Univerzita Pardubice

Fakulta ekonomicko-správní

Bezpečnostní politika organizace

Zuzana Scheuflerová

Bakalářská práce
2017

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2016/2017**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Zuzana Scheuflerová**
Osobní číslo:	**E13113**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Název tématu:	**Bezpečnostní politika organizace**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování:

Cílem práce bude zmapování současného stavu bezpečnostní politiky vybrané organizace. V případě identifikace problémů návrh na jejich odstranění.
Osnova:
- Teoretický úvod k bezpečnostní politice.
- Popis organizace a popis současného stavu bezpečnostní politiky.
- Zjištění nedostatků, identifikace problémů.
- Návrh zabezpečení.

Rozsah grafických prací:

Rozsah pracovní zprávy: **cca 35 stran**

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

Seznam odborné literatury:

BASL, Josef a Roman BLAŽÍČEK. Podnikové informační systémy: podnik v informační společnosti. 3., aktualiz. a dopl. vyd. Praha: Grada, 2012, 323 s. Management v informační společnosti. ISBN 978-80-247-4307-3.
BRUCKNER, Tomáš. Tvorba informačních systémů: principy, metodiky, architektury. 1. vyd. Praha: Grada, 2012, 357 s. Management v informační společnosti. ISBN 978-80-247-4153-6.
SODOMKA Petr a Hana KLČOVÁ. Informační systémy v podnikové praxi. 2. aktualiz. a rozš. vyd. Brno: Computer Press, 2010. ISBN 978-80-251-2878-7.
TVRDÍKOVÁ, Milena. Aplikace moderních informačních technologií v řízení firmy. 1. vyd. Praha: Grada, 2008. ISBN 978-80-247-2728-8

Vedoucí bakalářské práce: **Ing. Renáta Máchová, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **4. září 2016**

Termín odevzdání bakalářské práce: **28. dubna 2017**

doc. Ing. Romana Provazníková, Ph.D.
děkanka

L.S.

doc. Ing. Pavel Petr, Ph.D.
vedoucí ústavu

V Pardubicích dne 4. září 2016

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracoval/a samostatně. Veškeré literární prameny a informace, které jsem v práci využil/a, jsou uvedeny v seznamu použité literatury.

Byl/a jsem seznámen/a s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako Školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 9/2012, bude práce zveřejněna v Univerzitní knihovně a prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 28. 4. 2017 Zuzana Scheuflerová

PODĚKOVÁNÍ:

Tímto bych ráda poděkovala svému vedoucímu práce Ing. Renátě Máchové za její odbornou pomoc, cenné rady a poskytnuté materiály, které mi pomohly při zpracování bakalářské práce.

ANOTACE

Tato práce se zabývá zabezpečením informací v organizaci. Je představena problematika ochrany informací v širších souvislostech a nastíněny návrhy na zlepšení informační bezpečnosti při činnostech spojených se zpracováním a uchováváním informací v organizaci. V práci jsou identifikovány hrozby a zranitelnosti informací v konkrétní organizaci a popsány hlavní prvky ochrany informací. Rozsah práce koresponduje s obsahem studia.

KLÍČOVÁ SLOVA

Informační bezpečnost, bezpečnostní politika, ochrana informací, analýza rizik, hrozby, rizika

TITLE

Safety politics of organization

ANNOTATION

This work is concerning safety of organization's information. Problematics of information security in a wider context are introduced. There are outlined examples for improvement of informational safety associated with processing of information in the organization. In this work threats and vulnerabilities of information of concrete organization are identified, and main elements of information security are described. Scope of work corresponds with content of study plan.

KEYWORDS

Informational safety, Safety politics, Information security, Risk analysis, Threats, Risks

OBSAH

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

ZKRATKY

ADSL	Asymetric Digital Subscriber Line
BP	Bezpečnostní politika
CIA	důvěrnost, integrita a dostupnost (z angl.. confidentality, integrity, availability)
ČSN	Česká státní norma
ICT	Informační a komunikační technologie
IS	Informační systém
IT	Informační technologie
Mbit	Megabit
UPS	Uninterruptible Power Supply

Úvod

Vzhledem k neustálému rozvoji informačních a komunikačních technologií, je problematika ochrany informací v současné době velmi důležitou oblastí. Dochází k nárůstu citlivých dat, která mohou být terčem útoků různých podob, čímž se zvyšují rizika informační bezpečnosti. Využívání nových technologií pro zpracování informací, s sebou tedy přináší i vysoké nároky na jejich zabezpečení.

V současné době tvoří využívání informačních a komunikačních technologií nezbytnou součást efektivního provozu organizací. Technologie a systémy pro zpracování informací obsahují takřka veškeré informace organizace a jakékoliv ohrožení těchto systémů má nepříznivé dopady. Proto by měla každá organizace, bez ohledu na její velikost a předmět podnikání dodržovat určitá bezpečnostní pravidla, která vedou k zajištění ochrany informací. Tato pravidla jsou formulována v bezpečnostní politice organizace, která je chápána jako základní dokument celkového zabezpečení organizace obsahující všechny principy, zásady, omezení, pravidla a postupy, podle kterých jsou v dané organizaci řízena, chráněna a distribuována veškerá aktiva.

Cílem této bakalářské práce je představit problematiku bezpečnosti informací v souvislosti s bezpečnostní politikou a následně tyto teoretické poznatky využít v praxi. Před samotným vypracováním plánu zabezpečení informací v organizaci, tedy bezpečnostní politiky, bude prováděno zmapování současného stavu informační bezpečnosti v konkrétní organizaci, kdy budou zjištěny případné nedostatky a problémy, které bude sloužit jako podklad pro vytvoření návrhu na jejich odstranění.

1 TEORETICKÝ ÚVOD K BEZPEČNOSTNÍ POLITICE

Dříve, než bude rozvinuta problematika bezpečnostní politiky v organizaci, jsou v této úvodní kapitole definovány základní pojmy, které souvisí s tématem bezpečnosti organizace a některé z pojmů se v bakalářské práci často objevují.

Základní pojmy

Informace je název pro abstrakci a zobecnění toho, co přijímají naše smysly, co se sděluje jiným lidem a s čím se naučili pracovat i umělé objekty (výpočetní systémy, komunikační systémy,…). Informace může putovat odněkud někam, tzn. od odesílatele k příjemci, může být někde uložena nebo nějakým způsobem zpracovávána, aby ji mohl člověk, živočich či zařízení přijmout a využít. Jsou to tedy např. přijímané a posílané texty, obrázky, zvuky; znalosti o konkrétní situaci; znalost získaná ze studia, zkušeností; obecné přesvědčení atd. [6]

Data jsou nositelem informace. Představují údaje ve formě zpracovatelné informačními technologiemi. [2][6]

Aktivum je veškerý majetek organizace, tedy vše co má pro majitele nějakou hodnotu. Za nejcennější aktiva se považují data a informace, jejichž ztráta, zneužití či modifikace by organizaci způsobily škodu. Aktiva se dělí na hmotná a nehmotná. Hmotná aktiva tvoří především technické prostředky výpočetní techniky (počítač, server, kabelové rozvody, tiskárny, modemy a ostatní technická zařízení). Hodnota hmotných aktiv se dá přesně stanovit, v závislosti na jejich pořizovací ceně. Nehmotná aktiva představují [9][14]:

- **pracovní postupy** využívané v organizaci v oblasti IS/ICT,
- organizací vytvořené nebo převzaté **datové soubory**, které jsou důležité pro její provoz,
- **základní programové vybavení**, kam patří operační systémy, programové vybavení potřebné pro provoz počítačových sítí, nástroje pro správu a řízení informačního systému apod. a **aplikační programové vybavení** např. textové editory, grafické programy, tabulkové kalkulátory atd.,
- základní **služby** (zajištění provozu světlem, topením, klimatizací) a počítačové a komunikační služby.

Informační systém (IS) je soubor vybavení, který organizace využívá ke správě svých informací, potřebných k plánování, rozhodování a řízení. Tvoří ho[1][4][13][15][20]:

- hardware (procesor, paměti,…),
- software (programy, operační systémy,…),
- data (data uložená v databázi),
- lidé (personál, uživatelé).

Informační technologie (IT) je technika, která slouží ke zpracování informací a dat. Jde o výpočetní a komunikační techniku a její programové vybavení. [14]

Hrozba je skutečnost, díky které může dojít k poškození, zničení, ke ztrátě důvěry nebo hodnoty aktiva. Je to tedy jakékoliv nebezpečí, známé, reálné nebo potenciální, které ohrožuje informační systém nebo data v něm obsažena. Hrozby se dělí na [9][10][16]:

- objektivní:
  - přírodní, fyzické (povodeň, požár, výpadek proudu,…),
  - fyzikální (elektromagnetické vyzařování,…),
  - technické, logické (porucha paměti, krádež nebo zničení paměťového média nebo zrušení informace na něm),
- subjektivní – zdrojem hrozby lidský faktor:
  - neúmyslné (práce neškoleného uživatele, správce,…),
  - úmyslné – jedná se o hrozby, které byly naplánovány, kde je příčinou vnější útočník (teroristé, hackeři, konkurenti,…) nebo vnitřní útočník (současný či bývalý zaměstnanec). Odhaduje se, že 80% útoků, je vedeno zevnitř organizace.

Dále se hrozby dělí podle dopadu na systém na aktivní (dochází ke změně stavu systému na základě narušení integrity a dostupnosti) a pasivní (dochází k úniku informací) hrozby. [9][10][16]

Riziko je pravděpodobnost, s jakou bude dané aktivum poškozeno či zničeno působením konkrétní hrozby. [14]

Zranitelnost je nedostatek nebo slabina bezpečnostního systému, která může být zneužita hrozbou tak, že dojde k poškození nebo zničení aktiv. Jinak řečeno jsou to prvky,

které existují v každém informačním systému a jsou využitelná pro útočníka k útoku na data či celý systém. Mohou to být slabiny softwaru, ale i lidské chyby, neznalost či podcenění bezpečnosti. [14]

Útok je buď úmyslné využití zranitelného místa ke způsobení škod nebo ztrát na informačním systému, nebo neúmyslné vykonání akce, jejímž výsledkem je škoda na aktivech. [12]

Útočník je osoba, která se snaží o nepovolený průnik do informačního systému. Využije tedy úmyslně či neúmyslně zranitelné místo informačního systému a provede útok (krádež, zneužití, či poškození dat nebo celého systému). Podle znalosti a vybavenosti se rozeznávají tři typy útočníků [14][12]:

- útočníci slabé síly,
- útočníci střední síly,
- útočníci velké síly.

Bezpečnost představuje vlastnost objektu nebo subjektu, tedy informačního systému nebo informační technologie, která určuje míru jeho ochrany proti možným hrozbám. [14]

1.1 Informační bezpečnost

Informační bezpečnost se zabývá ochranou informací ve všech jejich formách a po celý jejich cyklus (vznik, zpracování, ukládání, přenos, likvidace). Pro bezpečnost informací je třeba zachování bezpečnostních funkcí, tj. důvěrnost, integrita a dostupnost informací. Tyto požadavky na bezpečné informace jsou také nazývány jako trojice CIA z angl. confidentality, integrity, availability. [3][9][12]

Důvěrnost informací

Důvěrnost informace je zajištění, že informace jsou přístupné pouze těm, kteří jsou k tomu oprávněni. Bývá zabezpečena pomocí autentizace, šifrování, klasifikace dat, školení zaměstnanců, atd. Narušením bezpečnosti informací je např. zneužití hesla pro přihlášení k cizí e-mailové schránce. [3][9][13]

Dostupnost informací

Dostupnost informací je opatření, aby informace byly dostupné oprávněným uživatelům v okamžiku její potřeby. Dostupnost bývá zajišťována zálohováním, duplicitní datovou sítí,

volbou vhodné infrastruktury, atd. Příkladem narušení dostupnosti informací je selhání datové sítě nebo serveru. [3][9][13]

Integrita informací

Integrita informací je požadavek na správnost a úplnost informací. Nežádoucí modifikací dat proto v informační bezpečnosti lze rozumět narušení jejich integrity. Integrita může být porušena jak úmyslným pozměněním (útočník změní číslo účtu v bankovní transakci), tak náhodným pozměněním (chyba v přenosu dat, porucha pevného disku). Integrita bývá zajišťována kontrolními součty, žurnálováním, samoopravnými kódy, atd. [3][9][13]

Bezpečnostní mechanismy

K dosažení cílů bezpečnosti informací, tzn. dosažení již zmíněných požadavků na informační bezpečnost, důvěrnost, dostupnost a integritu informací, jsou používány bezpečností mechanismy, které mohou být [12]:

- fyzického charakteru,
- logického charakteru,
- technického charakteru,
- administrativního charakteru.

Bezpečnostní mechanismy **fyzického charakteru** jsou např. trezory, zámky, protipožární ochrana, záložní generátory energie, chráněná místa pro záložní kopie dat a programů, ochranka, jmenovky atd. Bezpečnostní mechanismy **logického charakteru** (softwarového charakteru) jsou např. digitální podepisování, antivirové prostředky, ochranné nástroje v operačních systémech, ochranné nástroje v aplikačních programech, softwarové řízení přístupu apod. Autentizace na bázi identifikačních karet, autentizací kalkulátory, firewally, záložní kopie dat a programů jsou příkladem bezpečnostního mechanismu **technického charakteru** (hardwarového charakteru). Posledním bezpečnostním mechanismem jsou mechanismy **administrativního charakteru**, kterými jsou např. výběr a školení důvěryhodných osob, hesla, autorizační postupy, právní normy, zákony, vyhlášky, předpisy, etické normy, přijímací a výpovědní postupy, licenční politika, konfigurace systému atd. [12]

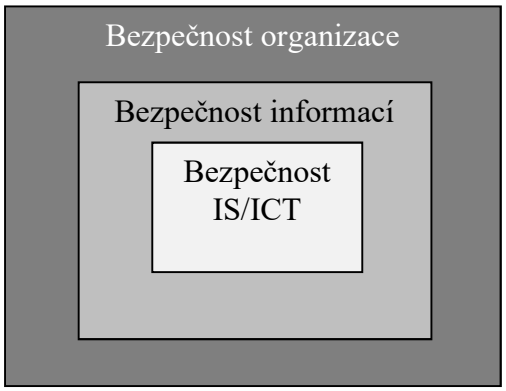
1.2 Řízení bezpečnosti informací

V souvislosti s pojmem bezpečnost informací, je třeba zmínit se o dalších dvou termínech a to bezpečnost organizace a bezpečnost IS/ICT. [9][21]

Nejvyšší kategorií je **bezpečnost organizace**, jejíž součástí je zajištění bezpečnosti objektů, majetku organizace, jako je kontrola přístupů do objektů, strážní služba atd. Některé z těchto činností napomáhají zároveň i k zajištění bezpečnosti IS/ICT (např. kontrola oprávnění fyzického přístupu do budov). [9][21]

Součástí bezpečnosti organizace je i **bezpečnost informací**. Cílem a úkolem řízení bezpečnosti informací je definovat zásady bezpečné práce s informacemi všeho druhu a všech typů, tedy nejen s informacemi v digitální formě. Bezpečnost informací zahrnuje navíc proti bezpečnosti IS/ICT např. způsob zpracování dat, jejich uložení a správy archivu nedigitálních dat, nakládání s informacemi během jejich přenášení na jiná místa, zásady skartace materiálů, zásady pro poskytování informací apod. [9][21]

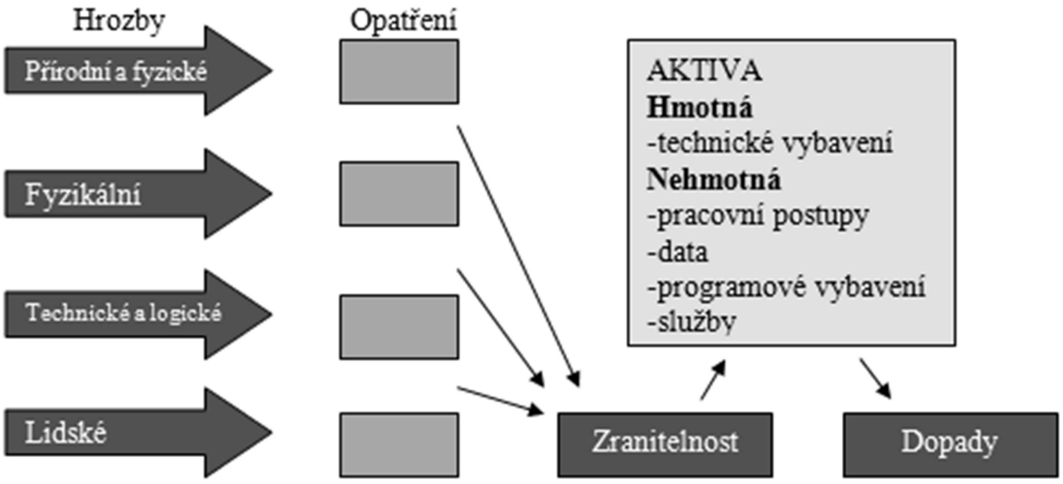
Bezpečnost IS/ICT je relativně nejužší oblastí řízení bezpečnosti, protože má za úkol chránit „pouze“ ta aktiva, která jsou součástí informačního systému organizace podporovaného informačními a komunikačními technologiemi. I přesto je ale sama o sobě komplikovaným problémem. Pracuje totiž s „neviditelnými“ daty, informacemi a službami, což některým lidem připadá pouze jako hra se symboly a ne jako práce se skutečnými hodnotami. Hodnotu pro organizaci nepředstavuje samotné viditelné médium, ale data na něm nahraná. Jde např. o pravidla pro zadávání a správu přístupových hesel k aplikacím a datům, pravidla provozu informačního systému organizace, pravidla pro kryptování dat apod. Vzájemné vztahy těchto tří pojmů znázorňuje následující Obrázek 1. [9][21]



Obrázek 1: Vztah úrovní bezpečnosti

Zdroj: upraveno podle [9][21]

Následující Obrázek 2 zobrazuje vztahy mezi aktivy organizace a hrozbami, které na ně mohou prostřednictvím zranitelnosti potenciálně působit, možnosti ochrany aktiv organizace formou opatření a dopady reálných hrozeb na tato aktiva. [9]



Obrázek 2: Schéma zajištění bezpečnosti IS/ICT ve firmě – aktiva, hrozby

Zdroj: [9]

Formalizace řízení bezpečnosti informací slouží ke snížení pravděpodobnosti bezpečnostního selhání a vytváří hierarchickou strukturu dokumentů, která obsahuje jednotlivé plány řízení bezpečnosti [12]:

- bezpečnostní politiky,
- bezpečnostní standardy,
- bezpečnostní normy,
- bezpečnostní postupy,
- bezpečnostní procedury.

Není vhodné je tvořit jako jeden dokument, ale jako separované dokumenty, jejichž výhodou je, že uživatelé nemusí znát všechny politiky, standardy, normy, postupy, procedury a v případě změny, se mění pouze příslušný dokument. [12]

Bezpečnostní politiky

Bezpečnostní politika je jedním ze základních pilířů, na kterém stojí systém řízení bezpečnosti informací. Pokud nejsou jednoznačně definovány základní parametry, může být celý systém budován neefektivně a neúčelně. Jde o strategický plán implementace bezpečnosti v organizaci. Tento plán řízení bezpečnosti je podrobněji popsán dále. [7][12][18]

Bezpečnostní standardy

Bezpečnostní standardy vymezují povinné požadavky na jednotné užití hardwaru, softwaru, technologií a bezpečnostní kontrolu. Poskytují průběh činností, kterými jsou procedury a technologie jednotně uskutečňovány uvnitř organizace. Bezpečnostní standardy představují taktické dokumenty, které definují postupy nebo metody, díky kterým bude dosaženo cílů a pokynů vymezených v bezpečnostních politikách. [7][12]

Bezpečnostní normy

Bezpečnostní normy určují minimální míru bezpečnosti, které musí daný informační systém v rámci organizace dosáhnout. Informační systémy, které nesplňují tuto minimální úroveň bezpečnosti, nesmí být v rámci organizace použity. [7][12]

Bezpečnostní postupy

Bezpečnostní postupy obsahují pokyny, jak bezpečnostní standardy a bezpečnostní normy implementovat a zajišťovat. Jsou to operativní průvodci určené pro bezpečnostní specialisty, ale i pro koncové uživatele. Bezpečnostní postupy jsou přizpůsobeny každému informačnímu systému a podmínkám. Definují, jaké bezpečnostní mechanismy mají být použity, avšak neurčují konkrétní produkt, výrobce, nebo detailní nastavení. [7][12]

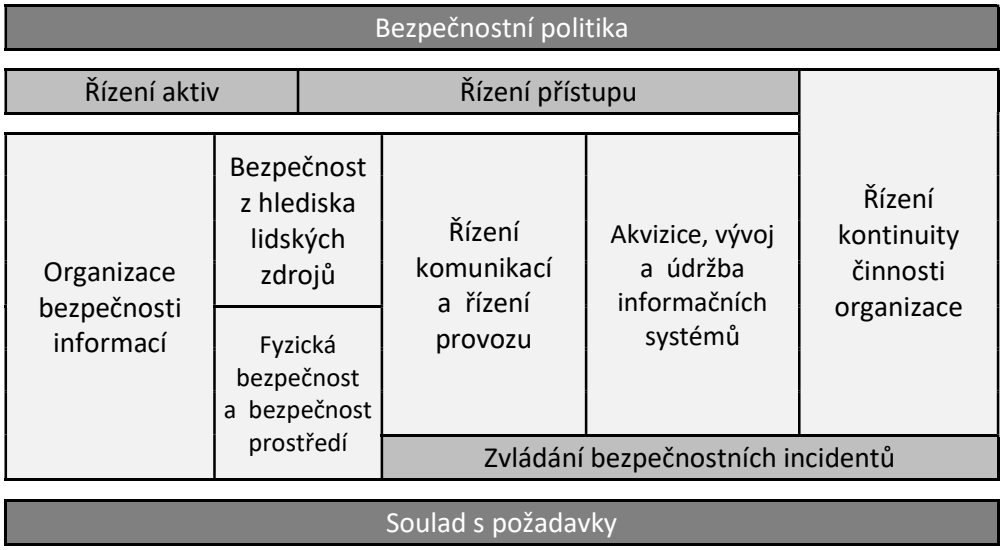
Bezpečnostní procedury

Bezpečnostní procedury jsou detailní návody popisující konkrétní akce, důležité pro implementaci bezpečnostních mechanizmů, bezpečnostních kontrol apod. Mohou být zaměřeny na celý systém nebo na jeden konkrétní produkt, jako je např. implementace a provoz firewallu, definice postupu aktualizace konkrétního antivirového programu. Bezpečnostní procedury musí být aktualizovány při aktualizaci hardwaru nebo softwaru. [7][12]

1.2.1 Oblasti bezpečnosti informací

Řízení bezpečnosti v organizaci se zabývá několika oblastmi, jak zobrazuje následující Tabulka 1. [9]

Tabulka 1: Oblasti bezpečnosti informací



Zdroj: [9]

Jednotlivé části obsahují [9]:

- **Bezpečnostní politika** – stanovení základních pravidel informační bezpečnosti a vyjádření podpory vedení organizace.
- **Řízení aktiv** – přehled o aktivech organizace a zajištění odpovědnosti za ochranu jednotlivých aktiv.
- **Řízení přístupu** – pravidla pro získávání přístupu ke všem informačním a komunikačním systémům a zároveň sledování využívání dostupných prostředků.
- **Organizace bezpečnosti informací** – stanovení organizačních struktur, které bezpečnost v organizaci řídí a prosazují.
- **Bezpečnost z hlediska lidských zdrojů** – definování povinností pracovníků vztahující se k ochraně informací.
- **Fyzická bezpečnost a bezpečnost prostředí** – vymezení pravidel pro přístup osob do určitých prostor organizace a ochrana zařízení ICT.
- **Řízení komunikací a řízení provozu** – zavedení opatření související se spolehlivým a bezpečným chodem produkčních informačních a komunikačních systémů organizace,

- **Akvizice, vývoj a údržba informačních systémů** – zavedení principů informační bezpečnosti do projektů rozvoje ICT a dalších podpůrných aktivit,
- **Řízení kontinuity činností organizace** – postupy prevence a minimalizace škod pro organizaci plynoucích z mimořádných událostí (havárie, živelné pohromy).
- **Zvládání bezpečnostních incidentů** – pravidla pro řešení bezpečnostních incidentů včetně shromažďování potřebných důkazů.
- **Soulad s požadavky** – organizace se zavazuje k naplnění požadavků vyplývajících z právních, smluvních a jiných závazků.

1.2.2 Legislativa – zákony, normy a ostatní právní předpisy

Při zpracování bezpečnostní politiky je nutno mít na zřeteli vždy nejen požadavky vyplývající z analýzy rizik, ale také požadavky a povinnosti vyplývající z legislativních úprav ve státě. Vzhledem k tomu, že oblast bezpečnosti informací je velice široká a úzce souvisí s ochranou hmotného majetku, života a zdraví zaměstnanců a další problematikou, jsou v této kapitole uvedeny pouze vybrané základní legislativní a jiné předpisy. [9][9]

1.2.2.1 Zákony

Zákon č. 499/2004 Sb. o archivnictví a spisové službě a o změně některých zákonů v platném znění.

Zákon č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů (krizový zákon) v platném znění.

Zákon č. 106/1999 Sb. o svobodném přístupu k informacím v platném znění.

Zákon č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti v platném znění.

Zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů v platném znění.

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů v platném znění (zákon o elektronických komunikacích).

Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů v platném znění (zákon o elektronickém podpisu).

Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně dalších zákonů v platném znění.

1.2.2.2 Normy

Norma ČSN ISO/IEC 17799 - Informační technologie – Soubor postupů pro řízení informační bezpečnosti.

Norma ČSN BS 7799-2 - Systém managementu bezpečnosti informací - Specifikace s návodem pro použití.

Norma ČSN ISO/IEC 15408 - Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT.

Norma ČSN ISO/IEC TR 13335-1 - Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 1: Pojetí a modely bezpečnosti IT.

Norma ČSN ISO/IEC TR 13335-2 - Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 2: Řízení a plánování bezpečnosti IT.

Norma ČSN ISO/IEC TR 13335-3 - Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 3: Techniky pro řízení bezpečnosti IT.

Norma ČSN ISO/IEC TR 13335-4 - Informační technologie - Směrnice pro řízení bezpečnosti IT - Část 4: Výběr ochranných opatření.

Norma ČSN ISO/IEC 15816 - Informační technologie - Bezpečnostní techniky - Bezpečnostní informační objekty pro řízení přístupu.

Norma ČSN ISO/IEC 10181 - Informační technologie - Propojení otevřených systémů - Bezpečnostní struktury otevřených systémů

1.2.2.3 Ostatní právní předpisy (v rámci EU)

Směrnice 1997/66/ES o ochraně dat v telekomunikacích.

Směrnice 1995/46/ES o ochraně osobních dat.

Směrnice 2002/58/ES o soukromí v elektronické komunikaci.

Směrnice 1999/93/ES o zásadách Společenství pro elektronické podpisy.

Směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí.

Nařízení 2001/45/ES o ochraně fyzických osob při zpracování osobních údajů orgány a institucemi.

Směrnice rady 1991/250/EHS o právní ochraně počítačových programů.

Směrnice rady 2001/264/EC o ochraně utajovaných informacích.

2 BEZPEČNOSTNÍ POLITIKA

Každá společnost, bez ohledu na její velikost a předmět podnikání musí dodržovat bezpečnostní pravidla, která jsou nejčastěji formulována v bezpečnostní politice organizace. Bezpečnostní politika (BP) je chápána jako základní dokument celkového zabezpečení organizace obsahující všechny principy, zásady, omezení, pravidla a postupy, podle kterých jsou v dané organizaci řízena, chráněna a distribuována veškerá aktiva firmy. [5][7][10][16][19]

Hlavní zásadou je chránit interní sítě a veškerá data nejen zvenku, ale i zevnitř. Bezpečnostní politikou je třeba chápat nejen základní dokument řídící dokumentace v oblasti bezpečnosti v organizaci, ale také veškerou navazující bezpečnostní dokumentaci. Obsahuje souhrn bezpečnostních požadavků pro řešení informační bezpečnosti na úrovni fyzické, personální, administrativní, počítačové a komunikační bezpečnosti a bezpečnosti vývojového prostředí. Bezpečnostní politika je užitečná tehdy, když je jejím přínosem snížení rizik, ovšem v rovnováze k nákladům na návrh, implementaci a správu bezpečnostní politiky. Stručně řečeno bezpečnostní politika definuje, co je třeba chránit, proti čemu a jakým způsobem. [5][9][16][17]

V případě rozsáhle organizace, se bezpečnostní politika netvoří jako jeden dokument, ale jako skupina hierarchicky uspořádaných dokumentů [12]:

- Celková bezpečnostní politika organizace,
- Celková bezpečnostní politika informačních technologií organizace,
- Systémové bezpečnostní politiky.

2.1 Proces tvorby bezpečnostní politiky

Při tvorbě bezpečnostní politiky se lze držet následujících kroků [12]:

1. Posouzení vstupních vlivů,
2. Analýza rizik,
3. Vypracování bezpečnostní politiky,
4. Implementace bezpečnostní politiky,
5. Nasazení bezpečnostní politiky, kontrola její účinnosti a vyslovování závěrů.

2.1.1 Posouzení vstupních vlivů

V prvním kroku procesu tvorby bezpečnostní politiky nejprve dochází k rozhodnutí managementu zabývat se bezpečnostní politikou. Jedná se o určení zásadních cílů, strategií a politik pro informační zabezpečení organizace, požadavků na informační bezpečnost podniku, pravomoci a odpovědnosti. Vychází z aktuálního stavu organizace a definuje klíčové problémové oblasti, které je nutno řešit. [14][23][23]

2.1.2 Analýza rizik

Pro správné vyhodnocení rizik spojených s ochranou informací je nutné pojmenování hrozeb, kterým jsou informace vystaveny a jejich bližší specifikace. Cílem analýzy rizik je tedy rizika identifikovat a kvantifikovat tak, aby bylo možné rozhodnout o jejich přijatelnosti pro organizaci. [12][16][19]

Způsoby provádění analýzy rizik [11][12][16][19]:

- **základní analýza rizik** – opatření jsou vytvořena na základě analogie podobných systémů a z všeobecných norem. Nevyužívá tedy žádné výpočty. Tento způsob analýzy je využíván v případě potřeby rychlého zavedení bezpečnostního opatření spolu s nízkými finančními náklady, je totiž časově i finančně nenáročná. Na jejím základě ale mohou být zvolena zbytečně drahá a silná, nebo naopak nedostatečně silná opatření. Navrhovaná bezpečnostní opatření tedy nemusejí přesně odpovídat daným rizikům. Může být vhodným řešením pro organizace s menší závislostí na IS a nižší požadovanou úrovní informační bezpečnosti.
- **neformální analýza rizik** (kvalitativní analýza) – analýza je provedena na základě znalostí odborníků na bezpečnost bez použití standardních metod. Je vhodná zejména pro malé organizace. Výhodou je finanční a časová nenáročnost. Stejně jako v přechozí metodě, je pro ni typické rychlé provedení, avšak hrozí vyšší pravděpodobnost opomenutí některých rizik a snadné ovlivnění voleb nedoloženými subjektivními názory řešitelů.
- **detailní analýza rizik** (kvantitativní analýza) - – je prováděna na základně formálních standardních metod ve všech jejich fázích. Na rozdíl od předchozí metody je zaručena malá pravděpodobnost opomenutí některých rizik, nesnadné ovlivnění voleb subjektivními názory řešitelů a dokazatelnost

oprávněnosti zvolených bezpečnostních opatření. Nevýhodou je vysoká finanční a časová náročnost. Je také náročná na odbornost řešitelů.

- **kombinovaná analýza rizik** - analýza, v níž je dle uvážení v jednotlivých oblastech použita analýza základní, neformální nebo detailní. Jde o nejčastěji používanou metodu a její předností je dosažení optimální výše nákladů vynaložených na analýzu rizik.

2.1.3 Vypracování bezpečnostní politiky

Pro vypracování bezpečnostní politiky může organizace využít vlastních zdrojů, tedy svých zaměstnanců, kdy jsou výhodou nižší náklady a vyšší spojení tvůrce s organizací, nicméně pokud firma nezaměstnává vlastního kvalitního bezpečnostního experta, může se stát, že pověřený zaměstnanec nebude mít dostatek znalostí a zkušeností s tímto druhem práce. V této situaci je pro firmu spolehlivější, pověřit externí firmu. Optimálním řešením je sestavení pracovního týmu, skládající se z pracovníků externí firmy a vlastních zaměstnanců. [5]

Při tvorbě bezpečnostní politiky, je kladen požadavek na úplnost dokumentu, tzn. musí pokrýt všechny významné oblasti informační bezpečnosti organizace. Při správné výstavbě bezpečnostní politiky, je zajištěna potřebná úroveň dostupnosti, důvěrnosti a integrity dat v informačním systému podniku. Zajišťuje také bezpečnost transakcí v distribuovaném prostředí (internet). [5][14]

Bezpečnostní politika obsahuje podmínky a metody reálného řešení informační bezpečnosti. Její návrh je zapotřebí provádět s ohledem na delší časové období, ne pouze na aktuální stav a všechny postupy je nutno ověřit a popsat jejich implementaci. Způsoby zabezpečení se neustále sledují a případně zdokonalují a v případě chyb a bezpečnostních incidentů se vyvozují závěry a protiopatření. [23][23]

Dokument bezpečnostní politiky organizace by měl obsahovat [18]:

- definici bezpečnosti informací, její cíle, rozsah a její důležitost,
- prohlášení managementu organizace o záměru podporovat cíle a principy bezpečnosti informací,
- stručný výklad bezpečnostních zásad, principů a norem a požadavky zvláštní důležitosti pro organizaci, např.:
    - dodržování legislativních a smluvních požadavků,

- požadavky na vzdělávání v oblasti bezpečnosti,
- zásady prevence a detekce virů i ostatního škodlivého programového vybavení,
- zásady plánování kontinuity činností organizace,
- důsledky porušení bezpečnostních zásad,

- stanovení obecných a specifických odpovědností pro oblast bezpečnosti informací včetně hlášení bezpečnostních incidentů,
- odkazy na dokumentaci, která může bezpečnostní politiku podporovat, např. na detailnější bezpečnostní politiky a postupy zaměřené na specifické informační systémy nebo bezpečnostní pravidla, která by měli uživatelé dodržovat.

2.1.4 Implementace bezpečnostní politiky

Dochází zde k postupnému řešení dílčích kroků a projektů (např. systém monitorování, zajištění bezpečnostního vzdělávání,…). Problémem nebo chybou v tomto kroku může být například provádění mnoha kompromisů, neadekvátní rozsah bezpečnostní politiky (negativní dopad výkonnost IS) nebo nedostatečná propagace bezpečnostní politiky. [14]

Obsah schvaluje vedení organizace a tato schválená podoba je závazná pro všechny zaměstnance firmy. Bezpečnostní politika by měla být srozumitelně formulována, aby jí zaměstnanci byli schopni dobře porozumět. Musí tedy splňovat tři základní principy, jinak se stává bezcennými pravidly řízení informační bezpečnosti - zpracována v písemné podobě, závazná pro všechny, známá. [5][9][18]

Pokud bezpečnostní politika není v písemné podobě, mohou nastat následující problémy. Každý může pochopit bezpečnostní politiku po svém, na základě čeho mohou vznikat nebezpečné mezery a nejasnosti. Chybí jasné postupy nebo důkazní materiály. Je třeba podotknout, že bezpečnostní politika dělá informační bezpečnost přehlednou, čemuž písemná podoba napomáhá. Jednak shrnuje veškerá aktiva, jednak poukazuje na nebezpečí, která jim hrozí, ale především definuje prvky bezpečnosti, které je zapotřebí nasadit. [8][18]

Dalším problémem, který způsobí závažné slabiny v informační bezpečnosti, je bezpečnostní politika závazná pouze pro někoho. Příkladem mohou být výjimky z omezení v přístupu na internet pro vedení organizace. [8][18]

Posledním principem je, že bezpečnostní politika musí být známá, tzn. ne jen těmi, kdo se na ní aktivně podílejí, ale každým, kdo k ní má jakýkoliv vztah, tedy všichni zaměstnanci organizace i smluvní externí firmy. S bezpečnostní politikou by měla být například seznámena i uklízečka, která sice nepracuje na počítači, tudíž se jí moc netýká informační bezpečnost, ale vzhledem k tomu, že má neomezený přístup do prostor společnosti, dostává se do vztahu k bezpečnostní politice prostřednictvím fyzické bezpečnosti. [8][18]

Zde je třeba zmínit, že existuje jen jedna politika, ale může mít několik podob. Aby se každý zaměstnanec mohl seznámit především s tím, co se ho přímo týká, musí být vypracováno více dokumentů, ve kterých je zapotřebí pravidla bezpečnosti rozlišit pro různé zaměstnance. Například správce systému, běžný uživatel a manažer pracující s citlivými daty, má odlišnou pravomoc i zodpovědnost. [8][18]

2.1.5 Monitoring a audit

Hodnocení, audit a monitoring stavu bezpečnosti v organizaci je nedílnou součástí procesu řízení bezpečnosti. Východiskem jsou vždy bezpečnostní cíle stanovené v bezpečnostní studii. [16]

Velké a některé střední firmy musí mít pro oblast zabezpečení firmy samostatného bezpečnostního technika, který bude zodpovídat za plnění a dodržování všeho, co souvisí s komplexní bezpečnostní politikou firmy a bude provádět přezkoumání, kdy je posouzena vhodnost, přiměřenost, efektivnost a aktuálnost stanovených pravidel. Součástí přezkoumání by mělo být zhodnocení možností pro zlepšení a změny v přístupu k bezpečnosti. [14][16]

Neprovádění hodnocení, auditu nebo nedostatečná úroveň monitoringu může mít za následek neodhalení bezpečnostních incidentů a škody potom mohou být vyšší než při včas odhalených incidentech. [16]

2.2 Typy bezpečnostních politik

Bezpečnostní politiky lze dělit podle účelu [12]:

- **Regulační bezpečnostní politika** – je požadována, pokud se organizace týkají jakékoliv průmyslové nebo národní standardy a normy. Vysvětluje, které regulační ustanovení musí být v organizaci dodržovány.
- **Poradní bezpečnostní politika** – vymezuje chování a aktivity, které jsou přijatelné a definuje následky jejich nedodržení. Jedná se o formulaci

požadavků vrcholového managementu. Touto formou je zpracovávána většina bezpečnostních politik.

- **Informativní bezpečnostní politika** – obsahuje informace o konkrétních subjektech, jako např. cíle společnosti, jak organizace komunikuje s partnery, zákazníky apod. Tato forma bezpečnostní politiky je nevynutitelná.

Typy bezpečnostních politik podle formulace [8][12][14]:

- **Promiskuitní bezpečnostní politika** – každému povoluje dělat vše, tedy i to, co by dělat neměl. Je obvykle provozně nenákladná, důvodem použití této politiky tedy může být ekonomická nenáročnost řešení. Zaručuje pouze minimální, nebo žádnou bezpečnost. Příkladem může být to, že pro autentizaci nenutí povinně používat ani hesla.
- **Liberální bezpečnostní politika** – každému povoluje dělat vše, až na věci explicitně zakázané. Nepominutelným požadavkem je nízká ekonomická náročnost řešení. Většinou je uplatňována v prostředích, kde se hrozby považují za málo až průměrně závažné. Zaručuje větší bezpečnost, než v promiskuitní bezpečnostní politice. Například se může opírat o zásadu volitelného řízení přístupu založeného na identitě subjektů.
- **Opatrná (racionální) bezpečnostní politika** – každému zakazuje dělat vše, co není explicitně povoleno. Tato politika je na zavedení nákladnější, avšak zaručuje vyšší stupeň bezpečnosti. Při uplatnění na nový informační systém většinou požaduje provedení klasifikace objektů a subjektů podle jejich schopnosti a citlivosti. Opírá se o zásadu povinného řízení přístupu založeného na rolích, prostřednictvím kterých vystupují subjekty při styku s informačním systémem. Při zavádění firewallů je obvykle počáteční bezpečnostní politikou v případě používání informačního systému v internetu.
- **Paranoidní bezpečnostní politika** – každému zakazuje dělat vše potenciálně nebezpečné, tedy i to co by nemuselo být explicitně zakázáno. Zpravidla vede k maximální izolaci systému, tudíž zaručuje nejvyšší úroveň bezpečnosti. Například zakazuje používat jakékoliv internetové služby (které by se daly zneužít).

3 ROZBOR KONKRÉTNÍ FIRMY

V této kapitole se budu zabývat rozborem konkrétní firmy, která si nepřeje, aby její jméno či jméno majitele bylo zveřejňováno. Zabývat se ochranou veškerých aktiv firmy, by vyžadovalo velký rozsah, proto se zaměřím pouze na informační bezpečnost.

3.1 Představení firmy

Firma XYZ je malá obchodní firma s 25 zaměstnanci, zabývající se nákupem a prodejem krmných a doplňkových produktů pro chovná domácí zvířata. Firma má svůj relativně pevný okruh dodavatelů i odběratelů jak velkoprodeje, tak maloprodeje.

Maloprodej probíhá prostřednictvím e-shopu nebo telefonických objednávek, přičemž doručení objednávek zákazníkům zajišťují přepravní společnosti, se kterými má firma XYZ uzavřenou smlouvu, obsahující všechny podmínky, povinnosti a požadavky týkající se doručování zásilek klientům na určená místa. Pro velkoobchodní prodej firma XYZ poskytuje své klientele i vlastní rozvoz zboží.

Vzhledem k tomu že se jedná o malou firmu, není její organizační struktura nijak složitá, tzn. všechna pracovní místa jsou z tohoto hlediska na stejné úrovni, kdy jedinou nadřazenou pozicí je zástupce vedoucího a dále jemu nadřazený vedoucí, který je zároveň majitelem firmy. Organizační strukturu zobrazuje následující Tabulka 2.

Tabulka 2: Organizační struktura firmy

Organizační struktura firmy					
Vedoucí					
Zástupce vedoucího					
Účetní	Telemarketingoví asistenti	Fakturanti	Skladníci	Kurýři	Obchodní zástupci

Zdroj: vlastní

3.2 Popis současného stavu zabezpečení

V této kapitole bude popsán současný stav zabezpečení ve firmě XYZ. Tento vstupní rozbor firmy slouží k zjištění, jaké úrovně informační bezpečnosti se zde dosahuje, což úzce souvisí i s fyzickou a personální ochranou.

3.2.1 Současný stav bezpečnostní politiky

Bylo zjištěno, že firma nemá zpracovaný základní dokument Bezpečnostní politika podniku, tedy písemný dokument, který určuje rámec bezpečnosti firmy a je po schválení vedením závazný pro všechny zaměstnance. Nejsou zde tedy nijak definovány základní cíle a postoje k informační bezpečnosti.

V podstatě zaměstnanci nemají žádné povědomí o informační bezpečnosti a nemají tedy představu o tom, co informace pro firmu znamenají a proč je důležité je chránit. Sice ve firmě již jsou zavedeny určité bezpečnostní mechanismy, ale pokud s nimi není řádně seznámen lidský faktor, který bývá nejčastější příčinou prolomení zabezpečení, pak tyto mechanismy plně nesplňují svou funkci a mohou tak představovat zranitelné místo, díky kterému firmě hrozí různá rizika.

3.2.2 IT zabezpečení

Klientské počítače: 13

Přenosné počítače: 2 (obchodní zástupci)

Server: Microsoft Windows 10

Připojení k internetu: pomocí ADSL modemu o rychlosti 20Mbit

Tiskárny: 3

Účetní program: MRP K/S

V oblasti zabezpečení sítě a počítačů jsem dospěla k těmto výsledkům:

Antivirová ochrana: nainstalovaná na všech počítačích, na přenosných počítačích není aktualizována.

Brána firewall: realizována pouze serverová brána firewall, na klientských i přenosných počítačích personální firewall chybí.

Software pro filtrování nevyžádané pošty: celá firma používá poštovního klienta Microsoft Outlook, který má omezenou funkci filtrování nevyžádané pošty, která není na žádných počítačích aktualizována.

Aktualizace: všechny počítače běží na systému Microsoft Windows 10, které jsou pravidelně aktualizovány.

Používání internetu: nepoužívají se nástroje k filtrování obsahu webu, bezpečné použití internetu zaleží tedy na každém zaměstnanci. Zásady bezpečného používání internetu znají pouze někteří zaměstnanci a dodržování těchto zásad není žádným způsobem kontrolováno.

Zálohování dat: každý den probíhá záloha dat z účetního programu MRP K/S, pomocí zálohovacího systému, který je součástí tohoto programu. Data se ukládají na velkokapacitní disk serveru a přístup k těmto zálohám je možný pouze přes přístupové heslo. Data se také jednou týdně zálohují v zašifrované formě na uložiště serveru Google.

Ověřování identity uživatelů: standardně probíhá pro přihlášení do účetního programu MRP K/S a přihlášení k e-shopu pod oprávněním „Admin“. Přihlašovací údaje jsou pro přístup k MRP K/S i e-shopu totožné. Pro přístup k operačnímu systému všech počítačů není aplikováno žádné zabezpečení.

3.2.3 Fyzické zabezpečení

Vstup do budovy není žádným způsobem kontrolován či evidován. Do budovy má od 8:00 hodin do 18:00 hodin volný přístup i veřejnosti a to pouze do prostor skladu a kanceláře, kde probíhá fakturace a platba zakoupeného zboží. Jak vstupní dveře, tak dveře od prostor veřejnosti nepřístupné jsou po celý pracovní den odemčené.

Zvnějšku je budova střežena centrálním alarmem s rozmístěním citlivých senzorů ve všech oknech a dveřích. V případě pokusu o neoprávněné vniknutí do budovy, je o tomto stavu informován majitel prostřednictvím telefonu a nejbližší policejní stanice. Tento systém je pro fyzickou bezpečnost uspokojivý.

Přenosné počítače nejsou vybaveny sériovými čísly ani evidenčními identifikačními prvky. Server je umístěn v jedné z kanceláří, do které mají neomezený přístup všichni zaměstnanci.

Záložní zdroj energie (UPS), tedy zařízení nebo systém, který zajišťuje souvislou dodávku elektřiny, ve firmě není.

Firma splňuje všechny požadavky v oblasti požární ochrany dle zákona č. 133/1985 Sb., o požární ochraně.

3.2.4 Personální zabezpečení

V této oblasti ve firmě není realizováno téměř žádné zabezpečení. Při přijímání nových zaměstnanců se pohled na bezpečnost nijak nezohledňuje, není ani zahrnuta v pracovních smlouvách. Nejsou zavedena žádná pravidla informační bezpečnosti.

Zaměstnanci nejsou proškoleni o významu informační bezpečnosti. Celý pracovní tým používá slabá hesla a navíc bylo zjištěno, že je někteří zaměstnanci mají napsaná na pracovním stole nebo přímo uložené v počítači.

3.3 Proces tvorby návrhu bezpečnostní politiky

V této části přicházím k samotné tvorbě návrhu bezpečnostní politiky, tedy plánu zabezpečení informací, kdy je nejprve nutno provést analýzu rizik, pro zjištění možných hrozeb a odhalení zranitelných míst. Poté bude následovat návrh dokumentu Bezpečnostní politika, kde budou specifikovány hlavní cíle a požadavky na informační bezpečnost a bezpečnostní opatření pro jednotlivé oblasti. Dalším krokem v procesu tvorby bezpečnostní politiky je její implementace, tedy zavedení navržených opatření a jejich následné testování. Tato druhá část už však není předmětem této bakalářské práce.

3.3.1 Cíl plánu zabezpečení

Vedení firmy připouští, že její zabezpečení není ideální, z čehož vyplývá, že firmě hrozí různá rizika a z toho důvodu došlo k rozhodnutí vedení zabývat se tvorbou plánu zabezpečení. Vzhledem k tomu, že je firma při vytváření plánu limitována finančními možnostmi, nemůže si dovolit dokonalé zabezpečení na armádní úrovni. Cílem tedy bude dosáhnout relativně kvalitního zabezpečení, aniž by bylo třeba na jeho realizaci vynaložit horentní sumy. Jako hlavní cíle lze uvést:

- identifikace rizik,
- zdokonalení prevence,
- návrhy plánů.

3.3.2 Analýza rizik

Analýza rizik může být zpracována několika způsoby. Já jsem z důvodu finanční a časové nenáročnosti zvolila neformální analýzu rizik. Znalosti potřebné k provedení analýzy jsem získala vlastní praxí, vzhledem k tomu, že jsem zaměstnancem firmy XYZ a na základě rozhovorů s vedoucími i řadovými pracovníky firmy.

Provedená analýza rizik bude sloužit jako podklad pro vytvoření dokumentu Bezpečnostní politika.

3.3.2.1 Specifikace aktiv firmy

Hlavními aktivy jsou:

- uzavřené smlouvy s dodavateli a informace o nich,
- vystavené faktury odběratelům,
- databáze zákazníků,
- informace týkající se skladového hospodářství,
- finanční informace (platby bankovním převodem),
- informace personálního charakteru,
- e-shop (přístup pod oprávněním „Admin“),
- e-mailová databáze.

Pro ocenění aktiv ve smyslu jejich důvěrnosti a důležitosti jsem využila klasifikační třídy, které jsou definovány následovně:

1. Veřejná data bez omezení přístupu
2. Neveřejná interní data, v případě prozrazení mimo hranice organizace nehrozí žádná závažná rizika.
3. Důvěrná data uvnitř organizace, požadavek na důvěrnost a integritu, v neautorizovaných rukou by tato data mohla vést k ovlivnění chodu organizace či poskytnutí konkurenční výhody druhé straně.
4. Tajná data, neoprávněný přístup k datům by mohl být kritický pro provoz společnosti, nutným požadavkem je integrita dat.

Tabulka 3 zobrazuje ocenění aktiv pomocí klasifikačních tříd.

Tabulka 3: Klasifikace dat

Data	Klasifikace
Smlouvy s dodavateli	3
Vystavené faktury	3
Databáze zákazníků	3
Skladové hospodářství	2
Finanční informace	4
Personální informace	3
E-shop	4
E-mailová databáze	3

Zdroj: vlastní

3.3.2.2 Stanovení hrozeb a zranitelnosti

Základem pro správné vyhodnocení rizik, je pojmenování hrozeb, kterými je firma XYZ vystavena. U každé hrozby je odhaleno zranitelné místo, prostřednictvím kterého může dojít k naplnění rizika.

Hrozba útoků

Jedná se o nebezpečí spojené s užíváním internetu. Každý, kdo je připojený, se stává potenciálním terčem útoku (viry, adware, spyware, spamy, neautorizovaný přístup, zneužití nebo škodlivé použití software, apod.). Zranitelným místem zde může být opět zaměstnanec, který může takový útok umožnit například otevřením nevyžádané pošty, nebo nedostatky v systému zabezpečení sítě a jednotlivých počítačů.

V systému zabezpečení sítě a jednotlivých počítačů byly odhaleny následující slabiny:

- absence personálního firewall na klientských počítačích,
- nedostatečné zajištění filtrování nevyžádané pošty,
- absence nástrojů k filtrování obsahu webu,
- slabá hesla.

Vzhledem k uvedeným slabinám v zabezpečení sítě a počítačů a k tomu, že většina zaměstnanců není poučena o zásadách používání internetu a závažnosti rizik spojené s jeho

užíváním je míra rizika útoků stanovena jako vysoká. Bezpečnostním opatřením v tomto případě může být zajištění těchto zjištěných slabin zakoupením, instalací a pravidelných aktualizací příslušného programového vybavení a s tím související školení zaměstnanců.

Hrozba vyzrazení informací zaměstnancem

Tato hrozba představuje únik informací přes zaměstnance. Tento únik může být neúmyslný, tedy vyplývá z neznalosti nebo nedbalosti zaměstnanců v oblasti informační bezpečnosti, nebo úmyslný. Mezi úmyslné formy vyzrazení informace patří:

- pořízení nové, neevidované kopie dat a následné předání neoprávněné osobě,
- ústní sdělení neoprávněné osobě,
- předání dat neoprávněné osobě za peněžní nebo materiální úplatu.

Naplnění rizika úmyslného vyzrazení nelze vyloučit. Zejména za finanční odměnu, případně jiné materiální plnění, je naplnění rizika reálné. Rovněž nelze vyloučit vyzrazení informací zaměstnancem, kterému je vyhrožováno použitím násilí nebo pohrůžkou použití násilí. Míra rizika úmyslného vyzrazení je stanovena jako střední.

Neúmyslná forma vyzrazení zaměstnancem je v podmínkách firmy pravděpodobnější. Toto riziko se dá zčásti eliminovat pečlivým poučením osob, jejich periodickým proškolováním a důslednou kontrolou dodržování pravidel informační bezpečnosti. Míra naplnění tohoto rizika je na střední úrovni.

Hrozba nakládání s informacemi a poškození informací neoprávněnými osobami, ztráta nebo únik informací

Příkladem útočníků v tomto případě může být konkurence nebo nespokojený bývalý zaměstnanec. Jedná se o cílené útoky se záměrem poškodit nebo odcizit informace nebo vybavení. Získané informace mohou potom tito útočníci využít k vydírání nebo úplné destrukci firmy. K útoku mohou tito útočníci využívat formy útoku spojené s užíváním internetu, jako v případě první uvedené hrozby nebo mohou získat přístup k informacím pomocí:

- sociálního inženýrství - způsob manipulace s lidmi za účelem provedení určité akce či získání určité informace,
- překonání technických prostředků, vloupání a odcizení,
- odcizení či ztráta nosiče informací - přenosné počítače,

Protože od počátku existence firmy, nebyl realizován žádný útok formou sociálního inženýrství, je pravděpodobnost tohoto rizika nízká, avšak možnost takového útoku přesto nelze zcela vyloučit. Naopak pokus o neoprávněný vstup do budovy, kdy pravděpodobně nebylo příčinou snaha získat informace, ale krádež movitých věcí, byl ve firmě zaznamenán přibližně jednou za dva roky. Míru tohoto rizika lze tedy stanovit jako vysokou. Odcizení či ztrátu přenosných počítačů nelze nikdy zcela vyloučit, a protože tyto počítače nemají nainstalovány téměř žádné zabezpečovací nástroje, je pravděpodobnost získání informací z těchto nosičů poměrně vysoká.

Navrhovaným opatřením proti této hrozbě je zdokonalit fyzickou ochranu firmy XYZ např. zavedením kontroly vstupu osob do budovy. Dále zavést fyzickou ochranu nosičů informací, např. označení přenosných počítačů evidenčními čísly, vybavení přenosných počítačů šifrovacím softwarem pro šifrování dat na nich uložených. I s touto hrozbou souvisí vzdělání zaměstnanců v oblasti informační bezpečnosti.

Hrozba poškození nebo ztráta informací živelní pohromou

Informace mohou být poškozeny či zničeny různými formami živelních pohrom. V tomto případě může být hrozbou například:

- požár, který může vzniknout následkem úderu blesku nebo selháním lidského činitele při práci s otevřeným ohněm, při kouření apod.,
- větrná bouře, případně tornádo, doprovázeným přívalovými dešti s následným poškozením budovy,
- záplavy vzniklé přívalovými dešti, povodněmi nebo následkem poruch na rozvodech vody v budově,
- poruchy elektrické sítě následkem živelní pohromy.

Z výše uvedených forem živelných pohrom je patrné, že lze předejít pouze vzniku požáru, např. důslednou kontrolou dodržování požárních předpisů, prováděním periodických revizí hromosvodů a přenosných hasicích prostředků, školením zaměstnanců z protipožárních opatření, apod. a poruchám elektrické sítě instalací záložního zdroje energie. Míra naplnění rizika poškození, případně zničení informace, požárem či výpadkem elektřiny je na střední úrovni.

Riziko poškození nebo zničení informace větrnou bouří, tornádem či přívalovými dešti je málo pravděpodobné, ale vyloučit ho nemůžeme. V lokalitě budovy firmy se riziko vzniku

povodně či rozsáhlých záplav neočekává, pravděpodobnost tohoto rizika je tedy stanovena jako malá.

3.3.2.3 Specifikace rizik

Tabulka 4 zobrazuje přehled hrozeb a stanovení míry rizik naplnění těchto hrozeb. Celkovou míru rizika neoprávněného nakládání s daty lze v současné době stanovit jako střední, z čehož vyplývá, že bude třeba k eliminaci rizik navrhnout bezpečnostní opatření.

Tabulka 4: Stanovení míry rizik

Hrozba	Míra rizika
Útoky prostřednictvím internetu	vysoká
Vyzrazení informací zaměstnancem	střední
Manipulace s informacemi neoprávněnými osobami	střední
Poškození, ztráta informací živelní pohromou	střední
Celková míra rizika	střední

Zdroj: vlastní

3.3.3 Vypracování návrhu bezpečnostní politiky

V této části práce bude navrhována bezpečnostní politika, která vychází ze studie současného stavu informační bezpečnosti v organizaci a udává, co má být chráněno a rámcově stanovuje, jakým způsobem toho má být dosaženo.

Typ bezpečnostní politiky lze stanovit podle účelu jako poradní bezpečnostní politiku a podle formulace jako liberální.

3.3.3.1 Úvodní ustanovení

Účelem tohoto dokumentu je stanovení bezpečnostní politiky firmy. Vedení firmy XYZ podporuje stanovené cíle bezpečnosti informací a touto bezpečnostní politikou vyjadřuje svoji strategii trvalého zajišťování bezpečnosti informací.

Bezpečnost informací pokrývá všechna důležitá informační aktiva společnosti. Bez spolehlivých informačních aktiv, by se společnost ocitla ve vážné nevýhodě. Proto tato politika ukládá všem zaměstnancům, smluvním partnerům a vedení firmy za povinnost být s touto politikou v souladu, aby byly informace řádně zabezpečeny. S tím souvisí zahrnutí

odpovědnosti zaměstnanců za bezpečnost do pracovních smluv. Všichni zaměstnanci a externí partneři musí být o bezpečnostní politice srozumitelně poučeni.

Tato politika stanovuje přístup k řízení bezpečnosti informací, aby zajistila patřičnou ochranu informačních aktiv před hrozbami, jako jsou chyby, podvody, vydírání, narušení soukromí, krádeže a přírodní pohromy, ať se již jedná o hrozby interní nebo externí, úmyslné či neúmyslné.

Vedení firmy XYZ má za povinnost a nese odpovědnost za zajištění ochrany informací. Navíc musí zajistit, že jsou informační aktiva chráněna minimálně způsobem, jakým jsou chráněna v ostatních organizacích podobného typu. Přiměřenou ochranu informačních aktiv musí udržovat v souladu se zákony a jinými právními předpisy ČR.

Aby bylo dosaženo tohoto cíle, musí být v pravidelných ročních intervalech prováděny analýzy rizik, kterým jsou informační aktiva firmy vystavena. Za revizi dokumentu bezpečnostní politiky odpovídá externí bezpečnostní manažer. Ten kontroluje aktuálnost a efektivnost působení tohoto dokumentu a o výsledcích kontrol vede záznamy. Pokud bezpečnostní incident nebo výsledek auditu poukáže na nedostatečnou úroveň bezpečnosti informací, musí vedení firmy XYZ okamžitě přijmout nápravná opatření k potlačení rizik. K provedení aktualizace a změny je zapotřebí vydání nového znění celého dokumentu.

3.3.3.2 Cíle a zásady bezpečnosti informací

Bezpečnostním cílem spojeným s bezpečnosti informací ve firmě XYZ je zajištění dostupnosti informačních aktiv jen oprávněným osobám, správnosti a kompletnosti informací, důvěrnosti a bezpečnosti jejich zpracování a ochrany informací proti náhodnému nebo neoprávněnému poškození nebo zničení, proti neoprávněnému přístupu, změnám nebo šíření a to v souladu se zákony a jinými právními předpisy.

Bezpečnost informací je charakterizována jako zajištění:

- důvěrnosti informací – informace jsou přístupné jen těm, kteří jsou k tomu oprávněni,
- integrity informací – informace nejsou neoprávněně nebo náhodně modifikovány, je zajištěna správnost a úplnost informací,
- dostupnosti informací – informace a s nimi spojená aktiva jsou oprávněným uživatelům vždy přístupná v době, kdy je potřebují.

3.3.3.3 Legislativní požadavky

Zajištění bezpečnosti informací firmy XYZ se realizuje v souladu s legislativními a smluvními požadavky zákonů a jiných právních předpisů s důrazem na povinnosti při ochraně informací.

Tam, kde je to relevantní, bude organizace udržovat soulad zejména s:

- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů,
- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím,
- Zákon č. 262/2006 Sb., zákoník práce,
- Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon),
- Zákon č. 513/1991 Sb., obchodní zákoník,
- Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích),
- Zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).
- ČSN ISO/IEC 17799,
- ostatní platné a aktuální interní normy, standardy, postupy a procedury.

3.3.3.4 Bezpečnostní odpovědnosti

Vedení firmy XYZ je odpovědné za:

- vytvoření podmínek pro bezpečnost informací ustanovením celkové bezpečnostní politiky informací v organizaci.
- jmenování manažera bezpečnosti informací, prostřednictvím externí firmy.
- jmenování správce IT prostřednictvím externí firmy.
- jmenování dalších externích partnerů, které se podílejí na řízení bezpečnosti ve firmě XYZ,
- zajištění vhodných školení a zvyšování bezpečnostního povědomí zaměstnanců,
- zajištění dodržování bezpečnosti informací v souladu s touto politikou a s ostatními příslušnými bezpečnostními standardy a normami, a se zákonem a jinými právními předpisy.

Manažer bezpečnosti informací je odpovědný za:

- implementaci efektivního způsobu řízení bezpečnosti informací,
- pomoc při formulaci politiky bezpečnosti informací,
- poradenství ohledně obsahu a implementace programu zajištění bezpečnosti informací,
- tvorbu návrhů organizačních norem, postupů a doporučení v oblasti informační bezpečnosti, předkládaných ke schválení vedení firmy XYZ.

Zaměstnanci jsou odpovědní za:

- jednání v souladu s bezpečnostní politikou.
- zajištění bezpečnosti aktiv firmy XYZ, tj. informací, hardwaru a softwaru a to konzistentním způsobem a v souladu s právními požadavky a s požadavky a závazky vedení.
- absolvování školení a správné využívání získaných znalostí,

3.3.3.5 Organizace bezpečnosti informací

Záměrem vedení firmy XYZ je řídit bezpečnost informací, koordinovat implementaci bezpečnostních opatření ve firmě dle stanovené působnosti a odpovědnosti a zlepšit řízení a koordinaci bezpečnosti informací dle normy ČSN ISO/IEC 17799.

Povinnosti spojené s řízením bezpečnosti informací ve firmě XYZ vykonává manažer bezpečnosti, který přezkoumává a sleduje bezpečnostní incidenty, sleduje významné změny zranitelnosti informačních aktiv a schvaluje hlavní kroky vedoucí ke zvýšení bezpečnosti informací.

Odpovědnost za bezpečnost informací v organizaci má nejen vedení organizace, ale také každý jednotlivý zaměstnanec a další smluvní partneři.

3.3.3.6 Řízení a klasifikace informačních aktiv

Účelem klasifikace a řízení informačních aktiv je udržovat jejich přiměřenou ochranu.

Nejvýznamnějšími informačními aktivy firmy XYZ jsou:

- uzavřené smlouvy s dodavateli a informace o nich,
- vystavené faktury odběratelům,
- databáze zákazníků,
- informace týkající se skladového hospodářství,
- finanční informace (platby bankovním převodem),
- informace personálního charakteru,
- e-shop (přístup pod oprávněním „Admin“),
- e-mailová databáze.

V rámci firmy XYZ je zavedena a udržována evidence důležitých informačních aktiv, u nichž je určen vlastník a je jednoznačně stanovena odpovědnost za dodržování povinností při jejich zpracování, shromažďování a uchovávání v souladu s platnými interními přepisy.

Informační aktiva firmy XYZ musí být klasifikována tak, aby byla naznačena jejich potřebnost, důležitost a stupeň ochrany při manipulaci s nimi.

Klasifikaci stanoví vedením firmy XYZ společně se smluvními externími partnery.

Klasifikace určuje způsob zacházení s informacemi s ohledem na jejich ochranu.

3.3.3.7 Personální bezpečnost

Účelem personální bezpečnosti je snížení rizika lidské chyby, krádeže, podvodu nebo zneužití prostředků organizace.

Posuzování uchazečů o zaměstnání z hlediska personální bezpečnosti je součástí výkonu personálních činností. Bezpečnostním cílem je zajištění vhodných postupů v rámci přijímacího řízení.

Seznámení zaměstnanců s bezpečnostní politikou je součástí vstupního školení a dalších periodických školení.

Všem zaměstnancům je poskytováno potřebné bezpečnostní poradenství, zvyšováno jejich bezpečnostní povědomí a podle potřeby poskytováno školení pro zdokonalení jejich znalostí

v oblasti informační bezpečnosti, přičemž účast na těchto školeních je uložena zaměstnancům jako povinnost.

Zaměstnanci jsou povinni zejména:

- používat pouze informace nezbytné k plnění jejich pracovních povinností,
- nakládat s informacemi tak, aby byla zachována bezpečnost informací a nedocházelo k bezpečnostním incidentům, dodržovat zásady práce s informacemi,
- chránit hardware, software a informace, které jsou jim svěřeny,
- chránit průnik škodlivého programového vybavení do IT systémů organizace,
- okamžitě oznámit bezpečnostní incidenty (selhání programového vybavení, podezřelé viry, chyby, slabiny nebo hrozby), které se v systému objevily bezpečnostnímu manažerovi nebo vedení organizace a učinit všechna opatření k minimalizaci následků bezpečnostních incidentů,
- dodržovat zásadu čistého stolu a zásadu čisté obrazovky.

Zaměstnanci mají zakázáno:

- sdílet účty či hesla s jinými osobami,
- kamkoliv psát nebo ukládat hesla,
- používání slabých hesel,
- snažit se vlámat do cizích uživatelských účtů,
- pořizovat kopie informací a odnášet informace v jakékoliv podobě z prostor organizace,
- poskytovat informační aktiva firmy neoprávněným osobám,
- užívání internetu nesouvisející s pracovní činností,
- stahovat do počítače jakékoliv soubory z internetu,
- používat firemní e-mail pro soukromé účely,
- zasahovat do programového vybavení,
- instalovat jakékoliv programové vybavení,
- kopírovat nelicencovaný software nebo to umožňovat jiným uživatelům.

Nedodržení bezpečnostních zásad může být kvalifikováno jako porušení povinností zaměstnance, případně porušení pracovní kázně s příslušnými důsledky pro zaměstnance, dle zákona č. 262/2006 Sb., zákoník práce.

Šetření bezpečnostních incidentů zajišťuje manažer bezpečnosti včetně zpracování protokolů o bezpečnostních incidentech, jejich evidence a předložení návrhů k zajištění bezpečnosti vedení firmy XYZ.

3.3.3.8 Fyzická bezpečnost a bezpečnost prostředí

Účelem fyzické bezpečnosti a bezpečnosti prostředí je předcházet neoprávněnému a přístupu k informacím, poškození a narušení informací.

Bezpečnostním cílem je zajištění fyzické ochrany informací a prostředí, ve kterém se informace nacházejí:

- kontrolou vstupu veřejnosti do budovy firmy XYZ,
- zabezpečením kanceláří a místností, ve kterých se nacházejí počítače či jiné nosiče informací,
- zabezpečením zařízení proti odcizení, poškození či zničení, zahrnující bezpečné umístění zařízení,
- umístění serveru do zabezpečené oblasti, kam má přístup pouze správce sítě,
- zajištěním podpůrných služeb pro provoz zařízení (dodávky energie),
- zabezpečení kabeláže a zajištění pravidelné a bezpečné údržby zařízení.

Stanovení režimu vstupu a výstupu osob včetně zajištění zabezpečených oblastí a definování fyzického bezpečnostního perimetru je ve firmě XYZ stanoveno samostatnou politikou.

Ochrana přenosných počítačů zahrnuje:

- nezanechání přenosného počítače bez dozoru,
- inventarizace včetně označení přenosných počítačů výrobním číslem,
- povinné hlášení odcizení či ztráty přenosných počítačů vedení firmy XYZ,
- označení přenosných počítačů evidenčními čísly, pro snadnou identifikaci,
- vhodné nastavení operačního systému,
- zálohování dat z přenosného počítače na externí disk,

- vybavení přenosných počítačů šifrovacím softwarem pro šifrování dat na nich uložených,

Zajištění požární bezpečnosti podle Zákona č. 133/1985 Sb., o požární ochraně a jiných právních předpisů je v organizaci upraveno zvláštním vnitřním předpisem.

3.3.3.9 Řízení přístupu

Účelem řízení přístupu k informačním aktivům firmy XYZ je zajistit, aby k nim měli přístup pouze oprávnění uživatelé. Pro přístup jsou stanovena pravidla, která určují postupy pro autorizaci, zřizování, změny a odebíraní přístupových práv.

Pro přístup k informacím bude zavedena politika „need to know“. Uživatelé dostanou pouze taková práva k informačním aktivům, která jim umožní plně vykovávat jejich práci. Uživatelská práva budou vždy udržována na minimální přípustné úrovni.

Za udělení a odebírání patřičných práv uživatelům je zodpovědné vedení organizace.

Přístup k informacím musí vyžadovat uživatelské jméno a heslo. Uživatelská jména musí mít pevný formát, například složenina iniciálu jména a příjmení osoby.

Na hesla jsou kladeny tyto požadavky:

- vynucená délka hesla – minimálně 8 znaků,
- alfanumerické složení hesla,
- obnova hesla v cyklu 90 dnů,
- hesla nelze opakovat třikrát po sobě jdoucí.

Tam, kde je to nutné, je implementována detekce nežádoucího proniknutí. Uživatelský účet bude zablokován po třech neúspěšných pokusech o přihlášení.

Pokud dojde k rozvázání pracovního poměru, je vedení organizace povinno odebrat práva pro přístup do systému dříve než je danému zaměstnanci oznámeno ukončení jeho pracovního poměru.

Heslo k zálohám uložených na velkokapacitním disku serveru je uloženo na bezpečném místě pro případ nouze či katastrofy, například v trezoru.

Souborové systémy musí mít maximální možnou úroveň zabezpečení. Kde je to možné, budou mít uživatelé práva jen ke čtení, aby se předešlo náhodné nechtěné modifikaci či smazání dat.

3.3.3.10 Řízení komunikací a řízení provozu

Účelem řízení bezpečnosti komunikací a provozu je zajistit správný a bezpečný provoz prostředků pro zpracování informací, minimalizovat riziko selhání systému, chránit integritu, dostupnost a důvěrnost informací, chránit integritu a dostupnost programů a zajistit ochranu počítačových sítí.

Bezpečnostním cílem je zajištění ochrany informací prostřednictvím:

- ochrany proti škodlivým a automaticky spuštěným programům – zakoupení, instalace, správná konfigurace a pravidelná aktualizace antivirového programu na všechny firemní počítače,
- zakoupení, instalace a správné konfigurace a pravidelná kontrola firewall na všech firemních počítačích,
- aktualizace a správné konfigurace operačních systémů všech firemních počítačů,
- využívání jen licencovaného software,
- každodenního zálohování, aby tak byla zajištěna obnova dat a systémů ve vazbě na zachování základních funkcí firmy XYZ,
- správy bezpečnosti počítačových sítí,
- zajištění dostupnosti informací a služeb,
- zajištění důvěrnosti informací při jejich přenosu pomocí kryptografické ochrany,
- ochrany před neautorizovanými zásahy dodržováním principu oddělení povinnosti a odpovědnosti při přidělování uživatelských práv,
- opatření pro zajištění bezpečnosti elektronické pošty - nastavení v poštovním klientu funkci filtrování nevyžádané pošty,
- dodržování bezpečnosti při zacházení s paměťovými médii.

3.3.3.11 Vývoj a údržba systémů

Účelem je prosadit bezpečnost informací do informačních systémů. Implementace a změny informačních systémů firmy XYZ jsou spojeny se stanovením vhodných bezpečnostních požadavků.

Vývoj a údržba informačních systémů v rozsahu infrastruktury firmy XYZ a uživatelsky vyvinutých aplikací je podle stanovené působnosti zajišťována dodavateli jednotlivých systémů včetně zajišťování implementace bezpečnostní politiky v oblasti procesů IT.

3.3.3.12 Řízení kontinuity činnosti organizace

Záměrem vedení firmy XYZ je zajistit připravenost k řešení krizových situací a zachování základních funkcí v rozsahu fungování kritické infrastruktury.

Bezpečnostním cílem je zabránění přerušení provozních činností, ochrana kritických procesů organizace před následky závažných chyb, minimalizace následků nežádoucích událostí (přírodní pohroma, nehoda, porucha zařízení nebo úmyslné poškození informačního systému) a zotavení se ze ztráty informačních aktiv na přijatelnou úroveň.

V procesu plánování kontinuity činnosti organizace, je vedení firmy XYZ odpovědné za zajištění vytvoření plánů obnovy funkčnosti a havarijní plány pro všechny kritické aplikace, systémy a sítě, které zajišťují rychlé obnovení nezbytných činností v organizaci.

Tyto dokumenty identifikují kritické činnosti organizace a jsou zde začleněny požadavky na řízení bezpečnosti informací. Základním cílem těchto dokumentů je zajištění přípravy, proškolení a připravenosti k výkonu činností spojených s řešením krizových situací, ochranou zdraví a života zaměstnanců a ochranou majetku.

Krizové řízení a přijetí preventivních opatření k zachování základních funkcí, které jsou blíže identifikovány v interních předpisech firmy XYZ, spadá do kompetence vedení firmy XYZ.

3.3.3.13 Soulad s požadavky

V rámci organizace musí být veden přehled platných právních norem a předpisů vztahujících se k problematice bezpečnosti informací.

Vedení firmy XYZ je zodpovědné za pravidelné provádění přezkoumání souladu všech oblastí s bezpečnostní politikou a s příslušnými standardy a normami, dále dodržování právních norem, soulad s legislativními předpisy a dodržování smluvních a bezpečnostních požadavků.

Firma XYZ dodržuje ustanovení o autorském právu a podmínky licenčních ujednání dodavatelů programového vybavení.

Firma XYZ přijímá a provádí opatření k zajištění ochrany osobních údajů a citlivých údajů v souladu se zákony a jinými právními předpisy.

3.3.4 Implementace bezpečnostní politiky

Procesem implementace se rozumí zavedení bezpečnostní politiky do praxe. Lze jej tedy chápat jako zavedení bezpečnostních opatření uvedených v bezpečnostní politice. Vzhledem k tomu, že firma nemá svého bezpečnostního experta, bude pro realizaci plánu zabezpečení využita specializovaná externí firma.

Aby bezpečnostní politika fungovala správně, musí být srozumitelná, závazná, vynutitelná a vztahovat se bez výjimky na celou organizaci. Také je nutné bezpečnostní politiku spravovat, aby i nadále vyhovovala požadavkům organizace. Tím rozumíme její modernizaci, aktualizaci a přidávání nových funkcí.

Požadavky na informační bezpečnost nejsou specifikovány pouze ve vytvořeném dokumentu Bezpečnostní politika, ale i v dalších interních bezpečnostních normách, standardech, postupech a procedurách. Je tedy zapotřebí, aby byla společně s implementováním Bezpečnostní politiky zavedena i veškerá navazující bezpečnostní dokumentace, která není předmětem této práce.

Bakalářská práce slouží pouze jako informační materiál, tudíž žádné z uvedených doporučení nebylo aplikováno.

3.3.5 Testování a audit

Poté co je bezpečnostní politika uvedena v platnost, je nutné ověřovat její bezchybné fungování. Přezkoumání jsou důležitá pro zajištění toho, že přístup organizace k řízení bezpečnosti informací je vyhovující, přiměřený a dostatečně účinný. K tomuto účelu slouží testování, pro které musí být vypracovaný a definovaný plán testů. Náhodné testování není průkazné. Jak již bylo zmíněno, pro realizaci plánu zabezpečení bude v této firmě využíváno specializované externí firmy, tudíž i činnosti spojené s testováním a případné modernizace a aktualizace bezpečnostní politiky jsou v kompetenci externího partnera.

ZÁVĚR

Cílem bakalářské práce bylo objasnění pojmu bezpečnostní politika a s ní související oblast informační bezpečnosti. Dříve než byla rozvinuta tato problematika, byly v úvodní kapitole práce definovány základní pojmy, které s tímto tématem souvisí a které jsou v práci zmiňovány.

V další části teoretického úvodu byl vysvětlen pojem informační bezpečnost, jako ochrana informací ve všech jejich formách. Bezpečné informace lze chápat jako ty informace, které splňují tři základní požadavky, a to zachování bezpečnostních funkcí, tj. důvěrnost, integrita a dostupnost informací. Dále jsou popsány bezpečnostní mechanismy různého charakteru, které se používají k dosažení zmíněných požadavků na informační bezpečnost.

V souvislosti s pojmem bezpečnost informací, bylo třeba se zmínit o dalších dvou termínech, a to bezpečnost organizace a bezpečnost IS/ICT, které společně tvoří celkové zabezpečení organizace. Z toho vyplývá, že bezpečnost informací je do jisté míry provázána s mnoha procesy v organizaci a je úzce spjata s personální i fyzickou bezpečností.

Dále byly popsány základní oblasti informační bezpečnosti. Tyto oblasti je třeba zahrnout do bezpečnostní politiky a pro každou oblast stanovit určité požadavky a pravidla. Tak tomu bylo i v této práci, kdy jsem tuto kapitolu použila jako osnovu k vytvoření dokumentu Bezpečnostní politika pro konkrétní organizaci.

Při zpracování bezpečnostní politiky je nutno mít na zřeteli vždy požadavky a povinnosti vyplývající z legislativních úprav ve státě, které byly zmíněny v další kapitole teoretického úvodu. Vzhledem k tomu, že je oblast bezpečnosti informací velice široká a úzce souvisí s ochranou hmotného majetku, života a zdraví zaměstnanců a další problematikou, byly uvedeny pouze vybrané základní legislativní a jiné předpisy.

V kapitole Bezpečnostní politika byl nejprve vysvětlen hlavní význam tohoto pojmu a dále popsány jednotlivé fáze tvorby bezpečnostní politiky, na základě kterých byl vytvářen návrh bezpečnostní politiky pro konkrétní organizaci. V prvním kroku procesu tvorby bezpečnostní politiky nejprve dochází k rozhodnutí managementu zabývat se bezpečnostní politikou a k určení základních cílů a požadavků na informační bezpečnost organizace. Vychází se z aktuálního stavu organizace a definují se klíčové oblasti, které je nutno řešit. Pro správné vyhodnocení rizik spojených s ochranou informací je nutné pojmenování hrozeb, kterým jsou informace vystaveny a jejich bližší specifikace, což je náplní analýzy rizik. Po této analýze lze přistoupit k samotnému vypracování bezpečnostní politiky, při kterém je třeba držet se

stanovených cílů a požadavků na bezpečnost informací a zohlednit hrozící rizika, které je nutno zajistit určitými bezpečnostními opatřeními. Po fázi vytvoření bezpečnostní politiky přichází na řadu její implementace, tedy zavedení do praxe a následné testování a monitoring, které zajistí její bezchybné fungování.

Vyhodnocením stávajícího stavu bezpečnostních opatření v oblasti bezpečnosti informací v konkrétní organizaci a provedením analýzy rizik, byly zjištěny určité nedostatky a rizika, které organizaci hrozí. Rezervy byly nalezeny především v nedostatečném školení a povědomí zaměstnanců o informační bezpečnosti a v nezpracovaném dokumentu bezpečností politiky. Tyto zjištěné problémy poté sloužily jako podklad pro vytvoření návrhu bezpečnostní politiky, tedy plánu zabezpečení informací, který má zvýšit a zároveň zkvalitnit bezpečnost informací v organizaci a snížit míru naplnění zjištěných rizik na co nejnižší úroveň.

LITERATURA

[1] BASL, J, BLAŽÍČEK, R. *Podnikové informační systémy: podnik v informační společnosti*. 3., aktualiz. a dopl. vyd. Praha: Grada, 2012. ISBN 978-80-247-4307-3.

[2] BÉBR, R, DOUCEK, P. *Informační systémy pro podporu manažerské práce*. Praha: Professional publishing 2005. ISBN 80-86419-79-7.

[3] BRABEC, František. *Bezpečnost pro firmu, úřad, občana.* Praha: Public History, 2011. ISBN 80-85858-29-0.

[4] BRUCKNER, Tomáš. *Tvorba informačních systémů: principy, metodiky, architektury*. 1. vyd. Praha: Grada, 2012. ISBN 978-80-247-4153-6.

[5] BUDIŠ, Petr. *Computer world: Deník pro IT profesionály*. Jak vypracovat bezpečnostní politiku v podniku. [online]. 2005 [cit. 2016-11-01]. Dostupné z: http://computerworld.cz/securityworld/jak-vypracovat-bezpecnostni-politiku-v-podniku-46442

[6] ČAPEK, J, MÁCHOVÁ, R. *Teoretické základy informatiky.* Pardubice: Univerzita Pardubice, 2013. ISBN 978-80-7395-574-8.

[7] ČERMÁK, Miroslav. *Clever and Smart.* Bezpečnostní politika a související dokumenty. [online]. 2010 [cit. 2016-11-27]. Dostupné z: http://www.cleverandsmart.cz/bezpecnostni-politika-a-souvisejici-dokumenty/

[8] ČÍŽ, Luboš. *DCIT.* Implementace bezpečnostní politiky v organizaci. [online]. 2015 [cit. 2016-11-26]. Dostupné z: http://www.dcit.cz/cs/system/files/Implementace%20bezpecnostni%20politiky%20v%20organizaci.pdf

[9] ČSN ISO/IEC 17799 *Informační technologie - Soubor postupů pro řízení informační bezpečnosti. Český normalizační institut. 2006*

[10] DOUCEK, P, NOVÁK, L, NEDOMOVÁ, L, SVATÁ, V. *Řízení bezpečnosti informací.* Praha: Professional publishing, 2011. ISBN 978-80-7341-050-8.

[11] DOSEDĚL, Tomáš, *Počítačová bezpečnost a ochrana dat*, Brno: Computer Press, 2004. ISBN 80-251-0106-1.

[12] HANÁČEK, P, STAUDEK, J. *Bezpečnost informačních systémů*. 1 vyd. Praha: Úřad pro státní informační systém, 2000. 127 s. ISBN 80-238-5400-3.

[13] HUB, Miloslav. *Bezpečnost a ochrana informací v prostředí internetu.* Pardubice: Univerzita Pardubice, 2013. ISBN 978-80-7395-701-8.

[14] CHLUP, Marek. *Bezpečnost IS/IT*. [online]. 2006 [cit. 2016-11-27]. Dostupné z: http://slideplayer.cz/slide/2019156/

[15] JAŠEK, Roman. *Informační a datová bezpečnost.* Zlín: Univerzita Tomáše Bati ve Zlíně, 2006. ISBN 80-7318-456-7.

[16] KAMENÍK, J, BRABEC. F a kol. *Komerční bezpečnost. Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur.* Vyd. 1. Praha: ASPI, a.s. 2007. ISBN 978-80-7357-309-6.

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

[18] PŘIBYL, T. *ICT security*. Bezpečnostní politika v praxi. [online]. 2010 [cit. 2016-11-27]. Dostupné z: http://www.ictsecurity.cz/odborne-clanky/bezpecnostni-politika-v-praxi.html

[19] SMEJKAL, V, RAIS, K. *Řízení rizik ve firmách a jiných organizacích.* Praha: Grada, 2013. ISBN 978-80-247-4644-9.

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

[21] STŘÍŽOVÁ, V. a kol. *Organizace v podmínkách informační společnosti.* Praha: Vysoká škola ekonomická v Praze, Nakladatelství Oeconomica, 2014. ISBN 978-80-245-2072-8.

[22] TVRDÍKOVÁ, Milena. *Aplikace moderních informačních technologií v řízení firmy*. 1. Vyd. Praha: Grada, 2008. ISBN 978-80-247-2728-8.

[23] ŽABA, Zdeněk. *Bezpečnostní politika*. [online]. 2003 [cit. 2016-11-27]. Dostupné z: http://slideplayer.cz/slide/3390816/