VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH ZAVEDENÍ BEZPEČNOSTNÍCH OPATŘENÍ PODLE ISMS VE SPOLEČNOSTI VYVÍJEJÍCÍ FINANČNÍ APLIKACI

PROPOSAL FOR THE IMPLEMENTATION SECURITY MEASURES ACCORDING TO ISMS IN THE COMPANY DEVELOPING FINANCIAL APPLICATION

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR

Bc. Luděk Bukovský

VEDOUCÍ PRÁCE
SUPERVISOR

Ing. Petr Sedlák

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

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

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

Návrh zavedení bezpečnostních opatření podle ISMS ve společnosti vyvíjející finanční aplikaci.

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Teoretická východiska práce
Analýza problému a současná situace
Vlastní návrh řešení, přínos práce
Zhodnocení a přínosy práce
Závěr
Seznam použité literatury

Cíle, kterých má být dosaženo:

Cílem práce je návrh a zavedení bezpečnostních opatření podle systému řízení bezpečnosti informací a zvýšit dosavadní zabezpečení serverovny v podniku, který vyvíjí finanční aplikaci určenou pro švýcarský trh.

Základní literární prameny:

ČSN ISO/IEC 27000. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Přehled a slovník. Praha: Český normalizační institut, 2014.

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

ČERMÁK M. Řízení informačních rizik v praxi. Brno: Tribun EU, 2009. ISBN 978-80-7399-731-1.

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.

POŽÁR J. Manažerská informatika. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 978-80-7380-276-9.

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

Cílem této diplomové práce je návrh zavedení bezpečnostních opatření do společnosti vyvíjející finanční aplikaci zaměřenou převážně na švýcarský trh. Tato opatření vycházejí z analýzy současného stavu bezpečnosti ve společnosti. Z výsledků analýzy rizik jsou pro společnost navržena bezpečnostní opatření, jenž jsou doporučením norem řady ISO/IEC 27000, která by měla snížit rizika působící na společnost.

Abstract

The goal of this Master Thesis is a proposal for the implementation security measures in the company developing financial software application focused primarily on the Swiss market. These measures are based on results from present state of security in the company. There are the proposal for the security measures on the risk analysis results which are recommendation of the series of standards ISO/IEC 27000 and should lead to the risk reduction affecting the company.

Klíčová slova

systém řízení bezpečnosti informací, rodina norem ISO/IEC 27000, bezpečnostní opatření, analýza rizik, hrozba, zranitelnost, aktivum, informační bezpečnost, vývoj softwaru

Keywords

information security management system, ISO/IEC 27000, security measures, risk analysis, threat, vulnerability, asset, information security, software development

Citace

BUKOVSKÝ, Luděk. *Návrh zavedení bezpečnostních opatření podle ISMS ve společnosti vyvíjející finanční aplikaci.* [online]. Brno, 2019. [cit. 2019-02-05]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/119831. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Ing. Petr Sedlák

Návrh zavedení bezpečnostních opatření podle ISMS ve společnosti vyvíjející finanční aplikaci

Prohlášení

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně pod vedením pana inženýra Petra Sedláka. 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).

.....
Luděk Bukovský
9. května 2019

Poděkování

Rád bych poděkoval mému vedoucímu panu inženýru Petru Sedlákovi za jeho cenné rady. Také bych chtěl poděkovat kolegům z práce za jejich spolupráci. Dále bych chtěl poděkovat kolegovi Tomášovi Hinkovi za jeho praktické rady v otázkách týkajících se možného zabezpečení serverovny.

Obsah

Kapitola 1

Úvod

Bezpečnosti informací se v minulosti nevěnovalo příliš mnoho pozornosti, což dokazuje i veřejné přiznání největší sociální sítě Facebook, že po dobu několika let ukládal hesla až stovek miliónů uživatelů v nešifrované textové podobě. S těmito přihlašovacími údaji se pak bylo možné přihlásit na cizí účty sociální sítě, ke kterým měli přístup zaměstnanci společnosti. Pro mnoho organizací je dnes bezpečnost informací vnímána jako nutná podmínka pro navázání nových obchodních vztahů. Společnosti si tak uvědomují důležitost svých informací, které mohou být uloženy v papírové či elektronické podobě, nebo přenášeny po síti Internet.

Společnosti nabízející určitý produkt, který je licencován po určitou dobu, jako například různé aplikace, hrozí rizika v několika ohledech. V případě kompromitace kontaktních údajů uživatelů, jenž mají předplacenou aplikaci, může dojít k převzetí zákazníků ze strany konkurenční společnosti nabízející obdobný produkt, který může být například cenově zvýhodněn. Dojde-li k přechodu klíčových fyzických či právnických osob ke konkurenční společnosti, může se společnost, jejíž data byla vyzrazena, dostat do existenčních potíží. Extrémním případem může být zveřejnění několikaletého budování know-how či duševního vlastnictví vedoucímu ke vzniku organizace zcela nové, která by získané informace využila k vytvoření nového výhodnějšího produktu. Organizacím podnikajících v obdobném sektoru by získané informace mohly pomoci k vyřešení důležitých problémů a objasnit tak některá dosud neznámá fakta.

Cílem práce je návrh zavedení bezpečnostních opatření do malé společnosti vyvíjející softwarovou aplikaci a zvýšit dosavadní bezpečnost serverovny dle využití norem řady ISO/IEC 27000.

Celý text je členěn do několika po sobě navazujících kapitol, které budou stručně uvedeny. Kapitola 2 představuje cíle práce. V kapitole 3 bude čtenář seznámen se základním názvoslovím a pojmy související se systémem řízení bezpečnosti informací, které jsou důležité pro jeho úplné pochopení. V Kapitole 4 bude představena společnost, její firemní procesy a aktuální stav bezpečnosti ve společnosti. Zároveň je čtenář seznámen s legislativními změnami týkajících se obecného nařízení na ochranu osobních údajů a nové vyhlášky o kybernetické bezpečnosti. Závěr kapitoly je věnován analýzou konkurenčního prostředí, zhodnocením současného stavu a očekáváním vedení společnosti od této práce. Kapitola 5 vymezuje rozsah práce. Následně jsou analyzována rizika, na která jsou navržena vhodná bezpečnostní opatření s možným časovým plánem pro jejich nasazení a zároveň je vyhotoveno ekonomické zhodnocení. Kapitola 6 pojednává o přínosech a zhodnocení této práce pro společnost.

Kapitola 2

Cíle práce

Cílem práce je návrh a zavedení bezpečnostních opatření podle systému řízení bezpečnosti informací a zvýšit dosavadní zabezpečení serverovny v podniku, který vyvíjí finanční aplikaci určenou pro švýcarský trh. Dílčí cíle diplomové práce jsou:

- teoretická východiska,
- analýza současného stavu,
- identifikace aktiv,
- ohodnocení aktiv,
- identifikace a analýza rizik,
- návrh bezpečnostních opatření,
- ekonomické zhodnocení návrhu řešení.

Práce nemá za cíl navrhnutí komplexního řešení, ale vybrat vhodná bezpečnostní opatření vztahující se na konkrétní prostředí a potřeby podniku. Výběr bezpečnostních opatření vychází z rodiny norem ISO/IEC 27000.

Kapitola 3

Teoretická východiska

Obsahem této kapitoly bude seznámení čtenáře se systémem řízení bezpečnosti informací (zkráceně ISMS). S tím souvisí také několik nových pojmů, které mohou být pro čtenáře neznámé a z toho důvodu je vysvětlím v sekcích 3.1 a 3.2. Ještě před samotným seznámením ISMS představím Demingův model, jenž se skládá ze čtyř základních činností, které budou využity v následující sekci o samotném systému řízení bezpečnosti informací. Jakmile bude mít čtenář základní informace o ISMS, je vhodné uvést normalizační instituce a normy řady 27000, jenž jsou pro systém řízení bezpečnosti informací základním kamenem a úzce spolu souvisí. Dále objasním metodiku COBIT a rámec ITIL. Kapitola bude zakončena obecným shrnutím GDPR a firemními procesy společnosti.

3.1 Základní názvosloví

Nerozlučně souvisí se základními pojmy v sekci 3.2 a dle [9] je za základní názvosloví považováno:

IT	—	Information Technology
	—	Informační technologie
ICT	—	Information and Communication Technology
	—	Informační a komunikační technologie
IS	—	Information system
	—	Informační systém
ISMS	—	Information security management system
	—	Systém řízení bezpečnosti informací

3.2 Základní pojmy

Pro úplné pochopení práce a jejího významu je důležité vysvětlit některé vybrané pojmy, které jsou v následujícím textu využity a navazují na praktickou část.

Data

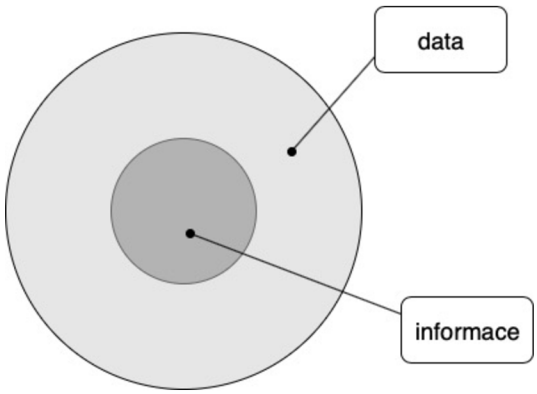
Data jsou většinou nezávislá na čase a jsou chápána jako statická fakta. Data lze získávat o realitě v jiném časovém okamžiku. Data lze získat čtením, pozorováním, měřením, vážením, kreslením, výpočtem nebo jiným způsobem [10].

Data je opakovaně interpretovatelná formalizovaná podoba informace, která je vhodná pro komunikaci, zpracování či vyhodnocování [9].

Informace

Informace je určitý význam přisouzený datům, který vyplývá z analýz a jejich zpracování, prezentaci dat ve formě, jenž bude přiměřený pro rozhodovací proces. Pojem informace není jednoznačný, ale lze se shodnout na tom, že základem pojmu informace je schopnost zvyšovat úroveň poznání lidské společnosti. Přesná a jednoznačná definice pojmu informace nebyla dosud vypracovaná a existuje mnoho definic. Informace představuje sdělení či zprávu, tedy takovou znalost, pro kterou existuje možný příjemce, jenž ji může využít a znalost se tak stává informací. Informace je tvořena tou částí znalosti, která je využívána k orientaci, k aktivnímu jednání, k řízení s cílem zachování, zdokonalování a rozvoje systému [10].

V informatice tvoří informaci kódovaná data v podobě fyzické interpretace na přenosovém médiu [9].



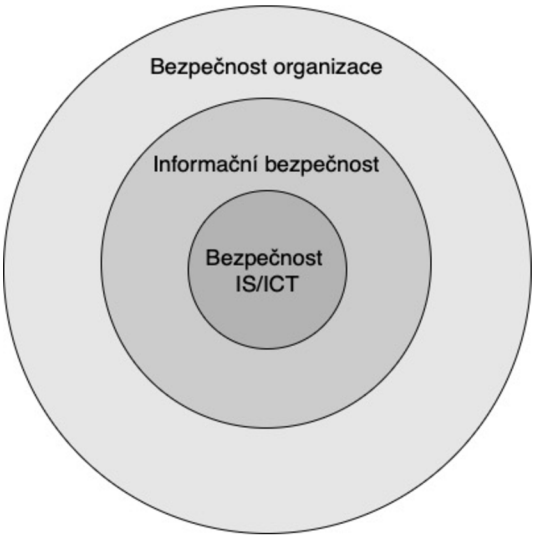
Obrázek 3.1: Vztah obsahu data a informace [9]

Informační systém

Existuje celá řada definic pojmu informační systém a každý uživatel nebo jeho tvůrce používá různé terminologie. Obecně lze říci, že informační systém (zkráceně IS) lze chápat jako systém vzájemně propojených informací a procesů, které s těmito informacemi pracují. Pojmem procesy rozumíme funkce, jenž zpracovávají vstupující informace do systému a transformující je na vystupující informace ze systému. Zjednodušeně můžeme říci, že procesy jsou funkce zabezpečující sběr, zpracovávání, přenos, uložení a distribuci informací [10] [9].

Bezpečnost informací

Bezpečnost informací neboli informační bezpečnost se zabývá ochranou informací a jejich dostupností. Je ve vzájemném vztahu s pojmy bezpečnost organizace a bezpečnost IS/ICT. Nejvýše je postavena bezpečnost organizace, která má za úkol zajistit bezpečnost objektu a majetku organizace. Bezpečnost informací zahrnuje kromě bezpečnosti IS/ICT práci s informacemi v nedigitální formě. Bezpečnost IS/ICT chrání pouze aktiva informačního systému podporovaná komunikačními a informačními technologiemi [9]. Tento slovní popis nejlépe vystihuje obrázek 3.2.



Obrázek 3.2: Bezpečnost organizace a její úrovně [10]

Pro bezpečnost informací je nezbytné zachovat důvěrnost 3.2, integritu 3.2 a dostupnost informací 3.2.

Důvěrnost

Zajištění přístupu k informaci pouze oprávněnému uživateli, entitě či procesu [9] [3].

Integrita

Zajištění neporušitelnosti, správnosti a úplnosti informace [9] [17].

Dostupnost informací

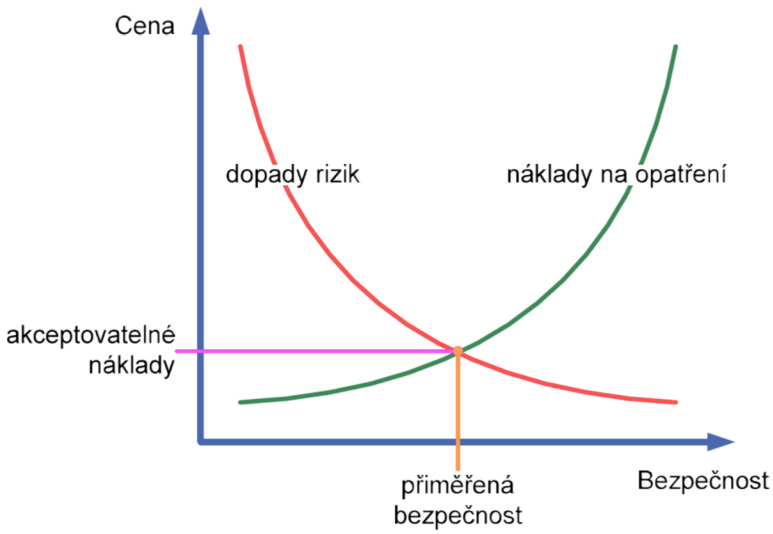
Zajištění přístupnosti k informaci oprávněnému uživateli v požadovaný okamžik [9] [17].

Bezpečnost

Vlastnost nějakého objektu či subjektu, jenž určuje míru a stupeň jeho ochrany proti možným škodám a hrozbám [10].

Přiměřená bezpečnost

Velikost investic a úsilí do bezpečnosti aktiv musí odpovídat hodnotě aktiv a míře možných rizik, jak lze vidět na obrázku 3.3 [9].



Obrázek 3.3: Graf přiměřené bezpečnosti za akceptovatelné náklady [9]

Cíl

Cíl znamená definování výsledku, jenž má být dosaženo. Cíle mohou být [19]:

- strategické
- taktické
- operativní

Cíle se mohou vztahovat k různým disciplínám jako:

- finanční
- zdraví a bezpečnost
- environmentální

Zároveň může být vyjádřen mnoha způsoby, jako třeba plánovaný zisk společnosti, nebo kritéria řízení, díky kterým má společnost možnost navýšit povědomí ohledně informační bezpečnosti ve společnosti nebo také běžnými výrazy, jako jsou úkol či záměr [19].

Organizace

Osoba nebo skupina osob mající jasně přiřazené funkce s náležitými zodpovědnostmi a mající vztah k dosažení svých cílů [19].

Politika

Politika definuje záměry a směr organizace vyjádřený vedením organizace [19].

Bezpečnostní politika

Bezpečnostní politika je soubor pravidel, zvyklosti a směrnic určující způsoby, kterými jsou v organizaci a jejích systémech řízena, chráněna a distribuována aktiva včetně citlivých informací [9].

Aktivum

Za aktiva se považují všechny hmotné i nehmotné statky a vše, co má pro společnost hodnotu [3]. Za nejcennější aktiva se považují peníze, majetek společnosti, data a informace, jejichž vyzrazení, zneužití, pozměnění nebo ztráta může společnosti způsobit škodu [10] [9].

Aktiva se dělí na:

- hmotná
  - hardware, komunikační technologie
- nehmotná
  - pracovní postupy v organizaci v oblasti IS/ICT
  - data vytvořená organizací nebo převzaté datové soubory, které pro provoz důležité
  - programové vybavení skládající se například z vývojového prostředí pro psaní zdrojového kódu, operačních systémů, programového vybavení pro správu počítačových sítí, kryptografických systémů a aplikačního programového vybavení, jakým můžou být textové editory, grafické programy, komunikační aplikace apod.
  - služby, které mohou být komunikační, počítačové, nebo základní služby jako zajištění provozu s dostatečným osvětlením, určitou teplotou v místnostech či správně nastavenou klimatizací
  - know-how

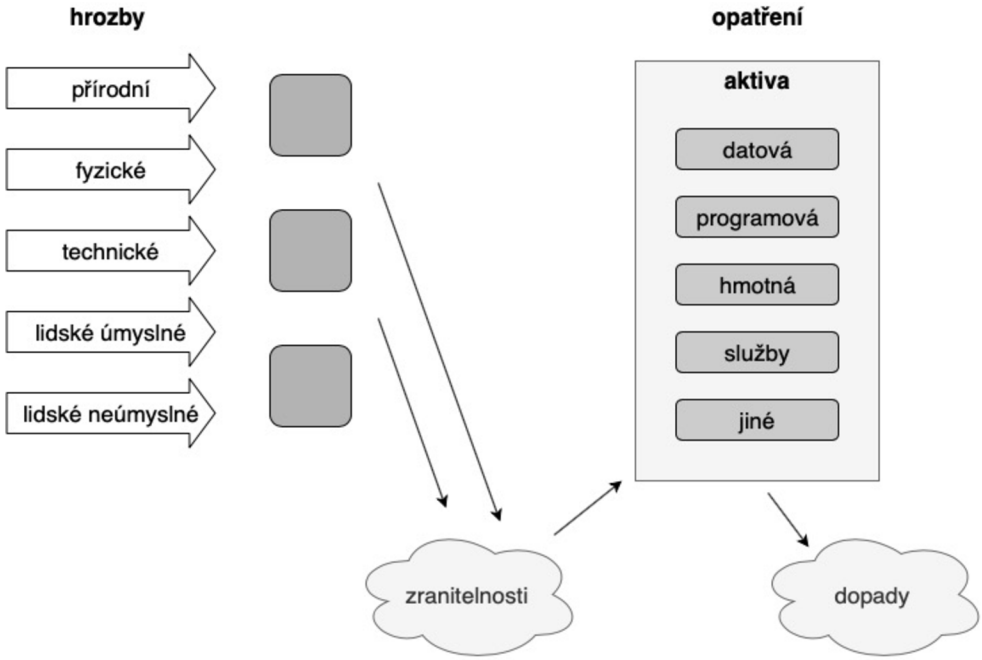
Hrozba

Jedná se o událost ohrožující bezpečnost při zneužití zranitelnosti. [9]. Hrozba je také skutečnost, síla nebo skupina osob, jejichž působení či činnosti můžou způsobit poškození, zničení, ztrátu důvěry nebo hodnoty aktiva. Hrozba může ohrozit bezpečnost například v podobě katastrofy, hackera či zaměstnance. Hrozby lze dělit podle hledisek zejména na [10]:

- objektivní
  - přírodní, fyzické (požár, povodeň, výpadek napětí, poruchy)
  - technické nebo logické, porucha paměti, softwarová (zadní vrátka), špatné propojení jinak bezpečných komponent, krádež, zničení média
- subjektivní
  - neúmyslné způsobené neproškoleným uživatelem či správcem informačního systému

- úmyslné, které je představováno potenciální existencí vnějších útočníků (špiónů, teroristů, konkurentů, hackerů)

Základní schéma zajištění bezpečnosti v IS/ICT představuje vztahy mezi aktivy organizace a hrozbami, které na ně mohou potenciálně působit. Dále možnou zranitelností aktiv reálnými hrozbami, dopady reálných hrozeb na tato aktiva a možnostmi ochrany aktiv organizace formou opatření.



Obrázek 3.4: Schéma zajištění bezpečnosti IS a ICT [10]

Zranitelnost

Zranitelností se myslí nedostatek, slabina nebo stav analyzovaného aktiva, jenž může být subjekt či jeho části a kterého může být využito hrozbou pro uplatnění jejího nežádoucího vlivu [17]. Tato veličina je vlastností aktiva vyjadřující míru citlivosti na působení dané hrozby. [12] Zranitelnost může být zneužita hrozbou způsobem, že dojde k poškození nebo zničení hodnoty aktiv [10]. Zranitelnost lze rozdělit na [3]:

- fyzickou
  - zahrnuje budovy a počítačové místnosti
- technickou spolu s programovými prostředky
  - projevuje se chybou nebo poruchou
- nosičů dat
  - selhání nosiče ve formě nemožnosti přečíst uložená data
- elektromagnetických zařízení

    - plyne ze schopnosti vyzařování, které může například smazat obsah nosiče dat při styku s intenzivním magnetickým polem
- komunikačních systémů a kabelových rozvodů
    - formou přerušení nebo i možným odposlechem komunikace
- personální
    - plyne z úmyslného či neúmyslného chování osob, jejich přirozených chyb

Zranitelné místo

Je místo, které využívá slabinu aktiva ke způsobení jeho škod či ztrátám. Existence zranitelných míst je důsledek chyb, selhání v analýze, při návrhu nebo v implementaci [10].

Opatření

Opatřením se má namysli řízení rizika včetně politik, směrnic, postupů, praktik nebo organizačních struktur, jenž mohou být povahy administrativní, technické, řídící nebo právní [3].

Je to také způsob aktivity umožňující snížení hrozby [9].

Příkladem opatření si lze představit vhodné umístění budov a místností, uzamykání objektů, použití hesel při přístupu k systému při procesu autentizace, detailní testování systému, užití homologovaných a schválených zařízení [3].

Podle charakteru rozdělujeme opatření na [3]:

- administrativní
    - patří zde zejména směrnice pro práci s IS/ICT v organizaci. Příkladem takové směrnice je směrnice pro zálohování dat
- fyzický
    - mezi tato opatření patří používání zámků, trezorů pro ukládání dat, čipové karty pro přístup do různých místností apod.
- technický a technologický
    - zde patří autorizace a autentizace přístupu uživatelů k aktivům IS/ICT, které se projevují například ochranou přístupu do informačního systému prostřednictvím hesel

Dále opatření sledují tyto cíle [3]:

- prevenční
    - předem minimalizovat rizika na co jejich nejmenší míru
    - jde například o odhlášení uživatele při jeho nečinnosti delší než pět minut, automatické uzavírání dveří apod.
- detekční
    - jde o zajištění odhalování potenciálních problémů a hrozeb

    - jedná se například o pravidelné vyhodnocování logovacích a auditních záznamů s možností identifikace bezpečnostních incidentů s případným vyhlášením poplachu

- korekční
    - tato opatření mají zajistit minimalizaci dopadů poté, co hrozba nastala a projevila se
    - takovým příkladem může být odstranění virů z pevných disků počítačů

Riziko

V nejširším slova smyslu riziko znamená vystavení nepříznivým okolnostem. V užším je pak riziko vnímáno jako možnost specifické hrozby využívající specifickou zranitelnost systému. [12]. Dále je rizikem míněna pravděpodobnost, s jakou bude daná hodnota aktiva poškozena nebo zničena působením dané hrozby, která působí na slabé místo této hodnoty. Je to tedy míra ohrožení konkrétního aktiva [10] [17].

Dopad

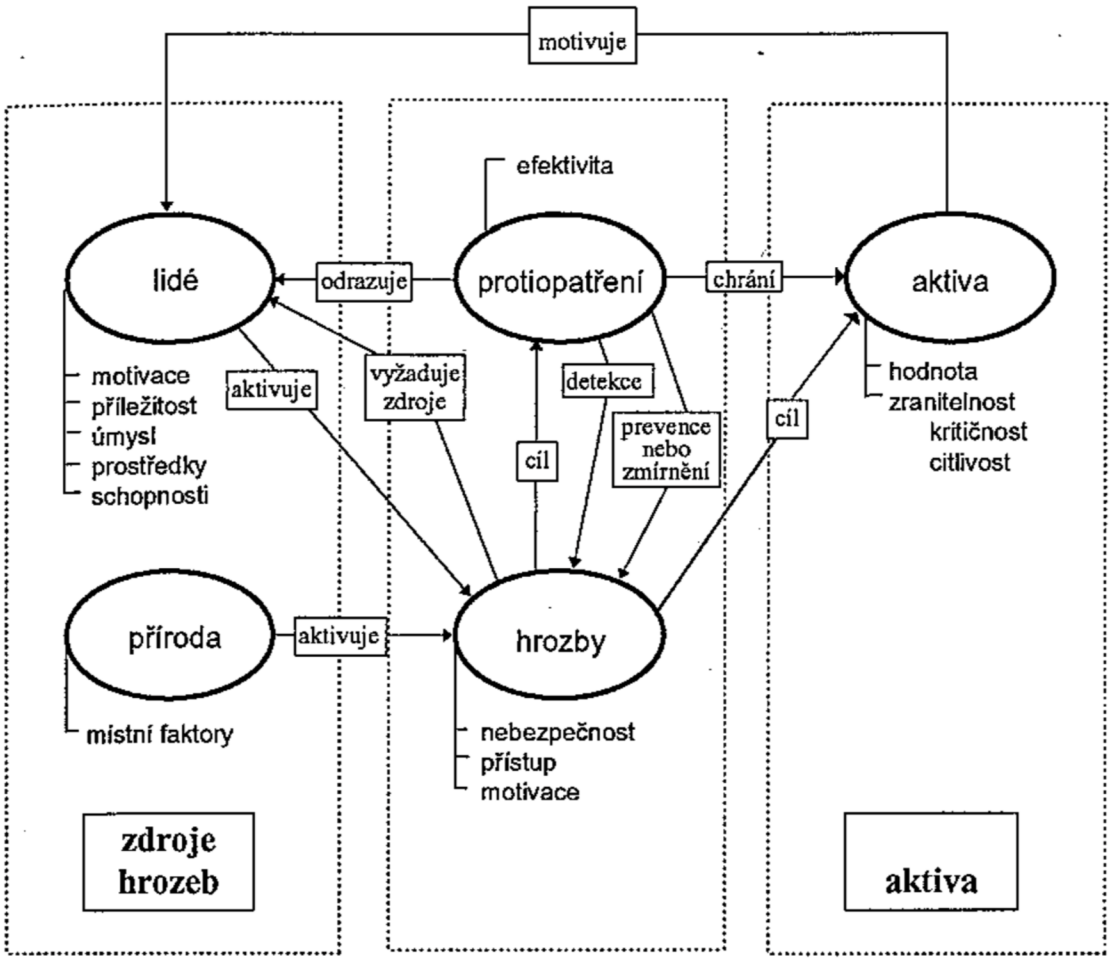
Je vznik škody v důsledku působení hrozby [9].

Řízení rizik

Je koordinace potřebná k řízení a kontrole organizace s ohledem na rizika [9]. Dále je řízením rizik myšlen proces, při němž se subjekt řízení snaží zamezit působení již existujících i budoucích faktorů a navrhuje řešení, která pomáhají eliminovat účinek nežádoucích vlivů. Za kritickou fázi v procesu řízení rizik je výběr vhodného řešení [12]. Zkušenosti získané při řízení rizik se promítly do mezinárodní normy *ISO 31000:2009 - Řízení rizik - Principy a směrnice*. Primární snahou této normy je stanovit obecný rámec řízení rizik, který je platný pro všechny typy organizací [3].

Analýza rizika

Analýzou rizik se myslí systematické používání informací pro odhad míry rizika a určení jeho zdrojů [9]. Na obrázku 3.5 je zobrazeno několik vztahů v analýze rizik, které jsou klíčové pro její úspěšné provedení [12].



Obrázek 3.5: Vztahy v analýze rizik [12]

Ocenění rizik

Je proces vyhodnocení hrozeb, které působí na aktiva, s cílem definovat úroveň rizika, kterému je aktivum společnosti vystaveno. Cílem je zjištění, jsou-li bezpečnostní opatření dostatečná, aby snížila pravděpodobnost vzniku škody na přijatelnou úroveň [10].

Zvládání rizik

Je proces výběru a přijímání opatření pro snížení rizika [9].

Akceptace rizik

Rozhodnutí o tom, zda se riziko příjme či ne [9].

Prohlášení o aplikovatelnosti

Jedná se o dokument s popisem opatření v ISMS organizace [9].

Bezpečnostní událost

Znamená identifikovatelný výskyt systému, služby nebo sítě indikující možné narušení politiky informační bezpečnosti, selhání opatření nebo neznámou předchozí situaci, která může být spojitelná s bezpečnosti informací [19].

Bezpečnostní incident

Jedna nebo série více nechtěných a nečekaných bezpečnostních událostí, které mají vysokou pravděpodobnost kompromitující operace související s obchodní činnosti organizace a ohrožují tak bezpečnost informací [19].

Síťová infrastruktura

Síťová infrastruktura zahrnuje všechny síťové prvky a zařízení použité při realizaci ICT prostředí. Myšlena mohou být také aktiva v oblasti informačních a komunikačních technologií sloužící k vytváření a podpoře informačního systému [9].

Počítačová síť

Je součástí síťové infrastruktury, jenž slouží k realizaci komunikačního prostředí mezi uživateli sítě [9].

Standard

Standardem se má na mysli dokumentovaná úmluva obsahující technické specifikace nebo jiná podobná přesně stanovená kritéria, která jsou důsledně používaná jako pravidla, směrnice, respektive jako definice charakteristických vlastností, jenž zabezpečují, že materiály, výrobky, procesy, služby a podobně jsou takové, jak se původně zamýšlelo. Příkladem může být protokol komunikace či politika poskytování služeb. [9].

Norma

Normou se myslí doporučení pro daný standard nebo řešení. Převážně v ICT se jedná o předpis či směrnici vydávanou různými konsorcii uživatelů a výrobců IT, jedná se tedy o doporučení použitelných standardů k realizaci požadovaného kompatibilního řešení [9].

3.3 Demingův cyklus

Demingův cyklus je metodou postupného zlepšování týkající se zejména služeb, procesů, aplikací či dat probíhající formou opakovaného provádění čtyř základních činností (PDCA) [9]:

- plan — plánuj
  - naplánování zamýšleného zlepšení, záměru
- do — dělej
  - realizace plánu
- check — kontroluj

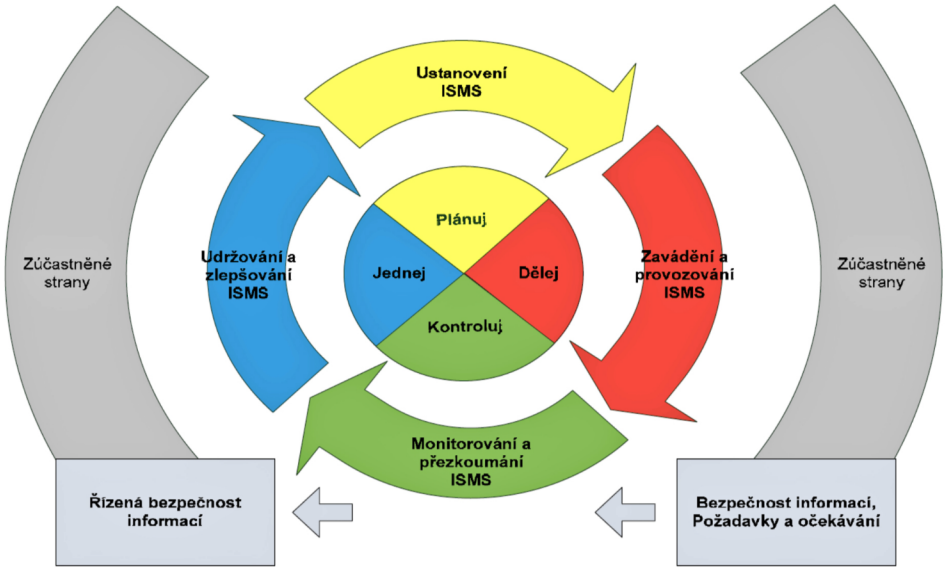
- ověření výsledku realizace oproti původnímu záměru

- act — jednej
  - úpravy záměru i vlastního provedení na základě ověření a plošná implementace zlepšení do praxe

Součástí tohoto modelu PDCA je zároveň dokumentace každé etapy jako jedna z klíčových částí celého modelu [9].

Procesy je třeba:

- identifikovat
- popsat a zdokumentovat
- řídit na základě dokumentace
- následně optimalizovat jejich průběh



Obrázek 3.6: Model PDCA v ISMS [9]

3.4 Systém řízení bezpečnosti informací

Definice systému řízení bezpečnosti informací (zkráceně ISMS) vychází již z jeho samotného názvu. Jedná se o řízení bezpečnosti informací se všemi atributy, které obnáší [9].

Obsahuje politiky, směrnice, procedury a aktivity, jenž jsou společně řízeny organizací, která trvale provádí ochranu informačních aktiv. Systém řízení bezpečnosti informací je systematický přístup k zavedení, implementování, řízení, hodnocení, údržbu a zlepšování informační bezpečnosti v organizaci k docílení jejich cílů a je založen na ohodnocení a akceptaci rizik v organizaci, která byla navržena pro efektivní řízení a nakládání s riziky. Analýzou požadavků na ochranu informačních aktiv a aplikací vhodného opatření těchto

aktiv, což je požadováno, má podíl na úspěšné implementaci systému řízení bezpečnosti informací [19].

Následující základní principy se také podílejí na úspěšném zavedení ISMS [19]:

- uvědomění si potřeby informační bezpečnosti
- přidělení určité zodpovědnosti pro informační bezpečnost
- zavazující začlenění managementu a smluvních stran
- zvyšování společenských hodnot
- ohodnocení rizik vedoucí k jejich řízení tak, aby byla úroveň rizika na přijatelné úrovni
- přijetí bezpečnosti jako základní prvek informačních systémů a sítí
- aktivní prevence a detekce incidentů informační bezpečnosti
- zajistit přístup informační bezpečnosti, který je srozumitelný managementu
- kontinuální
- neustálé přezkoumávání informační bezpečnosti a provádění vhodných úprav dle potřeb

Je třeba si uvědomit, že ISMS je částí celkového systému řízení organizace a využívá model PDCA, který byl představen v sekci 3.3, se čtyřmi následující etapy celého svého životního cyklu [9]:

- ustanovení ISMS
  - určuje rozsah a odpovědnosti
- zavádění a provoz ISMS
  - prosazení vybraných bezpečnostních opatření
- monitorování a přezkoumání ISMS
  - zajištění zpětné vazby a hodnocení řízení
- údržba a zlepšování
  - odstraňování slabin a soustavné zlepšování

Obsahy jednotlivých etap, jenž jsou obsahem norem *ISO/IEC 27001* a *ISO/IEC 27002* podrobně rozepíšu níže.

3.4.1 Ustanovení ISMS

První etapou budování ISMS je jeho ustanovení, při kterém jsou upřesněny vhodné formy řešení bezpečnosti informací. Kromě definice rozsahu ISMS a odsouhlasení *Prohlášení o politice ISMS*, jenž je v podsekci 3.4.1, patří mezi kritické činnosti provedení analýzy rizik a výběr vhodných bezpečnostních opatření pro snížení vlivu existujících rizik. Tato etapa prosazování ISMS by měla být ukončena souhlasem vedení se zavedením ISMS podle potřeb dané organizace, zjištěných při analýze a zvládání rizik ISMS [3].

Ustanovení ISMS je možné rozdělit na následující skupiny činností [3]:

- definice rozsahu, hranic a vazeb ISMS
- definice a odsouhlasení *Prohlášení o politice ISMS* (3.4.1)
- analýza a zvládání rizik
  - definice přístupu organizace k hodnocení rizik
  - identifikace rizika včetně určení aktiv a jejich vlastníků
  - analýza a vyhodnocení rizik
  - identifikace a ohodnocení variant pro zvládání rizik
  - výběr cílů a jednotlivých opatření pro zvládání rizik
- souhlas vedení organizace s navrhovanými zbytkovými riziky a se zavedením ISMS
- příprava *Prohlášení o aplikovatelnosti* (3.4.1)

Tato etapa budování má zásadní dopady na fungování ISMS během jeho úplném životního cyklu [3].

Prohlášení o politice ISMS

Z praktického hlediska je důležité, aby politika politika ISMS [3]:

- upřesnila cíle ISMS a definovala základní směr a rámec pro řízení bezpečnosti informací
- zohlednila cíle a požadavky organizace a související zákonné, regulativní a smluvní požadavky
- vytvořila potřebné vazby pro vybudování a údržbu ISMS v dané organizaci
- stanovila kritéria, podle kterých jsou popisována a hodnocena rizika
- byla schválena vedením organizace

Jedná se svým způsobem o krátký, za to však významem velmi důležitý dokument, jelikož jsou v něm prezentovány zájmy vedení organizace o řízení bezpečnosti informací a definuje klíčové podmínky pro ohodnocení rizik, což je základem pro celý ISMS. Správně definovaná politika ISMS může hodně usnadnit budoucí prosazování pravidel a požadavků na bezpečnost informací v organizaci [3].

3.4.2 Zavádění a provoz ISMS

Tato etapa životního cyklu ISMS věnuje pozornost na prosazení všech bezpečnostních opatření tak, jak byla navržena v předchozí etapě při ustanovení ISMS. Důležité je především připravit dílčí plány, ve kterých jsou upřesněny termíny, odpovědné osoby apod. [3].

Během této etapy zavádění ISMS je nezbytné provést následující činnosti [3]:

- formulovat dokument *Plán zvládání rizik*, jenž je v odrážkovém seznamu níže 3.4.2 a započít s jeho zaváděním

    - tento dokument je pro zvládání rizik důležitým, jelikož popisuje všechny činnosti ISMS, které jsou potřebné pro řízení bezpečnostních rizik, stanovené cíle a priority těchto činností a potřebné zdroje, jako jsou personální, technologické, znalostní, finanční apod.

- zavést plánovaná bezpečnostní opatření a zformulovat příručku bezpečnosti informací, která upřesní pravidla a postupy aplikovaných opatření definovaných oblastech bezpečnosti informací (podsekce 3.6)
- definovat program budování bezpečnostního povědomí a provést přípravu a zaškolení všech uživatelů, manažerů a odborných pracovníků z úseku informatiky a z oblasti řízení bezpečnosti
- upřesnit způsoby měření účinnosti bezpečnostních opatření a sledovat stanovené ukazatele
- zavést postupy a další opatření pro rychlou detekci a reakci na bezpečnostní incidenty
- řídit zdroje, dokumenty a záznamy ISMS

3.4.3 Monitorování a přezkoumání ISMS

Hlavním úkolem etapy zavádění ISMS je zajištění účinné zpětné vazby. V souvislosti s tímto požadavkem by proto mělo dojít k prověření všech aplikovaných bezpečnostních opatření a jejich důsledků na ISMS. Vlastní ověření začíná u přímé kontroly odpovědných osob ze strany jejich nadřízených či bezpečnostním manažerem. Důležitou roli také sehrává nestranné posouzení fungování a účinnosti ISMS pomocí auditů ISMS, jenž jsou provedeny interně [3].

Obecným cílem všech použitých zpětných vazeb je připravit dostatek podkladů o reálném fungování ISMS, které budou předloženy vedení za účelem přezkoumání, zda je realizace ISMS v souladu s obecnými požadavky organizace. Během této části zavádění ISMS je nutné provést tyto činnosti [3]:

- monitorovat a ověřit účinnost prosazení bezpečnostních opatření
- provést interní audity ISMS, jejichž náplň pokryje celý rozsah ISMS
- připravit zprávu o stavu ISMS a na jejím základě přehodnotit ISMS na úrovni vedení organizace

3.4.4 Údržba a zlepšování ISMS

Poslední etapou celého cyklu prosazování ISMS je jeho udržování a zlepšování. V této fázi je potřeba sbírat podněty ke zlepšování ISMS a napravovat tak všechny nedostatky či neshody, které se v ISMS objevují [3].

3.4.5 Přehled dokumentace ISMS

Povinná dokumentace pro ISMS se skládá z těchto částí [13]:

- rozsah ISMS
- bezpečnostní politika

- popis metodologie hodnocení rizik
- zpráva o hodnocení rizik
- prohlášení o aplikovatelnosti
- plán zvládání rizik
- zdokumentované postupy opatření
- záznam o fungování a účinnosti ISMS
- přezkoumání ISMS

3.5 Normalizační instituce

Spolu s oficiálními mezinárodními a národními normalizačními organizacemi, které vydávají normy mnohdy označované jako *de jure* standardy, působí v oblasti bezpečnosti řada dalších organizací, konsorcií a různých sdružení, které vydávají tzv. *de facto* standardy [9].

Mnohé *de jure* standardy, normy, vznikly následným přijetím *de facto* standardů některou z oficiálních normalizačních institucí [9].

Typickým příkladem *de facto* standardů jsou standardy sítě Internet. Tyto standardy jsou známé pod označením RFC[1] [9].

3.5.1 ISO

Úplný název zkratky ISO je *International Organization for Standardization* a jeho úkolem je podporování rozvoje standardizačních aktivit ve světě se zaměřením na usnadnění mezinárodních směn zboží a služeb a na spolupráci ve sféře intelektuálních, vědeckých, technologických a ekonomických aktivit [9].

3.5.2 IEC

Celým názvem *International Electrotechnical Commision* je celosvětová organizace připravující a vydávající mezinárodní normy z oblasti elektrotechnických, elektronických a jim příbuzných, jako je elektřina, magnetismus, elektromagnetismus, elektroakustika, multimédia, telekomunikace, výroba a distribuce energií, terminologie, měření, navrhování a také bezpečnost [9].

3.5.3 ITU

ITU je zkratkou pro *International Telecommunications Union* a jedná se o mezinárodní organizací spadající do hierarchie OSN[2]. Normalizační aktivity ITU, které již podpořily růst nových technologií jako například mobilní technologie a internet, nyní obrací svůj zájem na stavební prvky objevující se v globální informační infrastruktuře. Dále pak k tvorbě vyspělých multimediálních systémů, které využívají slučování hlasových, datových, zvukových a video signálů. ITU má svou vedoucí roli ve správě spekter rádiové frekvence a tím zaručuje , že rádiově založené systémy jako jsou mobilní telefony a pagery[3], letecké

[1] Request for Comment
[2] Organizace spojených národů
[3] Malé osobní telekomunikační zařízení, které umožňuje přijímat krátké textové zprávy

a námořní naváděcí systémy, vědecké výzkumné stanice, satelitní komunikace a rádiové a televizní vysílání dál hladce pokračují ve své činnosti a poskytují spolehlivé bezdrátové služby celému světu [9].

Technickou práci uskutečňují studijní skupiny, které jsou složeny z odborníků nejdůležitějších telekomunikačních organizací. Tyto skupiny připravují studie, které vedou k vydání směrodatných ITU doporučení (ITU Recommendations) [9].

Organizace ISO, IEC a ITU vydávají tzv. *základní normy*, které mají celosvětovou působnost. Při vypracovávání norem společně úzce spolupracují.

3.5.4 ČSNI

ČSNI neboli *Český normalizační institut* byl zpočátku zřízen jako státní příspěvková organizace, ale v současné době patří mezi organizace podřízené Ministerstvu průmyslu a obchodu [9].

ČSNI má statut národní normalizační organizace zastupující národní zájmy v mezinárodních a evropských normalizačních organizacích. Institut je členem mezinárodních normalizačních organizací ISO/IEC, evropských normalizačních organizací CEN[4] a CENELEC[5] a zastává funkci národní normalizační organizace v evropském normalizačním institutu pro telekomunikace ETSI[6] [9].

ČSN[7] vzniká dvojím způsobem [9]:

- přejímáním evropskách a mezinárodních norem do soustavy českých technických norem formou ČSN EN (ČSN IEC, ČSN ISO, ČSN ETS, atd.)
- tvorbou původních ČSN vyplývajících z národních potřeb a z hledisek zachování funkčnosti fondu ČSN.

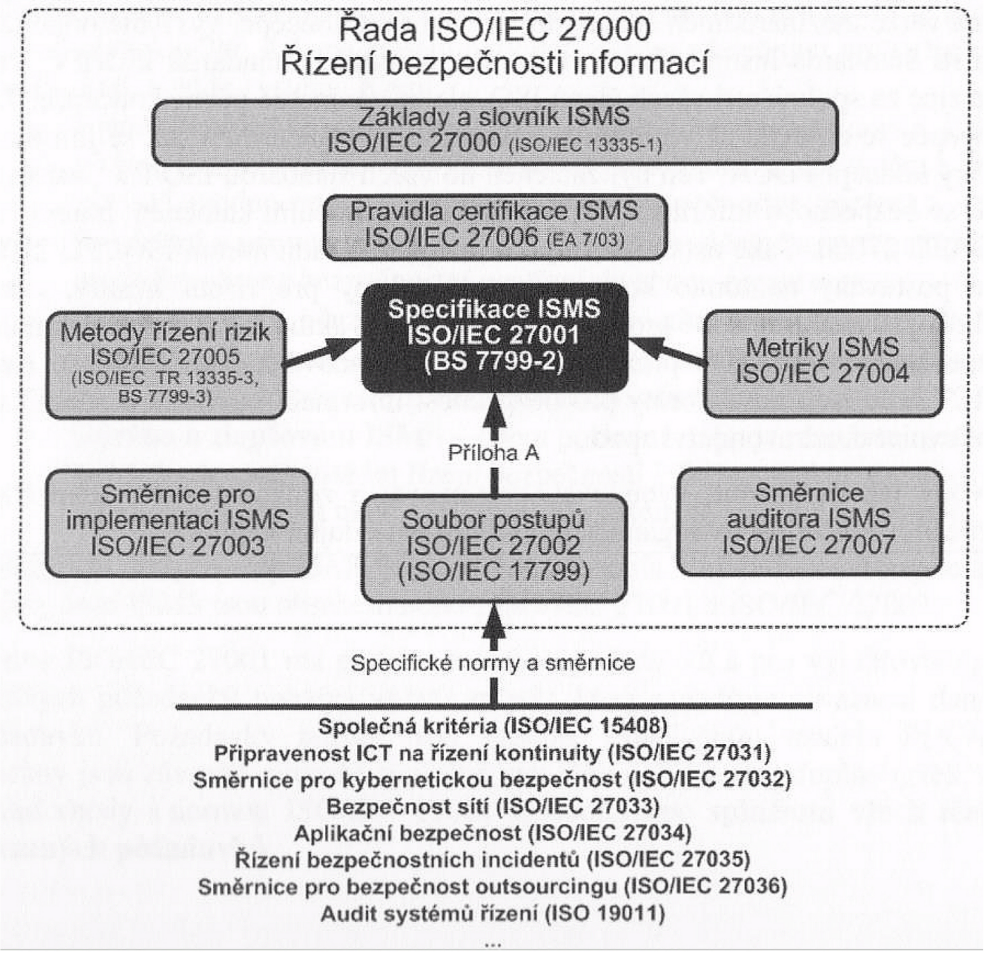
3.6 Normy

V této sekci seznámím čtenáře s mezinárodními normami řadou ISO/IEC 27000, které jsou zároveň nazývané jako *řada norem ISMS* [19]. Poté vyberu a zároveň představím převážně ty normy, ze kterých jsem při realizaci čerpal. V době psaní této diplomové práce jsou využity nejaktuálnější normy z roku 2017, které byly novelizovány normami z roku 2014.

Rodina těchto norem má pomoci organizacím všech typů a velikostí zavést a provozovat systém ISMS [19] [9].

Pro systém řízení bezpečnosti informací je nejvýznamnější mezinárodní norma řady ISO/IEC 27001 [3].

[4] European Committee for Standardization
[5] European Committee for Electrotechnical Standardization
[6] European Telecommunications Standards Institute
[7] Česká technická norma



Obrázek 3.7: Řada norem ISO/IEC 27000 [3]

ČSN ISO/IEC 27000

ČSN ISO/IEC 27000:2017 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Přehled a slovník

Tato mezinárodní norma poskytuje přehled systémů řízení bezpečnosti informací tvořící předmět rodiny norem ISMS a definující související termíny. Termíny a definice uvedené v této normě se týkají termínů a definic použitých obecně v rodině norem ISMS, nikoliv všech termínu a definic [9] [19].

Organizace mohou s využitím rodiny norem ISMS vyvinout a implementovat rámec pro řízení bezpečnosti svých bezpečnostních aktiv a připravit nezávislé ohodnocení týkající se ochrany informací, které mohou být například v podobě finančních informací, duševního vlastnictví a podrobnosti o zaměstnancích, nebo informací svěřených zákazníky nebo třetími stranami [9].

Rodina norem ISMS zahrnuje normy, které definují požadavky na ISMS. Dále normy, které tyto požadavky certifikují a normy poskytující přímou podporu, podrobné pokyny nebo interpretaci pro všechny procesy PDCA, které byly představeny v sekci 3.3 a které se zabývají směrnicemi pro ISMS specifickými pro jednotlivá odvětví a normy, které se zabývají posuzováním shody ve vztahu k ISMS [9].

ČSN ISO/IEC 27001:2017

ČSN ISO/IEC 27001:2017 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky

Norma nabízí doporučení jak aplikovat vybraná opatření v rámci procesu ustavení, provozu, údržby a zlepšování systému managementu bezpečnosti informací v organizaci. Norma prosazuje přijetí procesního přístupu k řešení ISMS a zavádí model známý jako PDCA, jenž byl představen v sekci 3.3, který může být aplikován na všechny procesy ISMS definované touto normou [20] [9].

V hlavní části této normy jsou specifikovány požadavky na vybudování, zavedení, provoz, monitorování, přezkoumání, udržování, zlepšování a případnou certifikaci zdokumentovaného systému managementu bezpečnosti informací. Zároveň se zde specifikují požadavky na výběr a zavedení bezpečnostních opatření, jenž chrání informační aktiva. V příloze jsou uvedeny cíle opatření a jednotlivá opatření [9] [20].

ČSN ISO/IEC 27002:2017

ČSN ISO/IEC 27002:2017 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Soubor postupů

Norma obsahuje bezpečnostní opatření podporující dosahování cílů organizace. Odpovědnost je za ně možné jednoduše přiřadit osobám s odpovídajícími funkcemi. Díky tomu lze velmi rychle zjistit stav bezpečnosti informačního systému organizace a zároveň vytvořit východiska pro jeho zlepšení, zejména vymezením oblastí, které nejsou dostatečně zajištěny [9].

V navzájem propojeném světě jsou informace a související procesy, systémy, sítě a pracovníci podílející se na jejich provozování, nakládání s nimi a ochraně aktiva, kterou jsou, stejně jako jiná významná obchodní aktiva, cenná pro podnikání organizace, a proto si zaslouží nebo vyžadují ochranu proti různým rizikům [21].

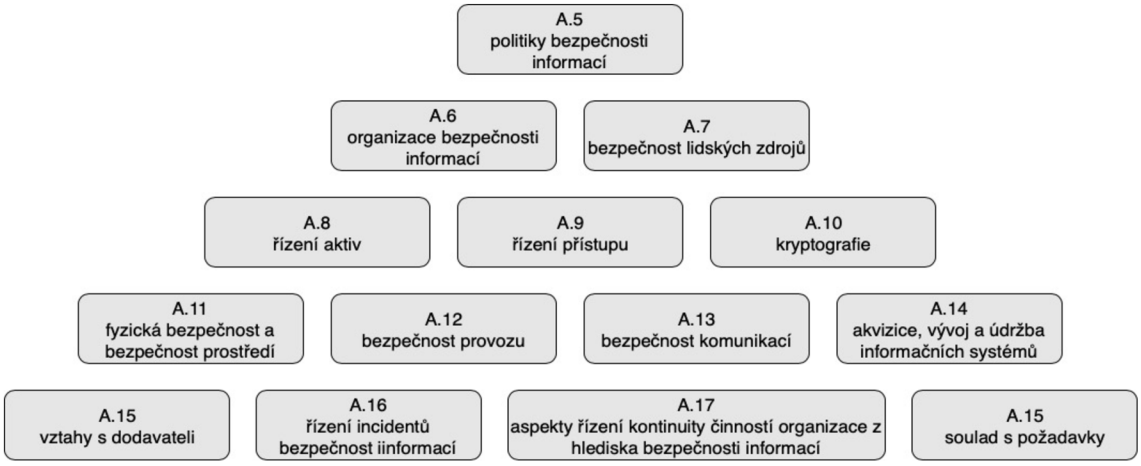
Aktiva jsou vystavena jak úmyslným tak neúmyslným hrozbám, zatímco související procesy, systémy, sítě a lidé mají vlastní zranitelnosti. Změny obchodních procesů a systémů nebo jiné vnější změny (například nové zákony a předpisy), mohou vytvářet nová rizika bezpečnosti informací. Proto, vzhledem k množství způsobů, kterými mohou hrozby zneužít zranitelnosti k poškození organizace, jsou rizika bezpečnosti informací vždy přítomna. Efektivní bezpečnost informací snižuje tato rizika tím, že chrání organizace před hrozbami a zranitelnostmi, čímž omezuje dopady na její aktiva [21].

Bezpečnost informací je dosažena zavedením vhodného souboru bezpečnostních opatření, včetně politik, procesů, postupů, organizačních struktur a softwarových a hardwarových funkcí. Tato opatření je potřeba stanovit, implementovat, monitorovat, přezkoumávat a zlepšovat tam, kde je to nutné, aby bylo zajištěno, že jsou splněny specifické cíle bezpečnosti a podnikatelské činnosti organizace. Systém ISMS, jako například systém specifikovaný v ISO/IEC 27001, používá holistický, koordinovaný pohled pohled na rizika bezpečnosti informací organizace se záměrem implementovat komplexní sadu opatření bezpečnosti informací v celkovém rámci uceleného systému řízení [21].

Mnoho informačních systémů nebylo navrženo tak, aby byly bezpečné ve smyslu normy ISO/IEC 27001 a této normy. Bezpečnost, které může být dosaženo technickými prostředky, je omezená a měla by být podporována vhodným řízením a postupy. Identifikace opatření, která by měla být zavedena, vyžaduje důsledné plánování a věnování pozornosti detailům. Úspěšný systém ISMS vyžaduje podporu ze strany všech zaměstnanců v dané organizaci [21].

Tato norma obsahuje 14 kapitol týkajících se opatření bezpečnosti společně obsahujících celkem 35 hlavních kategorií bezpečnosti a 114 kontrol [21].

Tyto kapitoly neboli oblasti ISMS jsou zobrazeny podle [21] v obrázku 3.8.



Obrázek 3.8: Oblasti ISMS podle normy ISO/IEC 27002 [21]

ČSN ISO/IEC 27003:2017

ČSN ISO/IEC 27003:2017 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Směrnice pro implementaci systému řízení bezpečnosti informací

V této normě je možné nalézt doporučení pro ustanovení a implementaci systému řízení bezpečnosti informací v souladu s požadavky normy ISO/IEC 27001. Norma je použitelná pro všechny typy organizací, které chtějí zavést ISMS. Norma objasňuje proces implementace ISMS. Výsledkem tohoto procesu je finální plán implementace projektu ISMS. Na základě tohoto plánu lze v organizaci realizovat projekt implementace ISMS. Norma popisuje proces plánování implementace ISMS v pěti etapách [9]:

1. získání souhlasu vedení organizace se zahájením projektu ISMS
2. definování rozsahu, hranic a politiky ISMS
3. provedení analýzy požadavků bezpečnosti informací
4. provedení hodnocení rizik a plánování zvládání rizik
5. návrh ISMS

Specifický finální plán implementace projektu ISMS organizace je hlavním výstupem poslední páté etapy. Zahrnuje návrh organizace bezpečnosti informací, bezpečnosti ICT, fyzické bezpečnosti a návrh dalších opatření naplňujících specifické požadavky ISMS jako je například zvyšování povědomí v oblasti bezpečnosti informací [9].

ČSN ISO/IEC 27005:2018

ČSN ISO/IEC 27005:2018 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Řízení rizik bezpečnosti informací

Tato mezinárodní norma poskytuje doporučení pro řízení rizik bezpečnosti informací v rámci organizace. Podporuje obecný koncept specifikovaný v ISO/IEC 27001 a je strukturována takovým způsobem, aby dostatečně podporovala implementaci informační bezpečnosti založené na přístupu rizik. Nicméně tato mezinárodní norma nenabízí konkrétní metodiku, tedy postup pro řízení rizik bezpečnosti informací. Záleží jen na organizaci, který způsob přístupu k řízení rizik zvolí, například v závislosti na rozsahu ISMS či kontextu řízení rizik. Norma je určená vedení společnosti, manažerům a pracovníkům, kteří jsou v rámci organizace odpovědní za řízení rizik bezpečnosti informací a tam, kde je to relevantní, také extrémním subjektům. Je aplikovatelná na všechny typy organizací (např. komerční společnosti, vládní organizace, neziskové organizace), které mají v úmyslu řídit rizika, která mohou narušit bezpečnost informací organizace [9].

3.7 Metodiky a rámce

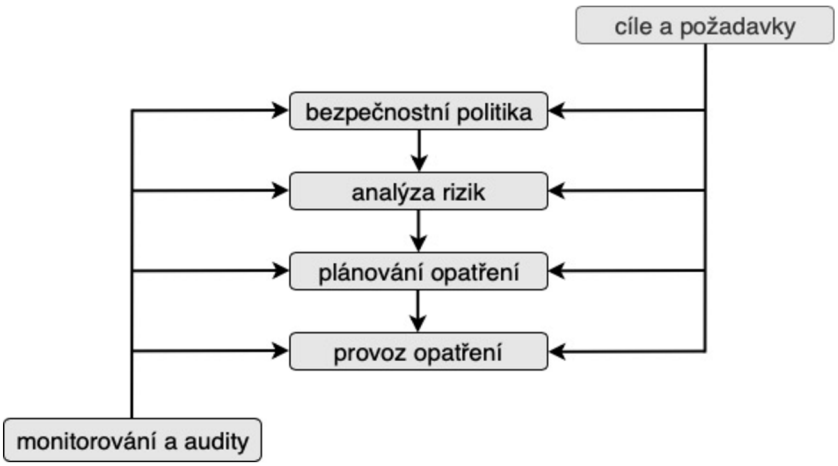
Z pohledu bezpečnosti informací zde představím rámec ITIL a metodiku COBIT, které jsou obecněji zaměřené a kromě oblasti řízení bezpečnosti se zabývají i dalšími aspekty týkající se řízení informatiky organizací. Tato metodika a rámec jsou celosvětově známé a rozšířené a v organizacích slouží jako podpora v podobě různých standardů, metodik a tzv. *best practises* [3].

3.7.1 ITIL

Information Technology Infrastructure Library (zkráceně ITIL) je rámec (nikoliv metodika) přístupů pro zajištění dodávky kvalitních IT služeb za přiměřených nákladů. Tento rámec vychází z nejlepších praktických zkušeností a knihovnu spravuje organizace *Office of Government Commerce* a je šířena formou knih, CD, školení, konzultací či certifikací [9].

V současnosti je ITIL již de-facto mezinárodním standardem pro oblast řízení IT služeb. (vizte *http://www.ogc.gov.uk/*) [9].

Knihovna ITIL je rozdělena do několika částí, které se zaměřují na specifickou oblast řízení IT služeb, jenž odpovídají zásadním procesům v IT oddělení a vzájemně se prolínají. Dodávka IT služeb (IT Service Delivery) a podpora IT služeb (IT service Support) se běžně dohromady označují jako IT Service Management (ITSM) [9].



Obrázek 3.9: Základní procesy řízení bezpečnosti informací dle ITIL [9]

Z knihovny ITIL předkládá sadu osvědčených postupů tzv. *best practises* z oblasti řízení služeb ICT. Pokud jsou tyto postupy implementovány, napomáhají k dosažení určité kvality. Z knihovny ITIL vychází britský standard *BS 15000* a norma *ISO/IEC 20000* [9].

Jak již bylo řečeno,ITIL není norma, ale knihovna obsahující doporučení a osvědčené postupy tzv. *best practises* [9].

Nová verze knihovny s označením *ITIL V3* snižuje počet knih a ve své koncepci se podřizuje životnímu cyklu služeb IT jako [3]:

- strategie služeb (service strategy)
    - základ rámce představující propojení aktivit organizace se strategií v oblasti IT a informační strategií
- návrh služeb (service design)
    - obsahuje návrhy služeb IT, jako je outsourcing či insourcing
- implementace služeb (service transition)
    - zahrnuje návody na implementaci služeb do reálného prostředí. Zahrnuje procesy jako řízení verzí, návrhy kontrol pro uvádění služeb do provozu aj.
- provoz služeb (service operation)
    - podporuje správu služeb v produktivním prostředí, řešení problémů, poruch, stanovení ukazatelů jakosti apod.
- průběžné zlepšování (continual service improvement)
    - pomáhá zlepšovat zavedené existující služby

Rámec ITIL se odjakživa vyznačoval několika charakteristickými znaky jako [3]:

- procesní přístup
    - považován za jeden z primárních znaků pro řízení informatiky a informatických služeb
- nejlepší zkušenosti
    - hlavním důvodem oblíbenosti rámce ITIL je jeho shrnutí tzv. *best practises* z praxe a díky rostoucímu množství implementací a tím i lidí znalých této problematiky se otevírá prostor pro její další zdokonalování
- respektování individuality
    - poskytuje návod, co by se mělo udělat, ale nikoliv jak by se to mělo udělat. Z toho důvodu poskytuje implementace organizacím dostatečnou volnost
- zákaznická orientace
    - základní myšlenkou je zvyšování práce zaměstnanců pomocí zvyšování jejich spokojenosti
- jednotná terminologie

    - špatná komunikace a nekonzistentní terminologie je zapotřebí pro vyhnutí se komunikačním problémům a šumu vzniklého uvnitř i mimo organizaci

- nezávislost na platformě
    - definuje hranice, pravidla a vazby a tím organizaci dává dostatečnou volnost
    - nezáleží totiž na tom, jaká informační a komunikační infrastruktura je řízena ani na službách, které jsou touto infrastrukturou poskytovány

V této verzi *ITIL V3* je proces Information Security Management (ISM) součástí cyklu služeb zmíněného výše v seznamu s odrážkami 3.7.1. Jedná se tak o nový proces, který má zajistit důvěrnost, integritu a dostupnost aktiv, informací, dat a služeb IT organizace. Zároveň nová verze intenzivně pracuje s řízením rizik včetně bezpečnostních rizik, skrze které se bezpečnost promítá do celého životního cyklu služby IT [3].

3.7.2 COBIT

Control Objectives for Information and Related Technology (zkráceně COBIT) je mezinárodně uznávanou metodikou opírající se o soubor všeobecně uznávaných praktik řízení informačních a komunikačních technologií, tak aby využití informací a nasazení ICT přispívalo k dlouhodobému rozvoji organizace. Zároveň je kladen důraz, aby metodika prohlubovala strategické cíle organizace a snižovalo rizika související s použitím ICT [9].

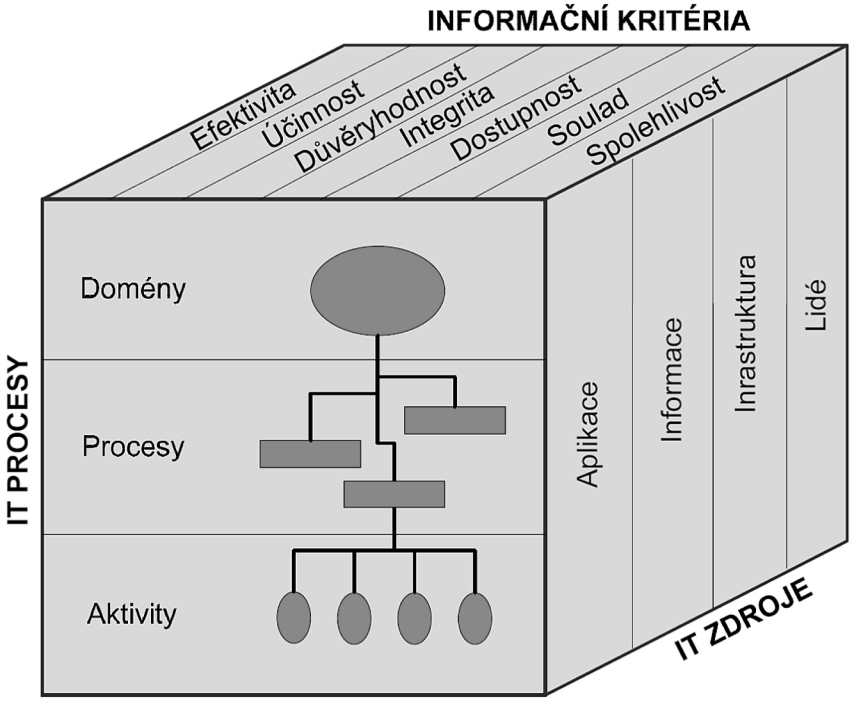
Cílem metodiky je propojení principů obecného řízení organizace s pravidly, která jsou uplatňována v IT prostředí. COBIT vychází z tvz. *best practice* a při jejím vyhotovení byl využit širší okruh zdrojů, jako například [9]:

- COSO (Committee of Sponsoring Organizations)
- ITIL (IT Infrastructure Library)
- ISO/IEC 27000
- CMMI (Capability Maturity Model Integration)
- PMBOK (Project Management Body of Knowledge)

Základní snahou této metodiky je jasně strukturovat velmi složitý systém řízení IT do srozumitelné struktury pro řídící pracovníky a uživatele bez hlubších znalostí IT. Metodika COBIT dovoluje těmto pracovníkům sestavit vhodná objektivní kritéria, podle kterých bude možné posuzovat úspěšnost či neúspěšnost jednotlivých oblastí řízení IT.

Metodika COBIT vychází z rámce ITIL. Z toho vyplývá, že se jedná o komplexnější metodiku. ITIL však řeší mnohem detailněji vybrané oblasti. Experti v oblasti doporučují kombinaci těchto dvou přístupů, jenž vedou ke splnění požadavků, které jsou kladeny na konkrétní prostředí a organizaci [3].

COBIT je často zobrazen v podobě multidimenzionální kostky, která je znázorněna na obrázku 3.10.



Obrázek 3.10: Kostka COBIT [9]

Jednotlivé dimenze COBIT kostky jsou:

- informační kritéria
  - v první dimenzi jsou kladeny požadavky na informace z pohledu efektivity, účinnosti, důvěryhodnosti, integrity, dostupnosti, souladu a spolehlivosti
- zdroje IT
  - druhá dimenze je tvořena zdroji jako jsou aplikace, informace, infrastruktura a lidé
- proces IT
  - poslední dimenze se skládá z procesů, které jsou rozděleny na domény, procesy a aktivity

3.8 GDPR

GDPR neboli *Obecné nařízení na ochranu osobních údajů* je doposud nejvíce uceleným souborem pravidel na ochranu dat na světě [22].

GDPR se týká všech, jež shromažďují, ukládají nebo zpracovává osobní údaje uživatelů z Evropy, včetně organizací a institucí mimo území EU[8], které působí na evropském trhu [22].

Nařízení cílí na všechny, ať už jde o jednotlivce, firmy či instituce, které zacházejí s osobními údajů skrze veškeré odvětvími od [22]:

- zaměstnanců
- zákazníků
- klientů
- dodavatelů

Nařízení s sebou přináší rovnocennou vymahatelnost práva v rámci celé EU. Dále pak stejné sankce a mnohem těsnější spolupráci státních orgánů. Nejen že budou muset být lidé o svých právech detailně informováni, ale budou pak moci po správcích údajů vyžadovat i to, co nebylo předtím možné. Jedná se například o právo vznést námitku proti zpracování dat o uživateli, kdy správce po takové námitce nebude moci uložené údaje nadále zpracovávat, nebude-li mít k tomu závažné a prokazatelné důvody. Dále jde o právo na přenositelnost osobních údajů od jednoho správce ke správci druhému, jestliže jsou údaje zpracovávány automatizovaně [22].

V rámci celé EU je GDPR účinné od *25. května 2018*. V České republice nahradí aktuální právní úpravu ochrany osobních údajů, která má směrnici *95/46/ES* a související *zákon č. 101/2000 Sb.*, o ochraně osobních údajů [22].

GDPR zároveň řeší *souhlas se zpracováním osobních údajů*, což znamená, že pokud je zpracování založeno na souhlasu, musí být správce schopen doložit, že fyzická osoba udělila souhlas se zpracováním svých údajů svobodně a byl konkrétní, informovaný, specifický a ničím nepodmíněný. Jedná se o dobrovolný projev vůle entity údajů, ke kterému nesmí být nucen [22].

[8] Evropská unie

3.9 Firemní procesy

Podle Systému managementu kvality je proces definován jako soubor vzájemně souvisejících nebo vzájemně působících činností, které přeměňují vstupy na výstupy [18].

Proces má následující základní znaky [14]:

- je opakovatelný
- jeho výstupem je produkt nebo služba s přidanou hodnotou
- je měřitelný parametry (náklady, čas, kvalita)
- má svého vlastníka (osoba či pracovní tým, jenž jsou zodpovědní za zlepšování a kontrolu)
- má zákazníka (interní, externí)
- má vymezen jeho začátek a konec a návaznost na další procesy
- využívá podnikové zdroje jako finance, hmotné nebo lidské

Procesy můžeme rozdělit do tří kategorií [14]:

- řídící procesy
  - zabezpečují rozvoj a řízení výkonu společnosti a vytvářejí podmínky pro fungování ostatních procesů
- hlavní procesy
  - vytvářejí hodnotu v podobě výrobku nebo služby pro externího zákazníka, jsou tedy součástí hodnotového řetězce organizace
- podpůrné procesy
  - zajišťují podmínky pro fungování ostatních procesů tím, že jim dodávají hmotné i nehmotné výstupy, přitom ale nejsou součástí hodnototvorného řetězce

Kapitola 4

Analýza současného stavu

V této kapitole představím společnost spolu s jejími nejhlavnějšími procesy, které firmě generují zisky. Poté provedu analýzu bezpečnosti vybraných oblastí ve společnosti. Následně zanalyzuji legislativní změny týkající se nové vyhlášky o kybernetické bezpečnosti a obecného nařízení na ochranu osobních údajů. Závěrem kapitoly zanalyzuji konkurenční prostředí, které patřičně zhodnotím. Kapitolu zakončím hlavními požadavky společnosti a jejím očekáváním od této práce.

4.1 Představení společnosti

Ihned z počátku je potřeba brát v úvahu, že tato diplomová práce je vypracována na základě reálné společnosti a téma zaměření práce se týká bezpečnosti. Z toho důvodu si společnost nepřeje uvést název a informace, které by mohly vést k odhalení společnosti a možnému narušení její bezpečnosti.

Společnost je dceřinou společností jedné ze švýcarských společností se sídlem v Curychu, která se zaměřuje na digitalizaci finančního poradenství, jež je aktuální trend ve finančním světě a nynější moto společnosti. Mateřská společnost na švýcarské straně je jediným zadavatelem práce a vyplývá z toho česko-švýcarský vztah. To v sobě skrývá velký potenciál úspěchu na švýcarském trhu. Důvodem je daleko levnější pracovní síla v České republice, a to až trojnásobně, než ve Švýcarsku. Pro srovnání uvádím tabulku rozdílů měsíčních mezd v českých korunách [11] [5] [7]. Pro přepočet jsem v době psaní této diplomové práce použil kurz 22 Kč za 1 švýcarský frank [6].

pozice	průměrná mzda (Švýcarsko)	průměrná mzda (Česko)
byznys analytik	192 500	60 000
grafický designér	165 500	85 000
projektový manažer	214 500	70 000
vývojář junior	110 000	45 000
vývojář senior	200 000	80 000

Tabulka 4.1: Průměrná měsíční mzda pro danou pracovní pozici v Kč

Tato skutečnost poskytuje mateřské společnosti dovolit si přijmout daleko větší počet odborníků, než firmám působícím pouze na švýcarském trhu. Zároveň je možné ušetřené náklady využít například na:

- přizpůsobení cenotvorby produktové licence finančním společnostem
- propagování a zviditelnění společnosti skrze marketing či sponzoring
- účasti společnosti na finančních konferencích
- pořádání vlastních konferencí
- inovaci webových stránek
- školení zaměstnanců
- reprezentativní a moderní kanceláře

4.1.1 Organizační struktura

Aktuální počet zaměstnanců na švýcarské straně v době psaní této diplomové práce je 24 a zastávají následující role:

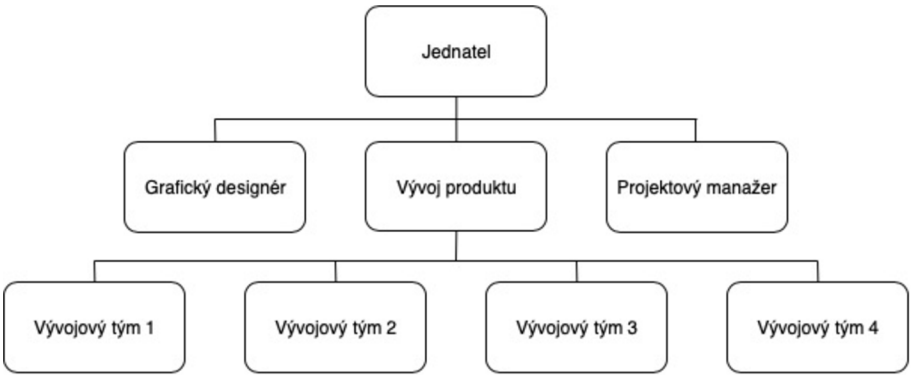
- vedení společnosti
- vedoucí projektů
- byznys analytici
- oddělení prodeje a inovací
- office manažerka[1]

Z důvodu zaměření se převážně na českou stranu firmy znázorním hierarchickou organizační strukturu detailněji a pro jednoduchost neuvedu komplexní strukturu složenou ze dvou firem.

Na české straně se aktuální počet pracovníků blíží k číslu 25 a má v plánu pokračovat z důvodu neustále přibývajících požadavků týkajících se rozšiřování stávajících modulů, založení modulů zcela nových, přidávání nových funkcionalit do stávajících modulů v aplikaci, změna požadavků na již implementovanou funkcionalitu, redukce technického dluhu[2] a v neposlední řadě údržba zdrojového kódu. Společnost má aktuálně pronajaté kancelářské prostory o velikosti 220 m^2 a již v době psaní této práce se poohlíží po nových a větších prostorech pro své budoucí sídlo.

[1] Řídí provoz kanceláře spolu s odpovědností za každodenní provoz

[2] Nedodržováním praktik čistého kódu vede ke skrytým chybám a dlouhému zaučení nových pracovníků



Obrázek 4.1: Organizační struktura společnosti

Testování aplikace není v organizační struktuře znázorněno, jelikož tester, který se zabývá automatizací pracuje vzdáleně z jiné země, než ve kterých obě dvě firmy působí.

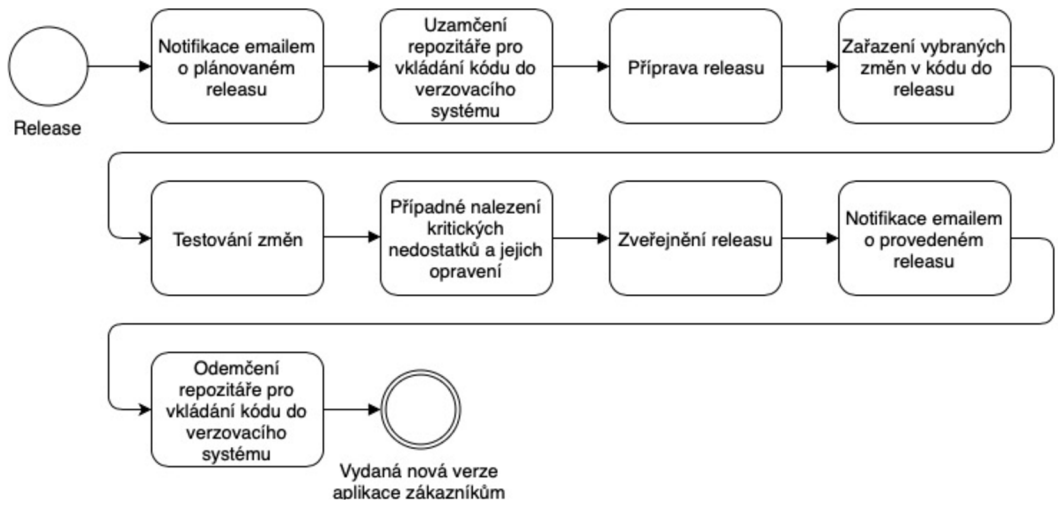
4.2 Firemní procesy

Jelikož se jedná o softwarovou společnost vyvíjející finanční aplikaci určenou pro švýcarský trh, uvedu zde pouze ty procesy, jenž společnosti vytvářejí největší hodnoty v podobě dosažených zisků z prodané licence aplikace.

Cílem kapitoly není zmapovat veškeré procesy, které ve společnosti probíhají, ale vybrat pouze ty stěžejní procesy související s činnosti společnosti zabývající se vývojem softwaru. Následně tyto procesy zohledním v analýze rizik, na která navrhnu vhodná opatření, jež povedou ke snížení rizik.

Na základě pracovní zkušenosti ve společnosti jsem identifikoval následující procesy s navazující posloupností činností.

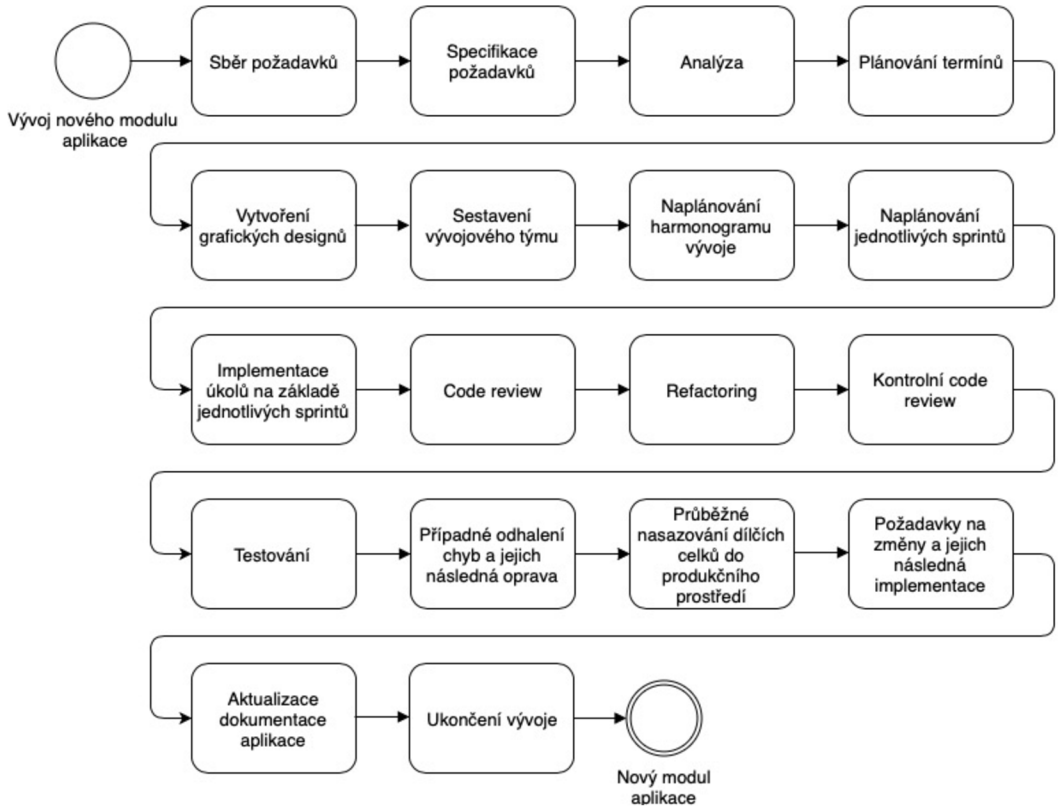
Release[3] aplikace



Obrázek 4.2: Proces release

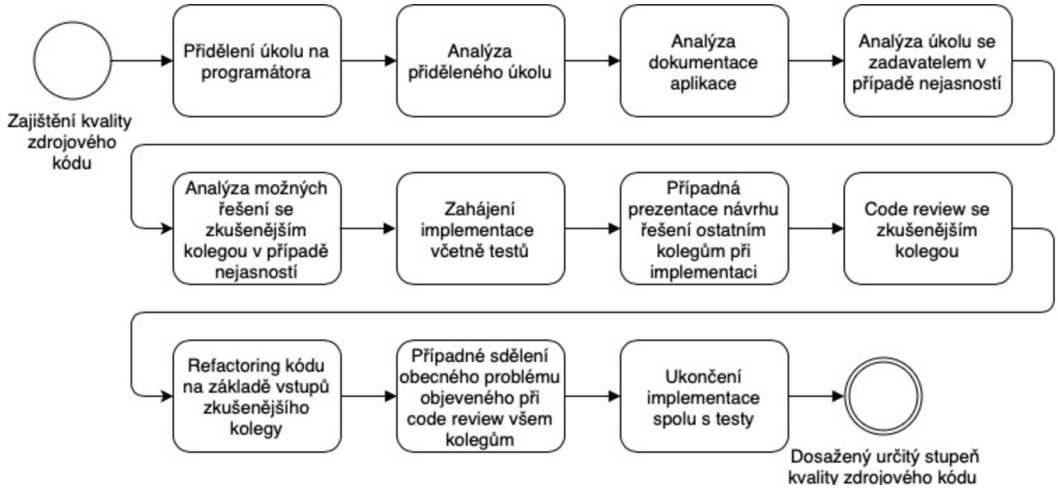
[3]Vydání nové verze aplikace zákazníkům do produkčního prostředí

Vývoj aplikace



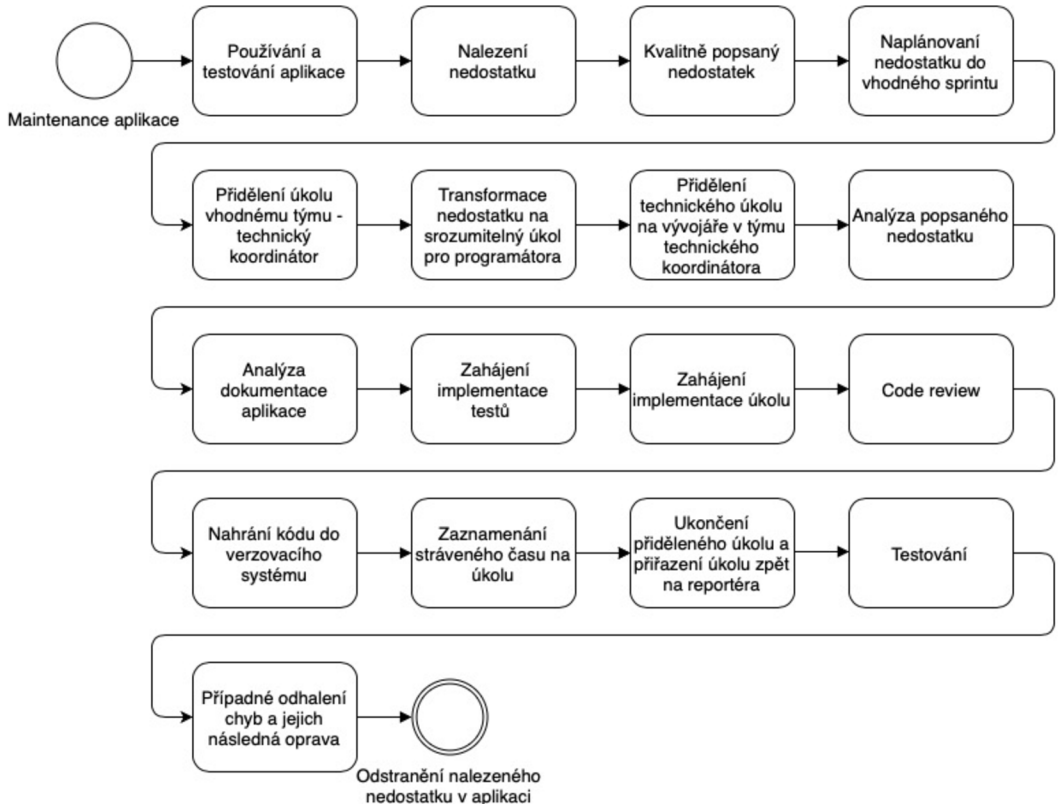
Obrázek 4.3: Proces vývoje

Zajišťování kvality zdrojového kódu



Obrázek 4.4: Proces zajišťování kvality kódu

Maintenance[4] aplikace



Obrázek 4.5: Proces maintenance

4.3 Současný stav bezpečnosti ve společnosti

Jak již bylo řečeno, zaměřím se pouze na dceřinu společnost se sídlem v České republice. Pro mateřskou společnost by bylo vhodné provést analýzu a návrh bezpečnostních opatření zvlášť, jelikož se sídlo společnosti nachází na švýcarské straně. Navíc se mateřská část společnosti soustředí na jiný druh úkolů, než vývojářská jednotka. Z toho plyne, že bude-li v textu použit výraz společnost, bude tím myšlena česká strana společnosti.

4.3.1 Fyzická bezpečnost a bezpečnost prostředí

Sídlo společnosti se nachází mimo hlavní cestu, kterou dělí část pozemku spolu se zelení, díky čemuž je sídlo společnosti odstíněno. Příjezd je tedy možný pouze po vedlejší cestě. Do společnosti se dá dostat dvěma až třemi způsoby. Zadním vchodem, který odděluje elektronicky řízená brána, kterou je možno otevřít pomocí dálkového ovladače. Brána je v průběhu dne většinu svého času otevřená, jelikož tento prostor společnost sdílí také s jinou firmou. Po příjezdu do společného areálu za branou, se lze do společnosti dostat dveřmi které mají nainstalovaný přístupový systém se čtečkou čipu, nebo klasickým způsobem s vuyžitím klíče. Dalším způsobem, jak se do společnosti dostat je možnost využít přední

[4]Neboli přeložený výraz údržba, která znamená opravu chyb či vylepšení výkonu

vchod, který odděluje uzamykatelná brána, jež je potřeba odemknout s využitím klíče pro vstupu. Jelikož je společnost umístěna ve dvou budovách, které jsou vnitřně propojeny, je pro vstup do jedné části budovy potřeba odemknout dveře stejným způsobem, jako u zadního vchodu (u příjezdové brány), tedy pomocí klíče či čipu. Tato část budovy je stejná. Do druhé části budovy se lze dostat primárně pomocí klíče. Při vstupu dovnitř budovy čidlo snímající pohyb spustí alarm, který je potřeba deaktivovat pomocí kódu, jež má každý zaměstnanec svůj vlastní. V případě, že dojde ke spuštění alarmu, vyjíždí na místo bezpečnostní služba. Alarm se opět automaticky zapíná ve večerních hodinách. Budova, ve které si společnost pronajímá kancelářské prostory má dvě patra, z nichž společnost má v jedné budově obsazeno celé přízemní patro a ve druhé části budovy má společnost pronajatou pouze část přízemního patra. Průchod mezi budovami je umožněn přes vnitřní prostory budovy, a dveře jsou opět opatřeny přístupovým systémem se čtečkou čipu. K průchodu je potřeba otevřít celkem dvojí dveře.

4.3.2 Kanceláře

Pro přístup do kanceláře mají zaměstnanci přidělen klíč, kterým lze odemknout i všechny ostatní kanceláře veškerých spolupracovníků, včetně vedení společnosti. Jediným prostorem, jež má jiný klíč, je serverovna. Každá kancelář má na okně připevněny bezpečnostní mříže, z důvodu zabrání přízemních pater budovy. V kanceláři se nacházejí také UPS[5] stanice, které se aktivují v případě výpadku elektrického proudu a jsou schopny udržet stroj v provozu po několik desítek minut. Aby nedošlo k poškození zařízení či zranění osob, je přívod vody nainstalován pouze v kuchyňkách. Některé kanceláře mají možnost nainstalovat klimatizaci, avšak pouze ty, které mají přizpůsobeny bezpečnostní mříže pro možnost jejího umístění z vnější části budovy. Hasící přístroj se nachází v uličce na chodbě mezi kancelářemi.

4.3.3 Serverovna

Serverovna je zabezpečena celkem dvěma kódovými zámky. Jeden z nich je umístěn u zadního vchodu a druhý je umístěn přede dveřmi serverovny. V serverovně se nachází další samostatné pohybové čidlo, které v případě neodkódování spustí alarm. Tak jako všechny ostatní místnosti má i serverovna připevněny bezpečnostní mříže na oknech. Na oknech jsou zároveň připevněny rolety, které chrání místnost před vzniku tepla ze slunečních paprsků. V případě výpadku elektrického proudu je zde několik UPS zařízení, které jsou v poměru 1:2 (UPS - servery). Tato sestava je schopna udržet zařízení v provozu až půl hodiny od vzniklého výpadku elektrické energie. V serverovně má společnost dva racky a vedlejší organizace v podstatě nemá přístup do serverovny. Přístup má pouze společnost a teoreticky i poskytovatel internetu, který provádí správu za druhou organizaci v budově. Jsou zde zabudované dvě klimatizace, které zabraňují vzniku požáru, jež by mohl vzniknout přehřátím některého ze zařízení. Zároveň je v serverovně čidlo zaznamenávající teplotu místnosti, které v případě výpadku klimatizace a následného zvýšení teploty v serverovně začnou hlásit, že je něco špatně. Další čidla teploty obsahují samotné UPS zařízení. Alarm se automaticky zapíná ve večerních hodinách i v případě, že se jej zapomnělo aktivovat.

4.3.4 Pracovní zařízení

Ve společnosti převládá počet stolních počítačů nad přenosnými notebooky, kdy notebook mají zhruba čtyři zaměstnanci, kteří jej využívají při práci z domu či na společném setkání

[5]Zdroj nepřetržitého napájení zařízení

obou společnosti na neutrálním místě. Tato přenosná zařízení by měla být šifrována v případě, že dojde k jejich odcizení. Šifrování pevných disků navrhnu v politice o použití kryptografických opatření.

Pracovní stanice mají nainstalovaný Windows 7. Zaměstnanci je vygenerováno a přiřazeno firemní heslo, které se nesmí měnit z důvodu, aby mohlo vedení společnosti kdykoliv přistoupit na klientský počítač a v případě nepřítomnosti kolegy například odeslat rozpracovaný zdrojový kód do verzovacího systému GIT. Každá pracovní stanice má nainstalovaný licencovaný antivirový program Norton AntiVirus.

4.3.5 Mobilní zařízení

Ve společnosti jsou dvě bezdrátové sítě a obě mají nastaveno heslo. Jedna má veřejné SSID[6] a slouží pro případné návštěvy společnosti, kdy je potřeba mít zajištěn přístup k internetu. Tato síť se nachází mimo interní síť a provádí se na ní testování aplikace z vnější sítě z důvodu, že z interní sítě může vše fungovat správně, ale z vnější to tak vždy být nemusí. Druhá síť má své SSID skryto a jedná se o interní síť, na které je připojené například testovací zařízení iPad (tablet) značky Apple. Toto zařízení slouží například k testování aplikace v případě responzivního designu.

Dále jsou na této interní bezdrátové síti připojení zaměstnanci společnosti se zařízeními jako notebooky, chytré telefony či chytré náramky. Ve společnosti není zaveden žádný mechanismus, který by řídil přístup k síti či filtroval zařízení, jež nabízí třeba standard 802.1X.

4.3.6 Zálohy dat

Každá pracovní stanice má ve společnosti nastavený pravidelný cyklus záloh dat v případě, že dojde k jejich ztrátě či zničení. Liší se pouze zálohovací cyklus, kdy pracovní stanice jsou zálohovány každý týden v pátek při restartu počítače na NAS servery, jež jsou umístěny v prosotech organizace. Denně jsou prováděny zálohy disků pracovních stanic, aby byla kdykoliv v případě výpadku nahraditelná. K zálohování dat je využit program Acronis True Image, který vytváří obrazy záloh konkrétních stanic.

V nepravidelných intervalech zhruba jednou měsíčně vedení společnosti provádí zálohu data na externí disk, jenž je umístěn mimo organizaci.

4.3.7 Řízení aktiv

Seznam aktiv a jejich evidence je řešena v kancelářském balíčku Microsoft Office v aplikaci Excel, kterou má na starost jednatel společnosti. V případě poruchy zařízení je potřeba komunikovat jeho výměnu či opravu s vedením společnosti. Veškerou montáž a instalaci zařízení zařizuje jednatel společnosti svými prostředky.

4.3.8 Bezpečnost lidských zdrojů

V případě kladného výsledku procesu pro přijetí nového zaměstnance se podepíše pracovní smlouva, ve které jsou definovaná obecná ustanovení, jako je například zachování mlčenlivosti, chránění majetku firmy proti odcizení a podobně. Po přijetí je zaměstnanci přiřazeno místo v určité kanceláři se zkušenějším kolegou pro jeho později mířené dotazy týkající se

[6] Service Set Identifier neboli identifikátor bezdrátové sítě

začlenění do pracovního procesu. Zaměstnanci si smí vytvořit přístupový kód k alarmu, který náleží jednomu konkrétnímu zaměstnanci.

V opačném případě, kdy dojde k rozvázání pracovního poměru, je se zaměstnancem sepsána smlouva, která opět zahrnuje například dodržení mlčenlivosti o informacích o zaměstnavateli, jeho provozu, struktuře, mzdách, klientech atp. Zároveň se zaměstnanec zavazuje zdržení jakéhokoliv jednání, které by mohlo poškodit zájmy, dobré jméno či dobrou pověst zaměstnavatele. Poté je potřeba vyřešit předání majetku zaměstnavateli, který představuje navrácení firemního svazku klíčů spolu s přístupovým čipem. Následně jsou data zaměstnance odstraněna zaměstnavatelem z pracovní stanice, na které vykonával zaměstnanec svou práci. Je mu také odebrán přístup z firemního emailu a Skype účtu.

4.3.9 Řízení přístupů

Jak již bylo zmíněno, zaměstnanci mají přístupové čipy a klíče, s kterými se mohou dostat do všech kanceláří, kromě serverovny. Zaměstnanci si nemusejí zaznamenávat příchod a odchod do práce, jelikož mají svou pracovní dobu (přítomnost) veřejně dostupnou v kalendáři, po kterou jsou k dispozici. Dále má zaměstnanec vytvořen přístup do přidělené pracovní stanice v podobě uživatelského jména a hesla, které se nesmí měnit, aby byl zajištěn přístup vedení společnosti do systému pracovní stanice zaměstnance. Každý zaměstnanec má možnost připojit se na interní webové stránky podniku, kde se nachází pracovní kontakty na ostatní zaměstnance, IP adresa a seznam všech přiřazených zařízení zaměstnanců, odkazy ke stažení na projekty, které jsou ve formě zdrojového kódu. Zaměstnanec zde může nalézt také návody na instalaci nového zařízení včetně všech potřebných aplikací pro budoucí vývoj softwaru a také užitečné rady a tipy, se kterými se ostatní zaměstnanci v průběhu vývoje setkali. Aktuálně se tyto interní webové stránky migrují[7] do softwarového online nástroje Confluence [1], který je vyvíjen společností Atlassian [1]. Určité vývojové týmy nemají přístup k jiným informacím jiných vývojových týmů. Příkladem je omezený přístup k dokumentaci integračního projektu, kdy zaměstnanec z jiného týmu potřeboval opravit určitou část a ověřit si platnost provedených změn zdrojového kódu s dokumentací, ke které neměl přístup. Řešením bylo stažení a následovné nahrání dokumentace jiným zaměstnancem na společný sdílený disk. Zaměstnanci mají přístup na společné disky, kde se nachází instalační balíčky k používaným programům ve společnosti, různým dokumentům definující standardní chování aplikace, grafickým designům aj.

Každý zaměstnanec má přístup k aplikaci VNC[8], přes kterou je možné se připojit k jiné pracovní stanici uvnitř firemní sítě včetně jednací místností s projektorem. Připojení je možno buďto pomocí IP adresy nebo přihlašovacího jména zaměstnance, které je zahrnuto v souboru hosts. Tato aplikace je zaměstnanci hojně využívána například při kontrole a zajišťování kvality zdrojového kódu před jeho nahráním do verzovacího systému zejména v případech, kdy se nachází zaměstnanec v druhé části budovy nebo potřebuje pracovat z domu.

Zaměstnanci mají možnost připojit se vzdáleně ze svého zařízení na svou pracovní stanici pomocí VPN[9] a následného použití klienta pro vzdálenou plochu. Toto nastavení musí být schváleno vedením společnosti, zároveň povoleno v antivirovém programu Norton AntiVirus a v nastavení systému pracovní stanice.

[7] Kompletní přesun dat z původního místa na místo nově určené

[8] Virtual Network Computing slouží k vzdálené administraci a správy počítače

[9] Virtuální privátní síť pro bezpečné spojení mezi koncovým zařízením a serverem uvnitř sítě organizace

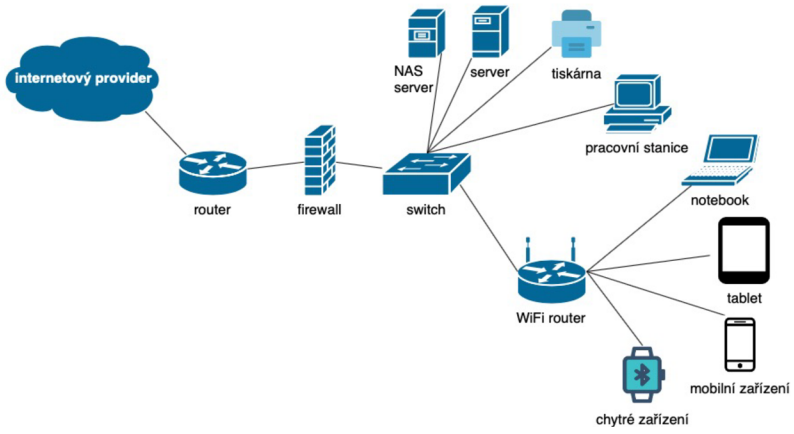
4.3.10 Řízení komunikace

Zaměstnanci společnosti používají v případě emailové korespondence Microsoft Outlook. Tato forma komunikace je vhodná k pořádání meetingů ať už ze strany české či švýcarské. Zároveň je to vhodný způsob pro korespondenci mezi více účastníky, kteří jsou zahrnuti v kopii zprávy a mají možnost reagovat, či koordinovat určitou událost. V Outlooku si zaměstnanci vedou informaci o své pracovní přítomnosti včetně již potvrzených meetingů či dovolených. V případě potřeby rychlejší komunikace se ve společnosti používá další produkt od Microsoftu, a to Skype, který slouží k videohovorům a rychlé odpovědi na případný dotaz, který není nikterak náročný. Osobní komunikace je na české straně nejvíce preferovaná forma, neboť se jedná o vývojovou jednotku a daleko snadněji se vysvětluje problém či jeho možné řešení u tabule, než online. Komunikace je tedy uložena na serverech Microsoftu, který má její zabezpečení ve své režii.

4.3.11 Infrastruktura společnosti

Infrastruktura společnosti lze znázornit pomocí zjednodušené topologie v obrázku 4.6. Do sídla společnosti je přístup internetu zajištěn poskytovatelem internetu do firemního routeru, odkud jde komunikace přes firewall až do vnitřní sítě. Ve vnitřní síti se nachází skrytá bezdrátová síť, servery, tiskárny. Na NAS[10] serveru běží například tyto služby:

- záloha dat
- Nexus Repository[11]
- Jenkins[12]
- GIT[13]



Obrázek 4.6: Zjednodušená topologie společnosti

Pro zajištění bezproblémového provozu služeb serverů jsou připraveny UPS stanice, které v topologii nejsou znázorněny. Organizace využívá především zařízení společnosti HP, od kterých má několik serverů řady HP Proliant. Dále je využit firewall od společnosti Fortinet a router značky MikroTik.

[10] Network Attached Storage neboli chytrá datová úložiště
[11] Spravuje artifakty uložené v repozitáři
[12] Kontinuální integrace a časté spouštění překladu zdrojových kódů projektu pro případné odhalení chyb
[13] Verzovací systém Linuse Torvalda, který byl vytvořen v roce 2005

4.4 Nová vyhláška o kybernetické bezpečnosti

Na konci roku 2018 v září jsem se účastnil konference CyberCon. Událost se konala v prostorách Univerzitního kina Scala v Brně a pořadatel byl NCKB[14]

Ve Sbírce zákonů vešla v platnost nová vyhláška pod označením *Vyhláška č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti).*

Průběh nové vyhlášky měl několik milníků. Jako první bylo potřeba svolat expertní tým, jež absolvoval celkem 11 schůzí, kdy každá trvala kolem 4 hodin. Tyto schůze proběhli v měsících červen až říjen roku 2017. Posléze se spolupráci s vládním CERT[15], byla zpřístupněná nová, avšak stále neoficiální verze vyhlášky pro veřejnost. To proběhlo 6.10. 2017. Koncem října byly zpracovány připomínky k vyhlášce a finalizovala se za RAP. Před Vánocemi proběhlo poslední setkání expertního týmu. Po novém roce 15.1. 2018 proběhlo předání vyhlášky právnímu oddělení NÚKIB[16] a probíhala finalizace za tento úřad. V květnu roku 2018 byla nová vyhláška podepsána ředitelem úřadu a dne 28.5.2018 vstoupila nová vyhláška v platnost.

Nová vyhláška v sobě zahrnuje tyto změny:

- logicky se změnily úpravy některých povinností (přidaní, odstranění, zjednodušení)
- změny povinností (zmenšen rozdíl mezi KII, PSZ, VIS)
- úprava formulací zahrnovala:
  - odstranění duplicit
  - nová formulace vybraných paragrafů, jako např. *Nástroj pro ochranu před škodlivým kódem* byl změněn na *Ochrana před škodlivým kódem*
- změnilo se pořadí některých paragrafů
- důležité je také zapojení požadavků a terminologie v souladu s tzv. *best practice*

Nejvýznamnější změny ve vyhlášce proběhly kupříkladu v organizačním opatření, kde se objevily *§7 bezpečnostní role, §11 řízení změn.* Následné změny týkajících se technických opatření např. *§17 fyzická bezpečnost, §19 správa a ověřování identit*, dále pak zmíněna ochrana před škodlivým kódem jako *§21 Ochrana před škodlivým kódem*, jež je pro společnost relevantní.

4.5 GDPR

Obecné nařízení na ochranu osobních údajů vešlo v platnost v polovině minulého roku, a to 28.5.2018 jednotně v celé Evropské unii. V České republice platí *zákon č. 101/2000 Sb. zákon o ochraně osobních údajů a o změně některých zákonů.* Společnost pro účel své práce využívá anonymizovaná data, které není možno zpětně rozklíčovat a určit tak konkrétní osobu tzn. data o uživateli nejsou s konkrétním uživatelem jinak spojitelná. Ve společnosti se kvůli nařízení GDPR bude muset odstranit veřejně dostupný seznam zaměstnanců s

[14] Národní centrum kybernetické bezpečnosti
[15] Computer Emergency Response Team
[16] Národní úřadu pro kybernetickou a informační bezpečnost

jejich osobními údaji jakými je jméno, datum narození a fotografický záznam. I když to vypadá nevinně a účel zveřejnění tohoto seznamu byl zveřejněn převážně pro informaci o narozeninách ostatních kolegů, je potřeba tento dokument odebrat a vyvarovat se obdobným aktivitám, jenž by mohli vést k opětovnému zveřejnění těchto osobních údajů. V opačném případě je možnost vzniku sankcí vůči společnosti.

4.6 Analýza konkurenčního prostředí

Jelikož se společnost zabývá vývojem finanční aplikace, která je určena pro švýcarský trh, nemá zde v České republice přímého konkurenta jako takového. Proto jsem provedl alespoň základní analýzu několika firem zabývajících se vývojem softwaru. Z webových stránek analyzovaných společností, které jsem vybral z webových portálů nabízejících pracovní pozice v oboru jsem zjistil, že žádná z mnou vybraných firem v aktuální době neposkytuje žádné informace o tom, jak se svými daty nakládá a ani o tom, zdali používá data anonymizovaná či pseudonymizovaná. Co se systému řízení bezpečnosti informací týče, nenašel jsem žádnou informaci o tom, že byl implementovaný. Stejného výsledku jsem se dopátral při analýze, zdali mají vybrané společnosti certifikát z rodiny norem 27000.

4.7 Zhodnocení současného stavu

Na základě analýzy současného stavu lze vypozorovat, že existují určité předpisy a pravidla, která však nejsou v nikterak strukturované podobě a ani nejsou nikde veřejně umístěna. Jedná se tak především o pravidla interní, jež jsou zaměstnanci sděleny při zaučení se do procesů fungování organizace nebo až v průběhu, narazí-li se na nějakou neshodu s vnitřním fungováním společnosti.

Firemní předpisy stanovují například politiku neměnného hesla, které je známo vedení společnosti nebo sekvenci kroků, jež je potřeba udělat v případě neúmyslného spuštění alarmu.

Dále ve společnosti není například nikterak vyřešena politika stahování a používání libovolného softwaru z internetu a jelikož má každý zaměstnanec ke své pracovní stanici nastavena administrátorská práva, není tak toto počínání kromě použití zdravého rozumu ničím omezeno.

Ze získaných poznatků z analýzy současného stavu bude zapotřebí navrhnout předpisy a zavedení pravidel, která budou známá všem pracovníkům společnosti, aby se zamezilo například nevědomému vyzrazení informací či neautorizovaného použití zařízení, které by mohlo nastat z příčiny nezavedené politiky řízení přístupu apod. Bezpečnostní opatření vedoucí k eliminaci neshod s vnitřním fungováním organizace a eliminaci těch nejzávažnějších rizik působících na společnost budou navržena v kapitole 5.

4.8 Očekávání vedení společnosti

Od této diplomové práce společnost očekává analýzu současného stavu bezpečnosti, ze které budou identifikována a ohodnocena aktiva. Dále pak analyzována rizika, na která budou navržena bezpečnostní opatření pro zvládání těch nejzávažnějších rizik, pro která společnost zváží jejich implementaci v závislosti na finanční náročnosti každého z nich. Společnost by také uvítala zvýšení bezpečnostního povědomí a informační bezpečnosti všech zaměstnanců ve společnosti.

Kapitola 5

Vlastní návrhy řešení

V této kapitole bude nejprve vymezen rozsah práce. Poté v kapitole analyzuji rizika působící na společnost. Tato rizika patřičně ohodnotím. Zároveň identifikuji a ohodnotím aktiva společnosti. Z matice zranitelnosti a matice rizik vyhodnotím nejzávažnější rizika, na která navrhnu vhodná bezpečnostní opatření, jež budou vycházet z rodiny norem ISO/IEC 27000 a to z důvodu, že systém řízení bezpečnosti informací z těchto norem vychází. Zavedení vhodných bezpečnostních by mělo vést ke snížení rizik a zvýšení informační bezpečnosti v podniku. Závěrem kapitoly zhodnotím celkové náklady řešení. Prohlášení o aplikovatelnosti ISMS pro navržená opatření je součástí přílohy.

5.1 Vymezení rozsahu práce

Společnost se v současné době nechystá zavádět ISMS neboli systém řízení bezpečnosti bezpečností. Z toho důvodu není cílem této práce uplatnit ISMS v plném rozsahu, ale vybrat pro společnost vhodná bezpečnostní opatření pro zvládání těch největších rizik působících na společnost. Pro implementaci těchto opatření společnost zváží jejich finanční náročnost, kde se porovná cena opatření oproti možným nákladům vzniklých z vědomého podstoupení rizika.

5.2 Analýza rizik

Pro analýzu rizik jsem nejprve identifikoval klíčová aktiva, která mají pro společnost určitou hodnotu a potřebují tak zajistit potřebný stupeň ochrany. K určení těchto aktiv bylo nutné nejprve analyzovat hlavní procesy ve společnosti, ze kterých jsem vycházel. Následně jsem tato aktiva ohodnotil hodnotami, které reprezentují význam aktiv pro společnost. Výsledné ohodnocení aktiv jsem konzultoval s vedením společnosti. Následně jsem ohodnotil hrozby a odhadl zranitelnost pomocí maticové metody se třemi parametry. Z výsledku předchozí metody jsem zhodnotil analýzu rizik a zpracoval akceptaci rizik. Následně jsem navrhl pouze ta bezpečnostní opatření, jenž nejsou ve společnosti zavedena a vedou ke snížení těch nejzávažnějších rizik v podniku.

5.2.1 Identifikace a ohodnocení aktiv

Na základě pracovní zkušenosti ve společnosti jsem v tabulce 5.2 identifikoval aktiva, které jsem dále rozdělil na tyto kategorie:

- data
- hardware
- software
- služby

Tato aktiva jsem ohodnotil na základě stupnice od jedné do pěti v tabulce 5.1. K vypočtení hodnoty aktiva jsem využil součtový algoritmus 5.1, který mi poskytl nejrychlejší způsob pro získání hodnoty aktiva a zároveň odpověděl na otázku, jaký bude pro organizaci dopad v případě zničení či poničení aktiva [9].

$$\text{hodnota aktiva} = \frac{\text{dostupnost} + \text{důvěrnost} + \text{integrita}}{3} \tag{5.1}$$

hodnota aktiva	**dopad rizika**	**míra rizika**
1	žádný dopad na organizaci	bezvýznamné riziko
2	zanedbatelný dopad na organizaci	akceptovatelné riziko
3	potíže či finanční ztráty	nízké riziko
4	vážné potíže či podstatné finanční ztráty	nežádoucí riziko
5	existenční potíže	nepřijatelné riziko

Tabulka 5.1: Hodnocení aktiv

kategorie aktiva	**aktivum**	**zdroj**	**hodnota**
data	data o zaměstnancích	servery	3
	data ze záloh	servery	5
	interní data	servery	3
	zdrojové kódy	servery	5
software	operační systém	pracovní stanice, notebooky, servery	3
	informační systém	servery, cloud	3
	antivirový program	pracovní stanice, notebooky	4
	nástroj pro vývoj softwaru	pracovní stanice, notebooky	4
hardware	pracovní stanice		4
	firewall		3
	server		4
	tiskárna		2
	síťové prvky	kabeláž, switch, router	5
služby	VPN připojení	pracovní stanice, notebooky	3
	internetové připojení	poskytovatel připojení	4
	elektrická energie	dodavatel elektrické energie	5
	interní servis a údržba	interní pracovníci	2
	elektronická komunikace	pracovní stanice, notebooky	2

Tabulka 5.2: Identifikace a ohodnocení aktiv

Z výsledného ohodnocení aktiv je patrné, že nejcennější aktiva jsou pro společnost aktiva spojena s vývojem softwaru. Jedná se o zálohy v případě jakéhokoliv zničení zařízení či při náhlé potřebě obnovy dat. Příkladem takové obnovy může být automatická aktualizace systému Windows, a následné zjištění chyby v aktualizaci, kdy je potřeba vyčkat na její opravu v podobě záplaty. Dalším významným aktivem jsou zdrojové kódy, které jsou uloženy ve verzovacím systému na NAS serveru. Samozřejmostí je dodávka elektrické energie, bez které není možno pro většinu pracovníků v tomto odvětví jakkoliv pracovat.

5.2.2 Identifikace hrozeb

Pro identifikaci hrozeb jsem sestavil tabulku 5.4 s možnou pravděpodobností výskytu hrozeb působících na aktiva společnosti. Pro hodnocení pravděpodobnosti jsem použil škálu v rozmezí jedna až pět. Následné hrozby jsou v tabulce 5.3 s možnou pravděpodobností jejich výskytu působících na aktiva společnosti. Pro hodnocení pravděpodobnosti jsem použil škálu v rozmezí jedna až pět.

kategorie hrozeb	hrozba	pravděpodobnost
přírodní	požár	2
	záplava	1
ztráta služeb	selhání informačního systému	2
	přerušení elektrické energie	3
	přerušení internetového připojení	3
	přerušení elektronické komunikace	2
fyzické poškození	poškození vybavení	3
	znečištění zařízení	1
selhání provozu zařízení	selhání síťových prvků	2
	selhání NAS serveru	3
	selhání pracovních stanic	3
	selhání tiskárny	3
	selhání UPS zařízení	3
selhání lidského faktoru	vyzrazení informací	5
	použití nelegálních kopií aplikací	4
	krádež hardwarového vybavení	2
	zveřejnění zdrojových kódů	4
technická selhání	chybně zapojené zařízení	3
	chybné chování aplikací	2
neoprávněné činnosti	neoprávněné použití zařízení	4
	neoprávněný přístup do místností	3
	neoprávněný přístup do budovy	4
ohrožení informací	odposlech komunikace	4
	podvržení komunikace	2

Tabulka 5.3: Identifikace hrozeb s pravděpodobností možnosti vzniku

hodnota hrozby	míra pravděpodobnosti výskytu
1	nízká
2	malá
3	střední
4	velká
5	trvalá

Tabulka 5.4: Hodnota hrozeb

5.2.3 Identifikace zranitelnosti

Na základě ohodnocených aktiv v tabulce 5.2 a ohodnocených hrozeb v tabulce 5.3 jsem vypracoval matici zranitelnosti, na které lze vidět jak hrozba působí na slabé místo aktiva společnosti. Škála od jedné do pěti je určena podobným způsobem, jako v tabulce 5.1, kde jedna značí nejmenší zranitelnost a pět značí nejvíce zranitelné aktivum vůči hrozbě.

zranitelnost		**aktivum**	data o zaměstnancích	data ze záloh	interní data	zdrojové kódy	operační systém	informační systém	antivirový program	nástroj pro vývoj softwaru	pracovní stanice	tiskárna	server	firewall	síťové prvky	VPN připojení	internetové připojení	elektrická energie	interní servis a údržba	elektronická komunikace
		A	3	5	3	5	3	3	4	4	4	3	4	2	5	3	4	5	2	2
hrozba	**T**																			
požár	2										2	1	5	4	5					
záplava	1										2	1	4	4	4					
selhání informačního systému	2		3		3			3			2					1				3
přerušení elektrické energie	3										5	1	5	3	3			4		
přerušení internetového připojení	3							2	1		3		5		4	4	4			5
přerušení elektronické komunikace	2				3	2					4									5
poškození vybavení	3										2	1	3	3	4				4	
znečištění zařízení	1										1		3	2	3					
selhání síťových prvků	2										2	1	3	3	3	3	5		3	2
selhání NAS serveru	3		2	4	4	5					2		3			1			2	
selhání pracovních stanic	3			f	4	5	2		1	3	5					5			2	3
selhání tiskárny	3				2						1	2								
selhání UPS zařízení	3										3			4	4				2	
vyzrazení informací	5		5		5	5		2												2
použití nelegálních kopií aplikací	4				2	3	3		4	3	5									
krádež hardwarového vybavení	2		4	2	4	4					4	1			3					
zveřejnění zdrojových kódů	4			3	4	5				2										1
chybně zapojené zařízení	3			3	3						4		4	4	4				2	
chybné chování aplikací	2				2	3	3	2	3	4										3
neoprávněné použití zařízení	4		5	3	5	4								3						
neoprávněný přístup do místností	3		5	3	4	3					4	1	4		4					
neoprávněný přístup do budovy	4		2		4									2	4		3			
odposlech komunikace	4		4		3						3		3		3	5				4
podvržená komunikace	2		4		3			2								4				

Tabulka 5.5: Matice zranitelnosti

5.2.4 Identifikace rizik

Z matice zranitelnosti, která spojovala tabulku hodnocení aktiv a tabulku hodnocení hrozeb s maticí zranitelnosti byla vytvořena výsledná matice rizik, ve které jsem vypočetl míru rizika podle následujícího vztahu:

$$R = T \times A \times V$$

kde konstanty mají následující význam:

- R — míra rizika
- T — pravděpodobnost vzniku hrozby
- A — hodnota aktiva
- V — zranitelnost aktiva

hodnota rizika	**dopad rizika**	**míra rizika**
0 až 10	žádný dopad na organizaci	bezvýznamné riziko
11 až 20	zanedbatelný dopad na organizaci	akceptovatelné riziko
21 až 30	potíže či finanční ztráty	nízké riziko
31 až 60	vážné potíže či podstatné finanční ztráty	nežádoucí riziko
61 a více	existenční potíže	nepřijatelné riziko

Tabulka 5.6: Hodnocení rizik

Příklad vypočtení míry rizika

Pro znázornění uvedu jeden výpočet míry rizika z hodnot předchozích tabulek, jehož výsledek je v tabulce 5.7 matic rizik.

- pravděpodobnost vzniku hrozby T — *neoprávněné použití zařízení*
  - hodnota = 4
- hodnota aktiva A — *zdrojové kódy*
  - hodnota = 5
- zranitelnost aktiva V — *přístup na cizí zařízení s přístupem ke zdrojovým kódům, které nejsou zveřejněný ve verzovacím systému pro daného pracovníka*
  - hodnota = 4

$$\textbf{míra rizika} = 4 \times 5 \times 4 = \boxed{\textbf{80}}$$

Výsledkem tohoto ukázkového příkladu je míra rizika, která je nepřijatelná a může mít za následek existenční potíže pro společnost.

riziko		aktivum	data o zaměstnancích	data ze záloh	interní data	zdrojové kódy	operační systém	informační systém	antivirový program	nástroj pro vývoj softwaru	pracovní stanice	tiskárna	server	firewall	síťové prvky	VPN připojení	internetové připojení	elektrická energie	interní servis a údržba	elektronická komunikace
		A	4	5	5	5	3	3	4	5	4	5	5	2	5	3	5	5	2	3
hrozba	T																			
požár	2										16	6	40	16	50					
záplava	1										8	3	16	8	20					
selhání informačního systému	2		18		18			18			16					6				12
přerušení elektrické energie	3										60	9	60	18	45			60		
přerušení internetového připojení	3							18	12		36		60		60	36	48			30
přerušení elektronické komunikace	2				18	20					32									20
poškození vybavení	3										24	9	36	18	60				24	
znečištění zařízení	1										4		12	4	15					
selhání síťových prvků	2										8	6	24	12	30	18	40		12	8
selhání NAS serveru	3		18	75	36	75					24		36			9			12	
selhání pracovních stanic	3				36	75	18		12	36	60					45			12	18
selhání tiskárny	3				18						12	18								
selhání UPS zařízení	3										36			24	60				12	
vyzrazení informací	5		75		75	125		30												20
použití nelegálních kopií aplikací	4				24	60	36		64	48	80									
krádež hardwarového vybavení	2		24	20	24	40					32	6			30					
zveřejnění zdrojových kódů	4			60	48	100				32										8
chybně zapojené zařízení	3			45	27						48		48	24	60				12	
chybné chování aplikací	2				12	30	18	12	24	32										12
neoprávněné použití zařízení	4		60	60	60	80								24						
neoprávněný přístup do místností	3		45	45	36	45					48	9	48		60					
neoprávněný přístup do budovy	4		24		48									32	80		48			
odposlech komunikace	4		48		36						48		48		60	60				32
podvržená komunikace	2		24		18			12								24				

Tabulka 5.7: Matice rizik

5.2.5 Zhodnocení výsledků analýzy rizik

Z tabulky matic rizik 5.7 lze rozpoznat, že nejčastější nepřijatelná rizika v tabulce 5.8 působí na aktivum společnosti v podobě zdrojových kódů. Ke ztrátě může dojít v případě, že dojde k výpadku pracovní stanice z důvodu selhání hard disku, na kterém jsou uloženy rozpracované zdrojové kódy od vývojáře, které ještě nebyly nahrány do verzovacího systému. Další hrozbou pro společnost působící na zdrojové kódy je jejich vyzrazení, kdy v tomto případě dojde ke zveřejnění návrhu struktury aplikace, ze které budou například odhaleny informace o entitách, jejich uložení a způsobech, jak se s nimi v systému pracuje.

Zároveň je ohroženo vlastní know-how, které si společnost vybudovala v průběhu několikaletého vývoje softwaru v různých technologiích. To spočívá v odhalení vlastního řešení a vypořádání se s různými nedostatky, které působí například na UI[1] aplikace ze strany webových prohlížečů v podobě:

- správná pozice umístění prvků na stránce
- správně nastavené vlastnosti viditelnosti prvků na stránce
    - dle priorit jsou prvky rozmístěny buďto do pozadí nebo popředí na stránce

[1] Zkratka pro uživatelské rozhraní. V originále user interface

- přizpůsobení se nedostatkům prohlížeče IE[2]
- správné použití pseudo elementů jako jsou:
    - *::before* a *::after*

Z důvodu uložení těchto dat na serveru týkajících se nejenom zdrojových kódů, je důležité, aby byla serverovna patřičně zabezpečena. Správa serverovny je ve vlastní režii společnosti. Data o zaměstnancích spadají do nepřijatelné kategorie z pohledu vyzrazení informací, které by mohlo společnosti způsobit pokutu až do výše 20 miliónů EUR nebo 4% celkového ročního obratu společnosti, což by mohlo být pro společnost až likvidační [22]. Ve společnosti nemůžou být veřejně dostupné údaje, které GDPR považuje za osobní [22]:

- jméno
- pohlaví
- věk
- datum narození
- osobní stav
- IP adresu
- fotografický záznam

Interní data spadají do této kategorie z pohledu vyzrazení duševního vlastnictví společnosti či zveřejnění dat o mzdách jednotlivých zaměstnanců, jenž by mohlo mít další následky, které by společnost musela řešit.

aktivum	**hrozba**	**míra rizika**
data ze záloh	selhání NAS serveru	75
zdrojové kódy	selhání pracovních stanic	75
	vyzrazení informací	125
	selhání NAS serveru	75
	zveřejnění zdrojových kódů	100
	neoprávněné použití zařízení	80
data o zaměstnancích	vyzrazení informací	75
interní data	vyzrazení informací	75
antivirový program	použití nelegálních kopií aplikací	64
pracovní stanice	použití nelegálních kopií aplikací	80
síťové prvky	neoprávněný přístup do budovy	80

Tabulka 5.8: Nepřijatelná rizika z matice rizik

Co se týče nežádoucích rizik, která jsou vložena do čitelné tabulky 5.8, jenž byla vyhotovena na základě výsledků tabulky matice rizik 5.7 je patrné, že nejvyšší míra rizika se týká hrozeb působících na síťové prvky, pracovní stanice či data ze záloh. Tabulka se po konzultaci s vedením týká pouze hodnot s nejvyšší mírou rizika, jež jsou pro společnost relevantní.

[2]Internet Explorer

aktivum	hrozba	míra rizika
data o zaměstnancích	neoprávněné použití zařízení	60
data ze záloh	zveřejnění zdrojových kódů	60
	neoprávněné použití zařízení	60
interní data	neoprávněné použití zařízení	60
zdrojové kódy	použití nelegálních kopií aplikací	60
pracovní stanice	přerušení elektrické energie	60
	selhání pracovních stanic	60
server	přerušení elektrické energie	60
	přerušení internetového připojení	60
síťové prvky	přerušení internetového připojení	60
	poškození vybavení	60
	selhání UPS zařízení	60
	chybně zapojené zařízení	60
	odposlech komunikace	60
	neoprávněný přístup do místností	60
VPN připojení	odposlech komunikace	60
elektrická energie	přerušení elektrické energie	60

Tabulka 5.9: Nežádoucí rizika z matice rizik

5.2.6 Akceptace rizik

Z výsledné tabulky matic rizik 5.7 jsem s vedením společnosti konzultoval, zdali má smysl zavádět rizika, jejichž míra je:

- bezvýznamné riziko
- akceptovatelné riziko
- nízké riziko

Výsledkem této konzultace bylo, že tato rizika budou akceptována a návrh zavedení bezpečnostních opatření se bude týkat pouze rizik, jejichž míra rizika je nežádoucí či nepřijatelná. Tato rizika jsou pro přehlednost zobrazena v tabulkách 5.8 a 5.9.

kategorie hrozeb	riziko	akceptovat
přírodní	požár	ano
	záplava	ano
ztráta služeb	selhání informačního systému	ano
	přerušení elektrické energie	ne
	přerušení internetového připojení	ne
	přerušení elektronické komunikace	ano
fyzické poškození	poškození vybavení	ne
	znečištění zařízení	ano
selhání provozu zařízení	selhání síťových prvků	ano
	selhání NAS serveru	ne
	selhání pracovních stanic	ne
	selhání tiskárny	ano
	selhání UPS zařízení	ne
selhání lidského faktoru	vyzrazení informací	ne
	použití nelegálních kopií aplikací	ne
	krádež hardwarového vybavení	ano
	zveřejnění zdrojových kódů	ne
technická selhání	chybně zapojené zařízení	ne
	chybné chování aplikací	ano
neoprávněné činnosti	neoprávněné použití zařízení	ne
	neoprávněný přístup do místností	ne
	neoprávněný přístup do budovy	ne
ohrožení informací	odposlech komunikace	ne
	podvržení komunikace	ano

Tabulka 5.10: Akceptace rizik

5.3 Návrh zavedení bezpečnostních opatření

Ze zjištěných výsledků analýzy rizik navrhnu bezpečnostní opatření, která budou vycházet z normy ČSN ISO/IEC 27001:2017 přílohy A a povedou ke snížení vybraných rizik působících vůči společnosti. Normu ČSN ISO/IEC 27002:2017 a její doporučení použiji při aplikaci bezpečnostních opatření. Jelikož se společnost v brzké době nechystá zavádět systém řízení bezpečností informací, nebudu vybírat všechna bezpečnostní opatření, která norma nabízí, ale vyberu pouze ta opatření, která vedou ke zvládání nejzávažnějších rizik. Zároveň vyberu taková opatření, která jsou pro společnost relevantní a která společnost nevytíží z prostředků jak finančních, tak lidských. Je potřeba brát v potaz, že podnik disponuje zhruba 25 zaměstnanci a jedná se tak o malý podnik.

Pro podnik jsem vybral následujících 36 opatření, které jsem pro přehlednost znázornil do tabulky 5.11.

kategorie hrozeb	hrozba	bezpečnostní opatření
ztráta služeb	přerušení elektrické energie	A.11.2.2
	přerušení internetového připojení	A.11.2.2, A.11.2.3
fyzické poškození	poškození vybavení	A.7.2.3, A.8.1.1, A.8.1.2, A.8.2.3, A.11.1.4, A.11.2.4, A.11.2.1
selhání provozu zařízení	selhání NAS serveru	A.8.2.3, A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.4, A.12.3.1
	selhání pracovních stanic	A.8.2.3, A.11.1.4, A.11.2.2, A.11.2.4, A.12.3.1
	selhání UPS zařízení	A.11.1.4, A.11.2.1, A.11.2.4
selhání lidského faktoru	vyzrazení informací	A.7.2.3, A.9.2.1, A.9.2.5, A.9.2.6, A.9.3.1, A.9.4.1, A.9.4.2, A.9.4.5, A.10.1.1, A.11.2.6, A.11.2.9, A.12.2.1,
	použití nelegálních kopií aplikací	A.7.2.2, A.9.1.1, A.9.1.2, A.9.2.5, A.12.2.1, A.12.6.2
	zveřejnění zdrojových kódů	A.6.2.1, A.6.2.2, A.7.2.3, A.7.3.1, A.9.2.1, A.11.2.6
technická selhání	chybně zapojené zařízení	A.7.2.2, A.8.1.3, A.11.1.2, A.11.2.1
neoprávněné činnosti	neoprávněné použití zařízení	A.7.2.2, A.7.2.3, A.8.2.3, A.9.2.3, A.9.2.5, A.9.3.1, A.9.4.1, A.9.4.2,A.9.4.5, A.11.2.1, A.11.2.8, A.12.4.1
	neoprávněný přístup do místností	A.7.2.3, A.11.1.1, A.11.1.2
	neoprávněný přístup do budovy	A.11.1.2, A.11.1.1
ohrožení informací	odposlech komunikace	A.7.1.2, A.9.1.2, A.9.2.1, A.9.3.1, A.10.1.1, A.13.2.1

Tabulka 5.11: Bezpečnostní opatření pro zvládání těch nejzávažnějších rizik

5.3.1 A.6 organizace bezpečnosti informací

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

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 zařízeni

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

Implementace: Jelikož je používání mobilních zařízení ve společnosti běžné, měla být věnovaná zvláštní pozornost tomu, aby nebyly kompromitovány informace, které se týkají činnosti organizace. V této politice by se mělo brát také v úvahu riziko práce s mobilními zařízeními v nechráněných prostředích.

Tato politika by měla brát v úvahu například:

a) registraci mobilních zařízení

b) požadavky na fyzickou ochranu

c) omezení instalace softwaru

d) požadavky na verze softwaru mobilních zařízení

e) omezení připojení k informačním službám

f) řízení přístupu

g) ochranu před malwerem

h) zálohy

Mobilní zařízení by měla být zároveň chráněna zaměstnanci před jejich možným odcizením, a nenechávat tak zařízení volně bez dozoru na místech jako, je automobil či jiných dopravních prostředcích. Dále se nedoporučuje mobilní zařízení nechávat na místech, jakými jsou hotelové pokoje, konferenční místa či centra, kde probíhají různá jednání.

Složení mobilních zařízení je ve společnosti převážně dvojího typu, a to s operačním systémem Android a iOS, jenž je systém od společnosti Apple. Zařízení od společnosti Apple jsou již samy o sobě zabezpečeny na dobré úrovni, která nabízí například:

- vzdálené vymazání obsahu zařízení
- možnost přehrát zvuk pro případ ztraceného zařízení
- možnost nastavení tvz. režimu *ztraceno*, ve kterém je možno zobrazení zprávy na displeji pro případ, že někdo telefon najde
    - zpráva může obsahovat například náhradní telefonní číslo, na které má nálezce zavolat
- možnost zobrazení GPS[3] polohy zařízení
- šifrovaná komunikace

Pro zvýšení dosavadní bezpečnosti mobilních zařízení ve společnosti doporučuji nasadit Norton Mobile Security, který je pro oba výše zmíněné mobilní operační systémy kompatibilní a zároveň má společnost s produkty Norton dobrou zkušenost.

Aplikace Norton Mobile Security nabízí funkce jako [16]:

- blokování malwaru[4]
- webovou ochranu proti phishingu[5]
- ochrana před ransomwarem[6]
- blokování hovorů a textových zpráv
- bezpečné procházení internetu
- ochrana proti krádeži (možnost vzdáleného zamknutí odcizeného zařízení)
- zabezpečení Wi-Fi sítí
- jednotné přihlášení k odběru pro různá zařízení

V této politice nejsou řešeny kroky v případě, že dojde ke ztrátě či odcizení zařízení, jenž by mohla rozšiřovat povědomí o postupech v čase, kdy taková situace nastane. V tomto případě doporučuji použití základních bezpečnostních prvků, kterým je například kódový

[3] Global Positioning System

[4] Škodlivý software, který infikuje počítač / mobilní zařízení pro účel získávání dat, jako osobní údaje, hesla, aj.

[5] Snaha podvodníků získat citlivé údaje, jako jsou hesla, údaje o platebních kartách či čísla bankovních účtů. Nejčastěji je šířen přes emailové zprávy nebo odkazem, který uživatele přesměruje na falešné stránky, které jsou svým vzhledem k nerozeznání od originálu

[6] Tento typ škodlivého softwaru omezuje uživatelům přístup k souborům uloženým na pevném disku. Pro jejich odemčení vyžaduje software zaplacení finanční částky ve prospěch účtu podvodníka

zámek obrazovky zařízení a poté také vyžadování zámku v případě otevření vybraných aplikací, jenž potřebují zvýšenou bezpečnost. Zároveň je doporučeno mít nastavené automatické uzamčení zařízení v určitém intervalu a po jeho uplynutí je kódový zámek pro odemčení zařízení opětovně vyžadován.

Náklady: 20x licence za 2 798 Kč, díky zvýhodněné ceny při odběru deseti licencí za cenu 1 399 Kč v době psaní této diplomové práce.

Čas potřebný k vypracování: 7 hodin

A.6.2.2 Práce na dálku

Opatření: Na ochranu informací, k nimž je přistupováno v rámci práce na dálku, zpracovávaných nebo ukládaných v místech práce na dálku by měla být zavedena politika a podpůrná bezpečnostní opatření.

Implementace: V Organizaci je umožněna práce na dálku, a proto by se měla vydat politika, která definuje podmínky a omezení pro používání práce na dálku. Jeli to aplikovatelné a zákonem povolené, měly by být brány v úvahu následující záležitosti:

a) stávající fyzická bezpečnost práce na dálku jako je bezpečnost budovy a místního prostředí

b) požadavky k zabezpečení komunikace s přihlédnutím k citlivosti informací, ke kterým bude přistupováno a které budou přenášeny

c) poskytování přístupu z virtuální pracovní plochy, který brání zpracování a uchovávání informací na zařízení v soukromém vlastnictví

d) hrozba neautorizovaného přístupu k informacím nebo zdrojům jinými osobami, například rodina a přátele

e) ochrana před malwarem a požadavky na firewall[7]

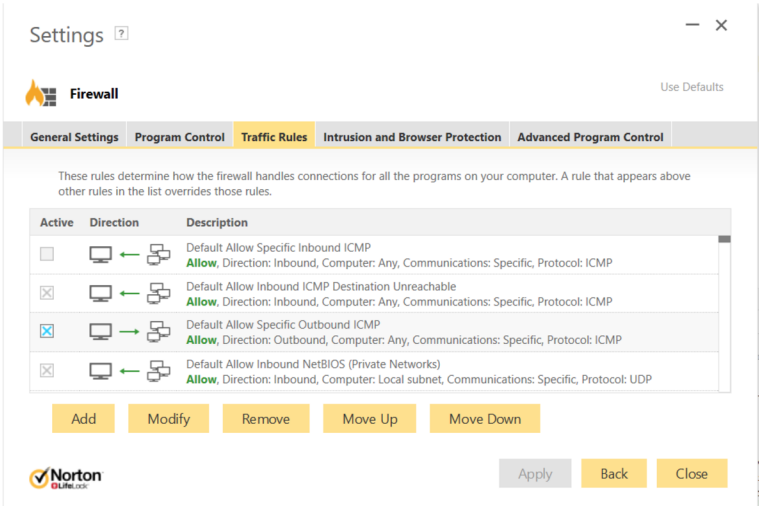
f) využití domácí sítě a požadavky nebo omezení týkající se konfigurace bezdrátových síťových služeb

Prací na dálku se myslí využití prostorů pro práci mimo kancelář a prostory organizace:

- práce z domova
- flexibilní pracoviště
- vzdálená práce
- virtuální práce

Ve společnosti se práce na dálku hojně využívá a v případě nemoci či potřeby práce z domova je pro práci nezbytná. Pro spojení je využito připojení VPN. Pro tento typ práce doporučuji použití výhradně zařízení od společnosti, tedy firemní, které jsou zaměstnanci přiřazeny k práci až po příslušném nastavení zařízení pracovníkem společnosti. Jedná se například o povolení vzdáleného přístupu k privátním sítím v antivirovém programu Norton, jenž zachyceno na obrázku 5.3.1

[7]Hardwarová nebo softwarová technologie, jejímž úkolem je zabránit neoprávněnému přístupu na síťové zdroje



Obrázek 5.1: Nastavení pravidel provozu v Nortonu pro zpřístupnění vzdálené plochy

V tomto nastavení je možno spravovat daleko více protokolů, než zmíněný RDP[8]. Zároveň doporučuji společnosti zabezpečit svá data pomocí šifrování pevných disků, jenž umožňuje nástroj BitLocker, který je zdarma součástí Windows, na kterých běží pracovní stanice ve společnosti. V případě odcizení zařízení, s nimž pracuje zaměstnanec na dálku, bude znemožněn přístup k obsahu pevného disku a data tak budou chráněna. Použití BitLockeru bude implementováno v opatření týkající se kryptografie (v 5.3.5).

Náklady: Nejsou zapotřebí žádné náklady, jelikož je Norton již předplacen a BitLocker je zdarma součástí Windows.

Čas potřebný k vypracování: 6 hodiny.

5.3.2 A.7 bezpečnost lidských zdrojů

Cíl: Zajistit, aby zaměstnanci a smluvní strany znali a chápali svoje povinnosti a zajistit, aby byli schopni jejich plnění.

A.7.1.2 podmínky pracovního poměru

Opatření: Smlouvy se zaměstnanci a smluvními stranami by měly uvádět odpovědnosti zaměstnanců či smluvních stran a také organizace za bezpečnost informací.

Implementace: Smluvní povinnosti zaměstnanců či smluvních stran by měly dodržovat politiky organizace pro bezpečnost informací. Dále je potřeba vyjasnit stanovení, které se týká:

a) zaměstnanci či smluvní strany, které mají přístup k důvěrným informacím by měli podepsat dohodu o zachování důvěrnosti či mlčenlivosti ještě před tím, než je udělen přístup k vybavení pro zpracování informací

b) právní odpovědnosti a práv zaměstnance týkající se autorských práv a legislativy na ochranu dat.

c) povinnosti zaměstnance nebo smluvní strany ve vztahu k zacházení s informacemi získanými od jiných společností nebo externích subjektů.

[8]Remote Desktop Protocol

Ještě před vznikem pracovního poměru společnosti doporučuji, aby bylo nově příchozímu zaměstnanci nebo smluvní straně předloženo prohlášení o mlčenlivosti, které bude vyhotoveno vedoucími pracovníky. Zároveň by měla společnost zajistit, aby zaměstnanci či smluvní strany souhlasili s pravidly a podmínkami v oblasti bezpečnosti informací, která odpovídá povaze a rozsahu přístupu, který budou mít k aktivům organizace. V případě, že budou tyto povinnosti porušeny bude následovat buď disciplinární řízení či ukončení pracovního poměru podle rozsahu způsobených škod.

Čas potřebný k vypracování: 4 hodiny.

A.7.2.2 povědomí, vzdělávání a školení o bezpečnosti informací

Opatření: Všichni zaměstnanci organizace a všude, kde je to vhodné tzn. i smluvní strany by měli mít určitou úroveň povědomí o bezpečnosti informací v podobě vzdělávání a školení a aktualizací politik organizace podle významu role, kterou zaměstnanec vykonává.

Implementace: Pro to, aby získali jak zaměstnanci, tak i smluvní strany povědomí o bezpečnosti informací doporučuji ve společnosti zavést školení, které se bude opakovat v pravidelných intervalech. Nemá smysl provést takzvané jednorázové nalití informací do účastníků školení, ale mnohem důležitější je postupné prohlubování nových a stávajících poznatků ohledně bezpečnosti informací. Jelikož se organizační struktura společnosti převážně z vývojářů, nebude zapotřebí školení rozdělovat na skupiny zaměstnanců. Základní školení budou mít v režii pracovníci na vedoucích pozicích, kteří mají své letité zkušenosti z praxe. Doporučeným postupem je, aby byl nově přijatý zaměstnanec seznámen s informacemi, které se probrali na minulých školeních, které povedou již stávající zaměstnanci, kteří se touto metodou předávání informací budou zároveň učit a etablovat získané poznatky z minulých školení. Tímto předáváním znalostí se bezpečnostní povědomí upevní v daleko větší míře, jelikož budou stávající zaměstnanci sami vysvětlovat problematiku zaměstnancům nově příchozím.

Vzdělávání a školení v oblasti bezpečnosti informací by mělo brát také v potaz i obecné aspekty jako:

a) základní postupy v oblasti bezpečnosti informací
   - prázdné pracovní stoly
   - bezpečnost hesel
   - kontrola malwaru
   - prázdná pracovní plocha

b) osobní odpovědnost za své vlastní jednání a nečinnost

c) potřeba seznámení se a dodržování platných pravidel a povinností v oblasti bezpečnosti informací, jak jsou definovány v politikách, normách, zákonech, předpisech, smlouvách a dohodách

Jakmile se ve společnosti ustálí základní pojmy a teoretická východiska bezpečnosti informací, doporučuji, aby společnost zvážila další, hlubší prohlubování znalostí a pokračovala tak v neustálém zvyšování informační bezpečnosti a povědomí.

Společnost ESET doporučuji, jenž má své etablované renomé, a nabízí řešení v podobě konzultací, které je zdarma pro firmy. Z této konzultace je možnost sjednání ceny podle toho, jaké oblasti společnost využije. Úkolem školení je předat zkušenosti odborníků a

připravit tak na míru šité školení v oblasti informační bezpečnosti. Cílem školení je vzdělávat a seznamovat zaměstnance s vnitřními předpisy, jak nakládat s informacemi, praxe při používání IT zařízení (počítače, tiskárny, telefony, aj.) nebo seznámení s bezpečnostními riziky [4].

Předmětem školení společnosti ESET jsou na výběr tyto oblasti [4]:

- vnitřní předpisy
- fyzická bezpečnost
- ochrana IT prostředků
- používání hesel
- bezdrátové sítě
- přenosná média
- internetové služby
- škodlivý kód a jeho šíření
- zvládání bezpečnostních incidentů
- nakládání s citlivými informacemi
- autorská práva IT
- ochrana osobních údajů

Náklady: orientačně 10 000 Kč dle typu a délky školení
Čas potřebný k vypracování: 6 hodin.
Čas potřebný pro pravidelné školení 12 hodin/ročně

A.7.2.3 disciplinární řízení

Opatření: Měl by existovat formální disciplinární proces, oznámený všem, pro podniknutí kroků vůči zaměstnancům, kteří se dopustili narušení bezpečnosti informací.

Implementace: Tento proces disciplinárního řízení by měl společnosti zajistit spravedlivé a správně zacházení pro zaměstnance, kteří jsou podezřelí z narušení bezpečnosti informací. Tento formální disciplinární proces by měl stanovit odstupňované reakce, které berou v úvahu například:

- první přestupek
- opakovaný přestupek
- příslušnou legislativu
- obchodní smlouvy
- zdali byl zaměstnanec v minulosti proškolen

V závažných situacích je také na zvážení rozvázaní pracovního poměru nebo určit finanční sankce dle dopadu vzniklých škod. Z důvodu malého kolektivu je však preferovanou volbou ústní domluva. Je důležité, aby disciplinární proces nezačal bez předchozího ověření, že opravdu došlo k narušení bezpečnosti informací. Zároveň je potřeba, aby byl disciplinární proces použit jako odstrašující prostředek odrazující zaměstnance k tomu, aby porušili politiky a postupy organizace v oblasti bezpečnosti informací.

Čas potřebný k vypracování: 12 hodin.

A.7.3 ukončení a změna pracovního poměru

Cíl: Chránit zájmy organizace jako součást procesu změny nebo ukončení pracovního poměru.

A.7.3.1 odpovědnosti při ukončení nebo změně pracovního poměru

Opatření: Odpovědnost a povinnosti v oblasti bezpečnosti informací, které zůstávají v platnosti i po ukončení nebo změně zaměstnání, by měly být definovány, sděleny zaměstnanci nebo smluvní straně a prosazovány.

Implementace: Sdělení zaměstnanci jeho odpovědností při ukončení zaměstnaná, které by měly zahrnovat pokračující požadavky na bezpečnosti informací a právní odpovědnosti a tam, kde je to vhodné, povinnosti obsažené v jakékoli smlouvě o mlčenlivosti a v podmínkách pracovního poměru (viz 7.1.2 v 5.3.2), trvající po definované období po skončení pracovního poměru nebo smlouvy se smluvní stranou.

Změny odpovědnosti nebo pracovního poměru by měly být řešeny jako ukončení současné odpovědnosti nebo pracovního poměru v kombinaci se započetím nové odpovědnosti nebo pracovního poměru.

Zaměstnanec musí odevzdat zpět veškeré firemní vybavení, jenž v průběhu pracovního poměru používal k výkonu své práce.

Zároveň je potřeba zaměstnanci odebrat veškeré možné přístupy, jako je deaktivování firemní emailové adresy, odebrání přístupu na bezdrátové sítě, přístupové čipy a klíče společnosti apod.

Čas potřebný k vypracování: 5 hodiny.

5.3.3 A.8 řízení aktiv

Cíl: Identifikovat aktiva organizace a definovat odpovědnosti za přiměřenou ochranu.

A.8.1.1 seznam aktiv

Opatření: Aktiva související s informacemi a vybavením pro zpracování informací by měla být identifikována a měl by být sestaven a udržován seznam těchto aktiv.

Implementace: Ve společnosti by se měla identifikovat relevantní aktiva v životním cyklu informací a měl by se dokumentovat jejich význam. Seznam by měl být aktuální a pro dodržení aktuálnosti je potřeba ho mít pod dohledem. Seznam aktiv bude mít na starost jednatel společnosti, který spravuje evidenci. Každému z identifikovaných aktiv by měl být přiřazen vlastník aktiva (viz 8.2.1 v 5.3.3) a měla by být identifikována jeho klasifikace (viz 8.2 v 5.3.3)

Čas potřebný k vypracování: 6 hodin.

Čas potřebný k aktualizaci seznamu aktiv: 4 hodiny/ročně

A.8.1.2 vlastníci aktiv

Opatření: Aktiva udržovaná v seznamu by měla mít vlastníka.

Implementace: Všechna identifikovatelná aktiva společnosti musejí mít přiřazeného svého vlastníka, nebo i jinou entitu, která byla schválena jako odpovědná za správu a řízení aktiva po dobu jeho životnosti.

Vlastníci aktiv mají zajistit:

a) aktiva jsou inventarizována

b) aktiva jsou náležitě klasifikována a chráněna

c) pravidelné přezkoumávání omezení přístupu k důležitým aktivům a jejich klasifikaci

d) správné zacházení, když je aktivum vymazáno nebo zničeno

Rutinní úkoly mohou být svěřeny například jiným zaměstnancům, kteří by se o aktiva starali, avšak odpovědnost zůstává pořád na vlastníkovi aktiv.

Čas potřebný k vypracování: 4 hodin.

A.8.1.3 přípustné použití aktiv

Opatření: Měla by být identifikována, dokumentována a implementována pravidla pro přípustné používání informací a aktiv spojených s informacemi a vybavením pro zpracování informací.

Implementace: Všichni, kdo používají aktiva nebo k nim mají přístup, tzn. zaměstnanci a uživatelé z externích stran organizace by měli být uvědoměni o požadavcích bezpečnosti informací na aktiva organizace spojené s informacemi a vybavením pro zpracování informací a zdroji. Měli by být odpovědní za použití jakýchkoliv zdrojů pro zpracování informací a jakéhokoliv podobného použití provedeného v rámci své odpovědnosti.

Čas potřebný k vypracování: 6 hodin.

A.8.2 klasifikace informací

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

A.8.2.3 manipulace s aktivy

Opatření: Pro zacházení s aktivy by měly být vyvinuty a zavedeny postupy, v souladu se schématem klasifikace informací přijatým organizací.

Implementace: Ve společnosti je potřeba vypracovat postupy pro zacházení, zpracování, ukládání a předávání informací v souladu s jejich klasifikací. Tyto postupy by měly brát v úvahu následující položky:

a) omezení přístupu podporující požadavky na ochranu na každé úrovni klasifikace

b) udržování formálního záznamu o oprávněných příjemcích aktiv

c) ochrana dočasných nebo trvalých kopií informace na úrovni odpovídající ochraně původní informace

d) skladování IT aktiv v souladu se specifikacemi výrobce

e) zřetelné označení všech kopií médií pro upoutání pozornosti oprávněného příjemce

Čas potřebný k vypracování: 12 hodin.

5.3.4 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.

Implementace: Vlastníci aktiv by měli stanovit vhodná pravidla řízení přístupu, přístupová práva a omezení pro specifické uživatelské role ve vztahu k jejich aktivům, s přesností a přísností opatření odrážející související rizika v oblasti bezpečnosti informací.

Tato opatření řízení přístupu jsou jak logická, tak fyzická (v 5.3.6) a měla by být zvažována společně.

Ve společnosti nejsou uceleně navržena pravidla řízení přístupu a ani přístupová práva. Ve společnosti neexistuje žádná politika klíčů a každý zaměstnanec je schopen se svým klíčem vstoupit do všech místností ve společnosti kromě serverovny. Běžný zaměstnanec má tak možnost přístupu do kanceláře vedení společnosti. V těchto kancelářích nejsou informační aktiva nikterak chráněna. Jedná se o informační aktiva v podobě citlivých údajů o zaměstnancích, pracovních smluv, vystavených faktur apod. Pro ochranu těchto aktiv jsem navrhl opatření, které je v 5.3.6. Přístup ke všem informacím napříč organizací je k dispozici na sdíleném disku. Dále jsou všechny zdrojové kódy přístupné ke stažení všech projektů společnosti v informačním systému.

Přístup by tak měl být řízen na základě rolí, kde programátor by neměl mít přístup k projektovým věcem a zase naopak by neměl mít projektový manager přístup ke zdrojovým kódům, jelikož pro jeho práci nejsou potřeba.

Vytvoření politiky by mělo brát v úvahu:

a) soulad mezi přístupovými právy a politikami klasifikace informací systémů a sítí

b) relevantní legislativu a jakékoliv smluvní závazky týkající se omezení přístupu k datům či službám

c) požadavky na pravidelné přezkoumání přístupových práv

d) role s privilegovaným přístupem

e) požadavky na autorizaci žádostí o přístup

f) řízení a správu přístupových práv v distribuovaném a síťovém prostředí, rozpoznávající všechny typy připojení, která jsou k dispozici

g) bezpečnostní požadavky jednotlivých aplikací organizace

Čas potřebný k vypracování: 20 hodin.

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.

Implementace: Tato politika by ve společnosti měla zohledňovat pravidla přístupu do sítě a k síťovým prvkům. Neměly by být volně přístupné kabely internetového připojení a pro bezdrátové sítě by bylo vhodné mít nastaven server RADIUS, který by podporoval autentizaci uživatele na základě uživatelského jména a hesla pro přístup do domény. Stejné nastavení pro přístup do systému je již nastavena na pracovních stanicích. Navržené řešení usnadní daleko přehlednější správu uživatelů na bezdrátové síti. Stolní pracovní stanice mají staticky nastavenou IP adresu a jejich správa je tak daleko jednodušší.

Čas potřebný k vypracování: 10 hodin.

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.

Implementace: Proces registrace uživatelů do domény je ve společnosti již zaveden a při přijetí nového zaměstnance je vytvořen nový doménový účet. Navíc je vnitřním pravidlem neměnit své přihlašovací údaje k pracovní stanici, což znamená, že má vedení společnosti možnost přihlášení se na pracovní stanici kteréhokoliv zaměstnance. Zároveň společnost pro přihlášení používá formát zkratky prvních dvou písmen ze jména a příjmení.

- příkladem užívaných zkratek demonstruji na jméně *Jan Novák*
    - přihlašovací údaj ze jméno je *JANO*

S narůstajícím počtem nových zaměstnanců bude brzy potřeba vymyslet další způsob vytváření uživatelských účtů.

Proces správy a řízení ID uživatele by měl dále zahrnovat:

a) okamžité zablokování nebo zrušení ID uživatelů, kteří opustili organizaci (9.2.6 v 5.3.4)

b) pravidelné identifikování a zrušení nebo zablokování duplicitních uživatelských ID

c) zajištění, aby duplicitní uživatelská ID nebyla přidělena jiným uživatelům

d) poskytnutí nebo zrušení přístupových práv k danému ID uživatele

e) použití jedinečného ID uživatele, umožňující propojit uživatele s jejich aktivitami a udržovat jejich odpovědnost za tyto aktivity

Čas potřebný k vypracování: 8 hodin.

A.9.2.3 řízení privilegovaných přístupových práv

Opatření: Přidělení a použití privilegovaných přístupových práv by mělo být omezeno a řízeno.

Implementace: Přidělování privilegovaných přístupových práv by mělo být ve společnosti řízeno prostřednictvím formálního procesu autorizace, který by měl brát v úvahu následující kroky:

a) měly by být definovány požadavky na expiraci privilegovaných přístupových práv

b) měly by být stanoveny a udržovány speciální postupy, jejímž cílem je zabránit neoprávněnému použití obecných administrátorských přihlašovacích údajů uživatele, s kterými lze systém konfigurovat

c) měla by být identifikována privilegovaná přístupová práva související s každým systémem nebo procesem

   - operační systém
   - databázový systém

d) privilegovaná přístupová práva by měla být přiřazena ID uživatele odlišného od ID používaných pro běžné činnosti v organizaci

e) pravidelné činnosti organizace by neměly být prováděny s použitím privilegovaného ID

Čas potřebný k vypracování: 4 hodin.

A.9.2.5 přezkoumání přístupových práv uživatelů

Opatření: Vlastníci aktiv by měli v pravidelných intervalech přezkoumávat přístupová práva uživatelů.

Implementace: Pro přezkoumávání přístupových práv uživatelů by se mělo ve společnosti myslet na to, zdali u uživatelů nedošlo k určité změně. Změna může být nová funkce či povýšení. Změny týkající se privilegovaných účtů by měly být zaznamenány ve formě logů, které je vhodné pravidelně přezkoumávat.

Čas potřebný k vypracování: 2 hodiny.

Čas potřebný pro ověření 3 hodiny/ročně

A.9.2.6 odebírání nebo úprava přístupových práv

Opatření: Přístupová práva všech zaměstnanců a uživatelů z externích stran k informacím a vybavení pro zpracování informací by měla být po ukončení jejich zaměstnaná, smlouvy nebo vypršení dohody odstraněna nebo ihned po změně upravena.

Implementace: V případě, že dojde k rozvázání pracovního poměru jakýmkoliv způsobem, je zapotřebí přístupová práva jednotlivce zablokovat, protože mohou souviset s informacemi, aktivy, souvisejícím vybavením nebo službami, které souvisejí se zpracováním informací. Poté se určí, zda je potřebné přístupová práva zrušit. Změny v pracovním poměru by se měly promítnout v odstranění veškerých přístupových právech, jenž nebyly schváleny pro nový pracovní poměr. Přístupová práva daného uživatele by se měla zrušit také fyzicky, což znamená odstraněním, revokací či výměnou klíčů, identifikačních karet, předplatného nebo vybavením, které slouží ke zpracování informací.

Zároveň je potřeba myslet na to, zdali zaměstnanec, který odchází zná hesla ostatních uživatelů, kteří ve společnosti zůstávají aktivní. V kladném případě je zapotřebí okamžitá změna hesla ihned po změně zaměstnání, dohody či smlouvy. Je potřeba si uvědomit, že přístupová práva k informacím a aktivům, která souvisejí s vybavením pro zpracování informací by měla být omezena, zablokována nebo případně odstraněna ještě před změnou nebo zánikem pracovního poměru. Při této změně je potřeba mít na paměti například tyto rizikové faktory:

a) stávající povinnosti uživatele, zaměstnance či externí strany

b) je změna či ukončení pracovního poměru iniciována zaměstnancem, uživatelem z externí strany nebo vedením společnosti, který měl důvod k ukončení pracovního poměru

c) hodnotu přístupných aktiv

Čas potřebný k vypracování: 4 hodiny.

A.9.3 odpovědnosti uživatelů

Cíl: Učinit uživatele odpovědné za ochranu svých autentizačních informací.

A.9.3.1 použití tajných autentizačních informací

Opatření: Po uživatelích by mělo být vyžadováno, aby při používání tajných autentizačních informací dodržovali postupy organizace.

Implementace: Při používání tajných autentizačních informací je velmi důležité držet se těchto několika kroků, o kterých by měly být zaměstnanci společnosti poučeni:

a) své tajné autentizační údaje je potřeba udržet jako důvěrnou a zajistit, aby nebyla vyzrazena.

   - nepoužívat hesla, jenž jsou spojitelná s konkrétní osobou jako:
     - datum narození
     - přezdívka
     - adresa trvalého bydliště
     - jména rodilých příslušníků
   - v blízkosti pracovní stanice nejsou nikde autentizační údaje napsána na papíře, který by mohl být schován například pod klávesnicí

b) v případě podezření či náznaku možné kompromitace je potřeba okamžitá změna autentizačních údajů

   - může se projevit v případech, kdy poslední čas přihlášení do systému neodpovídá reálnému času přihlášení uživatele
     - například měl zaměstnanec minulý týden dovolenou, avšak systém obsahuje zmínku o jeho přihlášení v minulém týdnu

c) v případě důležitých a složitých hesel je doporučeno použití dalšího zařízení např. trezoru s heslem a zámkem

d) nutnost zvolit kvalitní hesla, která:

- mají minimální délku 8 znaků
- jsou snadno zapamatovatelná
- nejsou zranitelná vůči slovníkovým útokům
- není snadné je uhádnout a nejsou spojitelná s konkrétní osobou

e) nesdílet své či cizí autentizační údaje uživatelů

f) nepoužívat stejnou tajnou autentizační informaci ve firemním prostředí a v osobním prostředí

g) nastavení zablokování přístupu do systému po několika neúspěšných pokusech přihlášení a nutnost obnovení zaměstnancem, jenž spravuje obnovení účtů

Je důležité si uvědomit, že používání SSO[9], neboli systémů jednotného přihlášení vede ke snížení množství tajných autentizačních informací, které jsou uživatelé povinni chránit a zvyšuje tak dopad v případě prozrazení tajných autentizačních informací.

Čas potřebný k vypracování: 6 hodin.

A.9.4 řízení přístupu k systémům a aplikacím

Cíl: Zabránit neoprávněnému přístupu k systémům a aplikacím.

A.9.4.1 omezení přístupu k informacím

Opatření: Přístup k informacím a funkcím aplikačních systémů by měl být omezen v souladu s politikou řízení přístupu.

Implementace: Politika omezení přístupu ve společnosti by měla být založena na individuálních požadavcích podnikových aplikací a v souladu se stanovenou politikou řízení přístupu.

Je potřeba brát v úvahu následující body s požadavkem na omezení přístupu k informacím:

a) omezování informací obsažených ve výstupech

b) kontrola k jakým datům může konkrétní uživatel přistoupit

c) kontrola přístupových práv jiných aplikací

d) zajištění fyzického nebo logického řízení přístupu pro izolaci citlivých aplikací, aplikačních dat nebo systémů.

e) kontrola přístupových práv uživatelů v podobě práv na čtení, zápis a mazání

Čas potřebný k vypracování: 5 hodin.

[9] Single Sign On

A.9.4.2 bezpečné postupy přihlášení

Opatření: Pokud to vyžaduje politika řízení přístupu, přístup k systémům a aplikacím by měl být řízen bezpečným postupem přihlášení.

Implementace: Pro bezpečné přihlášení a doložení tak prohlašované identity uživatele, jenž se snaží do systému přihlásit by měla být vybrána vhodná autentizační metoda.

Jeli někde potřeba navýšit autentizaci a ověření identity uživatelů, měly by být použity autentizační metody, jenž jsou alternativou ke klasickým heslům, jako jsou čipové karty, kryptografické prostředky či biometrické prostředky například v podobě otisku prstu.

Postup přihlášení do systému či aplikaci by měl být navržen tak, aby se snížila možnost neautentizovaného přístupu na co nejmenší možnou. To znamená, že je uživateli pokoušejícímu se o přihlášení poskytnuto o systému nebo aplikaci co nejméně informací. Díky tomu nedojde k poskytnutí nadbytečných informací neoprávněnému uživateli.

Pro bezpečný postup přihlášení je důležité brát v úvahu několik faktorů:

a) zobrazovat obecné varování, že systém či aplikace mohou používat pouze oprávnění uživatelé

b) v průběhu přihlašovacího procesu neposkytovat žádné pomocné informace, jenž by mohly být nápomocny neoprávněnému uživateli

c) omezit možný počet pokusů přihlášení a po několika nesprávně zadaných pokusech systém či aplikaci dočasně zablokovat

   - potřebné k ochraně před slovníkovými útoky
   - zároveň je doporučeno zaznamenávat formou logu tyto neúspěšné pokusy o přihlášení

d) v případě podezření o potenciální pokus o narušení, nebo již úspěšné narušení při přihlašování je potřeba vyvolat bezpečnostní událost

e) používat vícefaktorové autentizační metody

Pro bezpečné přihlášení do systému doporučuji společnosti doplnit řešení smart card, které nabízí zabezpečení v podobě fyzického elektronického autorizačního zařízení, které slouží k získání přístupu do systému. Smart card je aktuálně nabízen několika výrobci na trhu. V organizaci je vhodné pořídit zařízení od společnosti HP, jelikož má organizace velkou většinu firemního zařízení právě od nich. . Doporučuji použití klávesnic s podporou smart card pro každého zaměstnance, kdy cena klávesnice v době psaní této diplomové práce činí 699 Kč. Zároveň bude potřeba objednat čipové karty pro každého zaměstnance, kde cena karty je zhruba do 100 Kč/kus.

Obrázek 5.2: Klávesnice se zabudovanou čtečkou čipových karet

Náklady: 19 975 Kč, kde cena zahrnuje klávesnice s čipovými kartami pro všechny zaměstnance

Čas potřebný k zavedení: 6 hodin.

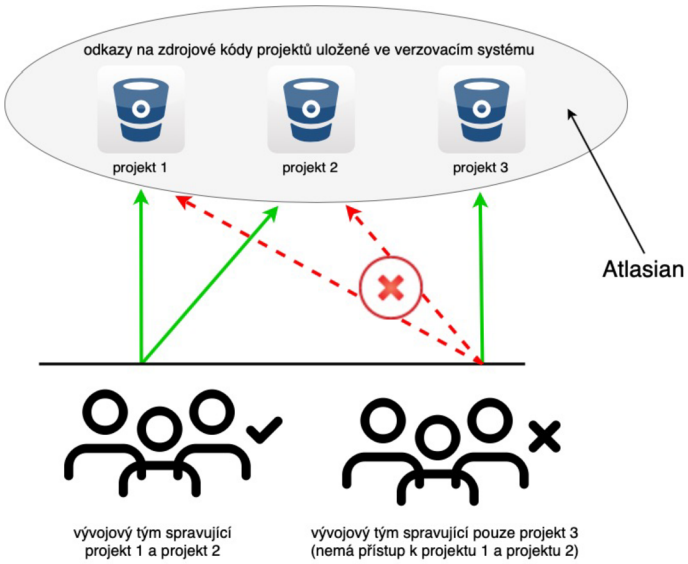
A.9.4.5 řízení přístupu ke zdrojovému kódu programu

Opatření: Přístup ke zdrojovému kódu programu by měl být omezen.

Implementace: Přístup ke zdrojovému kódu aplikace a k souvisejícím dokumentům, jenž společnost vyvíjí, by měl být omezen. Se zdrojovým kódem souvisí také dokumentace aplikace, navržená architektura aplikace, navržený databázový model či vytvořené grafické designy od grafika. Tato aktiva společnosti je zapotřebí přísně kontrolovat, aby nedošlo k neúmyslné změně či porušení duševního vlastnictví společnosti.

Je důležité zařídit, aby knihovny zdrojových kódů různých modulů, nejsou-li potřeba, nebyly uloženy v operačních systémech či někde na sdíleném disku s oprávněním pro všechny uživatele. Zároveň je potřeba zřídit záznam o všech přístupech ke knihovnám a samotným zdrojovým kódům aplikace společnosti.

Přístup ke zdrojovým kódům je v informačním systému Jira od společnosti Atlasian v modulu Confluence dostupný všem zaměstnancům. Doporučuji proto zavést politiku přístupu ke zdrojovým kódům pouze těm zaměstnancům, jenž jsou v rámci konkrétního týmu pracující s konkrétním modulem. Po následném dokončení projektu či přesun zaměstnance v rámci organizace do jiného vývojového týmu by měl se sebou nést také změnu možných oprávnění, ke kterým má mít tento zaměstnanec přístup.



Obrázek 5.3: Řízení přístupu ke zdrojovým kódům aplikace dle příslušného oprávnění

Čas potřebný k vypracování: 4 hodiny.

5.3.5 A.10 kryptografie

A.10.1

Cíl: Zajistit správné a efektivní využití kryptografie na ochranu důvěrnosti, autenticity 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.

Implementace: Ve společnosti je zapotřebí vypracovat politiku v oblasti kryptografie, která by měla zvážit následující aspekty:

a) při posuzování rizik by se měla určit požadovaná úroveň ochrany s ohledem na typ, sílu a kvalitu šifrovacího algoritmu

b) šifrovat komunikace pro ochranu informací přenášených prostřednictvím mobilních a přenosných zařízení, zařízení s možnou výměnou médií či komunikace přes komunikační linku

c) zajistit příslušné odpovědnosti a role

- kdo odpovídá za implementaci politiky
- kdo je zodpovědný za správu klíčů
- kdo generuje klíče nové

d) přístup ke správě klíčů pro obnovení zašifrované informace v případě ztráty, kompromitace nebo poškození klíčů

e) zajistit manažerský přístup ve vztahu k využití kryptografického opatření napříč celé organizace

- včetně obecných zásad, podle kterých by měly být informace společnosti chráněny

Ve společnosti doporučuji využít již zabudované řešení od společnosti Microsoft, které je dostupný již od verze OS Windows Vista. Jedná se o aplikaci BitLocker, která by společnosti zajistila ochranu informací uložených na pevném disku v případě ztráty či odcizení zařízení.

Zároveň je tak možné pomocí BitLockeru ochránit data, která potřebujeme vložit do jiného zařízení, jenž mohou být uložena na přenosných médiích, jako jsou:

- USB klíč
- externí hard disky
- SD[10] kartách apod.

Obrázek 5.4: BitLocker vyžadující heslo k obnově vedoucí ke zpřístupnění dat na disku

Náklady: Žádné, jelikož je BitLocker součástí operačního systému Windows
Čas potřebný k vypracování: 16 hodin.

5.3.6 A.11 fyzická bezpečnost a bezpečnost prostředí

A.11.1 zabezpečené oblasti

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

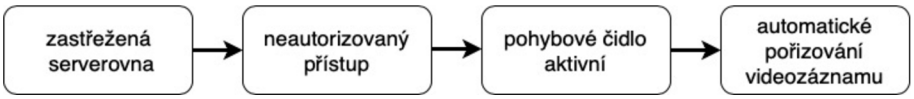
[10] Secure Digital

A.11.1.1 fyzický bezpečnostní perimetr

Opatření: Měly by být definovány bezpečnostní perimetry a ty by měly být použity k ochraně oblastí, které obsahují buď citlivé, nebo kritické informace a vybavení pro zpracování informací.

Implementace: Samotná společnost má již zavedený bezpečnostní perimetr v několika úrovních. Budova je chráněna plotem a bránami, které lze odemknout příslušným klíčem. Dále je řešen přístup do vnitřních prostorů společnosti, které jsou chráněny přístupovým systémem se čtečkou čipu. Zároveň je možné docílit přístupu do společnosti klasickým klíčem, jenž otevírá ty stejné dveře pouze jiným způsobem. Ihned po vstupu čidlo zaznamená pohyb a v případě zakódované budovy se spustí bezpečnostní alarm, po kterém vyjíždí společnost, jenž má na starost ostrahu objektu. Poté následuje přístup do kanceláří, které mají z vnější strany nainstalovány bezpečnostní mříže a přístup je možný pouze na klíč. Budovu společnosti lze tak považovat určitým způsobem za zabezpečenou.

Pro ještě vyšší bezpečnost lze navrhnout implementaci protipožárních dveří, které by byly implementovány do serverovny a chránily tak místnost před možným vzniknutím požáru. V serverovně již existuje čidlo pohybu, které v případě, že zaznamená neočekávaný pohyb spustí alarm. Doporučuji společnosti, aby čidlo doplnila o IP kameru s možností automatického nahrávání videozáznamu v případě, že v zakódované místnosti čidlo zaznamená pohyb. S tímto řešením je nutné upozornit všechny, kteří vstupují do serverovny, že je tam nainstalovaná bezpečnostní IP kamera snímající záznam. Proces automatického spuštění videozáznamu je možno vidět na obrázku 5.3.6.



Obrázek 5.5: Proces automatického spuštění videozáznamu při detekci neautorizovaného vstupu

Náklady: 5 499 Kč (protipožární dveře + IP kamera)
Čas potřebný k vypracování: 5 hodin.

A.11.1.2 fyzické kontroly vstupu

Opatření: Zabezpečené oblasti by měly být na vstupu chráněny vhodnými opatřeními, aby se zajistilo, že přístup mají povolen pouze oprávněné osoby.

Implementace: Jelikož ve společnosti není udržována a monitorována fyzická kniha záznamů, doporučuji společnosti zřídit zaznamenání vstupů do serverovny, kde by byl datum a čas příchodu a odchodu návštěvy. Dále by měli být všichni návštěvníci doprovázení se zodpovědným a pověřeným pracovníkem. Účel návštěvy by měl být konkrétní a zároveň by se měly sdělit pokyny týkající se bezpečnostních požadavků. Nemělo by se opomenout ani prověření totožnosti vhodnými prostředky. Pracovníci služeb podpory z externí strany, kteří se starají o internetové připojení by měli mít povinnost nosit určitou formu viditelného označení, v opačném případě je potřeba takový výskyt cizích osob v serverovně neprodleně nahlásit vedení společnosti a ověřit tak jejich totožnost vhodnými prostředky.

Čas potřebný k vypracování: 4 hodiny.

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.

Implementace: Jelikož má sídlo společnosti dobrou pozici vůči záplavám tzn. není v nížině, je situace v podobě zaplavení sídla společnosti nepravděpodobná.

Za to vznik požáru je ve společnosti daleko pravděpodobnější, jelikož se jedná o IT společnost, která disponuje mnoha zapojenými elektrickými zařízeními. Při manipulaci s těmito zařízeními může být úmyslně či neúmyslně učiněno nedokonalého zapojení a může tak vzniknout například zkrat, ze kterého je možné vzplanutí požáru. Proto společnosti doporučuji použít kouřová čidla pro detekci požáru a nainstalovat je jak do kanceláří, tak do společných prostorů, jako je například chodba, kuchyňka či zasedací místnost.

Náklady: 2 610 Kč (obsahuje 15 kouřových čidel)

Čas potřebný k zavedení: 6 hodin.

A.11.2 zařízení

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

A.11.2.1 umístění zařízení a jeho ochrana

Opatření: Zařízení by mělo být umístěno a chráněno tak, aby byla snížena rizika vyplývající z hrozeb a nebezpečí ze strany životního prostředí a z možností neoprávněného přístupu.

Implementace: Nejčastějším zařízením, jenž má každý zaměstnanec přiřazeno je přenosný počítač s dockovací stanicí nebo stolní pracovní stanice s jedním nebo více monitory. Pro zvýšení zabezpečení proti možné krádeži zařízení bych společnosti doporučil použít zámku na desktopové či přenosné zařízení spolu s periferními zařízeními od společnosti Kesington. V době psaní diplomové práce je dle [8] cena zámku 988 Kč za kus.

Zařízení vyžadující zvláštní ochranu, jako jsou ku příkladu NAS servery s uloženými daty, jsou umístěny v zabezpečené serverovně pro snížení potencionálních rizik, kterými jsou například krádež, poškození vodou, prach, vandalismus apod. Tato zařízení zároveň vyžadují k provozu určitou teplotu, kterou obstarávají dvě klimatizace v téže samé místnosti. Redundantní klimatizace zaručí udržení požadované teploty místnosti i v případě výpadku jedné z nich.

Obrázek 5.6: Zámek na desktop a periferní zařízení Kesington [8]

Náklady: 24 700 Kč
Čas potřebný k vypracování: 24 hodin.

A.11.2.2 podpůrné služby

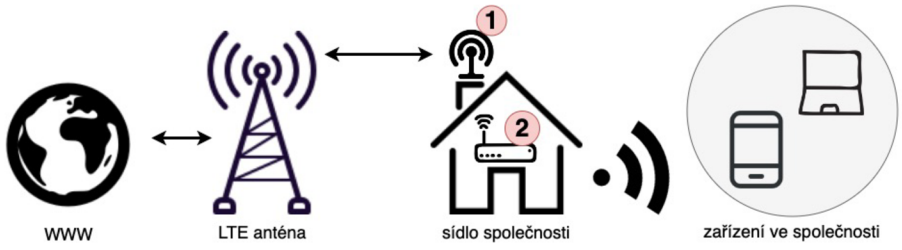
Opatření: Zařízení by mělo být chráněno před výpadkem napájení a dalšími poruchami způsobenými selháním podpůrných služeb.

Implementace: Pro ochranu zařízení před výpadkem a zajištění tak plynulého chodu ve společnosti doporučuji implementovat redundantní internetové připojení spolu se zdrojem nepřerušovaného napájení.

Pro redundantní připojení sítě internet v případě výpadku či závady kabelového připojení doporučují použít bezdrátové připojení nabízené od společnosti T-Mobile, která má aktuální nabídku s rychlostí stahování až 250 Mbit/s s neomezeným datovým limitem a měsíční cenou 799 Kč/měsíčně a 9 588 Kč/ročně. Způsobe pevného bezdrátového internetu, jenž společnost T-mobile nabízí je zachycen na obrázku 5.7.

Označení jedna v obrázku 5.7 je pro externí směrovou LTE anténu.

Označení dvě v v obrázku 5.7 je pro modem / Wi-Fi router.



Obrázek 5.7: Způsob připojení pevného internetu vzduchem

Při výpadku elektrické energie má společnost v serverovně k dispozici UPS zařízení, které dokážou udržet server po dobu několika desítek minut. Ve společnosti doporučuji udělat zátěžový test na již zavedená zařízení a v případě, že původní slíbená doba pro udržení provozu není dostačující, je vhodné nahradit zařízení za nová. V případě pracovních stanic doporučuji obměnit aktuální zdroje nepřerušovaného napájení za nové z důvodu jejich stáří

a pro případ, že zaměstnanci využívají práci na dálku přes VPN potřebují uložit aktuálně rozdělanou práci a neztratit tak editované změny. Doporučuji proto zařízení APC Back-UPS BX, na které je možno připojit až čtyři zařízení, což odpovídá maximálnímu počtu pracovních stanic na jednu kancelář. Cena za tento záložní zdroj v době psaní diplomové práce je 1 099 Kč.

Náklady: 17 281 Kč (záložní zdroje a roční připojení k internetu)

Čas potřebný k vypracování: 24 hodin.

A.11.2.3 bezpečnost kabelových rozvodů

Opatření: Silová a telekomunikační kabeláž určená pro přenos dat nebo podpůrných informačních služeb by měla být chráněna před odposloucháváním, rušením nebo poškozením.

Implementace: Pro ochranu kabeláže by měla být ve společnosti zvážena následující opatření:

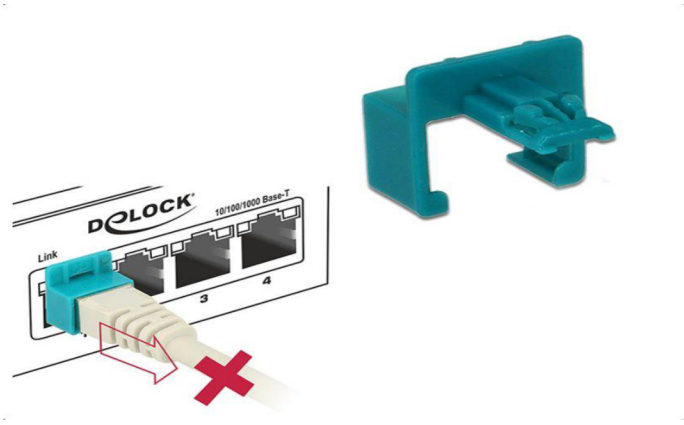
a) kabely sloužící k napájení by měly být odděleny od komunikačních kabelů pro minimalizaci rušení

b) napájecí a komunikační kabely pro zpracování informací by měly být vedeny nejlépe v podzemí, nebo by měly být chráněny jiným odpovídajícím způsobem

- uzamčení místností nebo skříní v koncových místech
- pravidelné technické prohlídky fyzických kontrol pro zjištění, zdali v kabeláži nejsou připojeny neoprávněné zařízení
- zavést řízení přístupu k propojovacím panelům

c) pro citlivé systémy by se navíc měla zvážit tato doplňující opatření:

Pro uzamčení kabelů a ochraně proti jejich odstranění a zároveň blokace zásuvky pro zajištění ochrany proti neoprávněnému použití doporučuji společnosti použít bezpečnostní spony Delock RJ45. Za cenu 386 Kč je v balení 40 bezpečnostních spon a jeden bezpečnostní nástroj pro jejich správu [15]. Řešení bezpečnostních spon je na obrázku 5.8.



Obrázek 5.8: Bezpečnostní spony pro RJ45 [8]

Náklady: 386 Kč

Čas potřebný k vypracování: 1 hodina.

Čas potřebný pro ověření 2 hodiny/ročně

A.11.2.4 údržba zařízení

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

Implementace: Pro údržbu zařízení je nutno vzít v potaz následující opatření:

a) zařízení by měla být udržována v souladu s doporučenými servisními intervaly a specifikací dodavatele

b) servis a opravy zařízení by měla být provedena autorizovanými pracovníky údržby

c) dodržení požadavků na údržbu, které vyplývají ze záručních smluv

Po údržbě či opravě je nutná kontrola, zdali zařízení funguje správně, nebo je nutná případná reklamace údržby, byla li vykonána externími pracovníky. V takovém případě je důležité při předávání zařízení externím společnostem vždy odebrat veškeré možné nosiče, na kterých se nachází data od společnosti. Za zařízení po údržbě je zodpovědný jeho vlastník. Zároveň je důležité dodržet základní údržbu zařízení, která se může týkat například odstranění prachu ze zařízení či konektorů.

Čas potřebný k vypracování: 2 hodiny.

A.11.2.6 bezpečnost zařízení a aktiv mimo prostory organizace

Opatření: Bezpečnost by se měla týkat aktiv mimo prostory organizace, s přihlédnutím k různým rizikům činnosti mimo prostory organizace.

Implementace: Použití jakéhokoliv zařízení pro uchovávání a zpracování informací mimo prostory organizace je potřeba schválit vedením společnosti. Schválení se týká zařízeních jak firemních, tak zařízeních v soukromém vlastnictví používané jménem organizace.

Jelikož společnost nabízí práci z domova, vznikají tak situace, kdy se zařízení nacházejí mimo prostory organizace. Zařízení je potřeba chránit proti odcizení či ztrátě na veřejných místech, kterými jsou například kavárny, knihovny, škola, restaurace či obchodní centra. Zároveň je potřeba mít aktivovaný BitLocker, jenž byl zmíněn v 5.3.5, který zajišťuje šifrování pevných disků. Zároveň je potřeba mít nastaveno řízení přístupu, jenž bylo navrženo v 5.3.4. Další zařízení, na která je dát pozor mimo prostory organizace jsou například přístupové čipy, mobilní telefony či různé firemní dokumenty.

Čas potřebný k vypracování: 3 hodiny.

A.11.2.8 neobsluhovaná uživatelská zařízení

Opatření: Uživatelé by měli zajistit přiměřenou ochranu neobsluhovaného zařízení.

Implementace: Je potřeba, aby všichni uživatelé měli povědomí o bezpečnostních požadavcích a postupech pro ochranu neobsluhovaného zařízení a také i jejich odpovědnost za realizaci této ochrany. Je nutné poučit zaměstnance společnosti, aby v případě dokončení činnosti či odchodu od zařízení se od svého zařízení odhlásili, a následně je potřeba nastavit vyžadování přístupového hesla do systému nebo jiné vhodné autentizované metody pro přihlášení při opětovném probuzení zařízení. Zaměstnanci by měli být rovněž poučeni o uzamčení svých kanceláří ihned po odchodu či v jiném případě jejich nepřítomnosti. V případe zapomenutí zařízení zamknout je důležité nastavit, aby zařízení přešlo do takového režimu automaticky po určité době nečinnosti, která může být stanovena v rozmezí 10-15 minut nečinnosti.

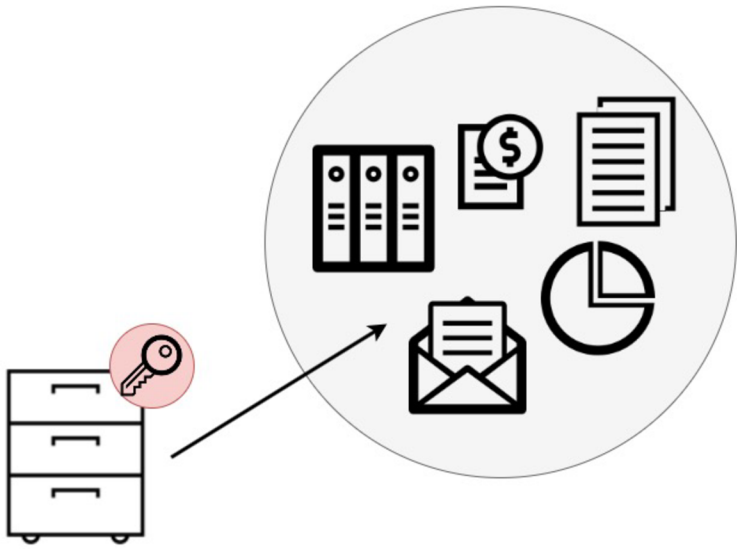
Čas potřebný k vypracování: 3 hodiny.

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.

Implementace: Pro vybavení zpracovávající informace by měla být ve společnosti přijata zásada prázdného stolu, týkající se papírových dokumentů a vyměnitelných paměťových médií (USB klíče, externí hard disky, interní smlouvy či dohody apod.) nebo zásada prázdné obrazovky.

Pro zajištění bezpečnosti vybavení zpracovávající ta nejdůležitější data doporučuji společnosti uložit toto vybavení do pojízdných zásuvkových kontejneru s centrálním zamykáním, kde využití je znázorněno v obrázku 5.9. Cena zmíněného kontejneru s výše uvedenými parametry je 2 799 Kč a tyto kontejnery budou umístěny v kancelářích pro vedení společnosti.



Obrázek 5.9: Možná ochrana dokumentů v pojízdném uzamykatelném kontejneru

Náklady: 11 196 Kč (4x kontejner)
Čas potřebný k vypracování: 3 hodiny.

5.3.7 A.12 bezpečnost provozu

A.12.2 ochrana 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.

Implementace: Ochrana před malwarem by měla být založena na detekci malwaru a opravných programech. Dále pak na povědomí o bezpečnosti informací odpovídajících opatření v oblasti přístupu k systému a řízení změn. Pro všechny pracovní stanice a servery

doporučuji i nadále využívat antivirový program od společnosti Norton. Doporučuji však stanice doplnit o aplikaci Norton Security Scan, která je bezplatná a prověřuje počítač na přítomnost virů, spywaru, trojských koňů a dalších bezpečnostních hrozeb. Pro ochranu mobilních zařízení je navrženo použití Norton Mobile Security v 5.3.1, který je pro kompatibilní se systémy Android a iOS.

Pro ochranu před phishingem, kdy se útočník snaží vylákat z uživatele citlivá data jako čísla kreditních karet či přihlašovací údaje, doporučuji zapnout Norton Safe Web.

Dále by měly být ve společnosti zváženy následující aspekty:

a) stanovit politiku, která zakazuje používání neautorizovaného softwaru

b) implementovat opatření detekující používání neautorizovaného softwaru

c) zavést opatření, které zabraňují či detekují navštěvování známých nebo podezřelých škodlivých internetových stránek

d) stanovení politiky na ochranu proti rizikům, jenž jsou spojena se stahováním souborů a softwaru z externích sítí nebo prostřednictvím jakéhokoliv jiného média

e) provádět pravidelné přezkoumání softwaru a datového obsahu systémů, které podporují kritické podnikové procesy

f) pravidelná aktualizace softwaru pro detekci malwaru (ve společnosti Norton) a opravných programů pro skenování počítače a médií jako preventivní opatření

g) skenování příloh elektronické pošty a stažených dat na přítomnost malwaru před jejich použitím

h) připravit postupy pro zotavení se z útoku, který byl zapříčiněn malwarem, včetně všech dat a záloh pro zotavení

i) izolovat prostředí, ve kterém mohou nastat katastrofické účinky

Náklady: Aplikace Norton Security Scan je zdarma a společnost již má předplacený antivirus Norton.

Čas potřebný k vypracování: 8 hodin.

A.12.3 zálohování

Cíl: Ochrana před ztrátou dat.

A.12.3.1 zálohování informací

Opatření: Pravidelně by měly být pořizovány a testovány záložní kopie informací, softwaru a bitových kopií systému v souladu se schválenou politikou zálohování.

Implementace: Ve společnosti je již zavedeno zálohování dat, která je prováděna na server NAS a v nepravidelných intervalech zhruba jednou za měsíc také na externí hard disk, jenž je uložen mimo prostory společnosti. Zálohování pracovních stanic se provádí každý pátek pomocí programu Acronis True Image.

Následující aspekty by se neměla opomenout při záloze dat:

a) vytvořit přesné a úplné záznamy o záložních kopiích

b) dokumentovat postupy v případě obnovy dat ze záloh

c) definovat rozsah záloh

- úplná
- rozdílová

d) uložit zálohy mimo prostory organizace aby v případě havárie nebyly zálohy poškozeny

e) záložním informacím by se měla poskytnout odpovídající fyzická a vnější ochrana (5.3.6) v souladu s normami aplikovanými v hlavním sídle

f) zálohy by měly být chráněny pomocí šifrování

Zároveň je důležité monitorovat průběh záloh a případné selhání procesu záloh naplánovat opětovný pokus zálohy dat pro zajištění úplnosti záloh.

Společnosti doporučuji použít sofistikovanější postup při záloze dat, která by byla mimo prostory organizace. Doporučuji použít datový sklad od společnosti Faster, které nabízí úložiště o kapacitě 1 TB s cenou 800 Kč/měsíčně. Pojem datový sklad může být matoucí, ale po ověření se jedná o službu klasického datového centra.

Faster nabízí pro zálohy dat [2]:

a) jednoduchou automatizaci záloh pomocí SW agenta

b) přenos dat po vyhrazené lince nebo VPN

c) ISO certifikaci

d) přístup k datům protokolem dle výběru

- FTP
- rsync
- scp
- Windows share

e) šifrování přenosu i uložených dat

f) automatickou replikaci dat do 3 geograficky nezávislých lokalit

g) diskovou kapacitu pro zálohování dat mimo budovu

Náklady: 9 600 Kč
Čas potřebný k vypracování: 20 hodin.
Čas potřebný pro pravidelné zálohování 12 hodin/ročně

A.12.4 zaznamenávání formou logů a monitorování

Cíl: Zaznamenávat události a generovat důkazy.

A.12.4.1 zaznamenávání událostí formou logů

Opatření: Musí být pořizovány, uchovávány a pravidelně přezkoumávány záznamy událostí formou logů zaznamenávající aktivity uživatelů, výjimky, selhání a události bezpečnosti informací.

Implementace: Záznamy události formou logů by měly obsahovat:

a) ID uživatele

b) činnost systému

c) datum, čas a podrobnosti důležitých událostí jako přihlášení a odhlášení

d) identitu nebo umístění zařízení a identifikátory systému

e) změny v konfiguraci systému

f) přidělené a privilegia a jejich použití

g) záznamy o úspěšných a zamítnutých pokusech o přístup k:

- datům
- systému
- dalším zdrojům

h) síťové adresy a protokoly

i) poplachy vyvolané systémem řízení přístupu

j) soubory, ke kterým bylo přistupováno s typem jejich přístupu

Jelikož záznamy události formou logů mohou obsahovat citlivá data a osobní údaje, měla by tak být přijata vhodná opatření na ochranu soukromí a pokud je to možné, správci systému by neměli mít oprávnění vymazat nebo deaktivovat záznamy formou logů o svých vlastních aktivitách.

Čas potřebný k vypracování: 10 hodin.

A.12.6 správa a řízení technických zranitelností

Cíl: Zabránit využívání technických zranitelností.

A.12.6.2 omezení instalace softwaru

Opatření: Měla by být stanovena a implementována pravidla řídící instalaci softwaru uživateli.

Implementace: Ve společnosti je zapotřebí definovat a prosazovat politiku, která určuje jaký typ softwaru mohou uživatelé instalovat na svá pracovní zařízení. Ve společnosti mají všichni zaměstnanci administrátorská práva a mají tak plnou kontrolu nad svou pracovní stanicí.

Společnosti doporučuji aplikovat princip minimálních privilegií a před instalovat veškerý potřebný software na pracovní stanici ještě před jejím předáním zaměstnanci. Dále by měla společnost zjistit, jaké typy instalace softwaru jsou povoleny. To zahrnuje například aktualizace a bezpečnostní záplaty již nainstalovaného softwaru. Dále zjistit, jaké instalace

jsou zakázány, kde spadá software pro osobní použití a software s potenciální škodlivostí od neznámého autora. Jednotlivá privilegia by měla být nastavena v souladu s aktuální roli daných uživatelů.

Čas potřebný k vypracování: 6 hodin.

5.3.8 A.13 bezpečnost komunikací

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.

Implementace: Při používání komunikačních zařízení pro přenos informací, by se mělo zvážit následující:

a) postupy pro detekci a ochranu před malwarem, který může být přenesen použitím elektronických komunikací viz. 5.3.7

b) postupy pro ochranu komunikovaných citlivých elektronických informací, které jsou ve formě přílohy

c) kontrolu a omezení spojené s používáním komunikačních zařízení

- například automatické přeposílání elektronické pošty na externí adresy

d) politiku omezující přípustné použití komunikačních zařízení

e) postupy navržené k ochraně přenášených informací před odposloucháváním, kopírováním, chybným směrováním, pozměněním či zničením

Ve společnosti se komunikuje převážně přes aplikaci Skype a jeho použití se doporučuje i nadále. Pro ochranu informací přenášených v podobě elektronických příloh doporučuji společnosti přílohy zašifrovat vhodným nástrojem.

Čas potřebný k vypracování: 4 hodiny.

5.4 Časový harmonogram a ekonomické zhodnocení

Společnost aplikuje pouze vybraná bezpečnostní opatření pro zvládání těch nejzávažnějších rizik, která byla identifikována na základě výsledků analýzy rizik. Zaváděním těchto opatření ve společnosti bude pověřen interní zaměstnanec se sazbou 400 Kč/hod. V případě externího bezpečnostního specialisty pak cena začíná na minimální sazbě 1000 Kč/hod. Vybraná relevantní bezpečnostní opatření s jejich časovou náročností a celkovými náklady jsou vyobrazena celkem do tří tabulek.

V sekci 5.4.2 v tabulce 5.13 zobrazím zvlášť náklady potřebné pro zavedení bezpečnostních opatření. Následně v sekci 5.4.1 v tabulce 5.12 shrnu náklady potřebné pro implementaci spolu s časovou náročností každého navrženého bezpečnostního opatření. Výsledky těchto tabulek budou v sekci 5.4.3 v tabulce 5.14, která je výsledkem a shrnutím tabulek předchozích, kde uvedu celkové pořizovací a implementační náklady navržených bezpečnostních opatření.

5.4.1 Náklady potřebné pro implementaci bezpečnostních opatření

opatření	časová náročnost v hod		náklady v Kč	
	počáteční	roční	implementační	roční
A.6.2.1 Politika mobilních zařízeni	7		2 800	2 800
A.6.2.2,Práce na dálku	6		2 400	2 400
A.7.1.2 podmínky pracovního poměru	4		1 600	1 600
A.7.2.2 povědomí, vzdělávání a školení o bezpečnosti informací	6	12	2 400	7 200
A.7.2.3 disciplinární řízení	12		4 800	4 800
A.7.3.1 odpovědnosti při ukončení nebo změně pracovního poměru	5		2 000	2 000
A.8.1.1 seznam aktiv	6	4	2 400	4 000
A.8.1.2 vlastníci aktiv	4		1 600	1 600
A.8.1.3 přípustné použití aktiv	6		2 400	2 400
A.8.2.3 manipulace s aktivy	12		4 800	4 800
A.9.1.1 politika řízení přístupu	20		8 000	8 000
A.9.1.2 přístup k sítím a síťovým službám	10		4 000	4 000
A.9.2.1 registrace a zrušení registrace uživatele	8		3 200	3 200
A.9.2.3 řízení privilegovaných přístupových práv	4		1 600	1 600
A.9.2.5 přezkoumání přístupových práv uživatelů	2	3	800	2 000
A.9.2.6 odebírání nebo úprava přístupových práv	4		1 600	1 600
A.9.3.1 použití tajných autentizačních informací	6		2 400	2 400
A.9.4.1 omezení přístupu k informacím	5		2 000	2 000
A.9.4.2 bezpečné postupy přihlášení	6		2 400	2 400
A.9.4.5 řízení přístupu ke zdrojovému kódu programu	4		1 600	1 600
A.10.1.1 politika použití kryptografických opatření	16		6 400	6 400
A.11.1.1 fyzický bezpečnostní perimetr	5		2 000	2 000
A.11.1.2 fyzické kontroly vstupu	4		1 600	1 600
A.11.1.4 ochrana před vnějšími a přírodními hrozbami	6		2 400	2 400
A.11.2.1 umístění zařízení a jeho ochrana	24		9 600	9 600
A.11.2.2 podpůrné služby	24		9 600	9 600
A.11.2.3 bezpečnost kabelových rozvodů	1	2	400	1 200
A.11.2.4 údržba zařízení	2		800	800
A.11.2.6 bezpečnost zařízení a aktiv mimo prostory organizace	3		1 200	1 200
A.11.2.8 neobsluhovaná uživatelská zařízení	3		1 200	1 200
A.11.2.9 zásada prázdného stolu a prázdné obrazovky monitoru	3		1 200	1 200
A.12.2.1 opatření na ochranu proti malwaru	8		3 200	3 200
A.12.3.1 zálohování informací	20	12	8 000	12 800
A.12.4.1 zaznamenávání událostí formou logů	10		4 000	4 000
A.12.6.2 omezení instalace softwaru	6		2 400	2 400
A.13.2.1 politiky a postupy při přenosu informací	4		1 600	1 600
celková časová náročnost a celkové náklady	**276**	**33**	**110 400**	**123 600**

Tabulka 5.12: Náklady potřebné implementaci bezpečnostních opatření

5.4.2 Náklady potřebné pro zavedení bezpečnostních opatření

opatření	název	náklady v Kč	
		pořizovací	roční
A.6.2.1	20x Norton Mobile Security		2 798
A.7.2.2	školení společností ESET na základě zvolené oblasti	10 000	
A.9.4.2	25x klávesnice se čtečkou čipových karet a čipové karty	19 975	
A.11.1.1	1x IP kamera s čidlem a 1x protipožární dveře	5 499	
A.11.1.4	15x kouřové čidlo	2 610	
A.11.2.1	25x zámek na desktop a periferní zařízení	24 700	
A.11.2.2	bezdrátové připojení k internetu		9 588
	4x zdroj nepřerušovaného napájení	4 396	
A.11.2.3	40x bezpečnostní spony pro RJ-45	386	
A.11.2.9	4x pojízdný uzamykatelný kontejner	11 196	
A.12.3.1	zálohování do datového centra		9 600
celkové náklady		**78 762**	**21 987**

Tabulka 5.13: Náklady potřebné k zavedení bezpečnostních opatření

5.4.3 Celkové náklady pro zavedení a implementaci bezpečnostních opatření

náklady	cena nákladů v Kč
zaváděcí	100 749
implementační	123 600
celkové	**224 349**

Tabulka 5.14: Celkové náklady pro zavedení a implementaci bezpečnostních opatření

Celkové náklady pro zavedení navržených bezpečnostních opatření činí 224 349 Kč. Tyto náklady nezahrnují zvládání všech rizik, které byly výsledkem analýzy rizik, ale pouze náklady pro zvládání těch nejzávažnějších rizik v tabulce 5.8 a tabulce 5.9, která na společnost působí a jsou pro společnost relevantní. Celkové náklady pro zavedení navržených bezpečnostních opatření činí 224 349 Kč. Tyto náklady jsou nezahrnují zvládání všech rizik, které byly výsledkem analýzy rizik, ale pouze náklady pro zvládání těch největších rizik v tabulce 5.8 a tabulce 5.9, která na společnost působí a jsou pro společnost relevantní. V pořizovacích nákladech je také zahrnuto navýšení bezpečnosti serverovny ve společnosti, které zahrnuje pořízení IP kamery a instalaci protipožárních dveří. V implementačních nákladech je pak zahrnuto například vytvoření fyzických kontrol při vstupu do serverovny.

5.4.4 Časový harmonogram návrhu zavedení bezpečnostních opatření

Celkový čas navržených bezpečnostních opatření byl odhadnut na 276 hodin, což je v přepočtu na člověkodny[11] 34.5 dne. Nejvhodnějším termínem pro zahájení zavádění bezpečnostních opatření je po prázdninách a dovolených, přesně datem 1. září 2019 s plánovaným dokončením do konce roku 2019. Zavádění navržených bezpečnostních opatření se může zpozdit, avšak rezerva v podobě čtyř měsíců, tedy do konce roku, je s odhadnutou časovou náročností zhruba 35 dní naprosto přijatelná. Celkem se jedná o 35 bezpečnostních opatření, která budou zavedena interním zaměstnancem.

Pro zavedení bezpečnostních opatření je třeba vypracovat plán, ve kterém budou jednotlivá bezpečnostní opatření postupně zavedena dle aktuálních potřeb společnosti a také dle priorit, které si společnost stanoví.

Po úspěšném zavedení těchto bezpečnostních opatření práce nekončí. Jedná se o nikdy nekončící proces neustálého zlepšování, přezkoumávání a udržování bezpečnostních opatření, jak bylo nastíněno v sekci 3.3. Vytvořené a zavedené politiky je potřeba chránit a kontrolovat jejich plnění a zároveň neustále aktualizovat, jelikož se mohou v průběhu času objevit hrozby nové, které mohly být v návrhu opomenuty nebo ty, které teprve vzniknou. Je proto potřeba vyhradit si čas pro kontroly těchto opatření v průběhu roku, které stanoví vedení společnosti na základě výsledků a získaných poznatků při provozu zavedených bezpečnostních opatření.

[11] Jednotka používaná při řízení projektů, která odpovídá 8 hodinám

Kapitola 6

Zhodnocení a přínosy práce

Přínosem této práce je bezpochyby zvýšení bezpečnostního povědomí všech pracovníků ve společnosti. Zaměstnanci byly poučení o informační bezpečnosti například v zásadách prázdného stolu a prázdné obrazovky monitoru popsané v 5.3.6 nebo o chování v případě používání tajných autentizačních informací popsaných v 5.3.4. Vedení společnosti bylo zase seznámeno například s odpovědností pří ukončení nebo změně pracovního poměru popsané v 5.3.2 nebo se všemi podmínkami, které je potřeba podchytit v pracovním poměru, jenž byl popsán v 5.3.2. Tohle byla pouhá ukázka toho, jak si obě skupiny uživatelů mohou zvýšit svůj přehled v problematice informační bezpečnosti a jak si mohou uvědomit možné bezpečnostní hrozby, jenž mohou být způsobeny i zcela neúmyslným chováním pracovníků a ve výsledku tak mohou působit na aktiva společnosti.

I přesto že se společnost v brzké době nechystá zavádět systém řízení bezpečnosti informací v plném rozsahu, má tak daleko větší konkurenční výhodu před ostatními organizacemi, které informační bezpečnost neřeší dle výsledků analýzy konkurenčního prostředí. V případě budoucího zájmu společnosti o úplného zavedení systému řízení bezpečnosti informací a případné certifikace dle ISO/IEC 27001 bude pro společnost jednodušší zavedení v plném rozsahu, protože již bude mít praxi s poměrně rozsáhlým rozpětím aplikovaných bezpečnostních opatření a bude se jednat pouze o doplnění nových bezpečnostních opatření.

Přínosem pro společnost je také zvýšení dosavadního zabezpečení serverovny, jenž bylo formulováno jako dílčí cíl této práce. Pro zvýšení bezpečnosti serverovny jsem navrhl opatření v podobě instalace IP kamery, která začne automaticky pořizovat videozáznam v případě, že dojde k pohybu v čase, kdy je serverovna zabezpečena. Zároveň je nutné zabezpečit kabely proti jejich odstranění a možnému neúmyslnému vytažení, proti čemuž jsem navrhl opatření s využitím bezpečnostních spon. Toto bezpečnostní opatření slouží zároveň k zamezení zapojení jakéhokoliv zařízení do příslušné zásuvky RJ-45. Jelikož je v této společnosti možné riziko vzniku požáru, navrhl jsem dále instalaci protipožárních dveří do serverovny a také jsem navrhl zavedení kouřových čidel. Krom toho se ve společnosti nevedl žádný záznam týkající se vstupu do serverovny. Navržená bezpečnostní opatření tedy kontrolují veškerý pohyb v místnosti. Zároveň byla navržena politika okamžitého informování vedení společnosti v případě, že se v serverovně vyskytuje neznámá osoba bez jasně viditelné formy označení pracovníka služeb podpory z externí strany.

Další přínos pro společnost spočívá v ušetřených nákladech, jenž by společnosti vznikly v případě vyhotovení analýzy rizik externí společností, která by si za obdobné vyhotovení mohla naúčtovat až několik desítek tisíc korun. V analýze jsem identifikoval řadu rizik působících na společnost, avšak podrobněji jsem navrhl pouze bezpečnostní opatření týkající se rizik nejzávažnějších a nejrelevantnějších. Pokud si společnost uvědomí přínos navržených

a následně zavedených bezpečnostních opatření pro běžný provoz, může navázat na tuto práci a svá bezpečnostní opatření dále rozšiřovat i o ta, která byla rozpoznána na základě analýzy rizik a která více nerozpracovávám.

Společnost jsem seznámil s politikou mobilních zařízení, která je pro ni určitě přínosem. V této politice navrhuji použít řešení aplikace Norton Security Mobile, jenž nabízí ochranu proti krádeži s využitím možnosti vzdáleného uzamknutí odcizených zařízení. S používáním mobilních a přenosných zařízení byla zároveň navržena politika používání kryptografických opatření, která šifruje pevné disky pomocí vestavěné aplikace BitLocker a jenž je součástí operačního systému Windows na každé pracovní stanici.

Pro příklad uvedu výši škody, která by vznikla v případě rozhodnutí neaplikovat bezpečnostní opatření zajišťující ochranu aktiv. Společnost vyvíjející software potřebuje pro své zaměstnance zajistit pracovní stanice. K pracovním stanicím je připojen jeden nebo dva monitory, dle zvyklostí konkrétního pracovníka. Cena jedné pracovní stanice začíná od zhruba 30 tisíc korunách. Cena za monitor je ve společnosti zhruba sedm až deset tisíc korun. Pokud má zaměstnanec k dispozici monitory dva, činí cena 14 až 20 tisíc korun. V případě, že by ve společnosti došlo ke krádeži pracovních stanic, vznikla by společnosti ztráta dosahující až 40 tisíc korun za jednu pracovní stanici včetně monitoru. Jelikož je ve společnosti zhruba 25 pracovníků, tedy i stanic, cena za všechny pracovní stanice dosahuje téměř jednoho milionu korun. Opatření eliminující vznik krádeže pracovních zařízení bylo navrženo v 5.3.6, které pojednává o ochraně zařízení a jeho umístění. Cena za ochranu jedné pracovní stanice je 988 Kč, tudíž cena za ochranu všech zařízení vychází na 24 700 Kč. Tato částka je zanedbatelná oproti finanční ztrátě v případě odcizení veškerých pracovních stanic. Škody by však dosahovaly větších rozměrů, jelikož by narušily chod firmy z důvodu ztráty rozdělané práce zaměstnanců. Dále by pak mohlo dojít ke kompromitaci informací týkajících se duševního vlastnictví společnosti například v podobě navržené architektury aplikace. Zmiňované následky jsou řešeny v dalších navržených bezpečnostních opatřeních. Tento příklad byl zaměřen zejména na ochranu zařízení a jeho umístění.

Přínosem práce je mimo jiné seznámení společnosti s GDPR, které vstoupilo v platnost 25. května 2018. Společnost byla informována o tom, jaké informace může o svých zaměstnancích shromažďovat na veřejně dostupných prostorech a které informace již nemohou být součástí elektronické pošty, jak tomu bylo doposud. I když problematika obecného nařízení na ochranu osobních údajů není hlavním tématem této práce, tak s informační bezpečností úzce souvisí. Z toho důvodu byly společnosti představeny alespoň její hlavní kritéria.

Kapitola 7

Závěr

Hlavním cílem této diplomové práce byl návrh zavedení bezpečnostních opatření do malé společnosti vyvíjející softwarovou aplikaci. Dílčím cílem bylo navýšit dosavadní zabezpečení serverovny. Tyto cíle byly splněny.

Pro dosažení výsledků bylo nejprve nutné seznámení se s problematikou informační bezpečnosti, které zahrnovalo teoretické základy pro objasnění použitých pojmů a názvosloví. Detailněji byl vysvětlen systém řízení bezpečnosti informací, který vychází z norem řad ISO/IEC 27000.

Na základě získaných poznatků jsem vyhotovil analýzu současného stavu bezpečnosti ve společnosti a zaměřil se na vybrané oblasti týkající se informační bezpečnosti. Současně společnost definovala svá očekávání spolu s požadavky na tuto práci. Poté jsem analyzoval poměrně nové změny týkající se legislativy, jenž souvisí s bezpečnosti informací.

Dále následoval návrh vlastního řešení, který vymezil rozsah práce. Ve svém navrženém řešení jsem vyhotovil analýzu rizik, ze které vychází návrh zavedení bezpečnostních opatření. Při návrhu bezpečnostních opatření jsem vycházel z normy ČSN ISO/IEC 27001:2017 přílohy A a normy ČSN ISO/IEC 27002:2017. Navrhl jsem celkem 36 bezpečnostních opatření, jenž jsou pro společnost nezbytná a jejichž zavedení by mělo být podle časového plánu dokončeno do roku 2019. Zároveň jsem provedl ekonomické zhodnocení bezpečnostních opatření, které bylo rozděleno do nákladů potřebných pro implementaci a nákladů potřebných pro zavedení. Zavedením těchto bezpečnostních opatření se předpokládá navýšení současného stavu bezpečnosti ve společnosti.

Zhodnocení práce a její hlavní přínosy pro společnost byly detailněji popsány v kapitole 6.

Vypracování této práce bylo pro mne velmi zajímavou zkušeností, která rozšířila mé znalosti v otázkách bezpečnosti informací.

Jelikož je systém řízení bezpečnosti informací nikdy nekončící proces, je potřeba iniciovat další kroky vedoucí k jeho neustálému zlepšování a přezkoumávání. Tímto se nabízí možnost pokračovat v práci do budoucna a přizpůsobovat navržená opatření nově se vyskytujícím hrozbám.

Seznam použitých zkratek

CEN	—	European Committee for Standardization
CENELEC	—	European Committee for Electrotechnical Standardization
COBIT	—	Control Objectives for Information and Related Technology
CSS	—	Cascading Style Sheets
ČSN	—	Česká technická norma
ČSNI	—	Český normalizační institut
ETSI	—	European Telecommunications Standards Institute
EU	—	Evropská unie
GPS	—	Global Positioning System
HP	—	Hewlett-Packard
ICT	—	Information and Communication Technology
IE	—	Internet Explorer
IEC	—	International Electrotechnical Commission
IP	—	Internet Protocol
IS	—	Information system
ISMS	—	Information security management system
ISO	—	International Organization for Standardization
IT	—	Information Technology
ITIL	—	Information Technology Infrastructure Library
ITU	—	International Telecommunications Union
KII	—	Kritická informační infrastruktura
MAC	—	Media Access Control
NAS	—	Network-attached storage
NCKB	—	Národní centrum kybernetické bezpečnosti
NÚKIB	—	Národní úřad pro kybernetickou a informační bezpečnost
OSN	—	Organizace spojených národů
RDP	—	Remote Desktop Protocol
RFC	—	Request for Comment
SD	—	Secure Digital
SSID	—	Service Set Identifier
SSO	—	Single Sign On
UI	—	User interface
VIS	—	Významné informační systémy
VNC	—	Virtual Network Computing
VPN	—	Virtual Private Network

Literatura

[1] Atlassian: *Nástroj pro vývoj softwaru.* [Online; navštíveno 8.02.2019].
URL https://www.atlassian.com/

[2] BEFASTER: *Služby datového centra.* [Online; navštíveno 9.4.2019].
URL http://zelenadata.cz/cs/sluzby/datovy-sklad/

[3] DOUČEK, P.; NOVÁK, L.; SVATÁ, V.: *Řízení bezpečnosti informací.* Praha: Professional Publishing, 2011, ISBN 978-80-7431-050-8.

[4] ESET: *Řízení informační bezpečnosti.* [Online; navštíveno 27.03.2019].
URL https://www.eset.com/cz/firmy/eset-services/

[5] Glassdoor: *Celosvětový průzkum mezd a pracovních pozic.* [Online; navštíveno 2.02.2019].
URL https://www.glassdoor.com/

[6] Kurzy: *Kurzovní lístek ČNB.* [Online; navštíveno 2.02.2019].
URL https://www.kurzy.cz/kurzy-men/

[7] LMC: *Aktuální nabídka práce v ČR.* [Online; navštíveno 2.02.2019].
URL https://www.prace.cz/

[8] Mironet: *Zámek na desktop a jeho periferní zařízení.* [Online; navštíveno 4.4.2019].
URL https://www.mironet.cz/kensington-zamek-na-desktop-perifereni-zarizeni+dp354938/

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

[10] POŽÁR, J.: *Manažerská informatika.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010, ISBN 978-80-7380-276-9.

[11] Profesia: *Průzkum platů v ČR.* [Online; navštíveno 2.02.2019].
URL https://www.platy.cz/

[12] RAIS, K.; DOSKOČIL, R.: *Risk management: studijní text pro kombinovanou formu studia.* Brno: Akademické nakladatelství CERM, 2007, ISBN 978-80-214-3510-0.

[13] SEDLÁK, P.: *Zavádění a provozování ISMS.* Brno [přednáška], 2019.

[14] SODOMKA, P.; KLČOVÁ, H.: *Informační systémy v podnikové praxi. 2., aktualiz. a rozš. vyd.* Brno: Computer Press, 2010, ISBN 978-80-251-2878-7.

[15] SUNTECH Computer: *Bezpečnostní spony Delock RJ45*. [Online; navštíveno 5.4.2019].
URL https://www.suntech.cz/produkt/435871-delock-rj45-bezpecnostni-spona-startovaci-sada-40-kusu/

[16] Symantec: *Funkce aplikace Norton Mobile Security*. [Online; navštíveno 20.03.2019].
URL https://support.norton.com/sp/cs/cz/norton-mobile/current/solutions/v77490791_EndUserProfile_cs_cz?inid=hho_supp_htm_mobile-cur-retail-topnms-03-v77490791&src=NMS_support&type=NMS_support

[17] ČERMÁK, M.: *Řízení informačních rizik v praxi*. Brno: Tribun EU, 2009, ISBN 978-80-7399-731-1.

[18] ČSN EN ISO/IEC 9000: *Systémy managementu kvality - Základní principy a slovník*. Praha: Úřad pro technickou normalizaci, 2016.

[19] ČSN ISO/IEC 27000: *Informační technologie - Bezpečnostní techniky – Systémy řízení bezpečnostní informací - Přehled a slovník*. Praha: Úřad pro technickou normalizaci, 2017.

[20] ČSN ISO/IEC 27001: *Informační technologie - Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, 2017.

[21] ČSN ISO/IEC 27002: *Informační technologie - Bezpečnostní techniky – Systémy řízení bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, 2017.

[22] ŠKORNIČKOVÁ, E.: *Obecné nařízení na ochranu osobních údajů*. [Online; navštíveno 4.02.2019].
URL https://www.gdpr.cz/

Seznam obrázků

Seznam tabulek

Přílohy

Příloha A

Prohlášení o aplikovatelnosti

A.5 Politiky bezpečnosti informací

A.5.1 Politiky bezpečnosti informací

Cíl: Poskytnou pokyny a podporu ze strany managementu pro bezpečnost informací v souladu s požadavky podnikatelské činnosti organizace a příslušnými tohle je zákony zákony a předpisy.

A.5.1.1 Pokyny managementu organizace k bezpečnosti informací

Opatření: Musí být definována sada politik pro bezpečnost informací, schválena managementem, zveřejněna a dána na vědomí zaměstnancům a relevantním externím stranám
Vyloučeno: Ano

A.5.1.2 Přezkoumání politik pro bezpečnost informací

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

A.6 Organizace bezpečnost 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 odpovědnosti bezpečnosti informací

Opatření: Všechny odpovědnosti za bezpečnost informací musejí být definovány a přiděleny.
Vyloučeno: Ano
Způsob plnění požadavku: Příručka ISMS

A.6.1.2 Princip oddělení povinností

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

Vyloučeno: Ano
Způsob plnění požadavku: Každý zaměstnanec má jasně definovanou roli a své odpovědnosti vůči organizace definované v dokumentu s popisem pracovní pozice.

A.6.1.3 Kontakt s autoritami

Opatření: Musí být udržovány přiměřené kontakty s příslušnými autoritami.
Vyloučeno: Ano
Způsob plnění požadavku: Veškerá komunikace ve společnosti probíhá na denní bázi, jelikož se jedná o malý podnik.

A.6.1.4 Kontakt se zvláštními zájmovými skupinami

Opatření: Musí být udržovány přiměřené kontakty se zvláštními zájmovými skupinami nebo dalšími fóry specialistů na bezpečnost a profesními sdruženími.
Vyloučeno: Ano
Způsob plnění požadavku: není používáno.

A.6.1.5 Bezpečnost informací v řízení projektů

Opatření: Bezpečnost informací musí být řešena v rámci řízení projektů, bez ohledu na typ projektu.
Vyloučeno: Ano
Způsob plnění požadavku: Ve společnosti jsou nastavena přístupová práva k informacím týkající se projektu na základě přiřazeného týmu, který má nastaven konkrétní projekt.

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 musí být přijata politika a podpůrná bezpečnostní opatření.
Vyloučeno: Ne
Způsob plnění požadavku: Musí být přijata politika a relevantní bezpečnostní opatření mobilních zařízení spolu s aplikací Norton Mobile Security pro správy mobilních zařízení na dálku.

A.6.2.2. Práce na dálku

Opatření: Na ochranu informací, k nimž je přistupováno v rámci práce na dálku, zpracovaných nebo ukládaných v místech práce na dálku musí být zavedena politika a podpůrná bezpečnostní opatření.
Vyloučeno: Ne
Způsob plnění požadavku: Musí být implementována politika a relevantní bezpečnostní opatření definující podmínky pro práci na dálku v prostorech mimo organizaci s aktivním šifrováním pevných disků pomocí aplikace BitLocker a zpřístupnění vzdálené plochy v antivirovém programu Norton.

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 musí být prováděno v souladu s příslušnými zákony, nařízeními a v souladu s etikou a musí být úměrné požadavkům souvisejícím s činností organizace, klasifikaci informací, ke kterým má být umožněn přístup a vnímaným rizikům.
Vyloučeno: Ano
Způsob plnění požadavku: Všichni uchazeči o zaměstnání musí být prověřeni podle platných zákonů, předpisů a v souladu s etikou. Prověření musí být prováděna na základě požadavků týkajících se činností organizace, dále s ohledem na klasifikaci informací, ke kterým by měli získat přístup, a také z hlediska potencionálních rizik.

A.7.1.2 Podmínky pracovního poměru

Opatření: Smlouvy se zaměstnanci a smluvními stranami musí uvádět odpovědnosti zaměstnanců/smluvních stran a organizace za bezpečnost informací.
Vyloučeno: Ne
Způsob plnění požadavku: pracovní smlouva.

A.7.2 Během pracovního poměru

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

A.7.2.1 Odpovědnosti managementu organizace

Opatření: Management musí od všech zaměstnanců a smluvních stran požadovat, aby aplikovali bezpečnost informací v souladu se zavedenými politikami a postupy organizace.
Vyloučeno: Ano
Způsob plnění požadavku: Příručka ISMS

A.7.2.2 Povědomí, vzdělání a školení o bezpečnosti informací

Opatření: Všichni zaměstnanci organizace a tam, kde je to vhodné, i smluvní strany musí získat odpovídající povědomí o bezpečnosti informací formou vzdělávání a školení a pravidelných aktualizací politik a postupů organizace, dle významu pro zastávanou pracovní funkci.
Vyloučeno: Ne
Způsob plnění požadavku: Ve společnosti je zaveden plán pro pravidelné vzdělávání a školení všech zaměstnanců.

A.7.2.3 Disciplinární řízení

Opatření: Musí existovat formální disciplinární proces, oznámený všem, pro podniknutí kroků vůči zaměstnancům, kteří se dopustili narušení bezpečnosti informací.
Vyloučeno: Ne
Způsob plnění požadavku: Příručka ISMS

A.7.3 Ukončení a změna pracovního poměru

Cíl: Chránit zájmy organizace jako součást procesu změny nebo ukončení pracovního poměru.

A.7.3.1 Odpovědnosti při ukončení nebo změně pracovního poměru

Opatření: Odpovědnost a povinnosti v oblasti bezpečnosti informací, které zůstávají v platnosti i po ukončení nebo změně zaměstnání, musí být definovány, sděleny zaměstnanci nebo smluvní straně a prosazovány.
Vyloučeno: Ne
Způsob plnění požadavku: Vytvořen dokument s postupnými kroky přístupových práv a účtů, které je potřeba odebrat.

A.8 Řízení aktiv

A.8.1 Odpovědnost za aktiva

Cíl: Identifikovat aktiva organizace a definovat odpovědnost za přiměřenou ochranu.

A.8.1.1 Seznam aktiv

Opatření: Aktiva související s informacemi a vybavením pro zpracování informací musí být identifikována a musí by být sestaven a udržován seznam těchto aktiv.
Vyloučeno: Ne
Způsob plnění požadavku: Seznam evidující aktiva společnosti

A.8.1.2 Vlastnictví aktiv

Opatření: Aktiva udržovaná v seznamu musí mít vlastníka.
Vyloučeno: Ne

A.8.1.3 Přípustné použití aktiv

Opatření: Musí být identifikována, dokumentována a implementována pravidla pro přípustné používání informací a aktiv spojených s informacemi a vybavením pro zpracování informací.
Vyloučeno: Ne
Způsob plnění požadavku: Dokument definující přípustné použití aktiv danými uživateli.

A.8.1.4 Vrácení aktiv

Opatření: Všichni zaměstnanci a uživatelé z externích stran musí po ukončení svého zaměstnání, smlouvy nebo dohody vrátit všechna aktiva organizace, která měli v držení.
Vyloučeno: Ano

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 musí být klasifikovány z hlediska právních požadavků, hodnoty, kritičnosti a citlivost ve vztahu k neoprávněnému prozrazení nebo modifikaci.
Vyloučeno: Ano

A.8.2.2 Označování informací

Opatření: Pro označování informací musí být vypracovány a implementovány vhodné soubory postupů, v souladu se schématem klasifikace informací přijatých organizací.
Vyloučeno: Ano

A.8.2.3 Manipulace s aktivy

Opatření: Pro zacházení s aktivy musí být vyvinuty a zavedeny postupy, v souladu se schématem klasifikace informací přijatým organizací.
Vyloučeno: Ne
Způsob plnění požadavku: Dokument obsahující postupy při manipulaci s aktivy.

A.8.3 Manipulace s médii

Cíl: Zabránit neoprávněnému prozrazení, modifikaci, odstranění nebo zničení informací uložených na médiu.

A.8.3.1 Správa výměnných médií

Opatření: Pro správu výměnných médií musí být zavedeny postupy, v souladu se schématem klasifikace přijatým organizací.
Vyloučeno: Ano

A.8.3.2 Likvidace médií

Opatření: Pokud již média nejsou zapotřebí, musí být bezpečně zlikvidována dle formálních postupů.
Vyloučeno: Ano

A.8.3.3 Přeprava fyzických médií

Opatření: Média obsahující informace musí být během přepravy chráněna před neoprávněným přístupem, zneužitím nebo poškozením.
Vyloučeno: Ano

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 musí být stanovena, dokumentována a přezkoumávána politika řízení přístupu.
Vyloučeno: Ne
Způsob plnění požadavku: Dokument s politikou řízení přístupu.

A.9.1.2 Přístup k sítím a síťovým službám

Opatření: Uživatelům musí být poskytován přístup pouze k těm sítím a síťovým službám, pro jejichž použití byli výhradně autorizováni.
Vyloučeno: Ne
Způsob plnění požadavku: Vhodně nastavena práva v Active Directory.

A.9.2 Správa a řízení přístupu uživatelů

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

A.9.2.1 Registrace a zrušení registrace uživatele

Opatření: Pro přidělování přístupových práv musí být zaveden proces formální registrace a deregistrace uživatele.
Vyloučeno: Ne
Způsob plnění požadavku: Dokumentovaný proces správy uživatelů.

A.9.2.2 Zřízení přístupu uživatele

Opatření: Musí být zaveden formální proces poskytování přístupu uživatele pro přiřazení nebo zrušení přístupových práv pro všechny typy uživatelů a ke všem systémům a službám.
Vyloučeno: Ano

A.9.2.3 Řízení privilegovaných přístupových práv

Opatření: Přidělení a použití privilegovaných přístupových práv musí být omezeno a řízeno.
Vyloučeno: Ne
Způsob plnění požadavku: Dokumentovaný proces správy uživatelů.

A.9.2.4 Řízení tajných autentizačních informací uživatelů

Opatření: Přidělení tajných autentizačních informací musí být řízeno prostřednictvím formálního procesu řízení.
Vyloučeno: Ano

A.9.2.5 Přezkoumání přístupových práv uživatelů

Opatření: Vlastníci aktiv musí v pravidelných intervalech přezkoumávat přístupová práva uživatelů.
Vyloučeno: Ne

A.9.2.6 Odebrání nebo úprava přístupových práv

Opatření: Přístupová práva všech zaměstnanců a uživatelů z externích stran k informacím a vybavení pro zpracování informací musí být po ukončení jejich zaměstnání, smlouvy nebo vypršení dohody odstraněna nebo ihned po změně upravena.
Vyloučeno: Ne
Způsob plnění požadavku: Dokumentovaný proces správy uživatelů.

A.9.3 Odpovědnosti uživatelů

Cíl:Učinit uživatele odpovědné za ochranu svých autentizačních informací.

A.9.3.1 Použití tajných autentizačních informací

Opatření: Po uživatelích musí být vyžadováno, aby při používání tajných autentizačních informací dodržovali postupy organizace.
Vyloučeno: Ne
Způsob plnění požadavku: Pracovní smlouva a interní příručka pro nového uživatele.

A.9.4 Řízení přístupu k systémům a aplikacím

Cíl:Zabránit neoprávněnému přístupu k systémům a aplikacím.

A.9.4.1 Omezení přístupu k informacím

Opatření: Přístup k informacím a funkcím aplikačních systémů musí být omezen v souladu s politikou řízení přístupu.
Vyloučeno: Ne
Způsob plnění požadavku: Dokument politiky pro řízení přístupů uživatelů s využitím Active Directory.

A.9.4.2 Bezpečné postupy přihlášení

Opatření: Pokud to vyžaduje politika řízení přístupu, přístup k systémům a aplikacím musí být řízen bezpečným postupem přihlášení.
Vyloučeno: Ne
Způsob plnění požadavku: Interní příručka pro nového uživatele.

A.9.4.3 Systém správy hesel

Opatření: Systémy správy hesel musí být interaktivní a musí zajistit kvalitní hesla.
Vyloučeno: Ano

A.9.4.4 Použití privilegovaných obslužných programů

Opatření: Použití obslužných programů, které by mohly být schopné potlačit systémová a aplikační opatření, musí být omezeno a přísně kontrolováno.
Vyloučeno: Ano

A.9.4.5 Řízení přístupu ke zdrojovému kódu programu

Opatření: Přístup ke zdrojovému kódu programu musí být omezen.
Vyloučeno: Ne
Způsob plnění požadavku: Dokument s politikou přístupu ke zdrojovým kódům.

A.10 Kryptografie

A.10.1 Kryptografická opatření

Cíl: Zajistit správné a efektivní využití kryptografie na ochranu důvěrnosti, autenticity a/-nebo integrity informací.
Opatření: Musí být vypracována a realizována politika použití kryptografických opatření na ochranu informací.
Vyloučeno: Ne
Způsob plnění požadavku: Dokument s politikou použití kryptografických prostředků a zacházení s informacemi uložených na přenosných médiích včetně aktivního nastavení aplikace BitLocker.

A.10.1.2 Správa klíčů

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

A.11 Fyzická bezpečnost a bezpečnost prostředí

A.11.1 Zabezpečené oblasti

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

A.11.1.1 Fyzický bezpečnostní perimetr

Opatření: Musí být definovány bezpečnostní perimetry a ty by musí být použity k ochraně oblastí, které obsahují buď citlivé, nebo kritické informace a vybavení pro zpracování informací.
Vyloučeno: Ne
Způsob plnění požadavku: Implementace několika úrovní bezpečnostního perimetru pro ochranu citlivých oblastí pomocí zabezpečeného vstupu do budovy, zabezpečení budovy pomocí alarmu a uzamykatelných kanceláří. V případě serverovny je bezpečnost navýšena o protipožární dveře a IP kameru se zabudovaným čidlem detekce pohybu.

A.11.1.2 Fyzické kontroly vstupu

Opatření: Zabezpečené oblasti musí být na vstupu chráněny vhodnými opatřeními, aby se zajistilo, že přístup mají povolen pouze oprávněné osoby.
Vyloučeno: Ne
Způsob plnění požadavku: Fyzická kniha záznamů s časem příchodu a odchodu včetně účelu vstupu do serverovny.

A.11.1.3 Zabezpečení kanceláří, místností a vybavení

Opatření: Musí být navržena a uplatněna opatření pro fyzickou bezpečnost kanceláří, místností a vybavení.
Vyloučeno: Ano

A.11.1.4 Ochrana před vnějšími a přírodními hrozbami

Opatření: Musí být navržena a uplatněna fyzická ochrana před přírodními katastrofami, zlomyslnými útoky nebo nehodami.
Vyloučeno: Ne
Způsob plnění požadavku: Implementace kouřových čidel v případě vzniku požáru.

A.11.1.5 Práce v zabezpečených oblastech

Opatření: Musí být navrženy a uplatněny postupy pro práci v zabezpečených oblastech.
Vyloučeno: Ano
Způsob plnění požadavku: Pro přístup do společnosti je vyžadována autentizace uživatele.

A.11.1.6 Oblasti pro nakládku a vykládku

Opatření: Místa přístupu, jako jsou prostory pro vykládku a nakládku, a další místa, kde by mohly neoprávněné osoby vstupovat do objektů musí být kontrolovány, a pokud je to možné, izolovány od vybavení pro zpracování informací, aby se zabránilo neoprávněnému přístupu.
Vyloučeno: Ano

A.11.2 Zařízení

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

A.11.2.1 Umístění zařízení a jeho ochrana

Opatření: Zařízení musí být umístěno a chráněno tak, aby byla snížena rizika vyplývající z hrozeb a nebezpečí ze strany životního prostředí a z možností neoprávněného přístupu.
Vyloučeno: Ne
Způsob plnění požadavku: Umístění důležitých zařízení, jako třeba servery NAS, vyžadujících zvláštní podmínky, jako například dodržení určité teploty místnosti, jsou umístěny v serverovně. Pracovní stanice jsou chráněny proti možnému vzniku krádeže zámkem pro desktop a periferní zařízení.

A.11.2.2 Podpůrné služby

Opatření: Zařízení musí být chráněno před výpadkem napájení a dalšími poruchami způsobenými selháním podpůrných služeb.
Vyloučeno: Ne
Způsob plnění požadavku: Zavedení redundantního připojení k internetu a zřízení zdroje nepřetržitého napájení.

A.11.2.3 Bezpečnost kabelových rozvodů

Opatření: Silová a telekomunikační kabeláž určená pro přenos dat nebo podpůrných informačních služeb musí být chráněna před odposloucháváním, rušením nebo poškozením.
Vyloučeno: Ne
Způsob plnění požadavku: Nasazení bezpečnostních spon pro ochranu před neúmyslným vytažením kabelu či před připojením neautorizovaného zařízení.

A.11.2.4 Údržba zařízení

Opatření: Zařízení musí být správně udržováno pro zajištění jeho stálé dostupnosti a integrity.
Vyloučeno: Ne

A.11.2.5 Přemístění aktiv

Opatření: Zařízení, informace nebo software nemůžou být přemístěny mimo organizaci bez předchozího povolení.
Vyloučeno: Ano

A.11.2.6 Bezpečnost zařízení a aktiv mimo prostory organizace

Opatření: Bezpečnost se musí týkat aktiv mimo prostory organizace, s přihlédnutím k různým rizikům činnosti mimo prostory organizace.
Vyloučeno: Ne
Způsob plnění požadavku: Dokument politiky řízení přístupu spolu s aktivním šifrováním pevných disků pomocí aplikace BitLocker.

A.11.2.7 Bezpečná likvidace nebo opakované použití zařízení

Opatření: Všechny části zařízení obsahující paměťová média musí být prověřeny s cílem zajistit, aby byla před likvidaci nebo opakovaném použití odstraněna nebo bezpečně přepsána všechna citlivá data a licencovaný software.
Vyloučeno: Ano

A.11.2.8 Neobsluhovaná uživatelská zařízení

Opatření: Uživatelé musí zajistit přiměřenou ochranu neobsluhovaného zařízení.
Vyloučeno: Ne
Způsob plnění požadavku: Interní příručka.

A.11.2.9 Zásada prázdného stolu a prázdné obrazovky monitoru

Opatření: Pro vybavení pro zpracování informací musí být přijata zásada prázdného stolu, týkající se papírových dokumentů a vyměnitelných paměťových médií, a zásada prázdné obrazovky.
Vyloučeno: Ne
Způsob plnění požadavku: Zavedení pojízdných kontejnerů s centrálním zámkem do kanceláří vedení společnosti.

A.12 Bezpečnost provozu

A.12.1 Provozní postupy a odpovědnosti

Cíl: Zajistit správné a bezpečné provozování vybavení pro zpracování informací

A.12.1.1 Dokumentace provozních postupů

Opatření: Provozní postupy musí být dokumentovány a být k dispozici všem uživatelům, kteří je potřebují.
Vyloučeno: Ano

A.12.1.2 Řízení změn

Opatření: Změny v organizaci, podnikových procesech, vybavení pro zpracování informací a systémech, které mají vliv na bezpečnost informací musí být řízeny a kontrolovány.
Vyloučeno: Ano

A.12.1.3 Řízení kapacit

Opatření: K zajištění požadováného výkonu systému z pohledu budoucích požadavků na kapacity musí být používání zdrojů monitorováno, optimalizováno a naplánováno.
Vyloučeno: Ano

A.12.1.4 Princip oddělení prostředí vývoje, testování a provozu

Opatření: Vývojová, testovací a provozní prostředí musejí být oddělena, aby se snížila rizika neoprávněného přístupu nebo změny provozního prostředí.
Vyloučeno: Ano

A.12.2 Ochrana 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: Musí být implementována opatření pro detekci, prevenci a zotavení na ochranu před malwarem, v kombinaci s vhodným zvyšováním povědomí uživatelů.
Vyloučeno: Ne
Způsob plnění požadavku: Nasazení Norton Mobile Security a Norton Safe Web. Zálohování dat v pravidelných intervalech a také mimo prostory organizace.

A.12.3 Zálohování

Cíl: Ochrana před ztrátou dat.

A.12.3.1 Zálohování informací

Opatření: Pravidelně musí být pořizovány a testovány záložní kopie informací, softwaru a bitových kopií systému v souladu se schválenou politikou zálohování.

Vyloučeno: Ne
Způsob plnění požadavku: Dokument s politikou definující proces zálohování. Využití zálohy dat v datovém centru mimo prostory organizace.

A.12.4 Zaznamenávání formou logů a monitorování

Cíl: Zaznamenávat události a generovat důkazy.

A.12.4.1 Zaznamenávání událostí formou logů

Opatření: Musí být pořizovány, uchovávány a pravidelně přezkoumávány záznamy událostí formou logů zaznamenávající aktivity uživatelů, výjimky, selhání a události bezpečnosti informací.
Vyloučeno: Ne
Způsob plnění požadavku: Dokument s politikou pro zaznamenávání událostí formou logů.

A.12.4.2 Ochrana logů

Opatření: Vybavení pro zaznamenávání formou logů a informace zaznamenané v logu musí být chráněny proti falšování a neoprávněnému přístupu.
Vyloučeno: Ano

A.12.4.3 Logy o činnosti administrátorů a operátorů

Opatření: Aktivity systémového administrátora a systémového operátora musí být zaznamenávány formou logů a záznamy formou logů musí být chráněny a pravidelně přezkoumávány.
Vyloučeno: Ano

A.12.4.4 Synchronizace hodin

Opatření: Zdroje času všech relevantních systémů zpracování informací v rámci organizace nebo bezpečnostní domény musí být synchronizovány s jediným referenčním zdrojem času.
Vyloučeno: Ano

A.12.5 Řízení a kontrola provozního softwaru

Cíl: Zajištění integrity provozních systémů.

A.12.5.1 Instalace softwaru na provozních systémech

Opatření: Musí být zavedeny postupy pro řízení a kontrolu instalace softwaru na provozních systémech.
Vyloučeno: Ano

A.12.6 Správa a řízení technických zranitelností

Cíl: Zabránit využívání technických zranitelností.

A.12.6.1 Správa a řízení technických zranitelností

Opatření: Musí být včas získány informace o technických zranitelnostech použitých informačních systémů a musí být vyhodnoceno ohrožení organizace takovými zranitelnostmi a musí být přijata přiměřená opatření k řešení souvisejících rizik.
Vyloučeno: Ano

A.12.6.2 Omezení instalace softwaru

Opatření: Musí být stanovena a implementována pravidla řídící instalací softwaru uživateli.
Vyloučeno: Ne
Způsob plnění požadavku: Dokument definující privilegia určitých rolí.

A.12.7 Hlediska auditu informačních systémů

Cíl: Minimalizovat dopad auditních aktivit na provozní systémy.

A.12.7.1 Opatření k auditu informačních systémů

Opatření: Požadavky na audit a činnosti zahrnující ověření provozních systémů musí být pečlivě naplánovány a dohodnuty tak, aby se minimalizovalo narušení procesů činnosti organizace.
Vyloučeno: Ano

A.13 Bezpečnost komunikací

A.13.1 Správa bezpečnostní sítě

Cíl: Zajistit ochranu informací v sítích a podpůrném síťovém vybavení pro zpracování informací.

A.13.1.1 Opatření v sítích

Opatření: Sítě musí být řízeny a kontrolovány pro ochranu informací v systémech a aplikacích,
Vyloučeno: Ano

A.13.1.2 Bezpečnost síťových služeb

Opatření: Ve smlouvách o síťových službách musí být identifikovány a zahrnuty bezpečnostní mechanismy, úrovně služeb a požadavky na správu a řízení všech síťových služeb, a to jak pro služby zajišťované interně, tak pro služby zajišťované pomocí vnějších zdrojů.
Vyloučeno: Ano

A.13.1.3 Princip oddělení v sítích

Opatření: Skupiny informačních služeb, uživatelů a informačních systémů musejí být v sítích odděleny.
Vyloučeno: Ano

A.13.2 Přenos informací

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

A.13.2.1 Politiky a postupy při přenosu informací

Opatření: K ochraně přenosu informací prostřednictvím všech druhů komunikačních zařízení musí být zavedeny formální politiky, postupy, opatření.
Vyloučeno: Ne
Způsob plnění požadavku: Šifrování přiložených příloh vhodným způsobem

A.13.2.2 Dohody o přenosu informací

Opatření: Dohody se musí řešit bezpečný přenos obchodních informací mezi organizací a externími stranami.
Vyloučeno: Ano

A.13.2.3 Elektronické předávání zpráv

Opatření: Informace zahrnuté v elektronicky předávaných zprávách musí být přiměřeně chráněny.
Vyloučeno: Ano

A.13.2.4 Dohody o důvěrnosti nebo mlčenlivosti

Opatření: Musí být identifikovány, pravidelně přezkoumávány a dokumentovány požadavky týkající se dohod o zachování důvěrnosti nebo mlčenlivosti odrážející potřeby organizace pro ochranu informací.
Vyloučeno: Ano

A.14 Akvizice, vývoj a údržba systému

A.14.1 Bezpečnostní požadavky informačních systémů

Cíl: Zajistit, aby se bezpečnost informací stala nedílnou součástí informačních systémů během celého životního cyklu. To zahrnuje také požadavky na informační systémy poskytující služby přes veřejné sítě.
Vyloučeno: Ano

A.14.1.1 Analýza a specifikace požadavků bezpečnosti informací

Opatření:V požadavcích na nové informační systémy nebo ve vylepšeních stávajících informačních systémů musí být zahrnuty požadavky související s bezpečností informací.
Vyloučeno: Ano

A.14.1.2 Zabezpečení aplikačních služeb ve veřejných sítích

Opatření: Informace zahrnuté v aplikačních službách probíhajících přes veřejné sítě musí být chráněny před podvodnou činností, smluvními spory a neoprávněným zpřístupněním a změnou.
Vyloučeno: Ano

A.14.1.3 Ochrana transakcí aplikačních služeb

Opatření: Informace zahrnuté v transakcích aplikačních služeb musí být chráněny, aby se zabránilo nedokončenému přenosu, chybnému směrování, neoprávněnému pozměnění zprávy, neoprávněnému zveřejnění, neoprávněnému duplikování nebo opakovanému zaslání zprávy.
Vyloučeno: Ano

A.14.2 Bezpečnost v procesech vývoje a podpory

Cíl:Zajistit, aby byla v rámci životního cyklu vývoje informačních systémů koncipována a implementována bezpečnost informací.

A.14.2.1 Politika bezpečného vývoje

Opatření:V rámci organizace musí být stanovena a při vývoji uplatněna pravidla pro vývoj softwaru a systémů.
Vyloučeno: Ano

A.14.2.2

Opatření: Změny systémů v rámci životního cyklu vývoje musí být řízeny a kontrolovány pomocí formálních postupů řízení změn.
Vyloučeno: Ano

A.14.2.3 Technické přezkoumání aplikací po změnách provozní platformy

Opatření: Při změnách provozních platforem musí být přezkoumány a otestovány aplikace kritické pro činnost organizace, aby se zajistilo, že změny nemají nepříznivý dopad na provoz nebo bezpečnost organizace.
Vyloučeno: Ano

A.14.2.4 Omezení změn softwarových balíků

Opatření: Modifikace softwarových balíků musí být omezeny na nezbytné změny a všechny změny musí být striktně řízeny.
Vyloučeno: Ano

A.14.2.5 Principy inženýrství bezpečných systémů

Opatření: Musí být ustaveny, zdokumentovány a udržovány principy inženýrství bezpečných systémů a aplikovány na všechny programy implementace informačního systému.
Vyloučeno: Ano

A.14.2.6 Bezpečné vývojové prostředí

Opatření:Organizace musí ustavit a přiměřeně chránit bezpečná vývojová prostředí pro vývoj systémů a integrační programy, které pokrývají celý životní cyklus vývoje systému.
Vyloučeno: Ano

A.14.2.7 Vývoj zajišťovaný externími zdroji

Opatření: Organizace musí monitorovat a dohlížet na vývoj systému zajišťovaného externími zdroji.
Vyloučeno: Ano

A.14.2.8 Testování bezpečnosti systému

Opatření: Testování funkčnosti bezpečnosti musí být uskutečněno během vývoje.
Vyloučeno: Ano

A.14.2.9 Testování akceptace systému

Opatření: Pro nové informační systémy, aktualizace a nové verze musí být ustaveny programy pro akceptační testy a související kritéria.
Vyloučeno: Ano

A.14.3 Data pro testování

Cíl: Zajistit ochranu dat použitých pro testování.

A.14.3.1 Ochrana dat pro testování

Opatření: Data pro testování musí být pečlivě vybrána, chráněna a kontrolována.
Vyloučeno: Ano

A.15 Vztahy s dodavateli

A.15.1 Bezpečnost informací ve vztazích s dodavateli

Cíl: Zajistit ochranu těch aktiv organizace, která jsou přístupná dodavatelům.

A.15.1.1 Politika bezpečnosti informací pro oblast vztahů s dodavateli

Opatření: Požadavky v oblasti bezpečnosti informací na zmírnění rizik spojených s přístupem dodavatele k aktivům organizace musí být s dodavatelem dohodnuty a zdokumentovány.
Vyloučeno: Ano

A.15.1.2 Řešení bezpečnosti v rámci smluv s dodavateli

Opatření: Musí být stanoveny všechny podstatné požadavky na bezpečnost informací a odsouhlaseny s každým dodavatelem, který může k informacím organizace přistupovat, zpracovávat je, ukládat, přenášet je nebo pro ně poskytovat komponenty IT infrastruktury.
Vyloučeno: Ano

A.15.1.3 Řetězec dodavatelů informačních a komunikačních technologií

Opatření: Smlouvy s dodavateli musí zahrnovat požadavky na řešení rizik v oblasti bezpečnosti informací souvisejících se službami informačních a komunikačních technologií a produkty řetězce dodavatelů.
Vyloučeno: Ano

A.15.2 Řízení dodávky služeb dodavatelem

Cíl: Udržovat dohodnuté úrovně bezpečnosti informací a dodávky služeb v souladu s dodavatelskými smlouvami.

A.15.2.1 Monitorování a přezkoumávání služeb dodavatelů

Opatření: Organizace musí pravidelně monitorovat, přezkoumávat a provádět audit dodávky služeb dodavateli.
Vyloučeno: Ano

A.15.2.2 Řízení změn služeb dodavatelů

Opatření: Změny v poskytování služeb ze strany dodavatelů, včetně udržování a zlepšování stávajících politik bezpečnosti informací, postupů a opatření musí být řízeny, s ohledem na kritičnost souvisejících informací, systémů a procesů, a opětovné posuzování rizik.
Vyloučeno: Ano

A.16 Řízení incidentů bezpečnosti informací

A.16.1 Řízení incidentů bezpečnosti informací a zlepšování

Cíl: Zajistit důsledný a efektivní přístup k řízení incidentů bezpečnosti informací, včetně komunikace ohledně bezpečnostních událostí a slabých míst.

A.16.1.1 Odpovědnosti a postupy

Opatření: Musí být ustanoveny odpovědnosti a postupy managementu s cílem zajistit rychlou, efektivní a řádnou odezvu na incidenty bezpečnosti informací.
Vyloučeno: Ano

A.16.1.2 Podávání zpráv o událostech bezpečnosti informací

Opatření: Události bezpečnosti informací musí být co nejrychleji oznámeny prostřednictvím příslušných řídících kanálů.
Vyloučeno: Ano

A.16.1.3 Podávání zpráv o slabých místech bezpečnosti informací

Opatření: Zaměstnanci a smluvní strany používající informační systémy a služby organizace musí být povinni upozornit a oznámit veškerá zpozorovaná nebo domnělá slabá místa bezpečnosti informací systémů nebo služeb.
Vyloučeno: Ano

A.16.1.4 Posuzování a rozhodování o událostech bezpečnosti informací

Opatření: Události bezpečnosti informací musí být posouzeny a musí být rozhodnuto, zda mají být klasifikovány jako incidenty bezpečnosti informací.
Vyloučeno: Ano

A.16.1.5 Odezva na incidenty bezpečnosti informací

Opatření: Na incidenty bezpečnosti informací musí být reagováno v souladu s dokumentovanými postupy.
Vyloučeno: Ano

A.16.1.6 Ponaučení z incidentů bezpečnosti informací

Opatření: Znalosti získané z analýzy a řešení incidentů bezpečnosti informací musí být použity ke snížení pravděpodobnosti nebo dopadu budoucích incidentů.
Vyloučeno: Ano

A.16.1.7 Shromažďování důkazů

Opatření: Organizace musí definovat a aplikovat postupy pro identifikaci, shromažďování, získávání a uchovávání informací, které mohou sloužit jako důkaz.
Vyloučeno: Ano

A.17 Aspekty řízení kontinuity činnosti organizace z hlediska bezpečnosti informací

A.17.1 Kontinuita bezpečnosti informací

Cíl: Kontinuita bezpečnosti informací musí být začleněná do systému řízení kontinuity činností organizace.

A.17.1.1 Plánování kontinuity bezpečnosti informací

Opatření: Organizace musí stanovit své požadavky na bezpečnost informací a kontinuitu řízení bezpečnosti informací v nepříznivých situací, například během krize nebo katastrofy.
Vyloučeno: Ano

A.17.1.2 Implementace kontinuity bezpečnosti informací

Opatření: Organizace musí ustavit, dokumentovat, zavést a udržovat procesy, postupy a opatření k zajištění požadované úrovně kontinuity bezpečnosti informací během nepříznivé situace.
Vyloučeno: Ano

A.17.1.3 Verifikace, přezkoumání a vyhodnocení kontinuity bezpečnosti informací

Opatření: Organizace musí ověřovat ustavená a zavedená opatření kontinuity bezpečnosti informací v pravidelných intervalech, aby se zajistilo, že jsou během nepříznivých situací platná a efektivní.
Vyloučeno: Ano

A.17.2 Redundance

Cíl:Zajistit dostupnost vybavení pro zpracování informací.

A.17.2.1 Dostupnost vybavení pro zpracování informací

Opatření: Vybavení pro zpracování informací musí být zaváděno s dostatečnou redundancí, aby byly splněny požadavky dostupnosti.
Vyloučeno: Ano

A.18 Soulad s požadavky

A.18.1 Soulad se zákonnými a smluvními požadavky

Cíl: Zamezit porušení právních, zákonných, předpisových nebo smluvních povinností souvisejících s bezpečností informací a jakýchkoliv požadavků bezpečnosti.

A.18.1.1 Identifikace příslušné legislativy a smluvních požadavků

Opatření: Všechny zákonné, předpisové, smluvní požadavky příslušné legislativy a přístup organizace ke splnění těchto požadavků musí být explicitně identifikovány, dokumentovány a udržovány v aktuálním stavu pro každý informační systém a organizaci.
Vyloučeno: Ano

A.18.1.2 Práva k duševnímu vlastnictví

Opatření: Pro zajištění souladu s legislativními, předpisovými a smluvními požadavky týkající se práv duševního vlastnictví a používání proprietárních softwarových produktů musí být implementována vhodná opatření.
Vyloučeno: Ano

A.18.1.3 Ochrana záznamů

Opatření: Záznamy musí být chráněny před ztrátou, zničením, falšováním, neoprávněným přístupem a neoprávněným vydáním v souladu s legislativními, předpisovými, smluvními požadavky a požadavky týkajícími se činnosti organizace.
Vyloučeno: Ano

A.18.1.4 Soukromí a ochrana osobních údajů

Opatření: Soukromí a ochrana osobních údajů musí být zajištěna v souladu s požadavky příslušné legislativy a nařízení tam, kde lze požadavky uplatnit.
Vyloučeno: Ano

A.18.1.5 Regulace kryptografických opatření

Opatření: Kryptografická opatření musí být používána v souladu se všemi příslušnými dohodami, legislativou a předpisy.
Vyloučeno: Ano

A.18.2 Přezkoumání bezpečnosti informací

Cíl: Zajistit, že bezpečnost informací je implementována a provozována v souladu s politikami a postupy organizace.

A.18.2.1 Nezávislé přezkoumání bezpečnosti informací

Opatření: Přístup organizace k řízení bezpečnosti informací a její implementaci (tj. cíle opatření, politiky ,procesy a postupy pro bezpečnost informací) musí být nezávisle přezkoumán v naplánovaných intervalech, nebo když dojde k významným změnám.
Vyloučeno: Ano

A.18.2.2 Soulad s bezpečnostními politikami a normami

Opatření: Vedoucí pracovníci musí pravidelně přezkoumávat soulad zpracování informací a postupy v rámci své působnosti s příslušnými bezpečnostními politikami, normami a jakýmikoliv dalšími požadavky na bezpečnost.
Vyloučeno: Ano

A.18.2.3 Přezkoumání technického souladu

Opatření:Informační systémy musí být pravidelně přezkoumávány z hlediska souladu s politikami a normami bezpečnosti informací organizace.
Vyloučeno: Ano