Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Bezpečnost informací

Bakalářská práce

Autor: Erik Vojtěch
Studijní obor: Aplikovaná informatika

Vedoucí práce: Ing. Ladislav Balík

Hradec Králové leden 2016

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

……

V Hradci Králové dne 27. 4. 2016 Erik Vojtěch

Poděkování:

Tímto bych rád poděkoval svému vedoucímu bakalářské práce Ing. Ladislavu Balíkovi za jeho odbornou pomoc, cenné rady a metodické vedení, které mi pomohly při psaní bakalářské práce.

Anotace

Tato bakalářská práce se zabývá zajištěním bezpečnosti informací v podniku, pomocí bezpečnostních norem. Nejprve se práce zabývá metodikou zajištění informační bezpečnosti. V další části je popsán obsah a rozdělení bezpečnostních politik. V poslední části je popis průběhu bezpečnostní analýzy rizik a její provedení u konkrétní organizace. Výstupem práce jsou výsledky samotné analýzy, a návrhy řešení nalezených nedostatků pomocí vhodných bezpečnostních opatření.

Annotation

Title: Information security

This bachelor thesis deals with ensuring security of information in a company, by using safety standards. At first, thesis deals with methodology to ensure information security. Next part describes content and distribution of security policy. In the last part, there is a description of the security risk analysis and its implementation in particular organization. The outcome of this work is the results of the risk analysis itself, and proposals to address found deficiencies through appropriate security measures.

Obsah

1 ÚVOD

V dnešní době stále roste potřeba modernizace a stále více se využívá výpočetní techniky, komunikačních a informačních technologií. Při tomto tempu si také stále více podniků a organizací osvojuje nové pracovní postupy a technologie, aby dokázali držet krok s konkurencí, nebo nad nimi získali výhodu. U každé nové technologie či postupu však vznikají nová ohrožení. Ta hrozí nejčastěji při práci a manipulaci s informacemi. Může vzniknout riziko jejich úniku či poškození, což by pro organizaci mohlo znamenat výrazné ztráty. Proto se mnoho organizací začíná soustředit také na zabezpečení a ochranu nejen svých informací, ale také používaných technologií, postupů a celého chodu organizace.

Pro zvládnutí tohoto úkolu neexistuje jeden jediný postup, který je správný a lze ho aplikovat pro každý podnik. Nelze to kvůli rozdílnostem v pracovním odvětvím a strukturám organizací, proto každý přistupuje k bezpečnosti jiným způsobem. Naštěstí existují obecná bezpečnostní doporučení a legislativní nařízení, která obecně popisují způsoby ochrany či zásady, podle který se mohou organizace řídit. Tyto zásady si pak mohou sami přizpůsobit a zavést pro své vlastní potřeby. Mezi obecné standardy a doporučení lze řadit mezinárodní sadu norem ISO/IEC 27000. Tato sada obsahuje specifikace k zajištění řízení bezpečnosti informací pomocí zavedení řídicího systému. Organizace se pak řídí požadavky, které jsou uvedeny v ISO/IEC 27001 a využívá doporučených postupů podle ISO/IEC 27002. Všechna tato opatření a zásady pak podporují zajišťování vysokého stupně zabezpečení na všech úrovních organizace.

Pro kontrolu bezpečnostních opatření a celkové bezpečnosti se používá analýza rizik. Ta poskytuje informace o působících hrozbách a aktivech, která jsou vůči těmto hrozbám zranitelná. Tím vznikají rizika, která se pomocí bezpečnostních opatření snižují na přijatelnou úroveň.

2 CÍL PRÁCE

Cílem práce je popsat důležité prvky spojené s riziky a bezpečností informací uvnitř organizace, které mají vliv na celý její chod. Seznámit s metodikami a frameworky, které jsou používány při řešení bezpečnosti informací. Obeznámit s existencí a výhodami bezpečnostních politik. Poté přiblížit postupy bezpečnostní analýzy společně s metodami pro vyhledávání a postupy pro vyhodnocování informačních rizik v organizaci. Nakonec realizování analýzy rizik u konkrétní organizace a návrh vhodných bezpečnostních opatření.

3 Bezpečnost informací

V každé organizaci hrozí, že může být narušena integrita či vnitřní systémy. To má za následek vystavení citlivých informací nečekaným rizikům. Bezpečnost informací je ovlivňována prostředím, pracovními procesy, zavedenými pravidly a hlavně zaměstnanci, kteří mají k datům přístup nebo s nimi manipulují. Nejčastějšími zdroji ohrožení dat a informací jsou pak lidské chyby, technické závady, záměrné útoky a přírodní katastrofy.

Informační bezpečnost lze chápat jako ochranu informací během jejich vzniku, zpracování, ukládání, přenosů a likvidace prostřednictvím logických, technických, fyzických a organizačních opatření, která musí působit proti ztrátě důvěrnosti, integrity a dostupnosti těchto hodnot. [6]

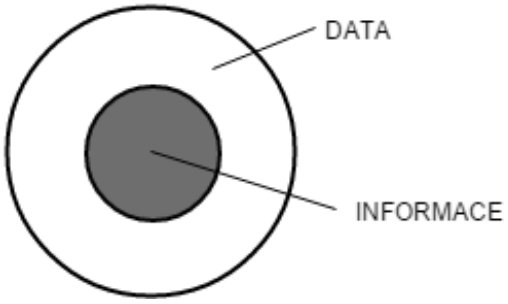
3.1 Základní pojmy

V následující části budou vysvětleny pojmy, které souvisejí s bezpečností informací.

Data

Data nebo údaje jsou fakta získaná čtením, pozorováním, výpočtem, měřením, vážením, kreslením atd. Jsou chápána jako: [14]

- vyjádření faktů a poznatků ve formě, která je vhodná pro další zpracování,
- vyjádření skutečností a myšlenek v předepsané podobě tak, aby je bylo možné přenášet a zpracovávat,
- objektivní, sledovatelné vyjádření skutečností nebo znalostí na nějakém médiu tak, že je lze předávat.



Obrázek 1 Vztah obsahu data a informace
Zdroj: Převzato z [14]

Informace

Informace je aktivum, a jako další důležitá aktiva organizace je podstatné pro činnosti organizace a následně vyžaduje odpovídající ochranu. Informace mohou být uchovávány v mnoha formách, včetně: digitální forma (například datové soubory uložené na elektronických nebo optických médiích), materiální forma (například zapsané na papíře), stejně jako nevyjádřené informace ve formě znalostí zaměstnanců. Informace mohou být přenášeny různými prostředky zahrnující kurýra, elektronickou nebo verbální komunikaci. Ať už má informace nebo prostředky, kterými je informace přenášena, jakoukoliv formu, vždy vyžaduje přiměřenou ochranu.

Informace organizace jsou závislé na informační a komunikační technologii. Tato technologie je podstatným prvkem v každé organizace a pomáhá usnadnit vytváření, zpracování, ukládání, přenášení, ochranu a zničení informací. [2]

Informační systém

Představuje konzistentní uspořádanou množinu komponent spolupracující za účelem tvorby, shromažďování, zpracování, přenášení a rozšiřování informací. Prvky informačního systému tvoří lidé, respektive uživatelé informací, a informatické zdroje. Komponenta je tvořena jedním nebo více prvky. [15]

Narušení bezpečnosti

Narušení lze chápat jako aktivní posloupnost odpovídajících událostí, které se záměrně snaží uškodit takovou měrou, že napadený systém je poté nepoužitelný. Při narušení dochází ke zpřístupnění informací neautorizovaným osobám nebo k nepovolené manipulaci s informacemi. [10]

Systém detekce narušení

Systém IDS může být definován jako soubor nástrojů, metod a zdrojů, které nám pomáhají identifikovat, zpřístupnit a hlásit neautorizované a neschválené síťové aktivity. [10]

Bezpečnost

Pojem bezpečnost lze chápat jako vlastnost nějakého objektu nebo subjektu (informačního systému či technologie), která určuje stupeň nebo míru jeho ochrany proti možným škodám a hrozbám. [14]

Důvěrnost

Důvěrnost je zatajování informací nebo zdrojů před neoprávněnými uživateli. Potřeba držení tajných informací vyplývá z využívání počítačů v citlivých vládních a podnikových oblastech. [1]

Integrita

Integrita se týká důvěryhodnosti dat nebo zdrojů, a to obvykle pokud jde o prevenci nesprávného nebo neautorizovaného pokusu o jejich změnu. Integrita zahrnuje datovou integritu (obsah informací) a původovou integritu (zdroj dat, často nazýván jako autentizace). [1]

Dostupnost

Dostupností se rozumí schopnost použít informace nebo zdroje v momentě, kdy jsou požadovány. Bezpečnostní aspekt dostupnosti je takový, že někdo může úmyslně odepřít přístup k datům či službám, a ty se pak stanou pro uživatele nedostupné. [1]

3.1.1 Definice z oblasti analýzy rizik

Aktivum

Aktivum je všechno, co má pro subjekt analýzy hodnotu. Tato hodnota může být zmenšena působením hrozby. Aktivum může být i sám subjekt, neboť hrozba může působit na celou jeho existenci. Hodnota aktiv je založena na objektivním vyjádření vnímané ceny nebo na subjektivním ocenění důležitosti (kritičnosti) aktiva. [16]

Za nejcennější aktiva se považují peníze, majetek a především data a informace, jejichž zneužití, ztráta nebo modifikace by organizaci nebo osobě způsobily určitou škodu. [14]

Hrozba

Hrozba je síla, událost, aktivita nebo osoba, která má nežádoucí vliv na bezpečnost nebo může způsobit škodu. Hrozbou může být například požár, přírodní katastrofa, krádež zařízení, získání přístupu k informacím neoprávněnou osobou nebo chyba obsluhy. Základní charakteristikou hrozby je její úroveň. Ta se hodnotí podle schopnosti hrozby způsobit škodu, pravděpodobnosti jejího výskytu a motivaci nebo zájmu iniciovat hrozbu vůči aktivu. [16]

Zranitelnost

Zranitelnost je nedostatek, slabina nebo stav analyzovaného aktiva (případně subjektu nebo jeho části), který může hrozba využít pro uplatnění svého nežádoucího vlivu. Tato veličina je vlastností aktiva a vyjadřuje, jak citlivé je aktivum na působení dané hrozby. Zranitelnost vzniká všude tam, kde dochází k interakci mezi hrozbou a aktivem. Zranitelnost aktiva se hodnotí podle jeho náchylnosti být poškozeno danou hrozbou a důležitosti aktiva pro podnik. [16]

Protiopatření

Protiopatření je postup, proces, procedura, technický prostředek nebo cokoliv, co bylo speciálně navrženo pro zmírnění působení hrozby (její eliminaci), snížení zranitelnosti nebo dopadu hrozby. Protiopatření jsou navrhována s cílem předejít vzniku škody nebo s cílem usnadnit překlenutí následků vzniklé škody. [16]

Riziko

Riziko vzniká vzájemným působením hrozby a aktiva. Hrozba, která nepůsobí na žádné aktivum, nemusí být při analýze rizik brána v úvahu. Aktivum, na které nepůsobí žádná hrozba, není předmětem analýzy rizik. [16]

3.2 Historie

Informační bezpečnost, dříve nazývaná počítačová bezpečnost, se začala řešit po nasazení prvních počítačů. Počáteční období se řadí do konce 80. let, kdy počítačová bezpečnost byla spojována hlavně s utajovanými informacemi a státními

složkami. Bylo využíváno speciálních šifrovacích automatů, které nikdy nebyly komerčně vyráběny. Větší zájem o bezpečnost podnítila až existence počítačových virů, které zaznamenaly vysoký vzestup v období kolem roku 1985. Až počátkem 90. let začal zájem o obor informační bezpečnost výrazně stoupat. Byla zahájena výuka kryptografie a začaly vznikat komerční bezpečnostní produkty. Také bylo vytvořeno oddělení počítačové kriminality a v roce 1992 by přijat první zákon o ochraně osobních dat. [9]

3.3 Informační bezpečnost

Způsoby ochrany se liší podle toho, co chce organizace chránit a jakou hodnotu chráněné objekty představují. U informační bezpečnosti jsou předmětem ochrany nejčastěji technická vybavení, programové vybavení, smlouvy, informace, data a datové struktury.

Bezpečnost informací a informačního systému se realizuje za pomocí bezpečnostních mechanismů a opatření. Ty se děli do několika skupin, které jsou popsány dále.

3.3.1 Organizační opatření

Organizační opatření jsou realizována formou vnitropodnikových nařízení a směrnic, které musejí zahrnovat veškerou činnost informačního systému, řešení krizových stavů a zásady personální bezpečnosti. Tyto směrnice vymezují a delegují zodpovědnost každého pracovníka za konkrétní věc. Všechna organizační opatření musí být vydána písemně a musí s nimi být seznámeni všichni zaměstnanci. Opatření je také potřeba pravidelně prověřovat, zda odpovídají reálné situaci. Patří sem zásady a pravidla pro používání technického vybavení, pravidla pro práci s hesly, postupy pro identifikaci uživatelů, apod. [6]

3.3.2 Fyzická opatření

Jsou všechna opatření, použitá k zajištění fyzické ochrany informačního systému proti náhodným a úmyslným hrozbám. Informační systém je umístěn v určitém fyzickém prostředí, které tvoří budovy a místnosti v nich. Úkolem fyzických opatření je zabezpečení budov, ve kterých je informační systém umístěn,

jeho ochrana před přírodními vlivy a opatření proti neoprávněnému vniknutí. Fyzická opatření slouží také k zajištění bezpečného uložení datových nosičů s informacemi a tiskových výstupů, ochraně proti přírodním živlům a požáru, zajištění nepřetržité dodávky elektrické energie. [6]

3.3.3 Technická opatření

Technická opatření zahrnuje nasazení technických prostředků (hardware) do informačního systému. Řadí se mezi ně například i ochrana technických prostředků před elektromagnetickým zářením. [6]

3.3.4 Programová opatření

Programová opatření chrání informace přímo v počítačích pomocí programových bezpečnostních prostředků. Hlavní účel těchto opatření spočívá v kontrole přístupu neoprávněných osob k informacím, ohlašování pokusů o narušení, a monitorování činností a podezřelých aktivit uživatelů. [6]

3.3.5 Šifrování

Kryptografie poskytuje řadu šifrovacích technik k utajení obsahu dat a zpráv, aby byly zabezpečené při ukládání a přenosu. Šifrování transformuje data do podoby, která není běžnými prostředky čitelná. V případě odcizení šifrovaných dat tak nedojde k úniku informací (pokud nedojde k vyzrazení šifrovacího klíče). [6]

3.3.6 Zálohování

Jedná se o proces, při kterém se v daném čase vytvoří jedna nebo více kopií požadovaných informací na záložních datových nosičích. Využívá se hlavně jako prevence a pojistka pro případ výpadku systému, jeho selhání nebo jiných katastrof. Pomocí záloh lze pak systém uvést zpět do původního nepoškozeného stavu. [6]

3.3.7 Antivirová ochrana

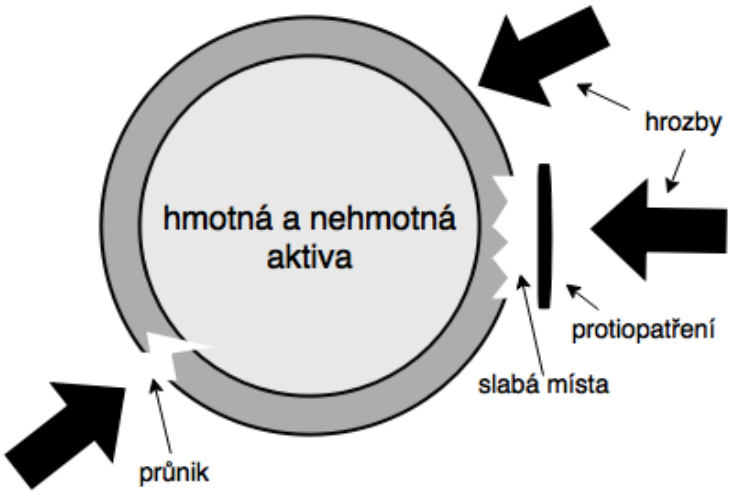
Antivirové nástroje chrání operační systémy před nákazou, jako jsou různé druhy virů, trojské koně, červi, spyware, malware a dalším podvodným software. Obsahují funkce jako skenování virů, heuristická analýza, ověřování kontrolních součtů, rezidentní ochrana a virové pasti. [6]

3.4 Hrozby

Při práci s informacemi a informačním systémem může, při nedodržení bezpečnostních pravidel a postupů, docházet k nechtěným chybám. Hrozby působí na celý informační systém, a jejich působení se omezuje pomocí bezpečnostních opatření. Objekty, které se nachází v počítačových systémech a jsou vystavovány nebezpečí, jsou například technická zařízení, programové vybavení, veškerá data společnosti, záznamová média, počítačové sítě a důležití lidé.

Nejčastěji se jedná o tyto hrozby: [14]

- **Přerušení**, kdy některá část systému je ztracena nebo nedosažitelná.
- **Zachycení,** znamená skutečnost, že neautorizovaný subjekt získá přístup k nějakému objektu systému a útočník tak zachytí a získá některé citlivé informace.
- **Modifikace,** vyjadřuje skutečnost, že neautorizovaný subjekt, útočník úmyslně mění, modifikuje některá data a informace či celé části systému.
- **Fabrikace,** pak znamená neautorizované vytvoření nového klamného objektu, o jehož existenci uživatel neví. Útočník pak může provádět nekontrolované akce, které narušují informační bezpečnost počítačového systému.



Obrázek 2 Působení hrozeb na informační systém
Zdroj: Převzato z [6]

Samotné hrozby lze pak rozdělit do několika kategorií:

- **Přírodní a fyzické** - živelné pohromy a nehody, jako jsou např. poruchy v dodávce elektřiny, požáry, povodně, zemětřesení;
- **Technické** – poruchy nosičů dat, počítačů nebo počítačových sítí;
- **Technologické** – poruchy způsobené škodlivými programy (viry, trojské koně apod.);
- **Lidské** – neúmyslné, které vyplývají z neznalosti, omylů nebo zanedbání, a úmyslné, které se dělí na působící zvenčí (hackeři, teroristé, špionáž) a zevnitř (zlomyslní, zneuznaní zaměstnanci, hosté, návštěvníci organizace apod.).

4 Metodiky a frameworky

Pro řízení bezpečnosti informací vznikají soubory pravidel a doporučených metod. Současné metodiky řízení bezpečnosti informací vycházejí hlavně ze zkušeností a nejlepší praxe. K zajištění bezpečnosti se využívají také bezpečnostní standardy a postupy podporující procesy řízení IT podle nejlepších zkušeností. Hlavně se jedná se o celosvětově rozšířené metodiky COBIT, ITIL a ISO. Každá metodika má své výhody a nevýhody. Proto vždy závisí na vedení organizace, zda dokáže z těchto metodik zkombinovat to nejlepší a nejvhodnější pro své specifické potřeby a tím pak dosáhnout nejlepších výsledků, spolu s vytvořením vynikající infrastruktury IT.

4.1 COBIT

Metodika COBIT (Control Objectives for Information and Related Technology) je pevně spojena s organizací ISACA (Information Systems Audit and Control Foundation). Jedná se o sadu všeobecně přijímaných procesů, návodů pro hodnocení, ukazatelů a nejlepších praktických zkušeností, která má za cíl pomoci organizaci maximalizovat užitek plynoucí z informačních technologií. [8]

4.2 ITIL

ITIL (Information Technology Infrastructure Library) představuje soubor knih, který obsahuje popis způsobů procesního řízení služeb včetně infrastruktury IT. ITIL se koncentruje na plánování, vytváření, modifikaci, dodávku, správu, analýzu a použití služeb IT. Jejím hlavním cílem je poskytnout ucelený soubor nejlepších zkušeností pro oblast řízení služeb IT a souvisejících procesů. [8]

4.3 ISO

ISO (International Organization for Standardization) vytvořila rodinu norem, které poskytují model pro zavedení efektivního systému řízení bezpečnosti informací (ISMS) v organizaci. Tento systém je využíván za účelem zvýšení kvality ochrany svých informací. Klíčové normy toho modelu jsou ISO 27001 a ISO 27002. Kdy první z norem specifikuje požadavky na správné zavedení ISMS. A druhá poskytuje podrobný přehled bezpečnostních opatření, která mohou být využita při

budování ISMS. Certifikace vytvořeného systému řízení pak probíhá podle ISO 27001. Následuje přehled norem ISO: [2]

ISO/IEC 27000	Systémy řízení bezpečnosti informací – Přehled a slovník
ISO/IEC 27001	Systémy řízení bezpečnosti informací – Požadavky
ISO/IEC 27002	Soubor postupů pro opatření bezpečnosti informací
ISO/IEC 27003	Směrnice pro implementaci systému řízení bezpečnosti informací
ISO/IEC 27004	Řízení bezpečnosti informací – Měření
ISO/IEC 27005	Řízení rizik bezpečnosti informací
ISO/IEC 27006	Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací
ISO/IEC 27007	Směrnice pro audit systémů řízení bezpečnosti informací
ISO/IEC TR 2008	Směrnice pro audit opatření ISMS
ISO/IEC 27010	Směrnice pro řízení bezpečnosti informací pro meziodvětvové komunikace a komunikace mezi organizacemi
ISO/IEC 27011	Směrnice pro řízení bezpečnosti informací pro telekomunikační organizace na základě ISO/IEC 27002
ISO/IEC 27013	Návod pro integrovanou implementaci ISO/IEC 27001 a ISO/IEC 20000-1
ISO/IEC 27014	Správa bezpečnosti informací
ISO/IEC TR 27015	Směrnice pro řízení bezpečnosti informací pro finanční služby
ISO/IEC TR 27016	Řízení bezpečnosti informací – Organizační ekonomika

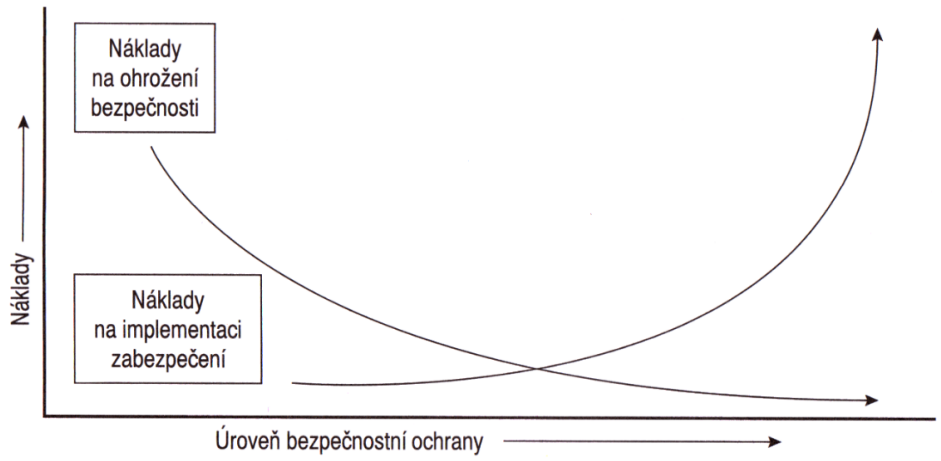
5 BEZPEČNOSTNÍ POLITIKA

Základním východiskem pro řízení ochrany organizačních systémů se nazývá bezpečnostní politika. Vyjadřuje bezpečnostní cíle, definuje zásady procesu ochrany, všechny principy, omezení, požadavky, pravidla a postupy, které určují způsob správy, ochrany a distribuce citlivých informací informačního systému. Cílem bezpečnostní politiky je minimalizovat vliv působících rizik. Podle oblasti působení a tím i různých požadavků na ochranu informací se bezpečnostní politika může velmi lišit (např. armáda, banky). Bezpečnostní politika by však neměla být chápána jako pojistka proti úniku informací nebo vzniku škody, je to prostředek, který redukuje rizika výskytu nebezpečí a určuje všeobecná pravidla a postupy pro různé systémy. [6]

Bezpečnostní politika organizace obecně vymezuje: [12]

- co vyžaduje ochranu,
- proti jakým hrozbám je ochrana budována,
- jakým způsobem se bude chránit.

Dobře navržená bezpečnostní politika podporuje návratnost investice do zabezpečení při porovnání s potenciálními ekonomickými ztrátami vzniklými z možného prolomení bezpečnosti. Náklady na zabezpečení, tedy na odstranění hrozeb a zranitelností, by neměly přesáhnout náklady vzniklé prolomením zabezpečení systému.



Obrázek 3 Rovnováha mezi náklady možného ohrožení bezpečnosti a náklady na implementaci zabezpečení
Zdroj: Převzato z [20]

5.1 Typy bezpečnostních politik

Bezpečnostní politiky se podrobněji rozdělují podle jejich specifických vlastností, priorit, na které se především soustředí a oblastí, ve kterých nalézají uplatnění. Takže je logické, že například bezpečnostní politika malého podniku se bude lišit od politiky vedené státem či bankou.

Obrázek 4 Hierarchie bezpečnostních politik
Zdroj: Upraveno podle [6]

5.1.1 Bezpečnostní politika státu

Nejvyšší postavení v řadě bezpečnostních politik zaujímá bezpečnostní politika státu. Tu tvoří především zákony a z nich odvozené předpisy, nařízení a směrnice, nařízení vlády a dokumenty s celostátně závaznou platností. Všechna výše uvedená ustanovení musí jednoznačně definovat a řešit problém, ale zároveň musí být dostatečně obecná, jinak by omezovaly resortní bezpečnostní politiky státu a bezpečnostní politiky organizací, které jsou hierarchicky na nižší úrovni. Politika státu je tvořena zejména těmito normativy: [6]

- **Zákon č. 148/1998 Sb**., o ochraně utajovaných skutečností a o změně některých zákonů [21]
- **Zákon č. 40/2009 Sb**., trestní zákoník [22]
- **Zákon č. 101/2000 Sb**., o ochraně osobních údajů a o změně některých zákonů [23]
- **Zákon č. 412/2005 Sb**., o ochraně utajovaných informací a o bezpečnostní způsobilosti [24]

Samotná bezpečnost informací je regulována především zákonem č. 101/2000 Sb., který upravuje ochranu osobních údajů a povinnosti související s ochranou informací při provozování IS, který pracuje s osobními údaji.

5.1.2 Resortní bezpečnostní politika

Jedná se o politiku podřízenou bezpečnostní politice státu. Jednotlivé podniky a resorty konkretizují individuální nařízení a směrnice pro svůj vlastní chod. Dále vyžadují speciální požadavky, které jsou specifické pro různé resorty (například ministerstva a banky), na bezpečnostní zásady a zabezpečení informačních systémů.

5.1.3 Systémová bezpečnostní politika

Na nejnižším stupni hierarchie se nachází systémová bezpečnostní politika. Tato politika detailně rozpracovává principy ochrany podle konkrétních potřeb daného systému. Dále pro ni platí, že nesmí být v rozporu s nadřazenými politikami. Pokud je informační systém obsáhlý a složitý, tak se u něj volí postup definování bezpečnostní politiky ve dvou krocích. V prvním kroku se zaměřuje na zpracování tzv. Globální systémové bezpečnostní politiky. Tato politika je v druhém kroku převedena do tzv. Detailní systémové bezpečnostní politiky, pomocí podrobné specifikace a konkretizace. [6]

5.1.4 Politiky podle zabezpečení

Bezpečnostní politiky se dále rozdělují podle jejich přístupu k bezpečnosti. Podle požadované úrovně zabezpečení lze rozpoznat bezpečnostní politiky čtyř obecných typů: [12]

- **Promiskuitní bezpečnostní politika**

je bezpečnostní politika nikoho neomezující, která každému v zásadě povoluje dělat vše, tedy i to, co by dělat neměl. IS s promiskuitní bezpečnostní politikou jsou obvykle provozně nenákladné, mnohdy ani nenutí povinně používat pro autentizaci alespoň hesla, a zaručují pouze minimální nebo vůbec žádnou bezpečnost. Důvodem používání IS s promiskuitní bezpečnostní politikou může být ekonomičnost řešení, potřebná úroveň bezpečnost může být zajišťována prostředky mimo IT.

- **Liberální bezpečnostní politika**

je bezpečnostní politika, která každému povoluje dělat vše, až na věci explicitně zakázané. Liberální bezpečnostní politika zaručuje větší bezpečí než promiskuitní politika. Liberální bezpečnostní politika je často uplatňována v prostředích, ve kterých se hrozby považují za málo až průměrně závažné a nepominutelným požadavkem je nízká ekonomická náročnost řešení bezpečnosti.

- **Opatrná bezpečnostní politika nebo Racionální bezpečnostní politika**

je bezpečnostní politika zakazující dělat vše, co není explicitně povoleno. Opatrná bezpečnostní politika je nákladnější na zavedení, avšak zaručuje vyšší stupeň bezpečnosti. Při aplikaci na obecný IS vesměs požaduje provedení klasifikace objektů a subjektů podle jejich schopností a citlivosti. Je opřena mimo jiné o zásadu povinného řízení přístupu založeného na rolích, ve kterých vystupují subjekty při styku s IS. Z hlediska používání IS v internetu je obvykle počáteční bezpečnostní politikou při zavádění firewallů.

- **Paranoidní bezpečnostní politika**

je bezpečnostní politika zakazující dělat vše potenciálně nebezpečné, tedy i to, co by nemuselo být výslovně zakazováno. Zaručuje nejvyšší stupeň bezpečnosti. Např. zakáže používat jakékoliv internetové služby (co kdyby hrozilo zneužití, ohrožení, atd.), resp. předepíše používat IS bez možnosti on-line napojení na komunikace. Politika je poté vedena k maximální izolaci systému. Paranoidní bezpečnostní politika stále může být pro mnoho organizací užitečná. Databázový

systém zpracovávající vysoce důvěrné informace lze fyzicky a technicky izolovat na systém s konečným počtem snadno kontrolovatelných vstupů a výstupů.

5.2 Obsah bezpečnostní politiky

Forma systémové bezpečnostní politiky musí mít podobu písemného dokumentu a být volně k dispozici všem uživatelům informačního systému, kteří se podílí na jejím dodržování. Tento dokument by měl být zaměstnanci prostudován ihned po nastoupení do své funkce, aby bylo zajištěno okamžitého plnění všech požadovaných částí dané politiky.

Bezpečnostní politika určuje metody a podmínky reálného řešení informační bezpečnosti a musí ve své finální podobě definovat základní postupy a metody řešení bezpečnostní problematiky. Musí také vycházet ze zásad nadřízené bezpečnostní politiky a politiky spolupracujících informačních systémů. Politiku je nutné navrhovat výhledově na delší časové období, a nikoliv pouze na aktuální stav. Všechny procedury a metody zabezpečení je nezbytné ověřit v praxi a detailně popsat jejich implementaci. I po praktickém ověření bezpečnostních mechanismů a celkového systému zabezpečení je málo pravděpodobné, že výsledek bude dokonalý. Způsoby zabezpečení je nutné neustále zdokonalovat a vyvozovat závěry a protiopatření ze zjištěných chyb. Je také vhodné průběžně sledovat počítačovou kriminalitu, nové trendy a metody zabezpečení a ze získaných poznatků vyvozovat patřičné závěry. [6]

5.2.1 Oblasti bezpečnostní politiky

Bezpečnostní politika zahrnuje a řeší tyto základní okruhy: [6]

- popis informačního systému
- cíle bezpečnostní politiky
- legislativní východiska
- definice citlivosti informací
- definice hrozeb
- definice bezpečnostních služeb
- zásady personální politiky
- zásady organizační politiky

- technické a provozní zabezpečení
- politiku zálohování
- plán obnovy po havárii
- metodiku řešení krizových stavů

Popis informačního systému

Zabezpečení musí být vždy navrhováno na konkrétní strukturu informačního systému konkrétní organizace. Bezpečnostní politika proto musí obsahovat popis organizační struktury organizace a reálného prostředí, do kterého bude budovaný informační systém umístěn. Dále bude obsahovat jeho cíle, popis úloh, které bude plnit, informační toky v rámci IS, a toky mezi IS a ostatní částí organizace. Je nutné stanovit, co všechno je informační systém, kde jsou jeho hranice, a tak i co je předmětem ochrany a jaký je vliv okolí IS, které může ovlivnit bezpečnost vlastního systému.[6]

Cíle bezpečnostní politiky

Cíle bezpečnostní politiky informačního systému přímo vyplývají z bezpečnostních cílů a požadavků organizace. Ty musejí jasně definovat bezpečnostní vlastnosti IS a priority zabezpečení informací. [6]

Legislativní východiska

Legislativní politika vymezuje právní předpisy a bezpečnostní normativy, které musí informační systém respektovat a splňovat. Definuje standardy, podle nichž se bude IS hodnotit a postup certifikace jeho bezpečnostních vlastností. Bezpečnostní politika informačního systému musí také vycházet ze zásad nadřízené bezpečnostní politiky a politiky spolupracujících informačních systémů. [6]

Definice citlivosti informací

Informace, zpracované v informačním systému, jsou klasifikovány podle citlivosti a celkového významu pro majitele. Výsledkem klasifikace informací je specifikace jednotlivých stupňů citlivosti, rozdělení informací do těchto skupin a zavedení systému označování citlivosti. [6]

Definice hrozeb

Bezpečnostní politika definuje výčet všech hrozeb, které mohou na systém působit a kterým má informační systém čelit a odolávat. [6]

Definice bezpečnostních služeb

Popisuje požadované bezpečnostní služby pro minimalizaci hrozeb, působících na IS, metody a způsoby ochrany dat a informačního systému na fyzické, organizační a logické úrovni. Dále požadavky na spolehlivost a dostupnost systému, přístupnost zdrojů, detekci chyb a odolnost proti nim. Při zkoumání nebezpečí úniku dat zpracovávaných v IS, nelze opomenout operace předcházející vlastnímu počítačovému zpracování dat a následující po něm. V těchto fázích, které bezprostředně navazují na elektronické zpracování dat počítačem, se data nalézají v různých formách a na různých typech médií, nebo je možné o jejich obsahu nebo závažnosti usuzovat z podkladů, které se v těchto fázích používají. Proto je nutné rozšířit ochranu dat i mimo vlastní elektronické zpracovávání, a to do všech fází pohybu informací. [6]

Zásady personální politiky

Bezpečnostní zásady personální politiky řeší problematiku přístupu osob k chráněným informacím, způsoby prověřování zaměstnanců a požadavky na odborné a kvalifikační kvality personálu. Všichni pracovníci organizace mají být s bezpečnostní politikou seznámeni a měla by jim být vysvětlena její důležitost i jejich role v rámci plnění bezpečnostních úloh. [6]

Zásady organizační politiky

Organizační zabezpečení IS zahrnuje především definici metod a způsobů správy a řízení informační bezpečnosti. Organizační zabezpečení stanovuje metody a způsoby koordinace informační bezpečnosti s majetkovou a osobní bezpečností organizace. Určuje orgány odpovědné za prosazování bezpečnostní politiky v rámci organizace, způsoby řešení nedostatků a bezpečnostních incidentů. Je třeba určit konkrétní osoby zodpovědné za zavedení a provozování konkrétních bezpečnost-

ních mechanismů, stanovit jim konkrétní povinnosti a odpovědnost za ochranu hodnot organizace.

Tyto zásady obsahují také metodiku vydávání a prokazování oprávnění přístupu, zásady pohybu osob, evidence dokumentů, likvidace nosičů informací, systém řízení a styk s okolním prostředím.

Měly by být popsány metody odhalování slabin systému, testování těchto slabin a popisy akcí, které je třeba podniknout v případě odhalení nové slabiny. [6]

Technické a provozní zabezpečení

Definuje požadavky na finanční zajištění nákupu, zavedení a provozu bezpečnostních mechanismů, požadavky na servisní zabezpečení provozu a časové plány řešení bezpečnosti informačního systému. [6]

Politika zálohování

Vytváření aktuálních záložních kopií systému je nutné pro zotavení informačního systému po havárii a pro překonání jakýchkoliv vzniklých škod. Konkrétní řešení zálohování závisí na počtu uživatelů a rozsahu systému, objemu a významu dat. [6]

Plán obnovy po havárii

Plán obnovy je důležitým prvkem, který podporuje kontinuitu činnosti organizace. Dovoluje jí se okamžitě vypořádat s následky havárie. Zapadá sem zotavování systému z výpadků serveru, narušení bezpečnosti nebo hurikánu. Plán obnovy má ve fázi plánování obvykle několik postupných kroků, ty však bohužel nemohou vždy odpovídat reálnému provedení, kvůli nepředvídatelné havárii. Snaha těchto plánů je hlavně zastavení působení vzniklé katastrofy vyřešení následků v co nejkratším čase. To může zahrnovat dočasné vypnutí všech systému, aby bylo možné vyhodnotit, které systémy jsou poškozeny či napadeny. [17]

Metodika řešení krizových stavů

Týká se řešení zjištěných bezpečnostních incidentů. Definuje opatření k nápravě a odstranění následků a nedostatků, eventuálně i způsoby postihnutí viníků. [6]

6 BEZPEČNOSTNÍ RIZIKA

Pod pojmem riziko si lze představit cokoliv, jelikož jeho definice není univerzální. Velmi záleží na odvětví, oboru a problematice, ve které se riziko vyskytuje. Riziko lze chápat jako nejistotu vztahující se k újmě, či v souvislosti s možným výskytem nějaké nebezpečné události. Pod jeho označením lze hledat nebezpečí fyzické, psychické nebo ekonomické. Dále označuje zvýšení četnosti a závažnosti ztrát, nebo pravděpodobnost vzniku nějaké újmy. Riziko je často jednoduše označeno jako zdroj nějakého nebezpečí. [18]

6.1 Vyhledávání rizik

Je náročná a problematická činnost, prováděná v rámci managementu rizik. Úkolem této činnosti je identifikovat nebezpečí, hrozby, zdroje jejich vzniku a odhadnout rizika, která z nich plynou.

Proces vyhledávání rizik by měl být založen na: [13]

- pozorování prostředí pracoviště – je možné využít kontrolních listů,
- identifikaci úkolů vykonávaných na pracovišti,
- posouzení všech úkolů vykonávaných na pracovišti,
- pozorování probíhající práce (kontrola postupů, které jsou stanoveny nebo se předpokládají) – podobné metodám „snímkování práce“,
- posouzení normálního průběhu práce (ke zjištění expozice zdroje rizika),
- posouzení vnějších faktorů, které by mohly ovlivnit pracoviště (například působením povětrnostních vlivů na zaměstnance pracující na venkovních pracovištích),
- zkoumání psychologických, sociálních a fyzikálních faktorů, které by mohly přispět ke vzniku stresu při práci, jejich vzájemné působení a působení spolu s jinými faktory v organizaci práce a v pracovním prostředí,
- pozornosti organizace v zájmu udržení stávajících podmínek včetně bezpečnostních opatření (například, že existují vhodné systémy

k hodnocení rizik u nových zařízení, materiálů apod. s cílem aktualizovat informace o rizicích).

Jednotlivá pracoviště nejsou nikdy zcela shodná, proto se vyhledávání provádí na všech pracovištích. Vždy je také nutné přihlížet ke změnám prostředí, okolností a podmínek na jednotlivých pracovních místech.

6.1.1 Metody vyhledávání

K vyhledávání rizik se používají různé techniky, které se liší rozsahem, časovou náročností a požadavky na prostředky. Některé jsou vhodné pouze pro specifické druhy podniků a u jiných je nelze aplikovat. Proto je doporučeno zvážit jejich kvality, potřeby podniku a vybrat nejvhodnější metodu, případně využít jejich kombinací. Vyhledávání se soustředí na objevení hrozeb, které přímo ovlivňují a ohrožují aktiva. Tyto hrozby pak představují hledaná rizika.

Následuje výčet některých metod, které se pro vyhledávání rizik využívají:

- **Kontrolní seznam** – využívá seznamu s otázkami na nedostatky a odlišnostmi provozního postupu;
- **SWIFT** – strukturovaná „Co se stane když“ technika;
- **HAZOP** – technika využívaná během nebo po projektové fázi k identifikaci a hodnocení nebezpečí v procesu;
- **Analýza SWOT** – analýza silných a slabých stránek, příležitostí a hrozeb v konkurenčním prostředí.

6.2 Vyhodnocení rizik

Po nalezení rizik následuje jejich vyhodnocení. Při hodnocení rizik je třeba dát si pozor na ohodnocení nižší hodnotou než je skutečná, nebo naopak vyšší hodnotou. Tyto dvě varianty jsou vysoce nežádoucí, protože první vede k vynaložení příliš vysokých nákladů na odstranění zanedbatelného rizika, a druhá způsobí nezabezpečení rizik, která ohrožují na životě nebo by znamenala vysoké ztráty.

Vyhodnocení rizik doprovází následující kroky: [16]

1. Určení úrovně tolerance – jaká rizika a náklady jsou přijatelné.

2. Přiřazení pravděpodobnosti rizika – podle zkušeností, vyhodnocení stavu, nebo odhadem.
3. Přiřazení nákladů rizik – ztráty jako ušlý zisk, dopad na podnikání, ztráta času či kvality.
4. Přiřazení priority rizikům – na základě úrovně tolerance, potenciálních nákladech na riziko a pravděpodobnosti, že k riziku dojde.

6.3 Stanovení opatření

Je v zájmu společnosti, aby na identifikaci a vyhodnocení rizik navazovalo stanovení opatření k omezení rizik nebo k jejich vyloučení. Závazně může zavedené opatření stanovit pouze zaměstnavatel nebo majitel. Zpracovatel vyhledávání a vyhodnocení rizik při práci má právo opatření pouze navrhnout. Při vytváření jednotlivých opatření by měla být zohledněna následující posloupnost: [13]

1. vyloučit riziko
2. nahradit nebezpečné, bezpečným nebo méně nebezpečným
3. bojovat proti riziku u zdroje
4. použít kolektivní ochranné zařízení, ne individuální ochranné prostředky
5. přizpůsobit se technickému pokroku a novým informacím
6. snažit se o zlepšení míry ochrany

Pokud nastane situace, kdy je nalezeno chybějící opatření, které přímo vyplývá z právního předpisu, je nutné navrhnout jeho plnění a upozornit na porušování těchto předpisů.

7 ANALÝZA RIZIK

Následující kapitola obsahuje seznámení se společností VIVANTIS a.s., ve které bude provedena analýza rizik. Tato analýza poskytne pohled na aktuální stav bezpečnosti a pomůže nalézt rizika, která v organizaci působí. Analýza je zaměřena na informační rizika a zranitelnosti. K vyhledání rizik je využito kontrolních listů a ohodnocení rizik je provedeno pomocí doporučení z mezinárodní sady norem ISO/IEC 27000. Pro nalezená rizika jsou pak navržena opatření, která slouží ke snižování nebo úplnému vyloučení působení těchto rizik.

7.1 Společnost VIVANTIS a. s.

Tato organizace byla vybrána jako vhodný subjekt pro analýzu bezpečnosti informací, díky vhodnému prostředí a provázanosti práce s daty a informacemi ohledně zákazníků a prodejů z provozovaných internetových obchodů.

7.1.1 Seznámení s organizací

VIVANTIS a. s. je ryze česká společnost, působící na internetovém prodejním trhu již od roku 2001. Jedná se o předního internetového prodejce v České Republice. Zabývá se především prodejem parfémů, hodinek, šperků a produktů pro zdraví a krásu. Jedná se tedy o prodejní portály parfemy.cz, krasa.cz, prozdravi.cz, sperky.cz, hodinky.cz a modnidoplnky.cz. Společnost VIVANTIS působí nejen na českém, ale také na slovenském trhu, na kterém funguje internetový e-shop Vivantis.sk. [19]

VIVANTIS a. s. je také členem Asociace pro elektronickou komerci APEK, a vlastní certifikáty APEK Certifikovaný obchod a APEK Certifikát kvality, které stvrzují, že provozovaný obchod dodržuje pravidla bezpečného a bezproblémového nákupu. Všechny internetové obchody společnosti VIVANTIS mají tedy certifikát APEK. [19]

7.2 Analýza rizik organizace

Analýza byla prováděna ve spolupráci s vedoucí IT oddělení paní Ing. Markétou Bakulovou a se správcem IT panem Petrem Kortanem.

7.2.1 Kontrolní list

K vyhledání rizik a zjištění aktuálního stavu zabezpečení byl použit kontrolní seznam. Metoda vyhledávání pomocí kontrolního listu byla vybrána, protože jde o jednu z nejjednodušších, nejpoužívanějších a zároveň velmi účinných technik pro vykonání analýzy rizik. Vytvořený seznam vychází z technické normy ČSN ISO/IEC 27001:2014 a je zaměřen na podporu provozování, udržování a zlepšování systému řízení bezpečnosti informací. Proto je vhodný pro zjištění nedostatků v zavedené informační bezpečnosti. Seznam je kvůli přehlednosti rozdělen do několika oblastí.

Tabulka 1 Kontrolní seznam - Bezpečnostní politiky

Oblast – Bezpečnostní politiky			
Rizikový faktor	**Ano**	**Ne**	**Nezjištěno**
Existuje v organizaci bezpečnostní politika	**X**		
Jsou všichni zaměstnanci a relevantní třetí strany srozuměny s její existencí a jejím dodržování?	**X**		
Probíhají kontroly a aktualizace bezpečnostní politiky?	**X**		
Jsou kontroly bezpečnostní politiky prováděny v pravidelných intervalech?	**X**		
Je prováděná mimořádná kontrola politiky vždy, když nastane významná změna v organizaci?	**X**		

Zdroj: [3]

Z prvního seznamu je patrné, že organizace splňuje veškeré požadavky z oblasti bezpečnostních politik a nevzniká žádné ohrožení z důvodů nedodržování ujednaných pravidel.

Tabulka 2 Kontrolní seznam - Organizace informační bezpečnosti

Oblast – Organizace informační bezpečnosti			
Rizikový faktor	**Ano**	**Ne**	**Nezjištěno**
Jsou veškeré odpovědnosti informační bezpečnosti definovány a přiděleny pověřeným osobám?	X		
Jsou povinnosti a oblasti odpovědností rozdělené tak, že nikdy nemá nad celým bezpečnostním systémem kontrolu pouze jedna osoba?	X		
Existují politiky nebo zavedené postupy, které určují, kdy a kým by měli být kontaktovány řídící orgány?	X		
Existuje v organizaci politika pro mobilní zařízení?		X	
Obsahuje politika pro mobilní zařízení dokumentaci rizik, která souvisejí s používáním těchto typů zařízení?		X	
Existuje v organizaci politika pro teleworking?		X	
Obsahuje politika pro teleworking bezpečnostní zásady a opatření k ochraně informací, které využívají vzdálení pracovníci?		X	

Zdroj: [3]

V organizaci chybí politika pro práci na mobilních zařízení. Tím vzniká ohrožení neoprávněného použití zařízení a následný neautorizovaný přístup k datům. V organizaci není zavedena politika pro práci z domova, protože tato možnost není zaměstnancům umožněna.

Tabulka 3 Kontrolní seznam - Bezpečnost lidských zdrojů

Oblast – Bezpečnost lidských zdrojů			
Rizikový faktor	**Ano**	**Ne**	**Nezjištěno**
Jsou zaměstnanci před nastoupením do zaměstnání prověřováni?	X		
Jsou zaměstnanci, pracovníci smluvních a třetích stran povinni podepsat dohodu o mlčenlivosti?	X		
Obsahují pracovní smlouvy ustanovení o odpovědnostech za bezpečnost informací?	X		
Jsou vedoucí pracovníci zapojeni do řízení bezpečnosti a usilují o uplatňování bezpečnostních politik a procedur?	X		
Podstupují zaměstnanci pravidelné školení z oblasti bezpečnosti, které odpovídá jejich roli a funkci v organizaci?	X		
Existuje formalizované disciplinární řízení, které dovoluje zakročit proti zaměstnancům, kteří se dopustili narušení informační bezpečnosti?	X		
Pokud odchází z firmy zaměstnanec s určitými bezpečnostní povinnostmi, je zajištěno, aby tyto bezpečnostních povinností převzal jiný zaměstnanec?	X		

Zdroj: [3]

Zajištění bezpečnosti v oblasti lidských zdrojů je na vysoké úrovni a hrozí zde opravdu minimální rizika. Stále je však důležité kontrolovat, zda jsou veškeré bezpečnostní postupy dodržovány.

Tabulka 4 Kontrolní seznam - Klasifikace a řízení aktiv

Oblast – Klasifikace a řízení aktiv			
Rizikový faktor	**Ano**	**Ne**	**Nezjištěno**
Existuje v organizaci evidence aktiv?		X	
Je evidence aktiv přesná a pravidelně aktualizovaná?		X	
Jsou informace klasifikovány s ohledem na právní požadavky, jejich hodnotu, kritičnost a citlivost?		X	
Existují pro označování a zacházení s informacemi nějaké postupy, které jsou v souladu s klasifikačním schématem?		X	
Existují v organizaci zavedené postupy pro správu přenosných médií? (USB disky, CD, DVD, přenosné HDD, …)		X	
Jsou přenosná média, která již nejsou k zapotřebí, bezpečně a spolehlivě zlikvidována?	X		
Jsou zavedená bezpečnostní pravidla pro přenos a manipulaci fyzických médií?		X	

Zdroj: [3]

V organizaci zcela chybí jakákoliv evidence aktiv, proto je velice obtížné určit zaměstnance, který je zodpovědný za ochranu jejich důvěrnosti, integrity a dostupnosti. Chybějící klasifikace informací může způsobit nechtěné vyzrazení důležitých dat, neoprávněnou modifikaci nebo neoprávněný přístup. U nechráněních fyzických médií, která zůstanou bez dozoru, hrozí únik citlivých informací.

Tabulka 5 Kontrolní seznam - Řízení přístupu

Oblast – Řízení přístupu			
Rizikový faktor	**Ano**	**Ne**	**Nezjištěno**
Je v organizaci zavedena politika řízení přístupu?	**X**		
Mají k počítačové síti a síťovým službám přístup pouze ti uživatelé, kteří byli k jejich užívání zvlášť oprávněni?	**X**		
Existuje postup pro formální registraci uživatelů, včetně jejího zrušení, který zajistí přiřazení přístupových práv?	**X**		
Existuje postup, díky kterému lze přiřazovat či odebírat přístupová práva pro všechny typy uživatelů, systémů a služeb	**X**		
Je přiřazování přístupových práv omezeno a řízeno?	**X**		
Je přiřazování uživatelských hesel řízeno formálním procesem?	**X**		
Jsou přístupová práva uživatelů kontrolována vedením organizace v pravidelných intervalech?	**X**		
Jsou přístupová práva odebrána všem uživatelům, kteří ukončili spolupráci, nebo pracovní vztah s organizací?			**X**
Je pro výběr a používání hesel dodržován stanovený bezpečnostní postup?	**X**		
Je přístup k aplikačním systémům omezen a v souladu s politikou řízení přístupu?	**X**		
Je přístup k operačním systémům řízen bezpečným postupem pro přihlašování?	**X**		
Je v organizaci využíván systém správy hesel, který zajišťuje efektivní a interaktivní posouzení kvality hesel?	**X**		
Je použití systémových nástrojů, které jsou schopné překonat systémové nebo aplikační kontroly omezeno, přísně kontrolováno a řízeno?	**X**		
Je omezen přístup ke knihovnám zdrojových kódů?	**X**		

Zdroj: [3]

Z oblasti řízení přístupu, lze vytknout pouze působící riziko neoprávněného přístupu bývalých zaměstnanců, kterým nebyla odebrána přístupová práva nebo smazán uživatelský účet.

Tabulka 6 Kontrolní seznam - Kryptografie

Oblast – Kryptografie			
Rizikový faktor	**Ano**	**Ne**	**Nezjištěno**
Je v organizaci zavedená politika obsahující pravidla pro používání kryptografických opatření na ochranu informací?			**X**
Je pro kryptografické techniky zaveden systém správy klíčů?			**X**

Zdroj: [3]

Pro ochranu přenášených informací nejsou zavedené žádné kryptografické postupy, které umožní tato data chránit a zajistit tak požadovanou úroveň důvěrnosti těchto informací, a vzniká tak riziko vyzrazení či špionáže.

Tabulka 7 Kontrolní seznam – Fyzická bezpečnost a bezpečnost prostředí

Oblast – Fyzická bezpečnost a bezpečnost prostředí			
Rizikový faktor	**Ano**	**Ne**	**Nezjištěno**
Jsou pro ochranu prostor, ve kterých se nachází informace nebo zařízení pro zpracování informací používány bezpečnostní perimetry? (chráněny prostor za pomocí bariér jako například zdi, vstupní turnikety, čipové karty, recepce, …)	X		
Jsou bezpečnostní prostory chráněny vhodným systémem kontroly vstupu, který zajišťuje přístup pouze oprávněným osobám?	X		
Jsou kanceláře, místnosti a zařízení fyzicky zabezpečené?	X		
Existují prvky fyzické ochrany proti rizikům zničení požárem, povodněmi, zemětřesením, výbuchem a dalším přírodním nebo lidmi způsobeným katastrofám?	X		
Jsou pro práci v zabezpečených oblastech dodržovány bezpečné pracovní postupy a kontroly zaměstnanců?	X		
Jsou přístupové prostory, místa pro nakládku a vykládku zboží a další místa, kterými mohou neoprávněné osoby vstoupit do prostorů organizace, kontrolovány?	X		
Jsou zařízení umístěna a chráněna tak, aby se snížilo riziko hrozeb a nebezpečí dané prostředím, a aby se omezily příležitosti pro neoprávněný přístup?	X		
Jsou podpůrná zařízení chráněna před selháním napájení a před dalšími výpadky způsobenými selháním podpůrných služeb?	X		
Jsou silové a telekomunikační kabelové rozvody, které jsou určeny pro přenos dat nebo podporu informačních služeb, chráněny před poškozením či odposlechem?	X		
Jsou zařízení správně a pravidelně udržovány pro zajištění jejich stálé dostupnosti a integrity?	X		
Je zajištěno aby, zařízení, informace a programové vybavené nebylo přemisťováno bez předchozího povolení?	X		
Jsou zařízení používaná mimo prostory organizace zabezpečené proti rizikům vyplývajících z jejich použití mimo organizaci?			X
Jsou veškerá zařízení obsahující paměťová média kontrolována tak, že je zajištěno, že před jejich likvidací nebo opakovaným použití jsou citlivá data a licencované programové vybavení odstraněna nebo přepsána?			X
Jsou zavedené bezpečnostní postupy na ochranu zařízení, která jsou bez dozoru? (automatické odhlašování, …)	X		
Je v organizaci zavedena politika bezpečného pracoviště? (čistý stůl, prázdné obrazovky, …)	X		

Zdroj: [3]

Úroveň fyzické bezpečnosti a bezpečnosti prostředí organizace je na dobré úrovni. Jediným rizikem je zde vyzrazení dat prostřednictvím vyřazených zařízení.

Tabulka 8 Kontrolní seznam - Provozní bezpečnost

Oblast – Provozní bezpečnost			
Rizikový faktor	**Ano**	**Ne**	**Nezjištěno**
Jsou provozní postupy zdokumentovány, udržovány a k dispozici všem zaměstnancům dle potřeby?	X		
Jsou veškeré změny v organizaci, obchodních procesech, zařízení pro zpracování informací a systémech, které ovlivňují informační bezpečnost kontrolovány?	X		
Jsou na ochranu proti škodlivým programům implementována opatření na jejich detekci, prevenci a nápravu spolu se zvyšováním povědomí uživatelů o těchto hrozbách?	X		
Jsou záložní kopie důležitých informací a programového vybavení organizace pořizovány a testovány v pravidelných intervalech?			X
Jsou auditní záznamy, obsahující chybová hlášení a jiné bezpečnostně významné události, pořizovány, uchovávány a přezkoumávány?			X
Jsou auditní záznamy a zařízení, která tyto záznamy pořizují, vhodným způsobem chráněny proti neoprávněnému přístupu a zfalšování?			X
Je v organizaci veden administrátorský a provozní deník?		X	
Jsou hodiny všech důležitých systémů pro zpracování informací v rámci organizace nebo domény synchronizovány se schváleným zdrojem přesného času?	X		
Je zajištěno ohlašování technických zranitelností v provozovaném informačním systému?	X		
Je u technických zranitelností vyhodnocena úroveň ohrožení organizace vůči této zranitelnosti a jsou následně přijatá příslušná opatření na pokrytí souvisejících rizik?	X		
Jsou zavedeny pravidla pro instalaci softwaru?		X	
Je audit informačního systému a kontroly provozních systému naplánovány tak, aby se nenarušovala činnost organizace?			X

Zdroj: [3]

Mezi nalezené nedostatky z oblasti provozní bezpečnosti se řadí nevytváření záložních kopií důležitých informací a zálohování dat obecně. Hrozí tak ztráta důležitých dat nebo programového vybavení. Chybějící auditní záznamy a zařízení pro jejich pořizování neumožní dohledat příčiny pozdějších bezpečnostních incidentů a bude obtížné jim přecházet. Vedení deníku nebo záznamů činnosti

administrátora může odhalit neautorizovanou činnost, pokud útočník například získá kontrolu nad účtem administrátora. Volnost při instalaci softwaru na pracovní stanice může způsobit nakažení systému škodlivým software.

Tabulka 9 Kontrolní seznam - Bezpečnost komunikace

Oblast – Bezpečnost komunikace			
Rizikový faktor	**Ano**	**Ne**	**Nezjištěno**
Jsou počítačové sítě spravovány a kontrolovány tak, aby chránily veškeré informace v systémech a aplikacích?	X		
Jsou u využívaných síťových služeb smluvně dohodnuty a zajištěny bezpečnostní požadavky organizace?			X
Jsou v počítačových sítích odděleny skupiny informačních služeb, uživatelů a informačních systémů?		X	
Jsou pro ochranu přenosu informací přes všechny typy komunikačních zařízení ustanoveny a do praxe zavedeny formální postupy, politiky, směrnice a bezpečnostní opatření?			X
Jsou elektronicky přenášené informace vhodným způsobem chráněny?	X		

Zdroj: [3]

V komunikacích hrozí neautorizovaný přístup k informacím a jejich následné zneužití. Potenciální útočník získá přehled na celou sítí a bude mu umožněno se v ní jednoduše a volně pohybovat díky chybějící segmentaci sítě.

Tabulka 10 Kontrolní seznam - Bezpečnostní incidenty

Oblast – Zvládání bezpečnostních incidentů			
Rizikový faktor	**Ano**	**Ne**	**Nezjištěno**
Jsou zavedené postupy a odpovědnosti pro zvládání bezpečnostních incidentů?			X
Jsou bezpečnostní události hlášeny příslušnými řídícími cestami ihned po jejich vzniku?			X
Jsou všichni zaměstnanci, smluvní strany, a další uživatelé informačního systému a služeb povinni zaznamenávat a hlásit jakékoliv bezpečnostní slabiny nebo podezření na bezpečnostní slabiny v systémech nebo službách?			X
Jsou znalosti získané z analýzy a řešení bezpečnostních incidentů využívány ke snížení pravděpodobnosti a rozsahu způsobených škod budoucích bezpečnostních incidentů?			X
Jsou u bezpečnostních incidentů, u kterých dojde k porušení právních předpisů, sbírány a uchovávány důkazy?			X

Zdroj: [3]

Chybějící postupy pro zvládání a zaznamenávání bezpečnostních incidentů může mít za následek opakující výskyt těchto incidentů a velmi obtížně se pak určují důvody jejich vzniku.

Tabulka 11 Kontrolní seznam - Řízení kontinuity

Oblast – Řízení kontinuity činností z hlediska bezpečnosti informací			
Rizikový faktor	**Ano**	**Ne**	**Nezjištěno**
Jsou požadavky na bezpečnost informací zahrnuty do procesu řízení kontinuity činnosti organizace?			X
Jsou vytvořeny a implementovány plány pro kontinuitu bezpečnosti informací?			X
Jsou plány pro kontinuitu bezpečnosti informací pravidelně testovány a aktualizovány?			X
Je u zařízení pro zpracování informací zajištěna jejich redundance, která postačuje na splnění požadavků na dostupnost?			X

Zdroj: [3]

Při mimořádných událostech jako je požár, povodeň, teroristický útok, loupež, výpadek elektřiny, apod., je potřeba, aby bezpečnostní služby a s ní spojené činnosti nebyly narušeny a případně byly ihned obnoveny. Hlavní hrozbou je tedy selhání bezpečnostních služeb.

7.2.2 Identifikace a ohodnocení

Metoda hodnocení aktiv organizace vychází z předepsaných doporučení normy ČSN ISO/IEC 27005:2011. Pro ohodnocení aktiv podle hodnoty, kterou představují pro organizaci je použita následující stupnice.

Tabulka 12 Stupnice hodnocení aktiv a hrozeb

Stupeň	Hodnota
0	Velmi nízká
1	Nízká
2	Střední
3	Vysoká
4	Velmi vysoká

Zdroj: Vlastní zpracování

Hodnocení je využito pro následující seznamy identifikovaných aktiv a hrozeb organizace. U aktiv označují hlavně hodnotu a důležitost, kterou představují pro organizaci. Hodnoty hrozeb značí frekvenci, s jakou se mohou různé typy ohrožení vyskytnout.

Tabulka 13 Identifikace a ohodnocení aktiv

Typ	Aktivum	Hodnocení
Budova	Hlavní budova	4
Budova	Pobočka - Praha	4
Budova	Sklad	4
Data	Data objednávek	3
Data	Databáze	3
Data	Účetnictví	4
Data	Webové stránky	3
Hardware	Access point	2
Hardware	Čtečky čárových kódů	2
Hardware	Docházkové terminály	2
Hardware	EZS	3
Hardware	Fotografické vybavení	2
Hardware	IP a mobilní telefony	1
Hardware	Pracovní stanice	3
Hardware	Projektory	2
Hardware	Stanice pro VPN	3
Hardware	Switche HP	2
Hardware	Tablety	1
Hardware	Terminálový server	3
Hardware	Tiskárny	2
Sítě	Podniková LAN	4
Sítě	Podniková WLAN	3
Sítě	VPN	4
Software	Informační systém K2	3
Software	OS Windows 8	3
Virtuální server	Aplikační server (pro K2)	4
Virtuální server	Docházkový server	2
Virtuální server	Mailový a poštovní server	2
Virtuální server	Souborový server	3
Virtuální server	Zálohovací server	2

Zdroj: Vlastní zpracování

V organizaci byla identifikována různá aktiva, se kterými se v organizaci pracuje. Největší hodnoty zde představují hlavně budovy, infrastruktura, aplikační server, účetní data. Nejníže ohodnocené je příslušenství kanceláří, které je sice nízké hodnoty, ale pro vykonávání práce je nezbytné. Následují identifikované hrozby.

Tabulka 14 Identifikace a ohodnocení hrozeb

Typ	Název	Frekvence
Fyzické poškození	Požár	1
Fyzické poškození	Úmyslné poškození zařízení	0
Lidské pochybení	Vyzrazení citlivých dat	3
Organizace	Neoprávněné použití zařízení	2
Organizace	Získání dat z vyřazených médií	1
Organizace	Krádež technické vybavení	0
Organizace	Škodlivý software	3
Organizace	Poškození dat bývalým zaměstnancem	1
Organizace	Špionáž	1
Organizace	Škodlivá činnost útočníka v síti	1
Technické selhání	Selhání zařízení	1
Technické selhání	Selhání bezpečnostních systémů	2
Ztráta služeb	Výpadek elektrické energie	1
Ztráta služeb	Výpadek webových serverů	2

Zdroj: Vlastní zpracování

Hrozby byly sestaveny z nalezených nedostatků v kontrolních listech. Doplněny byly některé obecné hrozby jako požár, výpadek elektrického proudu, a podobné, kterým se nelze vyhnout.

7.2.3 Vyhodnocení

Tabulka 15 Míra rizika

	Pravděpodobnost	velmi nízká	nízká	střední	vysoká	velmi vysoká
Dopad	velmi nízký	0	1	2	3	4
	nízký	1	2	3	4	5
	střední	2	3	4	5	6
	vysoký	3	4	5	6	7
	velmi vysoký	4	5	6	7	8

Zdroj: Vlastní zpracování

Míra rizika je vypočítána podle pravděpodobnosti působících hrozeb a jejich následnému dopadu, který se rovná hodnotám aktiv. Hodnota 0 až 2 bude znamenat nízké ohrožení a pro organizaci se riziko zařadí mezi rizika přijatelná. Míra rizika v rozmezí 3 až 5 označují střední ohrožení a představují nežádoucí rizika, která je potřeba řešit. V hodnotách 6 až 8 je ohrožení velmi vysoké a patří sem nepřijatelná rizika s nejvyšší prioritou. Tato rizika se musí řešit přednostně. V tabulce č. 17 jsou znázorněny úrovně tolerance hodnocení míry rizik.

Tabulka 16 Hodnocení míry rizik

Míra rizika	Riziko
0 - 2	Přijatelné riziko
3 - 5	Nežádoucí riziko
6 – 8	Nepřijatelné riziko

Zdroj: Vlastní zpracování

Následuje matice rizik, kde je pro jednotlivé hrozby určená zmíněná míra rizik.

Tabulka 17 Matice rizik část 1.

Matice rizik	**Frekvence hrozeb**	**Aktivum**	Hlavní budova	Pobočka - Praha	Sklad	Data objednávek	Databáze	Účetnictví	Webové stránky	Access point	Čtečky čárových kódů	Docházkové terminály	EZS	Fotografické vybavení
Dopad / Hodnota aktiv			4	4	4	3	3	4	3	2	2	2	3	2
Hrozba														
Fyzické poškození														
Požár	1		5	5	5	-	-	5	-	3	3	3	4	3
Úmyslné poškození	0		-	-	-	-	-	-	-	2	2	2	3	2
Lidské pochybení														
Vyzrazení citlivých dat	3		-	-	-	6	6	7	-	-	-	-	-	-
Organizace														
Neoprávněné použití	2		-	-	-	-	-	-	-	-	-	-	-	-
Získání dat z vyřazených médií	1		-	-	-	4	4	5	-	-	-	-	-	-
Krádež technického vybavení	0		-	-	-	-	-	-	-	2	2	2	3	2
Škodlivý software	3		-	-	-	-	-	-	-	-	-	-	-	-
Poškození dat bývalým zaměstnancem	1		-	-	-	4	4	5	4	-	-	-	-	-
Špionáž	1		-	-	-	4	4	5	-	-	-	-	-	-
Škodlivá činnost v síti	1		-	-	-	-	-	-	-	3	-	-	-	-
Technické selhání														
Selhání zařízení	1		-	-	-	-	-	-	-	3	3	3	4	3
Selhání bezpečnostních systémů	2		-	-	-	-	-	-	-	4	4	4	5	4
Ztráta služeb														
Výpadek elektrické energie	1		-	-	-	-	-	-	-	3	3	3	4	-
Výpadek www serverů	2		-	-	-	-	-	-	5	-	-	-	-	-

Zdroj: Vlastní zpracování

Tabulka 18 Matice rizik část 2.

Matice rizik	**Frekvence hrozeb**	**Aktivum**	IP a mobilní telefony	Pracovní stanice	Projektory	Stanice pro VPN	Switche HP	Tablety	Terminálový server	Tiskárny	Podniková LAN	Podniková WLAN	VPN	Informační systém K2
Dopad / Hodnota aktiv			1	3	2	3	2	1	3	2	4	3	4	3
Hrozba														
Fyzické poškození														
Požár	1		2	4	3	4	3	2	4	3	-	-	-	-
Úmyslné poškození	0		1	3	2	3	2	1	3	2	-	-	-	-
Lidské pochybení														
Vyzrazení citlivých dat	3		-	-	-	-	-	-	-	-	-	-	-	-
Organizace														
Neoprávněné použití	2		3	5	-	5	-	3	-	-	-	-	-	-
Získání dat z vyřazených médií	1		-	-	-	-	-	-	-	-	-	-	-	-
Krádež technického vybavení	0		1	3	2	3	2	1	3	2	-	-	-	-
Škodlivý software	3		4	6	-	6	-	4	6	-	-	-	-	6
Poškození dat bývalým zaměstnancem	1		-	-	-	-	-	-	-	-	-	-	-	-
Špionáž	1		-	-	-	-	-	-	-	-	5	4	-	-
Škodlivá činnost v síti	1		-	-	-	-	3	-	-	-	5	4	-	-
Technické selhání														
Selhání zařízení	1		2	4	3	4	3	2	4	3	-	-	-	-
Selhání bezpečnostních systémů	2		3	5	4	5	4	3	5	4	-	-	-	-
Ztráta služeb														
Výpadek elektrické energie	1		2	4	3	4	3	-	4	3	5	4	5	4
Výpadek www serverů	2		-	-	-	-	-	-	-	-	-	-	-	-

Zdroj: Vlastní zpracování

Tabulka 19 Matice rizik část 3.

Matice rizik	Frekvence hrozeb	Aktivum	OS Windows 8	Servery				
				Aplikační (K2)	Docházkový	Poštovní	Souborový	Zálohovací
Dopad / Hodnota aktiv			3	4	2	2	3	2
Hrozba								
Fyzické poškození								
Požár	1		-	5	3	3	4	3
Úmyslné poškození	0		-	4	2	2	3	2
Lidské pochybení								
Vyzrazení citlivých dat	3		-	-	-	-	-	-
Organizace								
Neoprávněné použití	2		-	-	-	-	-	-
Získání dat z vyřazených Médií	1		-	-	-	-	-	-
Krádež technického Vybavení	0		-	4	2	2	3	2
Škodlivý software	3		6	7	5	5	6	5
Poškození dat bývalým Zaměstnancem	1		-	-	-	-	-	-
Špionáž	1		-	-	-	-	-	-
Škodlivá činnost v síti	1		-	-	-	-	-	-
Technické selhání								
Selhání zařízení	1		-	5	3	3	4	3
Selhání bezpečnostních Systémů	2		-	6	4	4	5	4
Ztráta služeb								
Výpadek elektrické energie	1		-	5	3	3	4	3
Výpadek www serverů	2		-	-	-	-	-	-

Zdroj: Vlastní zpracování

8 SHRNUTÍ VÝSLEDKŮ

Z provedené analýzy rizik vyplývá, že v organizaci byly nalezeny hlavně rizika středního ohrožení. Tato rizika je vhodné řešit pomocí opatření, která jsou technického popřípadě organizačního charakteru. Cílem je vždy tato rizika eliminovat nebo alespoň snížit jeho působení na minimální přijatelnou hodnotu. Hrozby působí na různá aktiva, a proto se mění dopad jejich následků. V následující tabulce jsou hrozby seřazeny podle aritmetického průměru působící míry rizik jednotlivých hrozeb. Podle této tabulky lze určit nejzávažnější rizika.

Tabulka 20 Shrnutí hrozeb

#	Hrozba	Aritmetický průměr působení
1.	Vyzrazení citlivých dat	6,33
2.	Škodlivý software	5,5
3.	Výpadek webových serverů	5
4.	Špionáž	4,4
5.	Získání dat z vyřazených médií	4,33
6.	Selhání bezpečnostních systémů	4,28
7.	Poškození dat bývalým zaměstnancem	4,25
8.	Neoprávněné použití zařízení	4
9.	Škodlivá činnost útočníka v síti	3,75
10.	Výpadek elektrické energie	3,6
11.	Požár	3,59
12.	Selhání zařízení	3,28
13.	Krádež technického vybavení	2,28
14.	Úmyslné poškození	2,28

Zdroj: Vlastní zpracování

8.1 Doporučená opatření

1. Vyzrazení citlivých dat

Tato hrozba vytváří rizika hlavně kvůli nedostatečnému řízení informačních aktiv organizace. Pro eliminaci těchto rizik je doporučeno zavést důkladnou evidenci těchto aktiv. Evidence umožní snadněji určit rizika pro všechna důležitá aktiva při budoucí analýze rizik. Dále pomáhá určit vlastníka aktiva, čímž vytváří odpovědnost za dané aktivum.

V organizaci chybí klasifikace informací, která vychází ze zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Tento zákon doporučuje následující klasifikační schéma: [24]

a) Přísně tajné, vyzrazení nebo zneužití způsobí mimořádně vážnou újmu,
b) Tajné, vyzrazení nebo zneužití způsobí vážnou újmu,
c) Důvěrné, vyzrazení nebo zneužití způsobí prostou újmu,
d) Vyhrazené, vyzrazení nebo zneužití je nevýhodné.

Zmíněné schéma je využíváno hlavně pro utajované informace státu a pro informace uvedené v seznamu utajovaných informací, který je vydán vládou. Organizace nepracuje s informacemi z těchto seznamů, a proto je vhodné vytvořit vlastní schéma klasifikace informací, podle svých vlastních potřeb.

Je také doporučeno vytvořit předpisy pro zacházení s informacemi podle vytvořených schémat a zavést školení zaměstnanců, aby bylo zajištěno jejich dodržování. Pro kriticky ohrožené informace jako účetní data, lze zavést pravidelné kontroly dodržování smluvených předpisů a udělovat postihy za jejich porušení.

Zabránit neautorizovaným uživatelům v přístupu k datům je vhodné pomocí seznamu pro řízení přístupu, který je obsažen například ve službě Active Directory. Tato služba je součástí serverů se systémem Windows. Uživatelům jsou přidělována nebo odebírána oprávnění pro přístupu k vybraným objektům (datům), a tím lze zabránit v neoprávněnému přístupu a vyzrazení dat. Všechna přístupová oprávnění je důležité v pravidelných intervalech kontrolovat.

2. Škodlivý software

Proti napadení škodlivým softwarem musí být uživatelům nařízen zákaz:

- Instalovat software z jakýchkoliv externích zdrojů jako internet, CD / DVD, USB disk, a podobných na pracovní stanice.
- Přidávat vlastní spořiče obrazovky, tapety na plochu, fotografie nebo programové nástroje na pracovní stanice.

Software a jiné programové vybavení potřebné k práci, by na pracovní stanice měli instalovat výhradně správci sítě, či jiný k tomu kvalifikovaný personál.

Pro ochranu operačního systému Windows je nutné pravidelně aktualizovat databázi antivirové ochrany, operační systém pomocí záplat a ujistit se, že je v systému využíván firewall. Při použití prohlížeče Internet Explorer je nutné zapnout filtrovací funkci proti malware s názvem SmartScreen. Je vhodné také

zajistit antivirovou kontrolu elektronické pošty popřípadě se vyvarovat otevírání emailových zpráv a přiložených souborů od neznámých a podezřelých odesílatelů.

3. Výpadek webových serverů

Největším důvodem pro výpadek webových serverů je cílený DDoS útok, který může mít na svědomí konkurence, znepřátelené strany nebo hacker. Jedná se o distribuovaný útok na webové stránky, při kterých dojde k přehlcení serveru požadavky, které způsobí nedostupnost serveru pro běžné uživatele. Nefunkční webové stránky mohou pro e-shop znamenat obrovské finanční ztráty, obzvláště pokud je útok uskutečněn například o vánocích, kdy jsou prodeje a návštěvnost nejvyšší.

Pro ochranu serverů před útoky je doporučeno zavést ochranu Anti-DDoS. Na českém trhu existuje již řada poskytovatelů této služby, a mnoho dalších tuto službu zavádí a zahrnuje do svých standardních služeb. Je tedy důležité zjistit, zda podobný druh ochrany je nabízen u stávajícího provozovatele internetových obchodů a následně dohodnout zajištění podobné ochrany u ohrožených webových serverů.

4. Špionáž

Pro přenos informací mezi pobočkami se doporučuje používat virtuální privátní síť založenou na protokolu IPsec, což zajistí bezpečnou komunikaci na síťové vrstvě spolu s šifrovacími a autentizačními mechanismy. Lze také použít VPN na bázi SSL, která ovšem pracuje na aplikační vrstvě a nabízí nižší úroveň zabezpečení.

5. Získání dat z vyřazených médií

Vyřazené média a nosiče jsou především papír, optické, přenosné a pevné disky. Pro jejich bezpečné zničení nebo znehodnocení je nutné mít k dispozici prostředky, které tento úkol zvládnou. Pro papírové dokumenty slouží především skartovací zařízení a je vhodné je umístit tam kde údaje vznikají (poblíž tiskáren, počítačů …). Pro data na nosičích lze využít přepisovací software, který veškerá data nosiče několikrát přepíše, aby je nebylo možné obnovit. Další způsob je použití tzv. degausserů. Jedná se o speciální demagnetizační přístroj, který umožní trvalé odstranění zapsaných dat i z nefunkčních pevných disků či datových pásek.

6. Selhání bezpečnostních systémů

Opatření, která sníží působení této hrozby, vychází z normy ČSN ISO/IEC 27001:2014 z oblasti zajištění kontinuity bezpečnosti informací. Patří sem tato opatření: [3]

- Vytvoření požadavků na informační bezpečnost a kontinuitu řízení bezpečnosti informací během krizových situací a katastrof.
- Stanovit, zdokumentovat, zavést a udržovat procesy, postupy a opatření k zajištění vytvořených požadavků na kontinuitu řízení bezpečnosti informací během nepříznivých situací.
- Prověřování zavedených a implementovaných opatření, která zajišťují kontinuitu bezpečnosti informací v pravidelných intervalech, aby byla zajištěna jejich funkčnost a účinnost při nepříznivých situacích.

Všechna tato opatření přispívají ke snížení rizik, která vznikají působením hrozby selhání bezpečnostního systému. A zajišťují udržení požadované úrovně bezpečnosti pomocí nepřetržitého navázání fungování bezpečnostních systému a služeb během krizových situací.

7. Poškození dat bývalým zaměstnancem

Riziko lze eliminovat důkladnější správou přístupových práv a uživatelských účtů. Při ukončení pracovních vztahů musejí být danému zaměstnanci odebrána veškerá přístupová práva a odebrán uživatelský účet.

8. Neoprávněné použití zařízení

Ohrožení souvisí hlavně s neoprávněným použitím mobilních zařízení. Každý zaměstnance by měl být povinen zajistit přiměřenou ochranu neobsluhovaných zařízení, aby nedošlo ke zneužití. Popřípadě je vhodné zavést školení zaměstnanců ohledně zajišťování bezpečnosti svých zařízení. Pro pracovní stanice lze nastavit automatické odhlašování, popřípadě uzamčení heslem při neaktivitě uživatele.

9. Škodlivá činnost útočníka v síti

Proti útočníkům na počítačovou síť se doporučuje zavést systémy IPS pro prevenci průniku do sítě. Systém IPS využívá funkcí systému IDS pro detekci vniknutí a okamžitě po detekování přijímá odpovídající protiopatření proti těmto

útokům. Další možností je využití některých neautomatizovaných systémů či softwaru pro sledování aktivit a monitorování síťového provozu.

10. Výpadek elektrické energie

Problémy nejen s přerušením dodávky energie, ale také s jejími výkyvy (přepětí, podpětí, napěťové špičky, …), řeší systémy UPS. Tyto systémy slouží k zajištění nepřetržitého napájení a vytváří přepěťovou ochranu. Pro snížení působení rizik spojených s výpadkem elektrické energie je vhodné zavést tento systém u ohrožených zařízení.

11. Požár

Pro požární bezpečnost se doporučuje instalovat přenosné hasicí přístroje a automatické hasící systémy. Omezit kouření pouze na prostory k tomu určené. A provádět pravidelné protipožární školení zaměstnanců. Případně lze nainstalovat detektory kouře či systém pro elektronickou požární signalizaci. Nejdůležitějším je důkladné dodržování požárních směrnic. Ty definují postupy pro únik osob z objektů a záchranu majetku, je doporučeno vyzkoušet tyto postupy v praxi v rámci pravidelných školení zaměstnanců.

12. Selhání zařízení

Při selhání zařízení vznikají nebezpečné situace, jako například nefunkčnost bezpečnostních prvků, alarmů nebo požárních hlásičů. Dalším problémem může být nefunkční pracovní systémy a zařízení, což by znamenalo, že zaměstnanci nemůžou vykonávat svou práci. Proti těmto rizikům se lze bránit pomocí zajišťování redundantních zařízení, která ta nefunkční ihned nahradí. U technického vybavení je potřeba důkladného prověření výrobce a kontrolovat poruchovost pořizovaného zařízení. U zařízení, která pořizují a uchovávají data, je nutné provádět pravidelné zálohy. Proti poruchám pevných disků je vhodné zajistit zápis na RAID pole, které při selhání jednoho z disků může zachránit ztracená data.

9 ZÁVĚRY

První část práce zahrnuje vymezení základních pojmů týkajících se bezpečnosti informací a pojmů z oblasti analýzy rizik. Je zde také v krátkosti zmíněna historie informační bezpečnosti a důvody vzestupu vývoje tohoto odvětví. V této části jsou také způsoby ochrany, které se realizují různými typy opatření. Nakonec rozlišení druhů nebezpečí a hrozeb, které ovlivňují informace a informační systémy v organizacích.

Druhá kapitola obsahuje popis několika současně používaných metodik pro zajištění řízení informační bezpečnosti. Které se v různých ohledech liší a které také využívají bezpečnostní standardy a normy.

Ve třetí části práce jsou popsány bezpečnostní politiky, spolu s výhodami, které nám jejich zavedení přináší. Dále je znázorněno podrobné rozdělení politik podle obecné hierarchie a podle přístupu jednotlivých politik k bezpečnosti informací. Posléze je podrobně popsán obsah jednotlivých oblastí politiky.

Seznámení s riziky a procesy vyhledávání a vyhodnocování rizik je obsaženo v předposlední části práce. Současně s některými metodami pro vyhledávání a postupy při vytváření bezpečnostních opatření.

Závěrečná část práce je zaměřena na reálné provedení bezpečnostní analýzy rizik u vybrané společnosti. Analýza byla provedena ve společnosti VIVANTIS a. s. Tato část obsahuje seznámení s danou organizací, praktické použití kontrolního listu při vyhledávání rizik a následné vyhodnocení samotných rizik. Nalezená rizika, působící hrozby a doporučená opatření jsou následně shrnuta ve výsledcích.

V práci se podařilo využít kontrolního seznamu, který byl sestaven čistě z požadavků na vytváření, zavádění a udržování systému řízení informační bezpečnosti uvedených v technické normě ISO 27001. Díky zaměření této normy na informační bezpečnost bylo možné identifikovat jednotlivé hrozby a poté určit nejzávažnější z nich. Pro nežádoucí a nepřijatelná rizika byla navržena bezpečnostní opatření, která mají za úkol je eliminovat popř. snížit na přijatelnou úroveň.

10 SEZNAM POUŽITÉ LITERATURY

[1] BISHOP, Matt. *Introduction to Computer Security*. Boston: Addison-Wesley, 2005. ISBN 0-321-24744-2.

[2] ČSN ISO/IEC 27000:2014 – Informační technologie – Bezpečnostní techniky – Systém řízení bezpečnosti informací – Přehled a slovník.

[3] ČSN ISO/IEC 27001: 2014 – Informační technologie – Bezpečnostní techniky – Systém řízení bezpečnosti informací – Požadavky.

[4] ČSN ISO/IEC 27005:2013 – Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací.

[5] ČSN ISO/IEC 31000:2010 – Management rizik – Principy a směrnice.

[6] DOBDA, Luboš. *Ochrana dat v informačních systémech*. Vyd. 1. Praha: Grada, 1998, 286 s. ISBN 80-716-9479-7.

[7] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004, ix, 190 s. ISBN 80-251-0106-1.

[8] DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.

[9] DRASTICH, Martin. Systém managementu bezpečnosti informací. 1. vyd. Praha: Grada, 2011. Průvodce (Grada). ISBN 978-80-247-4251-9.

[10] ENDORF, Carl F, Eugene SCHULTZ a Jim MELLANDER. *Detekce a prevence počítačového útoku*. 1. vyd. Praha: Grada, 2005, 355 s. ISBN 80-247-1035-8.

[11] GÁLA, Libor, Jan POUR a Zuzana ŠEDIVÁ. Podniková informatika: počítačové aplikace v podnikové a mezipodnikové praxi. 3., aktualizované vydání. Praha: Grada Publishing, 2015. Management v informační společnosti. ISBN 978-80-247-5457-4.

[12] HANÁČEK, Petr a Jan STAUDEK. *Bezpečnost informačních systémů: metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií*. 1. vyd. Praha: Úřad pro státní informační systém, 2000, 127 s. ISBN 80-238-5400-3.

[13] NEUGEBAUER, Tomáš. Vyhledání a vyhodnocení rizik v praxi. 1. vyd. Praha: ASPI, 2008, 84 s. Bezpečnost práce v praxi. ISBN 9788073573560.

[14] POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005, 309 s. ISBN 80-868-9838-5.

[15] RATZAN, Lee. *Understanding Information Systems: What They Do and Why We Need Them*. Chicago: ALA Editions, 2004. ISBN 978-0838908686.

[16] SMEJKAL, Vladimír a Karel RAIS. Řízení rizik ve firmách a jiných organizacích. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013, 483 s. Expert (Grada). ISBN 978-80-247-4644-9.

[17] SNEDAKER, Susan a Chris RIMA. Business continuity and disaster recovery planning for IT professionals. Second edition. xxiii, 577 pages. ISBN 9780124105263.

[18] TICHÝ, Milík. Ovládání rizika: analýza a management. Vyd. 1. Praha: C.H. Beck, 2006, xxvi, 396 s. Beckova edice ekonomie. ISBN 80-7179-415-5.

[19] VIVANTIS a.s. internetové obchody [online]. © 2008 [cit. 2016-01-18]. Dostupné z: https://www.vivantis.cz/o-firme/

[20] WENSTROM, Michael J. Zabezpečení sítí Cisco: autorizovaný samostudijní výukový kurz. Vyd. 1. Brno: Computer Press, 2003, xxv, 753 s. Cisco systems. ISBN 80-7226-952-6.

10.1 Zákony

[21] Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů

[22] Zákon č. 40/2009 Sb., trestní zákoník

[23] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů

[24] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti

11 SEZNAM TABULEK, OBRÁZKŮ A ZKRATEK

11.1 Seznam obrázků

11.2 Seznam tabulek

11.3 Seznam zkratek

APEK	Asociace pro elektronickou komerci
CD	Compact Disc
COBIT	Control Objectives for Information and Related Technology
ČSN	Česká technická norma
DVD	Digital Video Disc
EZS	Elektronický zabezpeč
HAZOP	Hazard and Operability Analysis
HDD	Hard Disc Drive
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IPsec	Internet Protocol Security
IS	Informační systém
ISACA	Information Systems Audit and Control Foundation
ISMS	Information Security Management Systém
ISO	International Organization for Standardization
IT	Informační Technologie
ITIL	Information Technology Infrastructure Library
LAN	Local Area Network
OS	Operační systém
RAID	Redundant Array of Independent Disks
Sb.	Sbírka zákonů
SSL	Secure Sockets Layer
UPS	Nepřerušitelný zdroj napájení
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wide Area Network

Univerzita Hradec Králové
Fakulta informatiky a managementu
Akademický rok: 2015/2016

Studijní program: Aplikovaná informatika
Forma: Prezenční
Obor/komb.: Aplikovaná informatika (ai3-p)

Podklad pro zadání BAKALÁŘSKÉ práce studenta

PŘEDKLÁDÁ:	ADRESA	OSOBNÍ ČÍSLO
Vojtěch Erik	Filištínská 26, Chrudim - Chrudim I	I1200912

TÉMA ČESKY:

Bezpečnost informací

TÉMA ANGLICKY:

Information security

VEDOUCÍ PRÁCE:

Ing. Ladislav Balík - KIT

ZÁSADY PRO VYPRACOVÁNÍ:

Cíl práce:

Cílem práce je popsat důležité prvky spojené s riziky a bezpečností informací uvnitř organizace, které mají vliv na celý její chod. Seznámit s metodikami a frameworky, které jsou používány při řešení bezpečnosti informací. Obeznámit s existencí a výhodami bezpečnostních politik. Poté přiblížit postupy bezpečnostní analýzy společně s metodami pro vyhledávání a postupy pro vyhodnocování informačních rizik v organizaci. Nakonec realizování analýzy rizik u konkrétní organizace a návrh vhodných bezpečnostních opatření.

SEZNAM DOPORUČENÉ LITERATURY:

Podpis studenta: ..... **Datum:** 18.4.2016

Podpis vedoucího práce: ..... **Datum:** 18.4.2016