Analýza bezpečnosti přístupů k informačním systémům

Security Analysis of secure access to information systems

Bc. Michal Moravec

Diplomová práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Michal MORAVEC**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Analýza bezpečnosti přístupů k informačním systémům**

Zásady pro vypracování:

1. **Vypracujte literární rešerši na dané téma.**
2. **Popište hrozby z hlediska informační bezpečnosti, v závislosti na druzích informačních systémů.**
3. **Zhodnoťte a porovnejte typy používaných technologií pro přístup k informačním systémům.**
4. **Analyzujte využívané informační systémy podniku z hlediska bezpečnosti přístupů.**
5. **Zhodnoťte chování uživatelů a základní zásady bezpečnosti ve vztahu k bezpečnostní politice podniku.**
6. **Navrhněte optimalizaci přístupů v závislosti na bezpečnostní politice podniku.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **SODOMKA, Petr. Informační systémy v podnikové praxi. 1. vyd. Brno : Computer Press a. s., 2006. 351 s. ISBN 80-251-1200-4.**
2. **VRANA, Ivan, RICHTA, Karel. Zásady a postupy zavádění podnikových informačních systémů : praktická příručka pro podnikové manažery. 1. vyd. Praha : Grada Publishing, a.s., 2005. 187 s. Management v informační společnosti. ISBN 80-247-1103-6.**
3. **ČERMÁK, Miroslav. Řízení informačních rizik v praxi. 1. vyd. Brno : Tribun EU s.r.o., 2009. 134 s. ISBN 978-80-7399-731-1.**
4. **RAK , Roman, MATYÁŠ, Václav, ŘÍHA, Biometrie a identita člověka ve forenzních a komerčních aplikacích. 1. vyd. Praha : Grada Publishing, a.s., 2008. 664 s. ISBN 978-80-247-2365-5.**
5. **BASL, Josef, BLAŽÍČEK, Roman. Podnikové informační systémy : Podnik v informační společnosti -- 2. výrazně přepracované a rozšířené vydání. 2008. vyd. Praha : Grada Publishing, a.s., 2008. 288 s. ISBN 978-80-247-2279-5.**
6. **VYMĚTAL, Dominik. Informační systémy v podnicích : teorie a praxe projektování. 1. vyd. [s.l.] : Grada Publishing, a.s., 2009. 144 s. ISBN 978-80-247-3046-2.**

Vedoucí diplomové práce: **Ing. Radek Šilhavý, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **19. února 2010**

Termín odevzdání diplomové práce: **7. června 2010**

Ve Zlíně dne 19. února 2010

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

V této práci, pod názvem Analýza bezpečnosti přístupů k informačním systémům, si beru za cíl provedení analýzy bezpečnosti přístupů z hlediska používaných bezpečnostních mechanismů, z hlediska chování uživatelů, správců. V neposlední řadě také vytvoření postupů, doporučení při návrhu, implementaci a správě bezpečnostních mechanismů.

Teoretická část vymezuje základní pojmy a seznámí čtenáře, stručnou a přehlednou formou, s problematikou bezpečnosti informačních systémů. Praktická část se zaměřuje již na konkrétní bezpečnostní mechanismy, jejich analýzu a způsoby využití. Je zde také zpracován průzkum chování uživatelů při nakládání s těmito mechanismy. Závěrečná část obsahuje případovou studii a popisuje způsob uplatnění bezpečnostních mechanismů a doporučení pro jejich provoz.

Klíčová slova: informační systém, bezpečnost informačních systémů, analýza rizik, bezpečnostní mechanismy bezpečnostní funkce, informační bezpečnost, kritéria hodnocení bezpečnosti

ABSTRACT

This thesis named Security Analysis of secure access to information systems covers the analysis of secure access from the perspective of chosen security mechanism and from the perspective of users' or administrators' behavior. Last, but not least there is also part focused on introduction of methods and recommendations for design, implementation and administration of security mechanisms.

Theoretical part of this thesis explains basic terms and let the reader get know key issues of information systems security in a brief and well arranged way. Practical part is focused on particular security mechanisms analysis and ways of usage. There is also evaluated survey of users' behavior of handling with these security mechanisms. Finally there is a case study and description of the way to apply the security mechanisms and practical recommendations for daily operations.

Keywords: Information system, safety information systems, risk analysis, security mechanisms, security functions, information security, security evaluation criteria

Na tomto místě bych rád poděkoval Ing. Radkovi Šilhavému, Ph.D. za cenné rady a připomínky, kterými přispěl ke zdárnému završení této práce.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD **10**

I TEORETICKÁ ČÁST **12**

1 ZÁKLADNÍ PRINCIPY A DŮVODY ZABEZPEČENÍ INFORMAČNÍCH SYSTÉMŮ **13**

1.1 ZÁKLADNÍ PRINCIPY BEZPEČNOSTI IS 13

1.2 DŮVODY PRO ZABEZPEČENÍ PŘÍSTUPŮ K IS 14

2 VYMEZENÍ ZÁKLADNÍCH POJMŮ **15**

2.1 INFORMACE 15

2.2 INFORMAČNÍ SYSTÉM 15

2.3 BEZPEČNOST A BEZPEČNOSTNÍ POLITIKA 16

2.3.1 Bezpečnost 16

2.3.2 Bezpečnostní politika 16

2.4 ZRANITELNOST, HROZBA, RIZIKO, ÚTOK, ÚTOČNÍK 18

2.4.1 Zranitelnost 18

2.4.2 Hrozba 18

2.4.3 Riziko 19

2.4.4 Útok a útočník 19

2.5 ŘÍZENÍ RIZIK A ANALÝZA RIZIK 20

2.5.1 Analýza rizik 20

2.5.2 Havarijní plán 23

3 NORMY A KRITÉRIA HODNOCENÍ BEZPEČNOSTI **25**

3.1 NORMY 25

3.1.1 ISMS (Information Security Management System) 26

3.1.1.1 PDCA model aplikovaný v procesech ISMS 28

3.1.2 ISMS (Information Security Management System) 30

3.2 KRITÉRIA HODNOCENÍ BEZPEČNOSTI 31

3.2.1 Účel kritérií hodnocení bezpečnosti 31

3.2.2 Problémy bezpečnostních modelů 31

3.2.3 TCSEC (Trusted Computer System Evaluation Criteria) 32

3.2.3.1 Základní požadavky 33

3.2.3.2 Rozdělení kritérií TCSEC 34

3.2.4 ITSEC (IT Security Evaluation Criteria) 36

3.2.4.1 Třídy míry zaručitelnosti bezpečnosti IT 36

3.2.4.2 Třídy bezpečnostních funkcí 37

3.2.4.3 Stanovení požadavků na bezpečnostní funkčnost 37

3.2.5 CTCPEC (Canadian Trusted Computer Product Evaluation Criteria) 38

3.2.5.1 Bezpečnostní služby zajišťující důvěrnost 38

3.2.5.2 Bezpečnostní služby zajišťující integritu 39

3.2.5.3 Bezpečnostní služby zajišťující dostupnost 39

3.2.5.4 Bezpečnostní služby zajišťující účtovatelnost 40

3.2.6 FC (Federal Criteria) 40

3.2.7 CC (Common Criteria) 40
3.2.8 Srovnání kritérií a jejich přínosy 40
4 BEZPEČNOSTNÍ MECHANISMY A OPATŘENÍ INFORMAČNÍCH SYSTÉMŮ 42
4.1 ZNALOST 42
4.1.1 Statická a dynamická znalostně orientovaná identifikace osob 43
4.1.2 Zásady využívání a nakládání se znalostně orientovanou identifikací osob 43
4.2 VLASTNICTVÍ 44
4.3 BIOMETRICKÁ CHARAKTERISTIKA 45
4.4 NÁHODNÉ KONTROLNÍ OTÁZKY 47
4.5 BEZPEČNOSTNÍ OPATŘENÍ 47
4.5.1 Personální opatření 47
4.5.2 Fyzická opatření 48
4.5.3 Logická opatření 51
4.5.4 Technická opatření 53
4.5.5 Administrativní opatření 53
II PRAKTICKÁ ČÁST 56
5 IMPLEMENTACE BEZPEČNOSTNÍCH SLUŽEB VE VRSTVÁCH ISO/OSI 57
6 ÚVODNÍ ANALÝZA BEZPEČNOSTI PŘÍSTUPŮ K IS 59
6.1 CÍLE ANALÝZY 59
6.2 METODIKA PRŮZKUMU 60
6.3 STRUKTURA RESPONDENTŮ 60
6.4 BEZPEČNOSTNÍ INCIDENTY Z HLEDISKA DRUHU A PŘÍČINY 61
6.5 BEZPEČNOSTNÍ INCIDENTY Z HLEDISKA ÚTOČNÍKŮ 65
6.6 VYUŽITÍ BEZPEČNOSTNÍCH MECHANISMŮ 66
6.6.1 Využití jednotlivých druhů bezpečnostních mechanizmů 66
6.6.2 Využití biometrických metod identifikace 67
6.6.3 Využití identifikačních mechanismů založených na vlastnictví 69
6.7 CHOVÁNÍ UŽIVATELŮ PŘI VYUŽÍVÁNÍ BEZPEČNOSTNÍCH MECHANISMŮ 71
6.7.1 Tvorba a používání znalostních bezpečnostních mechanismů IT pracovníky 71
6.7.2 Používání znalostních bezpečnostních mechanismů běžnými uživateli. 74
6.8 ZÁVĚR K ANALÝZE BEZPEČNOSTI PŘÍSTUPŮ K IS 77
7 PŘÍPADOVÁ STUDIE: ZABEZPEČENÍ PŘÍSTUPŮ K IS SPOLEČNOSTI 79

7.1 SOUČASNÁ SITUACE 79
7.2 CÍLE A POŽADAVKY SPOLEČNOSTI 81
7.3 ZPŮSOB ŘEŠENÍ POŽADAVKŮ 82
7.4 VNĚJŠÍ BEZPEČNOST 83
7.4.1 Vzdálený přístup k firemním zdrojům a aktiva využívaná mimo společnost 83
7.4.2 Používané bezpečnostní mechanismy – vnější bezpečnost 85
7.5 VNITŘNÍ BEZPEČNOST 86
7.5.1 Přístup zaměstnanců k firemním zdrojům a aktivům uvnitř společnosti 86
7.5.2 Používané bezpečnostní mechanismy – vnitřní bezpečnost 88
7.6 OHODNOCENÍ AKTIV A ROZDĚLENÍ IS DLE BEZPEČNOSTNÍCH KRITÉRIÍ 89
7.6.1 Ohodnocení aktiv 89
7.6.2 Rozdělení IS dle bezpečnostních kritérií 92
7.7 IDENTIFIKACE HROZEB A ZRANITELNOSTÍ, VYHODNOCENÍ RIZIK 93
7.7.1 Vyhodnocení rizik - vnější prostředí 93
7.7.2 Vyhodnocení rizik - vnitřní prostředí 94
7.8 NAVRHOVANÉ ZMĚNY, OPATŘENÍ A DOPORUČENÍ 95
7.8.1 Ochrana notebooků proti odcizení nebo zneužití 96
7.8.2 USB porty, vypalovací mechaniky 96
7.8.3 Elektronické certifikáty, elektronické podpisy 96
7.8.4 Využívání systémů přístupných přes webové prohlížeče 97
7.8.5 Využívání internetu a elektronické pošty 97
7.8.6 Využívání VPN 97
7.8.7 RDP (Remote Desktop Protocol) 98
7.8.8 Protokolování činností v IS 98
7.8.9 Využití bezpečnostních mechanismů 98
7.8.10 Ochrana stolních počítačů 99
ZÁVĚR 100
ZÁVĚR V ANGLIČTINĚ 101
SEZNAM POUŽITÉ LITERATURY 102
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK 104
SEZNAM OBRÁZKŮ 106
SEZNAM TABULEK 107
SEZNAM PŘÍLOH 108

ÚVOD

Ze všech stran se na nás hrnou spousty informací, z různých informačních zdrojů, v různých podobách, v různé kvalitě a kvantitě. Není v lidských silách všechny tyto informace zpracovávat, analyzovat, vyhodnocovat, zapamatovat si je, dobře je interpretovat a především je využít v ten pravý čas na správném místě. K tomuto účelu slouží informační systémy. Mohou to být pouze jednoúčelové a jednoduché systémy nebo na druhou stranu sofistikované, obrovské a propracované systémy, nezávisle na jejich použití. Jaký systém tedy pro své potřeby vybrat? Na tuto otázku neexistuje jednoznačná odpověď a je mnoho faktorů, které mohou ovlivnit výběr. Vezmu-li to hodně obecně, je velmi důležitým měřítkem pro jejich porovnání, jejich kvalita. Paradoxně je to odpověď na otázku, která vyvolává mnoho otázek dalších. Bohužel však ani nejkvalitnější systém nemusí splnit to, co od něho očekáváme a co ke svému životu, podnikání potřebujeme. Důvodů může být hned celá řada. Pro práci s informacemi není využíván vhodný typ informačního systému nebo není využíván takovým způsobem, který je pro správnou funkčnost vhodný. Na druhou stranu, žádný informační systém není dokonalý a každý má své výhody, nevýhody, svá omezení a přednosti. Já se zde však nechci zaměřit na to, jaký systém pro konkrétní činnost vybrat. Tomu se ostatně věnuje celá řada jiných studií a prací.

Proto se chci zaměřit na otázku bezpečnosti přístupů k informačním systémům, respektive informacím obecně. Informace je pro každého jistý druh aktiva, který má určitou hodnotu a především v podnikání jsou klíčovým faktorem. V dnešním globalizovaném světě, je tato hodnota mnohonásobně umocněna. To však neznamená, že naše aktiva (informace) jsou vystavena pouze globálním hrozbám. Jak se říká, je nejprve nutné si zamést před svým prahem a podívat se na to jak my sami s informacemi nakládáme. Tím se dostáváme k tomu hlavnímu, co ovlivňuje bezpečnost našich informací. Bohužel je to velmi často lidský faktor. K čemu nám jsou špičkové, technologicky propracované bezpečnostní systémy, když je využíváme nekorektním způsobem, nedodržujeme obecné zásady nakládání s nimi nebo jsou pro daný typ informačního systému zvoleny a použity nevhodně. Ztráta či únik informací pak může znamenat pro každý podnik existenční problémy a v tom nejhorším případě i zánik. Proto je cílem této práce zpracoval a popsat způsoby jak s informacemi nakládat a především jakým způsobem k nim přistupovat. Snažím se zde popsat a porovnat způsoby zabezpečení informačních systémů, jaké

zabezpečení zvolit pro daný druh informačního systému, výhody a nevýhody jednotlivých řešení, rizika a hrozby. Nejde však pouze o strohé a teoretické konstatování současného stavu a možností. Vše se snažím ukázat na praktických situacích a zkušenostech, které jsem získal při implementacích, správě a údržbě informačních systémů.

Práce je rozdělena do tří částí. První teoretická část, je nutnou přípravou a uvedením do problematiky bezpečnosti informačních systémů. Popisuji zde základní pojmy týkající se bezpečnosti informačních systémů, základní legislativu a normy, kritéria hodnocení bezpečnosti a jaké možnosti v této oblasti máme. Druhá a třetí část je částí praktickou. Nejprve zde analyzuji způsoby zabezpečení informačních systémů, chování jejich uživatelů (základní chyby a omyly) a následně na konkrétním případě (organizaci) zpracovávám jednoduché vodítko jakým způsobem rozdělit informační systémy dle bezpečnostních kritérií, jaký stupeň a jaké zabezpečení pro konkrétní druh informačního systému použít a jak ho využívat.

Problematika bezpečnosti informačních systémů je velmi široká, přesto věřím, že tato práce může být jistým základem a pomocí při zpracovávání bezpečnostních politik podniků, pomůže pochopit důležitost ochrany informací v každém podniku a uceleně shrne stávající možnosti bezpečnostních technologií a postupů.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ PRINCIPY A DŮVODY ZABEZPEČENÍ INFORMAČNÍCH SYSTÉMŮ

Ač se mohou zdát důvody pro zabezpečení informačních systémů[1] na první pohled jasné, z vlastní praxe mohu říci, že tomu tak není. Řada zaměstnanců si zdaleka neuvědomuje, s jak důležitými informacemi pro fungování organizace nakládá, jaké prostředky k tomu využívá, jaká rizika to přináší a jaké nebezpečí hrozí nejen z vnitřního prostředí, ale také z vnějšího. Je především na managementu každé organizace, aby si toto uvědomil a přijal taková opatření, která povedou k předcházení, detekci, eliminaci a snižování možných rizik. To samozřejmě platí nejen pro zabezpečení IS, respektive bezpečnosti přístupů k nim, ale i pro obecnou bezpečnost. To vše samozřejmě musí korespondovat a být v souladu s dlouhodobými cíli a strategií organizace.

Jak už jsem uvedl na úvod, tak informace je pro podnik či jednotlivce aktivum (různé hodnoty a často velmi těžko vyčíslitelné) a musí být chráněno tak, aby s ním mohli nakládat pouze oprávněné osoby vymezeným způsobem. Musí být zajištěna korektnost a pravdivost informací, nesmí dojít k jejich nežádoucím a nekontrolovaným únikům. Měl by být záznam o tom, kdo s informacemi nakládá, to znamená, kdo informaci vytvořil, modifikoval nebo smazal. Především pak, aby byly informace dostupné v požadovaný čas a v požadované kvalitě.

1.1 Základní principy bezpečnosti IS

Je důležité si uvědomit, že neexistuje IS, který by byl absolutně bezpečný. Každý IS je zranitelný a bezpečnostní opatření pouze snižují pravděpodobnost úspěšného prolomení ochrany a zvyšují nároky na útočníka. To znamená, že útočník musí vynaložit vyšší úsilí k narušení bezpečnosti (časové, finanční, technologické).

IS z hlediska potřeb jeho zabezpečení můžeme rozdělit na objekt a subjekt IS. Objektem je pasivní entita přístupná autorizovaným subjektům, která pouze obsahuje nebo přijímá informace. Subjektem je entita aktivní (osoba, zařízení, proces), která na základě příkazu uživatele a jeho autorizace, slouží k získání informací z objektu. Autorizace subjektu

[1] Dále budu pojem *informační systém* zapisovat zkratkou IS

znamená, že daný subjekt je schválený, oprávněný k určité činnosti a je mu umožněn přístup. Před samotnou autorizací probíhá proces autentizace, což je ověření identity subjektu a jeho důvěryhodnosti. Pro ověření identity se používají tyto základní metody:

- Co uživatel zná (heslo, PIN – osobní identifikační číslo)
- Co uživatel má (privátní klíč, USB dongle, čipová karta, …)
- Čím uživatel je (biometrie – otisk prstu, snímek oční duhovky či sítnice, …)
- Co uživatel umí (náhodné kontrolní otázky)

1.2 Důvody pro zabezpečení přístupů k IS

Každá organizace se snaží si svá aktiva určitým způsobem chránit a především přístup k nim. A jaká vlastně mohou být rizika a proč přístup k IS chránit? Důvodů můžeme najít celou řadu a tak se pokusím zde uvést ty nejdůležitější:

- narušení soukromý a únik utajovaných informací
- zamezení úniku informací třetím osobám (například konkurenci)
- zamezení neoprávněného zvýšení uživatelských oprávnění
- zamezení modifikace oprávnění ostatních uživatelů
- ochrana před poškozením IS nebo doplněním o škodlivý kód (skryté funkce)
- ochrana před nežádoucí modifikací informací vedoucí k jejich zkreslení nebo nekorektnosti a následné ovlivnění činností z těchto informací vycházejících
- ochrana před změnami, které vedou k zbavení se zodpovědnosti nebo závazků plynoucích z manipulace s informacemi
- ochrana před skrytým sledováním činností v IS
- u uživatelů a jejich uživatelských práv dbát na princip need-to-know[2]

[2] Každý uživatel by měl mít přístup jen k takovým informacím, které nutně pro svou práci potřebuje

2 VYMEZENÍ ZÁKLADNÍCH POJMŮ

V předchozích odstavcích jsem psal o informacích, IS, jejich bezpečnosti, rizicích a dalších věcech souvisejících s bezpečností a pravděpodobně mnoho dalších pojmů ještě použiji. Proto bych zde rád napravil to, že nebyly zatím popsány či vysvětleny. Je velmi důležité pochopit význam všech použitých pojmů a uvědomit si jejich význam a roli, kterou mají v dané problematice. Na druhou stranu není účelem této práce nahradit výkladový slovník, proto uvedu jen ty nejdůležitější pojmy.

2.1 Informace

Začnu tedy úplně od začátku. Co je to informace? Musím se přiznat, že když jsem začal přemýšlet o významu tohoto slova, nebyl jsem schopen dát dohromady jednoduchou a výstižnou definici. Informace je velmi široký a obecný pojem, než aby se dal vložit do jediné definice. Slovo jako takové vzniklo z latinského *informatio*, což je utváření nebo ztvárnění, vtištění formy či tvaru. Z definic, které jsem měl možnost si přečíst nebo je slyšet, jsem se pokusil vybrat to nejpodstatnější, především ve vztahu k IS. Informace je všechno to, co nám nebo něčemu předává (podává) zprávu o věcech nebo událostech, které se staly, dějí nebo které nastanou. Z hlediska podnikových IS se tedy jedná o strojové zpracování dat (údaje, hodnoty znaky, čísla, grafy, symboly, obrázky, …).

2.2 Informační systém

Aby bylo možné všechny informace a data shromažďovat, uchovávat, zpracovávat a poskytovat v požadované podobě bylo nutné vymyslet nějaký systém, který by toto všechno uměl. Právě z tohoto důvodu vznikly IS. Tyto systémy nemusí být nutně zpracovávány pomocí informačních technologií[3], ale mohou být i v papírové podobě. Nicméně já se zaměřím především na systémy zpracovávané právě pomocí IT. Takovým příkladem IS může být například telefonní seznam, účetnictví, mzdový systém, výrobní systém, bankovní aplikace a další.

[3] Dále budu pojem *informační technologie* zapisovat zkratkou IT

IS je možné rozdělit na čtyři základní části. První částí je ***hardware*** (technické vybavení – PC, Servery, terminály, …), druhou ***software*** (operační systém, aplikační programy), třetí ***data*** (uložená v databázi, výstupní sestavy, vstupní data atd.) a konečně čtvrtou částí jsou ***lidé*** (peopleware - uživatelé, personál). Bez každé jednotlivé části by nebyl IS informačním systémem. Pokud se na IS podíváme z trochu širšího hlediska, mohli bychom k těmto základním čtyřem prvkům přidat ještě další dvě složky, které výrazně ovlivňují IS. Jsou to ***organizační prostředky*** (orgware – nařízení a pravidla, která jsou definována pro provoz IS) a ***vnější svět*** (různé normy, legislativa, informační zdroje atd.). V mnoha knihách, publikacích a článcích je uváděno, že první tři složky IS jsou právě ta aktiva, která jsou pro organizaci důležitá a je nutné je chránit. Já osobně se domnívám, že to není zcela přesné. I lidé mohou a jsou pro podnik jistým druhem aktiva (především jejich znalosti a vědomosti). Proto kvalita a bezpečnost IS je z velké části odvozena od jeho tvůrců, správců a uživatelů.

2.3 Bezpečnost a bezpečnostní politika

2.3.1 Bezpečnost

Stále zde hovořím o bezpečnosti. Co to vlastně ta bezpečnost je? Odpověď je jednoduchá. Je to ochrana něčeho před něčím. Ochrana něčeho je pro nás v tomto případě, ochrana našich aktiv, respektive IS. Ochrana před něčím, je ochrana před vnitřními a vnějšími vlivy, ale tomu se budu věnovat později.

Každý asi chápe, že při výběru vhodného zabezpečení přístupu k IS, je brán ohled na jeho konkrétní aplikační zaměření. Určitě je rozdíl v zabezpečení elektronického bankovního systému oproti zabezpečení systému pro evidenci pošty a příkladů by se dala nalézt celá řada.

2.3.2 Bezpečnostní politika

Bezpečnostní politika by měla přispívat ke zvýšení bezpečnosti. Bezpečnostní politika IS je nedílnou součástí všeobecné bezpečnostní politiky organizace a můžeme si pod ní představit ucelený souhrn bezpečnostních zásad, norem, praktik, předpisů definujících způsoby zabezpečení, souhrn bezpečného využívání informačních zdrojů v rámci organizace nezávisle na použitých IT. Konkrétněji určuje, která data jsou pro organizaci

důležitá (citlivá), definuje rozsah zodpovědností a strukturu organizace bezpečnosti, specifikuje bezpečnostní opatření a způsoby jejich implementace a užívání. To vše v souladu s plány a cíly organizace. V zásadě se jedná o neustálý proces, který nekončí tím, že zpracujeme nějaký dokument. Technologie se mění a zdokonalují, zkušenosti útočníků jdou neustále dopředu, mohou se měnit i cíle a plány organizace a proto je potřeba udržovat bezpečnostní politiku neustále v aktuálním stavu a periodicky jí udržovat. K tomu máme různé nástroje, jako je například analýza rizik. Můžeme si tuto údržbu bezpečnostní politiky přirovnat například k antivirovému programu, který si neustále stahuje nové aktualizace, aby byl schopen ochránit uživatele před novými viry a dalším škodlivým kódem.

Tab. 1 Obsah bezpečnostní politiky firmy [7]

Bezpečnostní politika firmy	
Název dokumentu	Popis
CISO	Definuje personální zajištění bezpečnosti
Analýza rizik	Identifikuje aktiva v systému a jejich cenu
Návrh opatření	Definuje, která aktiva a jakým způsobem budeme chránit
Havarijní plány	Popisuje rozsah činností při bezpečnostních incidentech a přírodních katastrofách
Administrativní část	Stanovuje pravidelné prověřování bezpečnostní politiky apod.

Bezpečnostní politika by měla odpovídat na několik základních otázek:

- Co chceme chránit
- Proč to chceme chránit
- Jakým způsobem to chceme chránit
- Jakým způsobem ověříme, že je ochrana dostatečná a funkční
- Co budeme dělat, pokud ochrana selže

2.4 Zranitelnost, hrozba, riziko, útok, útočník

2.4.1 Zranitelnost

Pod zranitelností si můžeme představit slabé místo IS, které je možné využít (zneužít) za účelem jeho poškození nebo způsobení jiných nežádoucích zásahů. Příčin vzniku slabých a zranitelných míst je hned několik. Může to být způsobeno chybami již při analýze, návrhu a vývoji IS nebo pří jeho implementaci. Zranitelnost se také může zvyšovat s rostoucím objemem a hustotou uložených informací, složitostí IS. Zranitelná místa IS mohou být charakteru:

- lidského faktoru – nejčastější příčina zranitelnosti
- fyzického – IS je umístěn na nevhodném místě, které je snadno přístupné (sabotáže, vandalismus, výpadek napětí, krádež)
- přírodního (požár, záplava, zemětřesení atd.
- hardwarového nebo softwarového (poruchy, chyby v kódu)
- fyzikálního (útoky na spoje, komunikaci a datové zdroje)

2.4.2 Hrozba

Hrozba znamená možnost využití zranitelnosti IS k útoku na něj a následné způsobení škody. Hrozby mohou být vnitřní, vnější nebo objektivní, subjektivní. Útočník může mít různé důvody, ať už je to finanční zisk, získání konkurenční převahy, pomsta a další. Důležité je také jak často a kdy může být hrozba naplněna a jak kritický je její dopad na celý systém.

Hrozby objektivní jsou:

- Přírodní a fyzické (požár, povodeň, poruchy – velmi obtížná prevence a je nutné mít zpracovány havarijní plány)
- Fyzikální - elektromagnetické vyzařování
- Technické nebo logické – porucha hardwaru, krádež, špatná implementace a použití bezpečnostních komponent, softwarová porucha (zadní vrátka)

Hrozby subjektivní jsou:

- Neúmyslné (například uživatel nebo správce, který nebyl dostatečně zaškolen)
- Úmyslné – vnější i vnitřní útočníci (teroristi, konkurenti, hackeři, zaměstnanci)

2.4.3 Riziko

To, že existuje hrozba, představuje riziko. Tím se rozumí míra pravděpodobnosti využití zranitelnosti IS a nebezpečí vzniku určité škody, poškození, ztráty čí zničení. Dá se charakterizovat jak mírou pravděpodobnosti výskytu bezpečnostního incidentu, tak i potencionálně způsobenou škodou. U IS je to možnost, že určitá hrozba využije zranitelnost IS a způsobí narušení důvěrnosti, integrity nebo dostupnosti aktiva. To vše samozřejmě vede ke vzniku škod na aktivech. Dá se tady říci, že úroveň rizika je určena hodnotou aktiva, zranitelností aktiva a úrovní hrozby.

2.4.4 Útok a útočník

Útok je velmi často označován také jako *bezpečnostní incident*. Může se jednat o úmyslné či neúmyslné jednání, které má však za následek způsobení škody nebo ztráty na aktivech, pokud se tedy jedná o útok úspěšný. Vždy se také jedná o využití slabých a zranitelných míst IS.

Na útoky lze nahlížet z různých hledisek, především při jejich analýze. Například jaké jsou možné formy útoku a jejich pravděpodobnost, kdo může útočit, jak se projeví a jaký dopad může útok mít a jak se před nimi chránit. Z hlediska IS můžeme rozdělit útoky jako útoky na hardware, software a data. Formy útoku mohou být různé a liší se dle napadené části. Může se jednat o pasivní útok, což může být například odposlech. Nebo to může být aktivní útok. Aktivním útokem mohou být činnosti jako poškození (přerušení) hardwarového nebo softwarového vybavení, jeho modifikace (úprava – přidání nějaké části nebo změna), odcizení, případně vymazání softwaru a další. Asi za nejnebezpečnější lze považovat útok na data, jelikož data umí interpretovat téměř každý a je velmi obtížné je chránit.

Útok vždy provádí nějaký útočník a je velmi důležité si uvědomit, že útoky nehrozí pouze z vnějšího prostředí (vnější útočník), ale mohou to být i útoky vnitřní (vnitřní útočník). U vnitřních útoků je nejčastějším útočníkem samotný zaměstnanec, ať už úmyslným nebo neúmyslným. Nejčastější jsou z hlediska vnitřních útočníků, útoky nechtěné a neúmyslné. Zejména se jedná o zaměstnance s nízkou kvalifikací v oblasti IT (nechtěné smazání či

modifikace dat, se kterými pracují, atd.). Tím se však nesnižuje míra nebezpečnosti těchto útoků. Na druhou stranu zaměstnanci mohou provádět i útoky úmyslné. K těmto činům mohou být zaměstnanci motivovány, například finančně (nezvýšení platu), povýšení kolegy na úkor jich samých a další.

Je jen na managementu firmy a dobře zpracované bezpečnostní politice společnosti, jak dokáže snižovat a eliminovat tyto útoky, zvyšovat loajalitu zaměstnanců a jejich spolehlivost. Nástrojů k tomu máji celou řadu, od odpovídajících ohodnocení, až po zvyšování kvalifikace každého zaměstnance (školení).

2.5 Řízení rizik a analýza rizik

Řízení rizik je velmi rozsáhlá problematika, která překračuje rámec této práce. Nicméně je velmi důležitým prvkem a základním krokem ke snižování rizik, která mohou ohrozit IS a jeho využívání. Proto zde uvedu základní principy a metody, které budou využity v praktické části této práce.

Prvním krokem při řízení rizik je vždy analýza rizik. Jedná se obvykle o proces definování hrozeb, pravděpodobnost jejich uskutečnění a dopadu na aktiva, tedy stanovení rizik a jejich závažnost. V dalších krocích následuje vyhodnocení rizik a zvládání rizik. Tyto kroky se skládají z jednotlivých dílčích kroků, které na sebe navazují. Nicméně v praxi se často stává, že je nutné provádět některé kroky současně, případně se vracet o několik kroků zpět nebo některé kroky i vynechat.

2.5.1 Analýza rizik

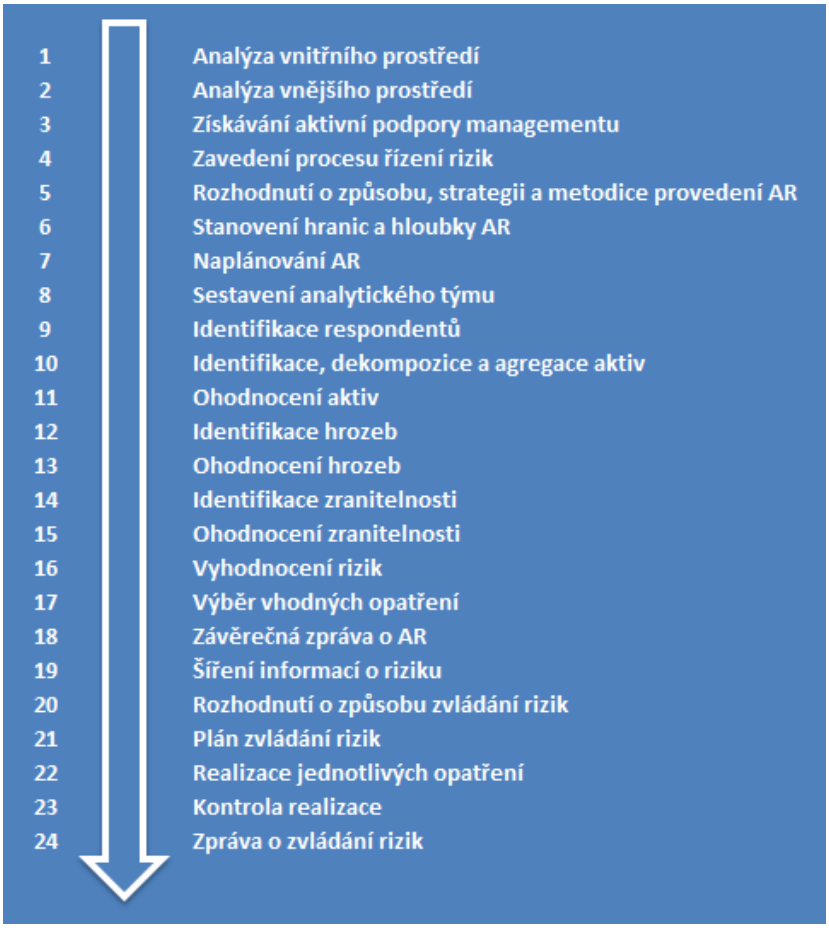
Jak bylo řečeno, jedná se o první a nejdůležitější krok při řízení rizik a zpravidla zahrnuje tyto činnosti:

- Stanovení hranice analýzy rizik a identifikace aktiv (aktiva, která budou zahrnuta do analýzy, vymezení posuzovaného subjektu, popis aktiv v jeho vlastnictví)
- Stanovení hodnoty aktiv (určení hodnoty a významu aktiv pro daný subjekt, ohodnocení dopadu při ztrátě, poškození aktiv)
- Identifikaci hrozeb a slabin (identifikace slabých míst subjektu a útoků, které mohou ohrozit aktiva)

- Stanovení závažnosti hrozeb a míry zranitelnosti (pravděpodobnost výskytu hrozby, míra zranitelnosti subjektu vůči dané hrozbě)

Na základě analýzy rizik jsou dále prováděny kroky, které vedou k určení priorit zvládání rizik, realizaci opatření k zamezení výskytu rizik a jejich rozsahu. Předchází také vlastnímu stanovení bezpečnostní politiky. Samozřejmě není možné eliminovat a odstranit všechna rizika, jelikož by to bylo příliš nákladné a mohlo by to také vést ke snížení funkčnosti a efektivnosti daného subjektu. Proto je důležité si stanovit priority a na základě nich pak realizovat příslušná opatření.

Existují různé přístupy a strategie při provádění analýzy rizik a liší se podle přesnosti odhadu rizik, přiměřenosti bezpečnostních opatření, způsobu dosažení vyrovnanosti časových a finančních nákladů.



Obr. 1 Proces řízení rizik [3]

Základní přístupy k analýze rizik:

- *Orientační* – používá se při tvorbě celkové bezpečnostní politiky a je vodítkem při volbě následujících analýz.
- *Elementární* – je tvořena na základě již existujících a podobných systémů, z obecných norem a doporučení; Výhodou jsou nižší finanční a časové náklady na analýzu rizik a zvolená bezpečnostní opatření. Nevýhodou pak může být zvolení nedostatečně silných opatření, nelze odhadnout dopad na bezpečnost při změnách IS.
- *Neformální* – tato analýza je prováděna na základě interních nebo externích odborníků na bezpečnost bez použití standardních strukturovaných metod. Výhodou je nízká časová a finanční náročnost na analýzu rizik a volbu bezpečnostních opatření. Proto je vhodná pro menší organizace. Nevýhodou může být vynechání některých rizik a ovlivnění subjektivním názorem. Je pak obtížné doložit vhodnost zvolených opatření, jejich síla a dopad.
- *Detailní* – použití standardních strukturovaných metod; Výhodou je minimální opomenutí rizik, není ovlivněno subjektivními názory, lze snadno odhadnout dopady na IS a jeho bezpečnost. Na druhou stranu je nevýhoda vynaložení vyšších finančních a časových nákladů na provedené analýzy a volbu bezpečnostních opatření.
- *Kombinovaná* – volba jednotlivých výše zmíněných metod dle rozdělení na kritické systémy IT a ostatní systémy IT.

Metody analýzy rizik:

- *Kvalitativní* – vyjádření rizik v různém rozsahu (například 1 až 10 nebo slovně). Jednotlivé úrovně jsou stanoveny kvalifikovaným odhadem. Výhodou je jednoduchost a rychlost, ale na druhou stranu jsou více subjektivní.
- *Kvantitativní* – založeny na matematických výpočtech rizika z frekvence výskytu hrozby a jejího dopadu. Většinou jsou vyjádřeny v tisících Kč, jako roční předpokládaná ztráta. Výhodou je přesné vyjádření rizik ve formě finanční, ale jsou velmi náročné na provedení a ne vždy postihnou specifika daného subjektu.

Určování hodnoty identifikovaných aktiv z hlediska:

- *dostupnosti* – náklady subjektu, když něco nefunguje

- *důvěrnosti* – náklady při neoprávněném zveřejnění, úniku citlivých informací
- *integrity* – náklady při narušení autenticity, přesnosti, úplnosti dat nebo softwaru

Je dobré vždy posuzovat a určovat hodnoty aktiv z těchto hledisek samostatně a následně ohodnocení kumulovat. Při určování se také berou v úvahu pořizovací náklady či jiné hodnoty aktiv, důležitost aktiv pro existenci či fungování subjektu, náklady na překlenutí škod způsobených na aktivech, rychlost odstranění škod a další hlediska.

Jakmile je analýza vypracována, tak se vypracuje přehled použitých opatření, jejich cena a provede se odhad ročních úspor získaných právě aplikací zvolených bezpečnostních opatření. Dobrou pomůckou jsou v dnešní době různé standardizované softwarové nástroje, které pomáhají s automatizací analýzy rizik a zajišťují podporu při analýze.

2.5.2 Havarijní plán

V případě vzniku bezpečnostního incidentu a jeho odhalení je nutné zajistit jeho urychlené řešení a znát všechny kroky vedoucí k návratu do původního stavu. K tomu slouží právě havarijní plán. Je v něm uvedeno, jak postupovat při odhalení útoku, jaké jsou náhradní řešení a způsoby uvedení do původního stavu. Kromě jiného obsahuje také další přílohy, jako je určení počtu a uskladnění náhradních dílů, způsoby a organizace záloh dat, metodiku udržování aktuálnosti všech komponent (hardware, software, data), metodiku jejich aktualizace a testování.

Při odstraňování škod je velmi důležitá rychlost obnovy důležitých částí IS a obnova dat. Je zcela jasné, že to vede ke snížení finančního dopadu a zmírnění dalších negativních vlivů. Proces řešení bezpečnostního incidentu lze charakterizovat takto:

- *Odstranění aktuálního nebezpečí* – je závislé na druhu a povaze útoku, může to znamenat třeba odpojení systému od počítačové sítě atd.
- *Obnova důležitých částí systému* – oprava či výměna poškozených částí (hardware, software), reinstalace či instalace nových verzí softwaru, změna nastavení systému a další.
- *Obnova poškozených dat* – není třeba zdůrazňovat, že je potřeba dělat zálohy všech důležitých dat a pokud je máme, tak můžeme v tomto kroku přistoupit k jejich obnově z poslední nepoškozené zálohy. Po obnově je nutné dávat pozor na

opětovný vznik havárie a je možné zpřístupnit systém třeba jen v omezeném rozsahu.

- *Zavedení protiopatření* – snaha o zavedení takových opatření, která povedou k eliminaci vzniku podobných havárií v budoucnu (firewall, antivir,…). Po těchto opatřeních je možné systém uvést do plného provozu.
- *Monitoring* – tato činnost by měla být průběžná a trvalá. Nicméně po vzniku bezpečnostních incidentu je několikanásobně důležitější a kontrola by měla být zvýšena. Tím je zajištěna zpětná vazba, zda přijatá protiopatření jsou dostačující a splňují naše očekávání.
- *Aktualizace bezpečnostní politiky* – pokud se přijatá opatření osvědčila, je nutné jejich zanesení do bezpečnostní politiky. To může následně znamenat například vydání nové směrnice či proškolení zaměstnanců. Což by mělo přispět k zamezení opakování bezpečnostního incidentu.

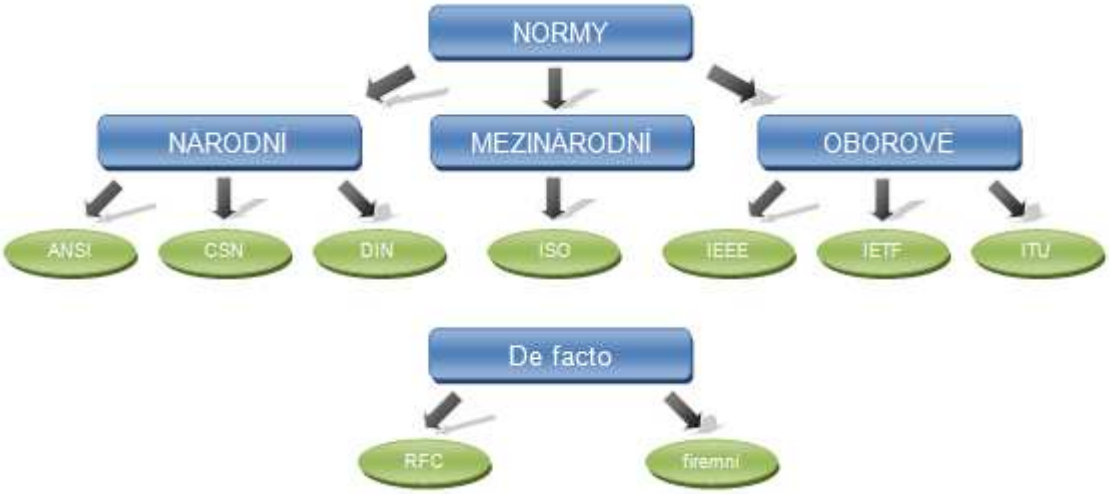
Při řešení bezpečnostního incidentu by měl havarijní plán také pamatovat na personální zajištění a zajistit příslušnému(-ným) pracovníkovi(-ům) dostatečnou pravomoc a prostředky.

3 NORMY A KRITÉRIA HODNOCENÍ BEZPEČNOSTI

Díky globalizaci a neustále se zvyšující potřebě sdílet, přenášet a zpracovávat data je nutné zajistit vzájemnou schopnost IS se mezi sebou dorozumět. Přitom mohou být tyto systémy od různých výrobců, z různých zemí a mohou pokrývat široké spektrum lidské činnosti. Toto samozřejmě platí i pro oblast počítačové bezpečnosti, bezpečnosti IS nevyjímaje.

3.1 Normy

Normy vytváří standardizační organizace a mohou být charakteru národního, mezinárodního nebo se může jednat o organizace působící v daném oboru (oborové organizace). V České republice je takovouto organizací od 1. ledna 2009 Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ). Do 31. Prosince 2008 to byl Český normalizační institut, státní příspěvková organizace řízená Ministerstvem průmyslu a obchodu. ÚNMZ vydává České státní normy – ČSN. Mezi nejvýznamnější mezinárodní normalizační organizace patří International Standardization Organization, která vydává normy s označením ISO. Také Evropská unie, vydává, prostřednictvím oborových organizací normy označené EN. ÚNMZ řadu norem přebírá a překládá, a proto se můžeme často setkat s normami kombinovanými s označením ČSN ISO nebo ČSN EN. Mezi další významné normalizační organizace patří oborová organizace IEEE - mezinárodní sdružení elektrotechnických inženýrů a IETF – organizace vydávající normy pro internetové komunikační standardy. Normy mohou být také vytvořeny a prosazovány jednotlivými organizacemi, které jsou pak v případě osvědčení se v praxi, ostatními přebírány. Existují také normy praktické (De facto standard), které nejsou schválené. Často neexistuje oficiální norma nebo je z nějakého důvodu nevhodná a tak skupina odborníků navrhne standard, ke kterému se mohou ostatní vyjádřit případně se jím řídit (firemní standardy, RFC – standardy popisující internetové protokoly, systémy apod.)



Obr. 2 Struktura norem [7]

3.1.1 ISMS (Information Security Management System)

Řízení bezpečnosti přístupu k informacím v současné době získává charakter řízení služby nebo řízení charakteru IS. Dochází k propojování postupů mezi klasickými složkami integrovaného systému řízení organizace, se systémem řízení bezpečnosti informací. Tyto systémy vycházejí ze společného modelu řízení **PDCA (Plan – Do – Check – Act)**. Jednou z nejznámějších norem, respektive řada norem pro řízení bezpečnosti informací ISO/IEC 2700 vychází ideově z modelu PDCA. Klíčovým normou je mezinárodní norma ***ISO/IEC 27001:2005 – Information security management system – Requirements (Systém řízení bezpečnosti informací – Požadavky).*** Druhou důležitou normou je norma ***ISO/IEC 27002 – Code of practice for information security management (Soubor postupů pro řízení bezpečnosti informací)***. Tato norma obsahuje soubor vhodných bezpečnostních opatření, která jsou rozdělena do jedenácti oblastí.

Obr. 3 IT – soubor postupů pro management bezpečnosti informací [10]

Na začátku roku 2009 byl zahájen proces aktualizace obou norem (ISO/IEC 27001 a ISO/IEC 27002) a v roce 2011 by měl být ukončen vydáním nových verzí.

Kromě výše zmíněných norem byla na začátku roku 2007 z řady norem ISO/IEC 27000 vydána norma ***ISO/IEC 27006 – Requirements for the accreditation of bodies providing certification of information security management systems (Požadavky na akreditaci orgánů provádějících certifikaci systémů řízení bezpečnosti informací*** [11]. Poslední vydanou normou je norma ***ISO/IEC 27005:2008 – Information security risk management (Řízení rizik bezpečnosti informací)*** [12]. Další připravované normy jsou ISO/IEC 27004 – Information security management measurements (Měření účinnosti řízení bezpečnosti informací) [13], dále norma ISO/IEC 27000 – Information security management system fundamentals and vocabulary (Základy a slovník systému řízení bezpečnosti informací), norma ISO/IEC 27003 – Information security management system implementation Guyance (Směrnice pro implementaci systému řízení bezpečnosti informací) a poslední by měla být norma ISO/IEC 27007 – ISMS Auditor Guidelines (Směrnice auditora ISMS).

3.1.1.1 PDCA model aplikovaný v procesech ISMS

Jak bylo již uvedeno, tak ISMS vychází ideově z modelu PDCA (Demingův model[4]). Model PDCA rozděluje proces řízení do čtyř kroků, které tvoří uzavřený cyklus:

- První krok ***Plan*** – Plánuj (implementace bezpečnostního rámce ISMS, analýza rizik);
- Druhý krok ***Do*** – Dělej (implementace a provoz ISMS);
- Třetí krok ***Check*** – Kontroluj (Monitorování, testování a přezkoumávání);
- Čtvrtý krok ***Act*** – Jednej (Údržba, zlepšování, opatření k nápravě, preventivní opatření);

Plan (Plánuj)

Plánování je prvním a základním krokem budování jakéhokoliv systému, nevyjímaje systému řízení informační bezpečnosti. Tento krok by měl obsahovat stanovení plánů, cílů, procesů, postupů a bezpečnostní politiky, to vše v souladu s plány a cíly organizace. „V souladu“ je velmi důležité spojení. Nejen, že je nutné zajistit v tomto kroku zvyšování informační bezpečnosti a zkvalitňování řízení rizik, ale také zajistit a podpořit cíle a plány organizace. Není možné, aby tyto činnosti šly proti sobě. Postup je takový, že se provede analýza (hodnocení) rizik a na základě toho je pak budováno ISMS v daném rozsahu.
V rámci plánováním provádí:

- Definice rozsahu systému řízení informační bezpečnosti;
- Stanovení a definice bezpečnostní politiky organizace;
- Analýza rizik;
- Ohodnocení aktiv, rizik a zranitelností;
- Opatření pro pokrytí rizik;
- Prohlášení o aplikovatelnosti.

Do (Dělej)

Praktická část, kdy je systém řízení bezpečnosti informací uveden do provozu. Je nutné mít zpracovanou důkladnou dokumentaci k plánovaným opatřením a činnostem. S tímto jsou pak seznámeni a zaškoleni zaměstnanci organizace. Je také nutné vypracovat systém, jak

[4] Tento model založil Americký průkopník na poli managementu William Edwards Deming

budou detekovány bezpečnostní incidenty ohrožující bezpečnosti informací a jaký způsobem budou řešeny.

V rámci zavádění se provádí:

- Plán zvládání rizik;
- Zpracování příručky bezpečnosti;
- Seznámení a zaškolení zaměstnanců;
- Řízení provozu a zdrojů (správa dokumentů a záznamů);
- Včasná detekce narušení a zvládání bezpečnostních incidentů.

Check (Kontrola)

Tento krok je velmi důležitý z hlediska hodnocení účinnosti a efektivnosti systému řízení bezpečnosti informací a především slouží jako prevence, identifikace bezpečnostních rizik a chyb. Proto jsou v rámci organizace zavedeny systémy kontrol, tedy systémy interních auditů informační bezpečnosti. Interní audit informační bezpečnosti slouží k posouzení, zda zvolené kroky vedou k pokrytí vybraných a zjištěných bezpečnostních rizik, v rámci dané organizace.

V rámci kontroly se provádí:

- Monitorování vybraných procesů v organizaci;
- Detekování bezpečnostních incidentů a sledování efektivnosti opatření;
- Kontrola zbytkových rizik a akceptovaných rizik (aktualizace analýzy rizik);
- Pravidelné provádění interních auditů bezpečnosti informací;
- Přehodnocování ISMS;
- Aktualizace bezpečnostních plánů;
- Záznam událostí s dopadem na účinnost a efektivnost zvolených opatření.

Act (Jednej)

Tento krok je posledním krokem cyklu PDCA, respektive ISMS. Na základě předchozích kroků jsou aplikována nápravná, preventivní opatření. Dále jsou navrhována možná vylepšení a zvyšování efektivnosti a účinnosti zavedeného systému řízení informační bezpečnosti.

V rámci zlepšování se provádí:

- Implementace opatření k nápravě a prevence;
- Vylepšování ISMS;
- Projednávání výsledků mezi všemi zainteresovanými stranami;

- Po aplikování zlepšení zpětná kontrola, zda bylo dosaženo požadovaných cílů.

Při zavádění systému řízení bezpečnosti informací je nutné mít všechny oblasti popsány v příslušných dokumentech, ať už se jedná o bezpečnostní politiku, definice a popis vybraných procesů. Je nutné zajistit kromě popisu, také testování bezpečnostní politiky a procesů. Je také doporučováno, aby řízení informační bezpečnosti bylo odděleno od řízení komunikačních a informačních technologií a bylo součástí například řízení bezpečnosti fyzické. Důležité je také to, aby jednotlivé části cyklu ISMS byly odděleny a pravidelně kontrolovány. U významných a důležitých činností zajistit kontrolu více pracovníky. Je také důležité říci, že informační bezpečnost je vždy individuální a není možné ji přenášet mezi organizacemi, i přesto, že jsou si podobné. Například už jen proto, že v každé organizaci pracují jiní lidé, organizace se nachází v jiné lokalitě a tak dále.

3.1.2 ISMS (Information Security Management System)

Existují samozřejmě i normy další, není však možné pojmout všechny a tak jsou zde uvedeny jen ty nejznámější a nejpoužívanější, například norma ISO 7799, na jejíchž základech byla postavena právě norma ISO/IEC 27001 ISMS. Dále to je norma ISO 20000 (také známá jako BS 15000). Tato norma je novým standardem, který je speciálně vztažen k managementu služeb IT. Zaměřím je směrována k zvyšování kvality, efektivity a snižování nákladů IT procesů. Svým obsahem a zaměřením se hodně blíží známým ustanovením IT Infrastructure Library (ITIL). Není to však ITIL, jak je často mylně uváděno. ITIL není standard ani metodika, je to rámec přístupů k zajištění kvalitních IT služeb vzhledem k nákladům a vychází z praktických zkušeností a doporučení. ITIL je v současnosti de-facto standardem pro oblast řízení IT služeb.

Dalšími normami jsou například ČSN ISO/IEC 17799:2001 Informační technologie – Směrnice pro řízení bezpečnosti. Dále norma ČSN ISO/IEC TR 13335 1-5. Jedná se o sadu technických zpráv, které jsou zaměřeny na jednotlivé kroky z hlediska zavádění bezpečnosti IT. Tyto normy se velmi často používají jako doplněk k zavádění systému řízení bezpečnostních rizik (analýza rizik, ohodnocení aktiv).

Jistě je celá řada dalších norem, ale není účelem zde všechny popsat a vyjmenovat. Nebylo by to ani účelné a rozhodně by to přesáhlo rozsah této práce. Nicméně je nutné vědět, že bezpečnostní a především bezpečností informací, bezpečnostních struktur a mechanismů se

zabývá celá řada norem, které mohou být vodítkem při implementaci bezpečnosti v organizacích.

3.2 Kritéria hodnocení bezpečnosti

Díky zvyšujícím se nárokům jsou IS stále složitější, náročnější na správu a údržbu. Jejich vzájemná integrace, jejich otevřenost a škálovatelnost sebou nesou jistá bezpečnostní rizika. Tím se samozřejmě zvyšuje obtížnost zhodnocení bezpečnosti daných systémů a není v silách zákazníka toto posoudit. Jak se tedy posuzují obdobné systémy ve stejné kategorii z hlediska bezpečnosti? Pro tento účel, byly zpracovány kritéria hodnocení bezpečnosti IS. Mohou posloužit nejen zákazníkům, ale i vývojovým pracovníkům, bezpečnostním manažerům a analytikům. Nejedná se samozřejmě jen o pouhé konstatování, zda je systém bezpečný nebo není. Z tohoto důvodu bezpečnostní kritéria rozdělují systémy do několika úrovní. Pokud systém dosáhne určité úrovně a získá osvědčení o splnění daných podmínek, můžeme hovořit o systému, který je certifikovaný. Proces certifikace je velmi časově a finančně náročný a není bezpodmínečně nutný u všech IS.

3.2.1 Účel kritérií hodnocení bezpečnosti

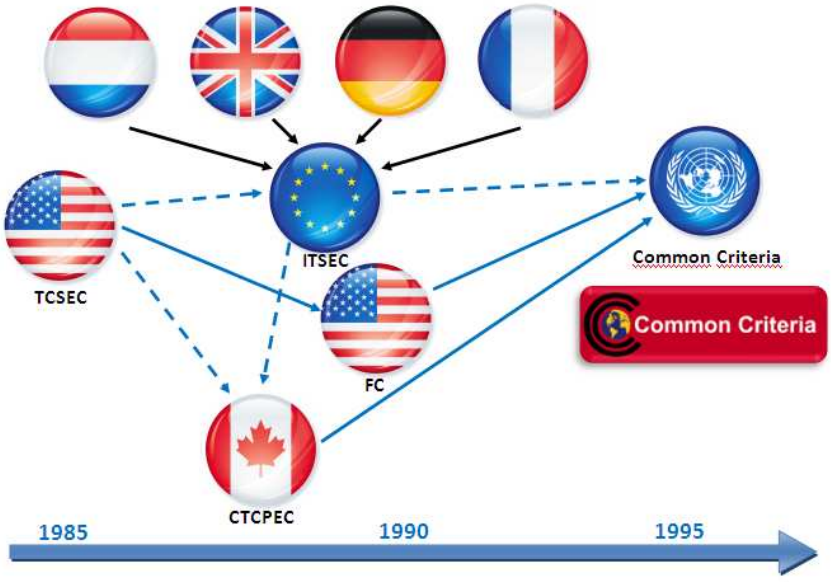
- zajištění měřítka, dle něhož lze vyhodnocovat stupeň zabezpečení, který může být použit v IS pro zajištění bezpečného zpracování informací
- užitečný nástroj při analýze rizik a podpora při zpracování a realizaci bezpečnostní politiky podniku
- u doplňkových specifikací IS, zajistit podklady pro definování požadavků ochrany
- zajištění zpětné vazby výrobcům, díky čemuž mohou implementovat do nových verzí IS nové bezpečnostní prvky, které vyhovují požadavkům zabezpečení aplikací

3.2.2 Problémy bezpečnostních modelů

- dosažení požadované úrovně bezpečnosti IS není konečným řešení jeho zabezpečení (implementační chyby, špatná konfigurace, lidský faktor, …)

- formální bezpečnost IS nezaručuje jejich skutečnou bezpečnost, bezpečnostní narušení může nastat za jiných předpokladů, než bylo uvažováno
- velmi vysoká časová a finanční náročnost
- modely (kritéria) založená na matematických základech nemusí vést k řešením, která jsou nereálná
- bezpečnostní modely mají své hranice a nepokryjí všechny oblasti
- paradoxem bezpečnostních modelů může být krytí nelegálních aktivit a trestních činů

Díky rychlému technickému pokroku, vývoji nových technologií a globalizaci jsou na IS kladeny větší a větší nároky. Pro zajištění bezpečnost již nestačí jen pouhé zpracování formálních bezpečnostních modelů. Je nutné využít všech dostupných prostředků, které zvýší kvalitu zabezpečení daných prvků. Těmito prostředky mohou být bezpečnostní úpravy a aktualizace IS, testování v ostrém provozu s využitím speciálních týmů (testovací pracovníci, hackeři, profesionálové), využití služeb třetích stran, či využití přídavných bezpečnostních produktů (antivirová řešení, firewally, hardwarové klíče, speciální čipové karty, elektronické podpisy, biometrii a další).



Obr. 4 Přehled vývoje bezpečnostních kritérií

3.2.3 TCSEC (Trusted Computer System Evaluation Criteria)

Jedny z nejznámějších kritérií pro hodnocení bezpečnosti. Byly vytvořeny v USA a jsou známé též pod názvem Orange book. V počátku sloužila především při posuzovány

systémů nasazovaných ve státní správě Spojených států amerických, časem však pronikla i do sféry komerční.

3.2.3.1 Základní požadavky

K zabezpečení každého IS, je nejprve nutné formulovat základní požadavky. Obecně lze říci, že u systémů s vyšším požadavkem na bezpečnost jsou vždy využity specifické způsoby ochrany a přístup k informacím mají pouze osoby, procesy, které byly schváleny a mají příslušné oprávnění. Požadavky lze rozdělit do šesti bodů. První čtyři zkoumají co je nutné ke kontrole přístupu k informacím a zbylé dva zkoumají, jak je možné získat záruku.

- **Politika**

  Bezpečnostní politika – stanovení souboru pravidel, který je systémem použit k určení oprávněnosti přístupu k danému objektu. IS musí vynucovat povinnost bezpečnostní politiky, která může podpořit a upřesnit přístupová pravidla pro manipulaci s klasifikovanými informacemi. To znamená, že například není možné získat přístup k chráněným informacím bez odpovídajících oprávnění. Na druhou stranu kontrola zabezpečení musí stanovit uživatele nebo skupiny uživatelů, kteří mohou mít přístup ke klasifikovaným informacím.

  Označení – definice (klasifikace) úrovně ochrany daného objektu nebo způsoby přístupu podle subjektů, které mají potencionálně k objektu přístup.

- **Odpovědnost**

  Identifikace - každý jednotlivý subjekt, který přistupuje k informacím, musí být jednoznačně identifikován. To znamená, že musí být jasné kdo, jaký subjekt, k informacím přistupuje a pro jakou třídu informací má oprávnění. Informace o identifikaci a autorizační informace, musí být v každém IS uloženy na bezpečném místě a spojený se všemi částmi IS, u kterých je nutné zabezpečit ochranu.

  Odpovědnost – každý IS by měl být schopen zajistit záznam všech důležitých akcí vztahujících se k zabezpečení. To znamená zajistit uložení všech aktivit, které souvisí s jeho zabezpečením. Takto uložené záznamy musí být bezpečně uložené a musí být chráněny proti modifikaci či zničení. Díky těmto informacím o ovlivnění bezpečnosti daného systému je možné trasovat akce až k odpovědné straně.

- **Záruka**

  Záruka – IS musí obsahovat softwarové nebo hardwarové mechanismy, které mohou nezávisle na sobě vyhodnocovat a v požadovaném rozsahu zaručovat, že systém vynucuje všechny výše popsané požadavky. Aby byla tato záruka poskytnuta, zda systém splňuje požadavek bezpečnostní politiky, označování, identifikace a odpovědnosti, musí být schopen hardwarově a softwarově zkontrolovat, které funkce splňuje. Řada těchto mechanismů je již implementována v operačním systému. Základ pro zabezpečení takových systémových mechanismů v jejich operačním uspořádání musí být jasně dokumentován, aby bylo možno nezávisle vyhodnotit, zda postačují [9].

  Nepřetržitá ochrana – všechny bezpečnostní mechanismy, které vynucují všechny základní požadavky, musí být nepřetržitě chráněny proti neautorizovaným změnám nebo zásahům, které by vedly k jejich vyřazení z činnosti nebo jejich obcházení. Systém nemůže být považován za bezpečný, jestliže dochází neautorizované modifikaci základních hardwarových a softwarových mechanismů, které vynucují bezpečnostní politiku. Zajištění nepřetržité ochrany má přímý vztah k životnosti celého IS.

Výše zmíněné požadavky tvoří základ pro zpracování kritérií hodnocení, která jsou aplikována na systémy zpracovávající informace.

3.2.3.2 Rozdělení kritérií TCSEC

Kritéria TCSEC jsou rozdělena do čtyř základních skupin D, C, B a A. Skupina A označuje systémy s nejvyšší úrovní zabezpečení a naopak třída D systémy, které nemusí plnit žádná kritéria. Třídy C a B jsou ještě rozděleny na podtřídy, celkem je tedy k dispozici sedm tříd.

- **Třída D** – do této třídy spadají systémy, jak již bylo zmíněno, které nesplňují žádná kritéria. Tyto systémy mají velmi nízké zabezpečení nebo ho nemají vůbec. Může se jednat i o kvalitní systém, který však požadovaná kritéria nesplnil, například z důvodu chybné dokumentace.
- **Třída C** – tato třída je rozdělena na podtřídu C1 a C2. Systémy těchto podtříd musí především splňovat: uživatelé pracující se systémem musí být identifikováni a autentizováni. Systém jim musí přidělovat prostředky podle pravidel nepovinného

řízení přístupu (DAC), musí také zabránit znovupoužití uvolněných prostředků (musí zajistit například to, že uživatel nedostane spolu s přidělenou pamětí zbytky dat zanechané v ní jiným uživatelem) [7]. Všechny činnosti v systému musí být protokolovány a pád jednoho z procesů nesmí způsobit pád celého systému.

Třída C1 vyhovuje požadavkům výběrové ochrany pomocí oddělení uživatelů a dat. To znamená, že uživatel má na základě kontrol, ochráněny své projekty a informace proti neoprávněnému čtení nebo zničení svých dat. U systémů této třídy se předpokládá, že každý uživatel zpracovává data na téže úrovni utajení.

Systémy třídy C2 mají jemnější a podrobnější řízení přístupu. To znamená, že po celou dobu jsou významné činnosti související s bezpečností zaznamenávány a je určena osoba za ně zodpovědná.

- **Třída B** – tato třída je rozdělena na podtřídy B1, B2 a B3. Tato třída proti třídě C1 a C2 vyžaduje od IS více bezpečnostních funkcí. Samozřejmostí je jako u třídy C, povinnost uživatelské identifikace a autentizace. Prostředky jsou přidělovány podle pravidel povinného řízení přístupu (MAC) a musí také zabránit, jako u třídy C, opětovnému použití uvolněných prostředků. Kromě již zmíněných požadavků třídy C musí být tyto systémy při návrhu důkladně analyzovány. Důvěryhodné entity musí být definovány v dokumentaci, uživatel musí být systémem naveden jak správně systém nakonfigurovat pro dosažení požadované bezpečnosti, musí být zajištěna funkce zotavení po chybě a v neposlední řadě je nutné zajistit průkazné bezpečnostní testy při vývoji systému.
- **Třída A** – nejvyšší stupeň zabezpečení systémů. Kromě kritérií třídy B, je jedním ze základních požadavků, aby byl systém formálně specifikován, což je pro většinu systému nedosažitelné. Celý systém musí být popsán pomocí formálních matematických prostředků a musí být proveden formální matematicky důkaz. Musí být také definována přesná konfigurace systému a distribuce, která je takto formálně popsána a to platí i pro skryté prvky systému.

Jak vyplývá z popisu jednotlivých tříd, čím vyšší třída, tím je systém složitější. Z tohoto důvodu jsou systémy třídy A, v porovnání se systémy třídy C, většinou poměrně jednoduché IS díky nutnosti formálního popisu. Tomu samozřejmě také odpovídají ceny systému certifikovaných dle těchto kritérií.

3.2.4 ITSEC (IT Security Evaluation Criteria)

Tato kritéria byla vytvořena v roce 1990 za přispění Německa, Francie, Velké Británie a Nizozemí. Vydána byla Úřadem pro oficiální publikace Evropského společenství a schválena jako doporučení v dubnu 1995. Díky tomu, že byla tato kritéria zpracována pro komerční využití, jsou oproti kritériím TCSEC mnohem propracovanější. Rozlišují rozdíl mezi produktem a systémem (systém – systém ušitý na míru pro konkrétního zákazníka; produkt – určen pro více zákazníků a je nutné počítat se všemi možnými situacemi, které mohou u jednotlivých instalací nastat).

Systémy jsou posuzovány ve dvou krocích. Odděleně se hodnotí bezpečnostní funkce a způsob zajištění jejich kvality. Rozlišujeme tedy takzvané třídy bezpečnostních funkcí a třídy míry zaručitelnosti bezpečnosti IT.

3.2.4.1 Třídy míry zaručitelnosti bezpečnosti IT

Kritéria ITSEC specifikují sedm tříd míry zaručitelnosti bezpečnosti IT a jsou označovány E0 až E6. Tyto třídy kladou požadavky zejména na proces vývoje, prostředí vývoje, provozní dokumentaci a provozní prostředí IS.

- **Třída E0 -** na systém a vývoj nejsou kladeny žádné speciální požadavky
- **Třída E1** - požadavek na neformální zadání bezpečnosti, neformálně popsanou architekturu systému a důkazní testy
- **Třída E2 -** požadavek na neformálně popsaný projekt (detailní popis návrhu), nutnost řízení vlastní tvorby projektu, nezávislé testy
- **Třída E3 -** stejně jako třída E2 a nutnost hodnocení (zdrojový kód u SW, obvodová schémata u HW), nutnost pořízení dokumentace o provedených testech
- **Třída E4 -** u této třídy je vyžadována alespoň jedna část dokumentace formálně (model bezpečnostního návrhu a provedení analýzy zranitelnosti)
- **Třída E5** - musí existovat detailní formální návrh, který koresponduje s implementací (zdrojový kód)

Třída E6 – stejně jako třída E5 a formální popis návrhu doložený konzistencí s matematickým modelem

3.2.4.2 Třídy bezpečnostních funkcí

Je definováno deset tříd bezpečnostních funkcí (F-XX). Prvních pět tříd odpovídá stejnojmenným kritériím TCSEC (F-C1, F-C2, F-C3, F-B1, F-B2, F-B3). Jak je vidět, tak dle evropských kritérií není třída A a D tak důležitá. Zbývající třídy (F-IN, F-AV, F-DI, F-DC, F-DX) nemají hierarchickou strukturu a jsou orientovány aplikačně. Uživatelé je mohou využívat dle svých požadavků a potřeb systému. Třída F-IN klade důraz na integritu dat, třída F-AV na dostupnost dat, třída F-DI na ochranu dat a integritu při výměně dat, F-DC na důvěryhodnost dat, během jejich výměny (například šifrovací zařízení) a F-DX na sítě s vysokými nároky na důvěryhodnost a integritu informací, které mají být vyměněny.

Norma umožňuje definici vlastních tříd bezpečnostních funkcí. Je tak možné si vytvořit třídy, které přesně odpovídají požadavkům na bezpečnost. Vlastní třídy mohou být vytvářeny například:

- kombinací tříd z druhé skupiny (F-AV + F-IN)
- využití již hotové třídy definované normou
- využití třídy vytvořené třetí osobou
- vytvoření vlastní třídy na míru ve spolupráci s bezpečnostními konzultanty

3.2.4.3 Stanovení požadavků na bezpečnostní funkčnost

V případě, že se uživatel rozhodne vytvořit si vlastní třídu funkčnosti, je doporučeno použití této osnovy. Některé funkce mohou patřit do více bodů osnovy a je nutné je uvádět ve všech bodech.

Identifikace a autentizace – zakládání nových a rušení starých identifikací uživatelů; náhled autorizovaných uživatelů na autentizací informace k ověření identity; zajištění integrity autentizacích informací nebo jejich neautorizované užití; omezení opakovaných pokusů o zadání falešné identity

Řízení přístupu – pravidla, kterými se řídí přístupová práva pro různé typy přístupu (dočasné omezení přístupu); zajištění výchozích přístupových pravidel; zajištění dedukce informací, které vzniknou agregací dat z jinak legitimních přístupů

Účtovatelnost – uchování informací o činnostech souvisejících s bezpečností

Audit – automatické nebo manuální kontrola protokolů o bezpečnostních událostech v IS; detekce potencionálních hrozeb;

Opakované užití – inicializace nebo mazání nepřidělených nebo opakovaně přidělených datových objektů; inicializace nebo mazání opakovaně použitých médií (magnetické pásky, disky); mazání výstupních zařízení (monitor)

Přesnost – zajištění přesnosti přenášených dat, tedy možnost předcházet a detekovat ztráty, modifikace; zajištění zdroje a místa určení přenosu dat proti změně

Spolehlivost a dostupnost služeb – zajištění přístupnosti zdrojů a využitelnosti na základě požadavků od uživatelů, procesů; detekce chyb a zotavení po chybě a minimalizace přerušení nebo ztráty služby; zajištění reakce na externí události v požadovaném časovém limitu.

Výměna dat – zajištění bezpečnosti dat při přenosu mezi komunikačními kanály

3.2.5 CTCPEC (Canadian Trusted Computer Product Evaluation Criteria)

Tyto bezpečnostní kritéria vznikla v Kanadě a systém, který je hodnocen pomocí těchto kritérií, je brán jako skupina bezpečnostních funkcí s úrovní záruk. Bezpečnostní funkce se zde nazývají *bezpečnostní služby*. Ty jsou rozděleny do čtyř kategorií a to na bezpečnostní služby zajišťující funkce důvěrnosti, integrity, dostupnosti a účtovatelnosti. Ty jsou dále rozděleny do několika úrovní, které jsou přesně definované, měřitelné požadavky nebo kvalita bezpečnostní služby vzhledem k určité množině hrozeb. Úrovně jsou hierarchické a jsou značeny od nuly, kde nula je považována za nejnižší stupeň ochrany.

3.2.5.1 Bezpečnostní služby zajišťující důvěrnost

Slouží k ochraně proti hrozbám, které mají za následek prozrazení informace neoprávněnému subjektu, subjektům. Jednotlivé úrovně jsou:

- *Skryté kanály (CC-0 až CC-3)* – Identifikace a odstranění přenosu informací, které jsou v rozporu s bezpečnostní politikou.
- *Nepovinné řízení důvěrnosti (CD-0 až CD-4)* – Mechanismy přístupových práv, seznamy přístupových práv přispívající k zajištění důvěrnosti dat.
- *Povinné řízení důvěrnosti (CM-0 až CM-4)* – Mechanismy pracující se stupněm klasifikace spravovaných objektů, přispívající k zajištění důvěrnosti dat.

- *Opětné použití objektů (CR-0 až CR-1)* – Zajištění, že objekt, který byl přidělen uživateli nebo procesu neobsahuje informace zbylé po předchozím vlastníkovi objektu.

3.2.5.2 Bezpečnostní služby zajišťující integritu

Tyto služby slouží k zamezení neoprávněné modifikace dat. Jednotlivé úrovně jsou:

- *Doménová integrita (IB-0 až IB-2)* – Důvěryhodná výpočetní báze (Trusted Computing Base, TCB) IS a schopnost ochrany před útokem a správy chráněných objektů.
- *Nepovinné řízení integrity (ID-0 až ID-4)* – Mechanismy přístupových práv, seznamy přístupových práv, které slouží k zajištění integrity dat.
- *Povinné řízení integrity (IM-0 až IM-4)* – Mechanismy pracující se stupněm klasifikace spravovaných objektů, které slouží k zajištění integrity dat.
- *Fyzická integrita (IP-0 až IP-4)* – Definuje ochranné pásmo centralizované části systému a slouží k ochraně komponent, které leží uvnitř tohoto pásma.
- *Návrat (IR-0 až IR-2)* – Pokud nastane chyba uživatele, havárie nebo útok, zajistí schopnost návratu systému do předchozího stavu.
- *Oddělení rolí (IS-0 až IS-3)* – Rozdělení pravomocí (přístupových práv) a zodpovědností mezi jednotlivé role, čímž jsou snižovány rizika potencionálních škod, které mohou vzniknout nekorektním zásahem uživatele nebo správce.
- *Autonomní testování (IT-0 až IT-3)* – testování zabezpečení hardwaru a softwaru na bezpečný stav.

3.2.5.3 Bezpečnostní služby zajišťující dostupnost

- *Přidělování prostředků (AC-0 až AC-3)* – Přidělování a využití prostředků uživateli a jejich následná kontrola.
- *Tolerance k chybám (AF-0 až AF-23)* – Vlastnost systému, že pokud dojde k chybě, je systém schopen nadále pracovat a umožnit odstranění chyby.
- *Robustnost (AR-0 až AR-3)* – Vlastnost systému zajistit dostupnost informací a služeb po výpadku některých částí systému.
- *Zotavení (AY-0 až AY-3)* – Vlastnost systému vrátit se do původního stavu po poruše nebo chybě.

3.2.5.4 Bezpečnostní služby zajišťující účtovatelnost

- *Audit (WA-0 až WA-5)* – tato služba zajišťuje uchování, detekci (protokolování) a analýzu událostí, které souvisejí s bezpečností.
- *Identifikace a autentizace (WI-0 až WI-3)* – Zjištění a ověření identity uživatele IS k zajištění bezpečnosti.
- *Důvěryhodná cesta (WR-0 až WT-3)* – Zajištění bezpečného komunikačního kanálu pro uživatele a IS.

3.2.6 FC (Federal Criteria)

Tento standard hodnotících kritérií byl zpracován v USA a jednalo se o pokus nahradit kritéria TCSEC, ale zůstalo jen u návrhu a toto úsilí bylo nahrazeno vznikem tzv. Common Criteria, která obsahují řadu nápadů a myšlenek právě z Federal Criteria. Tento standard je rozdělen na dva oddíly. První oddíl jsou vlastní kritéria (požadavky na funkční složky, požadavky na vývoj systému a požadavky na hodnotitelské záruky). Druhý oddíl jsou takzvané bezpečnostní profily (BP).

3.2.7 CC (Common Criteria)

Tato norma, kritéria, vznikla sjednocením a sladěním předchozích kritérií pro hodnocení bezpečnosti. Jedná se o mezinárodní normu ISO/IEC 15408, která se nazývá „Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT“. Nejvíce jsou tato kritéria podobná evropským kritériím ITSEC. Také definují třídy míry zaručitelnosti bezpečnosti IT a obdobu tříd bezpečnostních funkcí. Pro třídy bezpečnostních funkcí je však použit výraz komponenta funkčních požadavků.

3.2.8 Srovnání kritérií a jejich přínosy

TCSEC

- Nepřizpůsobivost novým podmínkám.
- Tyto kritéria jsou stále považována za základ hodnocení bezpečnosti (hodnocení bezpečnosti operačních systémů).
- Bezpečnost je vyjádřena pouze jednou hodnotou.

ITSEC

- Vícerozměrný výsledek hodnocení (míra záruk, funkčnost).

CTPEC

- Dobré přizpůsobení se novým podmínkám.
- Bezpečnostní funkce a jejich kvalita je vyjádřena nezávisle.

FC

- Bezpečnostní profil.
- Komplexní seskupení.
- Ucelený pohled na bezpečnost společně se specifikovanými podmínkami použití.

CC

- Umožňují porovnávat jednotlivé výsledky prováděných hodnocení bezpečnosti nezávisle na sobě.
- Vícerozměrný výsledek hodnocení (míra zaručitelnosti bezpečnosti, komponenta funkčních požadavků).

Tab. 2 Srovnání hodnotících kritérií bezpečnosti

TCSEC	ITSEC		CTCPEC	FC
	E0		-	-
D (minimální ochrana)	-		-	-
C1 (výběrový přístup)	E1	F-C1	-	-
C2 (řízený přístup)	E2	F-C2	T-1	T1
B1 (ochrana návěštím)	E3	F-B1	T-2	T2
-	-		T-3	T3
-	-		-	T4
B2 (strukturovaná ochrana)	E4	F-B2	T-4	T4
B3 (bezpečnostní domény)	E5	F-B3	T-5	T6
A1 (verifikovaný návrh)	E6	F-A1	T-6	T7

4 BEZPEČNOSTNÍ MECHANISMY A OPATŘENÍ INFORMAČNÍCH SYSTÉMŮ

Pro implementaci bezpečnostních funkcí (administrativní, fyzické, logické nebo technické) a jejich kombinací slouží bezpečnostní mechanismy. Velmi často se stává, že implementovaná bezpečnostní funkce je nedostačující, nepřesná a málo účinná. Z těchto důvodů se jednotlivé funkce kombinují, což nemusí mít pouze vliv na účinnost bezpečnostní funkce, ale může to mít i pozitivní ekonomický dopad. Některé bezpečnostní mechanismy je možné použít i pro implementaci několika aplikačně odlišných bezpečnostních funkcí. Příkladem může být čipová karta, kterou je možné využít například při přístupu ke svému bankovnímu účtu, tak i pro přístup do zabezpečených prostor. Na druhou stranu, některé bezpečnostní funkce mohou být implementovány pouze jedním bezpečnostním mechanismem a jiné zase pouze více bezpečnostními mechanismy.

Příkladem způsobu realizace a implementace bezpečnostní funkce identifikace a autentizace je hned několik. Je možné využít ověření znalosti tajné informace (heslo nebo osobní identifikační číslo) nebo také ověření pomocí vlastnictví určitého předmětu, jako je klíč, magnetická či čipová karta a další. Dalším způsobem je ověřování pomocí fyzických a biometrických charakteristik, což může být například otisk prstu, snímek oční duhovky nebo rohovky, geometrie ruky, krevní řečiště hřbetu ruky, DNA, rozpoznání tváře, hlasu, písma a další.

Jak bylo uvedeno v bodě 1.1 a popsáno výše, základní identifikaci osoby můžeme tedy rozlišovat pomocí následujících přístupů:

- Co uživatel zná - *Znalost*
- Co uživatel má - *Vlastnictví*
- Čím uživatel je - *Biometrická charakteristika těla a projevů*
- Co uživatel umí - *Náhodné kontrolní otázky*

4.1 Znalost

Jeden z nejjednodušších způsobů zabezpečení a identifikace osob. Bohužel také jeden z méně spolehlivých způsobů. Zpravidla se jedná o hesla nebo osobní identifikační číslo (PIN – Personal Identification Number). Tyto hodnoty jsou zpravidla přidělovány

administrátory systémů nebo si je může vytvářet uživatel sám. Pro usnadnění tvorby hesla existuje také celá řada softwarových nástrojů, které umějí generovat různá hesla na základě požadavků uživatele.

V dnešní době je uživatel nucen si pamatovat stále více a více identifikačních čísel, kódů a hesel (e-mail, PIN platební karty, telefonu, přístupové údaje do počítačů, aplikačních softwarů, atd.) a není v lidských silách si je všechny zapamatovat. Proto často dochází k tomu, že si uživatel usnadní používání a zapamatování těchto údajů tím, že například jeden nebo dva kódy využívá prakticky všude. Nebo také určitá hesla střídat stále dokola a v tom nejhorším případě si je někam nezabezpečeně poznačí. Ve všech těchto případech dochází ke zvýšení rizika zneužití, a proto je znalostně orientovaná identifikace osob obecně nespolehlivá. Na druhou stranu poměrně jednoduše a levně implementovatelná. Z těchto důvodů se využívá u systémů s nižšími nároky na bezpečnost.

4.1.1 Statická a dynamická znalostně orientovaná identifikace osob

Statická identifikace osob je všem známé klasické heslo, kód nebo osobní identifikační číslo, které běžně využívají. Naproti tomu se dnes prosazují hesla dynamická, která částečně odstraňují nedostatky klasických statických hesel. Při každém úspěšném přihlášení je heslo změněno a není možné použít heslo původní. Tyto změny mohou být buď v závislosti na čase, nebo místě použití hesla. Uživatel si také může velmi často zadat vlastní úroveň zabezpečení hesla. V některých případech je výpočet dynamického hesla příliš složitý a tak se využívají speciální softwarové prostředky nazývané Personal Digital Assistant (PDA).

4.1.2 Zásady využívání a nakládání se znalostně orientovanou identifikací osob

Existuje několik zásad, jak by mělo heslo vypadat a jak s ním nakládat:

- Heslo nesmí obsahovat běžné údaje z našeho života, jako je jméno, příjmení, přezdívka, různé datumy nebo jiná běžně používaná slova.
- Heslo by se mělo skládat minimálně z 6 - 8 znaků. Pro zvýšení bezpečností je možné samozřejmě využít i hesla delší.
- Heslo by mělo obsahovat různé znaky, jejich kombinace (velká písmena, malá písmena, číslice).

- Heslo by mělo obsahovat i speciální znaky (%, @, *, “, /, !, &, $, #, ~, mezera atd.).
- Heslo pravidelně měníme a jeho změna by neměla být pouhá kosmetická úprava, nemělo by být podobné minimálně pěti posledním použitým heslům.
- Heslo si nikam nepoznamenáváme a nikomu ho neprozrazujeme (existují sice programy pro uchování hesel, ale při jejich použití je potřeba zpravidla opět využít heslo)
- V případě, že jsme jediný uživatel nebo správce systému, je možné heslo bezpečně uložit například do fyzického nebo softwarového trezoru.
- Heslo neprozrazujeme ani správcům a administrátorům systému. Ti mají zpravidla možnost vaše heslo dočasně změnit nebo jiným způsobem obejít. To platí samozřejmě u hesel, které jste si zvolili sami.
- Příliš dlouhé a složité heslo neznamená automaticky zvýšení bezpečnosti. Pokud si jej uživatel nemůže zapamatovat, často si ho někde poznačí.
- V případě, že je přidělené heslo předáváno (administrátor – uživatel) je nutné toto učinit takovým způsobem, aby nedošlo k jeho prozrazení třetím osobám. Takovým způsobem může být například zapečetěná obálka, předaná z ruky do ruky. Použití telefonu nebo e-mailu není vhodná forma.

4.2 Vlastnictví

Nejrozšířenější způsob určování identity člověka. Jedná se o uměle získané nebo přidělené identifikační charakteristiky.

Patří sem:

- jméno a příjmení osoby
- osobní doklady (rodný list, občanský průkaz, řidičský průkaz,…)
- identifikační čísla a kódy (rodné číslo, číslo občanského průkazu, čárový kód, RFID (radiofrekvenční kódování),…)
- identifikační karty a čipy (platební karty, identifikační průkazy, …)
- biočipy (mikročipová identifikace lidí a zvířat)

V IS se u vlastnicky orientované identifikace osob uplatňují především identifikační karty a čipy a identifikační čísla a kódy. Velmi často jsou tyto metody kombinovány se znalostně orientovanou identifikací osob.

I zde je nutné dodržovat základní pravidla při tvorbě a používání těchto identifikátorů. U identifikačních čísel a kódů je nutné zabezpečit, aby nedošlo k duplicitním hodnotám, zabezpečit dostatečné kontrolní identifikátory – kontrolní číslice atd. U identifikačních karet a čipů je zase riziko ztráty, odcizení a zneužití. I přes snahu o jejich technické a bezpečnostní zdokonalování. Dobrým příkladem může být identifikační karta pro nakládání s vlastním bankovním účtem, prostřednictvím bankomatu. Dříve byly používány magnetické karty, které jsou dnes nahrazeny kartami čipovými a i přes to dochází k jejich zneužívání (okopírování karty přímo při manipulaci s bankomatem).

4.3 Biometrická charakteristika

To co známe, může být uhodnuto, odpozorováno, prozrazeno nebo jinak získáno. To co máme, nám může být odcizeno, okopírováno. Obojí může být tedy v praxi zneužito. Proto se velmi často tyto přístupy kombinují.

Každá osoba je identická jen a pouze sama se sebou. Jestliže prokážeme (a je prokázáno), že i naše fyzické (a psychické) charakteristiky jsou jedinečné, pak je lze úspěšně použít pro efektivní identifikaci osoby s velmi vysokým stupněm jedinečnosti a tedy následně i bezpečnosti a prokazatelnosti [4]. Takovouto identitu nelze tedy odcizit nebo jinak napodobit, jelikož je spojena s identifikovanou osobou. To je základní princip a myšlenka biometrické identifikace osoby.

Výhody:

- nelze ji zapomenout nebo ztratit
- je velmi těžké ji odcizit nebo napodobit
- nelze přenášet mezi jednotlivými osobami
- snadné a rychlé použití
- vysoká přesnost identifikace
- je pro člověka přirozená

Tento způsob identifikace se začíná s poslední době čím dál tím více prosazovat a do budoucna tomu nebude jinak. Výhody oproti předchozím metodám jsou nesporné a neoddiskutovatelné. Nevýhodou byly především finanční náklady na pořízení těchto technologií. To však již v dnešní době není již takový problém, díky rychlému vývoji nových technologií a klesání cen. V dnešní době není problém koupit běžný notebook se čtečkou otisku prstů bez nutnosti vysokých příplatků.

Základní členění biometrické identifikace a verifikace:

- Anatomicko fyziologické biometrické charakteristiky
    - Oční duhovka
    - Oční sítnice
    - Tvář
    - Tvar vnějšího ucha
    - Daktyloskopické otisky prstů, dlaní a chodidel
    - Geometrie prstů a ruky
    - Topografie žil zápěstí
    - Pach lidského těla
    - Obsah solí v lidském těle
    - Rozměry a váhy lidského těla
    - DNA
- Biometrické charakteristiky týkající se chování
    - Hlas
    - Lokomoce (typické rysy lidské chůze)
    - Písmo
    - Podpis
    - Dynamika psaní na klávesnici

4.4 Náhodné kontrolní otázky

Tento způsob je velmi často použit v kombinaci se znalostně orientovanou identifikací a samostatně není příliš využíván. Velmi časté použití je při zapomenutí hesla, kdy je uživatel vyzván k odpovědi na otázku a na základě správné odpovědi je mu umožněno nadefinovat si heslo nové nebo je mu zasláno. Tyto otázky jsou předem připraveny a uživatel si dopředu nadefinuje správné odpovědi. Příkladem může být například „Jaké je vaše číslo řidičského průkazu“ nebo „Jaké je křestní jméno vaší matky“ atd.

4.5 Bezpečnostní opatření

Opatření bezpečnostních funkcí můžeme rozdělit na:

- Personální opatření
- Fyzická opatření
- Logická opatření
- Technická opatření
- Administrativní opatření

4.5.1 Personální opatření

Tato opatření by měla pomoci s personálním zajištěním jednotlivých procesů. Zejména s tím, aby společnost měla dostatečný počet pracovníků s dostatečnou kvalifikací. Tato opatření se implementují po celou dobu pracovního procesu, počínaje přijímáním do zaměstnání, trváním pracovního poměru, konče ukončováním pracovního poměru.

Při přijímání by měla být ověřena totožnost a bezúhonnost uchazeče, měly by být ověřeny reference z předchozích zaměstnání a dosažené vzdělání. Smlouva, která je následně oběma stranami podepsána, by měla obsahovat údaje o zachování důvěrnosti a další nezbytné doložky.

V době trvání pracovního poměru je velmi důležité neustále vzdělávání v oblasti bezpečnosti informací a bezpečnostní politiky. Mělo by být zajištěno dodržování bezpečnostní politiky (kontrola). V případě vzniku bezpečnostních incidentů, je potřeba zajistit jejich nahlášení, prošetření a vyvození důsledků.

Při ukončování pracovního poměru je nutné pohlídat, zda pracovník odevzdal všechny předměty, které mu byly svěřeny při nástupu a během pracovního poměru. Samozřejmě v požadovaném stavu. Také by měly být zamezeny a zakázány veškeré přístupy do společnosti nebo jejich IS. To znamená odebrání veškerých přístupových práv, vymazání uživatele nebo deaktivace jeho účtů.

Samozřejmě je celá řada dalších způsobů a doporučení, jak provádět personální opatření. Není však možné je zde všechny detailně popsat, jelikož se liší společnost od společnosti, podle druhu a povahy daného odvětví a dalších vlivů.

4.5.2 Fyzická opatření

Tato opatření jsou neodmyslitelnou součástí zabezpečení téměř každého aktiva, před neoprávněným přístupem, zcizením, poškozením nebo zničením. Jednoduchým příkladem z praxe může být obyčejný kancelářský počítač s operačním systémem a nainstalovaným mzdovým či jiným systémem. V praxi se velmi často setkávám s uživateli, kteří bez problémů opustí počítač, na kterém mají spuštěný nějaký IS a neodhlásí se. K tomu všemu ještě nechají volně přístupnou kancelář a tak nic nebrání potencionálnímu útočníkovi provést útok. Přitom by stačilo kancelář alespoň zamknout.

Tato opatření pomáhají s fyzickým zabezpečením objektů, pomáhají s kontrolou pohybu osob, ochranou aktiv v objektu a mimo objekt a další.

Fyzický bezpečnostní perimetr

Měl by být vymezen bezpečnostní perimetr a zajištěno jeho nepřetržité sledování (čidla a senzory, kamerový systém). Vzhled objektu by neměl dopředu dávat najevo svůj účel. Je možné využívat bezpečnostní službu (ostraha), která svou přítomností odradí případného útočníka. Využití bezpečnostních dveří, oken s ochranou bezpečnostní fólií, neprůhledné ohrazení objektů (zdi, ploty), mříže, kamerový systém, různé detektory a další.

Kontrola pohybu osob

Sledování pohybu osob v objektu by mělo být zaznamenáváno a pro pozdější využití uchováváno. Měly by se také definovat přístupy do jednotlivých částí objektů jednotlivým osobám. Ke kontrole pohybu či vymezení přístupů se v praxi využívají klasické zámky na klíč, popřípadě zámky elektronické (karta, PIN, biometrie). Při vstupu do budovy bývá zvykem umístění recepce (kontrola a prohlídka osob při vstupu a odchodu), turnikety (průchod pouze jedné osoby, která se identifikuje například čipovou kartou). Pro sledování

osob jsou využívány kamerové systémy. Je vhodné také využívat různé formy identifikace osob (například visačky, uniformy, pracovní oděv dle zařazení atd.). Osoby, které nejsou zaměstnanci, by se neměli po objektu pohybovat osamocené a měl by jim být přidělen doprovod.

Ochrana aktiv v objektu a mimo objekt

Důležitá nebo cenná aktiva je nutné uchovávat v uzamykatelných skříních, kontejnerech či trezorech. Výpočetní technika by měla být zabezpečena proti nežádoucí manipulaci (spojení lankem s pevným nábytkem, uzamčení počítačových skříní a kabeláže,…). Konzumace potravin, tekutin a kouření by mělo probíhat jen v prostorech k tomu určených. Záložní zařízení, média a archiv by měly být uloženy mimo hlavní prostory objektu. Jakékoliv přemísťování aktiv by nemělo být možné bez souhlasu odpovědných osob. Nebezpečné a hořlavé látky by měly být umístěny v prostorech k tomu určených a manipulace s nimi by měla být prováděna dle platných předpisů. Existuje celá řada dalších opatření v závislosti na daném objektu.

Ochrana aktiv mimo objekt je většinou složitější a rizika jsou zde větší. Z těchto důvodů je nutné stanovit pravidla pro využívání aktiv mimo objekt organizace. Základními pravidly jsou, že aktivum by nemělo být přepravováno na viditelném místě a mělo by být přepravováno pouze schválenou osobou a prostředkem. Tato aktiva by neměla být ponechána bez dozoru. Také by měla být pojištěna proti zcizení, poškození.

Ochrana aktiv před poškozením, zničením

Poškození nebo zničení aktiva nehrozí pouze při útoku útočníka, ale jsou zde i další hrozby. Mezi tyto hrozby patří především přírodní vlivy, jako je voda (povodně), blesk a požár. Aktiva by měla být umístěna tak, aby v případě povodně nebo úniku vody nedošlo k jejich zničení. V případě blesku je nutné vybavit objekt hromosvody, ochrannými prvky (filtry), které ochrání aktiva před poškozením nebo zničením. Pro případ vzniku požáru by měl být objekt vybaven požárními hlásiči pro detekci kouře a ohně, automatickým hasícím systémem nebo jinými hasícími prostředky. V případě ohně, vody se může samozřejmě jednat i o úmyslné založení požáru nebo zaplavení a právě pro tyto případy existuje celá řada výše uvedených opatření, která ochrání naše aktiva.

Zabezpečení napájení

Pro případ výpadku elektrické energie by měly být nainstalovány záložní napájecí zdroje (UPS[5]), případně záložní generátory s příslušnou zásobou paliva (diselagregáty). Standardní výbavou záložních napájecích zdrojů, v dnešní době, je implementace různých ochran a filtrů (blesk, výkyvy napájecí sítě, …). Pokud to je možné, je také vhodné využít více přívodů do budovy z různých míst.

Zajištění vhodných klimatických podmínek

Měla by být zajištěna a udržována požadovaná teplota a vlhkost vzduchu v závislosti na požadavcích prostředí. Jiná teplota a vlhkost bude v kancelářích a jiná například v místnosti se servery. Hlavní přívod vody by měl být chráněn a měla by být zajištěna nepřetržitá dodávka vody. Všechny tyto podmínky je nutné sledovat (teploměry, vlhkoměry,…).

Ochrana kabelových rozvodů

Silové a datové kabely by měly být chráněny proti přerušení či odposlechu. To je možné zajistit vhodným vedením rozvodů. Elektrické kabely je možné vést pod zemí, případně ve zdech. Datové a telekomunikační kabely taktéž, případně pomocí nosných prvků (kolektory, lišty,…). Napájecí kabely by měly být odděleny od datových z důvodů interferencí (vzájemného ovlivňování). Je také důležité mít všechny rozvody zdokumentované a důsledně popsané.

Manipulace s paměťovými médii

Používaná média by měla být schválena a zaevidována. Manipulace s nimi musí podléhat určitým pravidlům. To znamená, že při opětovném použití by měla být bezpečně přepsána nebo smazána. Při jejich likvidaci je nutné jejich fyzické zničení, aby nebylo možné, žádným způsobem, data na nich původně uložena rekonstruovat. Likvidace by měla být také předem schválena. Paměťová média musí být také dostatečným způsobem chráněna. To znamená uschována na příslušném místě a neměla by být bez povolení vynášena mimo vyhrazené prostory. Využití vlastních paměťových médi, které si pracovníci zajistí z vlastních zdrojů, by nemělo být povoleno.

[5] UPS - uninterruptible power source (nepřerušitelný zdroj energie)

Umístění a uchovávání aktiv

Aktiva by měla být umístěna a uchovávána na místech k tomu určených. Platí zde takzvaná zásada čistého stolu. To znamená, že pokud je aktuálně nevyužívám, měla by být uložena na bezpečných místech (uzamykatelné skříně, kontejnery, trezory).

Evakuační plány

Je nutné zajistit jejich vypracování a pravidelné testování.

4.5.3 Logická opatření

Jak bylo uvedeno v bodě 1.2 je nutné přístup k informacím řídit na principu need to know. To znamená, že uživatel by měl mít přístup pouze k těm informacím, které nezbytně nutně potřebuje ke své práci.

Správa přístupových oprávnění a privilegií

Musí být jasné, kdo může žádat, schvalovat, zřizovat a rušit přístup k IS. To vše by mělo být zaznamenáváno a uchováváno v písemné podobě. Účty, které nejsou využívány, by měly být reaktivovány nebo vymazány a důsledně kontrolovány (v případě ukončení pracovního poměru). Úpravy oprávnění dle pracovních náplní a pracovního zařazení, jejich průběžná a neustálá kontrola. Uživatel by měl být seznámen s podmínkami přístupu, provozu a udělenými přístupy IS. Opět pokud možno v papírové podobě a zaměstnancem podepsané. Výchozí účty by měly být zakázány nebo přejmenovány a názvy účtů by neměly označovat jejich účel.

Správa a používání hesel

Viz. kapitola 4.1.2 Zásady využívání a nakládání se znalostně orientovanou identifikací osob.

Zásada prázdné obrazovky

Stejně jako u zásady čistého stolu je nutné v případě přerušení práce, aby uživatel uzamkl svůj počítač, případně se odhlásil z aplikací, které využíval. Je také možné nastavit periodu, po které se v případě nečinnosti počítač zamkne automaticky.

Řízení přístupu k síti a síťovým prvkům

Vymezení používaných protokolů, komunikačních portů a zařízení, která je možné do sítě připojit (nesmí být možné připojit neautorizovaná zařízení). Topologie sítě, konfigurace síťových prvků by měla být zdokumentována a veškerá nastavení by měla být zálohována.

K aktivním prvkům by mělo být možné přistupovat pouze po autentizaci. Síť je také možné rozdělit do různých zón s různým stupněm ochrany. Tyto zóny by měly být odděleny firewallem. Provoz v síti by měl probíhat pouze na základně stanovených pravidel a mělo by být možné jednotlivé přenosy šifrovat. V síti by měli pracovat pouze oprávněné osoby, stejně tak jako přistupovat do jiných sítí či internetu.

Řízení přístupu k operačním systémům

K operačnímu systému[6] by měl být povolen přístup pouze uživatelům, kteří jsou identifikováni a ověřeni. To znamená, že OS by měl být schopen uživatele identifikovat a ověřit na základě vstupních informací od uživatele. OS by také neměl identifikovat uživatele, dokud neproběhne úspěšná autentizace a měl by být schopen omezit dobu připojení uživatele. V případě hesel, by měl OS přispívat k jejich bezpečnosti, kontrolou síly hesla, měl by vyžadovat pravidelnou změnu, omezovat počet pokusů o jejich zadání. V případě chybného zadání přihlašovacích informací by neměl zobrazovat, která část je chybná. OS by také měl umět zobrazit po úspěšném přihlášení datum posledního přihlášení do systému. Z důvodu monitorování činnosti uživatelů a dalších je také nutné zajistit správné nastavení času OS (synchronizace času). V OS by měly běžet a být nainstalovány jen ty služby a software, který je nezbytný pro práci uživatele a nemělo by být umožněno tato nastavení měnit. To znamená, že uživatel by neměl mít možnost sám měnit obsah služeb a softwarového vybavení OS, včetně jeho klíčových a důležitých nastavení.

Řízení přístupu k aplikacím

Stejně jako u OS, by měl být umožněn přístup pouze oprávněným uživatelům. Přístup k nim by měl být řízen a monitorován. Platí zde pravidla správy přístupových oprávnění a privilegií, správa a používání hesel a zásada prázdné obrazovky.

Řízení přístupu k výstupním zařízením

Opět zde platí, že právo zapisovat na paměťová média (vyjímatelná) by měla mít pouze oprávněná osoba a platí zde zásady nakládání s paměťovými médii. To platí i pro tisk dokumentů a pořizování kopií. I zde by mělo toto být povoleno pouze oprávněným osobám.

---

[6] Dále budu pojem *operační systém* zapisovat zkratkou OS

4.5.4 Technická opatření

Je nutné zajistit odpovídající technické vybavení, které zajistí dostupnost a spolehlivost všech systémů organizace. Zařízení by měla být odolná vůči působení okolního prostředí a měla by být používána předepsaným způsobem. Doporučuje se využívat kryptografická opatření k zajištění důvěrnosti a integrity. K ochraně důvěrných a citlivých informací je vhodné využívat šifrování. Důležité dokumenty a materiály je vhodné opatřit elektronickým podpisem k zajištění jejich integrity. Přístupy k privátnímu klíči by měly být chráněny a měl by být uložen na bezpečném místě. Měla by být zpracována a využívána správa klíčů a klíče by měly být bezpečně uschovány. Kryptografický a další bezpečnostní HW a SW by měl být schválen, respektive certifikován.

4.5.5 Administrativní opatření

Opatření v rámci vlastní organizace

Každá organizace by měla mít zpracovánu bezpečnostní politiku a důsledně kontrolovat její dodržování a neustále provádět její ověřování. Právě z těchto důvodů je vhodné, pokud existuje v organizaci osoba za tyto činnosti odpovědná. Je také důležité, aby byl každý zaměstnanec s bezpečnostní politikou seznámen a toto stvrdil svým podpisem.

Opatření v rámci služeb třetích stran

V případě poskytování služeb třetí stranou je vždy nutná písemná smlouva, která by měla definovat, jak bude zajištěna důvěrnost, integrita a dostupnost. Jaké služby budou zpřístupněny a jak bude přístup řízen (logický, fyzický). Na druhou stranu, jaké služby bude třetí strana poskytovat, jak bude měřena jejich kvalita a jakým způsobem bude zajištěna ochrana osobních údajů, autorské právo. Je také důležité definovat podmínky spolupráce třetích stran s dodavateli a dalšími partnery. Nesmí se také zapomínat na definování způsobu monitoringu aktivit uživatelů třetích stran, a jakým způsobem budou hlášeny bezpečnostní a jiné incidenty, popřípadě nestandardní stavy.

Outsourcing

Opět jako u služeb třetích stran je nutná písemná smlouva, která ošetří důvěrnost, dostupnost a integritu, způsob splnění právních požadavků na provoz poskytovaných služeb, systému a v neposlední řadě postup v případě havárie nebo snížení dostupnosti.

Řízení přístupu

Stejně jako u logických opatření, respektive logického přístupu, by měly být pevně stanovena nejen logická, ale i fyzického pravidla přístupu pro jednotlivé uživatele a skupiny uživatelů. Pro přístupy by měla být využívána vícestupňová autentizace.

Klasifikace informací

Všechna aktiva by měla být evidována a měl by být stanoven jejich vlastník. Měla by existovat směrnice, která by určovala, jak provádět klasifikaci informací. Každé aktivum by mělo být označeno určitým stupněm klasifikace a dle toho bychom s ním měly také zacházet.

Vývoj a údržba systémů

Každý systém by měl obsahovat dokumentaci, která je pravidelně aktualizována dle prováděných změn. Produkční, vývojové a testovací prostředí je nutné od sebe oddělovat. Pokud je nutné kopírovat data z provozních do testovacích systému, mělo by toto být povoleno a po otestování by data měla být bezpečně smazána. Ověřování vstupních dat by mělo probíhat jak na straně klienta, tak i na straně serveru. Výstupní informace by měly být ověřovány (kontrolní součty). Při vývoji by měl být specifikován postup pro řízení změn a provedené změny je nutné zdokumentovat a zanést do dokumentace systému. Před nasazením je také nutné důkladné otestování a provedení auditu zdrojového kódu. Je možné také provádět testy, které simulují různé útoky a odhalí tak slabá místa IS. Neodmyslitelné je také zálohování veškerého programového vybavení, zálohy zdrojových kódů. Při vývoji je také nutné oddělovat jednotlivé vyvíjené verze systémů.

Auditing a monitoring IS

Úroveň auditování a monitoringu by měla být stanovena na základě analýzy rizik. Samozřejmé by mělo být monitorovat a zaznamenávat přístupy do systémů nebo aplikací (úspěšné i neúspěšné). Doporučuje se také provádět záznam a monitorování přístupu k datům a dalším důležitým funkcím. Záznamy by měly obsahovat označení události, uživatele, označení zařízení, datum a čas, případně další důležité informace specifické pro každý IS. Tyto záznamy by měly být dostatečně chráněny, aby nemohlo dojít k narušení jejich integrity (modifikace, smazání).

Provozní záznamy

U každého systému by měly být evidovány veškeré změny a zásahy, které byly učiněny. Záznam by měl obsahovat datum a čas, důvod zásahu, kdo ho provedl, jakým způsobem.

Není důležité, zda jsou tyto záznamy v elektronické podobě nebo papírové, je však opět důležité zajistit jejich bezpečné uložení.

Zálohování a archivace

Je důležité definovat, co bude zálohováno, či archivováno a také jakým způsobem. Je také důležitá pravidelná kontrola, zda vše probíhá tak jak má a zda jsou zálohovaná data obnovitelná a čitelná. Zálohy by také měly být uloženy odděleně mimo hlavní objekt organizace a patřičně zabezpečeny.

Ochrana před škodlivým kódem

V dnešní době je již takřka standardem, že každý počítač je chráněn antivirovým softwarem, který chrání počítač před škodlivým kódem a dalšími hrozbami. Antivirové programy již nejsou pouze ochranou proti virům, ale obsahují i další bezpečnostní prvky a stávají se komplexním bezpečnostním řešením (firewall, ochrana proti spamu a další.). Aby byl software chránící počítače účinný, je důležité provádět pravidelné bezpečnostní aktualizace a kontroly.

Zajištění kontinuity

V případě vzniku bezpečnostního incidentu, havárie, je nutné zajistit potřebné kroky vedoucí k nápravě zabezpečení provozu podniku. Všechny tyto kroky by měly být zpracovány a uvedeny například v havarijním plánu. Je také nutné pravidelné testování a pravidelná aktualizace, k čemuž je nutné stanovit odpovědné osoby.

Výše uvedená bezpečnostní opatření nejsou implementována samostatně, ale využívají se jejich kombinace, které se vzájemně doplňují. Proto je důležité si uvědomit, že systém je tak bezpečný, jak bezpečný je jeho nejslabší článek.

II. PRAKTICKÁ ČÁST

5 IMPLEMENTACE BEZPEČNOSTNÍCH SLUŽEB VE VRSTVÁCH ISO/OSI

V této části se krátce zmíním, v jakých vrstvách referenčního modelu ISO OSI by měly být bezpečnostní služby implementovány. Referenční model ISO OSI vychází z normy ISO 7498-2 ISO/OSI Security Architekture, která definuje základní bezpečnostní služby pro komunikační sítě. Model se skládá ze sedmi vrstev, kdy 1. fyzická vrstva zajišťuje přenos signálu mezi uzly na bitové úrovni. 2. linková vrstva organizuje telekomunikační provoz po datovém zdroji (přenos rámců dat). 3. síťová vrstva zajišťuje adresování a směruje tok dat (paketů) k cílovým zařízením. 4. transportní vrstva zvyšuje kvalitu komunikačních spojů a zajišťuje spolehlivé doručení paketů. 5. relační vrstva poskytuje pro IS nástroje pro řízení jejich dialogů, respektive řídí spojení mezi jednotlivými komunikujícími aplikacemi. 6. prezentační vrstva zajišťuje kódování a syntaxi výměny dat a konečně 7. aplikační vrstva poskytuje aplikačně orientované služby. Následující tabulka ukazuje, na kterých vrstvách je možné jednotlivé bezpečnostní služby aplikovat a jaké bezpečnostní mechanismy jsou k nim přiřazeny.

Tab. 3 Implementace bezpečnostních služeb a přiřazení bezpečnostních mechanismů

Bezpečnostní služba	Mechanismy	Vrstvy ISO/OSI						
		1	2	3	4	5	6	7
Autentizace spojení	Šifrování, el. podpis, kryptografická			✓	✓			✓
Autentizace odesílatele	Šifrování, el. podpis			✓	✓			✓
Řízení přístupu	Řízení přístupu (heslo, PIN)			✓	✓			✓
Důvěrnost spojení	Šifrování, řízení směrování	✓	✓	✓	✓		✓	✓
Důvěrnost přenosu	Šifrování, řízení směrování		✓	✓	✓		✓	✓
Selektivní důvěrnost	Šifrování						✓	✓
Důvěrnost toku dat	Šifrování, řízení směrování, zarovnání zpráv	✓		✓				✓
Integrita spojení	Šifrování, kryptografické mechanismy				✓			✓
Integrita spojení bez	Šifrování, kryptografické mechanismy			✓	✓			✓
Selektivní integrita	Šifrování, kryptografické mechanismy							✓
Integrita přenosu zpráv	Šifrování, el. podpis, kryptografické			✓	✓			✓
Selektivní integrita	Šifrování, el. podpis, kryptografické							✓
Nepopiratelnost	Šifrování, el. podpis, kryptografické							✓
Nepopiratelnost	Šifrování, el. podpis, kryptografické							✓

Z tabulky je patrné, že všechny bezpečnostní služby je možné implementovat na úrovni vrstvy aplikační. Je také možné říci, že bezpečnostní opatření je potřeba implementovat nejníže na úrovni síťové a transportní vrstvy. Nižší vrstvy nemusí být důvěryhodné.

6 ÚVODNÍ ANALÝZA BEZPEČNOSTI PŘÍSTUPŮ K IS

V této části se snažím zpracovat analýzu současného stavu bezpečnosti přístupů k IS, využívání bezpečnostních mechanismů a chování uživatelů. Zaměřil jsem se především na společnosti (uživatele) působící v oblasti obchodu a výroby. Velikostně se jedná především o společnosti ze segmentu SMB[7]. Proč jsem si vybral právě tyto podniky? Jednak v ČR je velké množství těchto malých a středních firem a ne vždy si mohou dovolit vynakládat na bezpečnost velké finanční prostředky. O to je důležitější umět využívat stávající bezpečnostní mechanismy a umět zvolit a implementovat nové. Druhým důvodem je znalost těchto společností, jelikož působím ve společnosti zajišťující prodej, distribuci a podporu IS, právě pro tento druh společností. Díky implementacím, podpoře a konzultacím znám velmi dobře jednotlivé procesy společností, jejich uživatele, využívané bezpečnostní mechanismy a jejich bezpečnostní politiky. To může být také do jisté míry zárukou a ověřením získaných dat, zda jsou relevantní a odpovídají skutečnosti.

Analýza je rozdělena do několika spolu souvisejících částí. První dvě části jsou důležité pro zjištění bezpečnostních incidentů jednak z hlediska jejich četnosti, druhu a především útočníků, kteří mohou bezpečnostní incident způsobit. Další části analyzují jednotlivé druhy bezpečnostních mechanismů a jejich využívání, jakým způsobem uživatelé s bezpečnostními mechanismy pracují a jakých chyb se dopouštějí. Závěrečná část je vyhrazena celkovému shrnutí a vyhodnocení získaných dat, informací.

6.1 Cíle analýzy

Díky rozdělení analýzy na jednotlivé části, je cílů několik. Snažil jsem se získat informace, z kterých by bylo možné zjistit a vyhodnotit tyto body:

- zjištění nejčastějších bezpečnostních incidentů;
- identifikaci a rozdělení útočníků;
- využívání jednotlivých bezpečnostních mechanismů;
- chování uživatelů ve vztahu uživatel – bezpečnostní mechanismus

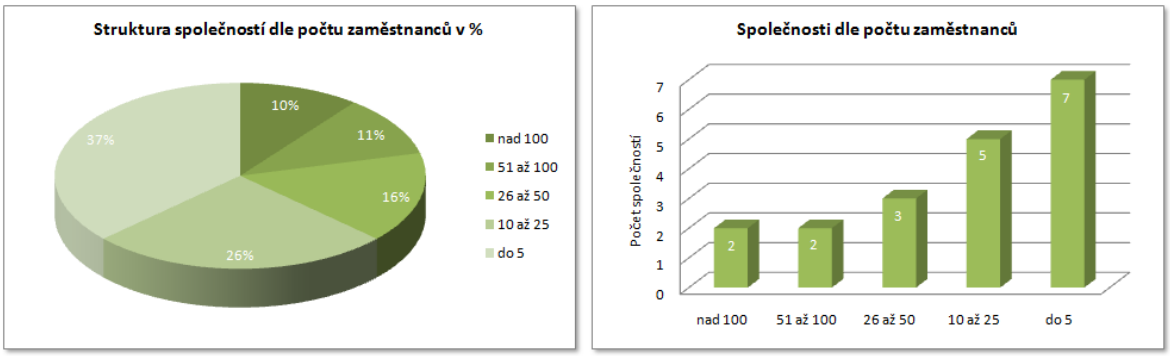
[7] SMB - Small and Medium Business – Malé a střední podniky

6.2 Metodika průzkumu

Pro zjištění potřebných informací, dat jsem využil sestavený dotazník, který jsem rozeslal prostřednictvím e-mailových adres nebo předal jednotlivým respondentům osobně. Jednotlivé e-mailové adresy byly získány z databáze kontaktů (zákazníci) mého zaměstnavatele. K dispozici byly dva druhy dotazníků, jeden pro běžné uživatele a jeden pro pracovníky IT či osoby zpracovávající bezpečnostní politiky.

6.3 Struktura respondentů

Pro vlastní vyhodnocení je velmi důležité znát strukturu oslovených společností. Celkem bylo osloveno 19 společností, z různých částí ČR. Celkový počet oslovených respondentů u těchto společností činil 138 a z toho bylo 23 IT pracovníků. Z toho 97 uživatelů a 17 IT pracovníků dotazník vyplnilo a vrátilo zpět.

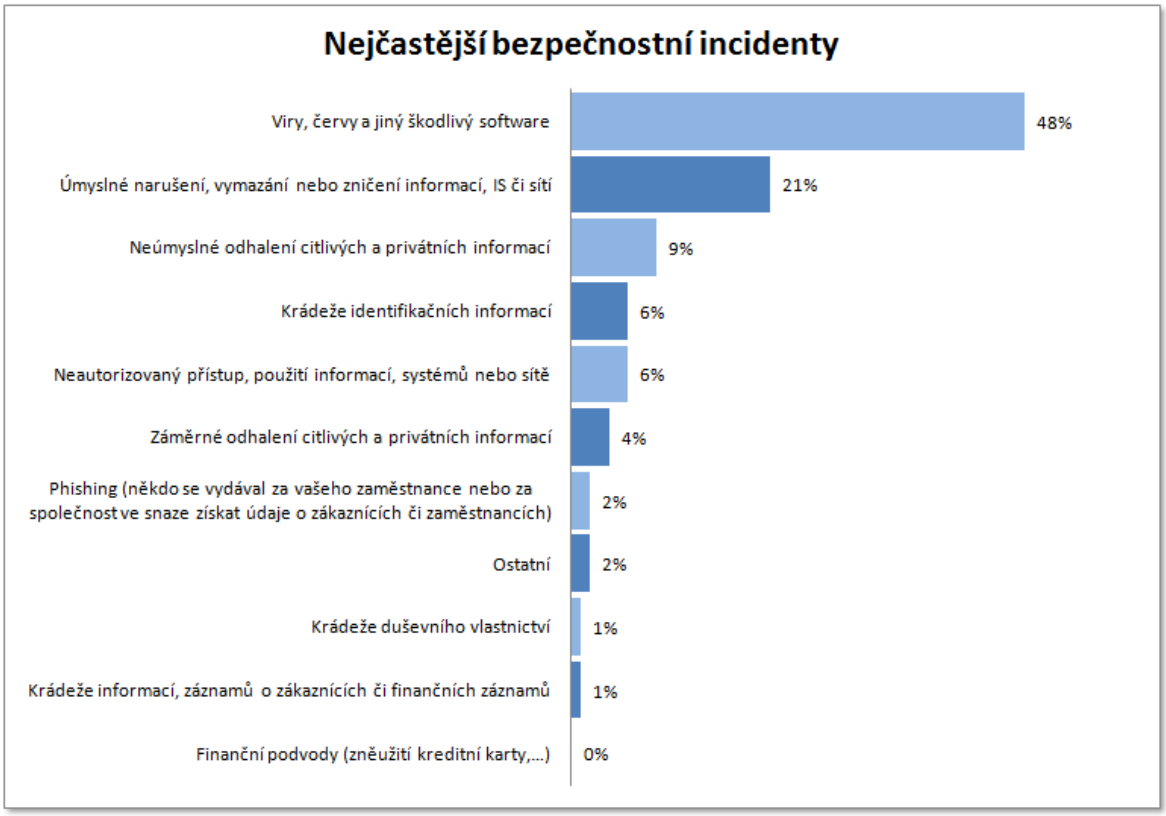


Obr. 5 Struktura respondentů dle počtu zaměstnanců

Obr. 6 Struktura respondentů dle odvětví a zaměření

6.4 Bezpečnostní incidenty z hlediska druhu a příčiny

Abychom se mohli úspěšně bránit a implementovat opatření proti bezpečnostním incidentům, musíme znát jejich povahu a příčiny. To znamená, že je nutné provést analýzu rizik a na základě této analýzy teprve podnikat příslušné kroky. Což je ostatně popsáno v teoretické části. K této části analýzy byly využity dotazníky určené pro IT pracovníky, jelikož jsou to právě oni, kdo zpravidla implementuje bezpečnostní mechanismy, řeší bezpečnostní incidenty a mají v dané oblasti největší přehled.



Obr. 7 Nejčastější bezpečnostní incidenty z hlediska druhu

Jak můžeme vyčíst z obrázku (obr. 7), tak nejčastějším bezpečnostním incidentem je infikování viry, červy a jiným škodlivým softwarem. I přes to, že dnes většina organizací vlastní antivirová řešení, jedná se poměrně o vysoké procento. Důvody můžeme hledat opět u chování uživatelů, případně nedostatečných aktualizací antivirových řešení nebo jejich konfiguracích.

Dalším nezanedbatelným bezpečnostním incidentem je úmyslné narušení, vymazání nebo zničení informací, IS či sítí. Tyto incidenty jsou velmi často páchány vlastními zaměstnanci, což potvrzuje následující obrázek (Obr. 8). Co je k tomu vede? Příčin může

být hned několik. Mezi nejčastější patří situace, kdy zaměstnanec dostane z nějakého důvodu výpověď z pracovního poměru a mstí se tímto způsobem svému zaměstnavateli. Nebo se může také jednat o rivalitu mezi kolegy, kdy si navzájem tímto způsobem mohou škodit. V praxi jsem se setkal nespočet krát s tímto problémem a ne vždy je možné těmto situacím zdárně předcházet. Je však možné přijímat opatření, která povedou ke snižování vzniku těchto incidentů, jejich předvídání a následně připravenosti na řešení těchto situací a snižování jejich dopadů.

Proč jsou právě tyto dva druhy zastoupeny v takové míře? Vyplívá to především z toho, že průzkum probíhal v malých a středních firmách působících v oborech, které nemají zpravidla tak velké požadavky na bezpečnost. Jejich finanční možnosti jsou omezené a vynaložené náklady na zabezpečení mohou být vyšší než cena chráněných aktiv či výše finanční ztráty v případě bezpečnostního incidentu. Samozřejmě vše je závislé na hodnotě aktiv, které je potřeba chránit. I malá firma může vlastnit aktiva obrovské hodnoty nebo mít potřebné finanční prostředky.

Neúmyslné odhalení citlivých a privátních informací je zastoupeno 9%, což je poměrně vysoké procento. Přitom těmto incidentům můžeme jednoduše předcházet neustálým zvyšování kvalifikace zaměstnanců, kteří s informacemi pracují. Počítačová gramotnost je dnes velmi důležitá a ne vždy je vzhledem k náplni práce daného zaměstnance dostačující. Kromě kvalifikace je však také nutné mít kvalitně zpracovány jednotlivé procesy a privilegia ve firmě, které dávají všem činnostem jistý řád.

6% bezpečnostních incidentů mají na svědomí krádeže identifikačních informací a neautorizovaný přístup, použití informací, systémů nebo sítě. Způsobů jak předcházet těmto incidentům je mnoho. Od kvalitně zpracované bezpečnostní politiky, kvalifikovaných pracovníků, přes využívání korektně přidělených práv, privilegií, procesů, fyzických překážek, až po chování zaměstnanců při zacházení s identifikačními a autentifikačními mechanismy. Krásným příkladem může být přístupové heslo poznamenané na papírek a nalepené například na rám monitoru. To už vlastně nelze považovat ani za krádež identifikačních informací, jelikož je potencionálnímu útočníkovi dáváme dobrovolně.

Záměrné odhalení citlivých a privátních informací (4%) má většinou stejnou příčinu jako úmyslné narušení, vymazání nebo zničení informací, IS či sítí. Z toho důvodu je i řešení obou těchto případů velmi podobné, stejné. Phishing[8] je zastoupen pouze 2%, nicméně se jedná o velmi nebezpečnou techniku, jak z uživatele vylákat citlivé informace prostřednictvím e-mailu. Obranou je opět zvyšování kvalifikace uživatelů a především používání zdravého rozumu. Pokud si však nejsme jisti, zda se nejedná o phishing, tak je dobré vše důkladně prověřit, než citlivé informace někomu poskytneme. Ostatní bezpečnostní incidenty a krádeže jsou již zastoupeny velmi malým procentem a jsou v segmentu SMB ojedinělé. Důvodem je, že s velmi citlivými a důležitými informacemi zpravidla pracuje velmi úzký okruh lidí nebo pouze jedna osoba.

To jsme si zhodnotili bezpečnostní incidenty z hlediska druhu a nyní se pojďme podívat na bezpečnostní incidenty z hlediska jejich příčiny. Jak už jsem zmínil výše, tak nejčastější příčinou jsou vlastní zaměstnanci společnosti. I z vlastní zkušenosti mohu potvrdit, že tomu tak je. Je však potřeba rozlišit zda se jedná o úmysl nebo nechtěný čin. Zpravidla se jedná o neúmyslně způsobené bezpečnostní incidenty, způsobené buď nízkou kvalifikací, nedostatečným zaškolením nebo nízkou informovaností. Neúmyslný čin však nikterak nesnižuje vážnost takovýchto bezpečnostních hrozeb, ba naopak. Jak jsem již v této kapitole psal, je nutné neustále zvyšovat kvalifikaci a informovanost zaměstnanců a nastavit všechny procesy v rámci činnosti společnosti tak, aby k těmto incidentům (úmyslným i neúmyslným) nedocházelo nebo alespoň v omezené míře.

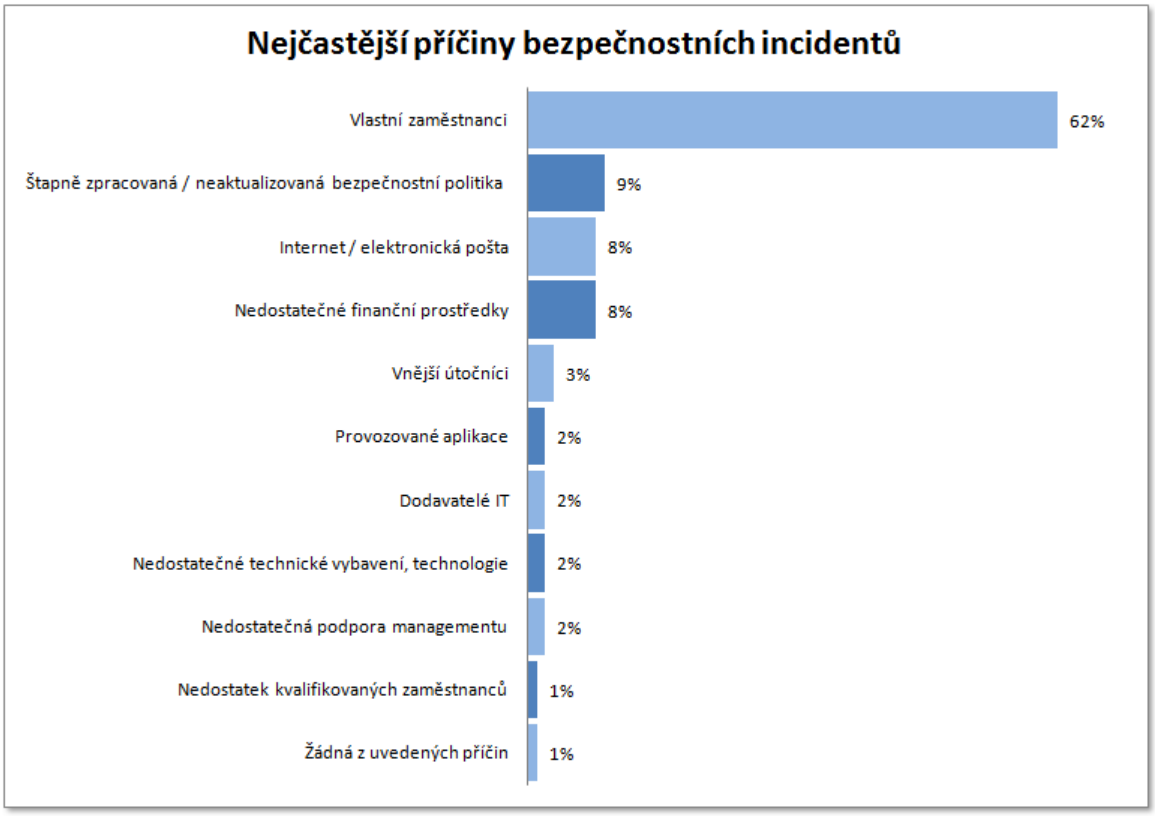
9% na vzniku bezpečnostních incidentů se podílí bezpečnostní politika, respektive její neaktuálnost nebo její zpracování. Zpracování bezpečnostní politiky vždy předchází důkladný bezpečnostní audit a analýza rizik. Pokud se toto podcení a na těchto základech se zpracuje bezpečnostní politika, je velké riziko vzniku bezpečnostních incidentů. Na druhou stranu i přes velmi dobře zpracovanou bezpečnostní politiku může dojít k bezpečnostním incidentům. Proto je velmi důležité pravidelně bezpečnostní politiku aktualizovat, vzhledem k novým technologiím, novým hrozbám, atd. Hned v závěsu za bezpečnostní politikou je internet a elektronická pošta. Opět zde platí, že pokud jsou prostředky pro využívání těchto technologií správně nakonfigurované a jsou využívány

[8] Phishing – podvodná technika používaná k získávání citlivých údajů vydáváním se za někoho jiného.

kvalifikovanými pracovníky, je možné snížit riziko vzniku bezpečnostních incidentů na minimum. Na stejné úrovní jako internet a elektronická pošta je s 8% procenty nedostatek finančních prostředků. Tady bych se rád trochu zastavil. Je samozřejmě důležité, aby si management uvědomoval důležitost investic do technologií, které přináší zvýšení bezpečnosti. Nicméně se domnívám, že se také z velké části jedná o alibismus IT pracovníků. U segmentu SMB toto platí dvojnásobně. Jak se říká, tak i za málo peněz lze udělat hodně muziky.

Další příčiny jsou samy o sobě zastoupeny malým procentem, dohromady však dávají 13% a i na ně je nutné myslet a přijímat taková opatření, která povedou k jejich eliminaci. Rád bych zde krátce zmínil provozované aplikace, které jsou zastoupeny 2%. Žádná aplikace není dokonalá a její provoz má svá rizika a úskalí. Nicméně pokud dodržuji základní pravidla práce s danou aplikací, instaluji aktualizační a bezpečnostní balíčky, konfiguruji danou aplikaci dle doporučení jejího výrobce, tak se tato příčina velmi výrazně snižuje. Neméně důležitý je také výběr vhodné aplikace pro konkrétní činnost a potřeby společnosti. 2% také přispívá nedostatečná podpora managementu. I přes to, že v posledních letech byl udělán v této oblasti velký posun, stále se můžeme s tímto jevem setkat. Může to být způsobené jednak neznalostí nebo neochotou se tím zabýt. Konec konců je to typická lidská vlastnost. Dokud se člověk nestane sám nebo někdo z blízkého okolí, obětí nějakého útoku, tak proč se tím zaobírat. Samozřejmě nic se nesmí přehánět a všechna opatření je nutná provádět účelně a adekvátně k hrozbě a chráněnému aktivu. Poslední příčinu, kterou bych zde chtěl ještě zmínit a zatím jsem o ní ještě nehovořil, jsou dodavatelé IT. I zde je velmi důležitý výběr vhodného a prověřeného dodavatele, který je schopen naplnit naše požadavky a potřeby. Reference jsou velmi důležitým faktorem při výběru. Neméně důležité jsou však i další parametry, jakou je záruční a pozáruční servis, poskytované služby a podpora, rychlost reakce na požadavky, spolehlivost, důvěryhodnost a další. Především u malých firem je u řady činností využíván outsourcing[9]. Platí zde stejná pravidla jako při výběru obchodních partnerů a všechny aspekty vztahu je nutné vždy písemně podložit, stanovit povinnosti a práva zúčastněných stran plynoucí z charakteru poskytovaného produktu, služeb.

[9] Outsourcing – využívání vnějších zdrojů a služeb externích pracovníků, namísto zaměstnávání vlastních zaměstnanců.



Obr. 8 Nejčastější příčiny bezpečnostních incidentů

6.5 Bezpečnostní incidenty z hlediska útočníků

Agentura Ogilvy Public Relations provedla v roce 2009 výzkum, v jehož rámci byl osloven management více než 150 významných společností působících v České republice s otázkami bezpečnosti v oblasti IT. Z výsledků výzkumu této agentury mimo jiné vyplynulo, že největší hrozbou z pohledu firemní bezpečnosti IS/IT jsou v 78 % vlastní zaměstnanci. Podobně vysoké procento bylo potvrzeno i mým výzkumem nejčastějších příčin vzniku bezpečnostních incidentů v rámci zkoumaných společností.

Výsledky získané výše uvedenou agenturou a mým průzkumem (a mými zkušenostmi) korespondují v mnoha ohledech s podobnými průzkumy ze zahraničí a ukazují, že společnosti berou rizika spojená s využívání IS/IT stále vážněji. V dalších ohledech se však již výzkumy (můj a agentury) rozcházejí. Je to dáno strukturou respondentů, kdy v mém průzkumu byly zkoumány především menší a střední firmy.

Vraťme se však ke struktuře útočníků. Z mého průzkumu vyplynulo, že 62% útočníků tvoří vlastní zaměstnanci. Z tohoto pohledu můžeme tedy útočníky rozdělit na útočníky působící

uvnitř organizace a útočníky vnější. Zaměstnanci samozřejmě spadají do první kategorie, vnitřních útočníků. Dále můžeme mezi vnitřní útočníky ještě zařadit dodavatele IT (2%). Tím je míněn outsourcing IS a IT produktů a služeb. Vnější útočníci tvoří dle průzkumu celkem 3% z nejčastějších příčin vzniku bezpečnostního incidentu. Zpravidla se jedná o osoby, skupiny osob, které nemají se společností nic společného. Může se však jednat i o bývalého zaměstnance. Nebezpečnost těchto útoků je různá a je závislá na technickém vybavení a odborné úrovni útočníka. Z tohoto pohledu můžeme vnější útočníky rozdělit na amatéry, hackery[10], profesionály. Amatéři jsou většinou lidé, kteří jen zkouší jaké to je. Používají k útokům návody či software, který našli na internetu a jejich nebezpečnost je mizivá. Jejich úspěšnost je zpravidla zapříčiněna například nesprávně zabezpečeným serverem. Na druhou stranu hackeři jsou již vysoce kvalifikovaní útočníci, kteří mají hluboké znalosti. Jejich nebezpečnost je poměrně vysoká a právě proti těmto útočníkům je většina IS chráněna. Poslední skupinou jsou profesionálové. Jedná se o vysoce kvalifikované a špičkově vybavené skupiny. Jejich nebezpečnost je velmi vysoká a ochrana proti nim je pro valnou většinu IS příliš nákladná a nedostupná. Na druhou stranu jejich útoky jsou vždy mířeny proti významným a důležitým cílům.

6.6 Využití bezpečnostních mechanismů

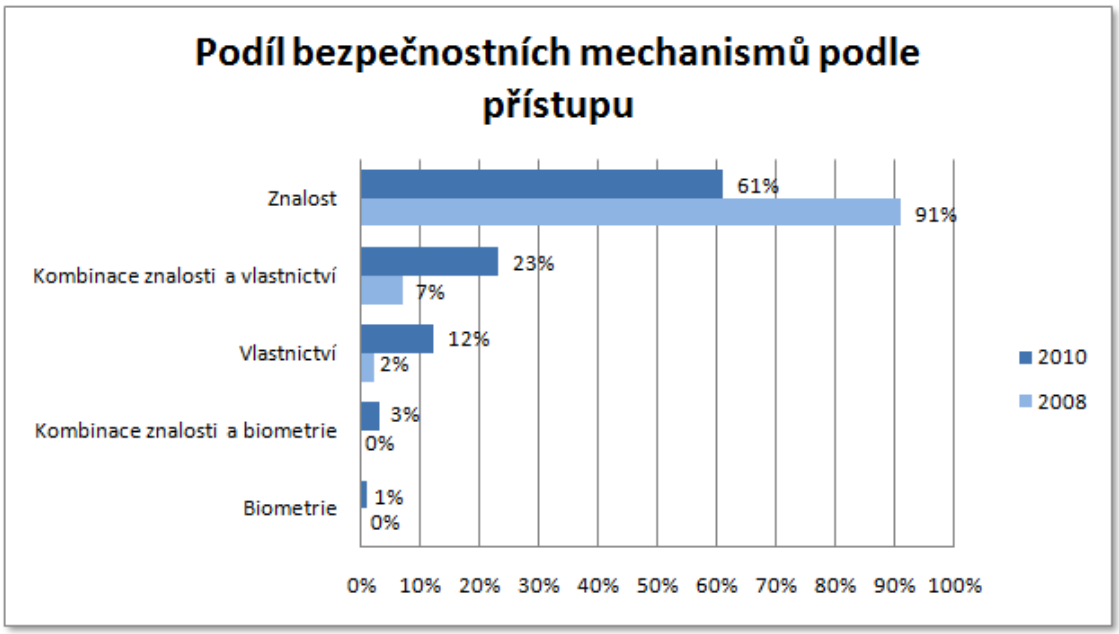
Jednotlivé druhy bezpečnostních mechanismů a míra jejich využití, je závislá na mnoha faktorech. Jiné mechanismy mohou být využívány v komerční sféře a jiné zase ve sféře veřejné. Vše je také závislé na bezpečnostních požadavcích a aktivech, která mají být chráněna. V této části analýzy jsem se zaměřil na zhodnocení aktuálního stavu využívání bezpečnostních mechanizmů. Jako v předchozí části, odpovídali na tyto otázky pracovníci IT, kteří mají největší přehled o použitých technologiích.

6.6.1 Využití jednotlivých druhů bezpečnostních mechanizmů

Již předem se dalo očekávat, že v segmentu SMB bude nejvyužívanějším bezpečnostním mechanismem identifikace a zabezpečení na základě znalostí (hesla, PIN). Přesto je velmi zajímavé porovnat situaci v roce 2008 se současností. Z obrázku (Obr. 9) je patrné, že od

[10] Hacker – počítačový odborník či programátor s detailními znalostmi o fungování systémů

roku 2008 došlo k jistému zvýšení podílu bezpečnostních mechanismů založených na kombinaci znalosti s biometrií, znalosti a vlastnictví. Je to dáno především tím, že technologie se stávají dostupnějšími, jsou dlouhodobě vyzkoušené a spolehlivé. Také jejich cena je podstatně nižší, což má určitě u menších a středních společností také velký vliv. Tento trend je také zapříčiněn nízkou bezpečností znalostních bezpečnostních mechanismů. Znalost v kombinaci s vlastnictvím nebo biometrií výrazně zvyšují bezpečnost. Tyto kombinace se označují jako dvoufaktorová autentizace. Příkladem může být využití čipové karty + hesla (stejně tak je možná i třífaktorová autentizace, kdy je například využito USB tokenu[11], znalosti a biometrie dohromady). Záměrně jsem vynechal kombinaci vlastnictví a biometrie nebo kombinací všech tří. Důvodem je, že tyto kombinace nejsou tak časté a v rámci zkoumaných organizací nebyly nikdy použity a používány nejsou.



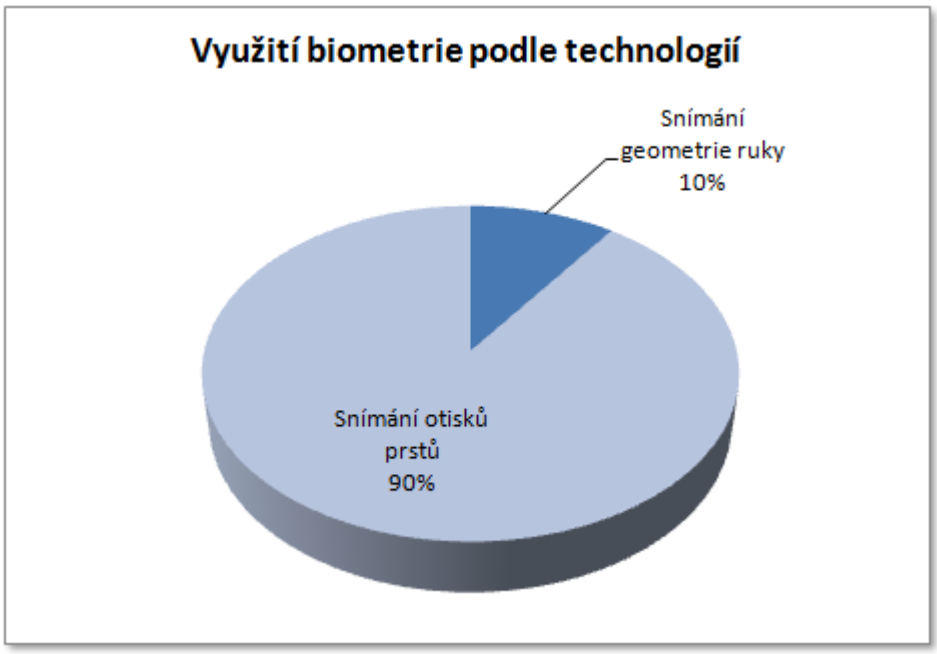
Obr. 9 Využívání bezpečnostních mechanismů podle přístupu v roce 2008 a 2010

6.6.2 Využití biometrických metod identifikace

V této kapitole je zpracován pohled na podíly technologií založených na biometrii. Respektive jaké technologie se u tohoto přístupu nejčastěji využívají u zkoumaných

[11] USB token – hardwarové zařízení sloužící k autentizaci (bezpečné uložení šifrovacího klíče).

organizací. Následující obrázek (Obr. 10) ukazuje podíl biometrických metod a použitých technologií, které jsou používány buď samostatně, nebo v kombinaci se znalostními bezpečnostními mechanismy. Z 19 oslovených společností využívá biometrické technologie a jejich kombinace s ostatními způsoby zabezpečení pouze 10 společností. Jak je vidět největší podíl mají technologie snímáni otisků prstu a to celých 90%. Je to dáno dostupností a cenou snímačů v řádu stovek korun. Velmi často se dnes také tyto snímače integrují do notebooku a dalších přenosných zařízení. Zpravidla se jedná o kontaktní snímače (optické, elektronické, opto-elektronické, kapacitní, tlakové a teplotní) nebo bezkontaktní (optické a ultrazvukové). Zbylých 10% připadá na technologie snímání geometrie ruky. Díky velikosti snímačů a snímaného objektu (ruky) jsou využívány zpravidla pro vstupy do objektů, prostor a také pro účely docházkových systémů. Tato zařízení jsou již poněkud dražší a jejich cena se pohybuje řádově v desítkách tisíc.

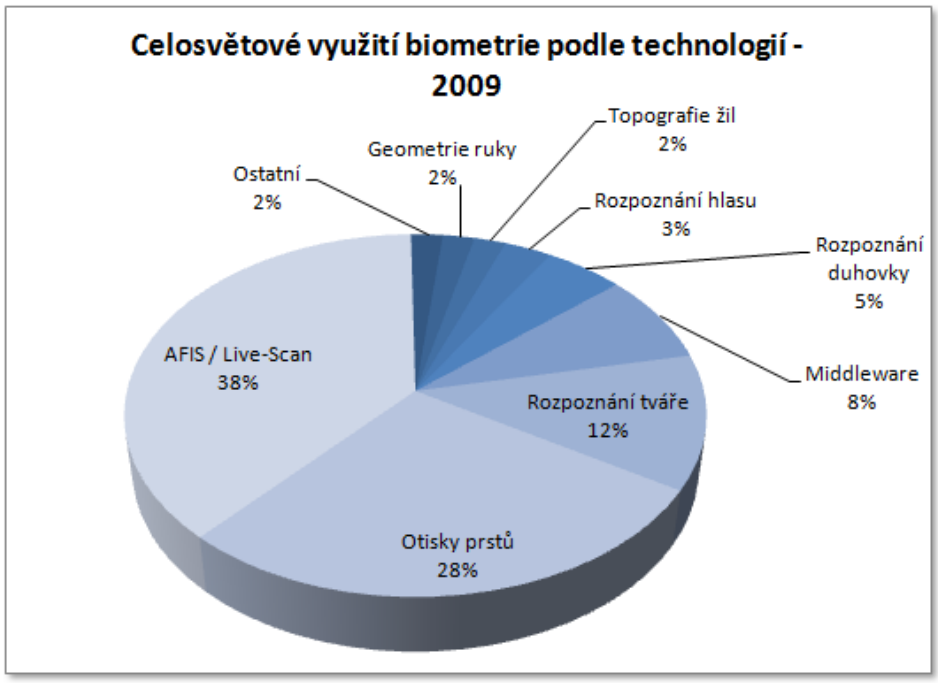


Obr. 10 Využívání biometrie podle použité metody

Zajímavé je srovnání s využitím biometrie z celosvětového hlediska. Největší podíl má AFIS / Live-Scan[12] a otisky prstů. Důvodem je především to, že daktyloskopie[13],

[12] AFIS / Live-Scan – Skupina počítačových aplikací, využívaných daktyloskopických metod pro identifikaci a verifikaci, primárně určená pro policejně-soudní potřeby.
[13] Daktyloskopie – nauka, která zkoumá otisky obrazců papilárních linií na vnitřní straně prstu, na dlaních, chodidlech a o stopách v nichž jsou papilární linie zobrazeny.

respektive znalost existence papilárních linií a použití pro identifikační účely, není žádnou novinkou. Ostatně tato metoda se využívala již ve staré Číně a Asýrii, minimálně 6 až 7 tisíc let před narozením Krista a byla také archeologicky doložena. V současné době je tato metoda využívána za pomoci výpočetní techniky, což velmi usnadnilo její používání a přispělo k rozšíření i do komerční sféry. Zbylé metody mají poměrně malý podíl a jsou využívány tam, kde je identifikace podle otisků prstů nevhodná nebo nedostačující. Každá metoda má svá pro a proti a záleží na konkrétních podmínkách vhodnosti jejich použití. Identifikace na základě otisků prstů je asi nejlepší volbou z pohledu spolehlivost / cena.

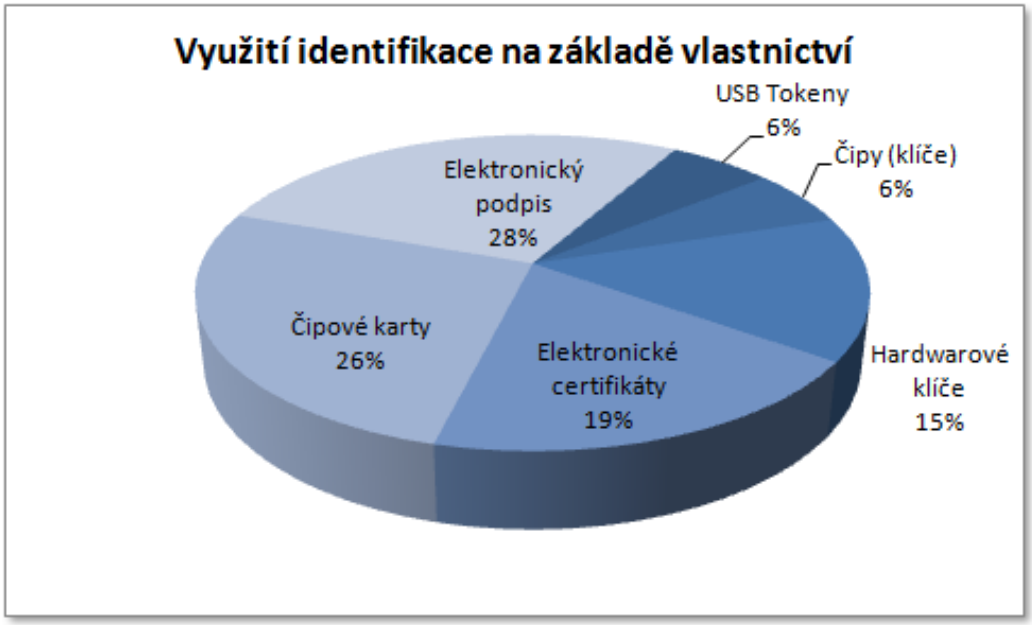


Obr. 11 Celosvětové využití biometrických technologií 2009 [16]

6.6.3 Využití identifikačních mechanismů založených na vlastnictví

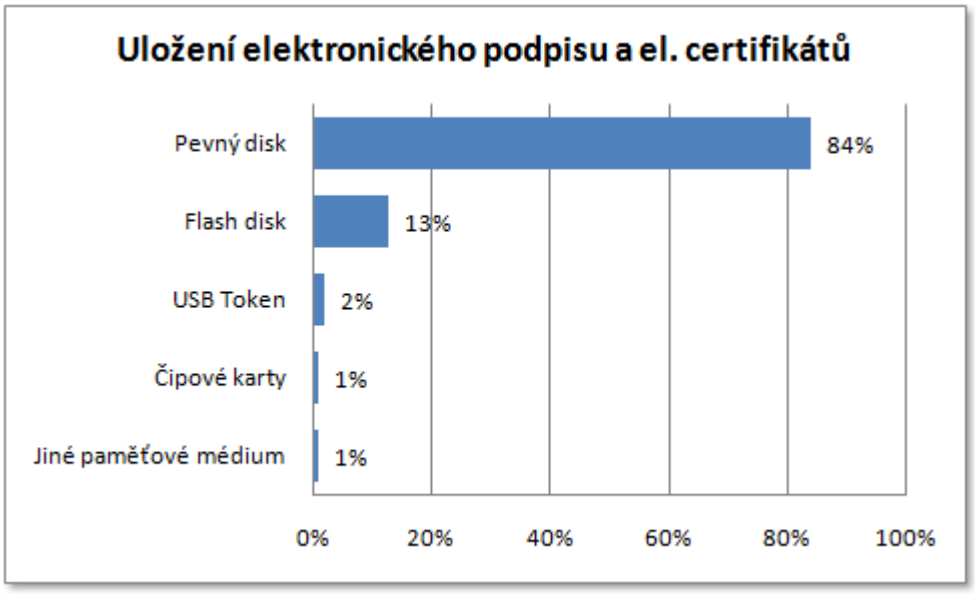
Tyto metody jsou založeny na tom, že osoba, která má být identifikována něco vlastní, co jí bylo uměle přiděleno. Zpravidla jsou to různé čipy, čipové karty, magnetické karty, autentizační kalkulátory, USB tokeny, hardwarové klíče a další. Jak jsme mohli vidět na předchozím obrázku (Obr. 9), podíl těchto identifikačních mechanismů v posledních letech významně vzrostl a využíván je zejména v kombinaci se znalostními mechanismy. Na následujícím obrázku můžeme vidět podíl jednotlivých technologií, které jsou v současné době zkoumanými společnostmi využívány. Čipové karty s 26% získaly svůj podíl především zásluhou elektronického bankovnictví, kde jsou v hojné míře využívány pro přístup k bankovním účtům dané společnosti. 15% tvoří hardwarové klíče, které se

používají především jako ochrana aplikačních programů. Bohužel však ze zkušenosti vím, že ve většině případů jsou trvale zasunuty do USB portu počítače. Tím samozřejmě ztrácejí na bezpečnostním významu a zajišťují pouze funkčnost dané aplikace. Čipy s 6% jsou zejména využívány pro přístup do budov a prostor doplněné o funkci docházkového systémů.



Obr. 12 Využití identifikačních mechanismů založených na vlastnictví

Záměrně jsem si na konec nechal elektronický podpis, elektronické certifikáty a USB tokeny. Jelikož využívání elektronického podpisu v poslední době výrazně vzrostlo, především z důvodů elektronické komunikace se státní správou, zajímalo mě také jakým způsobem je elektronický podpis a případně další elektronické certifikáty chráněny a zabezpečeny z hlediska jejich zneužití. Právě USB tokeny, případně i čipové karty jsou vhodným nástrojem pro uchování elektronického podpisu, privátních klíčů, atd. Musím říci, že výsledky byly pro mě překvapením, i když jsem něco podobného tak trochu čekal. Jak můžeme vidět na obrázku (Obr 13.), celých 84% držitelů elektronického podpisu jej má uložený na svém pevném disku a to je opravdu vysoké procento. Je jasné, že takovýto způsob uchování elektronického podpisu zcela degraduje bezpečnostní úroveň tohoto způsobu zabezpečení. Flash disk se 13% je možná ještě horší variantou. Pokud jej uživatel ztratí, není velkým problém pro nálezce z něj elektronický podpis získat a následně zneužít.



Obr. 13 Uchování elektronického podpisu a elektronických certifikátů

Jak je vidět, tak bezpečné uložení elektronického podpisu a dalších elektronických certifikátů je zastoupeno opravdu malým procentem, které je v porovnání s uložením na pevném disku nebo flash disku zanedbatelné. Věřme, že zvyšování kvalifikace zaměstnanců a možná právě výsledky tohoto průzkumu přispějí k nápravě současného stavu.

6.7 Chování uživatelů při využívání bezpečnostních mechanismů

V této části bylo mou snahou získat informace, jakým způsobem uživatelé s bezpečnostními mechanismy pracují a jak s nimi zachází. Zaměřil jsem se především na znalostní bezpečnostní mechanismy (hesla), které jsou zastoupeny v největší míře (Obr. 9). Zajímalo mě také, jakým způsobem jsou vytvářeny a předávány jednotlivým uživatelům. V této části také již byly respondenti složeny nejenom z IT pracovníků, ale i z řad běžných uživatelů.

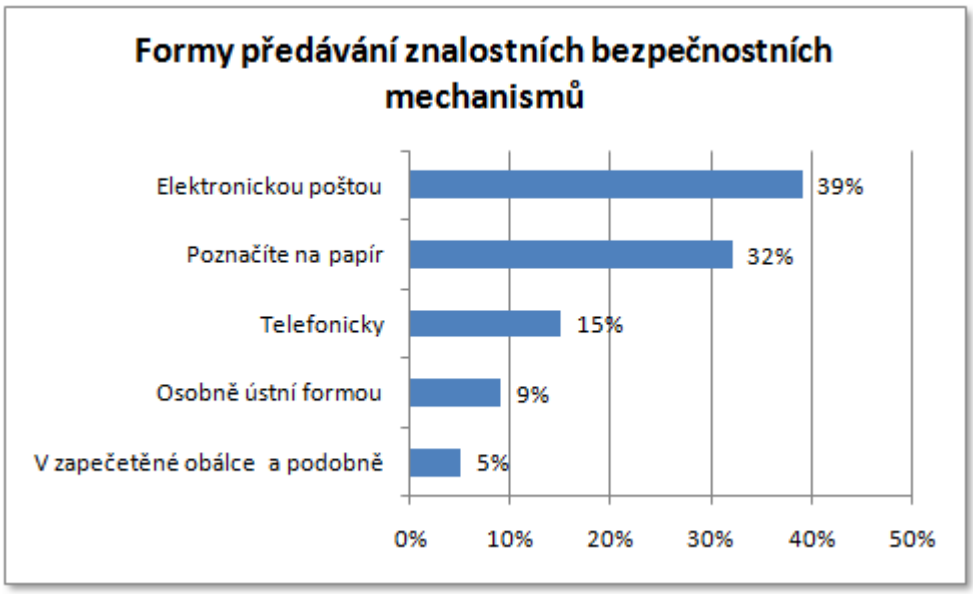
6.7.1 Tvorba a používání znalostních bezpečnostních mechanismů IT pracovníky

IT pracovníci byly dotazování, jakým způsobem jsou znalostní bezpečnostní mechanismy (zpravidla hesla) vytvářeny, jak jsou předávány uživatelům, jakým způsobem hesla uchovávají, jak často jsou měněna atd. Výsledky jsou velmi zajímavé a stojí se nad nimi zamyslet. Vypracoval jsem a položil celkem 7 otázek, které jsem považoval z mého hlediska za důležité a přispějí, velkou měrou, k naplnění cílů, které jsem si stanovil v úvodu.

První otázkou byl způsob, jakým jsou hesla vytvářena. Výsledkem bylo: 61% hesel je vytvářeno ručně, 7% jich je generováno pomocí specializovaných softwarů na generování hesel a zbylých 32% si vytváří uživatelé sami. Na tom by nebylo nic špatného, pokud by byla vytvářena hesla silná. Pokud si uživatel vytváří heslo sám, je nutné, aby aplikace, pro kterou je heslo vytvářeno, nutila uživatele o zadání hesla silného (min. požadovaná délka, obsah písmen a čísel, atd.).

Druhou otázkou bylo, zda správci (administrátoři) vytváří hesla silná. Tady jsem očekával převahu u odpovědi „ANO“. Tak tomu také bylo a 82% správců a administrátorů generuje hesla silná. Zbylých 18% je však i tak velká hodnota. Především tito pracovníci by měli být první, kdo dodržuje základní zásady při tvorbě a využívání znalostních bezpečnostních mechanismů.

Samozřejmě to, že generujeme silné heslo, ještě není zárukou vyšší bezpečnosti. Je mimo jiné velmi důležité, jakou formou toto heslo sdělíme jeho uživateli a jakým způsobem s ním pracuje. To byly také další otázky průzkumu. Výsledek té první je vidět na následujícím obrázku (obr. 14).



Obr. 14 Formy předávání znalostních bezpečnostních mechanismů jejich uživatelům

Jak můžeme vidět, tak nejvíce bezpečná forma je zastoupena pouze 5%. Nejvíce využívají IT pracovníci elektronickou poštu nebo zapsání hesla na kus poznámkového papíru. Na jednu stranu jich většina generuje poměrně silná hesla a na druhou stranu je předávají nevhodným způsobem. Sice elektronická pošta je lepší způsob než poznačení na papír, ale

díky tomu jak běžní uživatelé zachází s informacemi při své práci, není ani toto bezpečná forma.

Velmi důležitou veličinou je také možnost změny hesla uživatelem. Pokud je přiděleno uživateli nějaké silné heslo a má možnost si ho změnit, jaké heslo si uživatel nadefinuje? Na toto nám odpoví další kapitola, kde byli dotazování právě běžní uživatelé. Ale vraťme se k možnosti změny hesla uživatelem. Výsledkem je 67% k 33%., respective 67% uživatelů si heslo měnit nemůže a 33% ano. To je poměrně vysoké procento a je velmi důležité aby příslušný operační systém nebo aplikační software vyžadoval a kontroloval uživatelské zadání silného hesla. Tím vyvstává otázka, zda opravdu toto aplikace a operační systémy vyžadují. Z praxe vím, že situace není úplně příznivá a i přes to, že například v operačních systémech tato možnost konfigurace je, málo kdy je využita. O aplikačních systémech ani nemluvě, ale to už je jiná otázka.

Když už si uživatelé mohou měnit hesla nebo je vytváří správci, je také otázkou, jak často je změna hesla požadována. Výsledky jsou opravdu překvapující, leč očekávané. U 12% hesel je vyžadována změna. Na tomto procentu se zejména podílí bankovní aplikace, které společnosti využívají a kde je změna z důvodů bezpečnosti požadována. Zbylých 88% připadá na hesla statická a neměnná. Příliš častý požadavek na změny hesla samozřejmě není žádoucí a uživatelé tak často mění hesla dokola nebo si je začnou někde značit. Na druhou stranu čím déle jedno heslo využíváme, tím je větší riziko, že bude heslo prozrazeno. Je velmi těžké najít tu optimální hranici, periodu změny hesla a je to hodně individuální. I z těchto důvodů jsou bezpečnostní mechanismy založené na znalosti považovány za méně bezpečné.

Předposledním otázkou jsem se chtěl dozvědět, zda si správci a administrátoři generovaná hesla někam ukládají nebo je v případě potřeby změní. 73% si nějakým způsobem ukládá vygenerovaná hesla a 27% nikoliv. Způsob uložení je zpravidla v aplikaci Excel z kancelářského balíku MS Office a to buď v zaheslované podobě na lokálním disku nebo na síťovém disku s příslušným oprávněním. Ani jeden ze způsobů nepovažuji za dostatečně bezpečný. Pokud by však byly tyto soubory šifrovány, daly by se tyto způsoby v případě jejich zálohování považovat za bezpečné. To však nebyl ani jeden případ z dotazovaných respondentů.

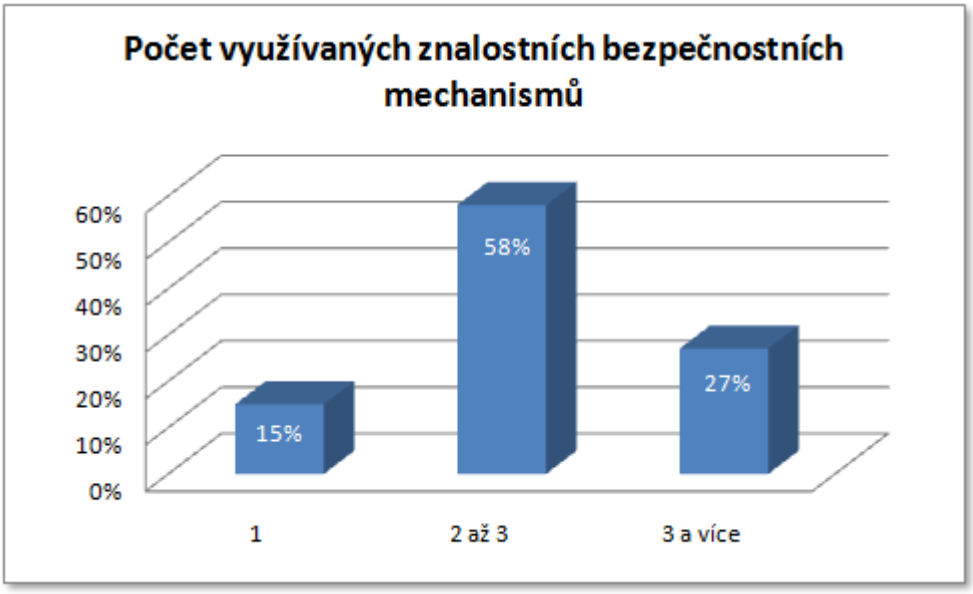
Poslední otázkou bylo, zda správci, administrátoři při řešení běžných provozních problémů, vyžadovali od svých uživatelů prozrazení jejich hesla. Tato otázka se může zdát

jako nesmyslná, vždyť administrátoři mají neomezený přístup, ale získané odpovědi jsou dosti velkým argumentem, proč jsem tuto otázku formuloval. A jaký byl tedy výsledek? 61% administrátorů v některých případech opravdu heslo od uživatele požadovalo a bylo jim prozrazeno. 27% nikdy prozrazení hesla nepožadovalo. To je docela alarmující hodnota. Administrátor by nikdy neměl heslo uživatele požadovat a uživatel by jej neměl sdělovat. V případě nutnosti je samozřejmě možné, že uživatel správci, administrátorovi heslo napíše do příslušného dialogu na počítači nebo se přihlásí do aplikace pro řešení konkrétních problémů, ale není opravdu nutné své heslo prozrazovat. Už jen z toho důvodu, že dané heslo může uživatel využívat i v jiných aplikacích.

Co tedy říci závěrem k této části, kdy byly dotazováni jednotlivý správci a administrátoři. Situace není nejlepší, ale ani katastrofální. Pokud bychom se podívali zpět o pár let, zjistili bychom, že situace byla mnohem horší i přes menší využívání IT. Přichází nové technologie, povědomí o nutnosti chránit svá aktiva je také větší a především se stává nutností.

6.7.2 Používání znalostních bezpečnostních mechanismů běžnými uživateli.

To jak uživatelé s hesly zacházejí, úzce souvisí již s předchozí kapitolou. Uživatelé mohou to, co jim správci a administrátoři dovolí. Pojďme se tedy podívat, jak na tom uživatelé opravdu jsou. Zpracoval jsem a položil, stejně jakou u IT pracovníků, celkem 7 otázek, dívajících se na danou problematiku z druhé strany. Tedy strany běžného uživatele. Nejprve jsem se snažil zjistit kolik hesel či PINů při své práci uživatelé běžně používají. Výsledek je vidět na obrázku (Obr. 15). Pokud bychom k výsledkům přidali ještě hesla a PINy, které jsou využívány v soukromém životě, musí si uživatel pamatovat poměrně hodně znalostních bezpečnostních mechanismů. Nepočítaje s nutností změn hesel či PINů. Když nad tím teď přemýšlím a spočítám si, kolik hesel si musím jako správce pamatovat a skutečně si pamatuji. Tak nejsem daleko od čísla 40, což už je poměrně slušná porce pro zapamatování. Uživatelé jsou na tom sice lépe, ale jsou úplně v jiné pozici než právě správci a administrátoři. Výsledky nejsou u uživatelů nikterak ohromující, ale stojí se zamyslet nad tím, zda je opravdu toto dobrá cesta jak zabezpečovat svá aktiva. Já se domnívám, že nikoliv. Závěry si však nechám až na konec.

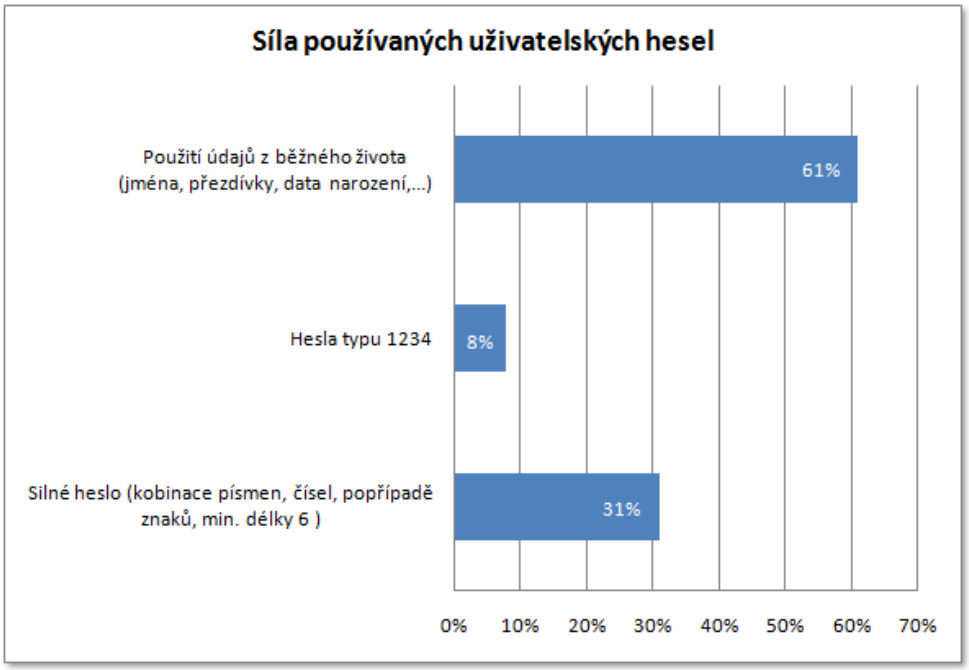


Obr. 15 Počet využívaných bezpečnostních mechanismů běžnými uživateli

Druhou položenou otázkou bylo, jak často si uživatelé hesla mění nebo jsou jim měněna. Část otázky již byla zodpovězena v předchozí kapitole. Ovšem 33% uživatelů si může měnit heslo a tak mohou výsledek značně ovlivnit. Výsledek není překvapující a jen potvrdil mé domněnky. V 85% není heslo vůbec měněno, v 12% je měněno jednou až dvakrát ročně a pouze v 3% je měněno častěji. Z tohoto důvodu je další otázka zcela logická a odůvodněná. Jestliže není heslo měněno, vzrůstá riziko jeho prozrazení. Proto jsem se zeptal, zda zná některé z hesel korespondenta jiná osoba, tedy kolega nebo správce, administrátor. Výsledek mě poměrně zaskočil, protože celých 57% respondentů odpovědělo kladně a pouhých 43% záporně.

Další otázka se vzhledem k předchozímu výsledku zdá trochu zbytečná. Respondenti byli dotazováni na sílu používaných hesel. Ani zde nejsou výsledky povzbudivé. Ostatně vše je vidět na obrázku (Obr. 16). U další otázky je stav podle očekávání podobný jako u dvou předchozích. Respondenti odpovídali na způsob uchování svého hesla. 58% uživatelů si své heslo pamatuje a nikde si ho nepoznamenává. 8% má heslo poznamenané, ale bezpečně uložené (trezor, …). Zbylých 34% uživatelů má heslo poznačená a lehce dostupné (papírek na monitoru, pod klávesnicí, poznámkový blok na stole, a další způsoby). Když se například na školení začnu s uživateli na toto téma bavit, často se setkávám s reakcemi, kdy se uživatel směje a diví se, jak může být někdo takto hloupý. Jak je však vidět, tak to zase až tak k smíchu není, je to bohužel tvrdá a smutná realita. Pokud

jsou hesla uživatelů takto lehce přístupná je možné je jednoduše zneužít. Proto mé další otázky správně směrovali k zabezpečení konkrétního pracovního místa.



Obr. 16 Síla používaných znalostních bezpečnostních mechanismů

Uživatelé byli dotazováni, jakým způsobem zabezpečí po svůj počítač při krátkodobém a dlouhodobém opuštění svého pracovního místa. Ani zde však nejsou výsledky příliš lichotivé. První ze dvou otázek byla, zda při krátkodobém opuštění pracoviště provedou odhlášení z využívaných aplikací nebo zda alespoň zamknout počítač, respektive operační systém. Ač je to k nevíře, tak celých 94% tak neučiní a pouhých 6% ano. Klasickou odpovědí uživatele na to je „vždyť jsem byl pryč jenom minutku“ nebo „byl jsem jen ve vedlejší kanceláři“. Bohužel, právě útočníkovi stačí ta malá chvilka na to, aby si nechal v systému otevřená zádní vrátka, kterými je pak schopný provést útok. Na druhou stranu při opuštění pracoviště na delší dobu, při odchodu z práce je situace již o něco lepší. 76% uživatelů svůj počítač zabezpečí, vypne a 24% uživatelů tak neučiní. Není to však dáno tím, že by uživatelé byli tak opatrní, ale jednoduše proto, že jsou zvyklí počítač vypnout. Takže nic nebrání jim se naučit počítač také zamykat, ale to už je úkol pro správce a administrátory. Správná konfigurace operačního systému, odhlášení po určitém čase nečinnosti nebo jiné způsoby se nabízí a nic nebrání je aplikovat.

6.8 Závěr k analýze bezpečnosti přístupů k IS

Na začátku samotného průzkumu jsem si stanovil čtyři základní cíle. Zjištění nejčastějších bezpečnostních incidentů, identifikaci a rozdělení útočníků, využívání jednotlivých bezpečnostních mechanismů a chování uživatelů ve vztahu uživatel – bezpečnostní mechanismus. Jsem přesvědčen, že formulované otázky napomohly k naplnění těchto cílů a výsledky jsou v mnoha případech velmi zajímavé a splnili očekávání. Přístup jednotlivých respondentů byl velmi zodpovědný a vyplněné dotazníky jsem se dostal od převážné většiny dotazovaných respondentů.

Myslím, že v poslední době si řada společností uvědomuje důležitost bezpečnosti IS/IT vzhledem k jejich primární podnikatelské činnosti. Přesto z průzkumu vyplynulo, že zdaleka není vše ideální a je zde stále velký prostor pro zlepšování, především v řadách běžných uživatelů. K tomu by měla přispět kvalitně zpracovaná interní bezpečnostní politika, která je pravidelně aktualizována. Aktualizace by neměla probíhat pouze jako reakce na nové nebo neočekávané hrozny, ale měla by být probíhat pravidelně a přijatá opatření by měla být také ověřována. Velmi často je také bezpečnost společností zaměřena pouze na bezpečnost síťovou, což není již v současné době dostačující a je potřeba se zaměřit na komplexní bezpečnostní politiku. Už jen z toho důvodu, že v segmentu SMB řada společností spoléhá na služby externích specializovaných firem (outsourcing). Jak už bylo zmíněno, tak většinu bezpečnostních incidentů mají na svědomí vlastní zaměstnanci společnosti. Jak je vidět, tak standardní informační kanály, jako jsou firemní směrnice, oběžníky nebo informační e-maily jsou ve většině případů nedostačující. Je nutné neustále zvyšovat povědomí zaměstnanců o nutnosti zabezpečení a především přijímat taková opatření, která budou uživatele nutit pracovat s bezpečnostními mechanismy vhodným způsobem. Pokud si toto management každé společnosti uvědomí, je napůl vyhráno. To platí i pro jednotlivé správce a administrátory informačních systémů, kteří by měli toto úsilí podpořit správnou konfigurací systémů a důsledným vyžadováním dodržování všech bezpečnostních zásad.

Z výzkumu také vyplynulo, že v porovnání například s bankovním sektorem, nejsou při dané struktuře respondentů využívány ty nejmodernější a nejbezpečnější technologie. Na druhou stranu je za poslední roky vidět posun a velmi často se jednotlivé technologie kombinují (znalostní bezpečnostní mechanismy a bezpečnostní mechanismy založené na vlastnictví), což samozřejmě přispívá ke zvyšování bezpečnosti a snižování rizika

úspěšného útoku. Nahrává tomu také neustálé snižování cen jednotlivých technologií a jejich dostupnost pro komerční sféru. V kombinování jednotlivých technologií a především v biometrii vidím velkou budoucnost a jsem přesvědčen, že vytlačí klasické znalostní bezpečnostní mechanismy do pozadí.

7 PŘÍPADOVÁ STUDIE: ZABEZPEČENÍ PŘÍSTUPŮ K IS SPOLEČNOSTI

V této části se pokusím na konkrétním případu (společnosti) ukázat a navrhnout způsoby zabezpečení využívaných IS, respektive zefektivnění a zvýšení spolehlivosti bezpečnostních mechanismů a bezpečnostních opatření, které daná společnost využívá. Z bezpečnostních důvodů jsem některé informace související s touto společností nekonkretizoval nebo záměrně neuvedl. Pro praktickou prezentaci řešení bezpečnostních požadavků, jsou však uvedené údaje naprosto dostačující.

7.1 Současná situace

Společnost XX a.s. je jedním z předních výrobců a prodejců PETFOOD v České republice. Je součástí nadnárodního uskupení a kromě České republiky má další pobočky na Slovensku a v Polsku. Ve všech třech lokalitách disponuje vlastní distribuční sítí, která je tvořena vlastními obchodními zástupci, konzultanty a regionálními manažery. Na rozdíl od prodeje, probíhá výroba výhradně v České republice. Kromě Slovenské a Polské pobočky vlastní také několik dceřiných společností, které působí v různých oborech mimo hlavní podnikatelskou činnost. Všechny tyto společnosti jsou řízeny mateřskou společností, která zajišťuje veškeré technologie, činnosti a služby v rámci IS a ICT[14]. To znamená, že všechny společnosti využívají pro svou primární podnikatelskou činnost, ve většině případů, stejné IS a ICT technologie. Na všech klientských stanicích a noteboocích jsou instalovány operační systémy Microsoft Windows XP Professional nebo novější Microsoft Windows 7 Professional v příslušných jazykových mutacích. Jako serverové operační systémy jsou využívány různé Linuxové distribuce, Microsoft Windows 2000, 2003 a 2008 Server. Dvě třetiny serverů jsou virtualizovány pomocí VMware ESX serveru. Veškeré servery (HW i SW) jsou fyzicky umístěné v České republice v samostatné klimatizované místnosti, v sídle mateřské společnosti. Výjimkou je umístění jednoho fyzického serveru v sídle Polské pobočky. Tento server má funkci fileserveru, databázového serveru, FTP[15] serveru a je zařazen do domény mateřské společnosti. U všech serverů je zakoupena služba

[14] ICT – Information and Communication Technologies – Informační a komunikační technologie
[15] FTP – File Transfer Protokol – protokol aplikační vrstvy určený pro přenos souborů mezi počítači

servisního zásahu do 24 hodin, v případě poruchy hardwaru. Celkový počet využívaných serverů je 15, z toho 5 fyzických a 10 virtuálních. Počet klientských stanic a notebooků je v průměru kolem 100 kusů. Z toho je zhruba 50 notebooků. Jsou také využívány zařízení PDA v počtu 12 kusů. Využívány jsou zejména top managementem a širším vedením, pro synchronizaci s emailovým serverem (e-maily, kontakty, kalendář). Veškerá důležitá data, jednotlivé databáze IS, data vybraných klientských stanic jsou zálohována na fyzický zálohovací server. Tento server je umístěný v jiné budově, než jsou umístěny ostatní servery společnosti a je umístěný ve vyhrazené místnosti a uzamčený v serverové skříni (rack). U všech klientských stanic a serverů je centrálně řízena instalace opravných a bezpečnostních záplat OS. Všechny OS jsou chráněny antivirovým programem, jehož konfigurace a stahování bezpečnostních aktualizací je taktéž řízena centrálně.

Systém řízení jakosti podle normy ISO 9001:2001, jehož je firma držitelem, se samozřejmě odráží ve všech činnostech společnosti. Jinak tomu není ani z hlediska bezpečnosti, nicméně opět zde je kladem důraz spíše na síťovou bezpečnost a zacházení s elektronickými dokumenty. Ukládání firemních dokumentů probíhá na fileserver nebo do dokumentů na pevných discích klientských stanic, které jsou synchronizovány s fileserverem. Každá kancelář má svou síťovou tiskárnu. V případě potřeby kopírovat dokumenty nebo skenovat a zaslat na příslušný e-mail, je k dispozici síťový kopírovací stroj, který je přístupný pomocí pěti místného kódu PIN (každé středisko má svůj, z důvodu sledování nákladů). Klientské stanice (HW) nejsou fyzicky žádným způsobem zabezpečené, USB porty jsou povolené a je možné připojovat externí paměťová média jako jsou externí disky a flash disky. Notebooky jsou zpravidla vybaveny vypalovacími mechanikami.

Všechny výše zmíněné společnosti využívají jednotný ERP[16] systém, který v sobě integruje a automatizuje velké množství procesů souvisejících s činností podniku. Zejména se jedná o logistiku, distribuci, prodej, výrobu, fakturaci, správu majetku, účetnictví, řízení Cash Flow[17] a další moduly, které jsou součástí daného řešení. Kromě ERP jsou využívány také další aplikace a to aplikace pro řízení vztahů se zákazníky (CRM[18]), specializovaná

[16] ERP – Enterprise Resource Planning
[17] Cash Flow – Peněžní tok
[18] CRM – Customer relationship management

aplikace pro řízení výrobních technologií, manažerský informační systém pro manažerské pohledy a reporty (MIS[19]), mzdový a personální systém, bankovní aplikace pro správu firemních bankovních účtů a další specializované aplikace. Většina aplikací je přístupná z lokální sítě po přihlášení do příslušné domény a po ověření službou Active Directory. Některé z aplikací jsou také přístupné z veřejné sítě internet. K tomu je využíván protokol RDP[20] pracující na principu klient-server. Pro přístup do lokální sítě zvenčí je využíváno VPN spojení, realizováno pomocí softwarové aplikace a hardwarového zařízení společnosti CISCO. Pro přístup k některým aplikacím je také využíván HTTPS[21] protokol, který zajistí šifrovaný přenos mezi webovým prohlížečem a webovým serverem. Tento způsob je používán i u přístupu k některým aplikacím přes mobilní zařízení (PDA). Někteří uživatelé také využívají pro přenosy souborů z/do organizace FTP. FTP server plní také funkci webové serveru, na kterém běží firemní webové prezentace, včetně prezentací dceřiných společností.

Ve většině případů jsou využívány bezpečnostní mechanismy založené na znalosti, tedy hesla různé síly. U většiny IS si mohou uživatelé měnit svá hesla sami. V bankovních aplikacích a pří komunikaci se státní správou je využíváno kombinace znalostních a vlastnických bezpečnostních mechanismů (heslo, PIN + čipová karta nebo heslo, PIN + elektronický podpis). U některých notebooků je kromě znalostních a vlastnických bezpečnostních mechanismů využito biometrie v podobě snímání otisků prstů. Tento způsob ověření uživatelů je však využíván výhradně pro přihlášení do OS.

Jednotlivá bezpečnostní opatření (Personální, fyzická, logická, technická a administrativní) využívaná u této společnosti jsou na různé úrovni a jejich podrobný popis by přesáhl rozsah této práce. Pokusím se však dále vybrat při návrhu řešení ty nejpodstatnější a z hlediska zaměření této práce ty nejdůležitější.

7.2 Cíle a požadavky společnosti

Jako u většiny společností jsou hlavní cíle zaměřeny na podporu dlouhodobé strategie, kterou tato společnost má. Díky velké konkurenci v daném odvětví je velmi důležité

[19] MIS – Management information system
[20] RDP – Remote Desktop Protocol – protokol umožňující uživateli ovládat vzdálený počítač

chránit firemní know-how a aktiva důležitá pro její fungování. To si samozřejmě tato společnost uvědomuje, přesto ale její bezpečnostní politika je v současné době zaměřena pouze na síťovou bezpečnost a ochranu před vnějšími útočníky. Základní zásady využívání síťových prostředků a prostředků souvisejících s ICT technologiemi jsou součástí směrnic systému řízení jakosti. Jsou však z hlediska bezpečnosti naprosto nedostačující a nepokrývají všechny oblasti firemní bezpečnosti. Z těchto důvodů je zde požadavek na zhodnocení stávajícího stavu míry zabezpečení, návrh změn a kroků, které jsou potřeba pro zvýšení bezpečnosti učinit.

Základní požadavky můžeme shrnout do těchto bodů:

- Provést analýzu vnitřního a vnějšího prostředí z hlediska bezpečnosti IS a bezpečnostních opatření.
- Ohodnocení aktiv z hlediska důležitosti pro společnost.
- Identifikace hrozeb a zranitelností.
- Vyhodnocení rizik.
- Návrh vhodných opatření.
- Navrhovaná opatření by měla být základem pro tvorbu komplexní bezpečnostní politiky.
- Navrhované řešení by mělo být v souladu s dlouhodobou strategií a s obchodními cíli společnosti.

7.3 Způsob řešení požadavků

Jak jsem již na začátku zmínil, díky omezenému rozsahu této práce a pro zjednodušení jsem návrhy jednotlivých opatření zaměřil především na ty nejdůležitější aktiva, z hlediska fungování organizace. Zaměřím se především na mateřskou společnost a její pobočky v Polsku a na Slovensku. Díky tomu, že dceřiné společnosti využívají stejné ICT prostředky a většina jich má stejné sídlo bude možné řadu těch nejpodstatnějších návrhů a opatření aplikovat také u nich. Samozřejmě s přihlédnutím k jejich specifikám.

---

[21] HTTPS – Hypertext Transfer Protocol Secure

Pří řešení požadavků a návrhu opatření mi bude nápomocen fakt, že společnost byla součástí průzkumu, který byl zpracován v předchozí části. Navíc právě z této organizace bylo velké procento respondentů, díky čemuž se můžu zaměřit na nejproblematičtější místa, která byla tímto průzkumem odhalena. U jednotlivých aktiv budu na základě vyhodnocení rizik navrhovat jednotlivá bezpečnostní opatření, pokud se bude jednat o aktivum v podobě softwaru, tak také provedu návrh použití konkrétních bezpečnostních mechanismů. Řešení jsem rozdělil do pěti základních kroků, po jejichž splnění bude provedeno celkové zhodnocení požadavků a navrhovaných opatření.

Základní kroky řešení požadavků:

- Zhodnocení a analýza vnější bezpečnosti.
- Zhodnocení a analýza vnitřní bezpečnosti.
- Ohodnocení aktiv a rozdělení IS za použití bezpečnostních kritérií – vnitřní a vnější prostředí.
- Identifikace hrozeb a zranitelností, vyhodnocení rizik.
- Návrh změn, opatření a doporučení.

7.4 Vnější bezpečnost

7.4.1 Vzdálený přístup k firemním zdrojům a aktiva využívaná mimo společnost

Jak jsem již zmínil v úvodu, tak společnost má vlastní distribuční síť, kterou tvoří obchodní zástupci, konzultanti a regionální manažeři. Tito pracovníci pracují mimo sídlo společnosti a samozřejmě, potřebují komunikovat a využívat ICT. Každý z nich má k dispozici osobní automobil, notebook a telefon. Tyto aktiva jim byla předána na základě předávacích protokolů, které při převzetí podepsali a nesou tak za ně odpovědnost. Osobní automobily jsou vybaveny GPS[22] modulem, díky čemuž je pak možné importovat knihu jízd do ERP systému a také sledovat pohyb všech osobních automobilů. Na noteboocích obchodních zástupců je nainstalován a nakonfigurován OS Microsoft Windows 7 Professional a u regionálních manažerů a konzultantů Microsoft Windows XP

Professional. Všichni mají nainstalovaný antivirový program, který je centrálně konfigurován ze sídla společnosti. Všechny tyto notebooky mají přístup k internetu a to prostřednictvím integrovaného GSM[23] modemu se SIM[24] kartou nebo pomocí propojení telefonu s notebookem. Všichni mají na svých noteboocích nainstalovánu lokální databázi s ERP systémem společnosti. ERP systém je prostřednictvím internetu synchronizován s centrální databází, takže všichni mají aktuální data, potřebná pro svou činnost. Synchronizace je nakonfigurována tak, že jsou přenášena jen ta data, která konkrétní obchodní zástupce, regionální manažer nebo konzultant potřebuje. Včetně nastavení přístupových práv k jednotlivým modulům systému, tiskových sestavám, formulářům atd. Přenášená data jsou v komprimované podobě a šifrována. Kromě ERP, přistupují všichni prostřednictvím internetového prohlížeče k CRM systému, který je provozován v sídle společnosti. Regionální manažeři mají také přístup do firemní sítě prostřednictvím VPN a také mají přístup k ERP prostřednictvím RDP. Všichni také využívají elektronickou poštu, jejíž provoz zajišťuje mail server umístěný v sídle společnosti, společně s ostatními servery.

Kromě těchto zaměstnanců, přistupují k firemním zdrojům také další pracovníci. Většinou se jedná o nepravidelnou práci z domu nebo pracovníky spolupracující externě. Ti stejně jako regionální manažeři využívají přístup k firemním zdrojům prostřednictvím VPN spojení nebo využívají přístup přes RDP. Zpravidla se jedná o přístup k fileserveru, kde mají příslušná oprávnění definovaná správci sítě na základě podkladů personálního oddělení. Velmi často je také využíván přístup k ERP společnosti, případně k dalším aplikacím. Ve většině případů přistupují k firemním zdrojům z hardwarových prostředků, které jim zajistila firma a byly nakonfigurovány pro tyto účely. V některých případech je nuzné zajistit přístup k firemním zdrojům také třetí straně. V těchto případech se využívají dočasné účty s potřebnými právy. Po ukončení spolupráce nebo dokončení nějakého činnosti vyžadující tento druh přístupu, jsou tyto účty deaktivovány nebo smazány. Tyto druhy přístupů jsou zpravidla ošetřeny také smluvně, v rámci dané spolupráce nebo poskytovaných služeb. Výše zmíněnými uživateli, spolupracovníky, třetími stranami je

[22] GPS – Global Positioning System
[23] GSM – Global System for Mobile Communications
[24] SIM – Subscriber Identity Module – účastnická identifikační karta

také využíváno FTP připojení pro výměnu dat. Opět se zde jedná, jak o trvalé, tak dočasné účty sloužící k různým účelům.

Mimo sídlo hlavní společnosti je také logistické centrum, které je vzdálené zhruba 2 km. Pracovníci zde umístění jsou zaměstnanci společnosti a využívají ke své práci RDP přístup k ERP systému, který zajišťuje kompletní evidenci skladového hospodářství a logistiku. Je zde umístěno celkem 5 počítačů s OS Microsoft Windows XP a 7 Professional, které jsou zařazeny do domény společnosti a připojeny prostřednictvím VPN spojení. Počítače jsou majetkem společnosti a jsou nakonfigurovány dle platných firemních směrnic. Počítače mají vypalovací mechaniky a volně dostupné a funkční USB porty pro připojení externích paměťových zařízení (směrnicemi je dáno, že jiné než firemní zařízení však využívat nelze). Jsou zde také 2 síťové laserové tiskárny a jedna termotiskárna na tisk etiket s čárovými kódy.

Prostředky a zdroje, které jsou dostupné z veřejné sítě internet:

- Poštovní server (HTTPS)
- Terminálový server pro přístup k ERP společnosti (RDP, Microsoft Windows Server 2008)
- Webový server (FTP, webové prezentace, elektronický obchod)
- CRM systém (HTTPS)

7.4.2 Používané bezpečnostní mechanismy – vnější bezpečnost

Přístup do OS osobních počítačů a notebooků je zabezpečen heslem, které bylo uživateli přiděleno správcem a lze jej pokládat za silné. V některých případech je ještě doplněno biometrii a to konkrétně snímání otisků prstů. Takže je možné se přihlásit buď heslem, nebo sejmutím otisku prstu. Současné použití obou dohromady není nakonfigurováno. Přístup k elektronické poště sice chráněn heslem je, ale heslo je ukládáno a tím pádem při otvírání klienta nevyžadováno. Elektronická pošta je přístupná i přes webový prohlížeč (HTTPS) a je zde nutné zadat uživatelské jméno a heslo, které je zpravidla stejné jako u OS. Hesla si uživatelé v tomto případě měnit nemohou. Pro navázání spojení VPN je nutné mít nainstalovaného klienta a znát heslo. Uživatelům je přiděleno správcem. Pro přístup přes RDP je vyžadováno doménové uživatelské jméno a heslo, stejně jako u přístupu do OS a opět ho nelze uživatelsky měnit. U ERP systému a CRM systému je situaci opačná.

Uživatelům je sice heslo přiděleno, ale mají možnost si ho změnit. Jiné bezpečnostní mechanismy nejsou v současné době využívány.

7.5 Vnitřní bezpečnost

Jak bylo prokázáno průzkumem, tak vnitřní bezpečnost je velmi důležitá. Právě vlastní zaměstnanci jsou viníky převážné většiny bezpečnostních incidentů a většina těch nejdůležitějších aktiv je umístěna právě uvnitř organizace. Chování zaměstnanců bylo podrobně analyzováno průzkumem, díky čemuž není nutné již v této části některé věci znovu rozebírat a opakovat.

7.5.1 Přístup zaměstnanců k firemním zdrojům a aktivům uvnitř společnosti

Proti pracovníkům pracujícím mimo sídlo společnosti, mají pracovníci v hlavním sídle společnosti širší možnosti při využívání IS, ICT a dalších aktiv, které pro svou práci potřebují nebo mohou potřebovat. Proto je velmi důležité správným způsobem rozdělit jednotlivé kompetence, zodpovědnosti a přidělit potřebná oprávnění a privilegia. To samozřejmě závisí na příslušném personálním zařazení a vnitropodnikovém středisku, na kterém zaměstnanec působí.

Jak jsem již avizoval u analýzy vnější bezpečnosti, tak osoby vstupují a odcházejí z hlavní administrativní budovy přes recepci. Druhá administrativní budova recepci nemá, jelikož při vstupu je pouze vstupní chodba a pak již vstupy do kanceláří. Přístupy do jednotlivých kanceláří a dalších místností mají pracovníci, kteří mají příslušný klíč. Respektive existují různé sady klíčů dle středisek a úrovní přístupů. Existují také univerzální klíče, které mají k dispozici vybraní zaměstnanci. Společnost v současné době nevlastní žádný docházkový systém, který by byl schopný primárně zajišťovat evidenci docházky a sekundárně zaznamenávat a monitorovat pohyb osob po budovách. Veškerý majetek společnosti je evidován v ERP systému. Každý majetek má svého vlastníka a je sledována jeho historie z hlediska vlastníků a umístění majetku. Každý vlastník majetku zodpovídá za majetek, který mu byl přidělen v době nástupu do zaměstnání nebo v jeho průběhu. V případě ukončení pracovního poměru je povinen tento majetek odevzdat v patřičném počtu a stavu. Všechny pohyby majetku jsou podloženy předávacími protokoly s vlastnoručními podpisy předávajícího a přijímajícího.

Pracovníky můžeme pro jednoduchost rozdělit na pracovníky administrativní a pracovníky výroby. Pracovníci výroby zpravidla nemají svůj vlastní počítač, ale je vždy společný pro daný výrobní úsek. Tyto počítače jsou součástí domény a uživatelé jsou ověřovány pomocí Active Directory. Každý počítač má zpravidla pouze jeden účet, který využívají všichni pracovníci daného úseku. Počítače jsou zapojeny do lokální sítě a uživatelé mají přístup k síťovým diskům na fileserveru dle příslušných oprávnění. Využívány jsou také pro přístup k ERP, prostřednictvím něhož je řízena výroba (skladové hospodářství, výrobní příkazy, technologické postupy, receptury, a další). Na každém počítači je tedy nainstalován klient a přistupuje se k ERP lokálně. Dále jsou některé počítače také určeny pro řízení výrobních technologií a kromě ERP mají nainstalován specializovaný software, který je s ERP propojen. Dalším využívaným softwarem je software pro tisk etiket a čárových kódů, který je zejména využíván na expedici zboží. Samozřejmě nechybí elektronická pošta pro komunikaci s administrativou a dalšími osobami.

U administrativních pracovníků je situace odlišná. Každý pracovník má svůj stolní počítač nebo notebook a ke své práci využívá mnohem více IS. Jak bylo uvedeno výše, na počítačích jsou nainstalované a nakonfigurované OS Microsoft Windows XP Professional nebo Microsoft Windows 7 Professional. Počítače jsou samozřejmě v doméně a každý uživatel má svůj uživatelský účet ověřovaný službou Active Directory. Po úspěšném přihlášení může přistupovat k přiděleným síťovým diskům a jejich obsahu, opět dle rozsahu svých přístupových práv. Každý počítač má nainstalovaného klienta a může přistupovat k ERP systému v rozsahu svých přístupových práv. Definice práv ERP sytému je velmi podrobná a je možné nadefinovat přístupy nejen k modulům, evidencím a formulářům, ale také k jednotlivým tiskovým sestavám, číselným řadám, bankovním účtům, skladům a dalším. Kromě ERP je také u některých uživatelů využíván CRM systém. Ten je přístupný, obdobně jako u vnější bezpečnosti, přes webový prohlížeč. Dále, je využíván mzdový a personální systém, který využívá mzdové a personální oddělení. Manažeři využívají MIS systém, do kterého jsou data natahována z ERP a dále analyzována. Zpravidla dva pracovníci mají elektronický přístup k bankovním účtům společnosti. Jelikož společnost má více účtů u různých bank, je také způsob připojení ke každému jednotlivému účtu odlišný. Dalším využívaným IS je aplikace (helpdesk) pro evidenci požadavků (úkolů) uživatelů na oddělení IT. Pro přihlášení k aplikaci se využívá webový prohlížeč a je nutné zadat doménové uživatelské jméno a heslo. Administrativní pracovníci samozřejmě využívají i další aplikace. Ty však nejsou z mého pohledu důležité.

Jednak je využívá velmi malé procento uživatelů a také nejsou z hlediska fungování společnosti nijak významné. Přístup k nim je buď s využití hesla, nebo není vyžadováno žádné ověření uživatele.

7.5.2 Používané bezpečnostní mechanismy – vnitřní bezpečnost

Situace s využíváním bezpečnostních mechanismů u vnitřní bezpečnosti je podobná jako u vnější bezpečnosti. Nejvíce jsou využívány znalostní bezpečnostní mechanismy. Výjimkou je využití biometrie u notebooků (snímání otisků prstů) pro přihlášení do OS a využití čipových karet (bankovní aplikace) nebo využití elektronického podpisu či dalších elektronických certifikátů při podepisování dokumentů či komunikaci se státní správou.

Stejně jako u přístupu z vnějšího prostředí je pro přístup k ERP a CRM využíváno uživatelské jméno a heslo, s tím rozdílem, že k ERP systému se uživatelé připojují lokálně a není nutné se ještě před přihlášením připojit pomocí RDP. Hesla si mohou uživatelé u těchto systémů opět měnit. U ostatních aplikací (mzdový a personální systém, MIS, helpdesk a další), které uživatelé uvnitř organizace využívají je situace obdobná, s tím rozdílem, že heslo je jim přiděleno a není možné jej měnit. Speciálním druhem aplikací jsou aplikace sloužící k správě bankovních účtů společnosti. Zde je zpravidla kombinace více bezpečnostních mechanismů (více úrovňová identifikace), důvod není nutné rozebírat. V jednom případě je využívána kombinace znalostního a vlastnostního bezpečnostního mechanismu, respektive čipová karta + PIN. V dalším případě je na daném počítači nainstalován klient, který je přístupný pod heslem a po úspěšném přihlášení je možné s účtem společnosti manipulovat. Posledním způsobem je identifikace na základě čísla účtu a přiděleného hesla, po úspěšném přihlášení může spravovat daný účet. Pokud však uživatel chce provést platbu, musí k tomu využít čipovou kartu. Jak je vidět, tak zejména administrativní pracovníci využívají velké množství bezpečnostních mechanismů, zejména hesla různé síly, PINy, biometrie v podobě snímání otisků prstů, elektronické certifikáty a čipové karty. To jak tyto bezpečnostní mechanismy uživatelé používají, vyplynulo z výzkumu, který byl zpracován na začátku praktické části a je zjevné, že situace není příliš dobrá.

7.6 Ohodnocení aktiv a rozdělení IS dle bezpečnostních kritérií

7.6.1 Ohodnocení aktiv

Jak bylo uvedeno v teoretické části, můžeme aktiva ohodnocovat na základě tří hledisek. Prvním je *dostupnost*. To jsou náklady, které je nutné vynaložit, když něco nefunguje. Druhým je *důvěrnost*, což jsou náklady při neoprávněném zveřejnění nebo úniku citlivých informací. Posledním hlediskem je *integrita*, což jsou náklady při narušení autenticity, přesnosti, úplnosti dat nebo softwaru. Při ohodnocování aktiv se využívají různé specializované nástroje, které ulehčují tuto činnost. Já v tomto případě žádný takový nástroj nemám a díky tomu, že nebudu zacházet do detailu, ani potřebovat nebudu. Pokusím se zde vybrat, z mého pohledu, ty nejdůležitější aktiva z hlediska fungování společnosti a následně je seřadit dle jejich hodnoty a popsat důvody. Samozřejmě jednotlivá aktiva spolu souvisí a jsou vzájemně ovlivňována. Proto není jednoduché je v některých případech rozdělit do jednotlivých bodů samostatně a seřadit dle jejich hodnoty. V některých případech ani není možné jejich hodnotu vyjádřit, proto se spíše snažím popsat jejich význam a důležitost pro činnost podniku.

Vybraná aktiva:

- Kvalifikování zaměstnanci společnosti
- Servery společnosti (uložení veškerých dat – databáze, zálohy, atd.)
- Know-how společnosti
- ERP systém
- Administrativní, výrobní a další prostory
- Výrobní technologie

Seřazení aktiv dle jejich hodnoty pro společnost a odůvodnění

- *Know-how*

  Tento termín popisuje technologické a informační znalosti, poznatky a zkušenosti důležité pro určitou činnost, zejména výrobu, ale i jiné činnosti. Týká se v tomto případě především výroby produktů, které nepodléhají patentům a licencím, ale současně to znamená znalost výrobních postupů, návodů či receptur pro výrobu. Z hlediska primární podnikatelské činnosti je tato znalost tím nejdůležitějším aktivem. Je úplně jedno, zda je konkrétní

znalost uložena v paměti zaměstnance nebo nějakém informačním systému, tím její význam není nijak ovlivněn. Samozřejmě vhodnost uložení této znalosti je již otázkou jinou. Bez znalosti nelze provádět žádnou lidskou činnost a její hodnota je nevyčíslitelná.

- *Kvalifikování zaměstnanci společnosti*

  Každou společnost tvoří především její zaměstnanci a bez nich nelze provádět žádné činnosti důležité pro fungování každé společnosti. Je velmi důležité umět si své zaměstnance vybírat, ale ještě důležitější (především v dnešní době) je umění si ty kvalitní udržet. V případě odchodu zaměstnance, je nutné umět zajistit jeho rychlou náhradu a co možná s nejmenšími náklady. U některých pozic je nutné a žádoucí vyžadovat kompletní dokumentaci dané činnosti, abychom snížili riziko odchodu zaměstnance i s důležitými informacemi pro společnost nebo danou pozici. Důležitým prvkem je také zastupitelnost jednotlivých pozic, například v případě nemoci. Tím je zajištěna nejen konkrétní činnost, ale i přenesení znalostí na další osoby. V tomto směru hraje důležitou roli personální oddělení a stanovená personální bezpečnostní opatření.

- *Servery společnosti a jejich obsah*

  Jak jsem již v úvodu případové studie uvedl téměř všechny servery (kromě serveru v Polské pobočce) jsou fyzicky umístěny v sídle společnosti. Bez jejich fungování by nebylo možné využívat téměř žádné ICT prostředky (ERP systém, elektronickou poštu, dokumenty uložené na síti, CRM, MIS, mzdový a personální systém a mnohé další). Navíc je tu uloženo velké množství dat pro společnost životně důležitých včetně velké části know-how společnosti. Prostřednictvím ICT jsou také řízeny výrobní technologie, které by jinak nemohly fungovat. Data uložená v jednotlivých databázích mají pro společnost nevyčíslitelnou hodnotu. Samozřejmě i použitý HW má nezanedbatelnou hodnotu. V případě jeho poruchy však není zase tak obtížné jej vyměnit nebo opravit. Při ztrátě dat je to již složitější a pokud nemá ani potřebné zálohy, jen těžko je budu získávat zpět.

- *ERP systém*

Je pravdou, že veškerá důležitá data, která jsou ERP systémem pořizována, jsou uložena na databázovém serveru a jeho funkčnost je závislá na jeho fungování. Proč je tedy tak významným aktivem? Opačně můžeme říci, že samotná databáze je k ničemu bez aplikace, která umí s daty v databázi pracovat. Jeho význam není pouze v jeho obsahu, ale především v tom jakým způsobem a jak jsou prostřednictvím něho nastaveny a řízeny jednotlivé firemní procesy. To má velký význam a vliv na správné fungování společnosti a její růst. Jelikož je tento systém využíván převážnou většinou uživatelů (včetně obchodních zástupců, regionálních manažerů a konzultantů) k mnoha činnostem, je nemožné nebo velmi obtížné, aby bez něho uživatelé vykonávali své pracovní povinnosti. Nefunkčnost systému znamená pro společnost velké problémy a velmi těžko se vyčíslují ztráty, které byly touto nefunkčností způsobeny.

- *Administrativní, výrobní a další prostory*

Každá společnost musí mít nějaké sídlo, kde vykonává svou podnikatelskou činnost. Záleží vždy na charakteru společnosti, jak velké prostory pro svou činnost potřebuje. V této případové studii se jedná o společnost výrobní a díky jejímu zaměření jsou požadavky na prostor značné. Je nutné někde skladovat velké objemy surovin potřebných pro výrobu, polotovary a hotové výrobky. Někde musí být umístěny výrobní linky, stroje a další zařízení. Díky velikosti společnosti je také zaměstnáván poměrně velký počet zaměstnanců (cca 150), pro které je nutné zajistit prostory pro výkon jejich práce a tak dále. Jejich hodnota je poměrně snadno vyčíslitelná.

- *Výrobní technologie*

Jelikož je primární činností společnosti výroba, jsou výrobní technologie neodmyslitelnou součástí fungování společnosti. Mohou to být jednoduché stroje, ale také velmi složitá technologická zařízení, výrobní linky atd. Málo která společnost je schopna v případě výpadku nějaké výrobní technologie (např. výrobní linka), jí nahradit jinou, záložní. Proto je důležité mít zajištěn kvalitní a rychlý servis těchto zařízení. Nejlépe z řad vlastních pracovníků, kteří mají v náplni své práce údržbu a opravy těchto technologií.

7.6.2 Rozdělení IS dle bezpečnostních kritérií

Rozhodnout, která kritéria pro tuto případovou studii vybrat, nebylo zase až tak složité. Díky značnému zjednodušení jsem se rozhodl pro kritéria TCSEC, která jsou považována za základ hodnocení bezpečnosti. Navíc je bezpečnost vyjádřena pouze jednou hodnotou, což v našem případě naprosto dostačuje. V předchozích částech jsem uvedl IS, které společnost využívá a nyní je můžeme rozdělit dle bezpečnostních kritérií.

Jak bylo uvedeno v teoretické části, tak TCSEC rozděluje IS na čtyři základní skupiny A – D. Skupina C a B je pak ještě rozdělena na podtřídy C1, C2 a B1, B2, B3. Pojďme si tedy ještě jednou shrnout ty nejdůležitější IS, které společnost využívá.

Seznam využívaných IS:

- ERP systém
- CRM systém (systém pro řízení vztahů se zákazníky)
- MIS systém (manažerské reporty a plánování)
- Mzdový a personální systém
- Systém na řízení výrobních technologií (řízení výrobních linek)
- Bankovní systémy (správa bankovních účtů společnosti)
- Systém podpory uživatelů (Helpdesk)
- Síťové disky (dokumenty, uživatelská data a další soubory)

Do třídy A nespadá žádný z uvedených IS, jelikož je tato třída pro většinu systémů nedosažitelná. Takže nám zbývají pro zařazení skupiny B, C a D respektive C1, C2 a B1, B2, B3 a D. Pro jednoduchost ještě třídu B uvedeme souhrnně

Zařazení do skupin a stručné odůvodnění:

- D
    - Systém podpory uživatelů (Helpdesk) – jednoduchá systém bez nutnosti většího zabezpečení, není protokolován
    - Systém na řízení výrobních technologií (řízení výrobních linek) – systém není protokolován

- CRM systém (systém pro řízení vztahů se zákazníky) – systém není protokolován
- MIS systém (manažerské reporty a plánování) – systém není protokolován
- Mzdový a personální systém – systém není protokolován
- ERP systém – činnosti v systému nejsou protokolovány, jinak by mohl být zařazen do kategorie C1.

- C1
  - Síťové disky (dokumenty, uživatelská data a další soubory) – činnosti jsou protokolovány a uživatelé mají své projekty a informace chráněny proti neoprávněnému čtení nebo zničení svých dat.
- B
  - Bankovní systémy – u bankovních systémů jsou požadavky na bezpečnost, díky zaměření, velmi vysoké.

Jak je vidět, tak většina systémů je zařazena do skupiny D. Zpravidla je to díky tomu, že systémy nemají záznamy o provedených změnách a činnostech uživatelů v systému. V ostatních případech zpravidla splňují základní požadavky vyšších tříd, respektive třídy C1 nebo C2 (například povinnost uživatelské identifikace a autentizace). U ERP nebylo zařazení tak jednoznačné, ale díky pouze částečnému protokolování jsem jej zařadil také do skupiny D.

7.7 Identifikace hrozeb a zranitelností, vyhodnocení rizik

Opět zde budu brát odděleně vnější a vnitřní prostředí a vyberu ty nejdůležitější hrozby, zranitelnosti a rizika vzhledem k nejdůležitějším aktivům.

7.7.1 Vyhodnocení rizik - vnější prostředí

Jak bylo již uvedeno, tak mimo firmu jsou využívána některá aktiva, která vlastní zejména obchodní zástupci, regionální manažeři a konzultanti. Byl to osobní automobil, notebook a telefon. U osobního automobilu hrozí jeho zničení vinou dopravní nehody nebo jeho odcizení. Proti těmto hrozbám jsou osobní automobily pojištěny. Také jejich uživatelé

musí mít pojištění v případě způsobení škody a jsou pravidelně proškolování. Já se chci ale zaměřit na osobní notebook. Zde jsou rizika podobná. Může dojít k odcizení, zničení nebo zneužití dat, informací, které jsou na něm uložena. Především je důležitá ochrana při odcizení, jelikož notebooky těchto pracovníků obsahují kompletní databáze zákazníků společnosti včetně jejich kontaktů a dalších údajů. V současné době jsou tyto data chráněna pouze přihlášením k OS a následně přihlášením do ERP. Pokud není disk žádným způsobem chráněn, není velkým problémem vykopírovat databázi ERP a další data na počítači uložená. Navíc díky možnosti změny hesla (u ERP) si uživatelé často volí slabá hesla, která jsou jednoduše odhadnutelná. V tom horším případě mají svá hesla nalepená přímo na notebooku nebo poznačené a uložená v tašce od notebooku. U regionálních manažerů, konzultantů je toto riziko několikanásobně větší, jelikož mají přístup do firemní sítě díky VPN spojení. Ostatně tyto tendence potvrdil i průzkum a osobně jsem se s tímto setkal. Pokud takovýto notebook někdo odcizí, je velmi jednoduché zneužít všechny informace na něm uložené. Situace u CRM systému není lepší. Jelikož se pro přístup využívá webový prohlížeč, uživatelé často využívají možnosti prohlížečů a uživatelské jméno a heslo si uloží, takže systém je bez ochrany.

Dalšími uživateli firemních IS či ICT jsou pracovníci, kteří nepravidelně přistupují z domova nebo externí spolupracovníci. Zde mohou být dva způsoby připojení. První pomocí VPN a druhé pomocí RDP. U obou případů hrozí riziko, že bude zadávané heslo prozrazeno a díky výsledkům průzkumu je toto riziko vysoké.

7.7.2 Vyhodnocení rizik - vnitřní prostředí

Opět zde budu opakovat, že největším bezpečnostním rizikem jsou vlastní zaměstnanci. Rizika jsou zde podobná jako u zaměstnanců pracujících mimo sídlo společnosti. Díky více využívaným IS, nutnosti si zapamatovat více přístupových údajů, možnosti si hesla (v některých případech) měnit vzrůstá opět riziko jejich prozrazení. Není nutné opakovat výsledky průzkumu. Velkým rizikem je také chování jednotlivých uživatelů, kteří nechají počítač s OS, kde jsou přihlášení, bez dozoru v nezabezpečené kanceláři. A ještě hůře klidně nechají otevřené aplikace, v kterých jsou přihlášeni. S tím se bohužel setkávám dnes a denně. Pokud bychom analyzovali fyzické zabezpečení vnějšího a vnitřního perimetru, zjistili bychom, že v tomto případě je to opravdu závažný problém, ale to je jiná problematika.

Dalším rizikem je problém s logováním změn, které byly uživateli v jednotlivých IS provedeny. Téměř žádná využívaná aplikace není v současné době schopna sledovat činnost uživatelů a také ji ukládat. Pokud tak nastane nějaký problém, není možné dohledat viníka. I přes to, že mají některé systémy (zejména ERP) propracovanou a velmi podrobnou definici uživatelských oprávnění, stačí to maximálně na snížení okruhu podezřelých.

Jednotlivé stolní počítače a notebooky nemají žádným způsobem zabezpečeny USB porty a vypalovací mechaniky. Díky čemuže není problém k USB portu připojit jakékoliv přenosné paměťové médium nebo vypálit citlivé informace na CD nebo DVD a vynést z firmy. U notebooků je situace horší díky tomu, že si je uživatelé nosí mimo společnost a mohou tak citlivé informace přenášet přímo v notebooku.

Uchovávání elektronických certifikátu, jak ukázal průzkum, je také velký problém. Uložení na pevném disku počítače nebo na jiném externím paměťovém médiu je využíváno také i v této společnosti. Externí paměťová média jsou v tomto případě ještě více nebezpečná, jelikož zde hrozí riziko jejich ztráty nebo odcizení. Zkopírovat pak takový certifikát z těchto médií zvládne i méně zkušený uživatel.

Elektronická pošta může být dalším zdrojem úniku citlivých informací a není snadné se proti takovýmto způsobům bránit. Jelikož má každý uživatel k dispozici internet, bez jakéhokoliv monitorování. Takže se může klidně přihlásit ke svému soukromému e-mailu a odeslat citlivá data prostřednictvím svého účtu nebo je uložit na kterékoliv internetové datové uložiště. Díky volnému přístupu k internetu je také vyšší riziko infekce viry, červi a dalším škodlivým kódem.

Jistě můžeme najít i další rizika, hrozby a zranitelnosti. Ty nejdůležitější jsem zde však uvedl, což v našem případě dostačuje.

7.8 Navrhované změny, opatření a doporučení

Možností jak řešit výše uvedená rizika, hrozby a zranitelnosti je celá řada a je na konkrétních požadavcích a finančních možnostech každé společnosti, které si zvolí. Já se zde pokusím navrhnout taková řešení, které dle mého názoru budou pro danou společnost vhodnou kombinací poměru bezpečnost/cena.

7.8.1 Ochrana notebooků proti odcizení nebo zneužití

Jak externí, tak interní zaměstnanci ve velké míře využívají přenosné počítače. Jako základní ochrana proti odcizení nebo zneužití jsou fyzická bezpečnostní opatření. To znamená, že není možné notebook nechat v osobním autě (obchodní zástupci, regionální manažeři, konzultanti) nebo jinak bez dozoru mimo společnost. Také je důležité stanovit pravidla jak se k danému zařízení chovat, aby se snížilo riziko jeho poruchy nebo zničení. Je tedy nutné stanovit základní pravidla nakládání s těmito prostředky (směrnice, bezpečnostní politika) a zaměstnance pravidelně s těmito pravidly seznamovat.

Dalším vhodným zabezpečením, zejména proti krádeži, je využití programů pro šifrování pevného disku, kdy je chráněna celá partition nebo pevný disk. Většinou je využíváno silného symetrického algoritmu (nejčastěji 256bitový). Aby bylo šifrování účinné a zašifrovali se i soubory OS je použita tzv. pre-boot autentizace. Master Boot Record disku je změněn a před spuštěním OS je uživatel vyzván k zadání přihlašovacích údajů. Po správném zadání jména a hesla, případně certifikátů se z těchto údajů vygeneruje klíč pro dešifrování hlavního šifrovacího klíče k disku. Pak je možné využívat OS, aplikační programy a soubory.

7.8.2 USB porty, vypalovací mechaniky

Tam kde to není nezbytně nutné je vhodné USB porty deaktivovat. To samé platí u vypalovacích mechanik, kde nejsou nutné, instalovat pouze standardní mechaniky pro čtení. Další možností, pokud je nutné přenosná paměťová média využívat, je vynucení používání pouze zašifrovaných médií. Tím je zajištěn bezproblémový přenos mezi zakódovanými stanicemi. Použití mimo firmu, třeba doma, však již možné není.

7.8.3 Elektronické certifikáty, elektronické podpisy

V tomto případě je žádoucí mít veškeré certifikáty uložené na bezpečném uložišti, což pevný disk nebo flash paměť není. V tomto případě je vhodné používat USB Tokeny nebo čipové karty. Pokud je uživatel ztratí, tak bez znalosti PIN kódu není možné klíče použit.

7.8.4 Využívání systémů přístupných přes webové prohlížeče

V těchto případech je nutné zajistit správnou konfiguraci prohlížeče, aby nebylo možné ukládání přihlašovacích údajů (CRM, MIS, Helpdesk). Kromě toho je možné provést celou řadu dalších nastavení, které zvýší jeho bezpečnost.

7.8.5 Využívání internetu a elektronické pošty

Jak bylo zmíněno, tak neexistuje žádná kontrola přístupu uživatelů na internet. V tomto případě existuje celá řada nástrojů s různými možnostmi a funkcemi. V žádném případě zde nejde o to, aby byli uživatelé sledování, zda místo práce nejsou na internetu. Jde o blokování potencionálně nebezpečných stránek a obsahu. Tím je do značné míry eliminováno riziko infekce viry a dalším škodlivým kódem. Je také možné sledování stahování a odesílání dat jednotlivými uživateli a v případě podezřelých datových toků je možné zakročit.

U elektronické pošty je vše závislé na správné konfiguraci, kterou zajistí správci a administrátoři (například omezení přijímání a odesílání určitých typů souborů, velikost souboru a další). Opět je zde nutné zajistit správnou konfiguraci webového prohlížeče, jelikož je pošta přístupná i tímto způsobem. Je také nutné upozornit uživatele aby poštovním klientu neuchovávaly žádné přijaté nebo odeslané údaje typu přístupových údajů a dalších citlivých informací. Firemní pošta by také měla být využívána výhradně k firemním účelům.

7.8.6 Využívání VPN

VPN smějí pouze schválení zaměstnanci, kterým bylo přiděleno uživatelské jméno a heslo + nainstalován VPN klient. VPN klient by neměl být instalován na jiný HW než ve vlastnictví společnosti. Pokud to však není možné, je nutné, aby byl počítač nakonfigurován dle pravidel, která jsou společností dána při využívání VPN připojení. V tu chvíli se musí uživatel chovat dle pravidel, která jsou ve firemní síti stanovena. Uživatel využívající VPN připojení je povinen zajistit, že nebude umožněno využívat tento způsob připojení neoprávněnou osobou (kolega, rodinní příslušníci a další). Na každém počítači s VPN klientem musí být funkční antivirový program, který je pravidelně aktualizovaný. Je také vhodné nakonfigurovat automatické odpojení VPN spojení po určité době nečinnosti (nastaví správci či administrátoři).

7.8.7 RDP (Remote Desktop Protocol)

Pokud uživatelé přistupují pomocí vzdálené plochy k firemnímu serveru, je využíván doménový účet, ověření Active Directory. Je nutné dodržovat základní zásady používání identifikačních údajů (uživatelské jméno a heslo). Tento přístup je využíván výhradně pro přístup k ERP systému a proto je nutné, aby nebylo možné prostřednictvím tohoto připojení přistupovat k dalším zdrojům. Vhodnou konfiguraci zajistí opět správci a administrátoři.

7.8.8 Protokolování činností v IS

Jak jsem již zmínil, tak žádný z využívaných systémů nemá implementováno monitorování a protokolování činností, které jsou v nich prováděny uživateli. V případě ERP je sice částečně tato funkce implementována, nicméně bude nutné ji plně integrovat do celého systému. Bez toho nebude nikdy možné dohledat viníka bezpečnostních incidentů a vzniku chyb. U ostatních systémů, díky menšímu počtu uživatelů, lze tuto funkci postrádat.

7.8.9 Využití bezpečnostních mechanismů

Prvním pravidlem by mělo být využívání silných hesel. Pokud je schopen si uživatel heslo měnit sám je nutné, aby ho systém donutil si silné heslo nadefinovat. To však valná většina využívaných systémů neumožňuje a bylo by nutné tuto vlastnost doplnit. U OS je toto již využíváno a u ERP systému by toto neměl být problém, díky tomu, že je systém vyvíjen samotnou společností. Pokud však uživatel využívá při své práci více hesel, je toto kontraproduktivní a nutí to uživatele si hesla poznamenávat nebo využívat všude stejná. V tomto případě by bylo vhodné využívat pro přístup k OS a ERP přístup pomocí biometrie (snímání otisků prstů) nebo její kombinace s heslem. Druhou variantou, kterou považuji za výrazně efektivnější je využití multitechnologických karet nebo alespoň čipových karet, které mají široké možnosti využití. Mohou sloužit pro přístup do budovy jako docházkový a přístupový systém. Současně mohou být použity jako logický vstup do počítače nebo IS, pro použití kopírky, a v mnoha dalších aplikacích. Pokud jsou jednotlivé funkce těchto karet svázány a uživatel odchází na oběd, nemůže se stát, že kartu zapomene a neodhlásí se. Důvodem může být třeba nutnost použít kartu pro přístup do prostor jídelny nebo je nutná pro výdej obědů, atd. Případně se v těchto případech opět mohou kombinovat se znalostními bezpečnostními mechanismy.

Ostatní IS jsou již využívány menší skupinou lidí a je možné pohlídat správné nakládání se znalostními bezpečnostními mechanismy a používání silných hesel. Proto je dobré každého zaměstnance pravidelně školit a seznamovat se základními pravidly používání bezpečnostních mechanismů.

7.8.10 Ochrana stolních počítačů

Řada, výše zmíněných doporučení, navrhovaných změn a opatření, přispívá ke zvýšení bezpečnosti využívání stolních počítačů. Jak jsem již v předchozím bodě navrhl, bylo by vhodné přístup do OS stolního počítače zajistit jiným způsobem, jelikož klasické znalostní bezpečnostní mechanismy nejsou dostatečně bezpečné. To může zajistit výše zmíněné použití biometrie nebo multitechnologických, případně čipových karet. V každém případě je nutné v případě opuštění počítače, provést jeho zabezpečení. To lze udělat buď odhlášením, zamknutím OS nebo jeho vypnutím. V každém případě se tak v současné době neděje, ať už je využíván jakýkoliv způsob bezpečnostního mechanismu.

ZÁVĚR

Není třeba zdůrazňovat význam a důležitost ochrany aktiv, ať už je vlastní obyčejný člověk nebo společnost. V obou případech může jejich ztráta nebo poškození způsobit potíže, kterým je potřeba předcházet. Právě prevence a využívání vhodných prostředků k jejich ochraně je základním klíčem k úspěchu. Já jsem se v této práci zaměřil na ochranu aktiv ve formě informací, které jsou uchovávány a zpracovávány v různých informačních systémech podporujících procesy související s podnikatelskou činností každé organizace.

Diplomová práce, kterou jsem zpracoval a nazval Analýza bezpečnosti přístupů k informačním systémům, si v úvodu stanovila několik cílů. Jsem přesvědčen, že jsem ve své práci tyto cíle naplnil a zmapoval tak současné způsoby využití bezpečnostních mechanismů, jejich druhy, chování uživatelů při jejich využívání a nejčastější příčiny vzniku bezpečnostních incidentů. Věřím také, že přečtení této práce pomůže i laikovi pochopit důležitost a význam ochrany IS každé společnosti. Teoretická část byla zpracovávána za pomoci mnoha informačních zdrojů a kromě teoretických poznatků jsem se snažil vnést do této části i své praktické zkušenosti, získané během mé praxe. Myslím, že se mi povedlo stručně a přehledně obsáhnout ty nejdůležitější a nejpodstatnější informace z dané oblasti, důležité pro pochopení této rozsáhlé problematiky.

Jak jsem již několikrát v této práci zmiňoval, je velmi důležité, aby každá organizace kladla velký důraz na zpracování komplexní bezpečnostní politiky. Prováděla její pravidelnou aktualizaci a kontrolu, seznamovala pravidelně své zaměstnance se změnami a důležitými aspekty jejího využívání a především vyžadovala její bezpodmínečné dodržování. Nemyslím, že na základě této práce lze zpracovat kompletní bezpečnostní politiku organizace, ostatně to ani nebylo mým cílem. Každá společnost má svá specifika a není možné zpracovat nějaký univerzální návod. Rozhodně jsem také nemohl, při daném rozsahu práce, obsáhnout všechny aspekty bezpečnostní politiky společnosti. Zato jsem přesvědčen, že tato práce může být významným pomocníkem při její tvorbě nebo aktualizacích.

Na závěr bych si dovolil zopakovat jednu velmi důležitou větu, kterou jsem použil v závěru teoretické části a tou bych rád tuto práci zakončil. ***Systém je tak bezpečný, jak bezpečný je jeho nejslabší článek.***

ZÁVĚR V ANGLIČTINĚ

There's no need to accentuate value and importance of protection of assets, no matter if owned personally or by a company. In either case loss or damage of assets can cause serious problems, which is better to prevent. Prevention and use of right resources for protection is the basic key to success. I have focused on protection of assets in form of information being stored and processed in various information systems supporting key processes of enterprise activities of each company. Diploma thesis I've elaborated and called Security Analysis Of Secure Access To Information Systems has set several goals. I am convinced, that I've fulfilled these goals in this thesis and so that I've mapped nowadays ways of use of security mechanisms, their kinds, users behavior in their usage and the most frequent reasons of security incidents.

I believe the reading of this thesis can help to understand importance and value of information systems' protection even to non-experts. Theoretical part was elaborated with help of information research and with my personal experience and knowledge. I do think I've comprised most important and most essential information necessary for understanding this extensive problematic in a brief and well arranged way.

As I've mentioned before in this thesis, it's very important for each company to insist on complex security policy, to perform its regular revision and updates, to educate employees with policy changes and important aspects of policy use and especially to require its necessarily keeping.

I don't think it's possible to prepare a complex company security policy based on this thesis, but it was not the goal. Each company is very specific and it's not possible to prepare some common directions. Also I was not able to include all aspects of company security policy in given size of this thesis. I'm convinced that this thesis could be considered as practical guide for creating or updating the security policy.

In conclusion I'd like to repeat one very important sentence, which is already used in resume of theoretical part and to end up with it: **Each system is as secure as its weakest part.**

SEZNAM POUŽITÉ LITERATURY

Monografie:

[1] SODOMKA, Petr. *Informační systémy v podnikové praxi*. 1. vyd. Brno : Computer Press a. s., 2006. 351 s. ISBN 80-251-1200-4.

[2] VRANA, Ivan, RICHTA, Karel. *Zásady a postupy zavádění podnikových informačních systémů : praktická příručka pro podnikové manažery*. 1. vyd. Praha : Grada Publishing, a.s., 2005. 187 s. Management v informační společnosti. ISBN 80-247-1103-6.

[3] ČERMÁK, Miroslav. *Řízení informačních rizik v praxi*. 1. vyd. Brno : Tribun EU s.r.o., 2009. 134 s. ISBN 978-80-7399-731-1.

[4] RAK , Roman, MATYÁŠ, Václav, ŘÍHA, *Biometrie a identita člověka ve forenzních a komerčních aplikacích*. 1. vyd. Praha : Grada Publishing, a.s., 2008. 664 s. ISBN 978-80-247-2365-5.

[5] BASL, Josef, BLAŽÍČEK, *Roman. Podnikové informační systémy : Podnik v informační společnosti* – 2. výrazně přepracované a rozšířené vydání. 2008. vyd. Praha : Grada Publishing, a.s., 2008. 288 s. ISBN 978-80-247-2279-5.

[6] VYMĚTAL, Dominik. *Informační systémy v podnicích : teorie a praxe projektování*. 1. vyd. [s.l.] : Grada Publishing, a.s., 2009. 144 s. ISBN 978-80-247-3046-2.

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

[8] HANÁČEK, Petr, STAUDEK, Jan. *Bezpečnost informačních systémů : Metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií*. Praha : Úřad pro státní informační systém, 2000. 127 s. Dostupný z WWW: http://www.micr.cz/files/479/uvis-Bezpecnost-20000701.pdf.

[9] *Kritéria hodnocení zabezpečených počítačových systémů : Trusted Computer System Evaluation Criteria*. Přeložil Bohumil Hospodka, ing. Vladimír Karas. 1983. vyd. Praha : BEN - Technická literatura, 1994. 128 s.

Normy:

[10] ČSN ISO/IEC 27002:2006, *Informační technologie – Soubor postupů pro management bezpečnosti informací*.

[11] ISO/IEC 27006: 2007 – *Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systém.*

[12] ISO/IEC 27004, *Information technology – Security techniques – Information security management measurements.*

[13] ISO/IEC 27005: 2008 – *Information technology – Security techniques – Information security risk management.*

Internetové zdroje:

[14] *Národní bezpečnostní úřad* [online]. 2010 [cit. 2010-01-31]. Dostupný z WWW: <http://www.nbu.cz/cs/>

[15] *Microsoft security* [online]. 2010 [cit. 2010-01-31]. Dostupný z WWW: <http://www.microsoft.com/cze/security/default.mspx>

[16] *International Biometric Group* [online]. 2008 [cit. 2008-10-31]. Dostupný z WWW: <http://www.biometricgroup.com/reports/public/market_report.php>

Seriálová literatura

[17] HASKIN, Jim, RADECKÝ, Alexandr. *10 mýtů o ochraně dat*. Business World. 1.6.2008, 2008, 6, s. 10-11.

[18] BERÁNEK, Ladislav. *Bezpečnostní metriky pro systémy správy identit*. Business World. 1.6.2008, 2008, 6, s. 18-19.

[19] BLÁHA, Ondřej. *Identity management : Řešení pro centrální správu uživatelských účtů*. Security World. 5.12.2008, 2008, 4, s. 2-8.

[20] KERST, Udo. *Vzdálený přístup k síti bez kompromisů*. Security World. 5.12.2008, 2008, 4, s. 32-35.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AFIS	Automated Fingerprint Identification System
CC	Common Criteria
CISO	Chief information security officer
CRM	Customer relationship management
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
ČSN	Česká technická norma
DAC	Discretionary Access Controls
EN	Evropská norma
ERP	Enterprise Resource Planning
FC	Federal Criteria
FTP	File Transfer Protocol
GPS	Global Positioning System
GSM	Global Systém for Mobile Communication
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ICT	Information and Communication Technologies
IS	Informační systém.
ISMS	Information Security Management Systém
ISO	International Organization for Standardization
IT	Informační technologie.
ITIL	IT Infrastructure Library
ITSEC	IT Security Evaluation Criteria
MAC	Mandatory Access Controls
OS	Operační systém

OSI	Open Systems Interconnection
PDA	Personal Digital Assistant
PDCA	Plan – Do - Check – Act
PIN	Personal Identification Number.
RDP	Remote Desktop Protocol
RFC	Request for Comments
RFID	Radio Frequency Identification
SIM	Subscriber Identity Module
SMB	Small and Medium Business
TCSEC	Trusted Computer System Evaluation Criteria
ÚNMZ	Úřad pro technickou normalizaci, metrologii a státní zkušebnictví
UPS	Uninterruptible power source
USB	Universal Serial Bus

SEZNAM OBRÁZKŮ

Obr. 1 Proces řízení rizik [3] 21
Obr. 2 Struktura norem [7] 26
Obr. 3 IT – soubor postupů pro management bezpečnosti informací [10] 27
Obr. 4 Přehled vývoje bezpečnostních kritérií 32
Obr. 5 Struktura respondentů dle počtu zaměstnanců 60
Obr. 6 Struktura respondentů dle odvětví a zaměření 60
Obr. 7 Nejčastější bezpečnostní incidenty z hlediska druhu 61
Obr. 8 Nejčastější příčiny bezpečnostních incidentů 65
Obr. 9 Využívání bezpečnostních mechanismů podle přístupu v roce 2008 a 2010 67
Obr. 10 Využívání biometrie podle použité metody 68
Obr. 11 Celosvětové využití biometrických technologií 2009 [16] 69
Obr. 12 Využití identifikačních mechanismů založených na vlastnictví 70
Obr. 13 Uchování elektronického podpisu a elektronických certifikátů 71
Obr. 14 Formy předávání znalostních bezpečnostních mechanismů jejich uživatelům 72
Obr. 15 Počet využívaných bezpečnostních mechanismů běžnými uživateli 75
Obr. 16 Síla používaných znalostních bezpečnostních mechanismů 76

SEZNAM TABULEK

Tab. 1 Obsah bezpečnostní politiky firmy [7] 17
Tab. 2 Srovnání hodnotících kritérií bezpečnosti 41
Tab. 3 Implementace bezpečnostních služeb a přiřazení bezpečnostních mechanismů 57

SEZNAM PŘÍLOH

P I Motivační dopis k dotazníkům.

P II Dotazník IT pracovníci.

P III Dotazník běžní uživatelé.

P IV Diplomová práce v elektronické podobě na CD

PŘÍLOHA P I: MOTIVAČNÍ DOPIS K DOTAZNÍKŮM

Bc. Michal Moravec

Lhotka 45

564 01 Žamberk

Dobrý den.

Jmenuji se Michal Moravec a studuji druhým rokem obor „Bezpečnostní technologie, systémy a management“ na Univerzitě Tomáše Bati ve Zlíně. Ve své diplomové práci zpracovávám průzkum využívání bezpečnostních mechanismů pro přístup k informačním systémům. Rád bych Vás touto cestou požádal o vyplnění krátkého dotazníku, který mapuje aktuální stav bezpečnosti přístupů k informačním systémům. Výsledky a závěry z tohoto průzkumu Vám v případě zájmu rád zašlu. Věřím, že pro Vás budou velmi zajímavé a pomohou Vám při zabezpečení Vašich aktiv.

Zdůrazňuji, že tento dotazník je naprosto anonymní a informace nebudou použity k jinému účelu než k tomuto výzkumu a nebudou jakýmkoliv způsobem zneužity.

Předem děkuji za vyplnění dotazníku a Váš zájem.

S pozdravem

Michal Moravec

V Žamberku 10.2. 2010

PŘÍLOHA P I: DOTAZNÍK IT PRACOVNÍCI

A. Nejčastější bezpečnostní incidenty

Z níže uvedeného seznamu vyberte bezpečnostní incidenty, které byly ve vaší společnosti za poslední rok zaznamenány a přiřaďte procentuální hodnoty, dle jejich četnosti vzniku ve vaší společnosti (max. do 100% celkem).

1. Finanční podvody (zneužití kreditní karty, atd.).
   ☐ _____
2. Krádeže informací, záznamů o zákaznících nebo finančních záznamů.
   ☐ _____
3. Krádeže duševního vlastnictví.
   ☐ _____
4. Phishing (někdo se vydával za vašeho zaměstnance nebo za společnost ve snaze získat údaje o zákaznících či zaměstnancích).
   ☐ _____
5. Záměrné odhalení citlivých a privátních informací .
   ☐ _____
6. Neautorizovaný přístup, použití informací, systémů a sítí .
   ☐ _____
7. Krádeže identifikačních informací.
   ☐ _____
8. Neúmyslné odhalení citlivých a privátních informací.
   ☐ _____
9. Úmyslné narušení, vymazání nebo zničení informací, IS či sítí.
   ☐ _____
10. Viry, červy a jiný škodlivý software .
    ☐ _____
11. Ostatní
    ☐ _____

B. Nejčastější příčiny bezpečnostních incidentů

Z níže uvedeného seznamu vyberte nejčastější příčiny vzniku bezpečnostních incidentů a přiřaďte procentuální hodnoty dle nejčastější příčiny jejich vzniku (max. do 100% celkem).

1. Nedostatek kvalifikovaných zaměstnanců.
   ☐
2. Nedostatečná podpora managementu.
   ☐
3. Nedostatečné technické vybavení, technologie.
   ☐
4. Vlastní zaměstnanci.
   ☐
5. Internet / elektronická pošta.
   ☐
6. Provozované aplikace.
   ☐
7. Dodavatelé IT.
   ☐
8. Špatně zpracovaná / neaktualizovaná bezpečnostní politika.
   ☐
9. Nedostatečné finanční prostředky.
   ☐
10. Vnější útočníci.
    ☐
11. Žádná z uvedených příčin.
    ☐

C. Využívané bezpečnostní mechanismy

Z níže uvedeného seznamu vyberte bezpečnostní mechanismy, které využíváte a přiřaďte procentuální hodnoty dle jejich využívání (max. do 100%).

1. Znalostní bezpečnostní mechanismy (hesla)

   ☐

2. Bezpečnostní mechanismy založené na vlastnictví (čipové karty, digitální podpis,…)

   ☐

3. Biometrie (snímání otisků prstů, snímání geometrie ruky,…)

   ☐

4. Kombinace znalostních bezpečnostních mechanismů (hesla) a biometrie

   ☐

5. Kombinace znalostních bezpečnostních mechanismů a mechanismů založených na vlastnictví

   ☐

D. Využívání biometrie dle technologií

V případě, že využíváte nějaké technologie založené na biometrické identifikaci, napište které (snímání otisků prstů, snímání geometrie ruky, topografie žil,…)

E. Využívání bezpečnostních mechanismů založených na vlastnictví

V případě, že využíváte bezpečnostní mechanismy založené na vlastnictví, napište které (USB tokeny, čipy a čipové karty, hardwarové klíče, elektronický podpis,…)

F. Uložení elektronického podpisu a el. certifikátů

Z níže uvedeného seznamu vyberte způsoby uložení elektronického podpisu a elektronických certifikátů, ve vaší společnosti (1..n).

1. ☐ Pevný disk
2. ☐ Flash disk
3. ☐ USB Token
4. ☐ Čipová karta
5. ☐ Jiné paměťové médium

G. Způsob využívání znalostních bezpečnostních mechanismů (hesel)

Odpovězte na níže uvedené otázky nebo rozdělte příslušné procentuální hodnoty.

Jakým způsobem generujete hesla?

1. ☐ Ručně
2. ☐ Generátory hesel
3. ☐ Uživatelé si vytváří vlastní

Vytváříte takzvaná silná hesla, v případě jejich vytváření?

1. ☐ ANO
2. ☐ NE

Jaký způsobem hesla uživatelům předáváte, v případě jejich vytváření?

1. ☐ V zapečetěné obálce nebo podobnou formou
2. ☐ Telefonicky
3. ☐ Poznačené na papír
4. ☐ Osobně ústní formou
5. ☐ Elektronickou poštou

Mohou si uživatelé svá hesla měnit?

1. ☐ ANO
2. ☐ NE

Je ve vaší společnosti vyžadována změna hesla za určité období?

1. ☐ ANO, jak často _____
2. ☐ NE

Uchováváte si hesla, která generujete?

1. ☐ ANO, jakým způsobem _____
2. ☐ NE

Vyžadovali jste někdy, v případě řešení nějakého problému, vyzrazení hesla uživatelem

1. ☐ ANO
2. ☐ NE

PŘÍLOHA P I: DOTAZNÍK BĚŽNÍ UŽIVATELÉ

Využívání znalostních bezpečnostních mechanismů uživateli

Odpovězte prosím na následující otázky

Kolik hesel využíváte při své práci?

1. ☐ 1
2. ☐ 2 až 3
3. ☐ 3 a více

Jak často si hesla měníte nebo jsou Vám měněna?

1. ☐ Nikdy
2. ☐ 1 až 2x ročně
3. ☐ Častěji

Zná nějaké Vaše heslo Váš kolega nebo správce?

1. ☐ ANO
2. ☐ NE

Jaká hesla využíváte?

1. ☐ Silná hesla (kombinace písmen, číslic, popřípadě znaků, min. délky 6 znaků)
2. ☐ Hesla typu 1234
3. ☐ Použití údajů z běžného života (jména, přezdívky, data narození,…)

Máte svá hesla někde poznačená, volně dostupná?

1. ☐ ANO, mám je volně na svém pracovním stole
2. ☐ ANO, ale mám je uschované na svém pracovním místě
3. ☐ ANO, ale jedná se o bezpečné uložení (trezor,…)
4. ☐ Ne, hesla si pamatuji

Pokud opustíte pracoviště na kratší dobu - provedete odhlášení z aplikačních programů, případně uzamknete OS?

1. ☐ ANO
2. ☐ NE

Pokud opustíte pracoviště na delší dobu - provedete odhlášení z aplikačních programů, případně zamknete OS nebo vypnete počítač?

1. ☐ ANO
2. ☐ NE