**VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU**

**BAKALÁŘSKÁ PRÁCE**

**Martin Vařečka**

**2011**

**bakalářská práce**

PODNIKOVÁ EKONOMIKA

|  |
| --- |
| Název BAKALÁŘSKÉ práce |
| Bezpečnost a nakládání s elektronickými dokumenty v podniku. |

|  |
| --- |
| TERMÍN UKONČENÍ STUDIA A OBHAJOBA (MĚSÍC/ROK) |
| Říjen/2011 |

|  |
| --- |
| jméno a příjmení / studijní skupina |
| Martin Vařečka / PE20 |

|  |
| --- |
| jméno vedoucího BAKALÁŘSKÉ PRÁCE |
| Ing. Miroslav Lorenc |

|  |
| --- |
| prohlášení studenta |
| Prohlašuji tímto, že jsem zadanou bakalářskou práci na uvedené téma vypracoval samostatně a že jsem ke zpracování této bakalářské práce použil pouze literární prameny v práci uvedené.  Datum a místo: 28. 8. 2011, Praha  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  podpis studenta |

|  |
| --- |
| poděkování |
| Rád bych tímto poděkoval vedoucímu bakalářské práce Ing. Miroslavu Lorencovi za metodické vedení a odborné konzultace, které mi poskytl při zpracování mé bakalářské práce. |

**VYSOKÁ ŠKOLA EKONOMIE A MANAGEMENTU**

**BEZPEČNOST A NAKLÁDÁNÍ S ELEKTRONICKÝMI DOKUMENTY V PODNIKU**

Security and handling of electronic documents in the company

Autor: Martin Vařečka

Souhrn

Tato předkládaná bakalářská práce, zabývající se problematikou bezpečnosti a nakládáním s elektronickými dokumenty v podniku, je rozdělena do dvou částí. V první, teoretické části jsou vymezeny dílčí oblasti, které působí a ovlivňují celkovou úroveň bezpečnosti v podniku. Volba těchto oblastí vychází ze skutečné situace řešené problematiky v podniku a dále z požadavků na bezpečnost informací vyplývajících z ISMS. Mezi hlavní dílčí oblasti patří klasifikace informací a dokumentů, řízení přístupu k nim a fyzická ochrana provozu výpočetních prostředků s informacemi. Ve druhé, praktické části je na vybraném podnikatelském subjektu provedena analýza jeho situace v uplatňování bezpečnostních principů při řízení bezpečnosti provozu a nakládání s elektronickými dokumenty. Výstupy o praktickém vypořádání problematiky jednotlivých oblastí, které musí podnik řešit, jsou hodnoceny z pohledu naplňování teoretických požadavků řízení bezpečnosti elektronických dokumentů. V závěru se práce věnuje shrnutí zjištěných výstupů a uvádí nástin doporučení a návrhů přinášejících podniku zlepšení v dané problematice.

Summary

This presented thesis dealing with safety difficulties and handling of electronic documents in the enterprise is divided into two parts. In the first, theoretical part, are defined the sub-areas, which affect the overall level of security in the enterprise. The choice of these areas is based on the actual situation of the issue that is being solved in the enterprise and further on the information security requirements resulting from the ISMS. The main individual areas include classification of information and documents, their control access and physical protection of the operation of computing resources with information. In the second, practical part, an analysis of the situation in the application of safety principles in managing its security operations and management of electronic documents is applied on the selected business entity. Outputs on the practical settlement of problems in individual areas, which the company must deal with, are evaluated in terms of fulfilling the theoretical requirements of safety management of electronic documents. In conclusion, the thesis is dedicated to a summary of the detected outputs and outline recommendations and proposals for bringing company to improve in this area.

Klíčová slova:

Bezpečnost, elektronický dokument, informace, informační technologie, ISMS.

Keywords:

Security, electronic document, information, information technology, ISMS.

JEL Classification:

C890 - Data Collection and Data Estimation Methodology; Computer Programs: Other

L860 - Information and Internet Services; Computer Software

M150 - IT Management

O300 - Technological Change; Research and Development: General

**Obsah**

[1 Úvod 1](#_Toc303790443)

[2 Teoreticko-metodologická část práce 3](#_Toc303790444)

[2.1 Systém řízení bezpečnosti informací (ISMS) 4](#_Toc303790445)

[2.1.1 Klasifikace informací (dokumentů) 6](#_Toc303790446)

[2.1.2 Analýza rizik 8](#_Toc303790447)

[2.2 Správa dokumentů a obsahu 9](#_Toc303790448)

[2.3 Zálohování a archivace 10](#_Toc303790449)

[2.4 Hrozby 11](#_Toc303790450)

[2.4.1 Hrozba narušení fyzické bezpečnosti 11](#_Toc303790451)

[2.4.2 Hrozba virové infekce 12](#_Toc303790452)

[2.4.3 Hrozba selhání výpočetního vybavení 13](#_Toc303790453)

[3 Analytická/praktická část práce 14](#_Toc303790454)

[3.1 Zavedený systém ISMS 15](#_Toc303790455)

[3.1.1 Řízení rizik 16](#_Toc303790456)

[3.1.2 Kategorizace informací a elektronických dokumentů 18](#_Toc303790457)

[3.1.3 Vnitropodnikový informační systém (ERP) 22](#_Toc303790458)

[3.2 Řízení přístupů k dokumentům 22](#_Toc303790459)

[3.2.1 Struktura složek pro práci s dokumenty 23](#_Toc303790460)

[3.2.2 Používání přenosných datových nosičů 26](#_Toc303790461)

[3.3 Zálohování elektronických dat 27](#_Toc303790462)

[3.4 Hrozby ovlivňující bezpečnost elektronických dokumentů 28](#_Toc303790463)

[3.4.1 Ohrožení fyzické bezpečnosti při provozu elektronických dat 29](#_Toc303790464)

[3.4.2 Virové hrozby 31](#_Toc303790465)

[3.4.3 Selhání počítačového vybavení 32](#_Toc303790466)

[4 Závěr 34](#_Toc303790467)

[Literatura 36](#_Toc303790468)

Seznam zkratek

AD Active Directory

BCM Business Continuity Management

CD Compact Disc

DRP Disaster Recovery Plan

DVD Digital Versatile Disc

ERP Enterprise Resource Planning

ICT Information and Communication Technologies

IS Information System

ISMS Information Security Management System

LAN Local Area Network

LDAP Lightweight Directory Access Protocol

HW Hardware

MPLS Multiprotocol Label Switching

OS Operation System

SLA Service Level Agreement

UPS Uninterruptible Power Supply

USB Universal Serial Bus

VPN Virtual Private Network

WAN Wide Area Network

Seznam tabulek

Tabulka 1 Kategorizace informací a dokumentů 18

Tabulka 2 Přehled bezpečnostních prvků pro jednotlivé kategorie 21

Seznam grafů

Graf 1 Zjištěné události elektronickými bezpečnostními systémy ve firmě Almax v roce 2010 30

Graf 2 Zaznamenané virové nálezy ve firmě Almax v roce 2010 31

Graf 2 Evidované poruchy hardwaru výpočetní techniky ve firmě Almax v roce 2010 33

Seznam obrázků

Obrázek 1 Organizační struktura bezpečnostního oddělení 17

# Úvod

V dnešní době silných mezifiremních konkurenčních tlaků může jakákoli chyba v úsudku nebo rozhodnutí firmy o dalším kroku v její obchodní činnosti znamenat zhoršení pozice podnikatelského subjektu na trhu nebo dokonce i jeho úpadek. Právě proto se zvyšuje potřeba chránit vnitropodnikové informace před jejich zneužitím. Každá osoba, ať již zaměstnanec nebo jinak zainteresovaný subjekt vně firmy, by měla dostat pouze ty informace, které jim přísluší. Můžeme zde uplatnit pravidlo „need to know“[[1]](#footnote-1). Dá se předpokládat, že zaměstnanec bude mít jiné požadavky a oprávnění přístupu k nakládání s vnitropodnikovými informacemi a dokumenty, než externí subjekt, ať je to už zákazník, dodavatel nebo pouze náhodný zájemce o obecné informace o daném podniku. Z toho je patrné, že na základě potřeb jednotlivých zainteresovaných skupin o tyto informace a data musí existovat jasná pravidla v přístupech k žádaným informacím a musí existovat jejich bezpečná správa, v ideálním případě s možností zpětné kontroly o přístupech. Tyto informace mohou mít různé podoby. Od subjektivních myšlenek a úvah v hlavách samotných činitelů, přes poznámky a dokumenty v papírové podobě, až po dnes převažující trend elektronické formy dat a dokumentů. Stále sílící požadavky právě na poslední zmíněnou formu správy dokumentů, tj. elektronizaci dokumentů, posilují trend využívání informačních technologií. Z toho důvodu je třeba dbát na správné nastavení informačních a komunikačních technologií (ICT) a jejich implementaci do vnitropodnikových procesů tak, aby nám pomáhaly dosahovat vysoké úrovně dostupnosti informací v čase a místě jejich využití, ale zároveň při dodržení požadované bezpečnosti.

**Cílem** předkládané práce je vymezení základního rámce oblastí, kterými můžeme ovlivňovat bezpečnost elektronických dokumentů a následné ověření jejich aplikovatelnosti v reálném podniku.

**Metodika** pro zpracování tématu je volena s ohledem na jeho komplexnost. Proto je nejprve problematika rozdělena na dílčí části. Ke specifikaci těchto oblastí se vychází jak ze základních požadavků ISMS týkajících se bezpečnosti informací a elektronických dokumentů, tak i z analýzy zjištěných souvislostí při provozu elektronických dokumentů na prostředcích ICT podniku.

Při psaní práce jsou použity teoretické vědomosti čerpané z odborné literatury tematicky zaměřené na řízení bezpečnosti informací a obecnou informatiku, které jsou podloženy osobními zkušenostmi v oboru. V praktické části je výstup pro hodnocení situace v bezpečnosti čerpán z vnitropodnikové dokumentace firmy a z interview prováděného se zástupci podniku pro danou problematiku.

Obsah práce je rozčleněn do několika částí. V úvodu je představena práce ve směru jejího zaměření a s popisem obsahového členění. Následuje teoreticko-metodologická část, ve které jsou zmíněny vybrané teoretické metody použitelné pro maximalizaci účinku ochrany dokumentů a informací v podniku. Mezi tyto součásti naplňování jisté bezpečnostní úrovně patří uplatňování ISO normy 27001[[2]](#footnote-2), možnosti správy dokumentů a jejich bezpečné uložení. Práce nahlíží na přístup k informacím jak z hlediska fyzické ochrany, tj. prostředky ochrany k zamezení neoprávněné osoby v přístupu ke kritickým prostředkům ICT (servery, počítače, komunikační prvky), tak i logické ochrany, tj. prostředky ochrany zamezující neoprávněnému přístupu k samotným elektronickým datům. V praktické části práce je analyzována situace ve zvoleném podniku, který je nejprve představen z hlediska oboru jeho podnikatelské činnosti a organizační struktury, a následně je na něm zjišťována úroveň uplatňování jak teoretických předpokladů v bezpečnosti nakládání s dokumenty, tak dodržování vnitřních předpisů podniku. Zjištěné skutečnosti jsou následně interpretovány a v závěru shrnuty v doporučení pro zlepšení situace v podniku.

# Teoreticko-metodologická část práce

Tato kapitola nám představí základní rámec teoretických postupů a přístupů, jakými můžeme vynucovat a řídit bezpečnost v nakládání s dokumenty v podniku. Abychom se ale mohli zabývat samotnou bezpečností elektronických dokumentů, je třeba si nejprve vysvětlit, co vůbec firemní dokumenty a informace jsou.

Podle J. Požára můžeme rozdíl mezi informacemi a daty chápat následovně*. „****Informace*** *jsou takové informace obíhající v organizaci, využívané v ovlivňování technologických, manažerských, informačních a jiných procesech. Týkají se především vztahů lidí k manažerské aktivitě, vztahům mezi sebou, jejich vzájemného působení, potřeb, zájmů, cílů apod. Oproti tomu* ***data*** *chápeme jako fakta získaná čtením, pozorováním, výpočtem atd. Data a údaje chápeme jako vyjádření faktů a poznatků ve formě vhodné pro další zpracování, vyjádření skutečností a myšlenek v předepsané podobě tak, aby je bylo možné přenášet a zpracovávat. Každá informace je tedy údajem, datem, ale jakákoli uložená data se nemusejí stát nutně informací.“*[[3]](#footnote-3)

Informace tedy mají také svou hodnotu a chápeme je jako aktivum organizace. Proto i informace obsažené v různých formách dat, jakými jsou i elektronické dokumenty, mají pro firmu nějakou cenu a důležitost. Vzhledem k tomu, že elektronický dokument není pouhým abstraktním pojmem, ale vyžaduje umístění na nějakém konkrétním médiu, vztahuje se i bezpečnost nejen na onen dokument, ale i na prostředí, ve kterém se technologické zařízení na uchovávání elektronických dokumentů nachází. Tím je myšleno, že je třeba se v bezpečnosti a možnostech přístupů k dokumentům pohybovat nejen v rovině technologicko-informační, ale také fyzické a personální. Pro stanovení těchto důležitých oblastí při řešení bezpečnosti ICT v podniku můžeme použít normu ISO 27001. Tato norma se metodicky věnuje bezpečnosti informací ICT, a proto se s ní v této práci blíže seznámíme.

Při stanovování přístupů k obecné bezpečnosti, nejen k elektronickým dokumentům, musíme také vycházet z konkrétní situace a možností podniku. Dá se totiž předpokládat, že důraz na bezpečnost se bude odvíjet od podnikatelské činnosti, velikosti organizace, jak co do počtu zaměstnanců nebo její složitosti v organizační struktuře, tak v geografickém umístění či dislokaci. Při rozhodování se o zvolené bezpečnosti a volbě informačního vybavení hraje také nemalou roli finanční situace a možnosti firmy, stejně tak volba firemní strategie zda je nakloněna podpoře a rozvoji informačních technologií. Firmy z bankovního sektoru kladou vyšší důraz na bezpečnost svých elektronických dat a informací než živnostník z oblasti řemeslné výroby. Stejně tak budou mít i jiné finanční možnosti, které si mohou dovolit investovat do svých informačních technologií a jejich zabezpečení. Pro většinu firem není ani žádoucí mít z vnitropodnikového prostředí nedobytnou pevnost, která neodpovídá jednotlivým úrovním chráněných informací a dat. V případě neefektivního přístupu k ochraně informací a dokumentů se může stát, že firma bude zbytečně vyžadovat vyšší restriktivní opatření, což povede ke zbytečným ekonomickým nákladům. Mají-li být tedy náklady na bezpečnost vynaloženy účelně a v rozumné míře, hovoříme podle D. Rodryčové o optimalizaci nákladů vynaložených na řešení bezpečnosti[[4]](#footnote-4).

## Systém řízení bezpečnosti informací (ISMS)

Pokud chceme zajistit bezpečnost podniku tak, aby informace i data v něm byla chráněna, musíme si nejprve uvědomit, co to vůbec bezpečnost je a za jakým účelem se jí chceme ve firmě významněji věnovat, to znamená stanovit si cíle v oblasti bezpečnosti. Bezpečnosti se věnujeme i z obchodních důvodů, stává se konkurenční výhodou. V případě vypisovaných tendrů na zakázky může být výběrové řízení podmíněno i splněním určitých bezpečnostních parametrů. Jednou z forem deklarování podniku o tom, že se úspěšně věnuje problematice bezpečnosti informací, může být vystavený certifikát pro mezinárodní normu ISO/IEC 27001:2005 – Information security management systém – Requirements (Systém řízení bezpečnosti informací – Požadavky), která vychází z britského standardu BS 7799-2[[5]](#footnote-5). Tento systém řízení bezpečnosti informací definujeme podle P. Doučka jako *„ISMS je část celkového řízení organizace, založená na přístupu (organizace) rizikům činností, která je zaměřena na ustanovení, zavádění, provoz, monitorování, přezkoumání, údržbu a zlepšování bezpečnosti informací.“[[6]](#footnote-6)* Systém řízení ISMS je založen na principu PDCA[[7]](#footnote-7). Jedná se o soubor požadavků na plnění bezpečnosti v oblasti informací, který podle P. Doučka můžeme vymezit ve čtyřech etapách[[8]](#footnote-8):

* **ustanovení ISMS:** v této etapě je třeba definovat rozsah a hranice, ve kterých bude řízení bezpečnosti aplikováno. Na základě ohodnocených rizik se vyberou bezpečnostní opatření;
* **zavádění a provoz ISMS:** cílem této etapy je efektivně a systematicky prosazovat bezpečnostní opatření;
* **monitorování a přezkoumání ISMS:** jedná se o zpětnou vazbu a hodnocení naplňování řízení bezpečnosti informací;
* **údržba a zlepšování ISMS:** jejím smyslem je neustálé zlepšování systému a odstraňování nedostatků.

Pro stanovení perimetru ochrany informací a tedy i elektronických dokumentů musí být stanoveny hranice, kde bude daná bezpečnost aplikována. Hranice jsou specifikovány jak na fyzické úrovni – objekty, místnosti, tak i na logické, technologicko-informační úrovni. Toto členění je důležité si uvědomit v kontextu možných hrozeb působících na elektronické dokumenty. Jeden a tentýž dokument může být nenávratně ztracen jak chybným smazáním uživatele, tak i odcizením celého serverového vybavení.

V převzatém výkladu od J. Mlýnka se při **zabezpečení informací** setkáváme se třemi pojmy, které musíme naplňovat[[9]](#footnote-9):

* + - * **důvěrnost**: prevence proti neoprávněnému užití informace;
      * **integrita**: prevence proti neautorizované modifikaci informace;
      * **dostupnost**: prevence proti znemožnění oprávněného použití informace.

Abychom mohli analyzovat rizika, která nám mohou ohrozit firemní aktiva tj. i dokumenty, musíme ještě definovat další používané pojmy, které mají podle J. Mlýnka následující význam[[10]](#footnote-10):

* **aktivum**, je hmotný nebo nehmotný statek, který má v ICT určitou hodnotu;
* **hrozba**, je akce nebo událost, která může způsobit záměrnou či náhodnou ztrátu nebo modifikaci informace vedoucí k negativní újmě organizace;
* **riziko**, vyjadřuje míru ohrožení aktiva, nebo se jedná o jiné vyjádření pravděpodobnosti uplatnění hrozby, vedoucí ke vzniku škody;
* **zranitelnost**, je slabé místo IS pro bezpečnost hodnoceného aktiva;
* **bezpečnostní opatření**, chápeme jako prostředek sloužící ke zmírnění působení hrozby.

Pro následující volbu úrovně zabezpečení aktiv musí být provedeno jejich ohodnocení. Zohledňujeme potenciální dopad na obchodní činnost organizace v případě trvalé či dočasné nedostupnosti aktiva, nebo potenciální dopad v případě vyzrazení nebo zneužití informačního aktiva. Samotné hodnocení aktiv provádí specialisté pro daný obor s dostatečnými kvalifikačními zkušenostmi a znalostí podniku nebo samotní ředitelé úseků.

### Klasifikace informací (dokumentů)

Klasifikaci informací a dokumentů zavádíme z důvodu efektivního řízení bezpečnosti a stanovení optimálních pravidel přístupu. V podniku se vyskytují dokumenty různých úrovní důležitosti a každá z těchto skupin je zastoupena určitou kvantitou. Organizace si proto musí dle své potřeby stanovit počet úrovní používaných pro kategorizaci informací a dokumentů. Podle J. Mlýnka se doporučuje zavést tři až čtyři klasifikační třídy[[11]](#footnote-11):

* **veřejné informace**: informace, které nevyžadují zvláštní ochranu. Jedná se o veřejně dostupné informace (př.: informace získané ve veřejném internetu). Jejich zastoupení se ve firmě odhaduje na 10%;
* **informace pro vnitřní potřebu**: jedná se o převážnou část interních dokumentů, ke kterým mají přístup zaměstnanci na základě jim přidělených pravomocí a oprávnění (př.: interní předpisy, provozní plány). Jedná se o nejpočetnější skupinu dokumentů, která pokrývá většinu firemní agendy a její výskyt se ve firmě pohybuje kolem 80%;
* **informace omezeného užití**: jsou to informace, které mají vysoce důvěrný charakter, a případné vyzrazení může vést k vážnému poškození organizace. Z toho důvodu se k těmto dokumentům maximálně omezuje přístup (např.: dokumenty strategického charakteru, finanční plány, bezpečnostní certifikáty). Z důvodu velmi omezovaného přístupu k těmto dokumentům je zastoupení této vysoce chráněné skupiny zastoupeno asi 10%.

Tyto třídy mají pak různé definice ochrany a zacházení s nimi a z toho vyplývající i rozdílné ekonomické náklady. Z toho důvodu je třeba věnovat pozornost zařazení dokumentu do správné kategorie. Právě proto musí mít každá informace, stejně tak jako aktivum, stanoveného svého **vlastníka**. Vlastníci informací jsou většinou schvalováni vyšším managementem firmy, a to z důvodu jejich odpovědnosti s jejich dalším nakládáním. Vlastník je zodpovědný za definování pravidel, jakými se bude s dokumentem zacházet, kdo k němu bude mít přístup a jaký. Dle znalosti prostředí organizace se musí definovat úroveň citlivosti informace a stanovit tak bezpečnostní režim zacházení s dokumentem. Kdyby nebyl stanoven adekvátní vlastník pro konkrétní informace a dokumenty, celá klasifikace by ztratila svůj význam. Klasifikace dokumentů by pak byla špatně zvolena a na základě chybného úsudku nezkušeného zaměstnance by tak mohlo docházet ke vzniku špatně řízeného přístupu k informaci, zvyšování rizika úniku nebo k poškození dat. Každá skupina klasifikace dokumentů také vyžaduje jiné bezpečnostní prvky ochrany a tedy i rozdílné finanční náklady. Chybné rozřazení dokumentů do skupin dle citlivosti a důvěrnosti by tak mohlo vést i k neefektivnímu mrhání prostředky firmy.

Z těchto důvodů J. Mlýnek předurčuje vlastníkovy informací a dokumentů následující povinnosti[[12]](#footnote-12):

* stanovit správnou klasifikaci informace nebo dokumentu na základě jeho ocenění a stanovené metodiky organizace;
* kvalifikovaně stanovit výši případných škod při znehodnocení dokumentu;
* v čase provádět přezkoumání platnosti a účelnosti klasifikace dokumentu;
* stanovit přístupy a bezpečnostní opatření k dokumentům.

### Analýza rizik

Jestliže máme definována firemní aktiva a známe hodnotu firemních informací a dokumentů, musíme také umět pojmenovat hrozby a rizika, která působí na tato aktiva. Při **analýze rizik** se věnujeme poznávání jednotlivých aktiv v celkovém kontextu firemní topologie. Mezi tato aktiva můžeme zařadit i vymezené informace a dokumenty. Při této deskriptivě musíme v souvislosti s citlivostí dat a vazeb k okolí přesně definovat a charakterizovat provozní prostředí, ve kterém se aktiva vyskytují. K jednotlivým charakteristikám se vytvářejí možné scénáře zranitelnosti pro jednotlivé a identifikované hrozby a stanovuje se pravděpodobnost, s jakou mohou nastat. K těmto hrozbám se musí stanovit protiopatření vedoucí ke snížení rizika poškození aktiva. Směrem k managementu je také žádoucí předkládat finanční náročnost pro jednotlivá protiopatření tak, aby vedení organizace bylo dostatečně informováno a mohlo se rozhodnout o správné volbě úrovně zabezpečení i z pohledu její efektivnosti. Některá protiopatření totiž mohou být finančně mnohem nákladnější než samotná hodnota aktiva nebo chráněné informace v dokumentu.

Za samotnou analýzou a řízením rizik stojí pečlivě vybraný a vedením organizace schválený tým specialistů s vysokou odbornou znalostí jak bezpečnostní problematiky a ICT, tak i firemní procesní bází. Tato skupina je nazývána **bezpečnostní radou firmy**[[13]](#footnote-13)a jednou z jejích činností je předkládat vedení firmy doporučující návrhy na zlepšení bezpečnosti ve firmě a prosazovat již přijatá bezpečnostní pravidla firmy. V čele bezpečnostního aparátu stojí **bezpečnostní manažer** (bezpečnostní ředitel), který bývá součástí nejvyššího vedení firmy, nebo je jím přinejmenším plně respektován. Bezpečnostnímu manažerovi jsou podřízení jednotliví **bezpečnostní manažeři organizačních jednotek**. Bezpečnostní radě mohou být k dispozici i externí bezpečnostní konzultanti, kteří přinášejí do řešené problematiky nezaujatý odborný úsudek a dokáží se tak na věc podívat i z jiného úhlu pohledu, než má samotná organizace, která si je za tímto účelem najímá.

## Správa dokumentů a obsahu

Počítače se skládají z hardwarového vybavení a tvoří použitelný základ pro fyzické umístění souboru na nich, ale ještě nám neumožňují provádět samotné operace se soubory. K tomu musí být na serveru nebo počítači nainstalován operační systém (OS), což je základní programové vybavení, které umožňuje ovládání a komunikaci všech ostatních programů, které jsou na počítači nainstalovány. Operační systém nám tedy již zajišťuje základní operace se soubory. *„****Souborem*** *je v počítačovém sytému posloupnost bitů uložených jako samostatná jednotka.“*[[14]](#footnote-14) Pro lepší orientaci při větším počtu souborů používáme k jejich logickému rozčlenění adresářů neboli složek. Akce, které mohou uživatelé se soubory provádět, závisí na právech a oprávněních, která jim systémoví administrátoři nastaví. Právem přiděleným uživateli, je mu umožněno provádět akce se soubory na serveru nebo počítači. *„****Oprávnění*** *označuje přístup, jenž má uživatel k určitým objektům, např. souborům, adresářům nebo tiskárnám.“*[[15]](#footnote-15) Oprávnění definujeme ve dvou rovinách, jednou jako oprávnění ke sdílení a podruhé jako oprávnění přiřazená systémem souboru. Pokud je složka v síti sdílená, může být uživateli přiděleno oprávnění ke čtení, modifikaci nebo k úplnému řízení obsahu složky. V případě oprávnění k souborům je ale důležité, aby byl souborový systém OS Microsoft Windows ve formátu NTFS. Pouze v něm je pak možné nastavit omezení přístupů k souborům i složkám, a to jak na lokální úrovni, tak i v síťovém provozu. Oprávnění můžeme přidělit buď explicitně na konkrétní soubor či složku, nebo může být oprávnění zděděné z nadřazeného adresáře.

V případě rozsáhlých systémů pro řízení těchto oprávnění se využívají různé varianty adresářových služeb v závislosti na použité platformě operačního systému. V případě asi nejpoužívanějšího operačního systému Windows od společnosti Microsoft hovoříme o službě **Active directory** založené na protokolu LDAP. Active directory nám umožňuje centrálně spravovat a řídit jednotlivé objekty v síti. Těmito objekty mohou být počítače, tiskárny, uživatelé a služby, které můžeme v Active directory strukturovaně seskupovat, hierarchicky členit a definovat jim vlastnosti chování v síti[[16]](#footnote-16).

## Zálohování a archivace

Velká pozornost je v řízení bezpečnosti dokumentů věnována také problematice záloh a jejímu managementu. Je třeba si uvědomit, že v záložních kopiích je většinou uložen veškerý důležitý obsah firemních dat. Z tohoto důvodu se nesmí podcenit jak samotný proces vytváření bezpečnostní zálohy, tak její následné bezpečné uložení.

Proces zálohování musí být jasně definovaný a dokumentovaný, protože se jedná mnohdy o poslední možnost opory v případě porušení nebo ztráty produkčních dat. Záloha se tak stává důležitou součástí provozu celého informačního systému. Ke každému zálohovacímu procesu musí být zvolen vlastník, který je zodpovědný za vytváření a následnou kontrolu zálohy. Zde je zapotřebí si rozdělit samotnou kontrolu do dvou úrovní. V prvé úrovni je pověřený pracovník povinen zkontrolovat, zdali se záložní kopie opravdu vytvořila. V druhé se testuje použitelnost záložní kopie, protože i když je záložní kopie produkčních dat vytvořena, může být porušena její vnitřní konzistence, a v případě obnovy dat ze zálohy by pak nemusela být bezpečnostní kopie čitelná.

Pro umístění bezpečnostních záloh volíme jiné místnosti nebo budovy, než jsou provozované zálohované servery s daty, a to z důvodu hrozeb s předpokládaným větším dopadem škod. Takovým příkladem může být požár v budově, v místech, kde jsou umístěny servery s daty. Taková záloha by pak postrádala smyslu. Pokud bude záloha uložena v bezprostřední blízkosti produkčních serverů a samotného požáru, může dojít k jejímu zničení spolu s technologickým vybavením a daty. Z tohoto důvodu volíme pro umístění záložních kopií jiné dislokované prostory. Tyto prostory by měly splňovat stejnou fyzickou bezpečnostní úroveň jako prostory se servery a produkčními daty. Nemělo by velkého významu mít vysokou fyzickou ochranu technologických datových center a zálohy mít položené na stole v nezamknuté místnosti. Pro případného útočníka je pak jednodušší zcizit takto nechráněnou záložní kopii veškerých firemních dat, než se složitě dobývat do vysoce chráněných prostor. Pro extrémně důležité zálohy, ale i jinak citlivé informace, může být vhodným prostorem bankovní nebo datový sejf. Tyto sejfy dokáží dle své třídy ochrany odolat jak samotnému požáru, tak i vysoké teplotě a ochránit tak uvnitř uložená přenosná datová média.

## Hrozby

Firemní aktiva, tedy i dokumenty, mohou být ohrožována různými riziky, která by mohla zapříčinit jejich ztrátu. Při neoprávněné modifikaci obsahu by mohl být příjemce informace uveden v omyl a poté se například chybně rozhodnout. To vše by pak mohlo vést k ohrožení funkčnosti nebo i k poškození jména firmy. Mezi takové hrozby můžeme zahrnout následující výčet.

### Hrozba narušení fyzické bezpečnosti

Do ochrany elektronických dokumentů spadá i fyzická bezpečnost tj. fyzická ochrana aktiv ve vytýčeném perimetru firmy. Při narušení fyzické bezpečnosti může dojít k ohrožení nebo zničení aktiva, na kterém jsou umístěny dokumenty s informacemi. Může se jednat o servery, počítače a media určená k přenosu a uchování dat. Takovým fyzickým ohrožením může být např. požár v budově nebo úmyslné odcizení ICT vybavení.

### Hrozba virové infekce

Modifikace obsahu dokumentu může být také provedena účelově napsaným programovým kódem – virem. Podle K. Eisenkolb můžeme vir definovat jako *„binární přívěšek výkonného souboru, tedy např. programu. Při otevření souboru se virus načte do paměti počítače. Zde se tento malý program osamostatní a provádí řadu aktivit. Mnohé viry mají za úkol poškodit systém počítače, tedy např. vymazáním souborů zničit příslušná data nebo vyřadit operační systém z provozu“*[[17]](#footnote-17).

* **Viry** mají za úkol poškodit systém počítače například smazáním důležitých souborů. Některé viry se zaměřují na vyhledání pracovních souborů uživatele, jako jsou soubory vytvořené v tabulkových a textových editorech, nebo jiných kancelářských aplikacích, a jejich následné poškození nebo úplné smazání.
* **Trojské koně** jsou programy, které se infiltrují do počítače samotným spuštěním souboru, a to díky zajímavé tématice, které uživatel podlehne a spustí si jej. Kód obsahuje sekvenci, která má destruktivní charakter a aktivuje se na nějaký impulz. Tím může být datum nebo nějaká počítačová akce uživatele. Trojský kůň se na rozdíl od viru nereplikuje.
* **Červi** jsou sebe replikující programy, které šíří své funkční kopie do jiných počítačových systémů a nevyžadují žádný hostitelský program[[18]](#footnote-18).

Jako prevence proti virové nákaze mají být firemní výpočetní prostředky opatřeny antivirovým programem, který umí vir detekovat, popřípadě ho i sám zneškodnit a zabránit tak jeho dalšímu šíření.

### Hrozba selhání výpočetního vybavení

Dalším ohrožením, se kterým je zapotřebí počítat, je neočekávaná porucha hardwarového vybavení, kde jsou dokumenty uloženy. Dnešní servery a jiná vybavení určená pro správu a uložení dat jsou vybaveny redundantními částmi systému, které v případě výpadku jedné z hlídaných komponent převezmou její funkci a systém tak může bez technologického výpadku pracovat dále. Na důležité a nosné části systému si firma může zřídit a udržovat servisní podporu externí organizace, která v případě potřeby ve smluvně dohodnutých časech a podmínkách vymění nebo jinak opraví vadnou komponentu systému. Pro tato neplánovaná selhání systémů by měly existovat plány a směrnice pro obnovu systému - DRP[[19]](#footnote-19). Ty by měly být rutinní součástí provozní IT a bezpečnostní dokumentace, protože až jejími rutinními návyky začíná firma skutečně řídit svou bezpečnost v oblasti BCM[[20]](#footnote-20).

Mezi jedny z důležitých a replikovaných částí serverů patří pevné disky nebo celá disková pole, kde jsou elektronické dokumenty uchovávány. Diskové pole je takové hardwarové spojení více nezávislých fyzických pevných disků, na které je díky řadiči diskového pole zajištěno řízení zápisu a čtení dat mezi jednotlivými disky. Tato technologie, která zvyšuje dostupnost uložených dat, se nazývá RAID (Redundant Array of Independent Disks)[[21]](#footnote-21).

# Analytická/praktická část práce

V praktické části této práce je z důvodu použití citlivých a důvěrných informací o společnosti, ve které byla analýza prováděna, změněno jméno firmy a její identifikátory, podle kterých by se dalo skutečnou firmu odvodit. Pro účely této práce budeme tedy firmu jmenovat a uvádět jako firmu „Almax“. Zjištěné informace k tématu jsou pak uváděny již v nezměněné formě.

Praktická/analytická část a získávání informací a dat ke zvolenému tématu práce o bezpečnosti a nakládání s dokumenty byla zpracována v organizaci Almax podnikající v oboru logistiky, nákupu a prodeje. Společnost Almax je jednou z nejvýznamnějších společností ve svém oboru a je součástí nadnárodní holdingové skupiny. Společnost Almax byla založena v 90. letech v Německu a již o pár let později vznikla její první pobočka i v Čechách. Od té doby se firma významně rozrostla, a jelikož český management Almaxu prokázal své odborné kvality v řízení podniku, dostal tak mandát k rozvoji své činnosti i v zahraničí. Vedle České republiky provozuje Almax svou podnikatelskou činnost v oboru ještě v dalších pěti zemích bývalého východního bloku a firma tak posílila pozici evropského lídra v oboru. V roce 2010 měla společnost Almax v ČR konsolidovaný obrat 260 milionů Euro a více než 1000 zaměstnanců. Společnost provozuje v ČR 10 logistických center a vedle svého hlavního podnikatelského oboru se věnuje i dalším obchodním aktivitám, kterými jsou projektování a výstavba parkovišť. K roku 2010 má firma zaveden integrovaný systém řízení a má vystaven certifikát jakosti ISO 9001. V roce 2010 byla společnost úspěšně auditována i na systém řízení bezpečnosti informací ISMS a obdržela certifikát ISO/EIC 27001:2005.

Společnost Almax má centrálně řízené IT s datovým centrem v Praze. Vedle již zmíněných logistických center má ještě dalších 25 administrativních poboček po celé ČR, které se připojují do datového centra vzdáleně pomocí sítě WAN. Síť WAN je vybudována na technologii MPLS[[22]](#footnote-22) v podobě pronajatých datových okruhů, spravovaných přímo telekomunikačním providerem. Na provoz celé sítě WAN má společnost Almax sepsanou rámcovou smlouvu včetně SLA[[23]](#footnote-23), která jí garantuje vysokou dostupnost sítě. K využití pronajatých okruhů, které jsou dedikovány pouze Almaxu, se firma rozhodla i z důvodu vysoké bezpečnosti technologie, protože jí garantuje, že do datového přenosu uvnitř sítě WAN nemůže vstoupit subjekt třetí strany a ohrozit tak bezpečnost provozu a důvěrnosti přenášených informací. Většina administrativně pracujících zaměstnanců je vybavena osobním počítačem nebo v případě obchodních zástupců notebookem. Pro potřeby určitého stupně mobility má zaměstnanec možnost využít, po předchozím schválení nadřízeným, vzdálený přístup do firmy. Vzdálený přístup do firemního datového centra je zprostředkován pomocí služby VPN[[24]](#footnote-24). Bez jejího úspěšného navázání nedostane zaměstnanec přístup k firemním aplikacím a sdíleným dokumentům dle jeho přiděleného bezpečnostního profilu. Podle charakteru pracovního zaměření zaměstnance a jeho potřebného stupně mobility má své dokumenty umístěné buď ve vyhrazeném sdíleném prostoru centrálního datového úložiště, nebo na svém lokálním počítači. Veškeré přístupy k vnitropodnikovým aplikacím a dokumentům jsou přísně řízeny a na každý přidělený přístup k těmto prostředkům ICT musí existovat vedoucím schválený písemný požadavek. To je i podmínkou naplňování požadavků z bezpečnostní normy ISO 27001, kterou se firma rozhodla dodržovat.

## Zavedený systém ISMS

Jak již bylo řečeno, společnost Almax je od roku 2010 úspěšně auditována pro normu ISO 27001, čímž se ale také zavázala dodržovat požadavky vycházející z této normy. Společnost si ustanovila jako rozsah a hranice pro uplatňování ISMS všechny její pobočky v ČR. Pro účely zavádění systému ISMS si Almax zvolil ve výběrovém řízení externí poradenskou firmu, která má v této oblasti dlouholeté zkušenosti. V průběhu zavádění ISMS prošli zaměstnanci několikerými školeními, které u nich prohloubily povědomí o bezpečnosti. Tato školení nadále probíhají a to dle přijatého vnitřního plánu školení zaměstnanců ve lhůtě dvakrát do roka, u vybraných klíčových zaměstnanců i častěji formou individuálních konzultací.

Zaměstnanci firmy mají volný přístup k řízené dokumentaci a směrnicím ISMS umístěným na firemním intranetu. Dokumentace je rozdělena do několika skupin. Jedná se o politiky, směrnice a prováděcí předpisy - řazeno ve vertikální hierarchii od obecných k detailním popisům s nakládáním vnitropodnikové bezpečnosti informací a v horizontálním členění na problematiku fyzické, informační a personální bezpečnosti. Veškerá dokumentace ISMS splňuje prvky řízené dokumentace, tj. na úvodní stránce dokumentu je vedle názvu vyznačena i verze, kategorie citlivosti a datum vydání dokumentu. Dále je stanoven správce a rozdělovník příjemců dokumentu a všechny stránky dokumentu jsou číslované. Společnost má vnitřními předpisy stanoven periodický půlroční interní audit, který má za úkol prověřit jakým způsobem a zda vůbec jsou v podniku dodržována přijatá bezpečnostní pravidla při nakládání s informacemi a dokumenty. Výstupy z těchto auditů jsou zpětnou vazbou pro bezpečnostní oddělení, které se tak může zaměřit na problémová místa, sjednat nápravu a efektivně plánovat rozvoj ISMS. Těmito kroky naplňuje fa Almax principy PDCA uváděných P. Doučkem.

### Řízení rizik

V organizační struktuře společnosti Almax je ustanoveno bezpečnostní oddělení, do jehož kompetencí spadá řízení a prosazování bezpečnosti uvnitř firmy, a to nejenom za pomoci direktivního vynucování směrnic ISMS, ale také kontinuálním pozvedáním bezpečnostního povědomí u zaměstnanců. Bezpečnostní skupina se schází dvakrát do měsíce a provádí vyhodnocení aktuálních bezpečnostních incidentů, řeší problematiku rozvoje bezpečnosti uvnitř firmy a předkládá nejvyššímu vedení společnosti zprávu o situaci spolu s návrhy na přijetí konkrétních bezpečnostních opatření. Organizační struktura tohoto oddělení je graficky znázorněna na obrázku 1.

Obrázek 1 Organizační struktura bezpečnostního oddělení

Zdroj: Almax, http://intranet/iso27001/p\_isms.pdf (data k 28. 7. 2011).

Zvolená struktura bezpečnostního oddělení ve firmě Almax kopíruje teoretické návrhy dle L. Gály o složení a funkci bezpečnostního aparátu firmy. Jako významný počin je vnímáno přímé zařazení bezpečnostního ředitele do nejužšího zastupitelstva firmy s respektem ostatních ředitelů. Díky tomu se u zaměstnanců lépe prosazují mnohdy i nepopulární kroky přijímané v oblasti bezpečnosti přístupu a nakládání s informacemi a dokumenty.

Společnost Almax má zpracovanou směrnici pro řízení rizik. Jejím obsahem je kromě definice pojmů i rozsáhlá Excelová tabulka, která obsahuje definovaná aktiva, mezi kterými jsou uvedeny i informace a elektronické dokumenty. K těmto aktivům jsou stanoveny hrozby a rizika s nastavitelnou váhou jejich pravděpodobnosti a účinku dopadu na firmu. Dalšími atributy nastavení hodnot určujících výslednou důležitost ochrany aktiva je stanovení úrovně důvěrnosti, integrity a dostupnosti, a to ve čtyřech stupních: nízký, střední, vysoký a kritický. Jednotlivé atributy a váhy stanovuje bezpečnostní oddělení spolu s garantem za danou problematiku a ředitelem úseku. Revize nastavení jednotlivých položek probíhá minimálně jednou za rok, pokud není okolnostmi vynucen kratší interval a následně je jako celek prezentována nejvyššímu vedení společnosti. Problematika řízení rizik ve firmě Almax a práce s pojmy převzaté v teoretické části od J. Mlýnka jsou v souladu s požadavky normy ISMS a jejich relevantnost nastavení je přezkoumávána pravidelnými audity firmy. Hlubší analýza této problematiky by zajisté dávala prostor k rozvinutí tohoto tématu pro další vědeckou práci.

### Kategorizace informací a elektronických dokumentů

Aby mohl být ve společnosti Almax uplatňován princip „need to know“, tj. aby se zaměstnanec dostal pouze k dokumentům vyplývajícím z jeho funkčního zařazení a jemu stanoveného bezpečnostního profilu, je ve společnosti, vedle řízení samotných přístupů k souborům a složkám pomocí Active directory, zavedeno i členění podle důležitosti obsahu informací v dokumentech, a to napříč celou firmou. To dává uvnitř firmy vzniknout průřezové matici přístupů k dokumentům, a to nejenom podle funkčního zařazení zaměstnance, promítnutého do nastavených oprávnění v Active directory, ale i podle samotného obsahu informací v dokumentech. Dokumenty vyskytující se uvnitř firmy jsou rozděleny do čtyř kategorií, označovaných S0 – S3 s následujícím členěním uvedeným v tabulce 1.

Tabulka 1 Kategorizace informací a dokumentů

|  |  |  |
| --- | --- | --- |
| Označení kategorie | Název kategorie | Popis kategorie |
| S3 | Tajné informace | Strategické firemní informace (strategické projekty). |
| S2 | Důvěrné informace | Informace důležité pro chod firmy (smlouvy, osobní údaje). |
| S1 | Interní informace | Vnitropodniková dokumentace dostupná všem zaměstnancům (ISO směrnice, firemní předpisy). |
| S0 | Veřejné informace | Informace určené pro zaměstnance a partnery (informace z webu, novinové články). |

Zdroj: Almax, http://intranet/iso27001/s\_adm\_bezp.pdf (data k 2. 7. 2011).

Uváděná klasifikace informací v tabulce 1 odpovídá doporučení J. Mlýnka s tou úpravou, že informace pro vnitřní potřebu jsou ve firmě Almax dále rozděleny na důvěrné informace S2 a volně dostupné interní informace S1. Toto členění umožňuje firmě pracovat s bezpečnostními profily jednotlivců i skupin potřebných pro udělení přístupu k dokumentům. Bezpečnostní profil zaměstnance vzniká na základě prověrky bezpečnostním oddělením a u požadavku k přístupu k nejcitlivějším informacím a dokumentům i za účasti člena vedení společnosti. V bezpečnostním profilu jsou uvedena možná rizika plynoucí ze zpřístupnění jednotlivých kategorií informací a dokumentů konkrétnímu zaměstnanci. Při vyhodnocování rizik plynoucích z přístupu zaměstnance k citlivým dokumentům se vychází z osobního pohovoru se zaměstnancem, prověřují se údaje v životopise a velkou váhu má i délka a průběh zaměstnaneckého poměru. Stejně jako na jednotlivce je možné požádat o stanovení bezpečnostního profilu a stanovení možných rizik i na skupinu, která je například pověřena speciálním úkolem, vyžadujícím zvláštní oprávnění přístupů k dokumentům.

V interní dokumentaci společnosti Almax je uveden výčet konkrétních dokumentů, který napomáhá zaměstnancům se lépe orientovat v klasifikaci dokumentů a správně je zařazovat do kategorií. Pouze u kategorie S3 neexistuje přesná specifikace, o jaký druh informace nebo dokumentu se jedná, protože se předpokládá, že do této kategorie patří minimum dopředu těžko předvídatelných projektů a skutečností vyžadujících speciální režim v přístupu. Prověrku k přístupu k dokumentům kategorie S3 dostává pouze vymezený okruh zaměstnanců a většinou se jedná o výše postavené osoby v organizaci firmy, které mají její vysokou důvěru.

Při práci s dokumenty jsou ve firmě Almax užívány dva pojmy, a to **vlastník dokumentu** a **uživatel dokumentu**. Při vzniku nového dokumentu je povinností zřizovatele jako vlastníka dokumentu stanovit jeho bezpečnostní kategorii. Vlastníkovi je také umožněno právo změnit kategorii, protože se předpokládá, že dokument v čase může nabývat na důležitosti a tedy i potřebě změny jeho ochrany, nebo může naopak v případě stárnutí a neaktuálnosti informace v dokumentu pozbývat na důležitosti. Povinností vlastníka dokumentu je také dbát na správné přidělení přístupových oprávnění ostatním uživatelům dotčeného dokumentu. Ustanovení vlastníka dokumentu a svěření mu pravomoci definovat výše zmíněné bezpečnostní atributy v přístupu k dokumentu jsou ve shodě s povinnostmi vlastníka uváděnými J. Mlýnkem. Naopak uživatelé, kteří přicházejí do kontaktu s klasifikovanými dokumenty, nemají možnost změnit úroveň zabezpečení a mohou s dokumentem pouze pracovat, pokud k němu mají přidělená dostatečná přístupová oprávnění. K tomu, aby se uživatelé přistupující k dokumentům dozvěděli, s jakou bezpečnostní kategorii přicházejí do styku, jsou vnitropodnikové dokumenty vytvářeny za pomocí šablon, které obsahují první stranu dokumentu jako překryvný list. Na této první stránce jsou pak vydefinovány základní informace o dokumentu včetně vlastníka dokumentu a jeho stanovené bezpečnostní kategorie. Tento překryvný list má také neopomenutelný bezpečnostní prvek v případě vytištění dokumentu na tiskárně a prací s ním v listinné podobě. Teoreticky by tak nemělo v případě ponechání volně ležícího dokumentu (např. na stole) docházet k jeho neoprávněnému čtení. Tato kategorizace má svůj smysl i ve fázi archivace dokumentů, kdy přístup k těmto archiváliím může mít pouze osoba s daným bezpečnostním oprávněním.

Jelikož s dokumenty je také zapotřebí pracovat, existuje ve společnosti Almax pro jednotlivé kategorie dokumentů, rozřazených podle citlivosti informací, definice bezpečnostních prvků, možnosti umístění dokumentů, jejich formy distribuce uvnitř a vně firmy. Zaměstnanec, který je zmocněn k tomu, aby dokument distribuoval dále třetí osobě, je povinován zodpovědností za volbu formy distribuce a případné informování příjemce o kategorii důvěrnosti dokumentu, a co z toho pro něj vyplývá. Základní výčet těchto opatření při nakládání s dokumenty, vztahujícími se k jednotlivým bezpečnostním kategoriím, je obsažen v následující tabulce 2. Pro dokumenty kategorie S0 neexistují zvláštní pravidla, protože se jedná o veřejně dostupné informace.

Tabulka 2 Přehled bezpečnostních prvků pro jednotlivé kategorie

|  |  |  |  |
| --- | --- | --- | --- |
| Opatření | Interní informace (S1) | Důvěrné informace (S2) | Tajné informace (S3) |
| Povinnost označení dokumentu | Není | Na prvním listě | Na prvním listě + vodotisk |
| Evidence počtu stran | Není | Označení počtu stran na prvním listě | Označení počtu stran na všech stranách dokumentu |
| Předání dokumentu třetí straně | Bez omezení | Musí existovat smlouva o mlčenlivosti, souhlas vlastníka dokumentu | Musí existovat smlouva o mlčenlivosti, souhlas vlastníka dokumentu a člena vedení firmy, záznam o předání |
| Přenášení dokumentů el. poštou – interně | Bez omezení | Omezit na nezbytné příjemce, bez další ochrany | Přenos dokumentů chráněn heslem, které je předáno jinou formou |
| Přenášení dokumentů el. poštou – externě | Bez omezení | Omezit na nezbytné příjemce, je-li žádoucí pak aplikovat ochranu heslem | Nepřípustné |
| Uložení na souborovém systému | Bez omezení | Pouze do určených složek, kde je omezený přístup | Dokumenty mohou být uloženy pouze lokálně |
| Revize přístupových oprávnění | 1x ročně | 1x za pololetí | 1x čtvrtletně |
| Ukládání dokumentů na mobilní počítače | Bez omezení | Pouze na nezbytně nutnou dobu a uživatel musí zajistit ochranu mobilního počítače před zcizením nebo zneužitím | Pouze v šifrované podobě a uživatel musí zajistit ochranu mobilního počítače před zcizením nebo zneužitím |
| Ukládání na výměnná média | Bez omezení | Pouze na nezbytně nutnou dobu a uživatel musí zajistit ochranu výměnného média | Pouze v šifrované podobě |

Zdroj: Almax, http://intranet/iso27001/s\_adm\_bezp.pdf (data k 2.7. 2011).

### Vnitropodnikový informační systém (ERP)

Společnost Almax má zavedený vnitropodnikový informační systém (ERP) od společnosti Microsoft, ve kterém má strukturovaně uloženou většinu svých provozních dat. Většina provozních modulů ERP byla vytvořena na zakázku. Tento informační systém ale zatím není přizpůsoben k využívání kategorizace citlivostí informací dle výše uvedeného členění S0 – S3, a to z důvodu vysokých nákladů na provedení potřebných změn. Společnost se však ve svém akčním plánu zavázala promítnout potřebné změny do další generace ERP. Dle vyjádření zástupců společnosti Almax disponuje stávající verze ERP dostatečnými mechanismy pro ochranu a řízení přístupů k jednotlivým částem sytému. Avšak připouštějí i fakt, že by promítnutí kategorizace citlivosti informací uvnitř ERP zvýšilo bezpečnost hlavně při pořizování výstupních sestav a jiných exportů dat ze systému.

## Řízení přístupů k dokumentům

Ve společnosti Almax je postup přidělování uživatelských oprávnění k prostředkům ICT řízený dle vnitropodnikové metodiky, která je závazná pro všechny zaměstnance firmy. Pro tyto účely má společnost Almax vypracovaný řízený dokument – formulář. Na tomto formuláři musí být specifikovány všechny požadované přístupy k firemním prostředkům ICT a po písemném schválení nadřízeným žadatele je tento požadavek postoupen do oddělení IT. Na sekretariátu oddělení IT je písemný požadavek digitalizován a umístěn do podnikového tiket systému, ve kterém má takto každý požadavek přidělené unikátní jednací číslo a odpovědnou osobu řešení problému. Díky tomu je možné kdykoliv dohledat historii požadavku a osobu, která se podílela na jeho řešení. Tento požadavkový tiket systém je z bezpečnostních důvodů a v něm se vyskytujících citlivých údajů vydělen od ostatních firemních systémů a slouží pouze pro účely oddělení IT. K základnímu výčtu položek na formuláři, o které musí zaměstnanec požádat, patří: přidělení e-mailu, vzdáleného přístupu do firmy prostřednictvím VPN, přístupy k jednotlivým uložištím dokumentů členěným podle funkčního zařazení zaměstnance i podle jeho bezpečnostního profilu, nebo si může vybrat ze seznamu vnitropodnikových aplikací a specifikovat v nich i oprávnění k přístupu. Ve formuláři je také ponecháno místo na volně kladený požadavek.

Zodpovědný systémový administrátor za danou oblast řízení přidělí uživateli potřebná oprávnění. Ve společnosti Almax je implementována centrální správa přístupů a oprávnění v podobě **Active directory**. Tato ověřovací služba běží pro vyšší dostupnost a bezpečnost na dvou oddělených serverech a díky nastavené synchronizaci mezi nimi dochází k replikaci všech vlastností a nastavení objektů obsažených ve strukturách Active directory. Takto zvolenou architekturou mají uživatelé sítě možnost se v případě výpadku jednoho ze serverů AD bezpečně autentizovat u druhého serveru AD a obdržet tak nejaktuálnější přidělená oprávnění k práci v síťovém prostředí firmy.

### Struktura složek pro práci s dokumenty

Počítačové servery, na kterých jsou strukturovaně uloženy dokumenty, nazýváme souborovými servery čili file servery. Jejich vnitřní hardwarové uspořádání má dnes již standartní redundantní prvky, kterými jsou zdvojený napájecí zdroj, síťové karty a to vše, stejně jako pevné disky serveru, je typu Hot plug[[25]](#footnote-25) a lze je v případě potřeby vyměnit za chodu serveru. Diskový subsystém file serverů je ve společnosti Almax vždy konfigurován jako RAID 5[[26]](#footnote-26) s jedním Hot spare diskem[[27]](#footnote-27). Už samotný RAID 5 firmě zaručuje bezztrátový provoz dat v případě poruchy a výpadku jednoho z pevných disků. I přesto se firma Almax jistí proti možnému výpadku více pevných disků naráz právě pomocí nakonfigurovaného disku Hot spare, připraveného převzít činnost za jakýkoliv další nefunkční disk v serveru nebo v diskovém poli. Na takto vybaveném a předpřipraveném serveru jsou pod správou operačního systému vytvořeny na diskovém poli logické oddíly, které slouží jako úložiště souborů a dokumentů.

Aby nemohlo dojít k neautorizovanému přístupu uživatelů k dokumentům, ke kterým nemají mít přístup, jsou jednotlivé dokumenty rozděleny do příslušných složek. Na těchto složkách se pak prostřednictvím Active directory stanovují uživatelská oprávnění pro práci s dokumenty v nich umístěných. Používaná struktura složek ve firmě Almax je následující.

Každý uživatel má přidělen svůj domovský adresář, který je považován za osobní složku uživatele, a může si do ní ukládat jak vlastní pracovní dokumenty, tak i soukromé, ale tématika souborů nesmí být v rozporu s pravidly o používání firemní techniky k soukromým účelům. Tím je dle firemní směrnice chápáno a zakázáno jakékoliv využívání firemní výpočetní techniky k soukromému obohacování se a stejně tak je zakázáno jejím prostřednictvím páchat trestné činy, stahovat, ukládat, přehrávat či jinak distribuovat multimediální a jiné programové soubory. Do domovského adresáře má umožněn přístup pouze jmenný vlastník složky a její obsah není nikým jiným dále sdílen. Tato osobní složka uživatele podléhá i jinému, volnějšímu režimu zálohování, protože se jedná pro firmu o dokumenty nižší důležitosti.

Vedle osobní složky je uživateli k dispozici i pracovní složka nebo složky, a to v závislosti na jeho pracovní činnosti a jeho zařazení. Pracovní složky jsou na file serveru vytvářeny pro jednotlivá oddělení nebo jinak specifikované skupiny uživatelů. Už z názvu vyplývá, že tyto složky jsou sdíleny pro vybraný okruh pracovníků a slouží jim k ukládání pouze oficiálních pracovních verzí dokumentů, které mohou dále mezi sebou sdílet. Tyto složky jsou nosnými informačními základnami pro firmu, proto podléhají i přísnému řízení struktury ukládání dokumentů v nich. Je to z důvodu případného předání práce s dokumenty jiné osobě, například z důvodu změny pracovního poměru zaměstnance, aby se zkrátila doba na převzetí pracovních činností s dokumenty přebírajícím zaměstnancem na minimum. Všechny pracovní složky jsou zařazeny do automatizovaného procesu zálohování.

Všem uživatelům sítě je mezi sebou umožněna výměna dokumentů, a to bez ohledu na pracovní oddělení nebo jiné firemní rozřazení, a to pomocí složky „Přenos“. Dle vyjádření představitelů oddělení IT firmy Almax tak uživatelé nezahlcují vnitropodnikový emailový systém velkými soubory, ale k přesunům větších objemů dat využívají právě složky pro přenos. Podmínkou je, aby si uživatel po zdárném přenesení dokumentu protistraně sám přenášený dokument smazal. Uživatelé si jsou vědomi, že musí dbát na bezpečnost takto přenášeného dokumentu a že je v jejich zájmu, aby se dokument v této složce přenosu dlouhodobě nevyskytoval, a to z důvodu vyššího rizika úniku informací ve formě zkopírování zde uložených dat neoprávněnou osobou. Uživatelé jsou seznámeni také se skutečností, že obsah složky „Přenos“ je každý den o půlnoci automaticky vymazán a že se složka nezálohuje.

Ve společnosti Almax je snahou veškeré dokumenty shromažďovat na centrálních úložištích - file serverech - lokalizovaných v data centru. Z tohoto důvodu jsou na nich vytvořeny i jiné složky než pouze výše zmíněné, a to za účelem ukládání souborů a dokumentů generovaných přímo z firemních aplikací. Pokud uživatel vytvoří sestavu v informačním systému ERP a pokud si ji chce uložit pro své další zpracování, je mu při vyvolání akce pro uložení automaticky předvolena nabídka s místem uložení, a to právě na file serveru, kam je z bezpečnostních důvodů následně umožněn přístup pouze uživateli, který daný exportní soubor nebo dokument vytvořil. Tím je zajištěno, že pokud by uživatel s vyšším oprávněním vytvořil dokument a uložil ho do sdílené složky na centrálním úložišti, nemůže se k tomuto dokumentu dostat jiný uživatel, kterému daná informace v dokumentu buď vůbec nepřísluší, nebo který má jiná třeba i nižší oprávnění.

Uživatelům systému je ale umožněno si cílové umístění dokumentu i změnit a uložit si ho tak na svůj lokální disk v počítači nebo notebooku. Společnost Almax si je vědoma toho, že touto cestou by mohlo dojít ke zneužití přístupu k vynášení citlivých informací mimo firmu. Na druhou stranu tuto pomyslnou slabost v systému firma odůvodňuje potřebou jisté flexibility práce uživatele na zadaných úkolech, který tak může pružněji reagovat na pracovní potřeby, což je pro firmu přínosem.

Na osobních počítačích a noteboocích mají tak uživatelé po jejich zapnutí a načtení pracovních profilů k dispozici portfolio síťových disků, které jim přísluší k jejich práci a mohou si na ně ukládat, mazat, editovat nebo jinak zpracovávat dokumenty dle jim přidělených práv a oprávnění. Vedle těchto síťových úložišť má každý uživatel pro uchovávání svých dokumentů k dispozici i lokální pracovní prostor na pevných discích jemu přiděleného osobního počítače. Na něm má nastavenou jakou výchozí složku pro ukládání dokumentů složku „Dokumenty“, ke které má daný uživatel přidělený plný přístup, opravňující ho provádět s dokumenty veškeré potřebné operace. Tato složka v období prováděného monitorování nakládání s dokumenty ve společnosti Almax nebyla začleněna do rutinního automatizovaného zálohovacího procesu. Zaměstnanci za tato data odpovídají sami a mají možnost si dokumenty odzálohovat do své osobní složky na file serveru nebo požádat oddělení IT o provedení zálohy vypálením na DVD.

### Používání přenosných datových nosičů

Dle firemní směrnice společnosti Almax o používání přenosných datových nosičů je jejich využívání možné, ale jen při použití schválených a oddělením IT vydaných zařízení. Jedná se především o USB flash disky nebo externí disky připojované k firemním počítačům, a to za účelem provádění specifických záloh datových souborů nebo sloužící k přenášení datových souborů mezi počítači. Používané firemní USB flash disky jsou šifrované a označené číslem. Zaměstnanec je firemní směrnicí seznámen s riziky plynoucími z používání přenosných zařízení, a to především z jejich ztráty. Z tohoto důvodu mají uživatelé dle směrnice odstranit již nepotřebné soubory ze zařízení tak, aby se opět minimalizovaly možné hrozby plynoucí především ze ztráty přenosného zařízení.

Zaměstnanci firmy Almax mohou ukládat své dokumenty na nosiče CD a DVD pouze pokud jim k tomu byla svěřena firemní výbava, ale nesou osobní odpovědnost za další nakládání s obsahem informací umístěných na přenosném nosiči. Každý multimediální nosič musí být označen jmenovkou a úrovní kategorie informací na něm uložených.

Skartace dále nepotřebných datových nosičů a médií se řídí skartačním řadem společnosti Almax. CD a DVD musí být zničena ve šrotovacím zařízení nebo odevzdána do oddělení IT, které je takovým zařízením vybaveno a které spolu se žadatelem provede odbornou skartaci média. V případě likvidace elektronických zařízení sloužících pro uchovávání elektronických dat, jako jsou pevné disky, USB flash disky a jiná nestandardní média, probíhá likvidace také pod odborným dohledem oddělení IT, které o tom provede skartační zápis. Disky jsou před samotným fyzickým zničením nejprve smazány a přeformátovány k tomu určeným speciálním softwarem tak, aby data na nich nemohla být zneužita.

## Zálohování elektronických dat

Firma Almax si uvědomuje důležitost zálohování, které je proto nedílnou součástí provozu informačních systémů ve firmě. Všechny důležité části systémů, tedy i úložiště s dokumenty, jsou zahrnuty do zálohovacích plánů. Tyto zálohovací procedury, mezi které patří i zálohování file serverů, kde se nachází většina firemních dokumentů, jsou plně automatizovány. Každý zálohovací proces je zdokumentován, má přiřazeného správce, který je zodpovědný za správné nastavení zálohovacího plánu a také má v povinnostech vykonávat denní pravidelnou kontrolu úspěšného vytvoření zálohy.

Celý proces zálohování je několikastupňový, kdy se postupně vytvořená záloha „posouvá“ mezi úložišti dedikovanými pouze pro uchovávání záloh, která jsou umístěna v různých lokacích, a to i geograficky. Takto nastavený proces zálohování se jeví jako bezpečný a firmě tak zajišťuje udržení vysoké dostupnosti historie záloh v čase a místě.

První stupeň zálohy vzniká v bezprostředním místě datového centra na rychlých sítí LAN, které umožňují zálohování velkého množství dat v poměrně krátkém čase. Společnost Almax již v minulosti musela řešit problém s nedostatečným časovým prostorem, který měla na probíhající zálohy v nočních hodinách k dispozici. I to bylo důvodem k rozfázování průběhu zálohovacího cyklu na více částí. První stupeň zálohy se vytváří každý den v nočních hodinách a zůstává uložen na rychlých diskových polích v datovém centru. Tím je čas potřebný k případné obnově dat ze zálohy snížen na minimum.

Druhý stupeň zálohovacího mechanismu probíhá v čase, kdy je systém opět plně využíván zaměstnanci ke svým pracovním úkolům. Z noci vytvořené zálohy se pak ukládají již v režimu off-line na externí přenosná datová média. Tato media jsou následně po softwarové kontrole čitelnosti záloh uložena v nehořlavém sejfu, určeném jako bezpečné úložiště v režimové místnosti, kam má přístup pouze omezené množství osob, a to ještě za vysokého stupně kontroly vstupů.

Třetím stupněm v zálohovacím procesu je kopírování zálohy z hlavního datového centra do záložního datového centra, které je umístěno geograficky jinde, a tudíž v případě úplné ztráty hlavního datového centra může být záložní pracoviště zprovozněno včetně obnovy elektronických dat pouze s jednodenní ztrátou firemních informací v elektronické podobě. To je pro firmu Almax považováno za akceptovatelnou ztrátu, v porovnání s odhadnutelnými škodami, které by mohly nastat v hlavním datovém centru.

Vytvořené zálohy jsou každý den kontrolovány a o úspěšném vytvoření zálohy je pořízen záznam v administrátorském deníku o zálohách. V případě, že se záloha z nějaké příčiny nevytvoří, je o této události vytvořen zápis, závada se musí neprodleně odstranit a pokud to nebrání provozu systému, je záložní operace spuštěna ručně odpovědným správcem systému. Společnost Almax si je vědoma citlivosti informací obsažených v zálohách s tím, že se v jednu chvíli nachází velké množství dat na jednom místě mimo produkční servery, proto firma věnuje velkou pozornost ochraně těchto vytvořených a na jiných místech umístěných záloh. Proto také k těmto zálohám mají přístup pouze osoby, které mají vysoký stupeň bezpečnostní prověrky a také důvěru firmy.

Uživatelé si mohou vytvářet na svých pracovních stanicích i své bezpečnostní kopie elektronických dokumentů a je na jejich zodpovědnosti ochránit tuto bezpečnostní zálohu před zcizením uschováním na bezpečném místě v uzamykatelné schránce.

## Hrozby ovlivňující bezpečnost elektronických dokumentů

Jednou z mnoha povinností vyplývajících z ISMS pro společnost Almax je schopnost řízení rizik. Pro tyto účely má fa Almax zpracován rozsáhlý dokument, který definuje aktiva společnosti včetně jejich ohodnocení co do důležitosti. K těmto aktivům, mezi která patří vedle budov a lidských zdrojů také elektronické dokumenty s informacemi a výpočetní technika, na které jsou elektronická data uchovávána, jsou stanovena možná ohrožení s váhou jejich pravděpodobnosti a následně také protiopatření, která mají těmto hrozbám předcházet. Z celkového výčtu možných hrozeb ohrožujících elektronické dokumenty jsou uvedeny oblasti fyzické bezpečnosti, virů a poškození výpočetní techniky uchovávající elektronická data. Vzhledem k tomu, že se jedná o sledované oblasti ICT se zpětnou vazbou, jsou jednotlivé události a incidenty dokumentovány a výstupy jsou použitelné ve statistikách.

### Ohrožení fyzické bezpečnosti při provozu elektronických dat

Do fyzického perimetru bezpečnosti zahrnuje firma veškeré prostory, kde se vyskytují firemní aktiva, která si stanovila jako klíčová pro své podnikání. Tato práce se zaměřila především na oblasti, kde dochází k uchovávání a manipulaci s dokumenty. Takovými místy jsou pro účely této práce serverové místnosti s datovými sklady a kanceláře zaměstnanců, kteří mají svěřenou výpočetní techniku, na které uchovávají firemní dokumenty.

Společnost Almax investovala v průběhu zavádění ISMS nemalé finanční náklady tak, aby povýšila zabezpečení svých serverových místností, ve kterých se uchovávají na prostředcích výpočetní techniky elektronické dokumenty, na takovou úroveň, která splňuje legislativní požadavky normy ISMS a vysokou dostupnost služeb. Místnosti jsou vybaveny zabezpečovacími elektronickými prvky, záplavovými čidly, samo-zhášecími protipožárními systémy, které v případě nějaké formy ohrožení automaticky danou situaci eliminují (např. požár), nebo samočinně informují patřičné bezpečnostní složky firmy. Firma se tím snaží minimalizovat případné škody na aktivech, na kterých jsou uchovávány vnitropodnikové dokumenty. Další možností, kterou by mohlo dojít k poškození aktiv společnosti a tím i dokumentů, je výpadek elektrického napájení datového centra, a proto je místnost serverovny vybavena bateriovým záložním zdrojem UPS, připojeným na dieselagregát, zajišťující trvalou dodávku elektrické energie.

Kanceláře zaměstnanců, kteří přicházejí do kontaktu s citlivými informacemi a dokumenty, jsou taktéž vybaveny elektronickými zabezpečovacími systémy, které rovněž snižují pravděpodobnost zcizení nebo zneužití výpočetní techniky i s uloženými dokumenty.

V následujícím grafu 1 jsou vyneseny zaznamenané události jednotlivými bezpečnostními systémy instalovanými ve firmě Almax za účelem zvýšení fyzické bezpečnosti při ochraně elektronických dat. Podle prostudovaných záznamů firmy došlo v oblasti fyzické bezpečnosti pouze v jednom případě ke ztrátě dat, a to z důvodu překonání bezpečnostního elektronického systému v kanceláři a následným zcizením notebooku. O této události je ve firmě založen protokol.

Graf 1 Zjištěné události elektronickými bezpečnostními systémy ve firmě Almax v roce 2010

Zdroj: Almax, http://intranet/incidents (data k 28.7. 2011).

### Virové hrozby

Firma Almax si uvědomuje nebezpečí plynoucí z možné infiltrace virové infekce do firmy v podobě škodlivého kódu, který může poškodit nebo úplně zničit elektronické dokumenty, a z těchto důvodů je na všech firemních serverech, počítačích a noteboocích instalován antivirový program AVG s centrální správou nastavení a kontrol výsledků. U notebooků se provádí zvláštní kontrola, protože u nich existuje možnost připojení i do nechráněného internetu mimo firmu a tudíž i větší pravděpodobnost nákazy počítačovým virem.

V následujícím grafu 2 jsou vyneseny počty zaznamenaných virových nálezů na výpočetních prostředcích. Ve firmě Almax jsou nastaveny tři kategorie v nastavení antivirových kontrol: pro servery, počítače a notebooky. Z pořízených záznamů firmy je potvrzen její správný předpoklad a zaměření se na zvýšenou kontrolu firemních notebooků. Právě tato skupina se jeví jako nejrizikovější.

Graf 2 Zaznamenané virové nálezy ve firmě Almax v roce 2010

Zdroj: Almax, Administrátorská konzole antivirového programu AVG (data k 28.7. 2011).

### Selhání počítačového vybavení

Společnost Almax má uzavřené smlouvy SLA na podporu dodávek počítačového vybavení pro případ jejich poruchy. Tyto SLA smlouvy se vztahují jak na hlavní servery, mezi které patří i úložiště s dokumenty, tak i na počítače a notebooky. Uzavřené SLA smlouvy se liší v dohodnuté době na odstranění závady dodavatelskou firmou. Databázový server s produkční verzí vnitropodnikového ERP sytému, má definovanou maximální dobu 6 hodin na vyřešení problému nefunkčního hardwarového vybavení serveru v místě společnosti. Ostatní servery s elektronickými datovými úložišti mají definovanou dobu 12 hodin na odstranění závady nefunkčního hardwarového vybavení serveru. Počítače a notebooky jsou opatřeny smlouvou na opravu v místě společnosti Almax ve lhůtě do 24 hodin od nahlášení poruchy zařízení.

Externí servisní organizace nejsou v případě selhání pevných disků nikterak vázány obnovou samotných dat. To je v odpovědnosti samotné firmy Almax a jejího oddělení IT. V průběhu mapování procesů v nakládání s daty vyšlo najevo, že v případě poškození pevného disku v datovém poli nemá firma ošetřenou situaci, kdy si servisní organizace odveze původní vadný disk bez jeho předchozí fyzické likvidace. Fyzické zničení disku je při tom uvedeno jako podmínka v případě likvidace datových médií, která již nejsou ve firmě znovu použita.

V následujícím grafu 3 jsou uvedeny počty zaznamenaných poruch hardware s dopadem na bezpečnost elektronických dokumentů ve firmě. Poruchy hardware jsou sledovány ve třech kategoriích: servery, počítače a notebooky. Jako nejchoulostivější sledovanou skupinou se vzhledem k vysoké poruchovosti jeví notebooky, které jsou díky své mobilitě vystavovány větším otřesům. Tyto otřesy pak mají negativní vliv hlavně na pevné disky, které tvoří 60% všech řešených oprav této skupiny. Tento fakt posiluje důležitost zálohování dokumentů umístěných na noteboocích. Ze záznamů firmy o poruchách bylo zjištěno, že použité off-line zálohy pro obnovu dat nebyly ve všech případech aktuální a došlo tak k částečné ztrátě většinou časově nejmladších dokumentů. U stacionárních počítačů sice dochází také k vysoké poruchovosti pevných disků, ale výhodou u této skupiny zařízení je umístění většiny dokumentů na síťových úložištích a tedy i nižší pravděpodobnost ztráty dat. Servery mají díky redundantním prvkům hardwaru a zvolené technologii ukládání dat RAID 5 vysokou úspěšnost bezztrátového provozu.

Graf 3 Evidované poruchy hardwaru výpočetní techniky ve firmě Almax v roce 2010

Zdroj: Almax, http://intranet/incidents (data k 28.7. 2011).

# Závěr

Ve společnosti Almax, ve které byla analyzována situace v bezpečnosti nakládání s elektronickými dokumenty a jejíž výstup je reprodukován v této práci, bylo zjištěno následující. Při celkovém zhodnocení a s přihlédnutím k velikosti a obchodnímu zaměření firmy můžeme říci, že firma Almax klade vysoký důraz na bezpečnost svých dokumentů. Uvědomuje si možná rizika působící na její aktiva a má přijata protiopatření a definovány řízené postupy. Dokladem toho je i obhájená certifikace v bezpečnosti informací ISO 27001. Uživatelé mají povědomí o principech bezpečného zacházení s dokumenty a přijatou klasifikací informací. Pravdou ale zůstává, že u některých zaměstnanců je pozorována jistá nezažitost pravidel systému ISMS. Jak samotní zástupci firmy přiznávají, je to způsobeno teprve krátkou dobou od samotné implementace ISMS a stále ještě probíhajícím zlepšováním systému. I z toho důvodu probíhají intenzivní školení zaměstnanců v této oblasti. Zavedené bezpečnostní oddělení má dostatečnou sílu a podporu vedení definovat a prosazovat pravidla v přístupu k informacím a elektronickým dokumentům.

Ve firmě byl zjištěn rozpor v provádění fyzické likvidace vadných disků a vnitropodnikových předpisů, kdy servisní organizace odveze vadný disk bez jeho předešlé likvidace ve firmě Almax, tak jak jí ukládá předpis. Tím může docházet k nechtěnému vynesení a zneužití firemních informací. Na toto zjištění reagovalo bezpečnostní oddělení firmy úpravou vnitřních předpisů.

V informační bezpečnosti má firma Almax silný opěrný pilíř v podobě klasifikace informací a dokumentů, který splňuje požadavky ISMS. Dokumenty jsou dle zjištění při sběru podkladů k této práci správně označovány a je s nimi i nakládáno v souladu s vnitropodnikovými směrnicemi. Bohužel tato klasifikace není promítnuta do nosné firemní aplikace, jakou je ERP, kde se nachází většina provozních informací a kde je také pořizována i většina dokumentů. Takové dokumenty pak neobsahují bezpečnostní prvky a záleží pouze na úsudku zaměstnance a nastavení restriktivní politiky v systému práv a oprávnění, které omezí zaměstnance v libovolném nakládání s dokumenty. Zde je jednoznačné doporučení v rámci možností usilovat o promítnutí kategorizace dokumentů do ERP.

Další oblastí, která se přímo dotýká bezpečnosti přístupů k elektronickým dokumentům, je Active directory. Ve firmě Almax je sice adresářová služba pro ověřování implementována, ale nejsou do ní začleněny všechny servery. Mohlo by se tedy stát, že dojde na serverech k rozdílnému nastavení v oprávnění k přístupu ke složkám s dokumenty. I toto patří mezi doporučení k posílení bezpečnosti řízení přístupů k dokumentům. Na druhou stranu u souborových serverů, které jsou začleněny do Active directory jsou přístupová práva k souborům a složkám řízena správně.

Zálohování, jako nezbytná součást bezpečného provozu informačních systémů je z pohledu zpracovaných zálohovacích procedur dostatečné a nevykazuje v průběhu zálohovacího procesu známky snížené bezpečnosti uchovávaných dat.

Fyzická bezpečnost je ve společnosti Almax na vysoké úrovni, a to z důvodu nově instalovaných bezpečnostních prvků při zavádění ISMS ve firmě, čímž je snížena pravděpodobnost zcizení výpočetní techniky včetně dat. V případě přístupů třetích stran k prostředkům ICT a dokumentům na nich umístěných, jsou s těmito subjekty sepsána smluvní ujednání včetně dodatků o mlčenlivosti.

V oblasti možných a monitorovaných hrozeb ve společnosti Almax je exponovanou skupinou výpočetní technika svěřená zaměstnancům, zejména pak notebooky, a to jak z důvodu zvýšeného rizika poruchy hardwaru, tak i virové nákazy.

Mezi zajímavé směry dalšího rozvoje této práce je možné zmínit oblast řízení rizik ve firmě Almax, která má tuto oblast detailně zpracovanou a dává tak prostor k její hlubší analýze, ale pro naše účely by dalece přesahovala rámec této práce.

Společnost Almax se zdárně vypořádává s bezpečností provozu elektronických dokumentů a podle vyjádření zástupců firmy, kteří definují směr rozvoje ICT a bezpečnosti, musí být přijímány pouze takové kroky v nastavení systému a bezpečnosti, které podpoří a neomezí obchodní aktivity firmy. Důkazem správného naložení s tímto prohlášením managementu firmy je ekonomický růst firmy a rozvoj obchodních aktivit.

# Literatura

**Monografie**

DOUČEK, P. a kol. *Řízení bezpečnosti informací.* První vydání. Praha: Professional Publishing, 2008. 239 s. ISBN 978-80-86946-88-7.

EISENKOLB, K. a kol. *Bezpečnost Windows 2000/XP.* První vydání. Praha: Computer Press, 2003. 501 s. ISBN 80-7226-789-2.

GÁLA, L. a kol. *Podniková informatika: 2., přepracované a aktualizované vydání.* Druhé vydání. Praha: Grada, 2009. 496 s. ISBN 978-80-247-2615-1.

MLÝNEK, J. *Zabezpečení obchodních informací.* První vydání. Brno: Computer Press, 2007. 154 s. ISBN 978-80-251-1511-4.

POŽÁR, J. *Informační bezpečnost.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2005. 311 s. ISBN 80-86898-38-5.

RODRYČOVÁ, D. STAŠA, P. *Bezpečnost informací jako podmínka prosperity firmy.* První vydání. Praha: Grada Publishing, 2000. 143 s. ISBN 80-7169-144-5.

RUSSEL, CH. CRAWFORD, S. *Microsoft Windows Server 2008, Velký průvodce administrátora.* První vydání. Brno: Computer Press, 2009. 1271 s. ISBN 978-80-251-2115-3.

SZOR, P. *Počítačové viry: analýza útoku a obrana.* První vydání. Brno: Zoner Press, 2006. 608 s. ISBN 80-86815-04-8.

**Internetové zdroje**

Almax: *Směrnice administrativní bezpečnosti: Klasifikace informací* *[online].* Praha: Almax, 2010. [cit. 2011-7-2]. Dostupné z intranetu Almaxu: <<http://intranet/iso27001/s_adm_bezp.pdf>>.

Almax: *Směrnice administrativní bezpečnosti: Pravidla nakládání s informacemi [online].* Praha: Almax, 2010. [cit. 2011-7-2]. Dostupné z intranetu Almaxu: <http://intranet/iso27001/s\_adm\_bezp.pdf>.

Almax: *Summary of Incidents [online].* Praha: Almax, 2011. [cit. 2011-7-28]. Dostupné z intranetu Almaxu: <http://intranet/incidents>.

Almax: *Vymezení ISMS: Organizační struktura bezpečnostního oddělení [online]*. Praha: Almax, 2010. [cit. 2011-7-28]. Dostupné z intranetu Almaxu: <http://intranet/iso27001/p\_isms.pdf>.

Microsoft: *Active Directory Domain Services [online].* [cit. 2011-6-6]. Dostupné z WWW: <<http://msdn.microsoft.com/en-us/library/aa746492(v=vs.85).aspx>>.

Techtarget: *RAID [online].* 2008. [cit. 2011-6-15]. Dostupné z WWW: <<http://searchstorage.techtarget.com/definition/RAID>>.

1. „Need to know“ - z anglického překladu: vědět pouze to co potřebuji. [↑](#footnote-ref-1)
2. ISO 27001 (ISMS): norma definující požadavky na bezpečnost informací. [↑](#footnote-ref-2)
3. POŽÁR, J. (2005). *Informační bezpečnost.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, str. 24-25. [↑](#footnote-ref-3)
4. RODRYČOVÁ, D. STAŠA, P. (2000). *Bezpečnost informací jako podmínka prosperity firmy.* Praha: Grada, str. 59. [↑](#footnote-ref-4)
5. DOUČEK, P. a kol. (2008). *Řízení bezpečnosti informací.* Praha: Professional Publishing, str. 90. [↑](#footnote-ref-5)
6. DOUČEK, P. a kol. (2008). *Řízení bezpečnosti informací.* Praha: Professional Publishing, str. 95. [↑](#footnote-ref-6)
7. PDCA – zkratka úvodních písmen: Plan - plánuj, Do - dělej, Check - kontroluj, Act - jednej. [↑](#footnote-ref-7)
8. DOUČEK, P. a kol. (2008). *Řízení bezpečnosti informací.* Praha: Professional Publishing, str. 95. [↑](#footnote-ref-8)
9. MLÝNEK, J. (2007). *Zabezpečení obchodních informací.* Brno: Computer Press, str. 5. [↑](#footnote-ref-9)
10. MLÝNEK, J. (2007). *Zabezpečení obchodních informací.* Brno: Computer Press, str. 17. [↑](#footnote-ref-10)
11. MLÝNEK, J. (2007). *Zabezpečení obchodních informací.* Brno: Computer Press, str. 52. [↑](#footnote-ref-11)
12. MLÝNEK, J. (2007). *Zabezpečení obchodních informací.* Brno: Computer Press, str. 57. [↑](#footnote-ref-12)
13. GÁLA, L. a kol. (2009). *Podniková informatika, 2., přepracované a aktualizované vydání.* Praha: Grada, str. 336. [↑](#footnote-ref-13)
14. GÁLA, L. a kol. (2009). *Podniková informatika, 2., přepracované a aktualizované vydání.* Praha: Grada, str. 41. [↑](#footnote-ref-14)
15. RUSSEL, CH. CRAWFORD, S. (2009). *Microsoft Windows Server 2008, Velký průvodce administrátora.* Brno: Computer Press, str. 240. [↑](#footnote-ref-15)
16. Microsoft: *Active Directory Domain Services* [online]. [cit. 2011-6-6]. Dostupné z WWW: <<http://msdn.microsoft.com/en-us/library/aa746492(v=vs.85).aspx>>. [↑](#footnote-ref-16)
17. EISENKOLB, K. a kol. (2003). *Bezpečnost Windows 2000/XP.* Praha: Computer Press, str. 64. [↑](#footnote-ref-17)
18. GÁLA, L. a kol. (2009). *Podniková informatika, 2., přepracované a aktualizované vydání.* Praha: Grada, str. 339. [↑](#footnote-ref-18)
19. DRP – Disaster Recovery Plan (Plánování aktivit při mimořádných situacích). [↑](#footnote-ref-19)
20. BCM – Business Continuity Management (Řízení nepřetržité obchodní činnosti). [↑](#footnote-ref-20)
21. Techtarget: *RAID* [online]. 2008. [cit. 2011-6-15]. Dostupné z WWW: <<http://searchstorage.techtarget.com/definition/RAID>>. [↑](#footnote-ref-21)
22. MPLS – Multi Protocol Label Switching, je protokol sloužící k propojení rozsáhlých sítí, který pracuje s přidělováním značek příchozím paketům na routeru a následně podle těchto značek volí ideální cestu pro pakety mezi směrovači providerů. [↑](#footnote-ref-22)
23. SLA – Service Level Agreement, je dohoda o úrovni poskytovaných služeb. [↑](#footnote-ref-23)
24. VPN – Virtual Private Network, umožňuje navázat bezpečné spojení mezi dvěma komunikačními body v síti internet. [↑](#footnote-ref-24)
25. Hot plug, jsou části serverového vybavení, která se dají odpojit a vyjmout za chodu systému, aniž by došlo k poruše zařízení. [↑](#footnote-ref-25)
26. RAID 5, je technologie ukládání dat na disková pole obsahující minimálně tři pevné disky, která je odolná vůči výpadku jednoho z disků zařazeného v poli. [↑](#footnote-ref-26)
27. Hot spare disk je pevný disk, který je nakonfigurovaný jako záložní a čekající na výpadek jiného aktivního disku z důvodu jeho poruchy. [↑](#footnote-ref-27)