrhována tak, aby snížili bezpečnostní rizika pro organizaci. Důležité je také, aby se vedení poradilo a dohodlo ohledně existujících zbytkových rizik, jestli je přijmout či nikoliv [4].

Prohlášení o aplikovatelnosti

Dokument obsahující prohlášení, ve kterém jsou uvedena dílčí bezpečnostní opatření v souladu s užitím na ISMS organizace a cíle plánovaných opatření. Tento dokument je povinný v případě, že cílí na soulad ISMS s normou ISO/IEC 27001 [4]. Kromě

plánovaných a současných cílů bezpečnostních opatření obsahuje dokument také cíle vyřazené. Bezpečnostní opatření vyřazená najdeme v příloze A i s odůvodněním jejich vyřazení [1].

Zavádění a provozování ISMS (Dělej)

Druhá část cyklu si klade za cíl úspěšně implementovat veškerá bezpečnostní opatření, jak bylo navrhováno v předchozí ustanovovací části. Pro tuto etapu je nutné mít připravené plány, termíny a odpovědné osoby. Součástí je vytvoření dokumentu „Plán zvládání rizik“, zavádění navržených bezpečnostních opatření a sepsání příručky bezpečnostních opatření a jejich postupy při aplikaci. Dále je třeba připravit školení všech pracovníků z informatického úseku, zejména ty co se podílí na řízení bezpečnosti a v neposlední řadě zformulovat program pro budování bezpečnostního povědomí. Bezpečnostní opatření musí mít specifikovány způsoby jejich měření. V důsledku na bezpečnostní incidenty, je třeba zavést opatření a definovat postup zajišťující rychlou detekci. Řídit dokumenty ISMS, záznamy a zdroje [4].

Monitorování a přezkoumání ISMS (Kontroluj)

Třetí část cyklu se věnuje pravidelnému monitorování a přezkoumávání účinnosti zavedených opatření. Děje se tak za pomoci výsledků auditů, měření účinnosti opatření všech zainteresovaných stran, návrhů incidentů. Přezkoumání definuje přiměřenosti, vhodnosti a efektivnosti přezkoumávaného předmětu [1].

Interní audity ISMS, jejich realizace a monitorování účinnosti uplatnění bezpečnostních opatření či vyhotovení zprávy o stavu ISMS, z níž se přehodnocuje ISMS na úrovni vedení organizace, rovněž patří do této etapy [4].

Údržování a zlepšování ISMS (Jednej)

Závěrečná část cyklu se skládá ze sběru podnětů ke zlepšení ISMS a nápravě neshod objevených v ISMS. Za neshodu je bráno neuskutečnění požadavku. Tato etapa přináší i zavedení identifikovaných možností zlepšení. Nedostatky je třeba odstranit za pomocí realizace příslušných opatření [4].

1.4 Normalizační instituce a normy

Norma – je doporučením pro dané řešení nebo standart, povětšinou ve formě směrnice. Směrnice plní funkci doporučení použitelných standardů pro samotnou realizaci [1].

Standard – úmluva, která obsahuje jasně definovaná kritéria určitého typu a je zdokumentována. Kritéria jsou považována za pravidla pro dosahování finálního stavu služeb, výrobků či procesů v rámci odvětví [1].

1.4.1 Normalizační instutice

ISO – International Organization for Standardization

Patří k nejvíce známým a největším standardizačním organizacím na světě. Zajišťuje podporu a rozvoj standardizačních aktivit v odvětvích mezinárodní směny zboží a služeb. Působí také v technologické a vědecké sféře, kdy se zapojuje do ekonomických aktivit spojených s touto sférou [1].

IEC – International Electrotechnical Commission

Mezinárodní standardizační organizace, působící v oblasti elektrotechniky a oblastech podobného zaměření, její hlavní funkcí je normalizační činnost [1].

ITU – International Telecommunications Union

Další z řady mezinárodních organizací, které vznikla původně pro oblast telekomunikací, ale s postupem času a spojením telekomunikací se sférou informačních technologií se tato instituce a její normy, které vydává, používají také v oblasti ICT.

Tato organizace se zasloužila o podporu moderních technologií, zejména pak mobilní a také internetové technologie. V současné době se její pohled ubírá k prvkům globální informační infrastruktury. Důležitou roli představuje ve správě spekter rádiových frekvencí [1].

ČSNI – Český Normalizační Institut

Český normalizační institut byl na počátku svého vzniku příspěvkovou státní organizací, která měla za cíl zastupovat národní zájmy v mezinárodních a evropských normalizačních

institucí z pozice národní normalizační instituce. Institut svým členstvím patří do několika mezinárodních normalizační organizací, např.: ISO, IEC či evropských CEN, CENELEC či v normalizačním institutu pro telekomunikace ETSI [1].

ČSNI se zaměřuje především na:

- tvoření českých technických norem,
- vydávání a distribuci českých technických norem,
- poskytuje informace o českých technických normách,
- spolupracuje s nevládními evropskými a mezinárodními normalizačními institucemi [1].

ČSN – Česká technická norma

Vzniká přejímáním mezinárodních a evropských norem do soustav českých technických norem ve formě ČSN EN (ČSN IEC, ČSN ISO, ČSN ETS, a další). Druhým způsobem je tvorba původních ČSN, které vyplývají z národních potřeb a z hlediska zachování funkčnosti fondu ČSN [1].

NIST – National institute for Standards and Technology

National institute for Standards and Technology je americkým vládním standardizačním orgánem, který se angažuje v oblastech vývoje a podpory standardů, technologií a také měřících technik. Jeho cílem je usnadnění obchodu, zvýšení produktivity a celkové zlepšení života [1].

1.4.2 Řada norem ISO/IEC 27000

Normy řady ISO/IEC 27000 někdy také označovány jako „Rodina norem ISMS“ jsou mezinárodní normy pro účel tvorby a provozu systému řízení. Tato rodina norem stojí za tím, že mohou organizace různých zaměření a velikostí zavádět a provozovat ISMS. Patří do ní čtyři typy, jak je možno vidět z tabulky níže [3].

Tabulka 1: Rodina norem ISMS (Zdroj: Vlastní zpracování dle ISO/IEC 27000:2018 [3])

Rodina norem ISMS				
Terminologie ISMS	**Požadavky ISMS**	**Směrnice ISMS**	**Odvětvové směrnice ISMS**	**Směrnice pro konkrétní odvětví**
27000	27001	27002	27010	27003x
	27006	27003	27011	27004x
	27009	27004	27017	
		27005	27018	
		27007	27019	
		TR 27008		
		27013		
		27014		
		TR 27016		
		27021		

Norma terminologie ISMS

ISO/IEC 27000:2018 *Systémy řízení bezpečnosti informací – Přehled a slovník*

Norma ISO/IEC 27000 obsahuje přehled všech norem a jejich definic. Součástí je i slovník užívaných termínů v těchto normách a popis principu ISMS. Věnuje se také systémům řízení bezpečnosti informací [3].

Normy upřesňující požadavky ISMS

ISO/IEC 27001:2013 *Systémy řízení bezpečnosti informací – Požadavky*

Norma popisuje požadavky na cyklus ustanovení, zavádění a provozování, monitorování a přezkoumávání, udržování a zlepšování ve spojitosti s celkovými riziky činností organizace. Obsahuje definice požadavků na bezpečnostní opatření v souvislosti s potřebami organizace nebo její části [3].

ISO/IEC 27006:2015 *Požadavky na orgány poskytující audit a certifikaci systémů řízení bezpečnosti informací*

Účelem této normy je podpora certifikačních orgánů. Norma popisuje požadavky a návody pro příslušné orgány k poskytování auditu a certifikace ISMS na základech normy ISO/IEC 27001 [3].

ISO/IEC 27009:2016 *Používání ISO/IEC 27001 pro specifická odvětví - Požadavky*

Obsahuje soupis požadavků pro užití normy ISO/IEC 27001 pro specifická odvětví. Smyslem je zabezpečit dodatečné nebo upravované požadavky v souladu s přílohou A ISO/IEC 27001, tak aby byly nekonfliktní [3]. V současnosti se očekává její brzké nahrazení novou normou ISO/IEC 27009.

Normy směrnic ISMS

ISO/IEC 27002:2013 *Soubor postupů pro opatření bezpečnosti informací*

Norma poskytuje směrnice pro standardy organizační bezpečnosti informací a postupy řízení informační bezpečnosti, včetně výběru, provádění a řízení kontrol s přihlédnutím k rizikům organizace v oblasti bezpečnosti informací [3].

ISO/IEC 27003:2017 *Směrnice pro implementaci systému řízení bezpečnosti informací*

Norma postavena na vysvětlení a návodu pro ISO/IEC 27001 [3].

ISO/IEC 27004:2016 *Řízení bezpečnosti informací – Měření*

Přináší směrnici určenou k tomu, aby pomohla organizacím posoudit účinnost systému řízení bezpečnosti s ohledem k normě ISO/IEC 27001 [3].

ISO/IEC 27005:2018 *Řízení rizik bezpečnosti informací*

Dokument obsahuje směrnice k řízení rizik v oblasti bezpečnosti informací. Podporuje obecné koncepce specifikované v normě ISO/IEC 27001 a je navrhnut, tak aby dopomohl k uspokojivé implementaci informační bezpečnosti založené na přístupu řízení rizik [3].

ISO/IEC 27007:2017 *Směrnice pro audit systémů řízení bezpečnosti informací*

Norma poskytující směrnice, které se týkají řízení programu auditu ISMS a provádění auditů ISMS. Také obsahuje kompetence auditorů [3]. V současné době prochází tato norma revizí.

ISO/IEC TS 27008:2019 *Směrnice pro návod na posuzování opatření ISMS*

Poskytuje směrnice k přezkoumání, hodnocení, provádění a provozu kontrol bezpečnosti informací včetně technického posouzení kontrol informačního systému v souladu s požadavky stanovené organizací na zabezpečení informací, včetně technického souladu s hodnotícími kritérii založenými na požadavcích na bezpečnost informací stanovených

organizací. Součástí je také směrnice, jak kontrolovat a posuzovat kontroly bezpečnosti informací, které jsou řízeny prostřednictvím systému pro správu bezpečnosti informací specifikovaného normou ISO / IEC 27001 [3].

ISO/IEC 27013:2015 *Návod pro integrovanou implementaci ISO/IEC 27001 a ISO/IEC 20000-1*

Obsahuje směrnice pro integrovanou implementaci ISO / IEC 27001 a ISO / IEC 20000-1 pro organizace, které využít jeden z následujících způsobů:

- implementovat normu ISO / IEC 27001, pokud je ISO / IEC 20000-1 již zavedena
- implementovat společně ISO / IEC 27001 a ISO / IEC 20000-1
- integrovat stávající řídicí systémy založené na ISO / IEC 27001 a ISO / IEC 20000-1 [3].

ISO/IEC 27014:2013 *Správa bezpečnosti informací*

Poskytuje směrnice k pojetí a zásadám pro řízení bezpečnosti informací, pomocí kterých mohou organizace v rámci organizace vyhodnocovat, řídit, monitorovat a sdělovat činnosti spojené s bezpečností informací. Tato norma platí pro všechny typy a velikosti organizací [3]. Momentálně se pracuje na její revizi.

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

V této technické zprávě jsou obsaženy směrnice pro to, jak může organizace rozhodovat o ochraně informací a pochopit ekonomické důsledky těchto rozhodnutí v kontextu konkurenčních požadavků na zdroje [3].

Normy specifických odvětví ISMS

Do těchto norem jsou řazeny ty, které patří k specifickým odvětvím ISMS, jak je uvedeno výše v tabulce 1. patří sem normy ISO/IEC 27010, 27011, 27017, 27018, 27019.

Jejich specifikaci zde nebudu popisovat, protože tato práce o nich kvůli svému zaměření pojednávat nebude.

1.5 Analýza rizik

Analýza rizik se provádí z důvodu identifikace zranitelných míst v informačním systému organizace. Vytváří a zachycuje seznam hrozeb působící na informační systém a stanovuje rizika pro každé zranitelné místo a to i hrozbám. Tento dokument se vytváří za účelem snížení rizik na přijatelnou úroveň pro danou organizaci. Akceptace zbytkových rizik je nutná u takových rizik, kde je jejich minimalizování neefektivní [1].

1.5.1 Metody analýzy rizik

Kvantitativní analýza

Analýza sloužící pro určení pravděpodobnosti a následků. Rizika jsou zde ve stupnici vyjádřené číselně. Analýza používá data z mnoha zdrojů a kvalita výstupů analýzy je úměrná přesnosti a úplnosti analyzovaných číselných hodnot. Tento typ analýzy často využije i starší data pojená s incidenty v historii [12].

Hlavní **výhodou** této metody je právě využívání dat z historie incidentů, což souvisí s bezpečnostními cíli a zájmy organizace. **Nevýhodou** je nedostatek dat u nejnovějších incidentů či zranitelností [12].

Tabulka 2: Stupnice míry rizika (Zdroj: Vlastní zpracování dle [1])

Míra rizika - R	
Stupeň rizika	**Kritérium rizika**
0-10	Bezvýznamné riziko
11-20	Akceptovatelné riziko
21-30	Mírné riziko
31-60	Nežádoucí riziko
61-125	Nepřijatelné riziko

Bezvýznamné riziko (zanedbatelné)

- nevyžaduje žádné specifické opatření
- je na něj nutno upozornit a uvést případná opatření [1].

Akceptovatelné riziko (přijatelné)

- přijatelné se souhlasem vedení organizace
- je třeba zvážit náklady na jeho řešení případně zlepšení

- pokud se nepodaří provést technická bezpečnostní opatření, je nutné zavést bezpečnostní opatření k jeho snížení dle místních podmínek (školení) [1].

Mírné riziko (významné)

- dle plánu a rozhodnutí firmy je třeba bezpečnostní opatření realizovat
- prostředky sloužící na snížení rizika musí být zavedeny v určeném časovém období (potřeba nápravné činnosti) [1].

Nežádoucí riziko

- vyžaduje co nejrychleji provést odpovídající bezpečnostní opatření vedoucí k jeho snížení na přijatelnou úroveň
- na snížení rizika je třeba přidělit potřebné zdroje
- pokud se riziko pojí závažnými následky, je třeba ho dále vyhodnotit tak, aby byla stanovena pravděpodobnost vzniku úrazu a sloužila jako podklad pro stanovení potřeby dosažení snížení rizika (vysoké riziko, bezprostřední bezpečnostní opatření) [1].

Nepřijatelné riziko

- kritické, nepřípustné a značné riziko s neustálou možností úrazů
- hrozí závažné nehody, je třeba okamžitě zastavit činnost, odstavit z provozu a to do doby než se realizují nezbytná opatření, opět vyhodnotí rizika a přijmou daná opatření
- práce se **nesmí zahájit** nebo v ní nějakým způsobem pokračovat, dokud se riziko nesníží (velmi vysoké riziko, zastavit činnost!) [1].

Kvalitativní analýza

Tato analytická metoda specifikuje hrozby podle dle jejich úrovní. Rozlišujeme tyto následky hrozeb: nízkou, střední, vysokou, kritickou a také jejich pravděpodobnosti. Stupnici lze upravit a navrhnout dle okolností. Kvalitativní analýza se používá, pokud není vhodné použít číselné ohodnocení, ale také za situace, kdy je tato analýza vhodnější pro rozhodnutí [12].

Výhodu může značit to, že se nejedná o příliš složitou analýzu z pohledu chápání pro pracovníky v organizaci. **Nevýhodou** se může stát právě zmiňovaná subjektivně špatně zvolená stupnice [12].

Tabulka 3: Stupnice akceptace rizik (Zdroj: Vlastní zpracování dle [16])

Úroveň rizika		Popis
1-3	**Nízká**	Riziko je akceptováno **automaticky**.
4-6	**Střední**	Riziko může akceptovat **Garant aktiva**.
7-8	**Vysoká**	Riziko může akceptovat **Garant aktiva**, společně s **Pověřencem pro ochranu osobních údajů** nebo **Zástupcem vedení organizace**
9-10	**Kritická**	Riziko nelze akceptovat.

1.5.2 Fáze analýzy rizik

Fáze 1

- Slouží k ohodnocení datových aktiv s cílem určit možné dopady narušení dostupnosti, důvěrnosti a integrity informací
- hlavním předmětem analýzy CRAMM jsou datová aktiva a především jejich hodnota, která tvoří stěžejní položku při učení míry rizika a bezpečnostních požadavků
- fyzická (HW), programová (SW) aktiva (hodnocena např. podle pořizovacích nákladů) [1].

Fáze 2

- hodnotí se hrozby a zranitelnosti (H, Z)
- cílem je zhodnocení potencionálních hrozeb vedoucích k výskytu následků zjištěných ve fázi jedna a zranitelnosti systému vůči těmto hrozbám
- stanovení míry rizik systému (na základě hodnocení hrozeb, zranitelností a ocenění aktiv)
- míra rizika aktiva nebo skupiny aktiv je určena spojením hodnoty aktiva s hodnocením hrozby a zranitelnosti [1].

Fáze 3

- pomocí výpočtu míry rizika se určí vhodná opatření (databáze metodiky CRAMM)

- Oblasti bezpečnosti je doporučeno rozdělit na: IT bezpečnost, Personální bezpečnost, Fyzickou bezpečnost, Komunikační bezpečnost, Administrativní bezpečnost [1].

1.6 Řízení rizik (Risk management)

Řízení rizik cílí na identifikaci a kvantifikaci rizik. Organizace čelí rizikům a je proto nutné rozhodnout jak tato rizika zvládnout. Mezi nejpoužívanější metody patří snížení rizika [1].

Jde o komplexní proces, který je složen z několika na sebe navazujících částí vytvářející cyklus [1].

Obrázek 6: Cyklus fází řízení rizik (Zdroj: [1])

Stanovení kontextu

V této fázi se popisuje proces řízení rizik, definují role a odpovědnosti v rámci procesu. Vybere se také metodika, která bude použitá v analýze rizik, stanoví se referenční úroveň, způsoby i kritéria hodnocení a zvládání rizik [1].

Analýza rizik (Risk analysis)

Fáze pro identifikaci a kvantifikaci aktiv, hrozeb zranitelností a v neposlední řadě je třeba stanovit míru rizika [1].

Vyhodnocení rizika (Risk evaluation)

Kritická fáze procesu řízení, prioritizují a vybírají se optimální opatření, která vedou ke snížení rizika [1].

Zvládání rizik (Risk treatment)

Závěrečná fáze, ve které je rozhodnuto o nejvhodnějším způsobu, jak zvládnout rizika (transfer, redukce, pojištění, retence a vyhnutí se riziku) [1].

Mezi součásti řízení rizika řadíme:

- šíření informací o riziku (Risk communication);
- vnímání rizika (Risk perception);
- akceptování rizika (Risk acceptance) [1, str. 96].

Každá fáze je zakončena rozhodnutím, které jsou povětšinou zastoupeny ve více variantách řešení. Pokud není úroveň rizik přijatelná, je třeba zastavit probíhající procesy a přijmout opatření na jejich snížení. Myšleno je i na zbytková rizika (opatření je nemusí efektivně snížit), pro která se vypracovávají krizové plány [1].

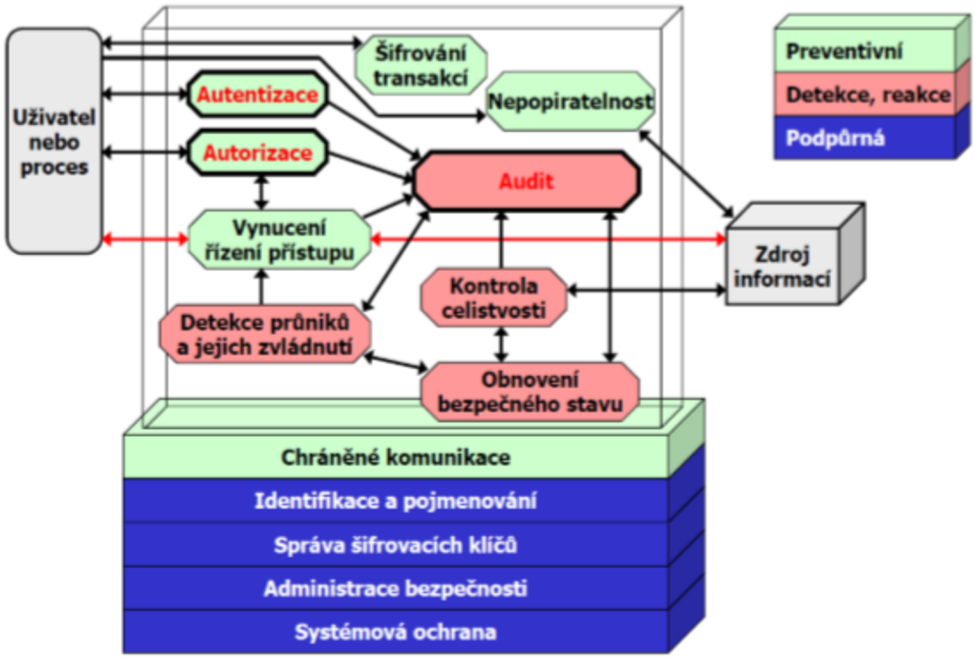
Pro oblast ISMS je vhodné zmínit normu ISO/IEC 27005:2018, která slouží jako podpora pro ISO/IEC 27001 a je tvořena, tak aby podporovala implementaci informační bezpečnosti stavěné na přístupu řízení rizik [1].

1.7 Opatření

Definice opatření je zmíněna již v části základní pojmy. Odpovídající ochrany lze dosáhnout za pomocí katalogů ochranných opatření. Katalogy popisují a navrhují sadu ochranných opatření pro ochranu systému IT proti obecným hrozbám [1].

Typy bezpečnostních opatření:

- preventivní,
- detekce a reakce,
- podpůrná [1].



Obrázek 7: Rozlišení bezpečnostních opatření (Zdroj: [1, str. 100])

Výběr opatření

Principem ochranných bezpečnostních opatření je minimalizace případných rizik. Mezi nejvýznamnější jsou zařazena tzv. „všeobecně aplikovatelná ochranná opatření“.

Základní kategorie jsou:

- řízení politiky bezpečnosti IT,
- kontrola bezpečnostní shody,
- řešení incidentů,
- personální opatření,
- provozní problémy,
- plánování kontinuity činností organizace,
- fyzická bezpečnost [1, str. 101].

Metodika CRAMM

Obsahuje velmi rozsáhlou databázi opatření a nazýváme ji jako knihovnu opatření. V této knihovně jsou zahrnuty opatření na pokrytí rizik. Metodika je podporována softwarovými nástroji a je schopna organizaci připravit certifikaci dle ISO/IEC 27001. Provádět lze také hodnocení rizik informačních systémů či navrhnout efektivní opatření s cílem zdokonalit informační bezpečnosti nebo provádět analýzy stavu vůči ISO/IEC 27001. Mezi další

vlastnosti patří řízení informačních rizik, vytváření bezpečnostních dokumentací havarijních plánů a plánů k zajištění kontinuity při provozu [1].

2 ANALÝZA SOUČASNÉHO STAVU

Tato část diplomové práce je zaměřená na analýzu současného stavu společnosti, jež mi poskytla potřebné informace. Nejprve je společnost představena, uvedena její organizační struktura a sepsaný seznam aktiv poskytnutý společností. Následně je společnost analyzována z pohledu infrastruktury, sítě a datových přenosů. Hlavním bodem této části je analýza vybraných oblastí a z ní plynoucí výsledky plnění. V závěru analytické části jsou představeny požadavky společnosti a nedostatky nalezené v oblastech analýzy.

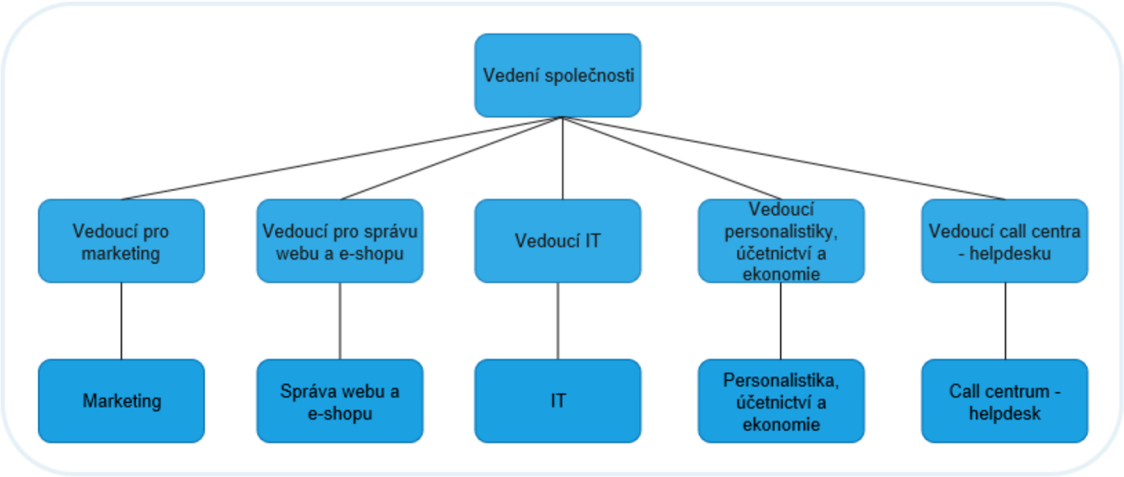
2.1 Představení společnosti

Vzhledem k vzneseným požadavkům společnosti, nebýt nijak identifikována ani jmenována, budu v diplomové práci společnost nazývat „společnost XYZ“ nebo prostým označením „společnost“. Pro ochranu společnosti před identifikací jsou její citlivé údaje anonymizované. Pro informace vedoucí k rozporům s bezpečnostními opatřeními platí totéž.

Právní norma společnosti je společnost s ručením omezeným a působí především v oboru výroby, obchodu a službách neuvedených v přílohách 1 až 3 živnostenského zákona. Nabízí celou řadu služeb jako např. zásilkový obchod, e-commerce, skladování, CRM, call-centrum. Sídlo i sklad společnosti se nachází v Pardubicích. Společnost XYZ zajišťuje také provoz čtyř e-shopů.

2.2 Organizační struktura

Ve společnosti je zavedena **liniová** organizační struktura. Zaměstnanci, kteří mají určitou odbornost, jsou sdruženi do jednotlivých specializovaných oblastí. Vedení společnosti dohlíží na činnost vedoucích všech dalších oblastí (marketing, správa webu a e-shopu, IT, personalistika, účetnictví a ekonomie, call centrum – helpdesk).



Obrázek 8: Organizační struktura společnosti (Zdroj: Vlastní zpracování)

2.3 Seznam aktiv společnosti

Pro zpracování této diplomové práce mi poskytla společnost seznam aktiv. Vzhledem k tomu, že z nich budu vycházet v analytické a především návrhové části, tak zde přidávám přehlednou tabulku s jednotlivými rozčleněnými aktivy.

Tabulka 4: Seznam aktiv (Zdroj: Vlastní zpracování)

Seznam aktiv					
Informační aktiva			Hardwarová aktiva	Softwarová aktiva	Služby
Veřejná	Interní	Důvěrné			
Nabídkové katalogy	Cenové nabídky	Data o zákaznících	Firewall	Operační systémy	Doménové služby
Informace na webu	Dokumentace	Data o zaměstnancích	Pasivní prvky sítě	Spamový filtr	E-shop
	Interní postupy	Nahrávky hovorů	Aktivní prvky sítě	MS SQL databáze	Webové stránky
	Zálohy dat	Obchodní tajemství	Mobilní zařízení	MS Dynamics CRM	VPN připojení
			IP kamery	Antivir	Internet
			Pracovní stanice	Software IP kamer	Zálohy
			IBM Server	VPN klient	Elektrická energie
			Notebooky	MS Exchange server	

2.4 Analýza společnosti

Následující kapitola se věnuje popisu společnosti z pohledu infrastruktury a prvků sítě.

2.4.1 Lokalita sídla společnosti

V sídle společnosti zaměstnanci používají jak stolní počítače (pracovní stanice), tak notebooky a mobilní přístroje, kterými se připojují do sítě. Jednotliví pracovníci mají přidělená zařízení. Server je umístěn v prostorech sídla společnosti. Zařízení jsou připojena k rozvaděči metalickou kabeláží, přičemž rozvaděč je připojen k páteřní síti

v budově. Páteřní síť je provozována na optické kabeláži. V sídle je realizována i Wi-Fi síť s rozmístěnými access pointy, aby byla pokryta celá budova. Pracovníci se připojují také pomocí VPN. Na serveru se nachází důležitá interní data společnosti. Data uchovává také v databázových systémech a zálohuje i na cloudové úložiště – Microsoft OneDrive, šifrovaný za pomoci protokolu TLS. Prostory společnosti jsou uzavřeném objektu, jako vjezd slouží brána. Budova je zabezpečena kamerovým systémem a interkomem. Jednotlivé kanceláře jsou zamykatelné. Ačkoliv nemá společnost dokument politik fyzické bezpečnosti, tak jsou přijata nezbytná opatření k zamezení neoprávněnému vstupu do vymezených prostor a jejich poškození. V souladu s tímto je předcházeno krádeži či kompromitaci aktiv a jsou uplatněny prostředky fyzické bezpečnosti pro zajištění a ochranu objektů. Přístup k rozvaděči mají pověření pracovníci IT oddělení a tato místnost je taktéž uzamykatelná.

2.4.2 Infrastruktura společnosti

Jak bylo zmíněno, server se nachází v sídle společnosti a má vyhrazenou serverovnu. Hardwarový server IBM AS/400 na kterém se provozuje za pomocí virtualizace databáze Microsoft SQL Server 2016, Microsoft Exchange Server 2016, VPN server a služby domény. Na serveru je také filtr proti spamu a provozuje se virtuální server Microsoft Dynamics CRM 2016. Server využívá operační systém Windows Server 2016 od Microsoft. Server je fyzicky přístupný jen pověřeným osobám. Vypadne-li elektrický proud, tak provoz zajišťuje UPS. Pokud nejsou v sídle společnosti, připojují se pracovníci k serveru pomocí VPN.

Kanceláře a sklad jsou součástí objektu společnosti, ve kterém je i sídlo. Pracovníci se připojují do sítě pomocí notebooků a pracovních stanic. V kanceláři se také využívá jak Wi-Fi sítě a je zde umístěno několik access pointů. Pracovníci skladu taktéž, využívají bezdrátové připojení, aby se mohli pohodlně pohybovat a využívat služeb Wi-Fi terminálů se kterými pracují.

2.4.3 Hardwarové a mobilní zařízení společnosti

Společnost XYZ používá ke své práci pracovní stanice a notebooky. Někteří pracovníci používají notebook pouze na pracovní výjezdy, jiní ovšem i místo pracovní stanice. Většina pracovníků používá k práci dva monitory. Zařízení fungují na operačním systému

Windows 10. Notebooky i pracovní stanice mají nainstalován aktuální verzi antivirového programu Kaspersky.

Společnost pracovníkům poskytuje mobilní telefony, které pak slouží pro komunikaci se zákazníkem, ale i mezi samotnými spolupracovníky. Mobilní telefony používají e-mailovou komunikace přes Microsoft Exchange a mají synchronizovaný kalendář. Společnost si zařízení od zaměstnance po ukončení pracovního poměru bere zpět. Nejsou zavedena bezpečnostní opatření pro ochranu dat, v případě odcizení nebo ztrátě zařízení. Zaměstnanci však mobilní zařízení zajišťují alespoň pomocí pin kódu nebo jinak nastaveného zámku displeje. Politika společnosti tyto zabezpečení nedefinuje. Při zabezpečení se tak společnost spoléhá na výrobce zařízení.

2.4.4 Datové přenosy

Společnost přenáší data zejména po síti, což obsahuje komunikaci se zákazníky, ale především mezi pracovníky. Komunikace serveru a zařízení (pracovních stanic a notebooků) je zabezpečena pomocí VPN (TLS). Mobilní zařízení nejsou zabezpečena. Komunikace a sdílení dokumentů společnosti stojí převážně na e-mailové komunikaci. Flash disky a starší média společnost využívá v omezené míře. Politika pro řízení a komunikace ve společnosti není zavedena, datové přenosy jsou částečně řešeny pravidly společnosti. IT oddělení má pověřené pracovníky, kteří řeší případné potíže s datovými přenosy a řízením komunikace. E-shopy provozuje společnost na web-hostingu, který je provozován třetí stranou.

2.4.5 Zálohování

Společnost zálohuje server a pracovní stanice. V případě pracovních stanic se zálohování ukládá na cloudové úložiště a uskutečňuje v sídle společnosti. Šifrování komunikace je zajištěno pomocí TLS. Společnost používá dvou-faktorovou autentizaci, kdy je zapotřebí heslo a vygenerovaný kód odeslaný na mobilní zařízení. Záloha serveru je ukládána, právě na server. Zálohovací politiky jsou částečně definovány pro všechny servery, aplikace a typy dat. Zálohy se realizují automaticky a kontrola záloh je prováděna výjimečně, většinou jde o situaci, kdy potřebuje obnovit data. Zálohování probíhá taktéž v případě IP kamer, kdy existuje možnost sledovat záznamy i v reálném čase při ukládání záznamu na paměťovou kartu IP kamery. Na server se zálohují po určitou dobu také nahrávky hovorů uskutečňované call-centrem společnosti.

2.5 Analýza vybraných oblastí

Tato kapitola se soustředí na rozhovor s pracovníky společnosti. V prvé řadě je nutno říci, že není pravidlem, že každý respondent zodpovídá za danou oblast, nicméně v mnoha oblastech to platí. Důvodem proč nedělat rozhovor přímo s pracovníkem zodpovídajícím za danou oblast vychází z praktických zkušeností. Mnohokrát respondent zodpovědný za danou oblast tvrdí, že mají např. pracovníci jiného oddělení nainstalovaný daný bezpečnostní nástroj, ale pokud se dotážeme přímo konkrétního oddělení, dojdeme k zjištění, že tomu tak není. Pomocí této metody jsme schopni odhalit nesrovnalosti mezi výpovědí odpovědného pracovníka a realitou.

Tabulka 5: Seznam respondentů pro každou oblast (Zdroj: Vlastní zpracování)

Oblast	Respondent
ISMS	Vedoucí IT
Řízení aktiv	Vedoucí IT
Řízení rizik	Vedoucí IT
Organizační bezpečnost	Vedení společnosti
Řízení dodavatelů	Vedoucí pro marketing
Bezpečnost lidských zdrojů	Vedoucí personalistiky, účetnictví a ekonomie
Řízení provozu a komunikací	Vedoucí pro správu webu a e-shopu
Řízení přístupu a bezpečné chování uživatelů	Vedoucí IT
Ověřování identity uživatelů	Vedoucí IT
Řízení přístupových oprávnění	Vedoucí pro správu webu a e-shopu
Akvizice, vývoj a údržba	Vedoucí IT
Aplikační bezpečnost	Vedoucí pro správu webu a e-shopu
Kryptografie	Vedoucí IT
Zajištění dostupnosti	Vedoucí IT
Bezpečnost ICS/SCADA	Neřešeno
Fyzická bezpečnost	Vedení společnosti
Ochrana integrity komunikačních sítí	Vedoucí IT
Ochrana před škodlivým kódem	Vedoucí IT
Log management	Vedoucí IT
Detekce kyberbezpečnostních událostí	Vedoucí pro správu webu a e-shopu
SIEM	Vedoucí IT
Incident handling	Vedoucí IT
Řízení kontinuity činností	Vedoucí IT

Pro získání potřebného přehledu bezpečnostních opatření ve společnosti je vytvořena následující analýza, která je provedena na základě pomůcky k auditu bezpečnostních

opatření, které jsou poskytované úřadem NÚKIB a to vyhláška č. 316/2014 Sb. Tato vyhláška byla nahrazena vyhláškou č. 82/2018 Sb., nicméně v době začátku přípravy této práce, ještě nebyla nová vyhláška dostupná. Na společnost se však nevztahují všechny oblasti, některé jsou nerelevantní a proto, jsou vynechány. Kupříkladu, zaznamenávání činnosti KII a VIS. Za každou částí je zhodnocující komentář. Analýza byla zhotovena dle této šablony:

Název oblasti	Požadavek/otázka
stav	Popis

Stav může nabývat čtyř eventualit a to: – **aplikováno**, **částečně aplikováno**, **neaplikováno** a **nerelevantní**.

2.5.1 Systém řízení bezpečnosti informací

ISMS	Stanoven rozsah a hranice ISMS. (Je určeno, kterých organizačních částí a technických prvků se ISMS týká.)
částečně aplikováno	Není formalizováno.

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.
částečně aplikováno	Neprobíhá vyhodnocování vhodnosti a účinnosti bezpečnostní politiky a ISMS.

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.
částečně aplikováno	Neprobíhá na pravidelné bázi.

ISMS	Je prováděna aktualizace ISMS a související dokumentace na základě zjištění auditů/penetračních testů, výsledků hodnocení účinnosti ISMS a v souvislosti s prováděnými změnami.
částečně aplikováno	Audity jsou prováděny v nepravidelných intervalech. Penetrační testy společnost neprovádí.

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

Systém řízení bezpečnosti informací není formalizován. ISMS nemá stanovené politiky a neprobíhá vyhodnocování jejich vhodnosti a účinnosti. Vyhodnocení kontrol dopadů bezpečnostních incidentů neprobíhá pravidelně. Společnost si neuvědomuje důležitost penetračního testování a tak zde vůbec neprobíhá. Audity se provádí v nepravidelných intervalech.

Společnost, ale alespoň monitoruje a zaznamenává činnosti spojené s ISMS a s ním souvisejícím řízení rizik.

2.5.2 Řízení aktiv

Řízení aktiv	Jsou identifikovány a evidovány primární aktiva.
částečně aplikováno	Evidence není úplná.

Řízení aktiv	Stanovena bezpečnostní politika pro klasifikaci aktiv.
neaplikováno	

Řízení aktiv	Určena bezpečnostní role: garant/vlastník aktiva.
částečně aplikováno	Role stanovena, nicméně někteří skuteční vlastníci nemají povědomí o této svoji roli a o vyplývajících povinnostech.

Řízení aktiv	Jsou určeni jednotliví garanti aktiv, kteří jsou odpovědní za primární aktiva.
částečně aplikováno	Vlastníci nejsou přiřazeni u všech primárních aktiv.

Řízení aktiv	Je hodnocena důležitost primárních aktiv z hlediska důvěrnosti, integrity a dostupnosti.
částečně aplikováno	Hodnocení není kompletní (není provedeno u všech aktiv).

Řízení aktiv	Při hodnocení důležitosti primárních 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.
částečně aplikováno	Zohledněny jen některé výše uvedené aspekty.

Řízení aktiv	Jsou identifikována a evidována podpůrná aktiva.
aplikováno	

Řízení aktiv	Jsou určeni garanti aktiv, kteří jsou odpovědní za podpůrná aktiva.
částečně aplikováno	Vlastníci nejsou přiřazeni u všech podpůrných aktiv.

Řízení aktiv	Jsou určeny vazby mezi primárními a podpůrnými aktivy. Jsou hodnoceny důsledky závislostí mezi primárními a podpůrnými aktivy.
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.
neaplikováno	

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	

Evidovány jsou pouze některá aktiva, přičemž není stanovena politika pro jejich klasifikaci. Bezpečnostní role jsou stanoveny, nicméně někteří pracovníci nemají povědomí o tom, že jim je nějaká přidělena a nemohou ji tak správně vykonávat. Některá aktiva nemají přiřazena vlastníky. Ohodnocení primárních aktiv není úplné a jsou zohledněné jen některé aspekty. Vazby mezi primárními a podpůrnými aktivy nejsou stanoveny, stejně tak nejsou rozděleny do úrovní.

Společnost však alespoň identifikuje a eviduje podpůrná aktiva.

2.5.3 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.
aplikováno	

Řízení rizik	Prováděna identifikace a hodnocení důležitosti VŠECH aktiv, které patří do rozsahu ISMS, výstupy jsou zapracovány do zprávy o hodnocení aktiv a rizik.
částečně aplikováno	Nejsou identifikována všechna aktiva.

Řízení rizik	Prováděna identifikace rizik, kdy jsou zohledňovány hrozby a zranitelnosti a jsou posuzovány možné dopady na aktiva.
částečně aplikováno	Nejsou identifikována všechna rizika.

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

Řízení rizik	Na základě bezpečnostních potřeb a výsledků hodnocení rizik je zpracováváno prohlášení o aplikovatelnosti (SoA).
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 (RTP) a plánu rozvoje bezpečnostního povědomí, a to nejméně jednou za 3 roky nebo v souvislosti s prováděnými nebo plánovanými změnami.
neaplikováno	

Řízení rizik	Při hodnocení rizik jsou zváženy hrozby, související s: - porušením bezpečnostní politiky, provedením neoprávněných činností, zneužitím oprávnění ze strany uživatelů a administrátorů - poškozením nebo selháním technického anebo programového vybavení - zneužitím identity fyzické osoby - užíváním programového vybavení v rozporu s licenčními podmínkami - kybernetickým útokem z komunikační sítě - škodlivým kódem (například viry, spyware, trojské koně) - nedostatky při poskytování služeb IS/KS KII nebo VIS - narušením fyzické bezpečnosti - přerušením poskytování služeb elektronických komunikací nebo dodávek elektrické energie - zneužitím nebo neoprávněnou modifikací údajů - trvale působícími hrozbami - s odcizením nebo poškozením aktiva
částečně aplikováno	Zohledněny jen některé výše uvedené aspekty.

Řízení rizik	Při hodnocení rizik jsou zváženy hrozby, související s: - porušením bezpečnostní politiky, provedením neoprávněných činností, zneužitím oprávnění ze strany administrátorů KII - pochybením ze strany zaměstnanců - zneužitím vnitřních prostředků, sabotáží - dlouhodobým přerušením poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb - nedostatkem zaměstnanců s potřebnou odbornou úrovní - cíleným kybernetickým útokem pomocí sociálního inženýrství, použitím špionážních technik - zneužitím vyměnitelných technických nosičů dat
částečně aplikováno	Zohledněny jen některé výše uvedené aspekty.

Řízení rizik	Zváženy zranitelnosti, související s: - nedostatečnou ochranou vnějšího perimetru - nedostatečným bezpečnostním povědomí uživatelů a administrátorů - nedostatečnou údržbou IS/KS KII nebo VIS - nevhodným nastavením přístupových oprávnění - nedostatečnými postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů - nedostatečným monitorováním činností uživatelů a administrátorů a neschopností odhalit jejich nevhodné nebo závadné způsoby chování - s nedostatečným stanovením bezpečnostních pravidel, nepřesným nebo nejednoznačným vymezením práv a povinností uživatelů, administrátorů a bezpečnostních rolí
částečně aplikováno	Zohledněny jen některé výše uvedené aspekty.

Řízení rizik	Zváženy zranitelnosti, související s: - nedostatečnou ochranou ICT - nevhodnou bezpečnostní architekturou - nedostatečnou mírou nezávislé kontroly - neschopností včasného odhalení pochybení ze strany zaměstnanců
částečně aplikováno	Zohledněny jen některé výše uvedené aspekty.

Společnost má stanoveny metodiky pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik včetně stanovení kritérií pro přijatelnost rizik. Jednou ročně je zpracována zpráva o hodnocení aktiv a rizik. Částečně jsou identifikována aktiva a rizika. Stejně je tomu u hrozeb a zranitelností.

2.5.4 Organizační bezpečnost

Organizační bezpečnost	Zavedena organizace řízení bezpečnosti informací (organizační bezpečnost), v rámci které je určen výbor pro řízení kybernetické bezpečnosti a bezpečnostní role a jejich práva a povinnosti související s ICT.
neaplikováno	

Organizační bezpečnost	Bezpečnostní politika: Organizační bezpečnost
neaplikováno	

Organizační bezpečnost	Určena bezpečnostní role: manažer kybernetické bezpečnosti / ISMS manažer.
neaplikováno	

Organizační bezpečnost	Určena bezpečnostní role: architekt kybernetické bezpečnosti.
neaplikováno	

Organizační bezpečnost	Určena bezpečnostní role: auditor kybernetické bezpečnosti.
neaplikováno	

Společnost nemá zavedenou žádnou organizaci řízení bezpečnosti informací. Bezpečnostní politika organizační bezpečnosti a bezpečnostní role nejsou definovány.

2.5.5 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.
částečně aplikováno	Není formalizováno, princip „security by design/default“ je zohledňován ad-hoc.

Řízení dodavatelů	Rozsah zapojení dodavatelů na rozvoji, provozu nebo zajištění bezpečnosti ICT dokumentuje písemnou smlouvou, jejíž součástí je ustanovení o bezpečnosti informací.
částečně aplikováno	Ne u všech relevantních smluv.

Řízení dodavatelů	Bezpečnostní politika: Řízení vztahů s dodavateli.
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	

Politika řízení vztahů s dodavateli není aplikována, přičemž se také neohodnocují rizika spojená s dodávkami.

Dohoda o úrovni poskytovaných služeb (SLA) je uzavírána vždy.

2.5.6 Bezpečnost lidských zdrojů

Bezpečnost lidských zdrojů	Bezpečnostní politika: Bezpečnost lidských zdrojů.
neaplikováno	

Bezpečnost lidských zdrojů	Bezpečnostní politika: Bezpečné chování uživatelů.
částečně aplikováno	V praxi neaplikováno u všech relevantních uživatelů.

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.
částečně aplikováno	Školení nejsou pravidelná.

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.
aplikováno	

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	

Bezpečnost lidských zdrojů	O školení jsou vedeny přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.
částečně aplikováno	Z některých školení takové záznamy nejsou – není možné jejich provádění zpětně prokázat.

Bezpečnost lidských zdrojů	Jsou stanovena pravidla pro určení osob, které budou zastávat bezpečnostní role, role administrátorů nebo uživatelů.
částečně aplikováno	Není formalizováno.

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).
neaplikováno	

Bezpečnost lidských zdrojů	Zajištěna změna přístupových oprávnění při změně postavení uživatelů, administrátorů nebo osob zastávajících bezpečnostní role.
částečně aplikováno	Neformalizován proces – řešeno ad-hoc v závislosti na požadavku nadřízeného.

Bezpečnostní politika ani plán rozvoje bezpečnostního povědomí, který zahrnuje např. školení osob, není zaveden. Citelným nedostatkem je absence pravidel a postupů při porušení bezpečnostních pravidel ze strany uživatelů, administrátorů či osob zastávající bezpečnostní role. Vstupní školení o bezpečnostní politice jsou prováděna, avšak nepravidelně. Záznamy ze školení nejsou vytvářeny na pravidelné bázi.

Kontrola dodržování bezpečnostních opatření je zajištěna, taktéž je tomu u vrácení svěřených aktiv a přístupových oprávnění.

2.5.7 Řízení provozu a komunikací

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

Řízení provozu a komunikací	Pomocí technických nástrojů (Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů, Nástroj pro detekci kybernetických bezpečnostních událostí, Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí) jsou detekovány kybernetické bezpečnostní události, pravidelně vyhodnocovány získané informace a na zjištěné nedostatky je reagováno v souladu se zvládáním kybernetických bezpečnostních událostí a incidentů.
částečně aplikováno	Události detekovány jen u některých technických aktiv.

Řízení provozu a komunikací	Bezpečnostní politika: Bezpečnost komunikační sítě.
neaplikováno	

Řízení provozu a komunikací	Bezpečnostní politika: Zálohování a obnova.
částečně aplikováno	Jen pro některé systémy/úložiště.

Řízení provozu a komunikací	Je prováděno pravidelné zálohování a prověřování použitelnosti provedených záloh.
částečně aplikováno	Jen pro některé systémy/úložiště.

Řízení provozu a komunikací	Provozní pravidla a postupy orgánu a osoby obsahují: - práva a povinnosti osob zastávajících bezpečnostní role, administrátorů a uživatelů.
částečně aplikováno	Neformalizováno.

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.
neaplikováno	

Řízení provozu a komunikací	Provozní pravidla a postupy orgánu a osoby obsahují: - postupy řízení a schvalování provozních změn.
aplikováno	

Řízení provozu a komunikací	Provozní pravidla a postupy orgánu a osoby obsahují: - postupy pro sledování, plánování a řízení kapacity lidských a technických zdrojů.
neaplikováno	

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

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.
neaplikováno	

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.
částečně aplikováno	Neformalizováno.

Řízení provozu a komunikací	Bezpečnostní politika: Dlouhodobé ukládání a archivace informací.
částečně aplikováno	Neformalizováno.

Řízení provozu a komunikací nemá stanovenou bezpečnostní politiku a to ani v případě bezpečnosti komunikační sítě. Provozní pravidla a postupy nejsou definovány pro činnosti jako je spuštění a ukončení chodu systému, postupy sledování kybernetických útoků, spojení na kontaktní osoby, které slouží jako podpora v případě nutnosti řešení systémových nebo technických potíží. Pro řízení technických zranitelností také není stanovena bezpečnostní politika, informace přenášené komunikačními sítěmi nejsou chráněny. Kybernetické bezpečnostní události jsou detekovány u některých technických aktiv. Zálohovací politiky jsou stanoveny, ale jen pro některé úložiště.

V této oblasti, tak společnost alespoň plní pravidla pro řízení a schvalování provozních změn a má oddělené vývojové, testovací a produkční prostředí.

2.5.8 Řízení přístupu a bezpečné chování uživatelů

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

Řízení přístupu a bezpečné chování uživatelů	Používán nástroj pro ověřování identity uživatelů (autentizační server).
aplikováno	

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

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	

Řízení přístupu a bezpečné chování uživatelů	Je prováděno pravidelné přezkoumání nastavení přístupových oprávnění včetně rozdělení jednotlivých uživatelů v přístupových skupinách nebo rolích.
částečně aplikováno	Prováděno ad-hoc.

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

Řízení přístupu a bezpečné chování uživatelů	Jsou zavedena bezpečnostní opatření potřebná pro bezpečné používání mobilních zařízení, příp. i bezpečnostní opatření spojená s využitím technických zařízení, kterými společnost nedisponuje.
nerelevantní	

Bezpečnostní politika řízení přístupu není definována. Bezpečnost používání mobilních přístrojů není pro společnost relevantní.

Tato oblast je však poměrně pokryta, kdy je řízen přístup k systémům a informacím, každý uživatel má své jednoznačné autentizační údaje a používá se i autentizační server. Nástroje pro řízení přístupových oprávnění jsou používány a přidělování administrátorských oprávnění je omezené.

2.5.9 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	Není dodržována lhůta pro povinnou výměnu hesla.

Ověřování identity uživatelů	Délka hesla u administrátorů min. 15 znaků (za uplatnění ostatních předchozích pravidel).
neaplikováno	

Ověřování identity uživatelů	Použita vícefaktorová autentizace.
částečně aplikováno	Neimplementováno řešení SSO, vícefaktorová autentizace. Použita jen u některých aplikací.

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.
aplikováno	

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

Hesla nedosahují požadované délky a složitosti a jejich lhůta pro výměnu není plněna. Vícefaktorová autentizace je využívána jen u některých aplikací.

Použití již užívaných hesel je zamezeno a nástroj pro automatické odhlašování v nečinnosti se také užívá.

2.5.10 Řízení přístupových oprávnění

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

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

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	

Nástroje pro řízení přístupových oprávnění jsou používány, stejně tak je tomu u nástroje pro logování přístupů.

2.5.11 Akvizice, vývoj a údržba

Akvizice, vývoj a údržba	Jsou stanoveny bezpečnostní požadavky na změny ICT spojené s jejich akvizicí, vývojem a údržbou a jsou zahrnuty do projektu akvizice, vývoje a údržby systému.
neaplikováno	

Akvizice, vývoj a údržba	Jsou identifikovány, hodnoceny a řízeny rizika související s akvizicí, vývojem a údržbou systémů.
neaplikováno	

Akvizice, vývoj a údržba	Je zajištěna bezpečnost vývojového prostředí a zároveň je zajištěna ochrana používaných testovacích dat.
částečně aplikováno	Vývojové prostředí není dostatečně zabezpečeno (např. není v samostatném segmentu sítě).

Akvizice, vývoj a údržba	Je prováděno bezpečnostní testování změn systémů před jejich zavedením do provozu.
neaplikováno	

Společnost nemá stanoveny požadavky na akvizice. Neprobíhá žádná identifikace, hodnocení, řízení rizik a testování změn systémů v souvislosti s akvizicemi. Vývojové prostředí se nachází v totožném segmentu sítě.

2.5.12 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	

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

Bezpečnostní testy zranitelnosti aplikací se neprovádí je však zajištěna jejich ochrana před neoprávněnou činností, kompromitací nebo neautorizovanou změnou. Transakce jsou zajištěny před jejich kompromitací, špatným směrováním nebo nedokončením.

2.5.13 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	U některých nástrojů nejsou aktuální odolné algoritmy podporovány.

Přihlašování k serveru je zajištěno autentizačním certifikátem, který ověřuje totožnost. Ověřování probíhá pouze na zařízeních od Microsoft, mobilní zařízení se certifikátem

neověřují. Společnost používá VPN používanou na protokolu TLS, přes kterou se připojují na server. Protokol využívá k zabezpečení kryptografických klíčů a algoritmů.

Společnost v oblasti kryptografie plní pouze z části jeden požadavek.

2.5.14 Zajištění dostupnosti

Zajištění dostupnosti	V souladu s bezpečnostními potřebami a výsledky hodnocení rizik je zajištěna potřebná úroveň dostupnosti informací.
částečně aplikováno	V současnosti není zohledněno hodnocení rizik, není prováděno.

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

Zajištění dostupnosti	Zajištěna odolnost systémů vůči kybernetickým bezpečno–stním incidentům, které by mohly snížit dostupnost.
částečně aplikováno	Netestováno, přiměřeně zohledňováno „best practices“.

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

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

Systémy se při zajištění odolnosti vůči kybernetickým útokům řídí „best practices“. Zálohování důležitých technických aktiv funguje za pomocí redundance a zajištěním náhradních technických aktiv.

2.5.15 Bezpečnost ICS/SCADA

ICS/SCADA	Zajištěno omezení fyzického přístupu k síti a zařízením průmyslových a řídících systémů.
nerelevantní	

ICS/SCADA	Zajištěno omezení propojení a vzdáleného přístupu k síti průmyslových a řídících systémů.
nerelevantní	

ICS/SCADA	Zajištěna ochrana jednotlivých technických aktiv průmyslových a řídících systémů před využitím známých zranitelností.
nerelevantní	

ICS/SCADA	Zajištěno obnovení chodu průmyslových a řídících systémů po kybernetickém bezpečnostním incidentu
nerelevantní	

Oblast bezpečnosti průmyslových ICS/SCADA není pro společnost relevantní.

2.5.16 Fyzická bezpečnost

Fyzická bezpečnost	Bezpečnostní politika: Fyzická bezpečnost.
neaplikováno	

Fyzická bezpečnost	Jsou přijata nezbytná opatření k zamezení neoprávněnému vstupu do vymezených prostor, kde jsou zpracovávány informace a umístěna technická aktiva.
aplikováno	

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.
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 nemá zavedenou politiku, avšak jsou přijata nezbytná opatření k neoprávněnému vstupu do vymezených prostor (např. serverovna). Další opatření se týkají zamezení poškození a krádeži informací a technických aktiv. Pro tento účel jsou instalovány různé možnosti ochrany na úrovni objektů.

2.5.17 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	

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.
aplikováno	

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.
aplikováno	

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.
neaplikováno	

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.
aplikováno	

Ochrana integrity je řešena řízením bezpečného přístupu mezi vnější a vnitřní sítí. Této ochrany je docíleno za pomocí segmentace sítě a použitím tzv. demilitarizovaných zón. Pro ochranu integrity rozhraní vnější komunikační sítě se používají kryptografické prostředky pro vzdálený přístup, správu nebo přístup pomocí bezdrátových technologií.

2.5.18 Log management

Log management	Je používán nástroj pro zaznamenávání činností ICT, který zajišťuje: Sběr informací o provozních a bezpečnostních činnostech, zejména typ činnosti, datum a čas, identifikaci technického aktiva, které činnost zaznamenalo, identifikaci původce a místa činnosti a úspěšnost nebo neúspěšnost činnosti.
aplikováno	

Log management	Je používán nástroj pro zaznamenávání činností informačního/komunikačního systému, který zajišťuje: Ochranu získaných informací před neoprávněným čtením nebo změnou.
částečně aplikováno	Aplikován pouze pro některé činnosti.

Log management	Pomocí nástroje pro zaznamenávání činnosti informačního/komunikačního systému je zaznamenáváno(y): Přihlášení a odhlášení uživatelů a administrátorů.
aplikováno	

Log management	Pomocí nástroje pro zaznamenávání činnosti informačního/komunikačního systému je zaznamenáváno(y): Činnosti provedené administrátory.
aplikováno	

Log management	Pomocí nástroje pro zaznamenávání činnosti informačního/komunikačního systému je zaznamenáváno(y):Činnosti vedoucí ke změně přístupových oprávnění.
aplikováno	

Log management	Pomocí nástroje pro zaznamenávání činnosti informačního/komunikačního systému je zaznamenáváno(y): Neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů.
aplikováno	

Log management	Pomocí nástroje pro zaznamenávání činnosti informačního/komunikačního systému je zaznamenáváno(y): Zahájení a ukončení činností technických aktiv.
aplikováno	

Log management	Pomocí nástroje pro zaznamenávání činnosti informačního/komunikačního systému je zaznamenáváno(y): Automatická varovná nebo chybová hlášení technických aktiv
aplikováno	

Log management	Pomocí nástroje pro zaznamenávání činnosti informačního/komunikačního systému je zaznamenáváno(y): Přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností.
částečně aplikováno	Aplikováno pouze pro některé činnosti.

Log management	Pomocí nástroje pro zaznamenávání činnosti informačního/komunikačního systému je zaznamenáváno(y): Automatická varovná nebo chybová hlášení technických aktiv
aplikováno	

Log management	Nejméně jednou za 24 hodin je prováděna synchronizace jednotného systémového času technických aktiv.
částečně aplikováno	Není formalizováno.

Log management	Záznamy činností (logy) jsou uchovávány nejméně po dobu 3 měsíců.
částečně aplikováno	Není formalizováno.

Společnost používá se nástroje ke sběru informací o provozních a bezpečnostních činnostech. Zaznamenává se přihlašování odhlašování administrátorů, činnosti, které provedli a činnosti které vedli ke změně přístupových oprávnění. Monitorují se také neúspěšné pokusy o činnosti v důsledku nedostatečných oprávnění. Pod drobnohledem jsou také technická aktiva, kdy se monitoruje jejich zahájení a ukončení činnosti. V neposlední řadě jsou zaznamenávány varovná nebo chybové hlášení.

V případě nutnosti jsou některé logy uchovávány déle než tři měsíce.

2.5.19 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	

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

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

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

Politiky ochrany před škodlivým kódem nejsou společností specifikovány. Nástroje pro ochranu jsou však používány zejména pro: komunikaci mezi vnitřní a vnější sítí, kontrolu serverů a datových úložišť, pracovních stanic. Zmíněné nástroje pro uplatnění ochrany před škodlivým kódem jsou pravidelně aktualizovány.

2.5.20 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.
neaplikováno	

Detekce kybernetických bezpečnostních událostí	Je používán nástroj pro detekci kybernetických bezpečnostních událostí, který zajistí ověření, kontrolu a případně zablokování komunikace serverů.
částečně aplikováno	Aplikováno pouze v omezené míře, řešeno aplikačně na úrovni některých stanic a serverů.

Kybernetické bezpečnostní události jsou detekovány, pouze na úrovni některých pracovních stanic a serverů. Události na jiných úrovních detekovány nejsou.

2.5.21 SIEM

SIEM	Bezpečnostní politika: Využití a údržba nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí (SIEM).
neaplikováno	

SIEM	Je používán nástroj typu SIEM (nástroj pro sběr a průběžné vyhodnocení kybernetických bezpečnostních událostí, který v souladu s bezpečnostními potřebami a výsledky hodnocení rizik zajišťuje: Integrovaný sběr a vyhodnocení kybernetických bezpečnostních událostí).
neaplikováno	

SIEM	Je používán nástroj pro sběr a průběžné vyhodnocení kybernetických bezpečnostních událostí, který v souladu s bezpečnostními potřebami a výsledky hodnocení rizik zajišťuje poskytování informací pro určené bezpečnostní role o detekovaných kybernetických bezpečnostních událostech.
neaplikováno	

SIEM	Je používán nástroj pro sběr a průběžné vyhodnocení kybernetických bezpečnostních událostí, který v souladu s bezpečnostními potřebami a výsledky hodnocení rizik zajišťuje nepřetržité vyhodnocování kybernetických bezpečnostních událostí s cílem identifikace kybernetických bezpečnostních incidentů, včetně včasného varování určených bezpečnostních rolí.
neaplikováno	

SIEM	Je zajištěna pravidelná aktualizace nastavení pravidel pro vyhodnocování kybernetických bezpečnostních událostí a včasné varování, aby byly omezovány případy nesprávného vyhodnocení událostí nebo případy falešných varování.
neaplikováno	

SIEM	Zajištěno využívání informací, které jsou připraveny nástrojem pro sběr a vyhodnocení kybernetických bezpečnostních událostí, pro optimální nastavení bezpečnostních opatření.
neaplikováno	

Nástroj SIEM pro sběr a vyhodnocování kybernetických bezpečnostních událostí nemá společnost zaveden.

2.5.22 Incident handling

Incident handling	Jsou přijata nezbytná opatření, která zajistí oznamování kybernetických bezpečnostních událostí ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a o oznámeních jsou vedeny záznamy.
aplikováno	

Incident handling	Oznámené incidenty jsou vyhodnocovány/evidovány/řešeny.
aplikováno	

Incident handling	Je prováděna klasifikace kybernetických bezpečnostních incidentů, přijímáno opatření pro odvrácení a zmírnění dopadu kybernetického bezpečnostního incidentu a je zajištěn sběr věrohodných podkladů potřebných pro analýzu kybernetického bezpečnostního incidentu.
aplikováno	

Incident handling	Jsou prošetřeny a určeny příčiny kybernetického bezpečnostního incidentu, vyhodnocena účinnost řešení kybernetického bezpečnostního incidentu a na základě vyhodnocení jsou stanovena nutná bezpečnostní opatření k zamezení opakování řešeného kybernetického bezpečnostního incidentu.
aplikováno	

Incident handling	Zvládání kybernetických bezpečnostních incidentů je dokumentováno.
neaplikováno	

Incident handling	Povinnost hlásit kybernetické bezpečnostní incidenty a to bezodkladně po jejich detekci Národnímu bezpečnostnímu úřadu (Vládnímu CERT týmu).
nerelevantní	

Existují opatření, které oznamují kybernetické bezpečnostní události ze stran uživatelů nebo administrátorů, o těchto jsou vedeny záznamy a evidence. Bezpečnostní incidenty podléhají klasifikaci, kdy dojde k přijmutí opatření pro odvrácení nebo zmírnění dopadu kybernetického bezpečnostního incidentu. Incidenty tohoto charakteru jsou sbírány a následně jsou vyhodnocovány jejich příčiny a také účinnosti řešení, na základě kterých by mělo dojít k zamezení opakování kybernetického bezpečnostního incidentu. Dokumentace se nesestavuje a povinnost hlásit kybernetické bezpečnostní incidenty Národnímu bezpečnostnímu úřadu (NBÚ) není pro společnost relevantní.

2.5.23 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)).
částečně aplikováno	Neformalizováno.

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).
částečně aplikováno	Neformalizováno.

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

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

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	

Strategie řízení kontinuity činností není stanovena. Společnost neformalizuje minimální úrovně poskytovaných služeb přijatelných pro užívání. V rámci řízení kontinuity činností nejsou formalizovány bezpečnostní role. Neprobíhá vyhodnocování a dokumentování dopadů kybernetických bezpečnostních incidentů.

2.6 Rekapitulace plnění

Analýza současného stavu odhalila, že společnost aktuálně plní 50 požadavků, částečně plní 45 požadavků, nesplňuje 60 požadavků a nerelevantní je pro ni 7 požadavků. Plnění je níže zobrazeno v přehledném 3-D koláčovém grafu.

Obrázek 9: Analýza vybraných oblastí – koláčový graf (Zdroj: Vlastní zpracování)

2.7 Souhrn analýzy oblastí k opatřením ISMS

V souvislosti s analýzou vybraných oblastí je vytvořena tabulka obsahující plnění jednotlivých opatření ISMS. V rámci tabulky je vyznačeno, zda společnost daná opatření plní nebo nikoliv. Opatření mohou nabývat stavů, rovněž jako u předchozí analýzy – aplikováno, částečně aplikováno, neaplikováno a nerelevantní. Tato opatření jsou převzata z normy ČSN ISO/IEC 27002.

Tabulka 6: Analýza vybraných oblastí - převod na opatření dle ISMS (Zdroj: Vlastní zpracování)

A.5 Politiky bezpečnosti informací	
A.5.1 Pokyny managementu organizace k bezpečnosti informací	
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	**Nerelevantní**
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	**Aplikováno**
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	**Částečně**
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	**Neaplikováno**
A.9.1.2 Přístup k sítím a síťovým službám	**Aplikováno**
A.9.2 Řízení přístupu uživatelů	
A.9.2.1 Registrace a zrušení registrace uživatele	**Aplikováno**
A.9.2.2 Správa uživatelských přístupů	**Částečně**
A.9.2.3 Správa privilegovaných přístupových práv	**Aplikováno**
A.9.2.4 Správa tajných autentizačních informací uživatelů	**Aplikováno**
A.9.2.5 Přezkoumání přístupových práv uživatelů	**Částečně**
A.9.2.6 Odebrání nebo úprava přístupových práv	**Aplikováno**
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	**Aplikováno**
A.9.4.2 Bezpečné postupy přihlášení	**Aplikováno**
A.9.4.3 Systém správy hesel	**Aplikováno**
A.9.4.4 Použití privilegovaných programových nástrojů	**Částečně**
A.9.4.5 Řízení přístupu ke zdrojovým kódům programů	**Částečně**

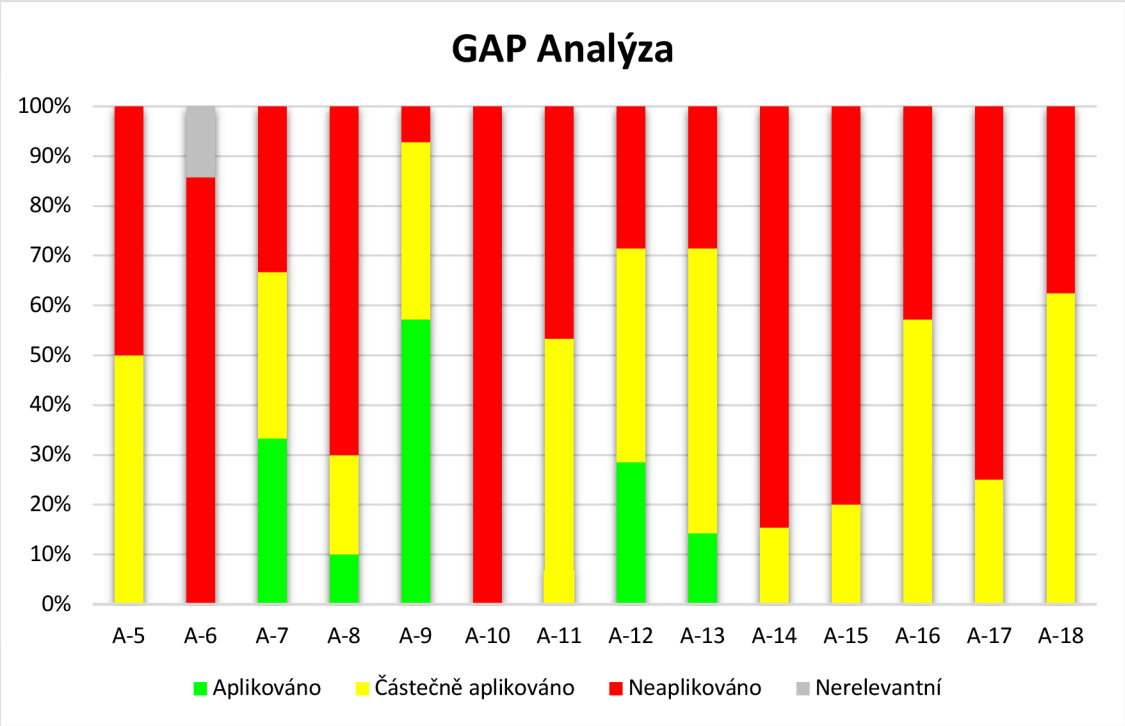
A.10 Kryptografie	
A.10.1 Kryptografická opatření	
A.10.1.1 Politika pro použití kryptografických opatření	**Neaplikováno**
A.10.1.2 Správa klíčů	**Neaplikováno**
A.11 Fyzická bezpečnost a bezpečnost prostředí	
A.11.1 Bezpečné oblasti	
A.11.1.1 Fyzický bezpečnostní perimetr	**Částečně**
A.11.1.2 Fyzické kontroly vstupu	**Částečně**
A.11.1.3 Zabezpečení kanceláří, místností a vybavení	**Částečně**
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	**Částečně**
A.11.2 Zařízení	
A.11.2.1 Umístění zařízení a jeho ochrana	**Částečně**
A.11.2.2 Podpůrné služby	**Částečně**
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	**Aplikováno**
A.12.4.2 Ochrana logů	**Částečně**
A.12.4.3 Logy o činnosti administrátorů a operátorů	**Aplikováno**
A.12.4.4 Synchronizace hodin	**Částečně**
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	**Částečně**
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	
A.14.1 Bezpečnostní požadavky informačních systémů	
A.14.1.1 Analýza a specifikace požadavků bezpečnosti informací	**Neaplikováno**
A.14.1.2 Zabezpečení aplikačních služeb ve veřejných sítích	**Neaplikováno**
A.14.1.3 Ochrana transakcí aplikačních služeb	**Částečně**
A.14.2 Bezpečnost v procesech vývoje a podpory	
A.14.2.1 Politika bezpečného vývoje	**Neaplikováno**
A.14.2.2 Postupy řízení změn systémů	**Neaplikováno**
A.14.2.3 Technické přezkoumání aplikací po změnách platformy	**Neaplikováno**
A.14.2.4 Omezení změn softwarových balíků	**Neaplikováno**
A.14.2.5 Principy inženýrství bezpečných systémů	**Neaplikováno**
A.14.2.6 Bezpečné vývojové prostředí	**Částečně**
A.14.2.7 Vývoj zajišťovaný externími zdroji	**Neaplikováno**
A.14.2.8 Testování bezpečnosti systémů	**Neaplikováno**
A.14.2.9 Testování akceptace systému	**Neaplikováno**
A.14.3 Data pro testování	
A.14.3.1 Ochrana dat pro testování	**Neaplikováno**
A.15 Vztahy s dodavateli	
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	**Částečně**
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	**Částečně**
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	**Částečně**
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**

2.8 GAP analýza úrovně shody s ISMS

Z obrázku č. 10 lze vyvodit, že společnost nemá v některých oblastech schváleny bezpečnostní politiky, např. oblast A-10, kde je neaplikováno zastoupeno 100%. Podobně je to však hned v několika dalších oblastech opět z důvodu nedostatku implementace bezpečnostních politik. Větší zastoupení má i částečně aplikováno společnost v mnoha oblastech bezpečnostní politiky alespoň rozpracovala, ale kromě oblasti A-9 nejsou nikde implementovány ve větší míře.



Obrázek 10: GAP analýza ISMS – sloupcový graf (Zdroj: Vlastní zpracování)

2.9 Požadavky společnosti

Společnost plánuje zavést ISMS kvůli požadavkům investora a zákazníků. Přestože společnost používá nástroje pro ochranu před škodlivým kódem, tak si přeje zvýšit úroveň bezpečnosti. Proti společnosti byl v minulosti veden útok ransomwarem. V souvislosti s tímto bezpečnostním incidentem se společnost rozhodla jednat a tudíž je požadavkem zabezpečení pracovních stanic šifrováním. Především jde tedy o stolní počítače a notebooky. Dalším požadavkem je zavedení systematického řešení řízení rizik, návrh zabezpečení aktivních prvků a ustanovení politik řízení lidských zdrojů.

2.10 Nedostatky nalezené v oblastech

Analýza vybraných oblastí upozornila na některé nedostatky a rizika z hlediska bezpečnosti organizace. Společnost nemá v mnoha oblastech zavedeny či formalizovány bezpečnostní politiky. Audity provádí jen nepravidelně a penetrační testy se neprovádí vůbec. Penetrační testování může společnosti sloužit jako podrobná analýza systému, která odhalí nedostatky plynoucí ze špatného nastavení systému či hardwarových a softwarových nedostatků nebo nedostatečně funkčních opatření. Mezi další nedostatky

patří nedostatečná evidence, identifikace aktiv, hrozeb, zranitelností a absence procesu řízení rizik. Řízení rizik je řešeno pouze jednotlivými oblastmi, např. oblast analýzy rizik, která však nebyla dostatečná. Organizační bezpečnost není ustanovena a nejsou určeny bezpečnostní role. Školení neprobíhají na pravidelné bázi. S tím souvisí i to, že pracovníci nemění svá hesla v daných intervalech nebo nedosahují stanovené délky. Pracovníci v některých odděleních si zapisují svá hesla na papírky apod. Prvky kryptografické ochrany jsou zavedeny částečně a to pouze na úrovni vzdáleného přístupu. Společnost detekuje kybernetické bezpečnostní události pouze na úrovni pracovních stanic a serverů.

3 NÁVRH ŘEŠENÍ

Návrhová část práce je věnována rozsáhlé analýze, vyhodnocení a zvládání rizik společnosti. Nejprve jsou identifikovány a ohodnoceny aktiva, poté určeny hrozby a jejich pravděpodobnosti. Jednotlivým aktivům je přiřazena zranitelnost a následně jsou vypočteny úrovně všech rizik. Rizika jsou zařazena do seznamů podle úrovně a pro vybraná rizika jsou navrhnuta bezpečnostní opatření. Po navrhnutí opatření je sestaven časový plán implementace a ekonomické zhodnocení.

3.1 Rozsah a hranice ISMS

V prvé řadě je nutno zmínit, že náplň této práce není věnována zavádění ISMS v plném rozsahu. Diplomová práce svým záběrem neumožňuje zohlednit veškeré oblasti.

Společnost XYZ v dohledné době neplánuje zavádět ISMS v plném rozsahu a to platí i v případě certifikace ISMS. Řešeny budou z pohledu rozsahu jen vybrané části, přičemž jako primární zaměření práce jsou zvolena navržení bezpečnostních opatření vycházející z analýzy rizik a také požadavků společnosti.

3.2 Analýza rizik

Nejprve se zpracuje analýza rizik, identifikují se a ohodnotí aktiva. V návaznosti identifikuji hrozby a zranitelnosti. Shrnutím výsledků je matice úrovní rizik a zhodnocení analýzy rizik.

3.2.1 Identifikace a ohodnocení aktiv společnosti

V prvé řade je třeba aktiva identifikovat. Existuje několik způsobů jak dělit aktiva. V této práci je vybrán standardní způsob, který rozřazuje aktiva do čtyř skupin: informační, hardwarová, softwarová a služby. V této části se běžně identifikují vlastníci aktiva, ale pro účel této práce a vzhledem k požadavku společnosti nebýt jmenována nebudou tyto informace zveřejněny.

Všechny tabulky jsou členěny dle úrovní na: Nízká – **N**, Střední – **S**, Vysoká – **V**, Kritická – **K**. Pokud počítáme hodnotu aktiva, je třeba převést označení na číselnou hodnotu, kdy N = 1; S = 2; V = 3; K = 4;

Každé aktivum se hodnotí podle nákladů. Zmíněné náklady vznikají z důvodu porušení hlavních atributů CIA (důvěrnost, integrita, dostupnost).

Následující tabulky stupnic jsou upraveny a převzaty z vyhlášky č.82/2018 Sb. [13].

Tabulka 7: Klasifikační stupnice pro hodnocení důvěrnosti aktiv (Zdroj: Vlastní zpracování dle [13])

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy povinné osoby.	Není vyžadována žádná ochrana. Likvidace/mazání aktiva na úrovni Nízká
Střední	Aktiva nejsou veřejně přístupná a tvoří know-how organizace, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním.	Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu. Likvidace/mazání aktiva na úrovni Střední
Vysoká	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (například obchodní tajemství, osobní údaje).	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací komunikační sítí jsou chráněny pomocí kryptografických prostředků. Likvidace/mazání aktiva na úrovni Vysoká
Kritická	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické obchodní tajemství, zvláštní kategorie osobních údajů).	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Dále metody ochrany zabraňující zneužití aktiv ze strany administrátorů. Přenosy informací jsou chráněny pomocí kryptografických prostředků. Likvidace/mazání aktiva na úrovni Kritická

Tabulka 8: Klasifikační stupnice pro hodnocení integrity aktiv (Zdroj: Vlastní zpracování dle [13])

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy povinné osoby.	Není vyžadována žádná ochrana.
Střední	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů organizace a může se projevit méně závažnými dopady na aktiva.	Pro ochranu integrity jsou využívány standardní nástroje (například omezení přístupových práv pro zápis).
Vysoká	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů organizace s podstatnými dopady na aktiva.	Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených komunikačními sítěmi je zajištěna pomocí kryptografických prostředků.
Kritická	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů organizace s přímými a velmi vážnými dopady na aktiva.	Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (například pomocí technologie digitálního podpisu).

Tabulka 9: Klasifikační stupnice pro hodnocení dostupnosti aktiv (Zdroj: Vlastní zpracování dle [13])

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).	Pro ochranu dostupnosti je postačující pravidelné zálohování.
Střední	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů organizace.	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.
Vysoká	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů organizace. Aktiva jsou považována za velmi důležitá.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.
Kritická	Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů organizace. Aktiva jsou považována za kritická.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.

Pro výpočet hodnoty aktiva je zvolen algoritmus součtu:

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

Pro atributy uvedené ve vzorci (důvěrnost, integrita, dostupnost), platí stejná stupnice (nízká, střední, vysoká, kritická) jako v tabulce č. 7.

Tabulka 10: Identifikace a ohodnocení aktiv (Zdroj: Vlastní zpracování)

Typ	Klasifikace	Aktivum (A)	Zdroj	C	I	A	HA
INFORMAČNÍ AKTIVA	Veřejná	Nabídkové katalogy	*e-shop*	N	S	S	2
		Informace na webu	*server*	N	N	S	1
	Interní	Cenové nabídky	*e-shop*	V	V	V	3
		Dokumentace	*server*	V	V	V	3
		Interní postupy	*server*	V	V	S	3
		Záloha dat	*server*	K	K	K	4
			cloud	K	V	V	3
			IP kamera	V	S	N	2
	Důvěrná	Data o zákaznících	*e-shop, CRM*	K	K	K	4
		Data o zaměstnancích	*server*	K	V	V	3
		Nahrávky hovorů	*server*	K	K	V	4
		Obchodní tajemství	*server*	K	K	S	3
HARDWAROVÁ AKTIVA	Firewall			K	K	K	4
	Pasivní síťové prvky		*rozvaděč, kabeláž*	K	K	K	4
	Aktivní síťové prvky		*router, switch*	K	K	K	4
	Mobilní zařízení			S	S	S	2
	IP kamery			V	V	V	3
	Pracovní stanice			V	S	S	2
	IBM Server			K	K	K	4
	Notebooky			V	S	S	2
SOFTWAROVÁ AKTIVA	Operační systémy		*server*	K	K	K	4
			prac. stanice,	V	S	S	2
	Spamový filtr		*server*	S	S	N	2
	MS SQL databáze		*server*	K	K	K	4
	MS Dynamics CRM		*server*	K	K	K	4
	Antivir			K	K	K	4
	Software IP kamer			V	V	N	2
	VPN klient			V	V	V	3
	MS Exchange server		*server*	K	K	K	4
SLUŽBY	Doménové služby		*server*	K	N	N	2
	E-shop		*poskytovatel*	V	V	V	3
	Webové stránky		*poskytovatel*	S	N	S	2
	VPN připojení		*VPN klient*	V	V	V	3
	Internet			V	V	V	3
	Zálohy		*MS OneDrive*	K	V	V	3
	Elektrická energie			V	V	K	3

Tabulka 10 obsahuje označení sloupců písmeny **C** – důvěrnost, **I** – integrita, **A** – dostupnost, značení bylo použito především k úspoře místa a zobrazení tabulky v plné velikosti. Poslední sloupec, jenž je označen písmenem **HA** – hodnota aktiva zobrazuje průměr hodnot v předchozích třech sloupcích.

Identifikace a ohodnocení aktiv prokázalo, že aktiva s největší hodnotou bývají umístěna na serveru. V tomto umístění najdeme většinu informačních aktiv (data o zákaznících, cenové nabídky). Mnoho hodnot se stupněm 4 je ale i v kategorii hardwarových aktiv (aktivní a pasivní prvky sítě). V softwarových aktivech nalezneme také pár nejvyšších stupňů a opět jde prvky umístěné na serveru (operační systém, antivirový software). Kategorie služeb obsahuje několik prvků z kategorie vážné potíže a velké ztráty (elektrická energie, VPN připojení).

Tabulka identifikace a příslušného ohodnocení aktiv byla vytvořena po konzultaci s vedoucím IT oddělení.

3.2.2 Identifikace a ohodnocení hrozeb s příklady zranitelnosti

Stejně jako v předchozí podkapitole je třeba nejprve identifikovat hrozby. Tyto hrozby disponují vlastnostmi, které mohou poškodit aktiva společnosti. Hrozbám je přidělena pravděpodobnost a pro příklad uvedena zranitelnost. Pro lepší představivost je vedle doplněn i konkrétní př. dané hrozby. Tato kapitola obsahuje identifikace hrozeb a stupeň pravděpodobnosti výskytu. Dále jsou uvedeny př. zranitelnosti v přehledné tabulce.

Tabulka stupnice je upravena a převzata z vyhlášky č.82/2018 Sb. [13].

Kritérium vzniku hrozby opět nabývá stavů (nízká, střední, vysoká, kritická) dle následující stupnice:

Tabulka 11: Klasifikační stupnice pravděpodobnosti vzniku hrozeb (Zdroj: Vlastní zprac. dle [13])

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.

Tabulka 10 identifikující hrozby je vytvořena v souladu s normou ČSN ISO/IEC 27005 [12].

Tabulka 12: Identifikace hrozeb (Zdroj: Vlastní zpracování dle [12])

Typ	Hrozba (T)
FYZICKÉ POŠKOZENÍ	Požár
	Poškození vodou
	Zničení zařízení nebo médií
PŘÍRODNÍ UDÁLOST	Povodeň
ZTRÁTA ZÁKLADNÍCH SLUŽEB	Selhání klimatizace nebo dodávky vody
	Přerušení dodávky elektřiny
	Selhání telekomunikačních zařízení
OHROŽENÍ INFORMACÍ	Vzdálená špionáž
	Odposlech
	Krádež médií nebo dokumentů
	Krádež zařízení
	Vyzrazení
	Data pocházející z nedůvěryhodných zdrojů
	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 13: Identifikované hrozby s pravděpodobností a příkladem zranitelnosti (Zdroj: Vlastní zpracování)

Hrozba (T)	SP	Příklad zranitelnosti
Požár	N	Manipulace s hořlavinami
Poškození vodou	N	Manipulace s vodou
Zničení zařízení nebo médií	S	Nedodržování pravidelných výměn
Povodeň	N	Poloha společnosti v zátopové oblasti
Selhání klimat. nebo dodávky vody	N	Silné změny teploty
Přerušení dodávky elektřiny	S	Citlivost na změny napětí
Selhání telekomunikačních zařízení	V	Komunikace uskutečňována převážně online
Vzdálená špionáž	N	Nedostatečná bezpečnost síťové infrastruktury
Odposlech	N	Nedostatečná ochrana komunikační linky
Krádež médií nebo dokumentů	S	Nedostatečná fyzická bezpečnost budov, oken atd.
Krádež zařízení	V	Nedostatečná ochrana zařízení
Vyzrazení	K	Nedostatečné postupy při výběru pracovníků
Data pocházející z nedův. zdrojů	V	Není řízeno odkud je povoleno získávat data
Falšování pomocí apli. prog. vybav.	V	Stahování a užívání nebezpečných programů
Odhalení pozice	S	Nedostatečná bezpečnost mobilních telefonů
Selhání zařízení	S	Nedostatky kontinuitních plánů
Chybné fungování zařízení	S	Neprovádění údržby zařízení
Chybné fungování aplikačního programového vybavení	S	Neaktualizovaná nebo nová aplikace
Chyba údržby	S	Nepravidelná údržba
Neoprávněné použití zařízení	S	Nedostatečná bezpečnost připojení do veřejné sítě
Podvodné kopírování aplikačního programového zařízení	N	Nedostatky v log managementu
Použití padělaného nebo zkopírovaného prog. vybavení	N	Nedostatečné postupy v aplikování souladu se zákony na ochranu duševního vlastnictví
Poškození dat	N	Velmi rozšířené programy
Nezákonné zpracování dat	N	Užívání nepotřebných služeb
Chyba používání	S	Nedostatek bezpečnostního podvědomí
Zneužití oprávnění	V	Neodhlášení se při odchodu od pracovní stanice
Odepření činnosti	S	Nedostatečná delegace odpovědnosti za bezpečnost informací
Nedostatek personálu	V	Nedostatky a nedbalosti při kontrole fyzického přístupu do budovy a kanceláří, recruiting pracov.

Sloupec, který je popsán písmeny **SP** označuje stupeň pravděpodobnosti vzniku hrozby.

3.2.3 Matice zranitelnosti

Matice zranitelnosti zobrazuje pravděpodobnost hrozby ve vzájemném vztahu s hodnotou aktiva. Určení zranitelnosti probíhá dle odhadu na slabé místo aktiva. Klasifikační stupnice vytvořená níže pojednává o zmíněných odhadech. Stupnice je opět členěna do úrovní: nízká, střední, vysoká, kritická.

Stupnice zranitelnosti je upravena a převzata z vyhlášky č.82/2018 Sb. [13].

Tabulka 14: Klasifikační stupnice pro zranitelnost (Zdroj: Vlastní zpracování dle [13])

Úroveň	Popis
Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Jsou zavedena bezpečnostní opatření, která jsou schopna včas detekovat možné zranitelnosti nebo případné pokusy o jejich zneužití.
Střední	Zneužití zranitelnosti je málo pravděpodobné až pravděpodobné. Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.
Vysoká	Zneužití zranitelnosti je pravděpodobné až velmi pravděpodobné. Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
Kritická	Zneužití zranitelnosti je velmi pravděpodobné až víceméně jisté. Bezpečnostní opatření nejsou realizována nebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.

Matice zranitelnosti přesahuje potřebné rozměry, aby mohla být vložena do textu práce, z toho důvodu je vytvořena příloha 1. Pro ukázku je na následující straně alespoň její část s vyhodnocením informačních aktiv.

Tabulka 15: Matice zranitelnosti (Zdroj: Vlastní zpracování)

Zranitelnost [V]		INFORMAČNÍ AKTIVA											
	Zdroj	*e-shop*	*server*	*e-shop*	*server*	*server*	*server*	*cloud*	*IP kamera*	*e-shop, CRM*	*server*	*server*	*server*
	Aktivum	**Veřej**		**Interní**						**Důvěrná**			
		Nabídkové katalogy	Informace na webu	Cenové nabídky	Dokumentace	Interní postupy	Zálohy dat			Data o zákaznících	Data o zaměstnancích	Nahrávky hovorů	Obchodní tajemství
	A	2	1	3	3	3	4	3	2	4	4	4	3
Hrozba	**T**												
Požár	N												
Poškození vodou	N												
Zničení zařízení nebo médií	S												
Povodeň	N												
Selhání klimatizace nebo dodávky	N												
Přerušení dodávky elektřiny	S	V	V	V	V	V	N	S	N	V	V	V	V
Selhání telekomunikačních zařízení	V	V	V	V	V	V	V	S		V	V	V	V
Vzdálená špionáž	N			V	V	V	V	V	N	V	V	V	V
Odposlech	N											V	
Krádež médií nebo dokumentů	S				V	V	N	N	N	V	N	V	V
Krádež zařízení	V												
Vyzrazení	K				V	V	S			S	S	V	V
Data pocházející z nedůvěryhodných	V												
Falšování pomocí aplikačního prog.	V						N	N	N				
Odhalení pozice	S												
Selhání zařízení	S												
Chybné fungování zařízení	S												
Chybné fungování aplikačního prog.	S												
Chyba údržby	S												
Neoprávněné použití zařízení	S												
Podvodné kopírování aplikačního prog.	N												
Použití padělaného nebo	N												
Poškození dat	N	S	S	S	S	S	S	S	S	S	S	S	S
Nezákonné zpracování dat	N	S	S	S	S	S	S	S	S	S	S	S	S
Chyba používání	S	S	S	S	S	S	S	S	N	S	S	S	S
Zneužití oprávnění	V	S	S	S	S	S	S	S	N	S	S	S	S
Odepření činnosti	S												
Nedostatek personálu	V												

3.2.4 Matice úrovní rizik

Po již provedeném ohodnocení aktiv, určení pravděpodobnosti hrozeb a zranitelnosti aktiva je třeba vypočítat úroveň rizika – **R**. Hodnotu úrovně rizika vypočteme dosazením všech tří parametrů do tabulky, kterou představuje tabulka č. 18. V závislosti na hodnotách každého z parametrů mohou vyjít hodnoty na stupnici **0-10**.

Hodnocení úrovní rizika, je vyobrazeno na této stupnici:

Tabulka 16: Klasifikační stupnice pro úroveň rizika (Zdroj: Vlastní zpracování dle [16])

Hodnota	Úroveň	Popis
1-3	Nízké	Riziko je považováno za přijatelné.
4-6	Střední	Zneužití zranitelnosti je málo pravděpodobné až pravděpodobné. Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.
7-8	Vysoké	Zneužití zranitelnosti je pravděpodobné až velmi pravděpodobné. Bezpečnostní opatření jsou zavedena, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
9-10	Kritické	Zneužití zranitelnosti je velmi pravděpodobné až víceméně jisté. Bezpečnostní opatření nejsou realizována nebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.

Při výpočtu úrovně rizika jsem vycházel z metodiky analýzy rizik. Aktiva, hrozby a zranitelnosti se všechny nacházejí v jedné tabulce a máme-li všechny tři potřebné parametry je možno určit úroveň rizika.

Tabulka 17: Klasifikační stupnice úrovně rizika (Zdroj: Vlastní zpracování dle [16])

	Úroveň hrozby	N				S				V				K			
	Úroveň zranitelnosti	N	S	V	K	N	S	V	K	N	S	V	K	N	S	V	K
Hodnota Aktiva	1	1	2	3	4	2	3	4	5	3	4	5	6	4	5	6	7
	2	2	3	4	5	3	4	5	6	4	5	6	7	5	6	7	8
	3	3	4	5	6	4	5	6	7	5	6	7	8	6	7	8	9
	4	4	5	6	7	5	6	7	8	6	7	8	9	7	8	9	10

Ukázkový příklad výpočtu rizika:

Výpočet spočívá v součtu hodnoty aktiva, pravděpodobnosti hrozby a zranitelnosti aktiva a odečtení hodnoty 2.

Vzorec: **Riziko** = Aktivum (dopad) + Hrozba + Zranitelnost – 2

Tabulka 18: Výpočet úrovně rizika (Zdroj: Vlastní zpracování dle [16])

Popis	Název	A + T + V - 2 = R
Hodnota aktiva **A**	Dokumentace	3
Pravděpodobnost hrozby **T**	Krádež médií nebo dokumentů	2
Zranitelnost aktiva **V**	Nedostatečná fyzická bezpečnost budovy	3
Výpočet úrovně rizika **R**		3 + 2 + 3 - 2 = 6

Pro takto zadané parametry je tedy úroveň rizika **R** = 6. Z klasifikační stupnice v tabulce č. 17 určíme, že se jedná o střední úroveň rizika.

Matice úrovní rizika přesahuje potřebné rozměry, aby mohla být vložena do textu práce, z toho důvodu je vytvořena příloha 2. Pro ukázku je na následující straně alespoň její část s vyhodnocením informačních aktiv.

Tabulka 19: Matice úrovní rizik (Zdroj: Vlastní zpracování)

Úroveň rizika [R]		INFORMAČNÍ AKTIVA											
	Zdroj	*e-shop*	*server*	*e-shop*	*server*	*server*	*server*	*cloud*	*IP kamera*	*e-shop, CRM*	*server*	*server*	*server*
		Veřejn		Interní						Důvěrná			
	Aktivum	Nabídkové katalogy	Informace na webu	Cenové nabídky	Dokumentace	Interní postupy	Zálohy dat			Data o zákaznících	Data o zaměstnancích	Nahrávky hovorů	Obchodní tajemství
	A	2	1	3	3	3	4	3	2	4	4	4	3
Hrozba	**T**												
Požár	N												
Poškození vodou	N												
Zničení zařízení nebo médií	S												
Povodeň	N												
Selhání klimatizace nebo	N												
Přerušení dodávky elektřiny	S	5	4	6	6	6	5	5	3	7	7	7	6
Selhání telekomunikačních	V	6	5	7	7	7	8	6		8	8	8	7
Vzdálená špionáž	N			5	5	5	6	5	2	6	6	6	5
Odposlech	N											6	
Krádež médií nebo dokumentů	S				6	6	5	4	3	7	5	7	6
Krádež zařízení	V												
Vyzrazení	K				8	8	8			8	8	9	8
Data pocházející	V												
Falšování pomocí aplikačního	V						6	5	4				
Odhalení pozice	S												
Selhání zařízení	S												
Chybné fungování zařízení	S												
Chybné fungování aplikačního	S												
Chyba údržby	S												
Neoprávněné použití zařízení	S												
Podvodné kopírování	N												
Použití padělaného nebo	N												
Poškození dat	N	3	2	4	4	4	5	4	3	5	5	5	4
Nezákonné zpracování dat	N	3	2	4	4	4	5	4	3	5	5	5	4
Chyba používání	S	4	3	5	5	5	6	5	3	6	6	6	5
Zneužití oprávnění	V	5	4	6	6	6	7	6	4	7	7	7	6
Odepření činnosti	S												
Nedostatek personálu	V												

3.2.5 Vyhodnocení analýzy rizik

Rizika, která byla vyhodnocena jako kritická s hodnocením 9-10 jsou obsaženy tabulce č. 20:

Tabulka 20: Seznam rizik kritické úrovně (Zdroj: Vlastní zpracování)

Hrozba	Aktivum	Zdroj	Úroveň rizika
Vyzrazení	Nahrávky hovorů	*server*	9

Výstupem analýzy rizik je pouze jedno kritické riziko. Riziko se týká vyzrazení v případě důvěrných dat společnosti, mezi které patří hovory, které zaznamenává call-centrum. V tomto případě se jedná o důvěrná data, která by mohla být zneužita v případě zneužití lidským faktorem. Rizika nelze zcela eliminovat, nicméně existují možnosti jak ho alespoň snížit a mít více pod kontrolou. Z analýzy lze poznat, že většina důležitých uchovávána na serveru. Společnost se stará o zabezpečení serveru sama, z pravidla, tak nebývá zabezpečen natolik dobře jako při jeho umístění do data-centra. Zabezpečení serveru je tedy pro společnost jedna z priorit.

Do kategorie rizik s úrovní rizika vysoké patří rizika s hodnotou 7-8. Tabulka č. 20 obsahuje seznam rizik označených stupněm vysoká:

Tabulka 21: Seznam rizik vysoké úrovně – část 1 (Zdroj: Vlastní zpracování)

Hrozba	Aktivum	Zdroj	Úroveň rizika
Povodeň	Firewall	*server*	7
	Pasivní síťové prvky	*rozvaděč*	7
	Aktivní síťové prvky	*router*	7
Přerušení dodávky elektřiny	Data o zákaznících	*e-shop*	7
	Data o zaměstnancích	*server*	7
	Nahrávky hovorů	*server*	7
	Firewall	*server*	7
	Pasivní síťové prvky	*rozvaděč*	7
	Aktivní síťové prvky	*router*	7
	Elektrická energie		7
Selhání komunikačních zařízení	Cenové nabídky	*e-shop*	7
	Dokumentace	*server*	7
	Interní postupy	*server*	7
	Zálohy dat	*server*	8
	Data o zákaznících	*e-shop*	8
	Data o zaměstnancích	*server*	8
	Nahrávky hovorů	*server*	8
	Obchodní tajemství	*server*	7
	VPN připojení	*VPN klient*	7
	Internet		8

Tabulka 22: Seznam rizik vysoké úrovně – část 2 (Zdroj: Vlastní zpracování)

Hrozba	Aktivum	Zdroj	Úroveň rizika
Krádež médií nebo dokumentů	Data o zákaznících	*e-shop*	7
	Nahrávky hovorů	*server*	7
Krádež zařízení	Firewall	*server*	7
	Aktivní síťové prvky	*router*	7
	Mobilní zařízení		7
Vyzrazení	Cenové nabídky	*e-shop*	8
	Dokumentace	*server*	8
	Interní postupy	*server*	8
	Data o zákaznících	*e-shop*	8
	Data o zaměstnancích	*server*	8
	Obchodní tajemství	*server*	8
Data pocházející z nedůvěryhodných zdrojů	MS SQL Databáze	*server*	7
	MS Dynamics CRM	*server*	7
Chybné fungování aplikačního prog. vybavení	MS SQL Databáze	*server*	7
	MS Dynamics CRM	*server*	7
Chyba používání	Pasivní síťové prvky	*rozvaděč*	7
	MS SQL Databáze	*server*	7
	MS Dynamics CRM	*server*	7
	Antivir		7
Zneužití oprávnění	Zálohy dat	*server*	7
	Data o zákaznících	*e-shop*	7
	Data o zaměstnancích	*server*	7
	Nahrávky hovorů	*server*	7
	Firewall	*server*	7
	Aktivní síťové prvky	*router*	7
	IP kamery		7
	IBM server		8
	Operační systémy	*server, PC*	7
	MS SQL Databáze	*server*	8
	MS Dynamics CRM	*server*	8
	Antivir		7
	MS Exchange server	*server*	7
Nedostatek personálu	MS SQL Databáze	*server*	7
	MS Dynamics CRM	*server*	7

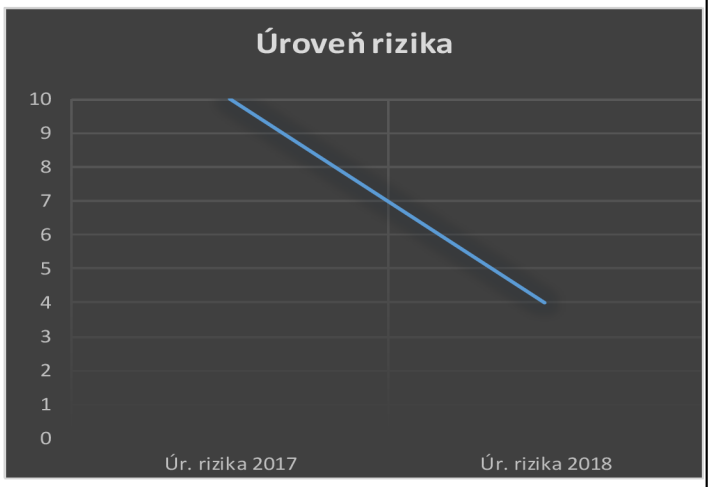
U rizik vysoké úrovně si lze všimnout, že většina aktiv se nachází opět na serveru. Tato rizika je třeba pečlivě sledovat. Většina hrozeb plyne ze selhání komunikačních zařízení, zneužití oprávnění, přerušení dodávky elektřiny či vyzrazení a chyby zařízení. Mezi hrozbami je možno nalézt například nedostatek personálu v případě softwaru CRM, kde se jedná zejména o schopnosti pracovat s programem. Stejně tak je tomu u databáze, ale také hrozí krádeže médií, dokumentů a zařízení.

3.3 Návrhy opatření k vybraným rizikům

Pro účel návrhů opatření pro jednotlivá rizika jsem vytvořil šablonu. Šablona pro návrhy opatření obsahuje: ID rizika, název, popis, aktivum, hrozbu a zranitelnost s jejich ohodnocením a úrovní rizika. Dále je určen vlastník rizika, zdroj informací, stav a popis zdroje odkud je čerpáno. V další sekci je pak vybrán typ zvládání rizika a popsaná opatření, stav řešení i s příslušnými daty. Doplněn je i historický pohled, kdy je bráno v potaz, že společnost dělá analýzu rizik k 1. březnu a opatření aplikované např. v dubnu 2017, se projeví až v analýze za rok 2018. K historické úrovni rizika je doplněn graf. V sekci zvládání rizik je zadáno opatření, zda bylo skutečně provedeno. Vedení spol. musí vše schválit z toho důvodu je dole možnost potvrzení vedením společnosti.

Tabulka 23: Návrh opatření - Šablona (Zdroj: Vlastní zpracování)

ID Rizika:	*RXX*				
Název Rizika:	*Název…*				
Popis:	*Popis…*				
				Hodnota:	**Úr. rizika:**
Aktivum:	*Aktivum…*			1	4
Hrozba:	*Hrozba…*			2	
Zranitelnost	*Zranitelnost…*			3	
Vlastník rizika:	*Vlastník…*	**Stav:**	*V řešení/vyřešeno/nevyřešeno*		
Zdroj info.:	*Zdroj inf…*	**Popis zdroje:**	*Analýza rizik/Audit/Dotazník*		
Typ zvládání:	*Snížení/Akceptace*		**Stav řešení:**	*Nezaháj./zaháj./dokonče.*	
Opatření:		*1. Opatření…*			
		2. Opatření…			
Očekav. datum usktečnění:		*XX. XX. XXXX*	**Skutečné datum usk:**	*XX .XX .XXXX*	
Historický pohled:					
Úroveň rizika:					
Úr. rizika 2017	10				
Úr. rizika 2018	4				
Zvládání rizik:					
Rok 2017:				**Provedeno?**	*Ano/Ne*
Rok 2018:	*Aplikováno opatření…*				
Schváleno:	*Vedení spol.*				

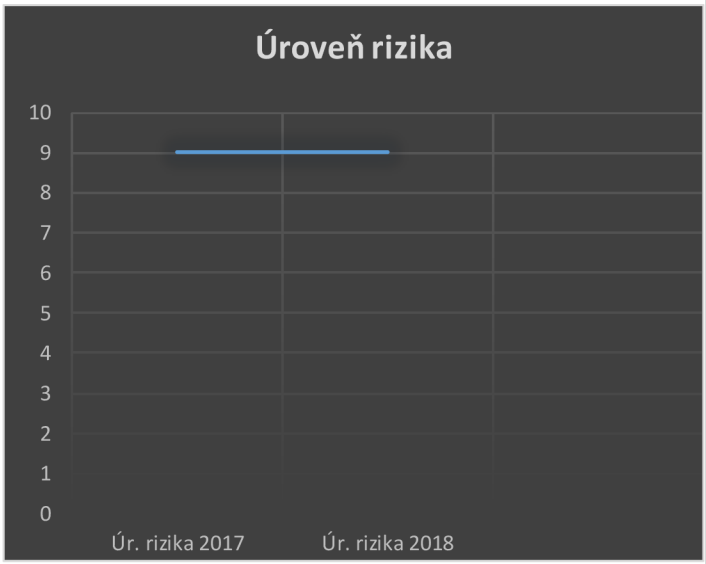


3.3.1 Registr rizik

Podkapitola registru rizik obsahuje návrhy opatření seřazeny dle přiděleného identifikátoru. Do registrů jsou vybrána rizika z tabulek č. 20 – 22. Registry slouží společnosti jako komplexní přehled informací o daném riziku.

Tabulka 24: Návrh opatření – R01 (Zdroj: Vlastní zpracování)

ID Rizika:	R01				
Název Rizika:	Vyzrazení důvěrných informací				
Popis:	Call-centrum nahrává a zaznamenává každý hovor				
				Hodnota:	**Úr. rizika:**
Aktivum:	Nahrávky hovorů			4	9
Hrozba:	Vyzrazení			4	
Zranitelnost	Nedostatečné postupy při výběru pracovníků			3	
Vlastník rizika:	Správce e-shopu	**Stav:**	V řešení		
Zdroj info.:	Vedoucí IT	**Popis zdroje:**	Analýza rizik		
Typ zvládání:	Snížení		**Stav řešení:**	Rozpracováno	
Opatření:	1. Zavedení důkladnějších postupů při výběru pracovníků (lépe zaměřené otázky, vytvoření procesu náboru) 2. Zavedení školení GDPR a zásad bezpečného chování pracovníků call-centra				
Očekav. datum usktečnění:	30. 6. 2019		**Skutečné datum usk:**		
Historický pohled:					
Úroveň rizika:					
Úr. rizika 2017	9				
Úr. rizika 2018	9				
Zvládání rizik:					
Rok 2017:				**Provedeno?**	
Rok 2018:					
Schváleno:	Vedení spol.				

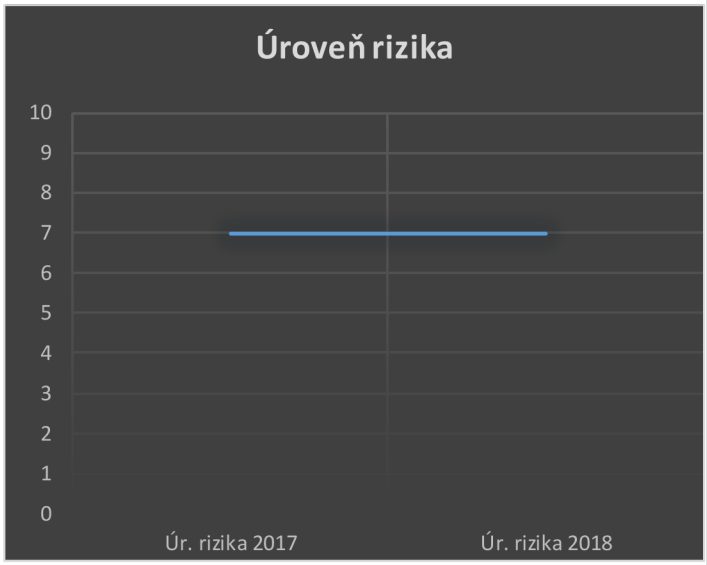


Tabulka 25: Návrh opatření – R02 (Zdroj: Vlastní zpracování)

ID Rizika:	R02				
Název Rizika:	Povodňové nebezpečí				
Popis:	Vypnuknutí záplav v dané oblasti				
				Hodnota:	**Úr. rizika:**
Aktivum:	Akt. síťové prvky			4	7
Hrozba:	Povodeň			1	
Zranitelnost	Poloha společnosti v zátopové oblasti			4	
Vlastník rizika:	Vedoucí IT	**Stav:**	Vyřešeno		
Zdroj info.:	Vedení spol.	**Popis zdroje:**	Analýza rizik		
Typ zvládání:	Akceptace		**Stav řešení:**	Dokončeno	
Opatření:					
Očekav. datum usktečnění:	1. 2. 2017	**Skutečné datum usk:**	1. 2. 2017		

Historický pohled:

Úroveň rizika:	
Úr. rizika 2017	7
Úr. rizika 2018	7



Zvládání rizik:

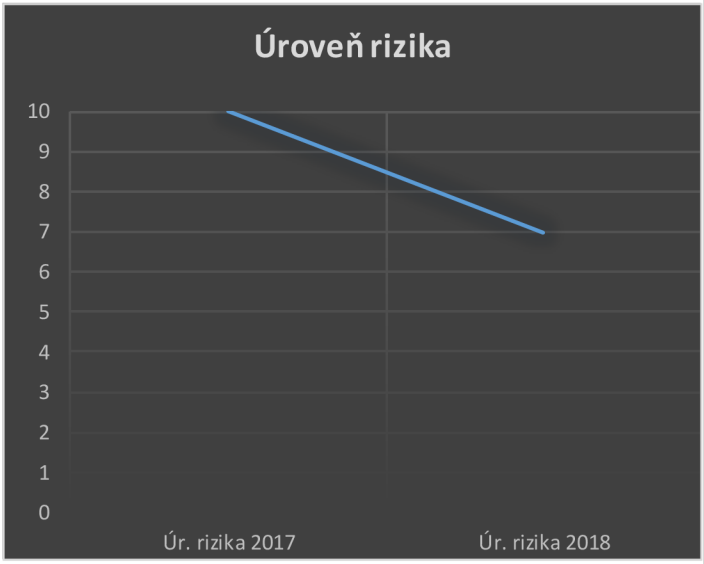
Rok 2017: Vytvořit studii bezpečnosti umístění společnosti **Provedeno?** Ano

Rok 2018:

Schváleno:	Vedení spol.

Tabulka 26: Návrh opatření – R03 (Zdroj: Vlastní zpracování)

ID Rizika:	R03				
Název Rizika:	Výpadek elektrické energie				
Popis:	Nastane výpadek elektřiny z důvodu citlivosti na změny napětí				
				Hodnota:	**Úr. rizika:**
Aktivum:	Data o zákaznících			4	7
Hrozba:	Přerušení dodávky elektřiny			2	
Zranitelnost	Citlivost na změny napětí			3	
Vlastník rizika:	Vedoucí IT	**Stav:**	Vyřešeno		
Zdroj info.:	Vedoucí IT	**Popis zdroje:**	Analýza rizik		
Typ zvládání:	Snížení		**Stav řešení:**	Dokončeno	
Opatření:	1. Společnost pořídila zdroj nepřerušovaného napájení (UPS)				
Očekav. datum usktečnění:	13. 12. 2017		**Skutečné datum usk:**	13. 12. 2017	
Historický pohled:					
Úroveň rizika:					
Úr. rizika 2017	10				
Úr. rizika 2018	7				
Zvládání rizik:					
Rok 2017:				**Provedeno?**	Ano
Rok 2018:	Pořízení UPS				
Schváleno:	Vedení spol.				



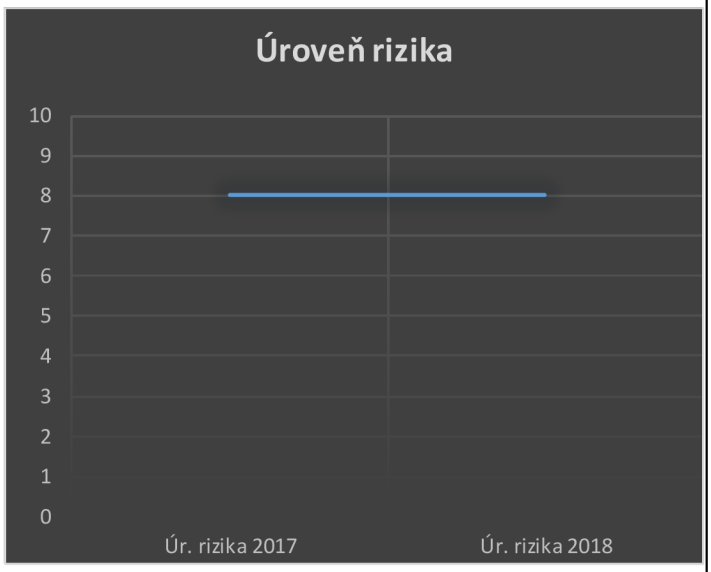
Tabulka 27: Návrh opatření – R04 (Zdroj: Vlastní zpracování)

ID Rizika:	R04				
Název Rizika:	Nefungující počítačová síť				
Popis:	Z důvodu nefunkční poč. sítě nelze zálohovat data				
				Hodnota:	**Úr. rizika:**
Aktivum:	Zálohy dat			4	8
Hrozba:	Selhání telekomunikačních zařízení			3	
Zranitelnost	Komunikace uskutečňována převážně on-line			3	
Vlastník rizika:	Vedoucí IT	**Stav:**	Nevyřešeno		
Zdroj info.:	Vedoucí IT	**Popis zdroje:**	Analýza rizik		
Typ zvládání:	Snížení		**Stav řešení:**	Nezahájeno	
Opatření:	1. Pořízení náhradního telekomunikačního				
Očekav. datum usktečnění:	31. 11. 2019		**Skutečné datum usk:**		

Historický pohled:

Úroveň rizika:

Úr. rizika 2017	8
Úr. rizika 2018	8



Zvládání rizik:

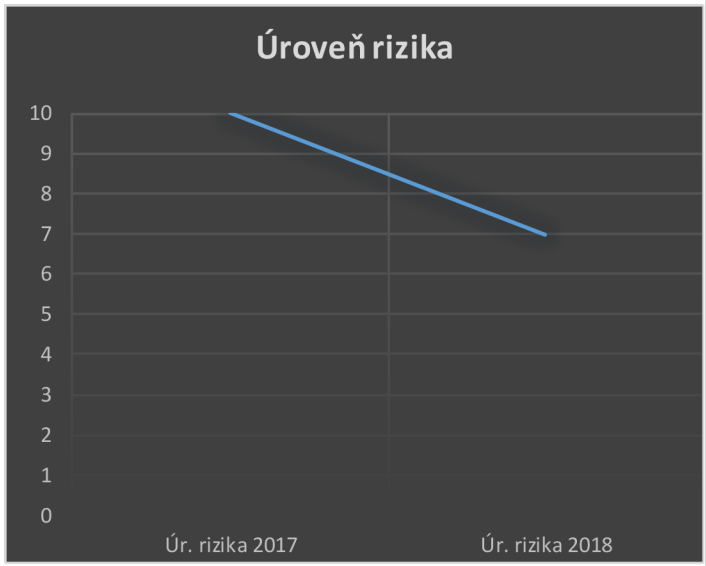
Rok 2017: **Provedeno?**

Rok 2018:

Schváleno:

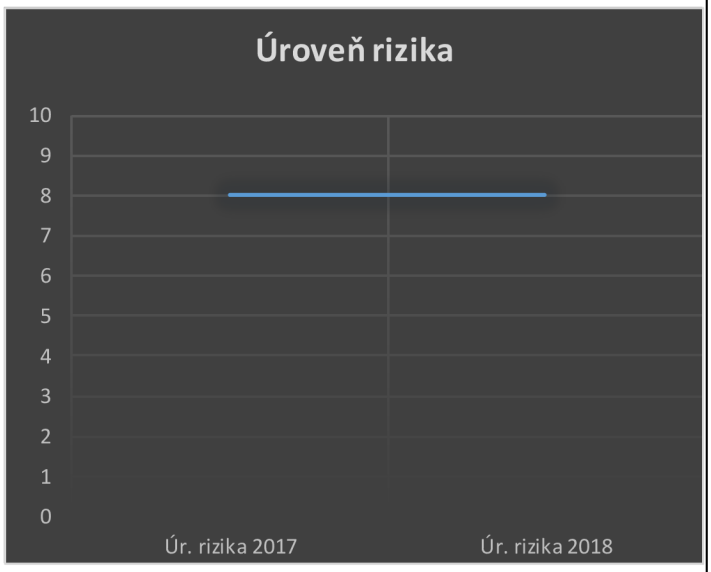
Tabulka 28: Návrh opatření – R05 (Zdroj: Vlastní zpracování)

ID Rizika:	R05				
Název Rizika:	Odcizení důvěrných dat				
Popis:	Krádež médií či dokumentů, které obsahují důvěrná data o zákaznících				
				Hodnota:	**Úr. rizika:**
Aktivum:	Data o zákaznících			4	7
Hrozba:	Krádež médií nebo dokumentů			2	
Zranitelnost	Nedostatečná fyzická bezpečnost budov, oken atd.			3	
Vlastník rizika:	Vedení spol.	**Stav:**	Vyřešeno		
Zdroj info.:	Vedení spol.	**Popis zdroje:**	Analýza rizik		
Typ zvládání:	Snížení		**Stav řešení:**	Dokončeno	
Opatření:	1. Nainstalování okenních mříží a zámků do dveří od kanceláří				
Očekav. datum usktečnění:	3. 9. 2017	**Skutečné datum usk:**	3. 9. 2017		
Historický pohled:					
Úroveň rizika:					
Úr. rizika 2017	10				
Úr. rizika 2018	7				
Zvládání rizik:					
Rok 2017:				**Provedeno?**	Ano
Rok 2018:	Pořídit okenní mříže a zámky				
Schváleno:	Vedení spol.				



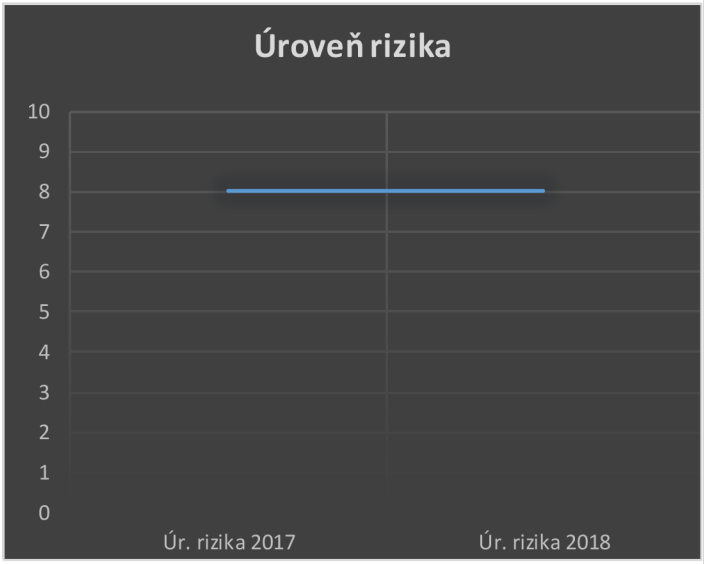
Tabulka 29: Návrh opatření – R06 (Zdroj: Vlastní zpracování)

ID Rizika:	R06				
Název Rizika:	Odcizení aktivních prvků sítě a mobilních zařízení				
Popis:	V důsledku nedostatečné fyzické bezpečnosti může dojít ke krádeži				
				Hodnota:	**Úr. rizika:**
Aktivum:	Akt. Síťové prvky a mobilní zařízení			4	8
Hrozba:	Krádež zařízení			3	
Zranitelnost	Nedostatečná ochrana zařízení			3	
Vlastník rizika:	Vedoucí IT	**Stav:**	V řešení		
Zdroj info.:	Vedoucí IT	**Popis zdroje:**	Analýza rizik		
Typ zvládání:	Snížení		**Stav řešení:**	Rozpracováno	
Opatření:	1. Snížení rizika zavedením terminálů pro autentizaci pomocí čipové karty				
Očekav. datum usktečnění:		1. 8. 2019	**Skutečné datum usk:**		
Historický pohled:					
Úroveň rizika:					
Úr. rizika 2017	8				
Úr. rizika 2018	8				
Zvládání rizik:					
Rok 2017:				**Provedeno?**	
Rok 2018:					
Schváleno:	Vedení spol.				



Tabulka 30: Návrh opatření – R07 (Zdroj: Vlastní zpracování)

ID Rizika:	R07				
Název Rizika:	Vyzrazení dokum. v důsledku nedostatečných postupů při náboru zaměst.				
Popis:	Na server se nahrává dokumentace, která je důležitým know-how společnosti				
				Hodnota:	**Úr. rizika:**
Aktivum:	Dokumentace			3	8
Hrozba:	Vyzrazení			4	
Zranitelnost	Nedostatečné postupy při výběru pracovníků			3	
Vlastník rizika:	Vedoucí IT	**Stav:**	V řešení		
Zdroj info.:	Správce e-shopu	**Popis zdroje:**	Analýza rizik		
Typ zvládání:	Snížení		**Stav řešení:**	Rozpracováno	
Opatření:	1. Zavedení důkladnějších postupů při výběru pracovníků (lépe zaměřené otázky, vytvoření procesu náboru)				
Očekav. datum usktečnění:	30. 9. 2019	**Skutečné datum usk:**			
Historický pohled:					
Úroveň rizika:					
Úr. rizika 2017	8				
Úr. rizika 2018	8				
Zvládání rizik:					
Rok 2017:				**Provedeno?**	
Rok 2018:					
Schváleno:	Vedení spol.				



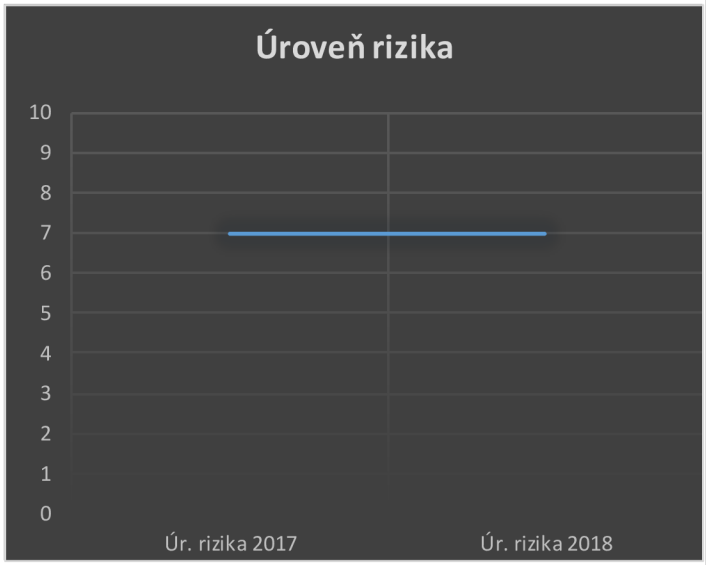
Tabulka 31: Návrh opatření – R08 (Zdroj: Vlastní zpracování)

ID Rizika:	R08				
Název Rizika:	Útok pomocí škodlivého softwaru				
Popis:	Pracovníci spustí soubor pochybného účelu				
				Hodnota:	**Úr. rizika:**
Aktivum:	MS Dynamics CRM			4	7
Hrozba:	Data pocházející z nedůvěryhodných zdrojů			3	
Zranitelnost	Není řízeno odkud je povoleno získávat data			2	
Vlastník rizika:	Vedoucí IT	**Stav:**	V řešení		
Zdroj info.:	Vedoucí IT	**Popis zdroje:**	Analýza rizik		
Typ zvládání:	Snížení		**Stav řešení:**	Rozpracováno	
Opatření:	1. Zavedení školení zásad bezpečného chování pro uživatele CRM software				
Očekav. datum usktečnění:	9. 10. 2019	**Skutečné datum usk:**			

Historický pohled:

Úroveň rizika:

Úr. rizika 2017	7
Úr. rizika 2018	7



Zvládání rizik:

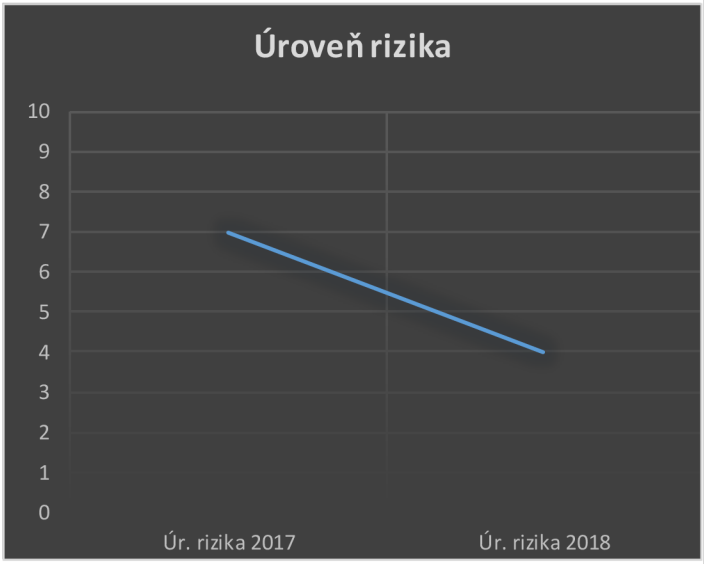
Rok 2017: **Provedeno?**

Rok 2018:

Schváleno:	Vedení spol.

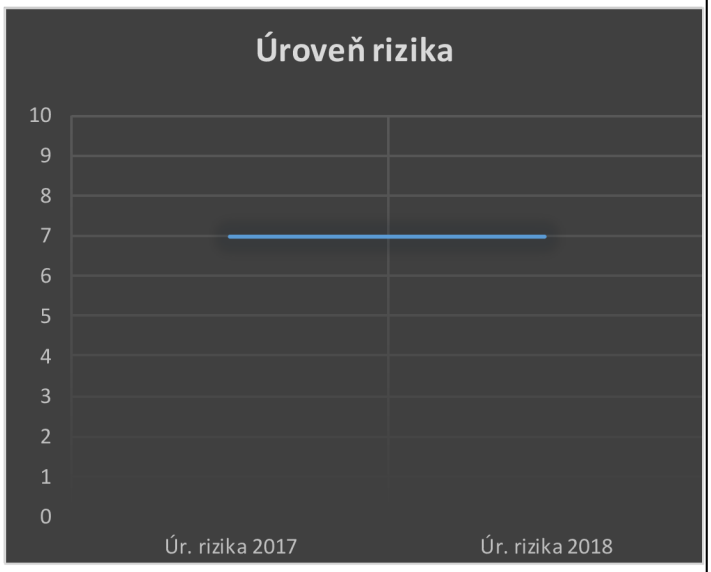
Tabulka 32: Návrh opatření – R09 (Zdroj: Vlastní zpracování)

ID Rizika:	R09				
Název Rizika:	Neotestovaná aktualizace databázové aplikace				
Popis:	Aktualizace pro aplikaci není odladěná				
				Hodnota:	**Úr. rizika:**
Aktivum:	MS SQL Databáze			4	7
Hrozba:	Chybné fungování aplikačního prog. vybavení			2	
Zranitelnost	Neaktualizovaná nebo nová aplikace			3	
Vlastník rizika:	Správce e-shopu	**Stav:**	Vyřešeno		
Zdroj info.:	Vedoucí IT	**Popis zdroje:**	Analýza rizik		
Typ zvládání:	Snížení		**Stav řešení:**	Dokončeno	
Opatření:	1. Testování nových verzí v testovacím prostředí a až následné zavedení do produkce				
Očekav. datum usktečnění:	12. 12. 2018		**Skutečné datum usk:**	12. 12. 2018	
Historický pohled:					
Úroveň rizika:					
Úr. rizika 2017	7				
Úr. rizika 2018	4				
Zvládání rizik:					
Rok 2017:				**Provedeno?**	Ano
Rok 2018:	Vytvoření testovacího prostředí				
Schváleno:	Vedení spol.				



Tabulka 33: Návrh opatření – R10 (Zdroj: Vlastní zpracování)

ID Rizika:	R10				
Název Rizika:	Chybné používání antivirového software v důsledku nedostatečných znalostí				
Popis:	Uživatelé manipulují s antivirovým softwarem				
				Hodnota:	**Úr. rizika:**
Aktivum:	Antivir			4	7
Hrozba:	Chyba používání			2	
Zranitelnost	Nedostatek bezpečnostního povědomí			3	
Vlastník rizika:	Vedoucí IT	**Stav:**	Nevyřešeno		
Zdroj info.:	Vedoucí IT	**Popis zdroje:**	Analýza rizik		
Typ zvládání:	Snížení		**Stav řešení:**	Nezahájeno	
Opatření:	1. Zákaz manipulace s antivirem, vyjímka platí pouze v případě urgence správcem antiviru				
Očekav. datum usktečnění:		21. 8. 2019	**Skutečné datum usk:**		
Historický pohled:					
Úroveň rizika:					
Úr. rizika 2017	7				
Úr. rizika 2018	7				



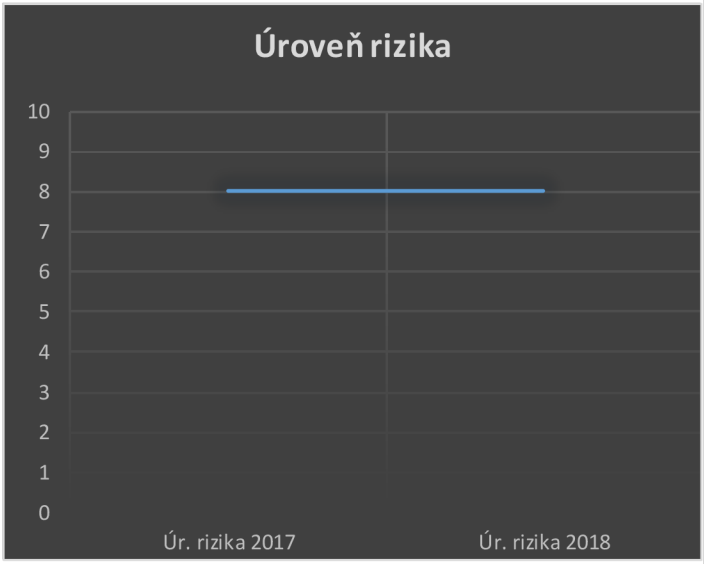
Zvládání rizik:	
Rok 2017:	**Provedeno?**
Rok 2018:	
Schváleno:	

Tabulka 34: Návrh opatření – R11 (Zdroj: Vlastní zpracování)

ID Rizika:	R11				
Název Rizika:	Úpravy nastavení serveru neproškoleným uživatelem				
Popis:	Pracovník IT se zapomene odhlásit z prac. stanice				
				Hodnota:	**Úr. rizika:**
Aktivum:	Server			4	8
Hrozba:	Zneužití oprávnění			3	
Zranitelnost	Neodhlášení se při odchodu od pracovní stanice			3	
Vlastník rizika:	Vedoucí IT	**Stav:**	Nevyřešeno		
Zdroj info.:	Vedoucí IT	**Popis zdroje:**	Analýza rizik		
Typ zvládání:	Snížení		**Stav řešení:**	Nezahájeno	
Opatření:	1. Zavedení politik "čistý stůl" a "čistá obrazovka" a nastavení zámku obrazovky, který se aktivuje po 5 minutové době nečinnosti				
Očekav. datum usktečnění:	4. 4. 2020	**Skutečné datum usk:**			

Historický pohled:

Úroveň rizika:	
Úr. rizika 2017	8
Úr. rizika 2018	8



Zvládání rizik:

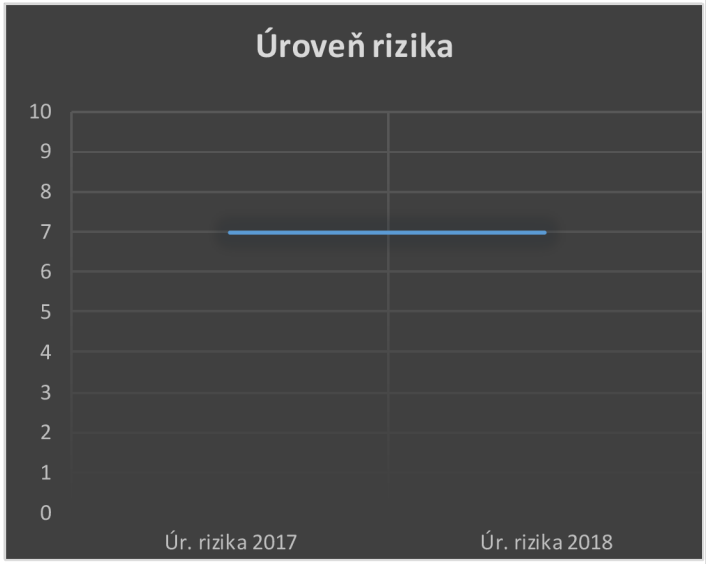
Rok 2017: **Provedeno?**

Rok 2018:

Schváleno:

Tabulka 35: Návrh opatření – R12 (Zdroj: Vlastní zpracování)

ID Rizika:	R12				
Název Rizika:	Nedostatek personálu kvůli nedostatečnému recruitingu				
Popis:	Personální oddělení nenabírá dostatek pracovníků				
				Hodnota:	**Úr. rizika:**
Aktivum:	MS Dynamics CRM			4	7
Hrozba:	Nedostatek personálu			3	
Zranitelnost	Nedostatečný recruiting			2	
Vlastník rizika:	Správce e-shopu	**Stav:**	Nevyřešeno		
Zdroj info.:	Vedoucí IT	**Popis zdroje:**	Analýza rizik		
Typ zvládání:	Snížení		**Stav řešení:**	Nezahájeno	
Opatření:	1. Revize a aktualizace benefitního systému, vytvoření lepších podmínek pro budoucí a stávající zaměstnance				
Očekav. datum usktečnění:		11. 10. 2019	**Skutečné datum usk:**		
Historický pohled:					
Úroveň rizika:					
Úr. rizika 2017	7				
Úr. rizika 2018	7				
Zvládání rizik:					
Rok 2017:				**Provedeno?**	
Rok 2018:					
Schváleno:					



Vzhledem k vyššímu počtu rizik s úrovní „vysoká“ bylo zvoleno od každé hrozby působící na aktiva jednu a navrhl daná opatření, která jsou v tabulkách č. 23 – č. 35.

3.3.2 Návrhy zavedení vybraných bezpečnostních opatření

Následující část je věnována konkrétním návodům pro zavedení vybraných politik za pomocí šablon politik bezpečnosti informací. Zaměřím se na tři politiky, přičemž první dvě řadíme do obecných a třetí do síťových bezpečnostních politik [15]. Na politiky poté navážou vybraná konkrétní opatření.

Tabulka 36: Výběr bezpečnostních opatření (Zdroj: Vlastní zpracování)

A.6 Organizace bezpečnosti informací
A.6.1 Interní organizace
A.6.1.2 Princip oddělení povinností
A.6.1.3 Kontakt s příslušnými orgány a autoritami
A.6.2 Mobilní zařízení a práce na dálku
A.6.2.1 Politika mobilních zařízení
A.7 Bezpečnost lidských zdrojů
A.7.1 Před vznikem pracovního vztahu
A.7.1.1 Prověřování
A.7.2 Během pracovního vztahu
A.7.2.2 Povědomí, vzdělávání a školení bezpečnosti informací
A.8 Řízení 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.11.1 Bezpečné oblasti
A.11.1.3 Zabezpečení kanceláří, místností a vybavení
A.11.1.4 Ochrana před vnějšími hrozbami a hrozbami prostředí
A.11.2 Zařízení
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.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

1) Politika přijatelné zásady šifrování

1. Účel

Účelem této politiky je poskytnout návod, který omezuje použití šifrování na ty algoritmy, které obdržely podstatnou veřejnou kontrolu a byly prokázány, že fungují efektivně. Tato politika navíc poskytuje směr, který zajistí, že budou dodrženy federální předpisy, a bude poskytnuta právní pravomoc pro šíření a používání šifrovacích technologií mimo Spojené státy.

2. Rozsah

Tyto zásady se vztahují na všechny zaměstnance a přidružené společnosti Společnost XYZ.

3. Politika

- **Požadavky na algoritmus**

1. Používané šifry musí splňovat nebo překračovat množinu definovanou jako "kompatibilní s AES" nebo "částečně kompatibilní s AES" podle IETF / IRTF Cipher Catalogu , nebo soubor definovaný pro použití v Národním institutu pro standardy a technologie Spojených států (NIST), publikace FIPS 140-2 nebo jakékoli nahrazující dokumenty podle data provedení. Pro symetrické šifrování se důrazně doporučuje použití standardu AES (Advanced Encryption Standard).
2. Používané algoritmy musí splňovat standardy definované pro použití v publikaci NIST FIPS 140-2 nebo v jakémkoli nahrazujícím dokumentu podle data implementace. Pro asymetrické šifrování se důrazně doporučuje použít algoritmy RSA a Elliptic Curve Cryptography (ECC).
3. Algoritmy podpisu

Tabulka 37: Algoritmy podpisu (Zdroj: Vlastní zpracování dle [15])

Algoritmus	Délka klíče (min)
ECDSA	P-256
RSA	2048
LDWM	SHA256

- **Požadavky funkce hash**

Obecně platí, že Společnost XYZ dodržuje zásady NIST týkající se funkcí hash.

- **Klíčová dohoda a ověřování**

1. Výměna klíčů musí používat jeden z následujících kryptografických protokolů: Diffie-Hellman, IKE nebo eliptická křivka Diffie-Hellman (ECDH).
2. Koncové body musí být ověřeny před výměnou nebo odvozením klíčů relace.
3. Před použitím musí být ověřeny veřejné klíče používané k vytvoření důvěryhodnosti. Příklady autentizace zahrnují přenos prostřednictvím kryptograficky podepsané zprávy nebo ruční ověření hash veřejného klíče.
4. Všechny servery používané pro ověřování (například RADIUS nebo TACACS) musí mít nainstalovaný platný certifikát podepsaný známým důvěryhodným poskytovatelem.
5. Všechny servery a aplikace používající protokol SSL nebo TLS musí mít certifikáty podepsané známým důvěryhodným poskytovatelem.

- **Generování klíčů**

1. Kryptografické klíče musí být generovány a uchovávány bezpečným způsobem, který zabraňuje ztrátě, krádeži nebo kompromisu.
2. Generování klíčů musí být nasazeno z průmyslového standardního generátoru náhodných čísel (RNG). Příklady viz NIST Příloha C: Schválené generátory náhodných čísel pro FIPS PUB 140-2.

4. Dodržování zásad

- **Měření shody**

Manažer bezpečnosti ověří soulad s touto politikou prostřednictvím různých metod, mimo jiné včetně zpráv o obchodních nástrojích, interních a externích auditů a zpětné vazby pro vlastníka politiky.

- **Výjimky**

Výjimky z této zásady musí být předem schváleny manažerem bezpečnosti.

- **Nesoulad**

Zaměstnanec, u kterého bylo zjištěno, že tuto zásadu porušil, může být předmětem disciplinárního řízení až do ukončení pracovního poměru.

5. Související standardy, zásady a postupy

Publikace Národního institutu pro standardy a technologie (NIST) FIPS 140-2,

Zásady NIST týkající se funkcí hash.

6. Definice a pojmy

Následující definice a termíny naleznete v slovníku SANS na adrese:

https://www.sans.org/security-resources/glossary-of-terms/

- Vlastní šifrování

7. Historie revizí

Tabulka 38: Změny v politice 1 (Zdroj: Vlastní zpracování dle [15])

Datum změny	Odpovědný	Souhrn změny
Červen 2014	Politický tým SANS	Aktualizováno a převedeno na nový formát.

2) Politika čisté pracovní plochy (stolu)

Politika čistého stolu může být důležitým nástrojem k zajištění toho, aby všechny interní / důvěrné materiály se odstranili z uživatelského prostředí a zamkly. Právě když položky nejsou v provozu nebo zaměstnanec opustí jeho pracovní stanice. Je to jedna z nejlepších strategií, které je třeba využít při snaze snížit riziko narušení bezpečnosti na pracovišti. Taková politika může také zvýšit povědomí zaměstnanců o ochraně citlivých informací.

1. Účel

Účelem této politiky je stanovit minimální požadavky na udržování „čistého stolu“ - kde jsou interní / kritické informace o našich zaměstnancích, našem duševním vlastnictví, našich zákaznících a našich prodejcích zajištěny v uzamčených prostorách a mimo pracoviště. Politika „Clean Desk“ není kompatibilní pouze s normou ISO/IEC 27001, ale je také součástí standardních základních kontrol ochrany osobních údajů.

2. Rozsah

Tyto zásady se vztahují na všechny zaměstnance a přidružené společnosti Společnost XYZ.

3. Politika

- **Požadavky politiky**

1. Zaměstnanci jsou povinni zajistit, aby všechny interní / důvěrné informace v tištěné nebo elektronické podobě byly na konci dne bezpečně umístěny, tak aby nebyly na pracovišti, zejména pokud se očekává, že budou po delší dobu pryč.
2. Počítačové pracovní stanice musí být uzamčeny, když je pracovní prostor neobsazený.
3. Počítačové pracovní stanice musí být na konci pracovního dne úplně vypnuty.
4. Veškeré interní nebo důvěrné informace musí být odstraněny z pracovního stolu a uzamčeny v zásuvce, když je stůl neobsazený a na konci pracovního dne.

5. Skříně na soubory obsahující interní nebo důvěrné informace musí být uzavřeny a uzamčeny, pokud se nepoužívají nebo pokud nejsou přítomny.
6. Klíče používané pro přístup k interním informacím nebo důvěrným informacím nesmějí být ponechány na pracovním stole.
7. Notebooky musí být buď uzamčeny uzamykacím kabelem, nebo zamčené v zásuvce.
8. Hesla nesmí být ponechána na poznámkách umístěných na počítači nebo pod počítačem a nesmí být ponechána zapsána na přístupném místě.
9. Výtisky obsahující interní nebo důvěrné informace by měly být okamžitě odstraněny z tiskárny.
10. Při likvidaci by měly být dokumenty s interním nebo důvěrným obsahem rozřezány v oficiálních zásobnících na drtiče nebo by měly být umístěny v příslušných nádobách na odpad.
11. Tabulky obsahující omezené interní nebo důvěrné informace by měly být vymazány.
12. Zamknout přenosná počítačová zařízení, jako jsou notebooky a tablety.
13. S velkokapacitními paměťovými zařízeními, jako jsou CD, DVD nebo USB disky, zacházejte jako s interními či důvěrnými zařízeními a zajistěte je v uzamčené zásuvce.

Všechny tiskárny a faxy by měly být po vytištění zbaveny papírů; To pomáhá zajistit, aby interní či důvěrné dokumenty nebyly ponechány v zásobnících tiskárny pro nesprávnou osobu.

4. Dodržování zásad

- **Měření shody**

Manažer bezpečnosti ověří dodržování této politiky prostřednictvím různých metod, včetně, ale bez omezení na periodické procházení, sledování videa, zpráv o obchodních nástrojích, interních a externích auditů a zpětné vazby pro vlastníka politiky.

- **Výjimky**

Výjimky z této zásady musí být předem schváleny manažerem bezpečnosti.

- **Nesoulad**

Zaměstnanec, u kterého bylo zjištěno, že tuto zásadu porušil, může být předmětem disciplinárního řízení až do ukončení pracovního poměru.

5. Související standardy, zásady a postupy

Žádný.

6. Definice a pojmy

Žádný.

7. Historie revizí

Tabulka 39: Změny v politice 2 (Zdroj: Vlastní zpracování dle [15])

Datum změny	Odpovědný	Souhrn změny
Červen 2014	Politický tým SANS	Aktualizováno a převedeno na nový formát.

3) Politika zabezpečení routeru a switche (směrovačů a přepínačů)

1. Účel

Tento dokument popisuje požadovanou minimální konfiguraci zabezpečení pro všechny směrovače a přepínače připojující se k produkční síti nebo používané ve výrobní kapacitě, jménem společnosti Společnost XYZ.

2. Rozsah

Tato pravidla musí dodržovat všichni zaměstnanci, dodavatelé, konzultanti, dočasní i jiní pracovníci společnosti Společnost XYZ a její dceřiné společnosti. Ovlivněny jsou všechny směrovače a přepínače připojené k výrobním sítím Společnosti XYZ.

3. Politika

Každý router musí splňovat následující konfigurační standardy:

- **Standardy politiky**

1. Na routeru nejsou nakonfigurovány žádné místní uživatelské účty. Routery a přepínače musí používat TACACS+ pro ověření všech uživatelů.
2. Heslo pro povolení na routeru nebo přepínači musí být uchováváno v zabezpečené šifrované formě. Směrovač nebo přepínač musí mít z podpůrné organizace zařízení nastaveno heslo pro aktivaci na aktuální heslo směrovače / přepínače.
3. Následující služby nebo funkce musí být zakázány:
    a. IP směrované vysílání
    b. Příchozí pakety na směrovači / přepínači jsou opatřeny neplatnými adresami, například adresami RFC1918
    c. TCP malé služby
    d. Malé služby UDP
    e. Všechno zdrojové směrování a přepínání
    f. Všechny webové služby spuštěné na směrovači
    g. Společnost XYZ protokol zjišťování na připojených rozhraních Internetu
    h. Služby Telnet, FTP a HTTP
    i. Automatická konfigurace
4. Následující služby by měly být zakázány, pokud není poskytnuto obchodní odůvodnění:
    a. Společnost XYZ protokol zjišťování a další protokoly zjišťování
    b. Dynamický kanál
    c. Skriptovací prostředí, například shell TCL
5. Musí být nakonfigurovány následující služby:
    a. Šifrování heslem

b. NTP nakonfigurován na firemní standardní zdroj

6. Všechny aktualizace směrování se provádějí pomocí zabezpečených aktualizací směrování.
7. Používejte firemní standardizované SNMP komunitní řetězce. Výchozí řetězce, například veřejné nebo soukromé, musí být odstraněny. SNMP musí být nakonfigurován tak, aby používal nejbezpečnější verzi protokolu povolenou kombinací zařízení a systémů správy.
8. Seznamy řízení přístupu musí být použity pro omezení zdroje a typu provozu, který může být ukončen na samotném zařízení.
9. Seznamy řízení přístupu pro přechod zařízení musí být přidány při vzniku obchodních potřeb.
10. Směrovač musí být součástí podnikového systému řízení podniku s určeným kontaktním místem.
11. Každý router musí mít následující prohlášení pro všechny formy přihlášení, ať už vzdálené nebo místní:

    "Neautorizovaný přístup k tomuto síťovému zařízení je zakázán. Musíte mít výslovný souhlas s přístupem nebo konfigurací tohoto zařízení. Všechny aktivity prováděné na tomto zařízení mohou být protokolovány a porušení těchto zásad může mít za následek disciplinární opatření a může být oznámeno donucovacím orgánům. Na tomto zařízení není žádné právo na soukromí, používání tohoto systému představuje souhlas s monitorováním.

12. Telnet nesmí být nikdy používán v žádné síti pro správu směrovače, pokud neexistuje zabezpečený tunel chránící celou komunikační cestu. SSH verze 2 je preferovaný protokol řízení.
13. Dynamické směrovací protokoly musí používat ověřování v aktualizacích směrování odeslaných sousedům. Pokud je podporován, musí být povoleno hash hesla pro ověřovací řetězec.
14. Norma konfigurace podnikového směrovače definuje kategorii důvěrných směrovacích a spínacích zařízení a vyžaduje další služby nebo konfiguraci na citlivých zařízeních, včetně:

a. Sčítání seznamu IP přístupů

b. Protokolování zařízení

c. Příchozí pakety na směrovači s neplatnými adresami, jako jsou adresy RFC1918 nebo adresy, které by mohly být použity ke zneužití síťového provozu, by měly být zrušeny.

d. Přístup ke směrovači a modemu musí být omezen dalšími ovládacími prvky zabezpečení

4. **Dodržování zásad**

- **Měření shody**

Manažer bezpečnosti ověří dodržování této politiky prostřednictvím různých metod, včetně, ale bez omezení na, periodického procházení chodem, sledování videa, zpráv o obchodních nástrojích, interních a externích auditů a zpětné vazby pro vlastníka politiky.

- **Výjimky**

Výjimky z této zásady musí být předem schváleny manažerem bezpečnosti.

- **Nesoulad**

Zaměstnanec, u kterého bylo zjištěno, že tuto zásadu porušil, může být předmětem disciplinárního řízení až do ukončení pracovního poměru.

5. **Související standardy, zásady a postupy**

Žádný.

6. **Definice a pojmy**

Žádný.

7. **Historie revizí**

Tabulka 40: Změny v politice 3 (Zdroj: Vlastní zpracování dle [15])

Datum změny	Odpovědný	Souhrn změny
Červen 2014	Politický tým SANS	Aktualizováno a převedeno na nový formát.

Následující návrhy už se netýkají pouze převzetí politik, ale obsahují i konkrétní opatření.

4) Politika reakce na únik dat a návrhy opatření k předcházení úniku dat

V analýze rizik bylo zjištěno riziko kritické úrovně ve formě vyzrazení důvěrných dat. Pro společnost může takový únik znamenat velké finanční ztráty, v nejhorších případech dokonce podnikání společnosti ukončit.

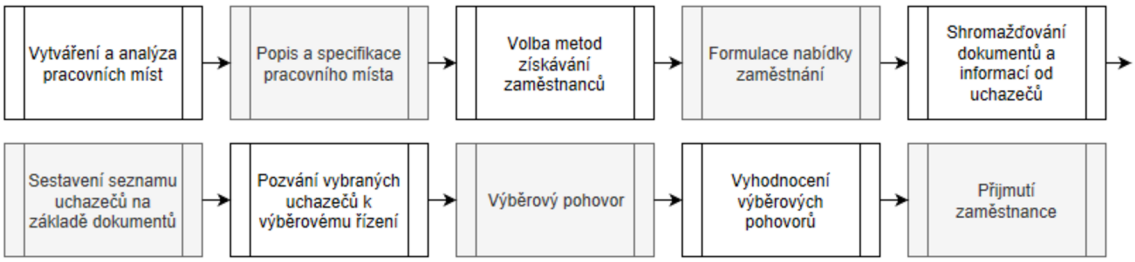
Účelem této politiky je stanovit cíle a vizi procesu reakce na narušení. Tato politika bude jasně definovat, na koho se vztahuje a za jakých okolností, a bude zahrnovat vymezení porušení, role zaměstnanců a odpovědnosti, normy a metriky (např. stanovení priorit incidentů), jakož i podávání zpráv, nápravu, a mechanismy zpětné vazby. Politika musí být zveřejněna a snadno dostupná všem pracovníkům, jejichž povinnosti zahrnují ochranu soukromí a údajů. Tyto zásady se vztahují na všechny osoby, které shromažďují, mají přístup, udržují, distribuují, zpracovávají, chrání, uchovávají, používají, přenášejí, nakládají nebo jinak zpracovávají osobní údaje nebo chráněné informace o zdraví členů společnosti [15].

Kromě politiky reakce na únik dat je, ale třeba zavést určité opatření a snížit tak riziko vyzrazení a pokusit se tak úniku dat předejít. V tomto případě jsou doporučeny následující opatření:

- vytvoření procesu náboru zaměstnanců
- zavedení školení GDPR a zásad bezpečného chování zaměstnanců
- zvyšování bezpečnostního povědomí zaměstnanců

Proces náboru zaměstnanců

S cílem výběru vhodných zaměstnanců je třeba vytvořit proces náboru zaměstnanců.



Obrázek 11: Proces náboru zaměstnanců (Zdroj: Vlastní zpracování dle [20])

Pomocí procesu náboru jsme schopni snížit některé hrozby (neúmyslné či úmyslné vyzrazení dat, nedostatečnou kvalifikace, konkurenční špionáž). Je třeba se zaměřit na některé specifické kroky procesu, které lépe vyfiltrují správné kandidáty.

Společnost nejprve určí, které pracovní místo je třeba obsadit a následně ho řádně specifikuje, čímž dosáhneme lepšího zaměření na cílovou skupinu kandidátů. Následně po konzultaci s vedením určí metodu, jak bude zaměstnance získávat a zformuluje konkrétní nabídky. V dalším kroku začne shromažďování dokumentů a informací od uchazečů, díky těmto materiálům a jejich kontrole lze o uchazeči zjistit podrobnější informace (jaké má zkušenosti, reference, znalosti a odbornost). Na základě těchto dokumentů a informací budou vybraní uchazeči pozváni k výběrovému řízení. Po dokončení výběrových pohovorů, společnost vyhodnotí, kteří kandidáti se nejvíce hodí na obsazení pracovních pozic. Pokud dojde k oboustrannému odsouhlasení podmínek, společnost zaměstnance přijme.

Zavedení školení GDPR a zásad bezpečného chování zaměstnanců

Ochrana osobních údajů a GDPR je novým nařízení Evropské unie. Vstoupilo v účinnost 25. 5. 2018 a jeho cílem je zvýšit úroveň ochrany osobních údajů a posílit práva občanů Evropské unie v této oblasti. GDPR se na společnost vztahuje např. pokud:

- má uložen seznam svých zákazníků
- spravuje databázi fyzických osob

Pokud společnost není v souladu s novou regulací hrozí ji velké pokuty až do výše 4% celosvětového obratu společnosti nebo 25.000.000 EUR, dle hodnoty, která je vyšší.

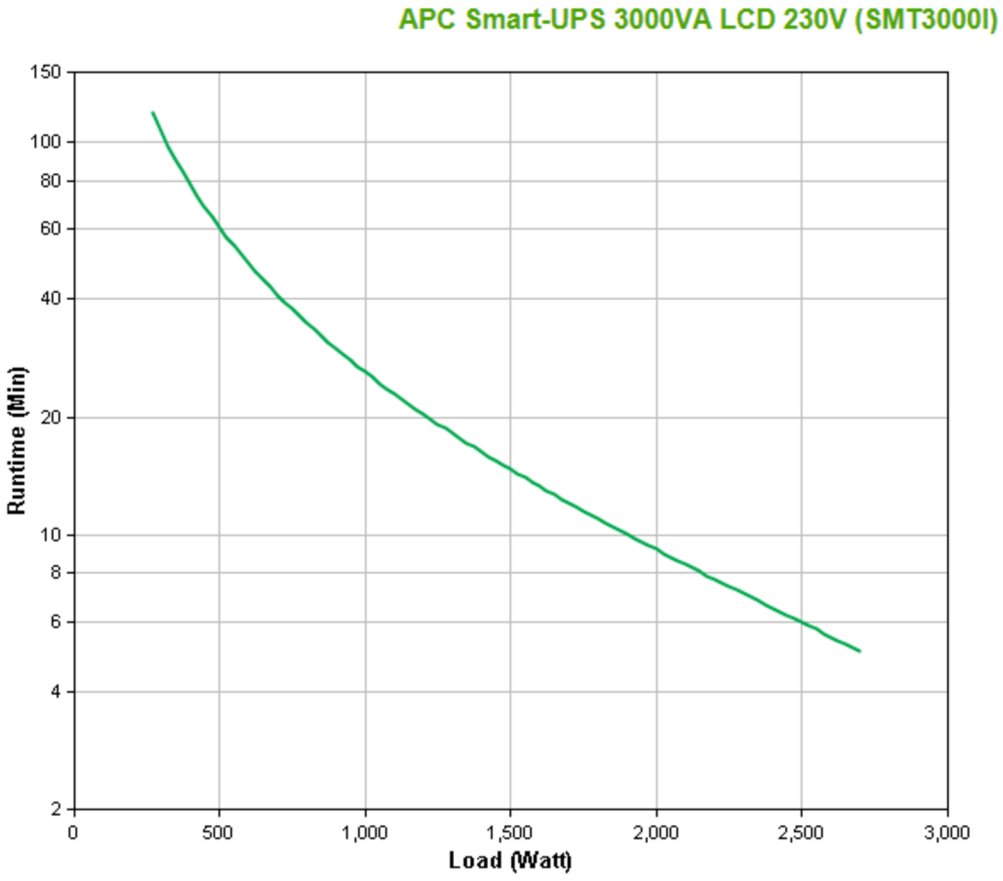
Zvyšování bezpečnostního povědomí zaměstnanců – (Cybersecurity awareness)

Jde o kontinuální program. Struktura a obsah školení jsou vždy situovány na míru. Primárně bývá obsah školení determinován politikami a směrnicemi zaměřenými na

používání informačních a komunikačních technologií v organizaci a zabezpečení informací a informačních a komunikačních technologií. Do školení je vždy rovněž zahrnuta problematika obecných zásad bezpečného chování v organizační síti i mimo ni. V zájmu maximálního osvětlení a zafixování látky jsou probírané koncepty doplňovány o praktické příklady aktuálních hrozeb a korektní postupy v případě styku s nimi.

5) Elektrická energie

V případě ztráty elektrické energie není společnost provozu schopná, proto je zajištění UPS náhradních napájecí zdrojů nutností. Za pomocí zdroje napájení UPS lze vytvořit redundantní obvody. Vzhledem k velikosti společnosti by bylo vhodné pořídit zdroj s výkonem okolo 2700 W, například APC Smart-UPS 3000VA LCD 230V. Výrobce dodává graf účinnosti zařízení při daném zatížení. Graf je vyobrazen na obrázku č. 11.



Obrázek 12: Doba fungování UPS v závislosti na odběru (Zdroj: [17])

Zdroj je schopen udržet napájení 60 minut při odběru 500 W. Při odběru 2700 W, což je maximální dosažitelná hodnota, lze provozovat zařízení 5 minut [17].

Vzhledem k situaci, kdy společnost provozuje servery ve svých prostorách je pořízení další UPS vhodně zvoleným opatřením.

6) Fyzické zabezpečení

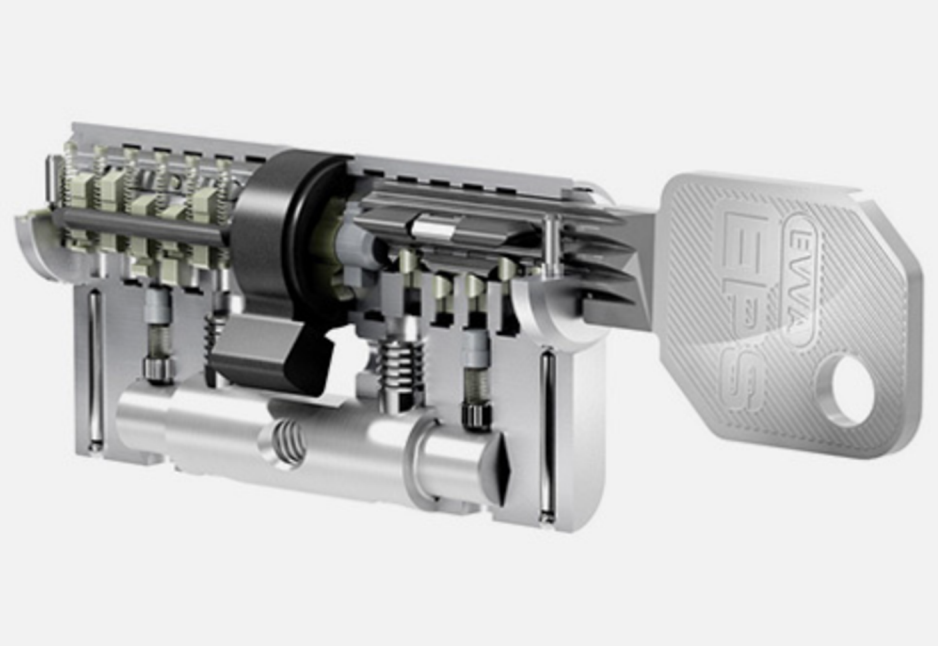
Vstup do areálu společnosti je chráněn vrátnicí, nicméně kanceláře se rozšiřují do nových prostor. Tyto nové prostory jsou v přízemí a nemají chráněná okna bezpečnostními mřížemi. Vzhledem k tomu, že tyto prostory ještě nejsou zcela dokončené, tak dveře nejsou opatřeny bezpečnostními zámky.

Nůžkové mříže jsou tradičním způsobem zabezpečení dveří, oken, průchodů i pasáží proti násilnému vniknutí. Díky svému technickému řešení umožňují bezpočet konkrétních variací (jednostranné, dvoudílné, dělené, sklopné, atd.) a také různé druhy zamykání. Nejsou náročné na údržbu a nezabírají téměř žádné místo v prostoru dveří, oken či průchodů [18].

Obrázek 13: Nůžkové mříže (Zdroj: [18])

Nůžkové mříže jsou vyrobeny z oceli. Chrání a zároveň je lze v případě potřeby odhrnout stranou. Mezi výčet výhod patří například snadná údržba a ovládání, bezpečnostní třída 2. a 3., certifikát NBÚ důvěrné a tajné. Mříž může být vícedílná a po shrnutí ji lze sklopit na zeď, takže je neviditelná. Po sklopení spodní lišty je zajištěn bezbariérový průchod. Samozřejmostí je různá povrchová úprava a barva dle výběru [18].

Do kanceláří a místnosti s aktivními prvky a serverem je vhodné nainstalovat bezpečnostní zámky. Využít lze například bezpečnostní cylindrické vložky s klíči Evva EPS, které plní 4. bezpečnostní třídu. Obsahují až 6 aktivních prvků detekce a až 20 dalších pozic detekce. Ověřují oprávnění uzamykat a odemykat. Masivní stavítka s dvojím účinkem zajišťují vysokou bezpečnost. Jsou k dodání v kompaktním nebo stavebnicovém modulovém provedení a jsou odolná proti „bumpingu“ (metoda, jak otevřít dveře bez klíče) [18].



Obrázek 14: Bezpečnostní vložka s klíčem (Zdroj: [18])

7) Ochrana před ransomware

Vzhledem k tomu, jak již bylo v požadavcích analytické části práce zmíněno, společnost byla v minulosti napadnuta ransomwarem. Z tohoto důvodu si přeje zabezpečit pracovní stanice a notebooky před malwarem a škodlivým kódem.

Ransomware je sofistikovaný program vytvořený někým s dobrými znalostmi počítačového programování. Nakazit se lze spuštěním zavirované přílohy emailu, prostřednictvím webového prohlížeče nebo náhodnou návštěvou webu, který je tímto typem malwaru infikován. Šířit se může také přes počítačovou síť [22].

Počítač napadený ransomware s největší pravděpodobností nebude moci získat přístup ke svým důležitým souborům.

Vhodný antivir pro společnost o velikosti 51 – 999 zaměstnanců, například Kaspersky Endpoint Security for Business slouží k zabezpečení do budoucna, které umožňuje transformaci podniku tím, že plně chrání i ty nejpokročilejší hrozby a odděluje odpovědnosti, což dává více času na to, se zaměřit na obchodní potřeby [19].

Kaspersky Endpoint Security bude zabezpečovat:

- pracovní stanice
- notebooky
- server
- mobilní zařízení
- e-mail službu

Vynikající schopnosti detekce jsou dosaženy použitím globálního „kyber-mozku“ v kombinaci s algoritmy strojového učení, poháněnými nesrovnatelnou lidskou odborností bezpečnostního týmu expertů [19].

Schéma popisující vyhodnocování kyber-bezpečnostních společností Kaspersky hrozeb na obrázku níže.

Obrázek 15: Schéma vyhodnocování kyber-bezpečnostních hrozeb (Zdroj: [19])

Hlavní vlastnosti antiviru jsou:

- zjednodušuje správu zabezpečení prostřednictvím jedné jednotné konzoly

- poskytuje ochranu proti nejnovějším kybernetickým hrozbám
- pomáhá společnostem přizpůsobit zabezpečení nových a starších systémů
- snižuje expozici vůči útoku tím, že zpevňuje koncové body společnosti
- šifruje data - zabraňuje ztrátě důvěrných informací
- eliminuje zranitelnost - odstraní vstupní body útoku
- podporuje regulační iniciativy
- chrání e-mail a webový provoz.
- snadné rozšiřování, zajišťuje různorodá prostředí a platformy
- flexibilní politiky s volností, kdy se mají migrovat na nové verze
- výkonné zabezpečení a řízení pro jakékoli statické nebo mobilní zařízení
- možnost vzdálené správy [19].

3.3.3 Souhrn návrhu opatření vzhledem k registru rizik a požadavkům

Z výsledků, vycházejících z analýzy rizik a základě požadavků společnosti byla navržena bezpečnostní opatření. Opatření jsou v souladu s normou ISO/IEC 27002. Tabulky č. 41 a č. 42 pojednávají o opatřeních dle ISMS a jsou dány do souvislosti s vytvořeným registrem rizik v kapitole 3.3.1. Tyto tabulky, tak ukazují které opatření je nutno aplikovat pro snížení úrovně kritických a vysokých rizik.

Tabulka č. 41 se zabývá vlastním návrhem opatření, kdežto tabulka č. 42 se zaměřuje na opatření, které jsou navrženy za základě požadavků společnosti.

Tabulka 41: Souhrn návrhu opatření v návaznosti na registr rizik (Zdroj: Vlastní zpracování)

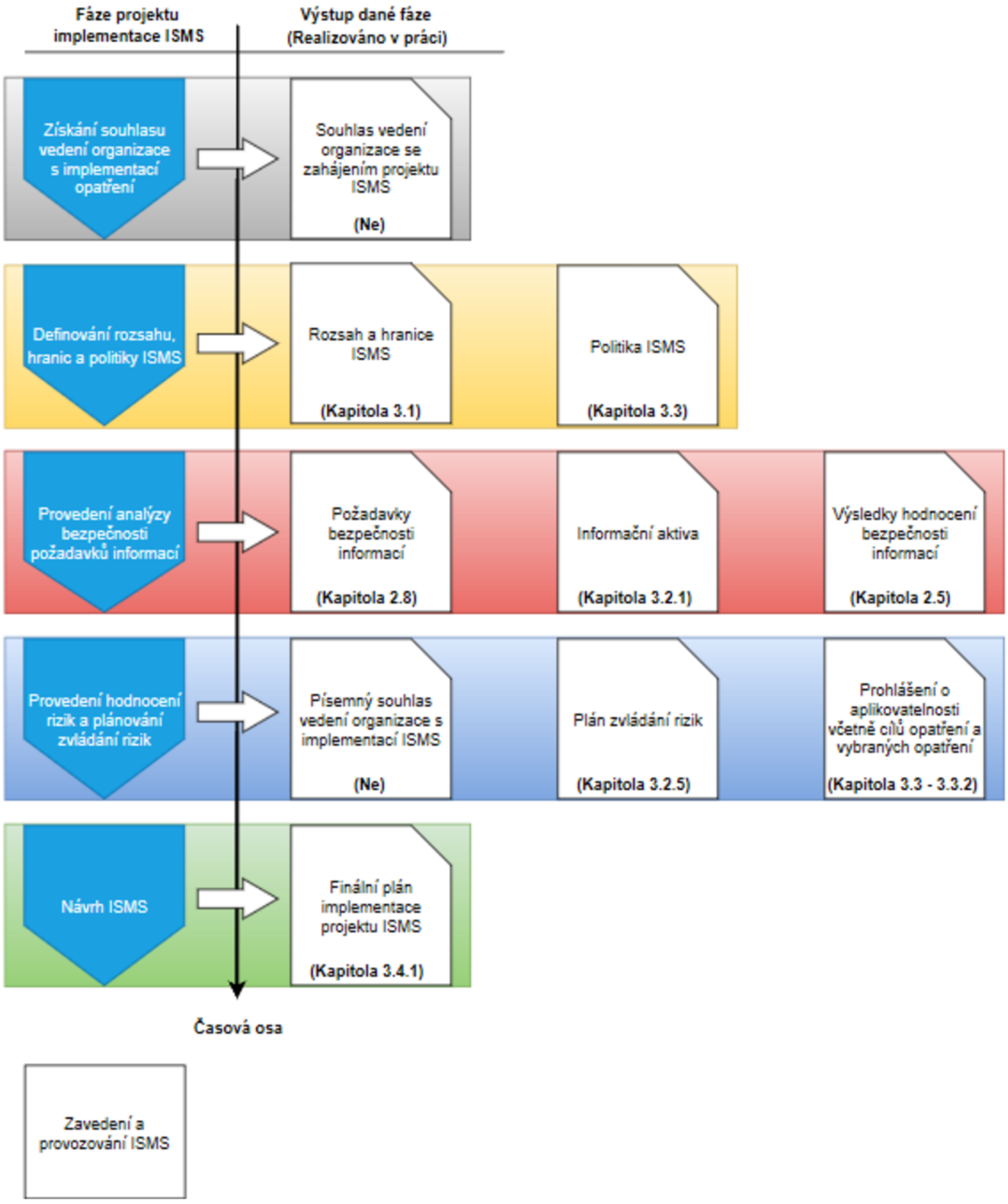
Implementace opatření	Registr rizik	Opatření dle ISMS
Politika „čisté“ pracovní plochy (stolu)	R11	A.11.2.9
Výpadek elektrické energie	R04	A.11.2.2, A.11.2.4
Politika reakce na únik dat a návrhy opatření k předcházení úniku dat a vyzrazení	R01, R07, R08	A.6.2.1, A.8.2.1, A.8.2.2, A.10.1.1, A.10.1.2, A.11.2.9 A.12.2.1, A.13.1.1, A.13.2.1
Fyzické zabezpečení nových prostor	R05	A.11.1.3, A.11.1.4

Tabulka 42: Souhrn požadavků na opatření v návaznosti na registr rizik (Zdroj: Vlastní zpracování)

Požadavek	Registr rizik	Opatření dle ISMS
Vytvoření procesu řízení rizik	R01 – R12	A.6.1.2, A.6.1.3
Šifrování pracovních stanic a ochrana před ramsonware	R10	A.10.1.1, A.10.1.2, A.12.2.1
Politika zabezpečení routeru a switche	-	A.9.1.1, A.9.1.2, A.9.2.1
Ustanovení politik řízení lidských zdrojů	R01, R07, R08, R10, R11	A.7.1.1, A.7.2.2

3.4 Implementace opatření

Provedení implementace bezpečnostních opatření vychází z doporučení, která se nachází v normě ISO/IEC 27003. Jednotlivé kroky a kapitoly v návrhové části práce se zabývali provedením činností, které jsou shrnuty v implementačním plánu. Více o implementačních fázích obsahuje kapitola 3.4.1 a obrázek č. 16. Obrázek je rozdělen na 5 fází implementace ISMS, z nichž každá obsahuje několik výstupů. U výstupů je specifikováno, v jaké kapitole se v této práci nachází. Jednotlivé fáze jsou odděleny barvami pro lepší přehlednost. Pokud se realizují všechny fáze, tak je naznačeno, že dojde k zavedení a provozování ISMS. Činnosti v jednotlivých fázích nejsou chronologicky uspořádány, jako je tomu v práci. Kapitoly, které jsou součástí práce, jsou uspořádány podle logické návaznosti. Tento obrázek je zpracován na základě normy ISO/IEC 27003, návrh ISMS není řešen komplexně, ale realizován je pouze plán implementace opatření.



Obrázek 16: Fáze projektu implementace ISMS (Zdroj: Vlastní zpracování dle [24])

3.4.1 Plán implementace vybraných opatření

Implementační plán je navrhnut, tak aby šli opatření za sebou v logické návaznosti. Z toho důvodu je opatření – A.6.1.3 Kontakt s příslušnými orgány, umístěn až na konec. Vzhledem k rozšíření společnosti do nových kanceláří je třeba vytvořit plány souvisejícími s opatřeními A.11.1.3 Zabezpečení kanceláří, místnostní a vybavení a

A.11.1.4 Ochrana před vnějšími hrozbami a hrozbami prostředí. Společnost si přeje mít kanceláře provozu schopné co nejdříve.

Opatření A.9.1.2 Přístup k sítím a síťovým službám není součástí plánu, jelikož je již společností aplikováno.

Tabulka 43: Plán implementace vybraných opatření (Zdroj: Vlastní zpracování)

Opatření	Alokace času
A.5.1.1 Politiky pro bezpečnost informací	1,25
A.6.1.1 Role a odpovědnosti bezpečnosti informací	0,5
A.6.1.2 Princip oddělení povinností	0,5
A.8.2.1 Klasifikace informací	0,5
A.8.2.2 Označování informací	0,25
A.11.1.3 Zabezpečení kanceláří, místností a vybavení	0,75
A.11.1.4 Ochrana před vnějšími hrozbami a hrozbami prostředí	0,25
A.6.2.1 Politika mobilních zařízení	1
A.7.1.1 Prověřování	0,5
A.7.2.2 Povědomí, vzdělávání a školení bezpečnosti informací	0,5
A.9.1.1 Politika řízení přístupu	1
A.9.2.1 Registrace a zrušení registrace uživatele	0,5
A.10.1.1 Politika pro použití kryptografických opatření	0,75
A.10.1.2 Správa klíčů	3
A.11.2.2 Podpůrné služby	1,5
A.11.2.4 Údržba zařízení	1
A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru	0,25
A.12.2.1 Opatření proti malwaru	4
A.13.1.1 Opatření v sítích	1,25
A.13.2.1 Politiky a postupy při přenosu informací	0,5
A.6.1.3 Kontakt s příslušnými orgány a autoritami	0,5
A.6.1.4 Kontakt se zvláštními zájmovými skupinami	0,25
A.5.1.2 Přezkoumání politik pro bezpečnost informací	0,5

Další strana obsahuje vytvořený Ganttův diagram s odhady na čas vynaložený na implementaci bezpečnostních opatření. Hodnoty v tabulce jsou uváděny v jednotkách člověkoden, přičemž 1 člověkoden = 8h. Vybrán byl časový úsek od 29. července do 26. srpna. Na implementaci se bude pracovat ve dnech pondělí – pátek a pro každý den je práce alokována na jeden člověkoden. Práce by měla být hotova na začátku 35. týdne. V posledním týdnu jsou k dispozici 4 člověkodny, které poslouží jako možnost časové rezervy.

Opatření	Alokace času [člověkoden]	31. týden					32. týden					33. týden					34. týden					35. 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	1,25	1	0,25																						
A.6.1.1	0,5		0,5																						
A.6.1.2	0,5		0,25	0,25																					
A.8.2.1	0,5			0,50																					
A.8.2.2	0,25			0,25																					
A.11.1.3	0,75				0,75																				
A.11.1.4	0,25				0,25																				
A.6.2.1	1					1																			
A.7.1.1	0,5						0,50																		
A.7.2.2	0,5						0,50																		
A.9.1.1	1							1																	
A.9.2.1	0,5								0,50																
A.10.1.1	0,75								0,50	0,25															
A.10.1.2	3									0,75	1	1	0,25												
A.11.2.2	1,5												0,75	0,75											
A.11.2.4	1													0,25	0,75										
A.11.2.9	0,25														0,25										
A.12.2.1	4															1	1	1	1						
A.13.1.1	1,25																			1	0,25				
A.13.2.1	0,5																				0.5				
A.6.1.3	0,5																				0,25	0,25			
A.6.1.4	0,25																					0,25			
A.5.1.2	0,5																					0,5			

Tabulka 44: Ganttův diagram (Zdroj: Vlastní zpracování)

3.5 Ekonomické zhodnocení

Následující tabulky č. 45 a č. 46 slouží jako ekonomický souhrn, který započítává náklady na pořízení aktiv a implementace. Součástí nákladů je také práce, vedoucí k zavedení jednotlivých opatření. Náklady bylo nutné příslušně oddělit, na náklady pro pořízení a náklady za jeden rok. Některé položky v tabulce se financují měsíčně a pro lepší přehlednost byly přepočítány na jeden rok. Ceny jsou uváděny v jednotkách Kč s DPH.

Tabulka 45: Seznam nákladů na pořízení aktiv (Zdroj: Vlastní zpracování)

Opatření	Označení	Množství	Náklady na pořízení	Náklady za 1 rok
A.11.2.2	APC Smart-UPS 3000VA LCD 230V	1 kus	55 265 Kč	-
A.10.1.2 A.12.2.1	Kaspersky Endpoint Security for Business Advanced	50 licencí	74 361 Kč	74 361 Kč
A.11.1.3	Zabezpečení kanceláří, místností a vybavení	-	-	-
A.11.1.4	Ochrana před vnějšími hrozbami a hrozbami prostředí	-	-	-
			129 626 Kč	**74 361 Kč**

Společnost Kaspersky nabízí značně nižší cenu při koupi licencí na více než jeden rok. Příkladem může být objednání 50 licencí na 2 roky, které vyjde na 118 885 Kč. Společnosti XYZ bych proto doporučil, pořídit tento bezpečnostní nástroj na více let. Při pořízení na 2 roky by 50 licencí vycházelo na 59 443 Kč ročně. Nutno dodat, že se jedná pouze o návrh a výběr už bude záležet přímo na společnosti. Ceny produktů jsou převzaty z ceníkových cen, které byly uvedeny v amerických dolarech. Pro lepší přehlednost byly přepočítány na české koruny a to dle současného kurzu k datu 29. 4. 2019, kdy hodnota činí 1 $ (USD) = 22,95 Kč [21].

V tabulce jsou uvedeny i opatření A.11.1.3 Zabezpečení kanceláří, místností a vybavení a A.11.1.4 Ochrana před vnějšími hrozbami a hrozbami prostředí u kterých není uvedena cena za pořízení. Kapitola 3.3.2 obsahuje konkrétní doporučení pro tyto opatření, avšak výběr dodavatele byl po vzájemné dohodě se společností přenechán na správce budov.

Tabulka 46: Seznam nákladů implementace vybraných opatření (Zdroj: Vlastní zpracování)

Opatření	Implementační náklady	Náklady na pořízení	Suma celkových nákladů na implementaci
A.5.1.1	5 000 Kč	-	5 000 Kč
A.6.1.1	2 000 Kč	-	2 000 Kč
A.6.1.2	2 000 Kč	-	2 000 Kč
A.8.2.1	2 000 Kč	-	2 000 Kč
A.8.2.2	1 000 Kč	-	1 000 Kč
A.11.1.3	3 000 Kč	-	3 000 Kč
A.11.1.4	1 000 Kč	-	1 000 Kč
A.6.2.1	4 000 Kč	-	4 000 Kč
A.7.1.1	2 000 Kč	-	2 000 Kč
A.7.2.2	2 000 Kč	-	2 000 Kč
A.9.1.1	4 000 Kč	-	4 000 Kč
A.9.2.1	2 000 Kč	-	2 000 Kč
A.10.1.1	3 000 Kč	-	3 000 Kč
A.10.1.2	12 000 Kč	(74 361 Kč)	12 000 Kč
A.11.2.2	6 000 Kč	55 265 Kč	61 265 Kč
A.11.2.4	4 000 Kč	-	4 000 Kč
A.11.2.9	1 000 Kč	-	1 000 Kč
A.12.2.1	16 000 Kč	74 361 Kč	90 361 Kč
A.13.1.1	5 500 Kč	-	5 500 Kč
A.13.2.1	2 000 Kč	-	2 000 Kč
A.6.1.3	1 500 Kč	-	1 500 Kč
A.6.1.4	1 000 Kč	-	1 000 Kč
A.5.1.2	2 000 Kč	-	2 000 Kč
	84 000 Kč	**129 626 Kč**	**213 626 Kč**

Náklady uvedené v závorce se do celkové sumy počítají pouze jednou a to z následujícího důvodu. Produkt Kaspersky Endpoint Security for Business Advanced svým záběrem pokrývá obě uvedená opatření.

Sazba pracovníka společnosti pro implementaci byla vypočtena na 500 Kč/h. Implementační náklady vychází na 84 000 Kč. Náklady na pořízení aktiv se rovnají 129 626 Kč. Suma veškerých nákladů na implementaci vybraných bezpečnostních opatření pro společnost XYZ činí 213 626 Kč.

3.6 Přínosy práce

Práce je koncipována tak, že hlavním z přínosů je zvýšení úrovně bezpečnosti informací ve společnosti XYZ. Tohoto přínosu bylo dosaženo za pomocí určení rizik působících na společnost a jejich úrovně. Přínosem je tedy i samotná návrhová část práce, která pojednává o registru rizik, který přehledně zobrazuje aktuální nalezená rizika a uvádí k nim opatření. Pokud by se společnost rozhodla používat registr rizik, zvládla by zavádět daná opatření rychleji a efektivněji rizika řídit. Nalezneme zde také návrh bezpečnostních opatření, která působí na bezpečnost společnosti tím, že snižují úroveň rizika.

Společnost pro zpracování této práce určila požadavky, kterých má být docíleno, a ty byly splněny. Přínosem je vytvoření procesu řízení rizik, které bylo splněno vytvořením registru rizik. Další podmínkou bylo zabezpečit společnost před útokem pomocí ransomwaru, který se jí přihodil v minulosti. K tomuto účel bylo navrhnuto pořídit bezpečnostní nástroj společnosti Kaspersky. Tento nástroj bude přínosem v mnoha oblastech včetně šifrování pracovních stanic, vzdálené správě, zabezpečení všech statických nebo mobilních zařízení a poskytuje ochranu proti nejnovějším kybernetickým hrozbám. V neposlední řadě je přínosem vytvoření politiky zabezpečení routeru a switche.

Mezi kritické prvky řadíme servery společnosti, ten musí být stále v provozu a důležité je, aby nebyly porušovány atributy důvěrnost, integrita a dostupnost, jinak budou vznikat společnosti finanční náklady. Přínosem jsou všechna navržená opatření, která společnost zabezpečují, aby nedošlo k velkým finančním ztrátám, ušlému zisku nebo existenčním problémům. Ačkoliv pro zvýšení bezpečnosti a implementaci daných opatření je třeba investovat, tak suma nákladů na implementaci vybraných opatření je značně nižší, než by tomu bylo při ztrátách plynoucích z uskutečnění rizika.

ZÁVĚR

Cílem práce bylo vytvořit GAP analýzu systému řízení bezpečnosti informací a návrh provedení nezbytných kroků vedoucích k zavedení systému řízení bezpečnosti informací. Předpokladem pro dosažení cíle bylo vytvoření analýzy současného stavu ISMS společnosti. Další části byly věnovány analýze rizik, z níž byly získány poznatky pro registry rizik. V návaznosti byli navrženy politiky řízení rizik vedoucí ke zvýšení bezpečnosti v organizaci.

Práce je rozdělena do několika hlavních kapitol, kdy každá měla odlišný cíl a výstup. První kapitola byla věnována teoretickým východiskům a soustředí se na osvětlení základních pojmů a názvosloví, nutných pro pochopení významu problematiky. Nalezneme v ní definice systému řízení bezpečnosti informací, informační a kybernetické bezpečnosti, norem ISO/IEC 27000, opatření, analýzy rizik a jejich metod.

Kapitola druhá podává informace o společnosti a analyzuje její současný stav z hlediska infrastruktury a bezpečnosti. Tato kapitola obsahuje rozsáhlejší analýzu vybraných oblastí, dle pomůcky k auditu bezpečnostních opatření. Z této analýzy lze vyvodit stav bezpečnosti v organizaci, ale ještě byl proveden její převod na opatření z normy ISO/IEC 27001 a vytvořena GAP analýza úrovně shody s ISMS. V tomto kroku, tak bylo zjištěno, nakolik společnost má aplikovány, neaplikovány, částečně aplikovány opatření nacházející se v této normě. Závěr této části obsahuje přehledné grafy plnění, požadavky společnosti a upozorňuje na nedostatky nalezené v oblastech.

Návrhová část se věnuje analýze rizik, kdy jsou identifikovány aktiva, hrozby, zranitelnosti a určeny úrovně rizik. Pro vybraná rizika kritické a vysoké úrovně byl vytvořeno registr rizik, obsahující patřičné informace v jaké stavu se riziko nachází, zda s ním bylo nějak zacházeno a vypsány možná opatření pro jeho případné snížení. Následuje výpis konkrétních bezpečnostních politik pro společnost a plán implementace bezpečnostních opatření. Z plánu implementace byl následně vytvořen časový plán a ekonomické zhodnocení, ve kterém se pojednává o nákladech za práci a implementaci navrhovaných opatření.

SEZNAM POUŽITÝCH ZDROJŮ

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

[2] POŽÁR, Josef. *Manažerská informatika.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 9788073802769.

[3] ISO/IEC 27000:2018: *Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary* [online]. 5. vydání. s. 27 [cit. 2019-01-12]. Dostupné z: https://www.iso.org/standard/73906.html

[4] DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM.* 2. rozšířené vydání. Praha: Professional Publishing, 2011. ISBN 978-80-7431-0508.

[5] KRAMER, Franklin D., Stuart H. STARR a Larry K. WENTZ. *Cyberpower and national security.* Washington, D.C.: Potomac Books, 2009. ISBN 978-1597974233.

[6] SCHMITT, Michael N. *Tallinn manual on the international law applicable to cyber warfare: prepared by the international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence*. New York: Cambridge University Press, 2013. ISBN 978-1-107-61377-5.

[7] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: první oficiální verze slovníku kybernetické bezpečnosti* [online]. Vyd. 1. elektronické. Praha: Policejní akademie České republiky, 2012 [cit. 2019-01-13]. ISBN 978-80-7251-377-2. Dostupné z: https://www.govcert.cz/download/slovnik/vykladovy_slovnik_KB_3_vydani.pdf

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

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

[10] NÚKIB. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. 2017 [cit. 2019-01-19]. Dostupné z: https://www.govcert.cz/

[11] *Kritická infrastruktura* [online]. [cit. 2019-01-21]. Dostupné z: https://www.hzscr.cz/clanek/web-krizove-rizeni-a-cnp-kriticka-infrastruktura-kriticka-infrastruktura.aspx

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

[13] Vyhláška č. 82/2018 Sb.: *o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)* [online]. 2018 [cit. 2019-02-25]. In: Sbírka zákonů. 2018, částka 43. Dostupné také z: https://www.govcert.cz/download/kii-vis/NovaVKB/VKB_82-2018sb.pdf

[14] ZWILLING, Moti. *System Integration: The importance of Big Data and System Integration*. 2019.

[15] SANS: *Information Security Policy Templates* [online]. [cit. 2019-04-12]. Dostupné z: https://www.sans.org/security-resources/policies/

[16] S.ICZ. *Metodika analýzy rizik* [online]. [cit. 2019-03-15]. Dostupné z: http://download.microsoft.com/documents/cs-cz/Priloha-1_Metodika-analyzy-rizik_health.pdf

[17] APC: *APC Smart-UPS 3000VA LCD 230V* [online]. [cit. 2019-04-24]. Dostupné z: https://www.apc.com/shop/cz/cs/products/APC-Smart-UPS-3000VA-LCD-230V/P-SMT3000I

[18] Next: *Nůžkové mříže* [online]. [cit. 2019-04-26]. Dostupné z: https://www.next.cz/nuzkove-mrize

[19] Kaspersky: *Kaspersky Endpoint Security for Business ADVANCED* [online]. [cit. 2019-05-01]. Dostupné z: https://www.kaspersky.com/small-to-medium-business-security/endpoint-advanced

[20] KOUBEK, Josef. *Řízení lidských zdrojů: základy moderní personalistiky*. 4., rozš. a dopl. vyd. Praha: Management Press, 2007. ISBN 978-807-2611-683.

[21] Kurzy.cz: *Dolar, Americký dolar USD, kurzy měn* [online]. [cit. 2019-04-29]. Dostupné z: https://www.kurzy.cz/kurzy-men/nejlepsi-kurzy/USD-americky-dolar/

[22] Avast.com: *Ransomware* [online]. [cit. 2019-05-06]. Dostupné z: https://www.avast.com/cs-cz/c-ransomware

[23] 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.

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

[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/kiivis/container-nodeid-580/vkbchecklistfinalv21rev.pdf

[26] 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.

SEZNAM ZKRATEK

A	Asset, Aktivum
AES	Advanced Encryption Standard
BCM	Business Continuity Management
BI	Bezpečnost informací
CD	Compact Disc
CEN	Comité Européen de Normalisation (European Committee for Standardization)
CENELEC	Comité Européen de Normalisation Électrotechnique (European Committee for Electrotechnical Standardization)
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity, Availability
CRAMM	CCTA Risk Analysis and Management Method
CRM	Customer Relationship Management
CSIRT	Computer Security Incident Response Team
ČSN	České technické normy
ČSNI	Český Normalizační Institut
DVD	Digital Versatile Disc
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ETS	European Telecommunications Standards
ETSI	European Telecommunications Standards Institute
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GAP	Gap analysis, Diferenční analýza
GDPR	General Data Protection Regulation
HA	Hodnota aktiva
HTTP	Hyper Text Transfer Protocol
HW	Hardware
IB	Informační bezpečnost
IBM	International Business Machines
ICT	Information and Communication Technology

ID	IDentifier
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IKE	Internet Key Exchange
IRTF	Internet Research Task Force
IS	Information System
ISMS	Information Security Management System
ISO	International Organization for Stardardization
IT	Information Technology
IP	Internet Protocol
ITU	International Telecommunication Union
KB	Kybernetická bezpečnost
KI	Kritická infrastruktura
MBCO	Minimum Business Continuity Objective
MS	Microsoft
NATO	North Atlantic Treaty Organization
NBÚ	Národní bezpečnostní úřad
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
PDCA	Plan, Do, Check, Act
PUB	Publication
R	Risk, Riziko (Úroveň rizika)
RADIUS	Remote Authentication Dial-In User Service
RFC	Request for Comment
RNG	Random Number Generator
RPO	Recovery Point Objective
RSA	Rivest-Shamir-Adleman algorithm
RTO	Recovery Time Objective
RTP	Risk Treatment Plan
SANS	System and Network Security
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
SLA	Service Level Agreement

SNTP	Simple Network Time Protocol
SOA	Statement of applicability
SP	Stupeň pravděpodobnosti
SQL	Structured Query Language
SSL	Secure Sockets Layer
SSH	Secure Shell
SSO	Single Sign-On
SW	Software
T	Threat, Hrozba
TACACS	Terminal Access Controller Access-Control Systém
TCL	Tool Command Language
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TR	Technical Report
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
USD	United States Dollar
V	Vulnerability, Zranitelnost
VIS	Významný informační systém
VPN	Virtual Private Network
XYZ	Fiktivní název pro společnost

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Příloha 1: Matice zranitelnosti (Zdroj: Vlastní zpracování)

Zranitelnost [V]		INFORMAČNÍ AKTIVA												HARDWAROVÁ AKTIVA								SOFTWAROVÁ AKTIVA									SLUŽBY						
Zdroj		*e-shop*	*server*	*e-shop*	*server*	*server*	*server*	*cloud*	*IP kamera*	*e-shop, CRM*	*server*	*server*	*server*		*rozvaděč*	*router, switch*						*server*	*PC,notebooky*	*server*	*server*	*server*			*server*	*server*	*poskytovatel*	*poskytovatel*	*VPN klient*		*MS OneDrive*	
Aktivum		Veřejná		Interní						Důvěrná																											
		Nabídkové katalogy	Informace na webu	Cenové nabídky	Dokumentace	Interní postupy	Zálohy dat			Data o zákaznících	Data o zaměstnancích	Nahrávky hovorů	Obchodní tajemství	Firewall	Pasivní síťové prvky	Aktivní síťové prvky	Mobilní zařízení	IP kamery	Pracovní stanice	IBM Server	Notebooky	Operační systémy		Spamový filtr	MS SQL Databáze	MS Dynamics CRM	Antivir	Software IP kamer	VPN klient	MS Exchange server	Doménové služby	E-shop	Webové stránky	VPN připojení	Internet	Zálohy	Elektrická energie
	A	2	1	3	3	3	4	3	2	4	4	4	3	4	4	4	2	3	2	4	2	4	2	2	4	4	4	2	3	4	2	3	2	3	3	3	3
Hrozba	**T**																																				
Požár	N													S	V	S	N	S	V	S	S													S		S
Poškození vodou	N													N	N	N	S	N	S	N	S													N		N
Zničení zařízení nebo médií	S													N	N	N	V	N	N	S	S													N		N
Povodeň	N													K	K	K	S	K	K	N	S													K		K
Selhání klimatizace nebo dodávky vody	N															S			S	S	V															
Přerušení dodávky elektřiny	S	V	V	V	V	V	N	S	N	V	V	V	V	V	V	V	N	V	S	N	N									N			V	V	N	K
Selhání telekomunikačních zařízení	V	V	V	V	V	V	V	S		V	V	V	V		N	N	S	S	S	N	S									S			V	K	N	
Vzdálená špionáž	N			V	V	V	V	V	N	V	V	V	V	S	N	S	V	S	N		S	N	N		S	S	S	N		S	N	S	N			V	
Odposlech	N											V																			N			N	V	S	
Krádež médií nebo dokumentů	S				V	V	N	N	N	V	N	V	V																								
Krádež zařízení	V													S		S	K	S	S	N	V																
Vyzrazení	K				V	V	S			S	S	V	V																								
Data pocházející z nedůvěryhodných zdrojů	V																S	S	S		S			S	S	N	N	N	N							
Falšování pomocí aplikačního prog. vybavení	V						N	N	N															N	N	N	N	N	N							
Odhalení pozice	S																S				N															
Selhání zařízení	S													S	N	S	N	S	N	S	N															
Chybné fungování zařízení	S													S	N	S	N	S	N	S	N															
Chybné fungování aplikačního prog. vybavení	S																					S	S	S	V	V	S	N	S	S						
Chyba údržby	S													N		N	N	N	N	S	N	N	N	N	S	S	S	N	S	S					S	
Neoprávněné použití zařízení	S													N	S	N	V	S	S	N	S															
Podvodné kopírování aplikačního prog. zařízení	N																					N	N	N	N	N	N	N	N	N						
Použití padělaného nebo zkopírovaného prog. vyb.	N																					N	N	N	N	N	N	N	N	N						
Poškození dat	N	S	S	S	S	S	S	S	S	S	S	S	S																		N	N				
Nezákonné zpracování dat	N	S	S	S	S	S	S	S	S	S	S	S	S												V	V	N	S			S	N				
Chyba používání	S	S	S	S	S	S	S	S	N	S	S	S	S	S	V	S	S	N	S	N	S	S	S	V	V	V	V	N	S	S				N	S	N
Zneužití oprávnění	V	S	S	S	S	S	S	S	N	S	S	S	S	S		S	V	V	V	V	V	S	S	S	V	V	S	N	S	S						
Odepření činnosti	S													S		S	N	S	N	S	N	S	S	S	N	N	V	S	V	S	S	V	N	K		S	
Nedostatek personálu	V																								S	S											

Příloha 2: Matice úrovní rizik (Zdroj: Vlastní zpracování)

Úroveň rizika [R]		INFORMAČNÍ AKTIVA												HARDWAROVÁ AKTIVA								SOFTWAROVÁ AKTIVA									SLUŽBY						
	Zdroj	*e-shop*	*server*	*e-shop*	*server*	*server*	*server*	*cloud*	*IP kamera*	*e-shop, CRM*	*server*	*server*	*server*		*rozvaděč*	*router, switch*						*server*	*PC,notebooky*	*server*	*server*	*server*					*server*	*server*	*poskytovatel*	*poskytovatel*	*VPN klient*		*MS OneDrive*	
	Aktivum	Veřejná		Interní						Důvěrná																											
		Nabídkové katalogy	Informace na webu	Cenové nabídky	Dokumentace	Interní postupy	Zálohy dat			Data o zákaznících	Data o zaměstnancích	Nahrávky hovorů	Obchodní tajemství	Firewall	Pasivní síťové prvky	Aktivní síťové prvky	Mobilní zařízení	IP kamery	Pracovní stanice	IBM Server	Notebooky	Operační systémy		Spamový filtr	MS SQL Databáze	MS Dynamics CRM	Antivir	Software IP kamer	VPN klient	MS Exchange server	Doménové služby	E-shop	Webové stránky	VPN připojení	Internet	Zálohy	Elektrická energie
	A	2	1	3	3	3	4	3	2	4	4	4	3	4	4	4	2	3	2	4	2	4	2	2	4	4	4	2	3	4	2	3	2	3	3	3	3
Hrozba	**T**																																				
Požár	N													5	6	5	2	4	4	5	3													4		4
Poškození vodou	N													4	4	4	3	3	3	4	3													3		3
Zničení zařízení nebo médií	S													5	5	5	5	4	3	6	4													4		4
Povodeň	N													7	7	7	3	6	5	4	3													6		6
Selhání klimatizace nebo dodávky vody	N															5			3	5	4															
Přerušení dodávky elektřiny	S	5	4	6	6	6	5	5	3	7	7	7	6	7	7	7	3	6	4	5	3									3			6	6	4	7
Selhání telekomunikačních zařízení	V	6	5	7	7	7	8	6		8	8	8	7		6	6	5	6	5	6	5									5			7	8	5	
Vzdálená špionáž	N			5	5	5	6	5	2	6	6	6	5	5	4	5	4	4	2		3	4	2		5	5	5	2		5	2	4	2			5	
Odposlech	N											6																		2			3	5	4	
Krádež médií nebo dokumentů	S				6	6	5	4	3	7	5	7	6																							
Krádež zařízení	V													7		7	7	6	5	6	6															
Vyzrazení	K				8	8	8			8	8	9	8																							
Data pocházející z nedůvěryhodných zdrojů	V																5	6	5		5			7	7	6	4	5	6							
Falšování pomocí aplikačního prog. vybavení	V						6	5	4															6	6	6	4	5	6							
Odhalení pozice	S																4				3															
Selhání zařízení	S													6	5	6	3	5	3	6	3															
Chybné fungování zařízení	S													6	5	6	3	5	3	6	3															
Chybné fungování aplikačního prog. vybavení	S																					6	4	4	7	7	6	3	5	6						
Chyba údržby	S													5		5	3	4	3	6	3	5	3	3	6	6	6	3	5	6					5	
Neoprávněné použití zařízení	S													5	6	5	5	5	4	5	4															
Podvodné kopírování aplikačního prog. zařízení	N																					4	2	2	4	4	4	2	3	4						
Použití padělaného nebo zkopírovaného prog. vyb.	N																					4	2	2	4	4	4	2	3	4						
Poškození dat	N	3	2	4	4	4	5	4	3	5	5	5	4																		3	2				
Nezákonné zpracování dat	N	3	2	4	4	4	5	4	3	5	5	5	4												6	6	4	3			4	2				
Chyba používání	S	4	3	5	5	5	6	5	3	6	6	6	5	6	7	6	4	4	4	5	4	6	4	5	7	7	7	3	5	6					4	5	4
Zneužití oprávnění	V	5	4	6	6	6	7	6	4	7	7	7	6	7		7	6	7	6	8	6	7	5	5	8	8	7	4	6	7							
Odepření činnosti	S													6		6	3	5	3	6	3	6	4	4	5	5	7	4	6	6	4	6	3	7		5	
Nedostatek personálu	V																								7	7											

Příloha 3: Prohlášení o aplikovatelnosti (Zdroj: Vlastní zpracování dle [26])

Prohlášení o aplikovatelnosti

Cíle opatření a jednotlivá opatření vychází z normy ISO/IEC 27002:2013 [26].

Vybraná opatření byla doporučena touto prací a většina prozatím není implementována, některé jsou pouze částečně.

A.5 Politiky bezpečnosti informací

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.

A.5.1.1 Politiky pro bezpečnost informací

Opatření: Definovat sadu politik pro bezpečnost informací, která bude schválena managementem, bude zveřejněna a dána na vědomí zaměstnancům a relevantním externím stranám.

Aplikováno: Částečně

Forma implementace: Politika ISMS

A.5.1.2 Přezkoumání politik pro bezpečnost informací

Opatření: Politiky pro bezpečnost informací by měly být přezkoumávány v plánovaných intervalech, nebo pokud dojde k významným změnám, aby byla zajištěna jejich neustálá vhodnost, přiměřenost a efektivnost.

Aplikováno: Ne

Forma implementace: Politika ISMS

A.6 Organizace bezpečnosti informací

A.6.1 Interní organizace

Cíl: Ustanovit řídící rámec pro zahájení a řízení implementace a provozu bezpečnosti informací v rámci organizace.

A.6.1.1 Role a odpovědnost bezpečnosti informací

Opatření: Všechny odpovědnosti za bezpečnost informací by měly být definovány a přiděleny.

Aplikováno: Ne

Forma implementace: Politika ISMS

A.6.1.2 Princip oddělení povinnosti

Opatření: Konfliktní povinnosti a oblasti působnosti by měly být odděleny, aby se omezily příležitosti pro neoprávněné nebo neúmyslné změny nebo zneužití aktiv organizace.

Aplikováno: Ne

Forma implementace: Zaměstnancům bude na sdíleném úložišti zpřístupněn dokument formalizující jejich povinnosti a odpovědnosti. Tento proces musí projít schválením od vedení společnosti. Dokument je možno upravovat pouze pověřeným pracovníkem, kterého schválí vedení společnosti. Zmíněný dokument pomáhá ke stanovení přístupových oprávnění ke sdíleným souborům ve společnosti.

A.6.1.3 Kontakt s autoritami

Opatření: Měly by být udržovány přiměřené kontakty s příslušnými autoritami.

Aplikováno: Ne

Forma implementace: Dokument specifikující postupy pro kontakt s autoritami. Postupy zahrnují, při jaké události má dojít ke kontaktu, kdo má kontaktovat autoritu (orgány vymáhající právo, regulatorní orgány, orgány dohledu).

A.6.1.4 Kontakt se zvláštními zájmovými skupinami

Opatření: Měly by být udržovány přiměřené kontakty se zvláštními zájmovými skupinami nebo dalšími fóry specialistů na bezpečnost a profesními sdruženími.

Aplikováno: Ne

Forma implementace: Pro zlepšení spolupráce a koordinace řešení bezpečnostních problémů mohou být uzavřeny dohody o sdílení informací. Takové dohody by měly stanovit požadavky na ochranu důvěrných informací. Sledování informací vydávaných

úřadem NÚKIB, národním CSIRT týmem a účast na konferencích pořádaných těmito organizacemi. Tím bude docházet ke zlepšování znalostí o doporučených postupech a sledování aktuálního vývoje v příslušné oblasti bezpečnosti informací.

A.6.2 Mobilní zařízení a práce na dálku

Cíl: Zajistit bezpečnost práce na dálku a bezpečnost použití mobilních zařízení.

A.6.2.1 Politika mobilních zařízení

Opatření: K řízení rizik zavedených používáním mobilních zařízení by měla být přijata politika a podpůrná bezpečnostní opatření.

Aplikováno: Ne

Forma implementace: Politika mobilních zařízení

A.7 Bezpečnost lidských zdrojů

A.7.1 Před vznikem pracovního poměru

Cíl: Zajistit, aby zaměstnanci a smluvní strany chápali své povinnosti, a zajistit, aby byli vhodní pro úlohy, pro které jsou uvažováni.

A.7.1.1 Prověřování

Opatření: Prověření minulosti všech uchazečů o zaměstnání by mělo být prováděno v souladu s příslušnými zákony, nadřízeními a v souladu s etikou a mělo by být úměrné požadavkům souvisejícím s činností organizace, klasifikací informací, ke kterým má být umožněn přístup, a vnímaným rizikům.

Aplikováno: Ne

Forma implementace: Byl vytvořen proces náboru zaměstnanců. Tento proces slouží k snížení rizik s přijetím zaměstnance. Proces by měl významně optimalizovat selekci uchazečů a to i pomocí informací a doporučení, které uchazeč dodá. Náborový proces by měl, pakliže budou splněny všechny náležitosti, společnosti pomoci najít správného uchazeče s požadovanou odborností na inzerovanou pozici.

A.7.2 Během pracovního poměru

Cíl: Zajistit, aby si zaměstnanci a smluvní strany byli vědomi svých povinností, a zajistit, aby je plnili.

A.7.2.2 Povědomí, vzdělávání a školení o bezpečnosti informací

Opatření: Všichni zaměstnanci organizace a tam, kde je to vhodné, i smluvní strany by měli získat odpovídající povědomí o bezpečnost informací formou vzdělávání a školení a pravidelných aktualizací politik a postupů organizace, dle významu pro zastávanou pracovní funkci.

Aplikováno: Ne

Forma implementace: Zavedení školení GDPR, zásad bezpečného chování zaměstnanců a zvyšování bezpečnostního povědomí.

A.8.2 Klasifikace informací

Cíl: Zajistit, aby informace získala odpovídající úroveň ochrany v souladu s jejím významem pro organizaci.

A.8.2.1 Klasifikace informací

Opatření: Informace by měly být klasifikovány z hlediska právních požadavků, hodnoty, kritičnosti a citlivosti ve vztahu k neoprávněnému prozrazení nebo modifikaci.

Aplikováno: Ne

Forma implementace: Politika klasifikace informací.

A.8.2.2 Označování informací

Opatření: Pro označování informací by měly být vypracovány a implementovány vhodné soubory postupů, v souladu se schématem informací přijatým organizací.

Aplikováno: Ne

Forma implementace: Politika klasifikace informací.

A.9 Řízení přístupu

A.9.1 Požadavky organizace na řízení přístupu

Cíl: Omezit přístup k informacím a k vybavení pro zpracování informací.

A.9.1.1 Politika řízení přístupu

Opatření: Na základě požadavků vyplývajících z podnikatelské činnosti a požadavků na bezpečnost informací by měla být stanovena, dokumentována a přezkoumávána politika řízení přístupu.

Aplikováno: Ne

Forma implementace: Politika řízení přístupu bude vycházet z dokumentu, který definuje role uživatelů ve společnosti. Oprávnění přístupu k sdíleným souborům budou nastavena a kontrolována pověřeným zaměstnancem, aby byla stále aktuální.

A.9.1.2 Přístup k sítím a síťovým službám

Opatření: Uživatelům by měl být poskytován přístup pouze k těm sítím a síťovým službám, pro jejichž použití byli výhradně autorizováni.

Aplikováno: Ano

Forma implementace: Po ověření serverem má uživatel k dispozici síťové služby, ke kterým má autorizaci.

A.9.2 Správa a řízení přístupu uživatelů

Cíl: Zajistit oprávněný přístup uživatelů a zabránit neoprávněnému přístupu k systémům a službám.

A.9.2.1 Registrace a zrušení registrace uživatele

Opatření: Pro přidělování přístupových práv by měl být zaveden proces formální registrace a deregistrace uživatele.

Aplikováno: Částečně

Forma implementace: Registrace a zrušení registrace uživatele je součástí dokumentu o řízení přístupu uživatelů.

A.10 Kryptografie

A.10.1 Kryptografická opatření

Cíl: Zajistit správné a efektivní využití kryptografie na ochranu důvěrnosti, autenticity a/nebo integrity informací.

A.10.1.1 Politika použití kryptografických opatření

Opatření: Měla by být vypracována a realizována politika použití kryptografických opatření na ochranu informací.

Aplikováno: Ne

Forma implementace: Politika přijatelné zásady šifrování. Bude vytvořen dokument, který bude stanovovat přístup ke vztahu k používání kryptografických opatření v rámci celé společnosti.

A.10.1.2 Správa klíčů

Opatření: Měla by být vypracována a realizována politika v oblasti použití, ochrany a životního cyklu kryptografických klíčů během jejich celého životního cyklu.

Aplikováno: Ne

Forma implementace: Politika přijatelné zásady šifrování. Budou určeny zodpovědnosti, kdo je odpovědný za implementaci politik a správu klíčů, včetně generování klíčů. Pro správu klíčů bude používán i bezpečnostní nástroj Kaspersky Endpoint Security.

A.11 Fyzická bezpečnost a bezpečnost prostředí

A.11.1 Fyzický bezpečností perimetr

Cíl: Zabránit neoprávněnému fyzickému přístupu, poškození a narušování informací a vybavení pro zpracování informací organizace.

A.11.1.3 Zabezpečení kanceláří, místností a vybavení

Opatření: Měla by být navržena a uplatněna opatření pro fyzickou bezpečnost kanceláří, místností a vybavení.

Aplikováno: Částečně

Forma implementace: Společnost rozšiřuje své prostory, dojde tedy k zabezpečení nových prostor, bezpečnostními zámky 4. bezpečnostní třídy a odolné proti bumpingu. Zároveň dojde k přezkoumání bezpečnosti již používaných prostor a případné revizi bezpečnosti.

A.11.1.4 Ochrana před vnějšími a přírodními hrozbami

Opatření: Měla by být navržena a uplatněna fyzická ochrana před přírodními katastrofami, zlomyslnými útoky nebo nehodami.

Aplikováno: Ne

Forma implementace: Do oken nových prostor se nainstalují nůžkové bezpečnostní mříže. V této souvislosti dojde k přezkoumání bezpečnosti již používaných prostor a případné revizi bezpečnosti.

A.11.2 zařízení

Cíl: Zabránit ztrátě, poškození, odcizení nebo kompromitaci aktiv a přerušení provozu organizace.

A.11.2.2 Podpůrné služby

Opatření: Zařízení by mělo být chráněno před výpadkem napájení a dalšími poruchami způsobenými selháním podpůrných služeb.

Aplikováno: Částečně

Forma implementace: V plánu je pořízení nové výkonné UPS, stav již používané je pravidelně kontrolován. Významná kritická zařízení společnosti jsou na ni napojena.

A.11.2.4 Údržba zařízení

Opatření: Zařízení by mělo být správně udržováno pro zajištění jeho stálé dostupnosti a integrity.

Aplikováno: Ne

Forma implementace: Údržba zařízení se bude dodržovat dle doporučených servisních intervalů a specifikací dodavatele. Servis a opravy zařízení budou provádět pouze autorizovaní pracovníci údržby.

A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru

Opatření: Pro vybavení pro zpracování informací by měla být přijata zásada prázdného stolu, týkající se papírových dokumentů a vyměnitelných paměťových médií, a zásada prázdné obrazovky.

Aplikováno: Ne

Forma implementace: Politika čisté pracovní plochy (stolu)

A.12.2 Ochran před malwarem

Cíl: Zajistit, že informace a vybavení pro zpracování informací jsou před malwarem chráněny.

A.12.2.1 Opatření na ochranu proti malwaru

Opatření: Měla by být implementována opatření pro detekci, prevenci a zotavení na ochranu před malwarem, v kombinaci s vhodným zvyšováním povědomí uživatelů.

Aplikováno: Částečně

Forma implementace: Užívání bezpečnostního nástroje Kaspersky Endpoint Security. Stanovení formální politiky zakazující používání neuautorizovaného softwaru (např. seznam povolených aplikací). Definování provozních postupů, které brání zavedení malwaru.

A.13 Bezpečnost komunikací

A.13.1 Správa bezpečnosti sítě

Cíl: Zajistit ochranu informací v sítích a jejich podpůrných prostředcích pro zpracování informací.

A.13.1.1 Opatření v sítích

Opatření: K ochraně informací v systémech a aplikacích musí být sítě řízeny, spravovány a kontrolovány.

Aplikováno: Částečně

Forma implementace: Politika správy a řízení sítě. Společnost má na správu a bezpečnost sítě utvořené IT oddělení.

A.13.2 Přenos informací

Cíl: Zachovat bezpečnost informací přenášených v rámci organizace a s jakýmkoli externím subjektem.

A.13.2.1 Politiky a postupy při přenosu informací

Opatření: K ochraně přenosu informací prostřednictvím všech druhů komunikačních zařízení by měly být zavedeny formální politiky, postupy a opatření.

Aplikováno: Částečně

Forma implementace: Politika postupy při přenosu informací. Společnost má vytvořeny postupy pro ochranu přenášených informací před odposloucháváním, kopírováním, pozměněním, chybným směrováním a zničením.