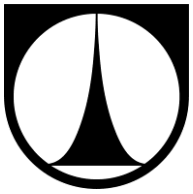
TECHNICKÁ UNIVERZITA V LIBERCI

Fakulta mechatroniky, informatiky a mezioborových studií



BEZPEČNOST INFORMACÍ V ORGANIZACI

BAKALÁŘSKÁ PRÁCE

Liberec 2014 Pavel Dvořák

TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta mechatroniky, informatiky
a mezioborových studií

Bezpečnost informací v organizaci

Bakalářská práce

Studijní program: B2612 Elektrotechnika a informatika
Studijní obor: 1802R022 Informatika a logistika

Autor práce: **Pavel Dvořák**
Vedoucí práce: Ing. Věra Pelantová, Ph.D.

Liberec 2014

TECHNICKÁ UNIVERZITA V LIBERCI
Fakulta mechatroniky, informatiky a mezioborových studií
Akademický rok: **2013/2014**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Pavel Dvořák**
Osobní číslo:	**M10000020**
Studijní program:	**B2612 Elektrotechnika a informatika**
Studijní obor:	**Informatika a logistika**
Název tématu:	**Bezpečnost informací v organizaci**
Zadávající katedra:	**Ústav nových technologií a aplikované informatiky**

Zásady pro vypracování:

1. Vytvořte úvod do problematiky systému managementu bezpečnosti informací organizace.
2. Analyzujte normativní požadavky systému managementu bezpečnosti informací vůči normativním požadavkům systému managementu kvality.
3. Proveďte průzkum stavu bezpečnosti informací v současné organizaci.
4. Vyhodnoťte získané výsledky vzhledem k procesnímu přístupu.
5. Navrhněte vhodné řešení a stanovte doporučení pro organizaci v současnosti.
6. Závěr.

Rozsah grafických prací: **dle potřeby**

Rozsah pracovní zprávy: **cca 45 stran**

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

Seznam odborné literatury:

[1] VEBER, J. a kol. Management kvality,environmentu a bezpečnost práce. 2. vyd. Praha: Management Press, 2010. ISBN 978-80-7261-210-9.
[2] TRUNEČEK, J. Management znalostí. Praha: C.H. Beck, 2004. ISBN 80-7179-884-3.
[3] Tuzemské a zahraniční odborné časopisy.

Vedoucí bakalářské práce: **Ing. Věra Pelantová, Ph.D.**
Ústav nových technologií a aplikované informatiky

Konzultant bakalářské práce: **Ing. Jaroslav Zajíček, Ph.D.**
Ústav nových technologií a aplikované informatiky

Datum zadání bakalářské práce: **21. října 2013**

Termín odevzdání bakalářské práce: **16. května 2014**

prof. Ing. Václav Kopecký, CSc.
děkan

L.S.

prof. Dr. Ing. Jiří Maryška, CSc.
vedoucí ústavu

V Liberci dne 21. října 2013

Prohlášení

Byl jsem seznámen s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb., o právu autorském, zejména § 60 – školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé bakalářské práce pro vnitřní potřebu TUL.

Užiji-li bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Bakalářskou práci jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací s vedoucím bakalářské práce a konzultantem.

Současně čestně prohlašuji, že tištěná verze práce se shoduje s elektronickou verzí, vloženou do IS STAG.

Datum 12. 5. 2014

Podpis

Poděkování

Chtěl bych poděkovat své vedoucí bakalářské práce Ing. Věře Pelantové, Ph.D. za odborné vedení, za pomoc a rady při zpracování této práce.

Abstrakt

Tato bakalářská práce popisuje, co je bezpečnost informace, a proč je důležité se bezpečností informací zabývat. Jaký je rozdíl mezi daty a informacemi a jejich uchováváním, přenášením a určováním ceny. V úvodní části jsou vysvětlené pojmy, které jsou spojené s bezpečností informací. Např. hrozba, zranitelnost, míra rizika a bezpečnostní incident. Také jsou popsány informační technologie, spojené s bezpečností informací. Nechybí ani popis nejčastějších útoků na IT v podobě spamu, phishingu a počítačových virů. V práci lze nalézt analýzu normativních požadavků na bezpečnost informací vůči normativním požadavkům managementu kvality a vysvětlení rozdílu mezi normativními požadavky a přímo implementovanými opatřeními.

Součástí práce je průzkum stavu bezpečnosti informací v organizacích s autorovými postřehy na tuto problematiku. Organizace jsou rozděleny do skupin podle počtu pracovníků a u jednotlivých skupin jsou vypsané nejčastější nedostatky a problémy, spojené s bezpečností informací. Výsledky průzkumu jsou vyhodnoceny vzhledem k procesnímu řízení. Je vysvětlena a odůvodněna spojitost procesního řízení a bezpečnosti informací. V navazující části práce jsou nastíněna jednoduchá řešení pro malé organizace a běžné uživatele informací, jak jednoduše začít s bezpečností informací. Jak postupovat, aby opatření měla správnou návaznost a co největší účinnost. Také je uvedeno řešení některých problémů, které byly patrné v průzkumu v organizacích. V této části jsou uvedeny jak obecné rady, tak konkrétní doporučení, které úzce souvisejí s bezpečností informací. V závěru práce autor pojednává o myšlence propojenosti managementu znalostí s bezpečností informací tak, aby systémy pracovaly v souladu a co nejúčinněji. Na konci práce je uveden názor autora této práce na propojené vzdělávání v IT s bezpečnosti informací.

Klíčová slova: Bezpečnost informací, informace, stav bezpečnosti informací v organizacích, opatření na ochranu informací, systém managementu bezpečnosti informací, procesní přístup

Abstract

This Bachelor's project describes what information safety is, why research in the field is of importance and what the differences between data and information are. In addition it deals with information storage, transfer and price determination. The introduction section explains terminology related to the information safety, for example it deals with threat, vulnerability, and risk rate or safety incident. The project also gives a brief overview of informational technologies (IT) associated with the safety of information. A part is dedicated to the most common attacks and exploits in IT: spam, phishing and computer viruses. The text in addition encapsulates analysis of normative or standard requirements on the information safety vs. normative requirements on the quality management and the difference between the normative demands and the actually implemented measures.

Part of the project is an examination of the current state of information safety in several organisations, which includes opinions of the author on the subject. The organisations are divided into groups based on worker numbers and each group is presented with a list of the most common insufficiencies and problems related to information safety. The results of the examination are interpreted with regards to the process management. The connection between process management and information safety is explained and warranted. The consecutive sections show solutions for smaller organisations and common users, how to simply, easily start with information safety; how to proceed in order for the precautions to have the correct order and maximum efficiency. Solutions to several problems apparent from the examination of organisations also follow. This part contains both general advice and specific recommendations, which are closely related to information safety. In the conclusions the author deals with the idea of relating the knowledge management and the information safety so that they would work together and efficiently. There is an opinion of the author on joined education in IT and in the information safety summarized at the end of the project.

Keywords: Information safety, information, security state in organisations, information protection measures, system of managing information safety, process approach

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

IT (Information technology) Informační Technologie

IS (Information Security) informační bezpečnost

USB (Universal Serial Bus) rozhraní pro připojení přídavného hardware.

MAC adresa (Media Access Control) jedinečný identifikátor síťového zařízen

PSIB ČR Průzkum stavu informační bezpečnosti v ČR

ISMS (Information Security Management System) Systém řízení bezpečnosti informací

PDCA („plan, do, check, act“ – „plánuj, udělej, zkontroluj, jednej“)

SSD (Solid-state drive) druh pevného disku

SIM (subscriber identity module) identifikátor v mobilní sítí

UPS (Uninterruptible Power Supply (Source) – nepřerušitelný zdroj energie

1 Úvod

Účelem této bakalářské práce je základní seznámení s problematikou bezpečnosti informací v prostředí malých a středních organizací a se základními postupy, kterými se tato problematika zabývá. Dále je cílem práce informovat, kdo se touto problematikou v současné době zabývá a z jakých důvodů a proč je vhodné se bezpečností informací zabývat. Je vytvořena sada normativních kroků ke zvýšení bezpečnosti sadou norem ČSN ISO/IEC 27001-6. Tyto normy poskytují jak jednotný směr k zajištění bezpečnosti informací, tak stanovují postupy, které tvoří komplexní návod a kroky i k možné certifikaci organizace dle normy ČSN/ISO/IEC 27001.

V praktické části je vytvořen základní postup jak zabezpečit organizaci z hlediska bezpečnosti informací, který se nebude týkat jen prostředí IT, ale i tzv. papírové bezpečnosti informací. Součástí tohoto základního postupu jsou kroky, které pomohou organizaci zabezpečit svá data před různými ztrátami. Tyto ztráty mají ve svém důsledku vždy finanční charakter. Z praxe je vyčleněno několik skutečných případů selhání v organizacích. Je zde zpracován návrh, jak tuto problematiku v dané organizaci řešit, kdo by se touto problematikou měl zabývat a kdo by měl kontrolovat správnost přijatých opatření.

V závěru práce, na základě vytvořeného základního postupu, je navržen postup, jak zlepšit ochranu informací v organizaci. Je poukázáno na nutnost neustálého přehodnocování, tvorby, kontroly a opatření na všech úrovních organizace.

2 Základní pojmy

2.1 Informace, bezpečnost a bezpečnost informací

Co je to vlastně informace? Na internetu je nejčastěji definována jako údaj o reálném prostředí, o jeho stavu a procesech v něm probíhajících [1]. **Informace** je poznatek týkající se jakýchkoliv objektů, např. fakt, událostí, věcí, procesů nebo myšlenek, včetně pojmů, které mají v daném kontextu smysl. [2]

Z pohledu managementu je možné informaci definovat jako to, co vyplývá z pečlivých analýz, zpracování a prezentace dat v takové formě, která bude vhodná pro rozhodovací proces. [3]

Z řešení bezpečnosti informace, plyne, že se v informacích skrývají různé údaje, které mají pro člověka různou cenu. Stejně jako u běžné věci, **čím větší je cena, tím větší by měla být její ochrana**. Toto by mělo být zlatým pravidlem v bezpečnosti informací.

Bezpečnost [security] je definovaná jako*:* „vlastnost, nebo stav ochrany (na určité úrovni) proti nevyhnutelným ztrátám“ podle publikace [4, s. 62] Prakticky se riziko nedá nikdy eliminovat na 100%. Proto je snaha míru bezpečnosti dostat na takovou úroveň, aby zbývající riziko bylo přijatelné. Vynaložené náklady na bezpečnost by neměly přesáhnout cenu dané věci, která je zabezpečovaná.

Bezpečnost informací [Information security] „je bezpečnost při manipulaci s informacemi, především vzhledem k požadavkům na důvěrnost, integritu a dostupnost informací.“ [4, s. 38]. Stručně řečeno, cílem bezpečnosti informací je snaha zajistit dostatečnou integritu, dostupnost a důvěrnost ochraňovaných informací a udržovat systém bezpečnosti informací v takovém procesním stavu, aby tyto tři základní podmínky byly dodrženy. Samotná bezpečnost informací je velmi složitá a velmi rychle se měnící činnost. Tento proces je nutné neustále řešit a to jak ve velkých organizacích, tak i v těch malých. Jde o neustálý a opakující se děj, kdy se využívá nástroj PDCA („plan, do, check, act“ – „plánuj, udělej, zkontroluj, jednej“), který je nutný k dosažení neustálého zdokonalování bezpečnosti informací v organizacích. V neposlední řadě by tyto činnosti a zásady měli využívat i malí živnostníci a samozřejmě jednotlivci v běžném soukromém životě. Při zajištění integrity, dostupnosti a důvěrnosti mohou některá opatření přinést i při minimálním vynaložení nákladů velký přínos

v bezpečnosti a v některých případech i úsporu nákladů v souvislosti s omezením způsobených škod nebo naprosté předejití možným škodám.

2.2 Data a informace

Data jsou základním stavebním kamenem při následném zpracování informací. Definice říká, že: „Údaje, data jsou fakta, čísla, události, grafy, mapy, transakce atd., které byly zaznamenány. Jsou základním materiálem, surovinou pro informace." podle [5, s. 24].

Informace jsou data, která byla zpracována do podoby užitečné pro příjemce. [5] Z těchto definic vyplývá, že všechny informace jsou daty, ale data nemusí být vždy informacemi. Data se mohou stát informací jejich zpracováním.

2.3 Cena informací

Cena informace je téma, které je již dlouhou dobu řešeno v celosvětovém kontextu. Existují dva rozdílné principiální přístupy. V první řadě se považuje cena informace za rovnost s náklady na její získání uchování a údržbu (koncept hmotného statku). Druhý směr definice ceny informace ji chápe jako takovou (koncept nehmotného statku).

Obě definice představují informace jako komoditu, která má následující vlastnosti:

- může nahradit kapitál, práci nebo materiál
- stejná informace může mít jinou hodnotu v závislosti na lidském vnímání
- po použití nezaniká, ale s časem se její hodnota mění
- informace lze velmi rychle a snadno distribuovat při relativně nízkých nákladech
- mohou se z rozsáhlé informace vyseparovat základní myšlenky

S cenou informace by měla přímo úměrně souviset míra její ochrany, tedy peněžní náklady investované do této ochrany. Při stanovení ceny informace se nesmí zapomenout na obsah informace, který může mít různou hodnotu pro různé vlastníky. Do ceny informace by se měl započítat i fakt, že v některých případech může mít organizace prospěch z toho, že danou informaci nevlastní nikdo další, i když organizace vlastnící informace nemá potřebu jí sama využívat.

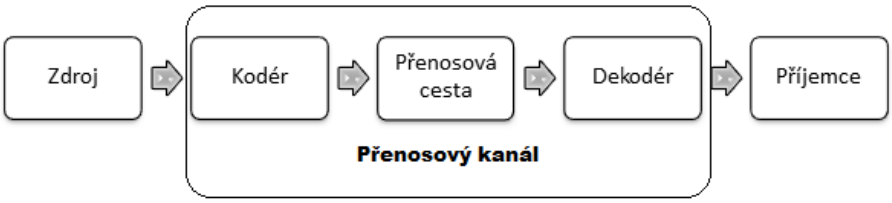
2.4 Nosiče informace

Informace jako taková je nehmotná. Nosičem informace je místo, kde je informace v ucelené formě uložena. Vždy musí být uložena v nosiči informace. Lidé, zabývající se bezpečností informace, se snaží informace chránit, ale toho lze docílit jen tak, že se zaměří na nosiče informace a přenosové cesty. V dřívější době se používaly dva základní nosiče informace - člověk a papír. Při posuzování člověka, jako nosiče informace z hlediska bezpečnosti, je možné se setkat s názorem, že člověk je jedna z nejnáchylnějších částí systému ke vzniku bezpečnostních incidentů. Člověk jako nosič informace má tyto parametry: loajalita k organizaci, jeho znalosti o bezpečnosti, jeho chování k citlivým datům. U papíru, tedy tištěných dat, bude nejdůležitější jejich uskladnění, přístup k těmto materiálům a jejich záloha. V dnešní době se od lidí a papíru, jako medií pro uložení informací, dosti ustupuje.

Nejrozšířenější způsob ukládání dat je dnes v elektronické formě na pevné disky, servery, mobilní telefony, osobní počítače, tablety apod. Tyto moderní vymoženosti přinášejí spoustu výhod, ale na druhé straně i problémy s bezpečností. Takto uložené informace jsou při správně zvoleném systému ukládání pro uživatele mnohem více přehledné, dostupnější, jednodušší pro úpravu. Přístup k těmto datům bývá dále mnohem rychlejší a je možnost se k nim dostat z několika míst najednou. To je sice příznivý parametr pro uživatele, ale nepříznivý pro samotnou bezpečnost informací. Prakticky jakýkoli přístroj připojený do libovolné sítě je v ohrožení. Pokud je počítač připojen do největší světové sítě, tedy internetu, riziko je o to větší. Dalším rizikovým faktorem je životnost nosičů, z té vyplývá nutnost zálohy dat.

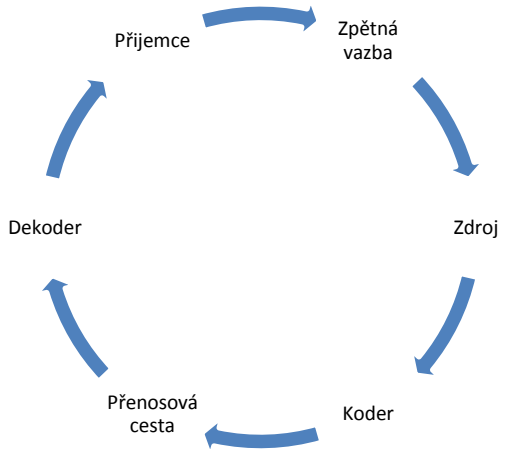
2.5 Přenos informace

Přenos informace se chápe jako přenos informace z jednoho nosiče informace na druhý. Informace jsou vždy přenášeny po přenosové cestě. U zdroje je vždy kodér ten informaci upravuje tak, aby mohla být přenesena po přenosové cestě. U příjemce je dekodér ten informaci převádí na formu vhodnou pro příjemce. Kodér, přenosová cesta a dekodér jsou dohromady přenosový kanál. Víc obr. 1.



Obr. 1 Přenos informace

Jsou dvě základní možnosti. Buď je přenášena informace z jednoho nosiče na druhý, ale ve zdrojovém nosiči po dokončení přenosu informace zůstává. Tento přenos se nazývá kopírování. Nebo lze informaci přenést s tím, že informace v původním nosiči není zachována po dokončení procesu, je už jen v druhém nosiči. U druhého způsobu je nutné ověření (zpětná vazba), že druhý nosič informaci přijal a uložil ve správném tvaru, než je informace odebraná z prvního nosiče. Zpětná vazba se využívá i v prvním případě, ale její důležitost je o něco menší. Kontrolu přenesených dat za uživatele vykonává operační systém, který má pro pracování s daty vlastní postupy a těmi se řídí. Zjednodušeně řečeno zkontroluje, jestli uložil vše, co bylo načteno. Pokud neuloží data na nový nosič, nesmaže původní. V druhém případě přenosu informaci nahlásí uživateli problém s přenosem.



Obr. 2 Přenosová cesta se zpětnou vazbou

2.6 Ztráta ceny informace

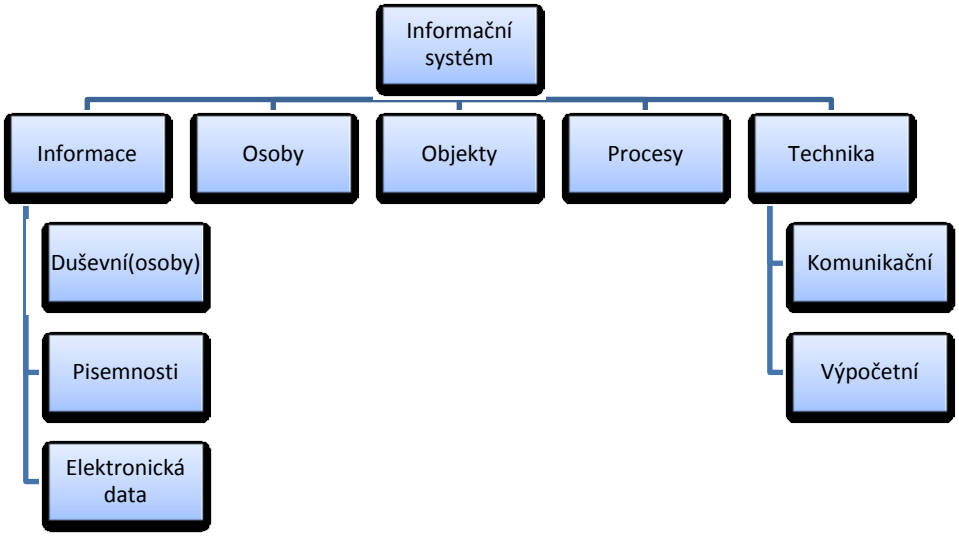
Problémem informací je nutnost uchovávat je i mimo relativní bezpečí mysli. Důvodem je, že objem dat a potřeba jejich sdílení to lidem nedovoluje. Informace může být ztracena tak, že se rozbije, nebo se poškodí nosič informace. Např. papír shoří, člověk zapomene, pevný disk v počítači se rozbije. V tomto případě majitel informací

o informace přišel, v některých případech nenávratně. Další možnost je, že se informace dostane do cizích rukou. Stále ji vlastní původní majitel, ale už ji má i někdo jiný. Cena takovýchto informací se může rapidně snížit, v extrémních případech u velmi tajných informací až na nulu. Existuje ještě třetí a nejhorší možnost a to ta, že informaci někdo vlastní, ale dostane se k ní někdo jiný, on si informaci zkopíruje a původní data smaže či poškodí. V tomto případě došlo k největší ztrátě. Další újmou při ztrátě informací můžou být sankce od státu za nechránění údajů, nebo sankce vyplývající ze smluvního závazku. Určitou újmu může utrpět i dobrá pověst organizace. Velmi citlivé informace mohou v některých případech ztratit svou hodnotu i v případě pouhého podezření na vyzrazení této informace.

Ke ztrátě ceny informace může dojít, buď jak již bylo zmíněno, poškozením nosiče informace, nebo při jejím přenosu. Hrozby při přenosu informace se odvíjejí od přenosové cesty. Pokud je informace předávána ústně, hrozí jí pouze odposlech. Pokud je předávána v tištěné nebo ručně psané podobě, může dojit ke ztrátě integrity, dostupnosti a důvěrnosti. Při sítové komunikaci opět může nastat ztráta ceny informace, pokud není zaručena integrita, dostupnost a důvěrnost. U sítové komunikace je tento problém velice častý z důvodu rozlehlostí sítí a velkého množství možných útoků na tyto sítě.

2.7 Informační systém

Informačním systémem se nazývá soubor všech činitelů, které se setkávají s informací. Mohou ji vytvářet, zpracovávat, ukládat či přenášet. Informační systém je budován za účelem zefektivnění šíření informací a jejich bezpečnosti.



Obr. 3 Informační systém

Dobře navržený informační systém usnadňuje práci všech zaměstnanců. Zjednodušuje přístup k informacím a datům, důležitým pro jejich práci. Dost často informační systém zamezuje zbytečným zmatkům, způsobeným nedostatkem informací nebo vznikem dezinformací. Dobře navržený informační systém má v sobě začleněné prvky, které napomáhají ochraně dat.

3 Další pojmy

3.1 Hodnota aktiv

Aktivum představuje v organizaci to, co organizace vlastní a má potenciál přinést v budoucnu ekonomický prospěch, např. majetek, zásoby, peníze licence. Z hlediska bezpečnosti informace si organizace ohodnotí svá aktiva na předem zvolené stupnici. Číslem jedna označí nejméně hodnotná aktiva pro organizaci a maximální hodnotou stupnice ty nejvíce cenné. Např. si organizace svá aktiva ohodnotí na stupnici 1-5.

3.2 Hrozba

Hrozbou jsou nazývány osoby, předměty, software a hardware, nebo jejich činnost, které můžou způsobit poškození, zničení nebo ztrátu důvěry. Hrozbou může být i přírodní jev, jako přívalové deště, rozvodnění řek, úder blesku apod. Hrozbou je nazýváno vše, co má potenciál ohrozit bezpečnost informací. Také hrozbám organizace přiřadí ohodnocení z předem určené stupnice. Nejmenší hrozby ohodnotí jedničkou největší nejvyšším číslem stupnice. Např. 1-5.

3.3 Zranitelnost

Zranitelnost je vlastnost aktiva. Např. objevené bezpečnostní slabiny v operačním systému zvyšují zranitelnost aktiva. Dobře chráněná aktiva organizace ohodnotí na předem určené stupnici číslem jedna. Ty nejzranitelnější ohodnotí nejvyšší hodnotou stupnice. Stupnice např. 1-5.

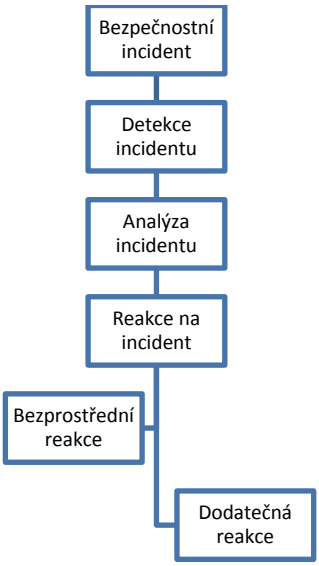
3.4 Míra rizika

Míra rizika je pravděpodobnost naplnění konkrétní hrozby. Riziko udává míru ohrožení konkrétního aktiva. Míra rizika=(Hodnota aktiva * Hrozba * Zranitelnost) Ocenění rizika je vyhodnocení hrozeb za účelem stanovení úrovně rizika, kterému je vystaven systém nebo jeho určitá část. Stanovení rizika je jednou ze základních činností při zajištění informační bezpečnosti.

Řeší se od největší hodnoty po nejmenší. Např. při stupnici 1-5 u všech třech závislých veličin je maximální hodnota 125. Organizace si určí, pod jakou hodnotu je pro ní akceptovatelné riziko. Např. do 50 může být pro organizaci akceptovatelné riziko. Ostatními aktivy s mírou rizika nad 50 se organizace bude zabývat.

3.5 Bezpečnostní incident

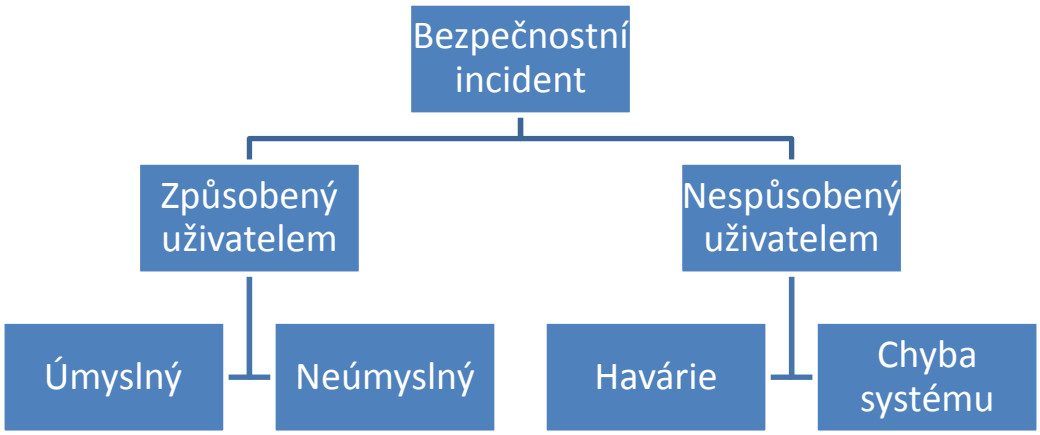
Bezpečnostním incidentem je nazývaná událost, zaviněná jak úmyslně, tak neúmyslně, která způsobila, nebo mohla způsobit škodu na aktivech. Např. narušení důvěryhodnosti, integrity nebo dostupnosti informací. Bezpečnostní incident by měl vyvolat odezvu v dané organizaci, která by měla postupovat podle následujících kroků (viz obr.4): detekce incidentu, analýza incidentu, reakce na incident. Reakce bývá rozložena na dva kroky. První je bezprostřední reakce, která se snaží co nejvíce zmírnit, nebo úplně zamezit následkům incidentu. Poté následuje druhý krok, časově náročnější, kdy se analyzuje příčina a důsledky incidentu, účinnost bezpečnostních opatření. Tyto získané údaje mohou přinést důležité informace, jak vylepšit svůj bezpečnostní systém, tak příště bezpečnostním incidentům předejít, nebo omezit jejich následky.



Obr. 4 Bezpečnostní incident

O bezpečnostních incidentech je dobré si vést záznamy. Z ohledu na bezpečnost informací je dobré, aby tyto záznamy měly předem stanovenou formu a vždy obsahovaly základní údaje, které budou vždy stejné u všech bezpečnostních incidentů. Proto bývají pro tyto události vytvořené formuláře s předem stanovenými body pro vyplnění. Důležité je, aby tyto předem stanovené údaje byly vždy smysluplné a byly 100% společné pro všechny typy incidentů. Pokud si touto podmínkou autor formuláře není jistý, je dobré tyto sporné údaje označit jako nepovinné. V opačném případě je dosti pravděpodobné, že pracovník, který tento protokol bude sepisovat, ho nebude vyplňovat s dostatečnou pozorností, protože mu nebude přisuzovat důležitost a některé, jinak důležité parametry mu mohou přijít v daném případě až směšné, což se velmi projeví na kvalitě informací zapsaných do protokolu. Přitom protokoly

o bezpečnostních incidentech mohou být velmi užitečné při správném ohodnocení bezpečnostního systému. Mohou odhalit slabá místa systému. V některých případech je možné, že příčina incidentu není odhalena hned po incidentu, ale až s uplynutím času, kdy se incidentů stane více a až z jejich protokolů je patrný společný zdroj problémů.



Obr. 5 Bezpečnostní incidenty

4 Základní pojmy IT bezpečnosti

4.1 Fyzické části

Nejzákladnější ochranou informací je věnování pozornosti lidem a IT (Informačním Technologiím). Základní pojmy v IT z hlediska bezpečnosti jsou: fyzické zabezpečení sítí, serverů, spojů a rozbočovačů. S těmito fyzickými částmi může nastat problém např. v případě, kdy se organizace nastěhuje do starší budovy, kde již byla vystavěna LAN síť, ale tato síť není zabezpečena proti připojení cizích osob. Např. je vytvořený spoj v místě s volným přístupem. Ještě větším rizikem je umístění vývodů na místě s volným přístupem. V těchto případech může hrozit přístup cizí osoby do sítě, protože drátové připojení do sítě nebývá omezené pomocí softwaru, jako např. u Wi-Fi sítí, kde je takovéto omezení pomocí kvalitního heslování nebo přístupu pouze s určitou MAC adresou naprosto nezbytné. U menších společností opět v nevyhovujících podmínkách může nastat problém s umístěním serveru. Přitom umístění serveru je jedna z nejzákladnějších věcí, jak chránit svá data. V ideálních podmínkách je server dobře přístupný tak, aby s ním mohla fyzicky pracovat osoba tímto úkolem pověřená a zároveň nepřístupný pro ostatní osoby, které k těmto částem sítě nemají mít přístup.U umístění serveru není důležitým parametrem jen přístup osob, ale také jeho umístění s ohledem na životnost serveru a s největší pravděpodobností na jeho bezproblémový chod. To znamená na suché a dobře větrané místo. Větrání je důležité z důvodu udržení dobrých podmínek pro součástky serveru, protože chod serveru je nezbytný pro bezproblémový běh sítě a předejití ztráty dat. Pokud není prostor dobře větraný, může docházet k poruchám, nebo dokonce ke zničení součástí serveru teplem, které sám server produkuje.

4.2 Autentizace, autorizace

Ochrana informace také znamená zamezení přístupu k těmto datům neoprávněným osobám. V této problematice se často používají dvě slova autentizace a autorizace. Tyto dva pojmy se velmi často zaměňují, ale každý má svůj vlastní význam.

Autentizace slouží k jednoznačnému určení uživatele, který přistupuje k systému, vstupuje do budovy apod. To znamená, že systém identifikuje danou osobu. Zjistí, s kým komunikuje. V praxi je nejčastějším způsobem použití databáze, kde každý uživatel je jeden řádek databáze. Při přístupu do systému uživatel zadá své uživatelské jméno a heslo. Jméno se porovná přímo. Hesla bývají v databázi uložená zpravidla

v zašifrované formě. Proto se zadané heslo nejdříve také zašifruje a až poté jsou obě šifry porovnány. Jen takovýto přístup je přípustný. Autentizace se nemusí provádět pouze jménem a heslem. Další možností jsou USB klíče, RFID štítky či karty, které pracují na podobném principu jako jméno a heslo. Jen jsou tyto údaje uloženy do karty a z ní jsou pomocí indukce načteny. Další možností je snímání otisku prstu, snímaní zornice nebo rozpoznání obličeje. Tyto metody jsou ovšem dražší a i přesto se dají oklamat. Nejhůře jsou na tom levné softwary na rozpoznání obličeje, kde stačí k oklamání systému pouhá fotografie.

Velmi oblíbená autentizace u mobilních zařízení, jako je mobilní telefon či tablet s dotykovým displejem, je vytvoření obrazce spojením několika bodů. Tento obrazec se musí shodovat s přednastaveným. Stejně tak jako u hesel zadávaných na klávesnici by se i vzor měl po čase měnit, protože je možné při opakovaném zadávání, že kombinaci po čase někdo pomocí pečlivého pozorování odhalí.

Autorizace je proces ověření přístupových oprávnění uživatele, vstupujícího do systému. Tento proces většinou navazuje na autentizaci.

Jednoduše řečeno autentizace zjišťuje, kdo jste, a autorizace zjišťuje, jaká máte práva. Např. administrátor a běžný uživatel jsou uloženi ve stejné databázi, ale každý má různá oprávnění k přístupu apod.

4.3 Záloha

Jednou ze základních pomůcek předejití ztráty dat je jejich záloha. U velkých organizací je nejčastěji vybudovaný server od zkušeného dodavatele. Záloha se provádí automaticky. Je možné najít mnoho publikací, které se touto problematikou zabývají např. kniha Bible vypalování a zálohování 2012 [25] nebo je možné najít články na různých webových stránkách, např. [6] web živě.cz článek: „Sedm nejlepších programů pro zálohování dat“ Bohužel v malých organizacích se tato problematika skoro neřeší. Přitom základní řešení nemusí být vůbec drahé. Lze jej vyřešit svépomocí při znalosti elektroniky, nebo s dobrým prodejcem elektroniky. Problémy se zálohou bývají v menších organizacích nebo u živnostníků velmi časté. Tyto podniky jsou malé a vlastní IT oddělení je naprosto nemyslitelné. Dost často se účetnictví, důležité informace a dokumenty a různé výsledky práce ukládají a vytvářejí na jednom počítači, nebo v horším případě notebooku. Bohužel i v dnešní době je spousta lidí, kteří berou počítač, notebook nebo mobilní telefon jako takzvanou černou skříňku, kterou koupí

z internetu. V těchto případech se velmi často stává, že ona černá skřínka jednou přestane fungovat a pak nastává problém, protože uživatel nemá dostupné své informace a data.

Pokud malá organizace ukládá veškerá data na jeden počítač, je přitom záloha dat velmi jednoduchá. Do počítače se nainstalují dva pevné disky. Při nahrání jakýchkoli dat na jeden disk se vytvoří kopie na druhém. Tomuto zapojení se říká **zrcadlení**. V tomto případě jsou data chráněna před ztrátou způsobenou náhlým selháním jednoho z disků. Možnost, že selžou oba disky najednou běžným opotřebením, je daná násobkem pravděpodobnosti poruchy na každém z nich. Tato ochrana je účinná ve většině případů. Bohužel neochrání data, pokud se stanou jiné havárie, jako je třeba zatopení počítače vodou nebo úder blesku. Zde je potřeba zálohovat data na externí nosič vzdálený server, externí pevný disk. Při malém objemu dat může pomoci i obyčejný flash disk. Náklady na takovéto opatření jsou takřka minimální.

Největší riziko pro data je notebook. Bohužel u malých organizací je běžné, že se veškerá data ukládají na jeden jediný notebook. Přitom riziko, že se notebook zničí, je obrovské. Velké množství těchto zařízení je zničeno obyčejným převrhnutím kávy do klávesnice. „Naštěstí“ nalití tekutin do notebooku většinou zničí veškeré součástky kromě pevného disku. Pro pevný disk existují nebezpečnější věci, než je hrnek s kávou. A to pád notebooku nebo jeho vibrace, tedy pouze pokud notebook obsahuje magnetický pevný disk. Zde je znovu problém s černou skřínkou. Pokud obsahuje přenosný počítač magnetický pevný disk, riziko jeho zničení při pádu nebo při otřesech během čtení disku či zápisu dat je veliké. Pokud je vyroben pevný disk technologií SSD (Solid-state drive), pády a otřesy na takto vyrobený disk nemají vliv. Bohužel tyto disky jsou dražší a jejich kapacita je nesrovnatelně menší. Např. běžný magnetický disk o kapacitě 1000GB stojí přibližně 2000 Kč, zato SSD disk s kapacitou 800 GB stojí přibližně 20000 Kč (orientační ceny z velkého internetového obchodu k 21. 4. 2014). Bohužel nebývá konstrukčně možné mít dva pevné disky uvnitř notebooku. Zde je zapotřebí externí záloha dat.

Záloha může ušetřit i dosti značné výdaje. Cena flash disku se pohybuje v řádech stokorun. Cena pevných disků se mění podle kapacity, ale je v řádech tisícikorun. Naproti tomu obnova dat z nefunkčních nosičů může stát i 10000 Kč i více. Navíc záchrana nemusí být 100%.

4.4 Záloha telefonních čísel

Velmi opomíjené je zálohování čísel z mobilních telefonů. Ztráta čísel je velmi častý problém u menších organizací, podnikatelů i soukromých osob. Nejzákladnější věc, kterou lze udělat, je mít kontakty jednak na SIM kartě a jednak i v telefonu. Tato praktika pomůže pouze v případech, kdy se jedna z částí rozbije. Pokud dojde ke ztrátě, SIM karta je vložená v telefonu, takže se nedá mluvit o záloze. Dalším problémem je, že SIM karta je schopná pojmout pouze 220 čísel a množství údajů je omezené pouze na číslo, jméno a příjmení a jen omezený počet znaků. Nejjednodušší je si nainstalovat do počítače software od výrobce telefonu a pravidelně provádět synchronizaci čísel. Množství ztracených čísel záleží pouze na uživateli podle toho, kolik přidal do telefonu kontaktů po poslední synchronizaci. Přenesení kontaktů z počítače do nového přístroje bývá často pracné, ale vždy řešitelné, v nejhorším případě manuálním způsobem.U moderních přístrojů je možná automatická synchronizace kontaktů přes internet. To přináší značné výhody. Např. sdílení kontaktů mezi více přístroji nebo velmi častá synchronizace, čímž se sníží riziko ztráty neuložených dat. Toto řešení v sobě skrývá riziko, spojené s napadením tohoto synchronizačního účtu cizí osobou. Všeobecně to způsobuje nižší bezpečnost chytrých telefonů. Velmi často jsou kritizované mobilní telefony s operačním systémem Android pro nízké zabezpečení systému. To potvrzují i různé nezávislé zdroje, např. publikace [7]

4.5 Ztráta telefonu

Odcizení nebo ztráta telefonu může znamenat komplikaci nejen v případě nezálohovaných čísel, ale i v případě nechtěného sdílení velkého množství dat, pokud telefon není chráněný proti přístupu cizí osoby. To znamená provádění autentizace při zapnutí telefonu, nebo lépe při odblokování klávesnice. Dobrou funkcí moderních telefonů v případě ztráty telefonu je zaměření pozice s využitím GPS přes internet. Tato funkce může pomoci opět nalézt telefon, ale data z něj už můžou být zneužita. Nevýhodou tohoto systému je případ zneužití zaměření pozice mobilního telefonu s GPS, kdy cizí osoba může sledovat pohyb osoby s telefonem.

5 Útoky na uživatele a systém

Útoků na uživatele a systém je nepočítaně. Druhy útoků se liší podle vybavení a činnosti dané organizace a jednotlivých uživatelů. Útoky jsou často modifikované s tím, jak se mění bezpečnostní opatření. Vypisovat jednotlivé útoky do této práce, podle názoru autora této práce, nemá smysl. Protože nejde nikdy vypsat všechny a i kdyby se tak stalo, není možné tuto práci neustále aktualizovat tak, aby popisovala nové útoky a jejich modifikace. Proto se autor této práce omezil na popis v současnosti nejčastějších útoků a to je Spam, phishing a počítačové viry. Ty to tři metody se neustále používají a s největší pravděpodobností ještě dlouho budou.

5.1 Spam

Slovem spam se označuje: „zneužití digitální komunikace, při kterém je na množství adres zasílána jedna a tatáž příjemcem nevyžádaná zpráva. Zpravidla komerčního charakteru.“ podle [5, s. 241]. Podle odborníků tyto zprávy tvoří 40-60% veškeré emailové komunikace, zdroj [5, s. 241]. Tento styl marketingu je sice pro někoho levná reklama, ale pro zbytek uživatelů je to ztráta času a zbytečné zatěžování telekomunikačních sítí. Obranou proti spamu je nastavení filtru, který poštu třídí a spam odkládá do zvláštní složky. Bohužel tato metoda není účinná proti spamu s neustále se měnícím odesílatelem a předmětem. Řešením tohoto problému může být „tvrdší “nastavení filtru, ale to může mít za následek zařazení do spamové složky i korespondence, která do spamu nepatří. To uživateli opět ubírá čas, protože složku musí jednou za čas zkontrolovat. Nejlepší obranou proti spamu je nevyplňovat svůj email na místa, kde to není nezbytně nutné. Hlavně nezadávat svoji emailovou adresu na pochybných stránkách apod.

5.2 Phishing

Phising je: „primitivní metoda, při které je odeslán falšovaný e-mail příjemci, který klamavým způsobem napodobuje legální instituci s úmyslem vyzvědět od příjemce důvěrné informace jako číslo platební karty nebo heslo bankovního účtu. Takovýto email většinou navádí uživatele, aby navštívili nějaké webové stránky a zde zadali tyto důvěrné informace. Tyto stránky mají design podobný jako instituce, za kterou se vydávají, aby získaly vaši důvěru. Stránky této instituci samozřejmě nepatří, výsledkem je ukradení vašich osobních údajů za účelem zisku.“ podle [8, s. 28].

Takto tuto praktiku definovali odborníci při jejím vzniku. Lze se s touto praktikou setkávat již od roku 2004. Přesto se najdou uživatelé, kteří se na pomyslný háček chytí. Znění definice by se sice mělo mírně pozměnit, protože útočníci již neloví pouze na emailech. Podle statistik má emailový phishing podíl pouhých 12% podle textu [9] a útoky už se neomezují pouze na bankovní účty, ty tvořily 20% podíl útoků podle [9]. Hlavním místem, kde útočnici provozují phishing nyní, je Facebook. Přitom obrana je naprosto jednoduchá a to je zvýšení základní informovanosti uživatelů. Lepší rozmýšlení svých kroků na internetu je zásadní.

5.3 Počítačové viry

Název je odvozen od jistých podobností s biologickými originály. Virus je schopen sebe-replikace, tedy množení sebe sama, ovšem za přítomnosti vykonatelného hostitele, k němuž je připojen. Hostitelem mohou být např. spustitelné (executable) soubory, systémové oblasti disku, popř. soubory, které nelze vykonat přímo, ale za použití specifických aplikací (dokumenty Microsoft Wordu, skripty Visual Basicu apod.). Jakmile je tento hostitel spuštěn (vykonán), provede se rovněž kód viru. Během tohoto okamžiku se obvykle virus pokouší zajistit další sebe-replikaci a to připojením k dalším vhodným vykonavatelným hostitelům podle zdroje [10].

Je možné najít i jiné definice. Nejdůležitější je mít na paměti, že počítačový vir je vždy škodlivý kód, před kterým je potřeba chránit své počítače, ale i nosiče dat jako jsou přenosné disky, flash disky i mobilní telefony. Nejčastěji jsou konstruovány za účelem pouze škodit, odcizit data nebo informace, zneužívat cizí výpočetní výkon nebo k jinému peněžnímu obohacení jejich autora.

Základní ochranou je mít antivirový program a ten neustále aktualizovat. Vyhýbat se podezřelým stránkám odkazům a emailům. Bohužel ani tento postup není 100%.

.

6 Management bezpečnosti informací a management kvality

Tato kapitola se nezabývá čistě vztahem managementu bezpečnosti informací vůči managementu kvality. Důvod je patrný, tyto dva systémy se od sebe dost liší. Hlavním cílem managementu bezpečnosti informací je zajistit důvěrnost, integritu a dostupnost informací. Management kvality se zjednodušeně snaží o shodu výsledného produktu s požadavky na produkt. Přes tyto patrně rozdílné cíle je možno najít shodu v některých postupech, nástrojích a požadavcích. Z důvodu různých požadavků u každé organizace, jak na management bezpečnosti informací, tak i na management kvality, zde budou srovnány normativní požadavky. Jak norma pro bezpečnost informací celým názvem: Informační technologie-Bezpečnostní techniky- Systémy managementu bezpečnosti informací ČSN ISO/IEC 27001(ISMS) [11] tak norma pro Systémy managementu kvality ČSN EN ISO 90001 [12] mají v úvodním textu napsáno, že je možné je použít na všechny typy organizací.

Počáteční je požadavek na procesní přístup, který se vyskytuje jak v managementu bezpečnosti informací, tak managementu kvality. Bezpečnost informací z procesního řízení využívá hlavně model PDCA (Plánuj, Dělej, Kontroluj, Jednej), stejně tak je využíván managementem kvality. Oba tyto systémy využívají požadavek na neustálé zlepšování, každé dílčí zlepšení má vést k zlepšení celkovému. Jak ISMS tak management kvality má využívat procesní přistup k dosažení svých cílů.

Všeobecné požadavky společné pro ISMS a management kvality vyžadují na organizaci ustavení, zavedení, provozování, monitorování, udržování a soustavné zlepšování dokumentovaného ISMS nebo managementu kvality. U ISMS se přidává, že je třeba předchozí podmínky plnit v kontextu všech činností a rizik. Pro tyto účely se v ISMS využívá model PDCA.

Při zavádění ISMS je požadováno určit rozsah, hranice a definovat politiku ISMS a také stanovit přístup organizace k hodnocení rizik. S tím se pojí identifikace a následné analýzy a vyhodnocení rizik. Organizace musí identifikovat a vyhodnotit varianty pro zvládání rizik. Pak musí vybrat cíle a jednotlivá bezpečnostní opatření pro zvládání rizik. Vedení organizace musí dát souhlas s navrhovanými zbytkovými riziky a povolit zavedení a provoz ISMS. Na závěr je prohlášení o aplikovatelnosti. Prohlášení o aplikovatelnosti vydává organizace jako dokumentované prohlášení popisující cíle a opatření, která jsou relevantní a aplikovatelná v rámci ISMS organizace.

K ustavení managementu kvality organizace musí určovat a aplikovat procesy, potřebné pro systém managementu kvality. Je zapotřebí určit posloupnost a vzájemné působení těchto procesů. Musí být určena kritéria a nástroje řízení a fungování těchto procesů. Požadováno je zajišťování dostupnosti zdrojů a informací pro podporu fungování a monitorování těchto procesů. Mají být uplatněna opatření, nezbytná pro dosažení plánovaných výsledků a neustálého zlepšování.

U ISMS je normou vyžadováno vedení dokumentace, která zahrnuje: dokumentovaná prohlášení politiky a cílů, rozsah ISMS, postup a opatření podporující ISMS, zprávu o hodnocení rizik, plán zvládání rizik, dokumentové postupy související s provozem a řízením bezpečnosti informaci a prohlášení o aplikovatelnosti.

U managementu kvality norma udává nezbytnou dokumentaci. Stejně jako u ISMS je zde nutná dokumentace o politice a cílech. Na rozdíl od ISMS jde o politiku a cíle vzhledem ke kvalitě. Naopak v managementu kvality je zapotřebí vytvoření příručky kvality, která obsahuje oblast použití systému managementu kvality, dokumentované postupy vytvořené pro systém managementu kvality nebo odkazy na tyto postupy a popis vzájemného působení mezi procesy systému managementu kvality. Rozdíl mezi systémy je dosud patrný u ISMS při důrazu na dokumentaci spojenou s riziky.

Řízení dokumentu u ISMS a managementu kvality podléhá v rámci norem skoro naprosto stejným kritériím, která se týkají schvalování obsahu, aktualizace a opakovaného schvalování, identifikace změn dokumentu, zajištění dostupnosti v místech jejich použití, zajištění čitelnosti a identifikovatelnosti, zajištění identifikace dokumentů externího původu, řízení distribuce dokumentů, zabránění neúmyslného použití starých verzí. ISMS zde přidává pouze jeden bod navíc oproti managementu kvality a to je potřeba odpovídajícího **uchovávání a likvidace dokumentů**. Stejně tak je od organizací normami požadováno vytvářet a udržovat záznamy o shodě s požadavky a o efektivním fungování ISMS a systému managementu kvality. U ISMS je dodán požadavek na tvoření a udržování záznamů o výskytech bezpečnostních incidentů, vztahujících se k ISMS.

Normativní požadavky na závazek vedení vyžadují jak v ISMS tak v managementu kvality, aby vedení organizace poskytovalo důkazy o své angažovanosti při vytváření a implementaci, jak ISMS tak managementu kvality. Stejně tak organizace

musí zajistit zdroje a způsobilost lidských zdrojů tak, aby byly splněny všeobecné požadavky. U managementu kvality norma udává nároky na pracovní prostředí a infrastrukturu.

Norma od vedení organizace dále vyžaduje přezkoumání ISMS a systému managementu kvality. Na závěr obě normy vyžadují neustálé zlepšování, opatření k nápravě nedostatků a zavadění preventivních opatření.

Ze srovnání by se mohlo zdát, že systém managementu bezpečnosti informací je skoro to samé jako systém managementu kvality, ale tak to rozhodně není. V samotném textu norem se nenajde zmínku o propojení těchto dvou norem. Až na doporučení propojení bezpečnosti informací se všemi částmi organizace. Je pravdou, že jejich normativní požadavky se často shodují v přístupu k dané problematice, dokumentaci, vnímání organizace a jejich zaměstnanců. Je důležité si však uvědomit, že oba tyto systémy mají naprosto odlišné cíle, kterých chtějí dosáhnout. Využijí jiná opatření, která budou více odpovídat skutečným organizacím. Norma jim dává řád, aby tato opatření nebyla chaotická a měla všechny sounáležitosti potřebné ke správnému chodu. Proto nelze považovat samotnou normu za řešení problematiky bezpečnosti informace, ale pouze jako pomůcku k jejímu docílení.

Tabulka 1 Normativní požadavky

Normativní požadavek	ČSN ISO/IEC 27001	ČSN ISO/IEC 9001
Procesní přístup	Prosazení procesního přístupu	Doporučení procesního přístupu
	Neustále zlepšování založené na objektivním měření	Pochopení požadavků a jejich plnění
	Propojení ISMS s organizací	Neustálé zlepšování procesů založené na objektivním měření
	Model PDCA	Model PDCA
Terminy a definice	Nutnost znát definice spojené s ISMS	Přejaté definice z ISO 9000
Všeobecné požadavky	Ustavení, zavedení, provozování, monitorování, udržování a soustavné zlepšování dokumentovaného systému, kontextu všech činností a rizik, model PDCA	ustavení, zavedení, provozování, monitorování, udržování a soustavné zlepšování dokumentovaného systému
	Určení rozsahu a hranic ISMS	Určení procesy potřebné pro management kvality
	Definice politiky ISMS	Určování posloupnosti a vzájemné působení těchto procesů
	Stanovit přistup organizace k hodnocení rizik	určovat kritéria a metody pro zajištění a řízení těchto procesů
	Identifikovat rizika	Zajišťování dostupnosti zdrojů
	Analyzovat a vyhodnotit rizika	
	Identifikovat a vyhodnotit varianty pro zvládaní rizik	
	Vybrat cíle opatření a bezpečnostní opatření	
	Získat souhlas vedení organizace s navrhovanými zbytkovými riziky	
	Získat povolení ze strany vedení organizace k zavedeni a provozu ISMS	
Požadavky na dokumentaci	Dokumentovaná prohlášení politiky a cílů	dokumentovaná prohlášení o politice kvality a cílech kvality
	Rozsah ISMS	příručka kvality
	Postup a opatření podporující ISMS	dokumenty, včetně záznamů, určené organizací jako potřebné k zajištění efektivního plánování, fungování a řízení svých procesů
	Zprávu o hodnocení rizik	
	Plán zvládání rizik	
	Dokumentové postupy související s provazu a řízení bezpečnosti informaci	
	Prohlášení o aplikovatelnosti	
Řízení zdrojů	Řízení zdrojů	Poskytování zdrojů
	Zajištění zdrojů	Lidské zdroje
	Školení, informovanost a odborná způsobilost	Infrastruktura a pracovní prostředí
Zlepšování	Neustálé zlepšování	Neustálé zlepšování
	Opatření k nápravě	Opatření k nápravě
	Preventivní opatření	Preventivní opatření

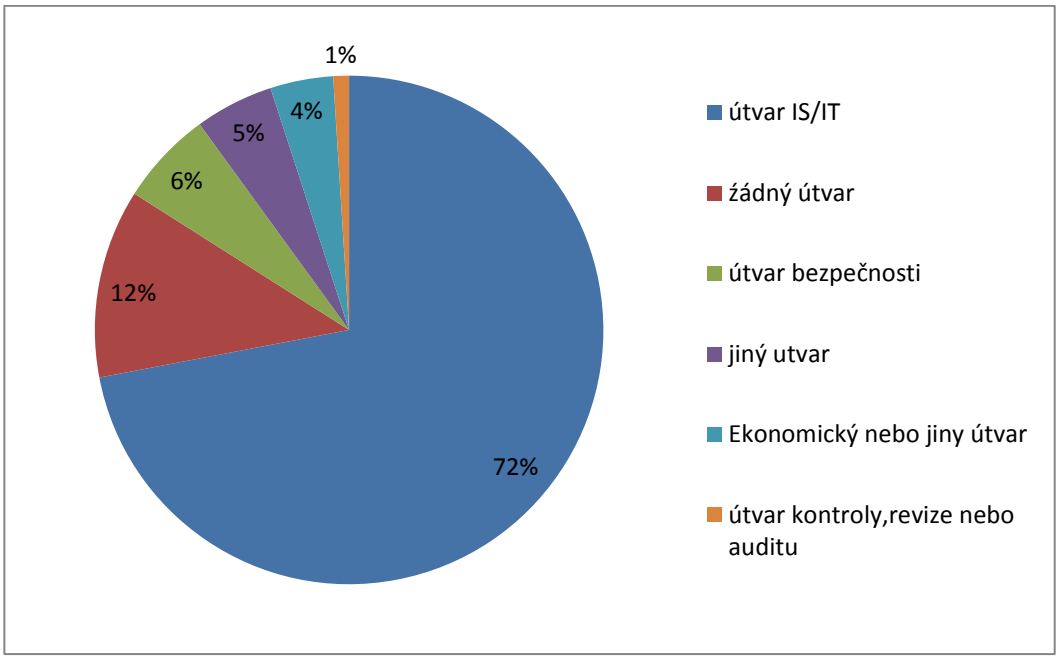
7 Stav bezpečnosti informací v České republice

7.1 Úvod

Na stav bezpečnosti informací v České republice je velmi těžké usuzovat. Organizace a soukromníci nejčastěji tuto problematiku neřeší buď z důvodu nedostatku financí, nebo neuvědomění si rizik a výhod, které jsou vypsány v předchozí části této práce. Velké množství přínosných informací obsahují zprávy Národního bezpečnostního úřadu, které se nazývají „Průzkum stavu informační bezpečnosti v ČR“, zkráceně PSIB ČR. Tyto zprávy byly vydávány od roku 2001 do roku 2009, s výjimkou roku 2002. Tyto zprávy se týkají ovšem větších organizací, se 100 a více zaměstnanci.

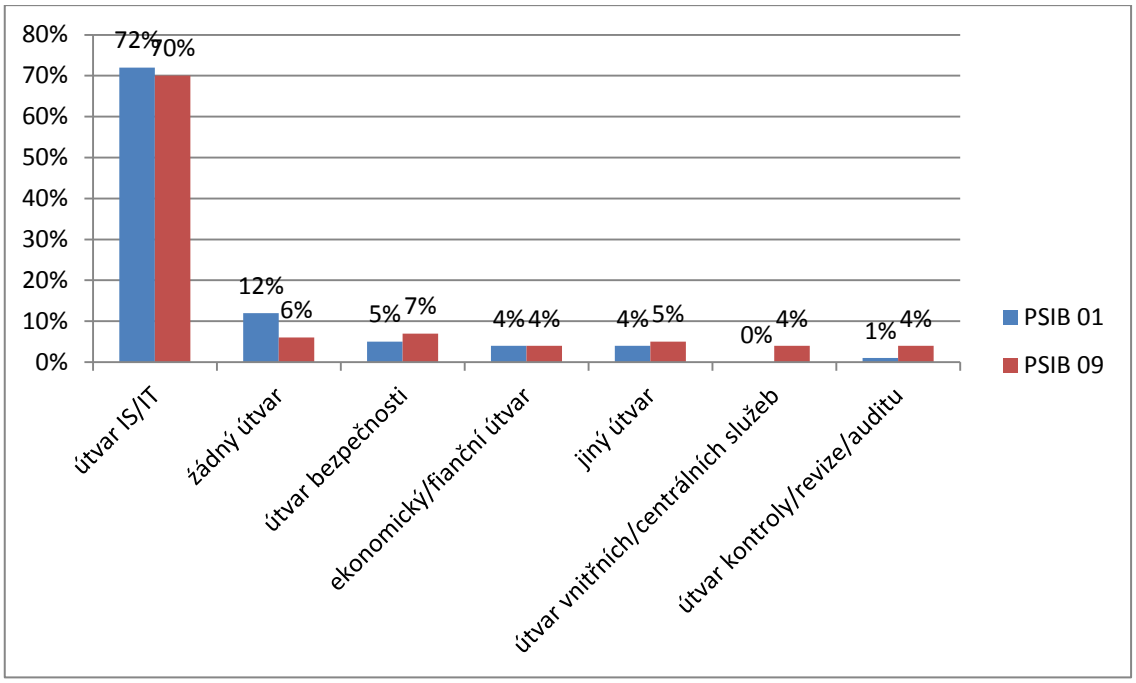
7.2 Kdo zodpovídá za bezpečnost informací

Z výsledků studie PSIB ČR z roku 2001 je jednoznačně zřejmé, že u většiny organizací je zodpovědnost za bezpečnost informací kladena na útvar IT/IS. Zdroj [13]



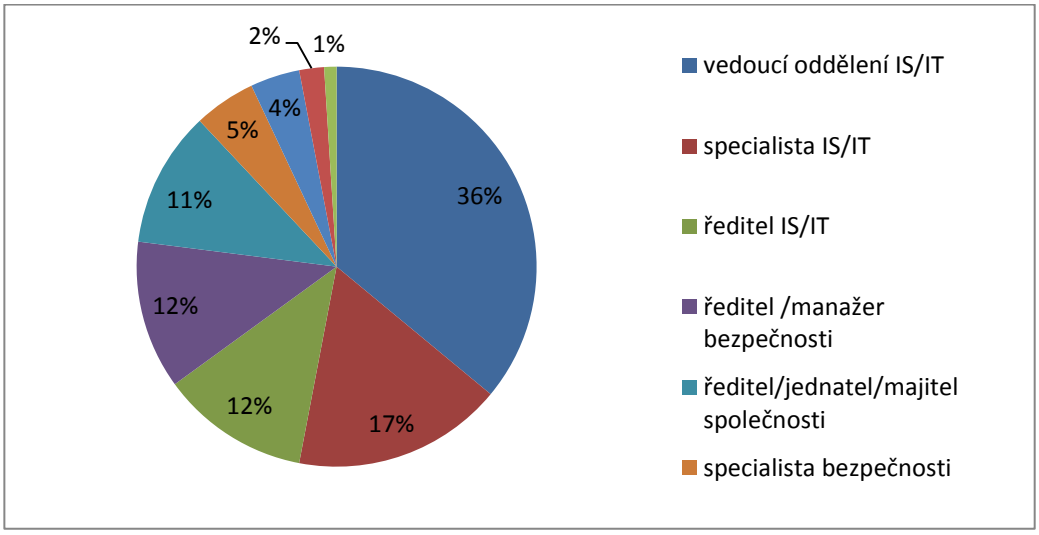
Obr. 6 Útvar zodpovědný za informační bezpečnost podle [13]

Z posledního šetření z roku 2009 je možno zjistit, že za 8 let se v této kategorii žádné velké změny neprojevily, až na jednu. Tou je snížení množství organizací, které nemají žádný útvar, který nese zodpovědnost za informační bezpečnost. Toto snížení je přesně na polovinu z 12% na 6% podle [13] a[14]. Celkové srovnání je viditelné v následujícím obrázku.



Obr. 7 Útvar zodpovědný za informační bezpečnost srovnaní podle [13]a[14]

Na obr. 8 je vidět podrobnější rozdělení odpovědnosti přímo na vykonávanou činnost osoby, zodpovědné za informační bezpečnost. Znovu je vidět že odpovědnost je předána nejčastěji na pozici, která má opět co dočinění s IT/IS. Zdroj [14]

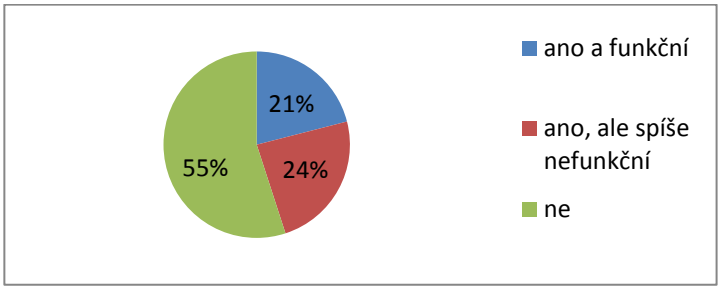


Obr. 8 Kdo za organizace odpovídá PSIB ČR 2009 [14, s. 8.]

V tom to šetření podle zdroje [14] byla také kladena otázka, zda se nějaký pracovník v organizaci věnuje informační bezpečnosti jako hlavní pracovní náplni. V roce 2009 vyšlo, že pouhý jeden zaměstnanec z pěti má jako hlavní pracovní náplň informační bezpečnost. Tento jev je opět způsobený častým přesouváním této problematiky na IT oddělení. Tím může vznikat jev absolutní moci nad systémem, nebo nezvládnutí základní problematiky.

7.3 Program na zvyšování bezpečnostního povědomí

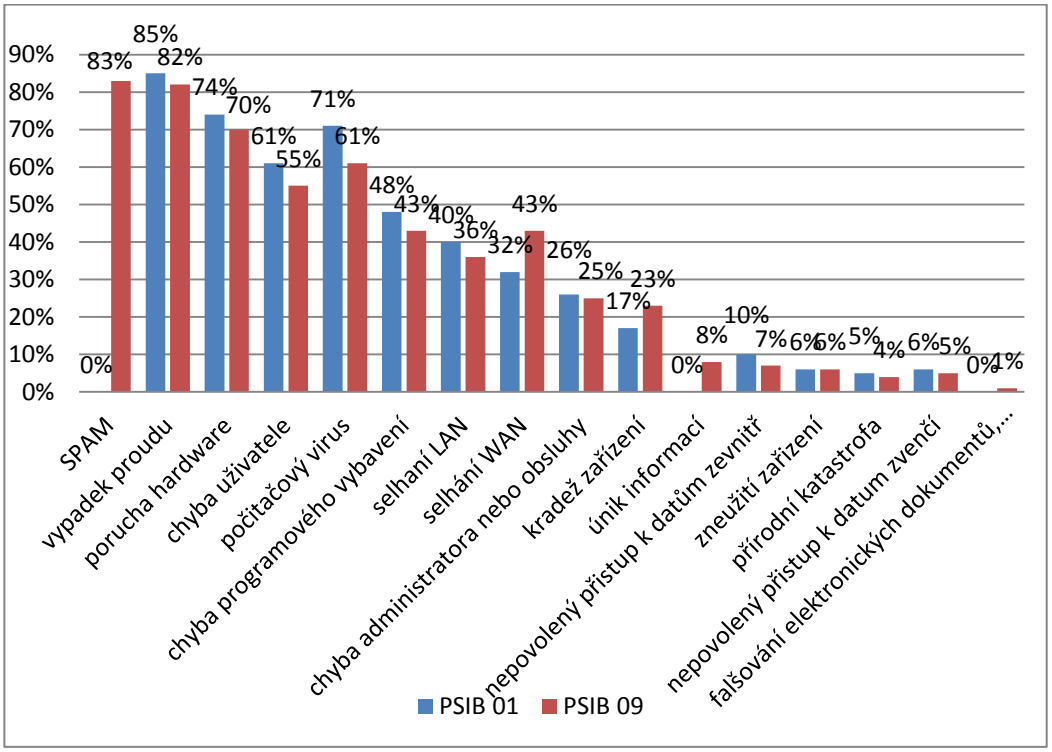
Bohužel podle PSIB zdroj [14] pouze 21% organizací potvrdilo, že má funkční program na zvyšování bezpečnostního povědomí svých zaměstnanců. Dalších 24% organizací má program, ale spíše nefunkční. Zbývajících 55% nemá žádný takový program. Toto číslo je vysoce alarmující a nahrává různým útokům a ztrátám informací. Je způsobené pouhou nevědomostí uživatele, nikoli neshodou softwaru nebo hardwaru. Tato neznalost pak např. nahrává phishingu apod. Autor práce si myslí, že tento faktor velmi úzce souvisí s mírou této kriminality nejen v ČR.



Obr. 9 Programu ke zvyšování bezpečnostního povědomí zaměstnanců. [14, s. 9]

7.4 Výskyt bezpečnostních incidentů

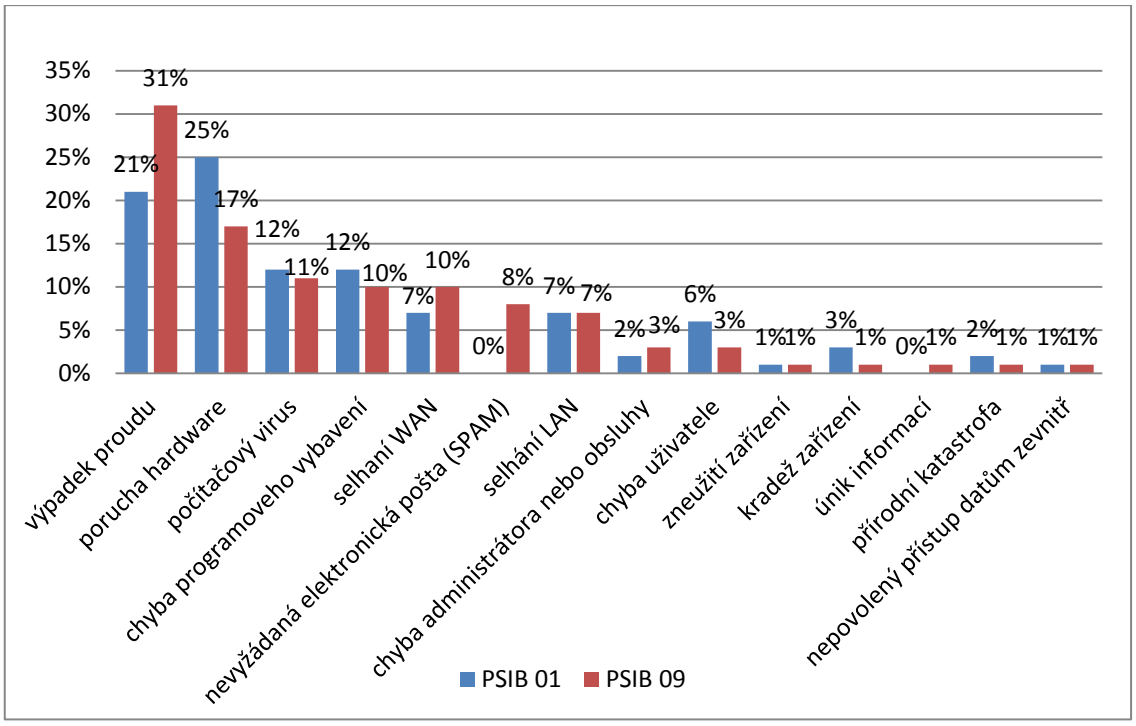
Z následujícího přehledu je vidět jaké byly nejčastější bezpečnostní incidenty v roce 2009 a s jakými incidenty se setkávaly organizace v roce 2001.



Obr. 10 Výskyt bezpečnostních incidentů zdroj [13, s. 7]a [14, s. 15]

Bohužel z obr. 10 je patrné, že u většiny položek není žádný znatelný pokles. Naopak je vidět vznik nových problémů jako např. SPAM. Tato otázka nebyla organizacím v roce 2001 vůbec kladena a v roce 2009 se s těmito incidenty setkalo 83% organizací. Z obrázku je také vidět větší závislost na sítích typu WAN (globální sítě). Větší využívání těchto sítí sebou přineslo větší množství incidentů spojených s těmito typy sítí (mezi sítě WAN se počítá i internet).

Ze statistik PSIB je možno také určit, jaké bezpečnostní incidenty mají největší dopad na organizace. Také je možno stanovit rozdíl ve vnímání závažnosti určitých incidentů jak v roce 2001, tak v roce 2009.



Obr. 11 Bezpečnostní incidenty s největším dopadem zdroj [13, s. 7] a [14, s. 15]

Z obr. 11 je patrná závislost organizací na elektrickém napájení a hardware a software a připojení k různým sítím. Pro někoho může být překvapivé, že největší problémy činí organizacím výpadky proudu. Bohužel při bližším zamyšlením se nad problematikou si člověk uvědomí, jak je jeho závislost na elektrickém napájení veliká. Výpadky proudu činí v organizacích hned několik druhů škod vzhledem k činnostem, kterými se organizace zabývají. Všechny organizace, ve kterých se autor práce sám dotazoval bez ohledu na to, ať pracovníci řešili problematiku bezpečnosti informace nebo ne, odpověděli, že výpadek proudu pro ně je vždy problém, protože nejsou schopni nahradit plně elektrické napájení ze sítě. Pokud dojde k výpadku proudu, nastane také přerušení činnosti, kterou vykonávají. Dopad je o to větší, že jsou i organizace, kde výpadek proudu znamená nejen přerušení činnosti, ale i ztráty na rozpracovaném materiálu, protože určité výrobní procesy nesnesou přerušení. Po takovém výpadku jsou nuceni rozpracovaný materiál zahodit a začít od začátku. Přesto je pro ně takové riziko přijatelné, protože náklady na zajištění velkých elektrických zdrojů jsou mnoho násobně vyšší. Obchodníci se také nesnaží udržet počítače v chodu při výpadku proudu, protože ve výsledku nestačí pouze zajistit napájení počítače nebo kasy, ale je zapotřebí osvětlení napájení počítačových sítí atd. Náklady na zajištění takto rozsáhlých funkcí jsou tak vysoké, že se jejich prevence nevyplatí.

7.5 Reálný stav v organizacích

Jako vzorek pro průzkum reálného stavu bezpečnosti informací byly použity organizace, ve kterých externě pracoval autor práce, nebo organizace, v nichž pracovali jeho známí či příbuzní, kteří byli následně podrobeni řízenému rozhovoru. Nemalá část podkladů vychází ze zkušeností autora získaných s opravami a údržbou IT vybavení. Organizace měly různý druh zaměření své produkce, různou velikost (od 1 do 5000 pracovníků) a působiště na území ČR. Např. živnostníci a malé organizace i velké organizace, pracující v oboru dřevozpracujícím, elektrotechnickém, strojírenském, automobilovém, plastikářském, programátorském, obchodním, servisním a zpracování administrativy. Mezi organizacemi byla i malá, která byla certifikovaná podle normy ČSN/ISO/IEC 27001.

Ze získaných podkladů autor rozdělil organizace do čtyř pomyslných skupin.

7.5.1 První skupina malé organizace

První skupina jsou malé organizace, nejčastěji živnostník buď pracuje sám, nebo celá organizace čítá jen pár osob, nejčastěji „rodinné firmy“. V těchto organizacích se většinou nenachází velké množství informací, které tyto organizace potřebují chránit, jako je tomu u velkých organizací. Dost často si pracovníci sami neuvědomují, že tyto informace vlastní. Nejčastěji až při dotazování autora na informace k vypracování této práce v organizaci přišli na to, že ve své organizaci mají informace, které pro ně mají vysokou cenu, ale berou je jako samozřejmost. V některých organizacích sami věděli, že určité informace mají určitou cenu. V těchto organizacích nejčastěji nějaký problém s bezpečností informace již řešili a proto si uvědomovali, že tyto informace vlastní a jsou pro ně důležité. Např. jde o údaje o svých dodavatelích a zákaznících, výrobní postupy, ceny materiálu, licence, účetnictví, rozpracovanou práci. Tyto organizace jsou velmi spjaté s pracovníky. Je to dáno malým množstvím pracovníků v organizaci. Ve výsledku to vypadá tak, že přístup k bezpečnosti informací je dán pouze chováním a znalostmi osob, pracujícími v organizaci. V organizaci to vypadá jako v běžné domácnosti. Informace v tištěné nebo písemné formě jsou nejčastěji ukládané na jedno místo, nejčastěji do skříně. Uživatelé v nich nemívají velký přehled a pořádek. U těchto informací nejčastěji dotazované osoby zodpověděly, že největším problémem je dostupnost těchto informací. Buď zrovna potřebují dané informace a v tento okamžik se k nim fyzicky nemohou dostat, nebo je zrovna nemůžou najít. Hledání jim zabírá čas, který by pracovníci vyplnili jinou činností. Objevily se i odpovědi, že informace

v papírové formě pracovnici ztratili, nebo jinak zničili, nejčastěji svojí nepozorností nebo špatným systémem ukládání. Nikdo neodpověděl, že by za ztrátou informace v papírové formě stála cizí osoba.

Počítačové vybavení a sítě si v těchto organizacích nejčastěji spravuje přímo nějaká osoba z organizace nebo jeho příbuzný či známý. U některých organizací byly sítě a počítače dodány a nainstalovány odbornou organizací, ale po instalaci již neprováděla žádné další služby, spojené s údržbou či aktualizací. Počítačové vybavení je velmi často používáno jak pro pracovní účely, tak pro soukromé účely. Připojení k internetu je dodávané externí firmou, v dnešní době nejčastěji přivedeno na router[1], který obstarává oddělení internetové sítě od domácí a rozdělením signálu na více počítačů, šíření signálu bezdrátově. Stejně jako domácnosti i v těchto případech routry bývají málo zabezpečené, používají se staré protokoly, nepoužívá se třídění MAC[2] adres. V malých organizacích a v domácnostech je naprosto běžné, že heslo pro přístup k wifi zůstává pořád stejné od nainstalování zařízení až do doby, kdy zařízení přestane pracovat. Tento jev stále nevymizel. Nejčastější odpovědí na dotaz: „Jak často měníte heslo na wifi?“, je „Nikdy.“. Není ani ojedinělá odpověď: „Nevím, jaké tam je heslo. Někde to mám napsané.“

U těchto organizací je skoro pravidlem, že emailová adresa je zřízena pod jinou organizací, nejčastěji v současné době je to Seznam, Google, dříve např. Volný, Atlas apod. Heslo k emailovému účtu většinou nikdo nemění a dost často si ho ani nepamatuje. Je uložené v prohlížeči. Je velice snadné najít organizaci z tohoto okruhu, která měnila emailovou adresu po tom, co se jim rozbil počítač a nepamatovali si heslo. To dále doprovází ztráta doručené pošty, ztráta uložených kontaktů, tištění nových vizitek, nedostupnost, protože spousta lidí má uloženou starou adresu apod.

Zálohování v malých organizacích je snad nejvíce opomíjeným místem. V malých organizacích se buď nezálohuje vůbec, nebo záloha probíhá ručně. S ruční zálohou je spojená spousta opomíjených věcí. Velmi často se na ni zapomíná, bývá nepravidelná a neobsahuje všechny důležité údaje. Většinou se stává, že zálohovaným informacím

[1] Router (směrovač) je v počítačových sítích aktivní síťové zařízení, které procesem zvaným routování přeposílá datagramy směrem k jejich cíli.
[2] MAC adresa (Media Access Control) je jedinečný identifikátor síťového zařízení.

chybí správný řád či smysluplné pojmenování. Proto je dost obtížné nalézt správný soubor s poslední zálohou.

Záloha telefonních kontaktů je v těchto organizacích také velmi slabá. Někteří uživatelé používají zálohu přes internet na mobilních telefonech s operačním systémem Android, ale tito uživatelé bývají nejčastěji mladší 30 let. Najdou se i takoví uživatelé, kteří mají telefon s touto funkcí, ale nevědí o ní, nebo nejsou schopni ji využít. Někteří uživatelé z okolí autora odpověděli, že ukládají kontakty do počítače pomocí synchronizace, ale žádný uživatel neodpověděl, že by synchronizaci prováděl v pravidelném časovém úseku.

7.5.2 Druhá skupina organizace bez IT oddělení

Nejčastější rozdíl mezi touto a předchozí skupinou je ve změně řízení a chování celé organizace. V těchto organizacích, se už ztrácí nahodilost a individualita jednotlivých bezpečnostních opatření. Vztah k bezpečnosti informací jednotlivých zaměstnanců se odvíjí od zaměstnavatele. Organizace již má více zaměstnanců, ale není dostatečně veliká, aby měla vlastní IT oddělení. Počítače a sítě bývají zřizovány odbornou organizací. V organizacích se absence interního IT pracovníka řeší tím, že na menší zásahy a úpravy bývá vyhrazen jeden člověk, ale není to jeho hlavní pracovní náplní. Při problémech nebo potřebě změn se organizace obrací na externí podnik, se kterým je předem domluvena a tato firma se problémem zabývá.

V těchto případech je problém v tom, že externí pracovník zná spoustu detailů o vnitřním uspořádání informačního systému. Je velice časté, že externí pracovník zná slabá místa informačního systému někdy i přístupová hesla. V těchto případech se často sází na dobré osobní vztahy mezi organizací a externím podnikem. Nelze 100% říct, že externí podnik rovná se ihned chyba v bezpečnosti informace, ale organizace již ztrácí možnost sama být paní situace a musí se spolehnout na bezúhonnost cizí organizace. Může nastat i scénář, že sama externí organizace nechce nijak zneužít údaje, které o cizí společnosti zná, ale sama se může stát terčem určitého útoku a tím ohrozit i ostatní organizace, na ní závislé.

7.5.3 Organizace s IT pracovníkem

Organizace, která má velké množství IT vybavení a její činnost je na tomto vybavení hodně závislá, se již nejčastěji nespoléhá na externí dodavatele služeb, ale má svého IT pracovníka či pracovníky. V těchto organizacích sice odpadají rizika spojená

s externí společností, ale přibývají jiné velmi časté jevy. V organizacích s jedním či dvěma IT pracovníky se stává, že daná osoba je takzvaný „pán systému“. Pokud je IT pracovník pouze jeden, jev vznikne tím, že pracovník spravuje celý IT systém. Má sice nadřízené pracovníky, ale ti se v systému nevyznají. Sice dostává pokyny, co má dělat apod., ale jeho kroky prakticky nikdo nekontroluje, protože kontrolou IT vybavení je pověřen IT pracovník. Dost často tento pracovník přiděluje přístup a práva k systému a nepotřebuje k tomu nikoho dalšího. IT pracovník bývá administrátorem systému, což je logický krok. Ovšem podle hierarchie organizace platí, že čím výše postavený pracovník, tím vyšší má práva. To ovšem znamená, že nadřízený pracovník by měl mít také administrátorské právo, ale jeho neodborné zásahy můžou způsobit velké potíže. Částečně v některých organizacích tento problém řeší tím, že zde pracující dva IT odborníci, i když by na práci stačil jeden. Určité zásahy musí vykonávat pouze společně. Myšlenka je taková, že jeden by měl kontrolovat druhého. I toto opatření není 100%, protože se pracovníci mohou spřátelit, nebo si chtějí ulehčit práci a svoje přihlašovací údaje znají navzájem.

7.5.4 Velké organizace

U velkých organizací je problematika bezpečnosti informací velmi složitá. Organizace mají celé IT oddělení. Struktura organizace je velmi rozlehlá. V organizacích se projevují bezpečnostní opatření z jiných oddělení. Vyhlášky přicházejí z center, velmi často ze zahraničních. Na řešení problematiky se najímají celé specializované organizace. Každá organizace musí řešit jiné problémy, používat jiné postupy. Jediná věc je ve všech velkých organizacích stejná a to je, že v ní pracují lidé. Ti jsou rozděleni do různých vrstev a dle autorova názoru neexistuje žádná organizace, ve které se nenajde zaměstnanec, který nechápe, nebo si není schopen odůvodnit smysl některých opatření a proto je nedodržuje. Ve spoustě organizací si ve vedení myslí, že na nich je vymýšlet a na podřízených je poslouchat. Občas není na škodu věci více vysvětlit a naopak naslouchat zpětně, co si o opatřeních myslí podřízení.

7.6 Stav bezpečnosti informací vzhledem k procesnímu přístupu

7.6.1 Hlavní body procesního přístupu

Procesní přístup se v dnešní době využívá v organizacích k zlepšení návaznosti procesů, určení slabých míst, a poté k navazujícímu zlepšování, které by mělo vést k větší efektivitě a splnění přání zákazníka. Podle zdroje [15] bezpečnost informací využívá nebo by v ideálním případě měla používat některé postupy, které stanovuje procesní řízení implementovat je a díky nim se dostat blíže k dosažení svých cílů.

Bezpečnost informací by si z procesního řízení měla využít:

-Model PDCA

-Každá část bezpečnosti informací musí pracovat tak dobře, aby nekazila celkoví výsledek

-Oddělení zabývající se bezpečnosti informací by měl spolupracovat, se všemi ostatními úseky na neustálém zlepšování.

-Ideálně pracovník danou práci musí vykonávat a současně jí chce vykonávat

-Organizace by měla vést k neustálému zlepšování

-Každé dílčí zlepšení by mělo, vést ke zlepšení celku

7.6.2 Zhodnocení

Některé organizace, hlavně ty menší, nevyužívají procesní řízení v žádných svých činnostech, v některých se nevyužívá vědomě, nebo spíše využívají jeho principy, ale nepojmenovávají tyto kroky jako procesní řízení. A v některých je procesní řízení využíváno naplno. Podle autora není nutné hned zavádět kompletní procesní systém z důvodu náročnosti, která může u organizace způsobit pravý opak, než je kýžený výsledek, ale naopak je velmi výhodné využít některé myšlenky a postupy, které procesní řízení přináší.

Většina špatných výsledků z ohledu bezpečnosti informací souvisí s nedodržením modelu PDCA. Ten nahlíží na organizaci jako na celek, proto většina neshod vyplývá jeho z nedodržení. Některé organizace málo dodržují poctivý výkon, všechny čtyři kroky modelu PDCA. Nejčastější problém je, že vykonávají druhý krok, tedy, „dělej“ bez toho, aby pracovníci měli nejdříve dobře zvládnutý krok „plánuj“, tím pádem nemůže být opatření tak účinné, jak by mohlo být. Stejně tak opomíjení kroků

„kontroluj“ a „jednej“ vede k nedoladění bezpečnostních opatření do potřebného výsledku. Druhá možnost, spojená s procesním řízením a modelem PDCA je, že organizace provede tento postup správně, ale pouze jako jednorázovou akci. V tom případě se nejedná o organizaci, která se snaží o neustálé zlepšování, což je v rozporu s procesním řízením.

Z výsledků PSIB i zkušeností autora z praxe vyplývá, že bezpečnost informací závisí na vybavení a na pracovnících. Pracovníky je možno ještě rozdělit do dvou skupin, na ty co vymýšlejí pravidla a ty co se s nimi mají řídit. Jak vybavení tak pracovníci obou skupin musí pracovat propojeně a vyrovnaně. Pokud tato podmínka není splněna, je to v rozporu s procesním řízením. Problém vede k zbytečnému oslabení bezpečnosti informací. Tyto tři časti si lze představit jako řetěz a ten je silný jako jeho nejslabší část. Dobrý systém lze stavět pouze na dobrém a vhodném vybavení, dobrých nařízeních a ty musí být správně pochopeny a vykonávány.

Některé bezpečnostní problémy nejen v bezpečnosti informací jsou spojené s tím, že pracovníci některé činnosti vykonávají, protože musí, ne protože chtějí. Toho je všeobecně dost těžko dosáhnout, ale občas stačí problém vysvětlit a zdůvodnit, proč je nutné činnost vykonávat, ke zlepšení. Zlepšení nebude vždy, od „musím“, na „chci vykonávat“, ale může vést od „musím“, ale nedělá, na není oblíbená činnost, ale vykonává. K zlepšení může dojít tím, že činnost je přizpůsobena uživateli, ne uživatel činnosti. Tato myšlenka je opět z procesního přístupu a je málo kdy implementovaná do bezpečnosti informace.

Z reálných organizací je také viditelný problém v přenášení veškeré zodpovědnosti za bezpečnost informací na IT oddělení. Tím pak vzniká místo, kde je nakumulováno velké množství práv a povinností. Může se pak stát, že samo toto místo může být bezpečnostním problémem a zároveň problém vzhledem k procesnímu řízení, protože toto místo je místem úzkým a celou organizaci zdržuje.

8 Jak chránit své informace?

Prvním krokem je uvědomit si důležitost informací. Druhým krokem je chtít je chránit. Jednou z možností je postupovat podle normy a zavést ISMS (Information Security Management System). Jak zavést ISMS je popsáno v normě ČSN ISO/IEC 27001. Ovšem samotná norma je pouhým výčtem postupů a zásad. Jejich implementace závisí na druhu organizace, množství pracovníků atd. Vytvoření ISMS podle normy ocení hlavně velké organizace, kde jsou pracovníci více zvyklí využívat normy. Následující doporučení se nebudou vztahovat na velké organizace, protože by dle autorova názoru nemělo žádný smysl je v této práci řešit, protože u velkých organizací je individualita jejich potřeb a rozsáhlost systému tak veliká, že se v těchto organizacích tímto problémem zabývají celé týmy. Na tuto problematiku rozsah této bakalářské práce nestačí. Proto se bude tato kapitola zabývat menšími organizacemi. Zde je podle autorova názoru spousta problémů velmi snadno řešitelná a přitom velmi opomíjená.

8.1 Jak začít?

V každé organizaci je dobré postupovat podle nástroje PDCA [11]. Prvním krokem je „plánuj“. Zde by si organizace měla uvědomit hodnotu svých aktiv, možnosti hrozeb a zranitelnost. Záleží pouze na organizaci, jak bude postupovat. Jestli bude spolupracovat s nějakým externím podnikem, nebo zvládne problém řešit sama.U malých organizací, kde problematiku pracovnici dosud naprosto opomíjeli, je i pouhá rozvaha ředitele a jeho zaměstnanců přínosným krokem. Hodnota aktiv, hrozby a zranitelnost je popisována v této práci výše. Zde je také popsán nesnadný systém hodnocení.

Pokud je hotová analýza, přijde na řadu druhý krok „dělej“. V této části by organizace měla zavádět opatření na místech a v rozsahu, která vyplynula z předchozího kroku plánování. Pokud organizace zná hodnotu svých aktiv, hrozby a zranitelnost, může vynakládat úsilí na nejdůležitější opatření. Organizace proti některým rizikům vytvoří protiopatření. Některá rizika může vyhodnotit, jako akceptovatelná příp. si může zjednat pojištění, které by mohlo částečně pokrýt vzniklé ztráty.

Možná opatření jsou školení personálu, záloha dat, autentizace, autorizace, změna práce s daty a s nosiči informace, lepší zabezpečení přenosových cest, bezpečná práce s datovými médii, rozložení práv mezi více lidí (obtížný krok, kumulace práv je bezpečnostní riziko, rozdělení práv může způsobit menší efektivitu práce). Do

bezpečnostních opatření se počítá také stanovení postupů pro zálohování a zpětné použití záloh a postupy pro řešení problémů. V některých případech je postačující vědět, kam se obrátit v případě bezpečnostního incidentu.

Další krok se nazývá „kontroluj“. Zde by měla organizace zhodnotit, jak jsou účinná její protiopatření. Organizace by měla být schopná zpětně posoudit, jak účinná byla její preventivní opatření. Např. snížení množství nebo úplné zamezení bezpečnostním incidentům. Důležité je také snížení jejich dopadu, tj. pasivní testování. Je možné i aktivní testování. např. namátková kontrola, zkouška použití záložních dat, nebo ty složitější, jako jsou útoky na vlastní systém.U testu, jako nabourávání vlastního systému, je třeba mít o problematice velké znalosti, nebo je třeba si na toto testování pozvat cizí organizaci. Tyto testy mohou odhalit slabiny systému dříve, než je odhalí skutečný útočník a pomáhají uživatelům se připravit na situace, které mohou nastat. Můžou si je zkusit tzv. „nanečisto“ a tím urychlit a zpřesnit své počínání ve skutečné situaci.

Čtvrtý krok je „jednej“. Je to krok, ve kterém by měly organizace opravit, nebo vyladit preventivní opatření a zásahy, které organizace stanovila v kroku „dělej“ a během třetího kontrolního kroku se ukázalo, že jsou tato opatření nedostačující, nebo nefungují tak, jak by měla. Tento krok je sice poslední, ale pouze v pořadí kroků.

Pro kvalitní bezpečnost informací je třeba po čtvrtém kroku znovu začít prvním. Z důvodu možných změn, které nastaly v organizaci od vykonání prvního kroku do čtvrtého. Dalším důvodem je vývoj technologií. Stejně tak jak organizace buduje svoji ochranu, útočníci neustále vynalézají nové „zbraně“ a vylepšují ty stávající. Proto je nutné provádět tento cyklus pořád dokola tak, aby vedl k neustálému zlepšování systému.

Je doopravdy důležité po čtvrtém kroku „neusnout na vavřínech“ a neříct si, konečně je hotovo a skončit. Je pochopitelné, že tempo po uzavření prvního cyklu trochu opadne, ale je důležité neustále systém analyzovat a modifikovat.

8.2 Jaké kroky dělat přednostně

Nejjednodušší rozhodovací mechanismus co dělat přednostně, dává již zmiňovaný vzorec: Hodnota aktiva * Hrozba * Zranitelnost= Míra rizika. Tam, kde je Mira rizika největší, by organizace měla podnikat opatření přednostně. Další možnost rozhodovaní

je začít tam, kde za nejmenší náklady je možno docílit největšího přínosu v bezpečnosti informací.

Lze také použít nástroje spojené s managementem kvality jako např. Paretův diagram. Díky němu lze získat podíl bezpečnostního opatření na celkovém účinku a tím naznačit prioritní opatření. Nebo je možné použit diagram příčin a následků a to v případě, kdy se organizace snaží zamezit určitým následkům za pomocí vyřešení jejich příčin.

U menších organizací, nebo organizací, které zrovna nemají volný kapitál, který by mohly investovat do ochrany informací, je dost pravděpodobné, že se nebudou chtít zabývat složitými postupy, jako zakoupení a studium norem. Proto v další části práce budou vypsány některé části a postupy, které jsou vhodné pro tyto organizace nebo i pro jednotlivce v běžném životě.

8.2.1 Informace

První krok, který musí člověk nebo organizace řešit, je, jaké informace vlastní. Pak si musí položit otázku, které informace je potřeba chránit. Následuje zamyšlení nad formou použití nosiče informace a jaké využívá přenosové cesty.

8.2.2 Chování uživatele

Tou naprosto nejzákladnější ochranou informací může být i správné chování uživatele. Je spousta možností, jak může uživatel přispět k ochraně informací bez vynaložení jediné koruny. Např. trocha rozvahy v rozhovorech, jak v pracovních, tak soukromých. Občas se doopravdy vyplatí se zamyslet, co a komu člověk řekne. Druhá rada zní, nenechávat nikdy nikde ležet žádný nosič informace. Např. dávat papírové dokumenty do zásuvky stolu. Volně na stole jsou mnohem více v ohrožení než v zásuvce, která nemusí být ani zamčena. Nenechávat datová media (flash disk, externí disk, CD, DVD) volně ležet, nebo jejich obsah alespoň ochránit heslem. Když uživatel opustí počítač, je dobré zamezit přístupu cizím osobám. Např. je dobré odhlásit uživatele ručně, nebo používat automatické odhlášení při nečinnosti. Stejně by se měl člověk chovat s mobilním telefonem. Uživatel internetu a emailu by se měl na internetu chovat s rozvahou a neklikat všude bez rozmyslu. Např. emaily o výhrách a speciálních akcích neotevírat. Vždy je předem lepší zamyslet se, jestli se člověk nějaké soutěže zúčastnil, podívat se na příchozí adresu a až potom otevírat odkazy a stahovat přílohy.

Uživatel by měl být ještě více na pozoru, pokud se připojuje na email, nebo zadává nějaké osobní údaje na cizím zařízení. V těchto případech je dobré využít anonymního módu, pokud jej zařízení podporuje. V anonymním módu se neukládá historie, HTTP cookie ani hesla. Pokud zařízení tento mód nepodporuje, je dobré po ukončení činnosti smazat danou část historie a cookies. A v žádném případě nepotvrzovat uložení uživatelského jména a hesla. Pokud se tak stane, je opět zapotřebí heslo z prohlížeče vymazat (bohužel u každého prohlížeče je mazání uložených hesel umístěno jinde, nejčastěji v části Nabídky, spojené s Nastavením a Nástroji). Pro větší jistotu je dobré po odhlášení, např. emailu, zkontrolovat, jestli si prohlížeč doopravdy jméno a heslo nepamatuje. (Zde je vlastní zkušenost autora, kdy půjčil mobilní zařízení příteli, aby se mohl podívat na email a heslo i jméno bylo uloženo, přestože přítel tvrdil, že zadal neukládat. Stejnou věc autorovi této práce potvrdili i jiní uživatelé s jinými mobilními zařízeními).

Uživatelé by se měli vyvarovat ještě jednomu častému nešvaru a to je vytváření nevhodných hesel, jako jsou rodná čísla, rok narození nebo datum narození. Heslo by ideálně nemělo být reálným slovem, nebo jej alespoň obohatit o velká písmena na místa, kde ve slově normálně nejsou nebo přidat číslice. Nevyjímaje to, že heslo by mělo být přiměřeně dlouhé. A nejdůležitější je se vyhnout heslům jako: „abcd, 12345, heslo, password, qwerty“ apod. Další příklady může čtenář najít v tomto zdroji [16]. Dobrou radou je hesla měnit a nevyužívat svá nejdůležitější hesla na více službách, natož používat stejné heslo na službách propojených. Např. na službách, kde je přihlašovací jméno emailová adresa uživatele, **nepoužívat stejné heslo**, jaké má nastavené pro přístup k poště této emailové adresy.

8.2.3 Papírová data a papírové informace

Záznamy na papíře jsou velmi úzce spojené s uživatelem těchto dokumentů. Pokud se zlepší chování uživatele, s ohledem na bezpečnost informací hrozí menší riziko i těmto záznamům. Další ochranou je správné třídění a uchování. Vynaložený čas na třídění se může velice rychle vrátit v případě hledání dokumentu, kdy správné vytřídění šetří čas a je prevencí ztráty dokumentu. Ochranou proti ztrátě může být vytváření kopií. V tomto ohledu se ovšem musí organizace rozhodnout, co je pro ni větší riziko, zda je to ztráta informací nebo nechtěné sdílení. Pokud se vytváří kopie, je menší riziko ztráty, ale s rostoucím množstvím kopií roste riziko nechtěného sdílení.

Pokud jsou vytvářeny elektronické kopie, je důležité zaměřit se na zabezpečení elektronických dat.

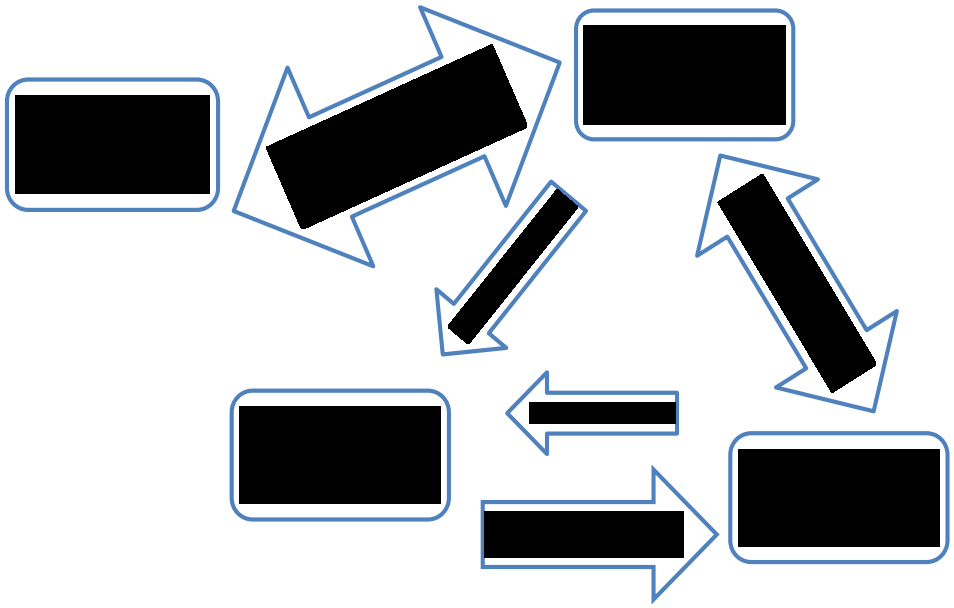
8.2.4 Elektronická data a elektronické informace

Základní doporučení je znát svoje elektronické vybavení. Pokud uživatel nemá ani minimální znalosti o svém elektronickém vybavení, je to veliký problém. V tom případě buď spoléhá na náhodu, nebo se musí spoléhat na cizí osoby, což sebou přináší opět riziko. Když člověk zná své vybavení, může předejít problémům s nevhodným zacházením, které vede k zničením vybavení nebo ke zkracování životnosti. Znalost může vést k většímu využití potenciálu zařízení.

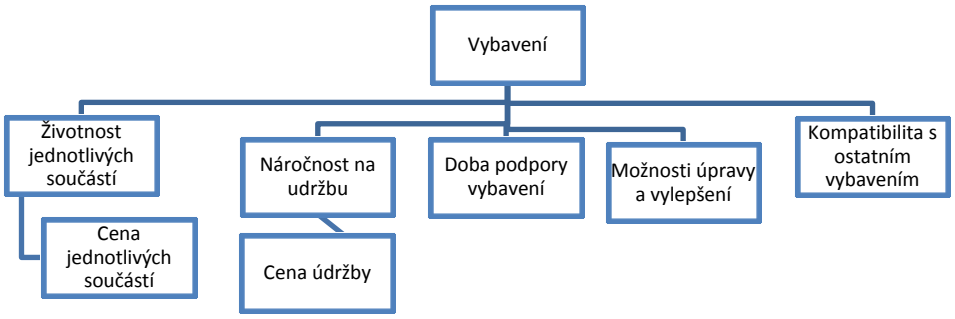
První věc je datové propojení zařízení. Je důležité vědět, jestli je drátové, nebo bezdrátové. Pokud je drátové, kudy vede, kde jsou spoje a výstupy jak je chráněno. U bezdrátových zajímá uživatele, do jaké vzdálenosti se do sítě lze připojit a hlavně jaká jsou aplikovaná bezpečnostní opatření.

Další nepostradatelnou součástí každého člověka či organizace jsou stolní a přenosné počítače. Znovu je třeba vědět, jakému zacházení se má člověk u daného výrobku vyhnout a co naopak dělat pro prodloužení životnosti. Nejdůležitější je se zaměřit na chlazení a média pro ukládání dat.

Je důležité využívat antivirové programy a další pomůcky, které jsou mnohým uživatelům přístupné, ale nevyužívané pouze z neznalosti. Při nákupu nových zařízení je důležité, aby zařízení co nejvíce odpovídalo podmínkám a požadavkům, kterým bude počítač vystavován. Stejné je to u mobilních telefonů. Na moderních mobilních telefonech je třeba mít antivirové programy a stejně tak vhodné zařízení a nastavení může mít velký dopad na bezpečnost informací. Je mnoho uživatelů, kteří kupují různá zařízení bez dostatečného promyšlení věci. Nejčastěji se tak děje z důvodu, že dané problematice nerozumí a nechtějí ztrácet nákupem čas. Bohužel ve většině případů je to jen pouhá domněnka, že čas šetří. Dost často se později projeví, že zařízení není vhodné, např. není dost spolehlivé, nebo jeho funkce není optimální. A uživatel znovu vynakládá čas a finance, někdy i větší než ušetřil při prvním nákupu. Pokud je možné, má se přizpůsobit vybavení uživateli a nepřizpůsobovat uživatele vybavení.



Obr. 12 Ideální způsob pořizování vybavení vzhledem k informační bezpečnosti



Obr. 13 Důležité přitom málo kladené otázky na vybavení

8.3 Stolní počítače, notebooky a mobilní telefony

Tyto tři produkty jsou nejčastějším vybavením organizací a běžných lidí v soukromí. Mají velkou souvislost s informacemi, protože jejím prostřednictvím lze informace získávat, ukládat a šířit. Vztahují se na ně všechna předchozí upozornění a také rady spojené elektronickým vybavením. Z důvodu jejich masového rozšíření zde autor této práce chce popsat problematiku tohoto vybavení konkrétněji. Z požadavku na dostupnost informací vyplývá, nutnost udržovat tyto tři druhy zařízení v co nejlepším stavu, tak aby zařízení pracovala přiměřenou rychlostí a co nespolehlivěji. To znamená

provádět softwarovou a hardwarovou údržbu a nevystavovat zařízení nevhodným podmínkám.

8.3.1 Stolní počítače

Všechny stolní počítače jsou chlazeny pasivně i aktivně, minimálně elektrický zdroj a procesor. Dost často i grafická karta je chlazená pasivně i aktivně. Pasivní chlazení znamená umístění žebrování z teplo vodivého kovu v blízkosti zahřívající se části. Toto žebrování teplo odvádí ze zahřívajících se častí, díky žebrování pak dále teplo sálá do prostoru. Aktivní chlazení znamená nejčastěji použití elektrického ventilátoru. V ojedinělých případech je vodní chlazení. Ventilátory dělají z počítače vysavač na prach. Pokud je počítač zanesen prachem, prudce se zvedá teplota některých součástí. To způsobuje zmenšení životnosti nebo až zničení některých částí počítače. Běžné je snížení výkonu z důvodu autoregulace teploty. V některých případech dochází ke zvýšení hlučnosti, protože větráčky zvýší počet otáček a snaží se součástky uchladit. Proto je třeba **počítač čistit od prachu**. Jedna možnost je dát jej do servisu, nebo ho může uživatel vyčistit sám vysavačem, nebo stlačeným vzduchem. (Počítač by měl být vypnutý! Je lepší neroztáčet lopatky ventilátorů externím proudem vzduchu, lopatky jemně přidržet.) Mezi chlazením procesoru a procesorem je pasta, kterou je potřeba měnit (2-3 roky podle kvality pasty a zatížení PC).

PC by se mělo chránit proti „úderu“ elektrického proudu, tj. odpojit napájení, sítě LAN a připojení internetu. Odpojovat pouze napájecí kabel je značně neefektivní. Nebo je tu druhá možnost, pořídit si zásuvku nebo prodlužovací kabel s ochranou napájení včetně ochrany datových připojení. Jako přepěťová ochrana může sloužit i jednotka UPS, která slouží primárně jako krátkodobý náhradní zdroj energie při výpadku elektrického napájení. Díky tomu může vyrovnat krátké zakolísání sítě, nebo dát uživateli čas na uložení rozpracované práce při dlouhodobějším výpadku.

Pokud stolní počítač obsahuje magnetický pevný disk, je třeba se vyvarovat vibracím a otřesům PC při jejich chodu. Např. vibrující přístroje nebo bouchání do stolu.

Je zapotřebí dbát i na softwarovou část, stahovaní aktualizací hlavně u antivirového programu. Provádět defragmentaci disku je doporučeno pouze pro magnetické disky.U SSD disku defragmentace není potřebná, pouze zkracuje jeho životnost. Je zapotřebí provádět testování dat pomocí antivirového programu. Pokud má

uživatel pocit, že počítač nemá takový výkon, jaký měl a není to způsobené přehříváním a antivirový program nic nenašel, není od věci zkusit jiný antivirový program. Autor této práce viděl několik případů, kdy samotný antivirový program byl napaden škodlivým virem.

8.3.2 Notebooky

Notebook lze považovat za zvláštní druh počítače. Po softwarové stránce platí stejná pravidla, jak v přechozí časti se stolními počítači. Hardwarová část se od klasického počítače liší zmenšením velikosti všech částí. Použité komponenty jsou vybírány s ohledem na nízkou spotřebu elektrické energie. Chlazení je zde centralizované pomocí trubiček, vedoucích teplo k jedinému ventilátoru. Vzduch je nejčastěji nasáván přes klávesnici. Napájení obstarává buď vestavěná baterie, nebo zdroj napájení, který je externí. Při práci s notebookem musí být vždy otvor ventilátoru nezakrytý. Pokud obsahuje magnetický pevný disk a nemá speciální ochranné funkce, nesmí se s ním třást a klepat stejně jako u klasického PC. Notebooky mají díky své stavbě dva problémy, nedají se snadno čistit, jako klasické stolní počítače, ale čistění je stejně potřebné jako u klasických PC. Část nečistot lze odstranit vysavačem. Pro doopravdy účinné čištění je třeba notebook rozebrat, což většina uživatelů sama nedokáže a rozebrání notebooku může vést ke ztrátě záruky. Druhý problém je spojený s nasáváním vzduchu přes klávesnici. Pokud se nalije tekutina do klávesnice, proteče na všechny elektrické části. V takovém případě je třeba odpojit napájení a vyndat baterii. Notebook je pak nutno celý rozebrat a vyčistit, nejlépe speciálním čistidlem.

Existují i notebooky odolné vůči vodě, ale ty jsou méně rozšířené. V dnešní době někteří uživatelé místo notebooku využívají tablet. Ty sice nebývají vodotěsné vůči ponoru do tekutiny, ale běžné polití jim nevadí. Většina modelů nemá aktivní chlazení, prach se nemá jak do tabletu dostat, proto jej není potřeba čistit. Některé tablety mají mnohem delší provoz na jedno nabití baterie než notebooky. Naopak tablety mají zatím omezený výkon. Některý software na nich nejde použít, protože jej daná platforma nepodporuje. Ale hranice mezi notebooky a tablety se pořád zmenšuje a je pravděpodobné, že budou vznikat a už pomalu i vznikají produkty, kombinující výhody obou těchto výrobků.

8.3.3 Mobilní telefony

Uživatelé by neměli zapomínat zálohovat telefonní kontakty.U chytrého telefonu jsou k tomu uzpůsobená internetová úložiště u všech běžných platforem, tedy android, IOS, Windows, Blackberry. Uživatelé, kteří nevěří těmto funkcím, by měli využít klasickou zálohu přes počítač. V tomto případě je zapotřebí, aby na ni uživatel nezapomínal a vykonával ji pravidelně v dostatečně krátkých intervalech.

Pokud si uživatel pořídí chytrý telefon, měl by dbát na ochranu svých dat podobně, jako u počítačů. Tato zařízení se jim mílovými kroky blíží. To znamená, mít antivirový program, neinstalovat podezřelé aplikace. Pro přístup k telefonu používat nějaký druh autentizace (tyto rady jsou platné i pro tablety, většina tabletů se dá považovat za zvětšený chytrý telefon).

Osobní názor autora je, že pokud uživatel nemá v plánu využívat přínosné funkce, které chytré telefony přinášejí, je naprosto nesmyslné si jej pořizovat. Zbytečně se vystavují možným útokům, např. na bankovní konta, jak udává zdroj [17]. Naopak, pokud uživatel využívá přínosné funkce a sám se zajímá o tuto problematiku, může být telefon značným pomocníkem.

8.4 Zálohování

Nejzásadnější věcí je záloha dat. Každá organizace i uživatel by měl zálohovat! Jde pouze o to, v jakém množství a jakým stylem to provést. Znovu je nejzásadnější nejdříve stanovit požadavky a podle nich stanovit systém zálohování. Je důležité nezapomenout na to, že záloha je ochrana před ztrátou dat, nikoli ochrana před nechtěným sdílením. Tomu naopak nahrává. Největší doporučení je zde pro jednotlivé uživatele a malé organizace. Vyzkoušet si některé funkce, které dříve byly parketou jen velkých organizací, jako jsou sdílené dokumenty mezi pracovníky, např. pomocí internetových uložišť nebo speciálních programů. Pro některé organizace a uživatele může využívání takových služeb přinést ochranu pro jejich data v takové míře, kterou by sami nemohli dosáhnout. Naopak pro některé organizace mohou tyto funkce být nedostatečně chráněné, protože jejich ochrana je vyšší, protože pracují s velmi citlivými informacemi.

Organizace, které nechtějí svá data ukládat na cizí servery, si mohou vytvořit vlastní, nebo zvolit levnější ukládaní na jednotlivá média, jako jsou CD, DVD, Blu-Ray (BD-R,BD-RE) paměťové karty, flash disky, magnetické disky, SSD disky. Nedá se

doporučit jednoznačně jedno médium. Každé je vhodné pro určitý případ zálohování. CD a DVD jsou nejlevnější, ale neumožňují přepis, CD-RW,DVD-RW,BD-RE přepis umožňují. Kapacita CD, DVD je značně omezená, u CD 700 MB, DVD 4,7/8,5 GB, je zapotřebí tyto nosiče správně popisovat, protože při větším množství se stávají značně nepřehlednými. Blu-Ray má několika násobně větší kapacitu 25/50 GB, cena je už vyšší.U všech těchto médii je třeba mít vypalovací a čtecí mechaniku. Poškození hrozí hlavně poškrábáním. Je zapotřebí zkontrolovat data hned po vypálení. Nosič se může zdát nefunkční v jednom přístroji a v druhém může být i plně funkční. Možná i proto jsou ty to technologie velké míře na ústupu. Teoretická životnost je i 100 let, ale k té je zapotřebí velké množství okolností podle zdroje [18].

Karty a flash disky jsou naopak na vzestupu. Životnost dat se odhaduje kolem 10 let, ale toto číslo je vysoce spekulativní, je mnoho výrobců a je spousta okolních vlivů. Největší výhoda je vysoká kompatibilita díky USB. Nevýhodou může být jejich selhání, přicházejí velice náhle.

Jako hlavní úložiště jsou dnes využívány magnetické disky a SSD disky. Magnetické disky mají největší kapacitu, nejčastěji 1-6 TB. Mají prý takřka neomezenou životnost uložených dat a množství přepisů z technologického hlediska. Ale rozbijí se na něm mechanické části, zaleží na výrobci a zacházení. Mechanické části se dají ve specializovaných firmách vyměnit. SSD disky jsou nejdražší, ale zato nejrychlejší, mají konečný počet přepisů, ale nemají mechanické části. Díky tomu jim nevadí otřesy a časté čtení nebo zápis malých souborů. Konečný počet přepisů disk sice omezuje, ale ne zase tak moc. Podle testů ve zdroji [19] i při zapisování doopravdy velkého množství dat (100GB) každý den, disk přestane fungovat až za 5 let. Ale při selhání SSD disku je obnova mnohem složitější oproti opravě mechanických částí.

Proto i u zálohování je třeba nejprve provést analýzu, co je potřeba vyřešit a pak zvolit nejvhodnější řešení. Tak, aby to odpovídalo potřebám na kapacitu, rychlostem ukládání a čtení, podmínkám, kterým bude médium vystaveno. Bylo cenově přijatelné a umožňovalo uživatelům jej využít všude, kde potřebují.

8.5 Sdílení informací

Někomu by se mohlo zdát po přečtení této práce, že její autor zastává názor nesdílet data pro jejich ochranu. Tak to rozhodně není. Informace je rozhodně třeba rozvíjet a sdílet. Ale je třeba mít na paměti, jakou formu zvolit. Co je vhodné sdílet a co

není. Bezpečnost informací by neměla zabraňovat ve sdílení informací, ale zabraňovat nechtěnému sdílení informací. K tomuto tématu autora této práce dovedla kniha Management znalostí [20]. Management znalostí bývá také některými autory nazýván managementem informací. V knize je vyjádřena myšlenka důležitosti sdílení informací, bohužel jejich ochrana je naprosto opomíjena. Přitom správně navržený systém by mohl ulehčit jak sdílení tak i ochranu dat a informací, popřípadě znalostí.

8.6 Vzdělávání a učení

Potom, co se člověk v dětství naučí psát na papír, následně se naučí, co s papírem nesmí dělat, aby si ho nepřečetl někdo, kdo ho číst nemá. A co je naopak nutné pro to, aby informace z papíru mohl dlouhou dobu využívat.U moderní techniky by to mělo být stejné. Měl by se naučit, jak na ni informace ukládat, ale stejně je zapotřebí se naučit i druhý krok, jako u papíru, jak informace správně sdílet a správně chránit. Bohužel IT technika není 100% funkční a má svoji problematiku. Někteří lidé znají informační systémy a jejich znalost využívají proti lidem, kteří tuto znalost nemají, proto je nutné, aby zbylí lidé, kteří své znalosti nechtějí zneužívat, tyto znalosti šířili v přijatelné formě mezi ty méně zkušené. A naopak ti méně zkušení by se měli vzdělávat v tomto oboru. Bohužel nelze informační techniku pouze využívat. Je zapotřebí se neustále zdokonalovat ve znalostech jejich potřeb a pravidel. Neomezovat se na studium výhod, ale i nevýhod. Základní osvojení myšlenek, spojených s bezpečností informací, pomáhá jak v organizacích, tak v osobním životě.

Zajímavou myšlenkou je, že by se měli učit jednotlivci, tak celé organizace podle knihy [20]. Je důležité, aby se jednotlivci vzdělávali. Pokud jim v tom organizace pomáhá a sama se tím obohacuje, je to ještě mnohem lepší. V tomto ohledu autor této práce s J. Trunečkem souhlasí. Bohužel je škoda, že více lidí se nesnaží nahlížet na informace jako na celek a ani v díle [20] není sebemenší zmínka o vyučování bezpečnosti informací. Přitom by bylo velmi užitečné, kdyby, např. u přednášek o sdílení informací, byl věnován alespoň malý prostor pro bezpečnost informací.

Za zamyšlení by stála i myšlenka přiřazení bezpečnosti informací k výuce informatiky jak v kurzech, tak i na základních a středních školách. Všechna tato opatření závisí na velké spoustě lidí, bylo by zapotřebí financí a mnohdy i složité změny systému.

Jednoduchým řešením je nebýt netečný a vzdělávat se sám a průběžně. Např. sledovat průběžné nějaký web nebo odebírat nějaký odborný časopis (např. mobilmanie.cz, zive.cz, jnp.zive.cz). Bohužel je třeba dát si pozor na některé uživatele, komentující určité články, prezentující názory, které nejsou pravdivé. Z těchto důvodů bývají komentáře hodnocené počtem kladných a záporných hodnocení.

9 Závěr

Lidé by si měli uvědomit, že existují i nehmotné statky, které je třeba chránit jak v soukromém životě, tak v organizacích. Proto by měli přizpůsobit své chovaní i vybavení, aby informace splňovaly tyto podmínky: integritu, dostupnost a důvěrnost. Před nástupem moderní digitální techniky bylo šíření informací mnohem složitější a náročnější. Dříve bylo třeba vytvářet ručně kopie a zapamatovávat si velké množství informací, nebo nosit s sebou velké množství papírů. Dnes je práce v tomto směru zjednodušená tím, že byla přenesena na elektrotechnickou úroveň, kde je možné čerpat z mnoha výhod, ale nesmí se zapomenout na nevýhody a na pravidla, která se člověk musí naučit. IT vybavení přináší velkou míru využití, ale také zneužití. Čím více informací se centralizuje, tím více se musí toto centrum chránit. Protože při jeho ztrátě uživateli nic nezbyde. Čím více se snažíme zpřístupnit informace na jakémkoli místě, tím více jsou vystavovány nebezpečí.

Při zavedení systému bezpečnosti informací lze využít normy, které mohou organizaci práci zjednodušit a dodat jí správný řád a náležitosti. Lze využít shody některých normativních požadavků bezpečnosti informací a managementu kvality.

Z průzkumu o bezpečnosti informací je patrné, že problémy s bezpečností informací jsou jak u jednotlivých uživatelů, tak i v organizacích. Nejčastěji jsou způsobené špatným chováním a vzděláním lidí, nebo problémy souvisejí s vybavením. Některé problémy jsou společné, některé naopak souvisejí s velikostí organizace a jejich pracovním zaměřením. Řešení některých problémů lze najít v procesním řízení.

Organizace by měly dbát na preventivní ochranu a naučit se bránit proti častým útokům jako je spam, phishing a počítačové viry. Tyto útoky jsou neustále využívané, nejčastěji na místech, kde existuje přístup k co největšímu počtu uživatelů. V roce 2014 to je Facebook a mobilní telefony. Dříve to byly emaily a přenosné disky, ani z těchto míst útoky nevymizely. Je pravděpodobné, že v následující době se najdou další nová místa kde zaútočit.

Základem je správná práce s informacemi, s nosiči informace a přenosovými cestami, vhodné vybavení, jeho správné využití plynoucí z dostatečného vzdělávání a vhodný systém zálohování. Nemělo by se zapomínat na vhodný systém autentizace a s ním související vytváření odolných hesel a jejich preventivní obměňování. V neposlední řadě jde o neustálé zdokonalování všech prvků, spojených s bezpečností.

Použité zdroje

[1] Autoři Informace. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 3.2.2014 [cit. 2014-02-05]. Dostupné z: http://cs.wikipedia.org/wiki/Informace

[2] ČSN ISO/IEC 2382-1 Informační technologie. Český normalizační institut, 1997

[3] LAUDON, K. C. a LAUDON, J.P.. Management information systems: managing the digital firm. 12th ed., global ed. Harlow: Pearson, 2012. ISBN 978-0-273-75453-4.

[4] HÖNIGOVÁ, A. Anglicko-česká terminologie bezpečnosti informačních technologií. 1. vyd. Praha: Computer Press, 1996, 95 s. ISBN 80-858-9644-3.

[5] POŽÁR, J. Informační bezpečnost. Plzeň: Aleš Čeněk, 2005, 309 s. Vysokoškolské učebnice (Aleš Čeněk). ISBN 80-868-9838-5.

[6] KRAUS, J. Sedm nejlepších programů pro zálohování dat. In: Živě.cz [online]. 2012 [cit. 2014-03-10]. Dostupné z: http://www.zive.cz/clanky/sedm-nejlepsich-programu-pro-zalohovani-dat/sc-3-a-161771/default.aspx

[7] PAVLOVIČ, R. Android je podle FBI nejčastějším cílem škodlivého softwaru. In: Mobilmania [online]. 2013 [cit. 2014-01-20]. Dostupné z: http://www.mobilmania.cz/bleskovky/android-je-podle-fbi-nejcastejsim-cilem-skodliveho-softwaru/sc-4-a-1324614/default.aspx

[8] JAMES, L. Phishing bez záhad. 1. vyd. Praha: Grada, 2007, 281 s. ISBN 978-80-247-1766-1.

[9] SOUKUP, T. Phishing je stále aktuální, z e-mailů se ve velkém stěhuje na sociální. In: Živě.cz [online]. 2013 [cit. 2014-02-06]. Dostupné z: http://www.zive.cz/bleskovky/phishing-je-stale-aktualni-z-e-mailu-se-ve-velkem-stehuje-na-socialni-site/sc-4-a-169427/default.aspx

[10] Hák, I. Moderní počítačové viry třetí vydání [cit. 2014-03-19]. Dostupné z http://viry.cz/download/kniha.pdf

[11] ČSN ISO/IEC 27001. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky. Český normalizační institut, 2006

[12] ČSN EN ISO 90001:2008. Systém managementu kvality - Požadavky. Český normalizační institut, 2008.

[13] Kol. autorů: PSIB ČR ´01, PricewaterhouseCoopers,DSm –data security management,NBÚ NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. PSIB ČR '01 : průzkum stavu informační bezpečnosti v ČR. 2001. 2001. ISBN 80-902858-3-X

[14] Kol. autorů: PSIB ČR ´09, Ernst & Young, NBÚ,DSM-data security management NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. PSIB ČR '09 : průzkum stavu informační bezpečnosti v ČR. 2009. 2009. ISBN 978-80-86813-19-6. Dostupné z: http://www.tate.cz/en/psib-cr-2009/

[15] FIŠER, R. Procesní řízení pro manažery. 2014. ISBN 978802475038-5

[16] KASÍK, Pavel. Najdete v této tabulce své heslo? Tak se chyťte za hlavu a změňte ho. In: Technet [online]. 2011 [cit. 2014-04-25]. Dostupné z: http://technet.idnes.cz/najdete-v-teto-tabulce-sve-heslo-tak-se-chytte-za-hlavu-a-zmente-ho-p9n-/sw_internet.aspx?c=A111129_185621_sw_internet_pka

[17] VENTURA, Tomáš. Banky varovaly: Hackeři se k vašemu účtu zkoušejí dostat i přes mobil. In: Idnes [online]. 2013 [cit. 2014-05-05]. Dostupné z: http://ekonomika.idnes.cz/hackeri-se-k-uctum-dostavaji-i-pres-mobil-ffn-/ekonomika.aspx?c=A131004_162054_ekonomika_ven

[18] Kol. autorů: Novinky. DVD vydrží i 100 let, ale musí být správně uskladněno [online]. 2007 [cit. 2014-04-30]. Dostupné z: http://www.novinky.cz/internet-a-pc/hardware/126462-dvd-vydrzi-i-100-let-ale-musi-byt-spravne-uskladneno.html

[19] JAVŮREK, K. Ze světa: výdrž SSD po zápisu 200 TB dat. In: Živě [online]. 2013 [cit. 2014-04-30]. Dostupné z: http://www.zive.cz/clanky/ze-sveta-vydrz-ssd-po-zapisu-200-tb-dat/sc-3-a-171125/default.aspx

[20] TRUNEČEK, J. Management znalostí. Vyd. 1. Praha: C. H. Beck, 2004, xii, 131 s. ISBN 80-717-9884-3.

[21] PLÍVA Z., DRÁBKOVÁ J., KOPRRNICKÝ J., PETRŽÍLKA L., Metodika zpracování bakalářských a diplomových prací, Technická univerzita v Liberci 2014, ISBN 978-80-7494-049-1

[22] VEBER, J. Management kvality, environmentu a bezpečnosti práce: legislativa, systémy, metody, praxe. 2. aktualiz. vyd. Praha: Management Press, 2010, 359 s. ISBN 978-80-7261-210-9.

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

[24] BUDAI, David. Bible vypalování a zálohování 2012. Brno: Extra Publishing, 2012. ISBN 9771802122177.