

Návrh implementace bezpečnostní politiky v informačním a komunikačním systému vybrané firmy

Bc. Jan Kolář



ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: Bc. Jan KOLÁŘ
Osobní číslo: A14501
Studijní program: N3902 Inženýrská informatika
Studijní obor: Bezpečnostní technologie, systémy a management
Forma studia: kombinovaná

Téma práce: Návrh implementace bezpečnostní politiky v informačním a komunikačním systému vybrané firmy

Téma anglicky: Design Implementation Security Policy in the Information and Communication System.

Zásady pro vypracování:

1. Formou literární rešerše popište současný stav předmětné problematiky a úroveň jeho řešení v informačních zdrojích.
2. Vytvořte model informačního a komunikačního systému pro subjekt v bankovní sféře.
3. Popište zásady tvorby bezpečnostní politiky informačního a komunikačního systému z hlediska komplexního způsobu zabezpečení – systémové, fyzické, personální, atd.
4. Analyzujte bezpečnostní rizika pro vnější a vnitřní prostředí a na základě této analýzy navrhnete implementaci bezpečnostní politiky.
5. Zpracujte metodiku analýzy rizik pro využití v obdobných institucích.

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: tištěná/elektronická

Seznam odborné literatury:

1. BÍLA, Jiří. HLAVÁČ, Vladimír a KRÁL, František. Informační technologie: databázové a znalostní systémy. Vyd. 2., přeprac. Praha: Vydavatelství ČVUT, 126 s. ISBN 8001027902.
2. JAŠEK, Roman. Informační a datová bezpečnost. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006, 140 s. ISBN 80-7318-456-7.
3. GÁLA, Libor. POUR, Ján a ŠEDIVÁ, Zuzana. Podniková informatika. 2 vyd. Praha: Grada Publishing, a.s., 2009, 496 s. ISBN 978-80-247-2615-1.
4. VALOUCH, Jan. Projektování integrovaných systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 152 s. ISBN 978-80-7454-296-1. Dostupné z: <https://dspace.k.utb.cz/handle/10563/25814>.
5. POŽÁR, Josef. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005, 309 s. ISBN 80-8689-838-5.
6. LUDVÍK, Miroslav. Teorie bezpečnosti počítačových sítí, Praha: Computer Media, 2008, 98 s. ISBN 80-86686-35-3.

Vedoucí diplomové práce:

doc. Ing. Jiří Gajdošík, CSc.

Ústav bezpečnostního inženýrství

Datum zadání diplomové práce:

5. února 2016

Termín odevzdání diplomové práce:

16. května 2016

Ve Zlíně dne 5. února 2016



doc. Mgr. Milan Adámek, Ph.D.
děkan



doc. RNDr. Vojtěch Kresálek, CSc.
ředitel ústavu

Jméno, příjmení: Jan Kolář

Název bakalářské/diplomové práce: Návrh implementace bezpečnostní politiky v informačním a komunikačním systému vybrané firmy

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 přípouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- 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/bakalářské 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, dne

.....
podpis diplomanta

ABSTRAKT

Diplomová práce se věnuje problematice bezpečnostní politiky v informačním a komunikačním systému organizace. V teoretické části se věnuje zásadám tvorby bezpečnostní politiky v organizacích a komplexnímu přístupu k otázkám bezpečnosti informačních systémů. Je popsána základní struktura řady norem ISO/IEC 27000. Praktická část pojednává o modelu informačního systému organizace působící v bankovní sféře, analýze rizik tohoto systému. V závěru práce je zpracována zobecněná metodika analýzy rizik s možností aplikace v obdobných organizacích.

Klíčová slova: bezpečnost, bezpečnostní politika, riziko, analýza rizik, informační systém

ABSTRACT

This Master thesis deals with the problem of security policy in the information and communication system of an organization. The theoretical part is dedicated to the principles of creating a security policy in organizations and to a complex approach to security of information systems. It also describes the basic structure of standard series ISO / IEC 27000. The practical part deals with the model of information system in an organization operating in the banking sector and its risk analysis. The last part of this thesis describes a general methodology of a risk analysis for use in similar organizations.

Keywords: safety, security policy, risk, risk analysis, information system

Poděkování

Tímto děkuji vedoucí mé práce doc. Ing. Jiřímu Gajdošíkovi za odborné vedení, cenné rady, věcné připomínky, vstřícnost při konzultacích a vypracování diplomové práce. Dále chci poděkovat mé rodině, přítelkyni a přátelům za pozitivní přístup a podporu během celého studia.

Motto:

„Považuješ-li něco za nemožné, snaž se jednu možnost najít.“ [1]

Bruce Lee

OBSAH

ÚVOD.....	10
I TEORETICKÁ ČÁST.....	11
1 TERMINOLOGIE	12
2 PROBLEMATIKA A ZÁSADY TVORBY BEZPEČNOSTNÍ POLITIKY	17
2.1 CÍLE A STRATEGIE ŘEŠENÍ BEZPEČNOSTI INFORMACÍ	18
2.2 ANALÝZA RIZIK IS	18
2.3 BEZPEČNOSTNÍ POLITIKA.....	19
2.3.1 Obsah dokumentu bezpečnostní politiky	20
2.3.2 Tvorba bezpečnostní politiky	21
2.3.3 Formulace, rozsah a přijetí bezpečnostní politiky.....	21
2.4 BEZPEČNOSTNÍ STRATEGIE, PROJEKT, STANDARD.....	22
2.4.1 Bezpečnostní strategie.....	22
2.4.2 Bezpečnostní projekt	22
2.4.3 Bezpečnostní standard.....	22
2.5 IMPLEMENTACE BEZPEČNOSTI.....	23
2.6 AUDIT A MONITORING	23
2.6.1 Bezpečnostní incidenty a ponaučení	23
3 KOMPLEXNÍ ZPŮSOBY ZABEZPEČENÍ	25
3.1 PERSONÁLNÍ BEZPEČNOST	26
3.2 REŽIMOVÁ BEZPEČNOST	26
3.3 FYZICKÁ BEZPEČNOST	27
3.4 BEZPEČNOST BĚHEM KOMUNIKACE	27
3.5 BEZPEČNOST HW	27
3.6 BEZPEČNOST SW	28
3.7 ADMINISTRATIVNÍ BEZPEČNOST	28
4 ŘADA NOREM ISMS	29
4.1 OBECNĚ.....	29
4.2 NORMY POPISUJÍCÍ PŘEHLED A TERMINOLOGII	30
4.2.1 ISO/IEC 27000	30
4.3 NORMY SPECIFIKUJÍCÍ POŽADAVKY	30
4.3.1 ISO/IEC 27001	30
4.3.2 ISO/IEC27006.....	30
4.4 NORMY POPISUJÍCÍ OBECNÉ SMĚRNICE	30
4.4.1 ISO/IEC 27002.....	31
4.4.2 ISO/IEC 27005.....	31
4.5 NORMY POPISUJÍCÍ SMĚRNICE SPECIFICKÉ PRO JEDNOTLIVÁ ODVĚTVÍ.....	31
4.5.1 ISO/IEC TR 27015	32
5 POŽADAVKY DLE VYHLÁŠKY ČNB Č. 163/2014 SB	33
5.1 POŽADAVKY NA INFORMAČNÍ SYSTÉMY A TECHNOLOGIE.....	33
II PRAKTICKÁ ČÁST	36
6 POPIS ORGANIZACE.....	37

6.1	CHARAKTERISTIKA.....	37
6.2	ORGANIZAČNÍ STRUKTURA ORGANIZACE	37
7	BEZPEČNOSTNÍ SITUACE ORGANIZACE	38
7.1	ANALÝZA RIZIK INFORMAČNÍHO SYSTÉMU	38
7.1.1	Identifikace komponent (model informačního systému)	38
7.1.1.1	Analýza dopadů incidentu (BIA)	39
7.1.2	Identifikace aktiv	40
7.1.3	Hodnocení aktiv	41
7.1.4	Odhad a hodnocení hrozeb	43
7.1.4.1	Odhad frekvence hrozeb, úrovně zranitelnosti a stávající opatření	43
7.1.5	Stanovení míry rizika	46
7.2	POPIS SW NÁSTROJE ARIS.XLS	47
7.2.1	Podklady.....	47
7.2.1.1	Aktiva.....	47
7.2.1.2	Katalog hrozeb	48
7.2.1.3	Hrozby	51
7.2.1.4	Zranitelnost a protiopatření.....	53
7.2.2	Stanovení prahové hodnoty	54
7.2.3	Zpracování.....	55
7.2.4	Příprava prohlášení o aplikovatelnosti	58
8	METODIKA ANALÝZY RIZIK.....	59
8.1	ÚVODNÍ USTANOVENÍ.....	59
8.1.1	Účel	59
8.1.2	Metodika	59
8.1.3	Hranice analýzy rizik	59
8.2	PROVEDENÍ ANALÝZY RIZIK S VYUŽITÍM METODIKY ŘÍZENÍ RIZIK	60
8.2.1	Proces analýzy rizik	60
8.2.2	Vstupy do procesu AR v oblasti ISMS	60
8.2.3	Výstupy procesu AR v oblasti ISMS	60
8.2.4	Role AR v oblasti ISMS.....	60
8.3	ANALÝZA RIZIK.....	61
8.3.1	Stanovení hranic analýzy aktiv	61
8.3.2	Identifikace komponent a stanovení hranic analýzy aktiv	61
8.3.2.1	Model informačního systému – identifikace komponent	62
8.3.2.2	Analýza dopadů incidentu (Business Impact Analysis, BIA).....	63
8.3.3	Identifikace a hodnocení aktiv	63
8.3.4	Odhad hrozeb	65
8.3.5	Odhad frekvence hrozeb	66
8.3.6	Odhad zranitelnosti (dopadů).....	66
8.3.7	Odhad účinnosti protiopatření.....	67
8.3.8	Hodnocení míry rizika.....	68
8.3.9	Akceptace rizik, varianty zvládání rizik.....	69
8.3.9.1	Kritéria pro hodnocení rizik - obecná definice	69
8.3.9.2	Kritéria pro akceptaci rizik	69
8.3.9.3	Varianty pro zvládání rizik	70
8.3.10	Zpráva z analýzy rizik	70

8.4	ÚDRŽBA ANALÝZY RIZIK	70
9	NÁVRH IMPLEMENTACE BEZPEČNOSTNÍ POLITIKY	71
9.1	BEZPEČNOSTNÍ POLITIKA.....	71
9.2	ORGANIZACE BEZPEČNOSTI INFORMACÍ	71
9.3	ŘÍZENÍ AKTIV	72
9.4	BEZPEČNOST LIDSKÝCH ZDROJŮ.....	72
9.5	FYZICKÁ BEZPEČNOST A BEZPEČNOST PROSTŘEDÍ	72
9.6	ŘÍZENÍ KOMUNIKACÍ A ŘÍZENÍ PROVOZU	73
9.7	ŘÍZENÍ PŘÍSTUPU	73
9.8	AKVIZICE, VÝVOJ A ÚDRŽBA INFORMAČNÍCH SYSTÉMŮ	74
9.9	ZVLÁDÁNÍ BEZPEČNOSTNÍCH INCIDENTŮ	74
9.10	ŘÍZENÍ KONTINUITY ČINNOSTÍ ORGANIZACE.....	75
9.11	SOUŁAD S POŽADAVKY	75
	ZÁVĚR	76
	SEZNAM POUŽITÉ LITERATURY.....	77
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	79
	SEZNAM OBRÁZKŮ	81
	SEZNAM TABULEK.....	82
	SEZNAM ROVNIC	83
	SEZNAM PŘÍLOH.....	84

ÚVOD

Trendem současnosti je masivní rozvoj různých druhů informačních systémů. Není tedy vůbec pošetilé dnešní svět a společnost nazývat „informační“. Rozvoj technologií na výměnu, zpracování a uložení dat je důležitý a společně s tímto rozvojem je nutné brát ohled na otázky bezpečnosti těchto systémů. Problematikou bezpečnosti a bezpečnostní politiky se v dnešní době zabývají jak subjekty soukromé, tak subjekty veřejné.

Tato diplomová práce se věnuje problematice bezpečnostní politiky informačních systémů subjektů bankovní sféry. Cílem této práce je vytvoření modelu informačního a komunikačního systému, jeho zhodnocení z pohledu rizikovosti provedením analýzy a tvorba samotné metodiky analýzy rizik.

Teoretická část této práce vysvětluje problematiku bezpečnostní politiky organizace, zásady její tvorby, komplexním způsobům zabezpečení informačních systémů z různých pohledů. Mezi další oblasti v této části práce patří problematika ISMS z pohledu řady norem ISO/IEC 27000 se zaměřením na provoz bankovních informačních systémů. Poslední kapitolou teoretické části jsou požadavky České národní banky na informační systém a technologie.

Praktická část analyzuje stávající klíčové procesy organizace zastoupené danými aktivy a jejich ohodnocení. Jsou popsány dílčí kroky analýzy a samotné zpracování analytickým nástrojem. Nastiňuje jednotlivé kroky implementace bezpečnostní politiky a její udržování. Dále praktická část předkládá metodiku analýzy rizik použitelnou v obdobných organizacích bankovní sféry, zpracovanou formou prováděcí směrnice pro danou organizaci.

I. TEORETICKÁ ČÁST

1 TERMINOLOGIE

Aktivum (Asset)

Cokoliv, co má pro organizaci hodnotu. [2]

Aktivum primární

Informace nebo služba, kterou zpracovává nebo poskytuje informační systém.

Pozn.: Zejména se jedná o nehmotná aktiva – informace a informační služby, které jsou organizací využívány, a funkční procesy a aktivity organizace, znalosti a know-how, které mají pro systém řízení bezpečnosti informací určitý význam, tj. je potřeba nějakým způsobem zajistit jejich bezpečnost. [3]

Aktivum podpůrné

Technické aktivum, zaměstnanci a dodavatelé, které se podílí na provozu, rozvoji, správě nebo bezpečnosti informačního systému.

Pozn.: Zejména se jedná o hmotná aktiva – technické vybavení, komunikační infrastrukturu, ale i programové vybavení nebo pracovníky či dodavatele, kteří se podílejí na chodu organizace a jejich organizační uspořádání, prostory, které organizace využívá apod. [3]

Analýza aktiv AA

Proces identifikace a hodnocení aktiv

Analýza dopadů incidentu (BIA)

Analýza dopadů incidentu (Business Impact Analysis, BIA) je hodnocením dopadů bezpečnostních incidentů, které se projeví ztrátou dostupnosti, integrity či důvěrnosti do fungování organizace.

Bezpečnost informací (Information security)

Zachování důvěrnosti, integrity a dostupnosti informací. [4]

Bezpečnostní incident

Bezpečnostní incident je každá nestandardní bezpečnostní situace, při které došlo nebo mohlo dojít k ohrožení bezpečnosti (dostupnosti, integrity a/nebo důvěrnosti) dat.

Hodnocení rizik (Risk assessment)

Hodnocení hrozeb působících na informace a zařízení informace zpracovávající, jejich zranitelnosti a pravděpodobnosti jejich výskytu i jejich dopadu na informace.

Hodnota

Základní charakteristikou aktiva je hodnota aktiva, která je založena na objektivním vyjádření obecně vnímané ceny nebo na subjektivním ocenění důležitosti (kritičnosti) aktiva, popř. kombinaci obou přístupů. Hodnota aktiva je relativní v závislosti na úhlu pohledu hodnocení. (Typickým příkladem je hodnota informace, která může být pro někoho nulová, pro někoho nesmírná.)

Hrozba

Hrozba je síla, událost nebo aktivita osoby, která má nežádoucí vliv na bezpečnost organizace nebo může způsobit škodu na jejích aktivech. (Hrozbou může být např. požár, přírodní katastrofa, krádež zařízení, získání přístupu k informacím neoprávněnou osobou, chyba obsluhy apod.)

Škoda, kterou způsobí hrozba při jednom působení na určité aktivum, se nazývá dopad hrozby. Dopad hrozby se může odvodit od absolutní hodnoty ztrát, do které jsou zahrnuty náklady na znovuoobnovení činnosti aktiva nebo náklady na odstranění následků škod způsobených hrozbou. Základními charakteristikami hrozby jsou její úroveň a četnost výskytu.

Informační systém (Information system) IS

Aplikace, služby, aktiva informační technologie nebo další komponenty zacházející s informacemi. [4]

Informační systém Společnost a.s. (IS Společnost a.s.)

Systém zpracování informací Společnosti a.s. od jejich vzniku až po jejich likvidaci, či předání.

ISMS

Systém řízení bezpečnosti informací.

Komponenta či subsystém

Soubor aktiv příbuzných dle vhodně zvoleného klíče: Dle funkční nebo technologické podobnosti. Informační systém je dekomponován nejdříve na komponenty, následně jsou v rámci komponenty identifikována aktiva.

Pojem komponenta zahrnuje i tzv. aktivum primární.

Ochranné opatření

Nebo také protiopatření je proces, procedura, technický či právní prostředek nebo cokoliv jiného, co bylo speciálně navrženo pro zmírnění působení hrozby (její eliminaci), snížení zranitelnosti nebo dopadu hrozby. Protiopatření se navrhuje s cílem předejít vzniku škody nebo s cílem usnadnit překlenutí následků vzniklé škody.

Z hlediska bezpečnostní analýzy je protiopatření charakterizováno efektivitou a náklady. Efektivita protiopatření vyjadřuje, nakolik protiopatření sníží účinek hrozby. Používá se ve fázi zvládání rizik jako jeden z hlavních parametrů při hodnocení vhodnosti použití daného protiopatření.

Protiopatření se zaměřují do oblastí snížení úrovně hrozby, snížení úrovně zranitelnosti, snížení následků působení hrozby, detekce nežádoucího vlivu s cílem včas indikovat působení hrozby a předejít možnosti jejího plného uplatnění, a do oblasti obnovení činnosti po působení hrozby.

Do nákladů na protiopatření se započítávají náklady na pořízení, zavedení a provozování protiopatření. Společně s efektivitou protiopatření jsou tyto náklady důležitými parametry při výběru protiopatření. Výběr vhodného protiopatření spočívá v optimalizaci, kdy se hledají nejúčinnější protiopatření, jejichž realizace přinese co nejmenší náklady.

Osobní údaj

Jakákoliv informace týkající se určeného nebo určitého subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu. [5]

Posuzování rizika (Risk assessment)

Celkový proces identifikace rizika, analýzy rizika a hodnocení rizika. [4]

Riziko

Riziko vyjadřuje míru ohrožení aktiva, míru nebezpečí, že se uplatní hrozba a dojde k nežádoucímu výsledku, vedoucímu ke vzniku škody. Velikost rizika je vyjádřena jeho úrovní.

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

Úroveň rizika je určena hodnotou aktiva, zranitelností aktiva a úrovní hrozby. Na růstu úrovně rizika se podílí úroveň hrozby, zranitelnost a hodnota aktiva. Jedině protiopatření úroveň rizika snižuje.

Zbytkové riziko je takové riziko, které je tak malé, že je pro systém přijatelné a není nutné podnikat další protiopatření k jeho snížení.

Správce aktiva

Osoba pověřená vlastníkem aktiva, která odpovídá za plnění konkrétních postupů a opatření dle směrnice.

Systém řízení bezpečnosti informací (Information security management system, ISMS)

ISMS sestává z politik, postupů, směrnic a příslušných zdrojů a činností, které organizace řídí, aby zajistila ochranu informačních aktiv. ISMS představuje systematický přístup k ustavení, implementování, provozování, monitorování, přezkoumávání, udržování a zlepšování bezpečnosti informací organizace tak, aby byly dosaženy její cíle. [4]

Vlastník aktiva, komponenty

Osoba, která odpovídá za identifikaci, ohodnocení a klasifikaci aktiv. Vlastník aktiva musí být určen pro každé aktivum. Pro potřeby prosazení individuální odpovědnosti určí vedoucí pracovníci vlastníky pro všechna aktiva, která daná součást organizace spravuje.

Uživatel aktiva

Osoba, která obdržela od vlastníka aktiva právo k užití aktiva.

Zranitelnost

Zranitelnost je nedostatek, slabina nebo stav analyzovaného aktiva, kterého může být využito hrozbou pro uplatnění jejího nežádoucího vlivu. Tato veličina je vlastností aktiva a vyjadřuje, jak citlivé je aktivum na působení dané hrozby.

Zranitelnost vznikne všude tam, kde dochází k interakci mezi hrozbou a aktivem.

Základní charakteristikou zranitelnosti je její úroveň. Úroveň zranitelnosti aktiva se hodnotí podle citlivosti (náchyllost aktiva být poškozeno danou hrozbou) a kritičnosti (důležitost aktiva pro organizaci).

2 PROBLEMATIKA A ZÁSADY TVORBY BEZPEČNOSTNÍ POLITIKY

Bezpečnostní politika je pojem, kterým je nazván dokument organizace. Tento dokument je nadřazený všem dílčím dokumentům a směrnicím organizace. Bezpečnostní politika zajišťuje požadavky a nařízení dané organizace na všech úrovních.

Nedílnou podmínkou existence Bezpečnostní politiky je to, že musí být v souladu s pojetím politiky celé organizace a musí být naplňována. Jedná se o dokument, který popisuje základní strategie organizace, role, odpovědnosti týkající se bezpečnosti a cíle bezpečnostní politiky. Je závazná pro všechny zaměstnance.

Analýza rizik je nedílnou součástí při tvorbě bezpečnostní politiky. Provádí se zpravidla před samotným prvotním vytvořením bezpečnostní politiky a následně v pravidelných definovaných intervalech, při významné změně v organizaci či při naplnění významné bezpečnostní události, jejíž následek vyžaduje přehodnocení bezpečnostních opatření v organizaci. Cílem analýzy rizik je ohodnocení aktiv či významných klíčových procesů v organizaci, ohodnocení hrozeb a rizik.

Bezpečnostní politika by měla být stručná, přehledná a srozumitelná. Měla by pokrývat veškeré otázky ohledně konfliktů a bezpečnosti dat.

Dalšími důležitými dokumenty spojenými s bezpečnostní politikou jsou havarijní plány. Ty definují postupy při ohrožení či narušení fungování organizace a také obsahují postupy obnovy činností organizace a jejich dílčích procesů. Kontrolní činnost je další nedílnou součástí při naplňování bezpečnostních opatření a je v kompetenci bezpečnostních auditů. Bezpečnostní audity jsou zpravidla zpracovávány externími auditory či u větších organizací interními bezpečnostními auditory. Provozní předpisy, pracovní řády či pracovní postupy jsou dalšími podklady, které definují opatření pro naplňování bezpečnostní politiky potažmo eliminaci zranitelnosti organizace.

Proces řešení bezpečnosti informací potažmo bezpečného informačního systému je obvykle tvořen 6 základními kroky:

- cíle a strategie řešení bezpečnosti informací;
- analýza rizik IS;
- bezpečnostní politika organizace;

- bezpečnostní projekt, standard a strategie;
- implementace bezpečnosti;
- hodnocení, monitoring a audit.

2.1 Cíle a strategie řešení bezpečnosti informací

Cílem řešení bezpečnosti informací je minimalizace ztrát, které mohou vzniknout zneužitím, poškozením, zničením nebo nedostupností informací. Dále je to otázka vytvoření celistvého nákladově optimalizovaného a efektivně fungujícího řízení bezpečnosti informací. Organizace běžně stanovují také další cíle, mezi které patří:

- určení principů řízení a požadované úrovně v oblasti bezpečnosti informací;
- zhodnocení současného stavu bezpečnosti informací;
- návrh dílčích kroků postupu k dosažení požadované úrovně bezpečnosti;
- příprava a vytvoření prostředí pro udržování a zvyšování bezpečnosti.

Definice cílů, požadavků a hranic bývá součástí dokumentu, který se nazývá studií bezpečnosti. Tento dokument je obvykle tvořen popisem současného stavu informační bezpečnosti organizace a vytyčuje hlavní směry dalšího postupu.

2.2 Analýza rizik IS

Nutností pro správně vyhodnocení rizik informačního systému je pojmenování hrozeb, kterým jsou informační systémy vystaveny a jejich bližší specifikace. Cílem analýzy rizik je tedy rizika identifikovat a kvantifikovat tak, aby bylo možné rozhodnout o jejich přijatelnosti pro organizaci, či rozhodnutí o opatřeních tyto hrozby snížit.

Využívají se 4 přístupy pro provedení analýzy rizik:

- základní analýza rizik – opatření jsou tvořena dle analogie podobných systémů a z všeobecných standardů;
- neformální analýza rizik (kvalitativní analýza) – analýza je provedena na základě znalosti bezpečnostních odborníků bez využití standardních metod;

- detailní analýza rizik (kvantitativní analýza) – analýza je provedena s využitím standardních strukturovaných metod ve všech fázích analýzy, jde o přesnou metodu, časově i finančně nejnáročnější;
- kombinovaná analýza rizik – dle názvu tedy kombinace základní, neformální nebo detailní analýzy.

Tyto přístupy nejsou universální pro každou organizaci. Rozhodnutí o volbě přístupu pro provedení analýzy rizik činí vedení organizace s ohledem na typ organizace a stávajících okolností.

Jako další typ členění analýzy rizik je členění dle toho, kdo danou analýzu provádí:

- vlastní přístup – analýzu provádí kmenoví zaměstnanci organizace;
- partnerský přístup – analýzu provádí zaměstnanci organizace pod odborným vedením konzultační organizace;
- dodavatelský přístup – analýzu provádí kompletně dodavatel.

Výstupem analýzy rizik bývá popis odhadovaných rizik a zároveň definování bezpečnostních požadavků, které jsou cestou pro snížení rizik na přijatelnou úroveň. Z pohledu možné klasifikace informací v organizaci, bývá výstupní dokument analýzy rizik označován jako velmi citlivý. Důvodem jsou podrobné informace o rizicích v organizaci. Přístup k těmto informacím je umožněn pouze managementu organizace a úzkému okruhu zaměstnanců. [6]

2.3 Bezpečnostní politika

Bezpečnostní politika organizace je souhrn informací týkajících se systému řízení informační bezpečnosti v dané organizaci. Je základním dokumentem v této oblasti a definuje cíle, strategie a zásady bezpečnosti informací.

Bezpečnostní politiku není jen základní dokumentací v oblasti řízení bezpečnosti informací ale i jako navazující bezpečností dokumentací (soubor dílčích pracovních řádů a směrnic). Hlavní zásadou je ochrana interních sítí a veškerých dat:

- ochrana zvenku;
- ochrana uvnitř.

Bezpečnostní politika je souhrnem bezpečnostních požadavků informační bezpečnosti v oblastech:

- fyzické bezpečnosti;
- personální bezpečnosti;
- administrativní bezpečnosti;
- počítačové a komunikační bezpečnosti;
- bezpečnost vývojového prostředí. [7]

Užitečnost bezpečnostní politiky můžeme charakterizovat jako soulad či rovnováhu vynaložených prostředků na návrh, implementaci a správu bezpečnostní politiky s přínosem samotné bezpečnostní politiky jako výsledek, který způsobí snížení rizik. [8]

2.3.1 Obsah dokumentu bezpečnostní politiky

- Definice bezpečnosti informací, cíle bezpečnostní politiky informací, rozsah a její důležitost.
- Prohlášení vedení organizace o vůli a záměru podporovat cíle a dané principy.
- Stručný výklad bezpečnostních zásah, principů a norem.
- Požadavky zvláštní důležitosti pro organizaci.
 - Požadavky na vzdělávání v oblasti bezpečnosti.
 - Dodržování legislativních požadavků a smluvních požadavků.
 - Zásady plánování kontinuity činností organizace.
 - Důsledky porušení bezpečnostních zásad.
 - Zásady prevence a detekce virů a jiného škodlivého SW.
 - Stanovení generálních a specifických odpovědností pro oblast managementu bezpečnosti informací včetně hlášení bezpečnostních incidentů.
 - Odkazy na dokumentaci, která může bezpečnostní politiku podporovat, např. detailní bezpečnostní politiky a postupy zaměřené na specifické informační systémy nebo bezpečnostní pravidla, která by měli uživatelé dodržovat. [9]

Některé organizace mají zavedenou také *systémovou bezpečnostní politiku*. Cílem této systémové bezpečnostní politiky je zajištění aktiv, která jsou součástí dílčích informačních systémů organizace. Systémová bezpečnostní politika udává:

- architekturu informačních systémů;
- využívané technologie při provozu informačních systémů apod.

Pokud je bezpečnost řešena jednotně nemusí být tento dokument zpracováván. [8]

Prvky bezpečnosti obsažené v systémové bezpečnostní politice:

- požadavky na bezpečnost PC;
- provoz;
- správa dat;
- bezpečnostní politika počítačové sítě;
- řízení přístupu k IS;
- bezpečnost datových přenosů;
- osobní odpovědnost správců dat;
- právní a etické otázky;
- vzory dokumentů.

2.3.2 Tvorba bezpečnostní politiky

Bezpečnostní politice předchází studie bezpečnosti, na kterou se sama bezpečnostní politika odvolává. Uvádí, co má být chráněno a v rámci stanovuje způsoby, jak toho má být dosaženo. Udává pravomoci, zodpovědnosti, role a prostředky pomocí kterých dosahuje cílů. [6]

2.3.3 Formulace, rozsah a přijetí bezpečnostní politiky

Důležitým faktorem v této otázce je forma řízení organizace. Faktory jako je samotný charakter organizace či její velikost je méně důležitý či zanedbatelný.

Dělení bezpečnostní politiky:

- stručná, tvoří ji základní oblasti a zásady. Je označována také jako „high-level-policy“;

- detailní, dokument obsahuje dílčí bezpečnostní opatření, která jsou závazná pro celou organizaci a jsou společná pro všechny IS v organizaci.

Následný dokument tvoří všeobecný plán, který odpovídá na otázky:

- Co?
- Kde?
- Proč?

Odpověď na tyto otázky určuje aktiva společnosti, která se mají chránit. Jedná se o dokument s dlouhodobým charakterem a i z tohoto důvodu zde bývají formulace spíše obecné. Jde tedy o předem určené bezpečnostní cíle a jejich naplňování pomocí standardů, směrnic, opatření či procedur. [6]

Bezpečnostní politika je interní dokument, který je závazný pro všechny zaměstnance dané organizace. Musí být vyhotoven v písemné podobě a všichni zaměstnanci s tímto dokumentem musí být prokazatelně seznámeni. Jako ostatní interní dokumenty i tento musí být schválen vedením organizace.

2.4 Bezpečnostní strategie, projekt, standard

2.4.1 Bezpečnostní strategie

Stanovuje základní zásady bezpečnostní politiky. Nejdůležitější součástí strategie je stanovení rozsahu chráněných aktiv (informací). To vše pro jasné určení zodpovědnosti a z pohledu důvodu jejich ochrany. Strategie je nezávislá na personálním obsazení vedoucích funkcí a na použitém technickém vybavení v organizaci. Je povinností s touto strategií seznamovat všechny zaměstnance. [6]

2.4.2 Bezpečnostní projekt

Je naplněním závěrů bezpečnostní politiky společnosti. Jde o konkrétní opatření ať už technická, organizační či administrativní.

2.4.3 Bezpečnostní standard

Standard vychází z bezpečnostní politiky organizace a je s ní ve shodě. Jde o organizační opatření, která plynou z bezpečnostního projektu a jsou zpracována ve formě zá-

vazných interních dokumentů. Bezpečnostní standard podrobně popisuje postupy pro dílčí oblasti bezpečnosti.

2.5 Implementace bezpečnosti

Samotným aktem implementace je chápán proces uvedení bezpečnostní politiky do praxe. V případě změn, které mají vliv na informační bezpečnost v organizaci, je aktualizace bezpečnostních standardů. Otázkou implementace bezpečnostní politiky je stanovení strategie řízení rizik. Existují 3 základní strategická rozhodnutí:

- přenesení rizika – přesun rizika či pokrytí rizika opatřením třetích stran, tzn. nejčastěji je to otázka pojištění;
- zmírnění rizika – snížení hrozby pro chráněné aktivum tzn. volbou opatření;
- přijetí rizika – pokud organizace neučiní žádná opatření, akceptuje tím možné bezpečnostní následky ohrožených aktiv.

2.6 Audit a monitoring

Audit, monitorování a hodnocení bezpečnosti patří do procesu řízení bezpečnosti, je jeho nedílnou součástí. Bezpečnostní studie definuje cíle a ty jsou východiskem hodnocení, monitoringu a auditu.

Pokud organizace neprovádí audit, hodnocení či má nedostatečně nastaven monitoring, dochází ke špatnému odhalování bezpečnostních incidentů. Včasné odhalení incidentů snižuje způsobené škody.

2.6.1 Bezpečnostní incidenty a ponaučení

Bezpečnostní incident jako jediný poskytuje informace o skutečném naplňování bezpečnosti informací a jejím stavu. Odráží skutečnost, není výsledkem modelování, jako tomu bývá u analýz. Ponaučení se z bezpečnostního incidentu je tedy důležitým krokem v procesu řízení bezpečnosti.

Obecně můžeme definovat u bezpečnostního incidentu tyto fáze:

- detekce;

- zvládání;
- vyhodnocení.

V procesu zvládání bezpečnostního incidentu je potřeba minimalizovat jeho škodlivé dopady pomocí postupů a struktur určených v bezpečnostní politice.

Vyhodnocení příčin vzniku bezpečnostního incidentu a ponaučení se z něj je důležitou fází. Ponaučení je obvykle reprezentováno preventivním opatřením, jelikož prevence předchází opakování bezpečnostních incidentů.

3 KOMPLEXNÍ ZPŮSOBY ZABEZPEČENÍ

Jde o ochranu informačních systémů popř. informací po dobu jejich přenosu, uchování a zpracování. Cílem je ochrana informací před zneužitím, odcizením či poškozením. Ochranu informačních systémů naplňujeme hlavně pomocí kombinace technických, fyzických, organizačních a logických opatření.

Dle bezpečnostní politiky bezpečnost ICT obsahuje prevenci a zmírnění dopadů hrozeb na informační systém. Z tohoto důvodu je možné hrozby členit následovně:

- napadení síťové infrastruktury;
- napadení serverů;
- napadení počítačů (pracovních stanic);
- napadení aplikací;
- odcizení dat;
- nežádoucí přenosy dat;
- znemožnění poskytování služeb. [10]

Mezi další členění můžeme zařadit dělení na:

- vnitřní;
- vnější.

U obou členění jsou možné hrozby:

- nedostupnost služeb:
 - způsobené chybou osoby (vnitřní členění);
 - způsobené úmyslnou či náhodnou akcí nepovolaných osob;
- ztráty;
- zničení;
- modifikace;
- kompromitace dat (z pohledu vnitřního členění).

Působením hrozeb, kvantifikací jejich pravděpodobnosti vznikají rizika potažmo škody. Škoda může být vyvolána chybou systému či jednotlivcem. Člověk způsobuje škody:

Úmyslně:

- cíleně formou penetračních testů (simulace útoku na systém);
- napadením IS (poškození či odcizení dat).

Neúmyslně – běžně formou chyb způsobených při programování aplikací. Neúmyslné chyby jsou běžně odhalovány formou testování před uvedením do produkce. [11]

3.1 Personální bezpečnost

Personální bezpečnost se zaměřuje na prevenci hrozby, která vzniká v řadách vlastních zaměstnanců společnosti. Právě praxe ukazuje, že nejvíce ohrožují ICT právě zaměstnanci. Právě těmito nechtěným situacím se předchází pomocí prověrek a testů v řadách stávajících i budoucích zaměstnanců.

Organizace při výběru nových zaměstnanců na pozice správců informačních systémů by neměla podceňovat výběrová řízení a vybírat si budoucí zaměstnance s ohledem na jejich schopnosti a dovednosti. Na těchto pozicích je potřeba vybírat kvalitní lidi, kteří budou pro organizaci přínosem. [12]

3.2 Režimová bezpečnost

Mezi oblasti zájmu, které spadají do režimové bezpečnosti, řadíme:

- řízení přístupových práv a pravomocí osob přistupujících k určitým typům informací;
- řízení klasifikace informací – vymezení klasifikačních stupňů a informací pro klasifikaci;
- postupy při nakládání s utajovanými (klasifikovanými) informacemi;
- řízení přístupu a pohybu osob v prostorách organizace;
- definování organizačního řádu.

3.3 Fyzická bezpečnost

Jedná se o soubor opatření s cílem ochrany dat, nosičů dat a informačních zdrojů před fyzickým útokem osob, které by mohly odcizit či poškodit aktiva společnosti. Mezi běžné požadavky na prostory s prostředky ICT patří:

- perimetrická ochrana;
- ochrana před neautorizovaným přístupem a zneužitím;
- ochrana rozvodů a dodávek energií. [12]

3.4 Bezpečnost během komunikace

V této oblasti je hlavním zájmem ochrana přenášených dat a informací v informačních kanálech. V dnešní době se využívá hlavně prostředků kryptografické ochrany či detekce náhodných popř. záměrných změn. Informační kanály je třeba chránit před útočníky, kteří mohou tuto komunikaci odposlouchávat. [10]

V praxi se tak hojně využívá mezi komerčními subjekty např. služeb certifikačních autorit – certifikátů. V procesu výměny informací dochází tedy nejdříve k autentizaci a identifikaci subjektů a pak až následně ke komunikaci samotné.

3.5 Bezpečnost HW

V této oblasti bezpečnosti je zájem zaměřen na problematiku přístupu k technickým prostředkům, otázky spojené s ochranou proti odposlouchávání (zjišťování a odstraňování) popř. i problematiku ochrany před elektromagnetickým zářením.

Tato činnost se zajišťuje pomocí pravidelných či jednorázových prohlídek vybavení a prostor se zařízeními jako jsou šumové generátory či šifrovací zařízení zabraňující odposlechům či zajišťující rušení. Dále je třeba zajišťovat kontroly:

- týkající se funkčnosti zařízení ochrany informací;
- provádění technických prohlídek k odhalení zařízení k úniku informací;
- plnění organizačních opatření (na specifických úsecích, které toto vyžadují). [13]

3.6 Bezpečnost SW

Do této oblasti bezpečnosti spadá ochrana softwaru před zneužitím. Jedná se hlavně o procesy ověřování uživatele, identifikace, dělení pravomocí jednotlivých uživatelů. Všechny tyto postupy mají společný cíl a to ochrana před zneužitím nežádoucím uživatelem.

3.7 Administrativní bezpečnost

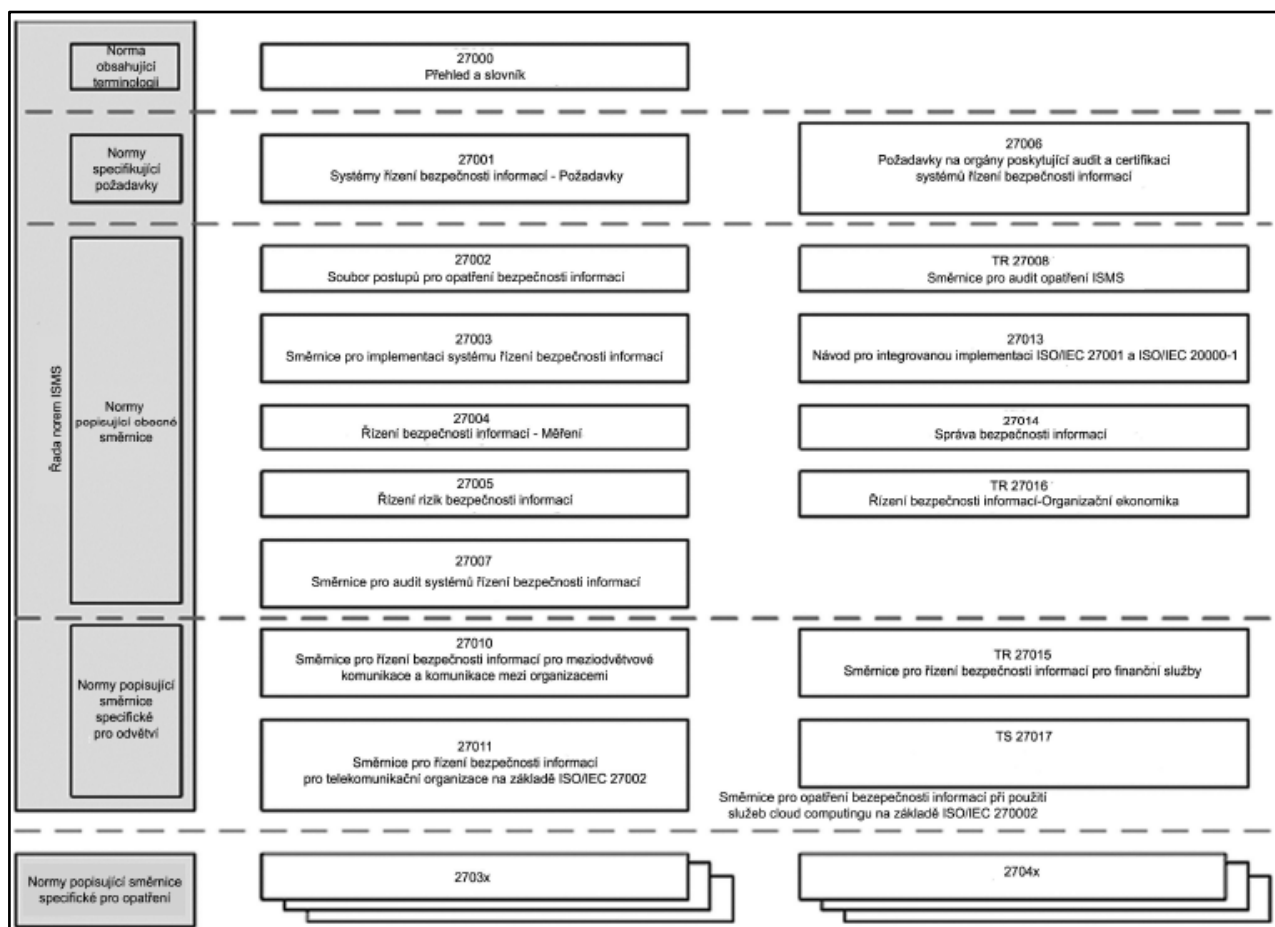
Úkolem administrativní bezpečnosti je definování postupů při nakládání s utajovanými popř. jinak citlivými informacemi ve společnosti. K těmto účelům jsou definovány pracovní postupy či směrnice klasifikace informací. Obsahem těchto dokumentů by mělo být:

- postup tvorby dokumentů;
- přijetí, zpracovávání a řazení dokumentů;
- postupy odesílání a formy přepravy;
- postupy evidence a skartace;
- formy přenášení;
- požadavky na uložení či archivaci;
- popř. jiné jako jsou požadavky na zabezpečení. [12]

4 ŘADA NOREM ISMS

4.1 Obecně

Řada norem ISMS 2700x je skladba vzájemně souvisejících norem definující požadavky a návody pro různé implementace. Číselné členění řady norem viz. Obr. 1 Vztah mezi normami řady ISMS.



Obr. 1 Vztah mezi normami řady ISMS [4]

Dělení:

- normy popisující přehled a terminologii;
- normy specifikující požadavky;
- normy popisující obecné směrnice;
- normy popisující směrnice specifické podle odvětví.

Na základně výše uvedeného členění je níže zpracován výčet dílčích norem a citovány normy vztahující se k problematice této diplomové práce.

4.2 Normy popisující přehled a terminologii

4.2.1 ISO/IEC 27000

Mezinárodní norma poskytující:

- přehled řady norem ISMS;
- úvod do systémů řízení bezpečnosti informací (ISMS);
- přehled používaných terminologií a definic.

„ISO/IEC 27000 popisuje základy systémů řízení bezpečnosti informací, které tvoří předmět řady norem ISMS, a definuje související termíny.“ [4]

4.3 Normy specifikující požadavky

4.3.1 ISO/IEC 27001

„Tato mezinárodní norma specifikuje požadavky na ustanovení, implementování, provozování, monitorování, přezkoumávání, udržování a zlepšování formalizovaných systémů řízení bezpečnosti informací (ISMS).“

„ISO/IEC 27001 poskytuje normativní požadavky na vývoj a provoz ISMS, včetně sady opatření pro řízení a zmírnění rizik spojených informačními aktivy, které se organizace provozováním ISMS snaží chránit. Organizace provozující ISMS mohou mít příslušnou shodu doloženou auditem a certifikací.“ [4]

4.3.2 ISO/IEC27006

„Tato mezinárodní norma specifikuje požadavky a poskytuje návod pro orgány poskytující audit a certifikaci ISMS v souladu s ISO/27001, vedle požadavků obsažených v ISO/IEC 17021.“ [4]

4.4 Normy popisující obecné směrnice

Jedná se o výčet norem:

- ISO/IEC 27002 Soubor postupů pro opatření bezpečnosti informací;

- ISO/IEC 27003 Směrnice pro implementaci systémů řízení bezpečnosti informací;
- ISO/IEC 27004 Řízení bezpečnosti informací – Měření;
- ISO/IEC 27005 Řízení rizik bezpečnosti informací;
- ISO/IEC 27007 Směrnice pro audit systémů řízení bezpečnosti informací;
- ISO/IEC 27008 Směrnice pro audit opatření ISMS;
- ISO/IEC 27013 Návod pro integrovanou implementaci ISO/27001 a ISO/IEC 20000-1;
- ISO/IEC 2714 Správa bezpečnosti informací;
- ISO/IEC 27016 Řízení bezpečnosti informací – Organizační ekonomika.

4.4.1 ISO/IEC 27002

„Tato mezinárodní norma poskytuje seznam obecně akceptovaných cílů opatření a opatření pro doporučené postupy, které mají být použity jako návod k implementaci při výběru a provádění opatření, jejichž cílem je dosáhnout bezpečnosti informací.“ [4]

4.4.2 ISO/IEC 27005

„Tato mezinárodní norma poskytuje směrnice řízení rizik bezpečnosti informací.“
„ISO/IEC 27005 poskytuje návod pro implementaci procesně orientovaného přístupu k řízení rizik, aby tak pomohla uspokojivě implementovat a splnit požadavky na řízení rizik bezpečnosti informací uvedené v ISO/IEC 27001.“ [4]

4.5 Normy popisující směrnice specifické pro jednotlivá odvětví

Jedná se o výčet norem:

- ISO/IEC 27010 Směrnice pro řízení bezpečnosti informací pro meziodvětvové komunikace a komunikace mezi organizacemi;
- ISO/IEC 27011 Směrnice pro řízení bezpečnosti informací pro telekomunikační organizace na základě ISO/IEC 27002;
- ISO/IEC TR 27015 Směrnice pro řízení bezpečnosti informací pro finanční služby;

- ISO/IEC 27799 Řízení bezpečnosti informací ve zdravotnictví využívající ISO/IEC 27002.

4.5.1 ISO/IEC TR 27015

„Tato technická zpráva poskytuje směrnice pro iniciaci, implementaci, udržování a zlepšování bezpečnosti informací v organizacích poskytující finanční služby vedle návodu uvedeného v řadě norem ISO/IEC 27000.“ [4]

5 POŽADAVKY DLE VYHLÁŠKY ČNB Č. 163/2014 SB

Vyhláška České národní banky č. 163/2014 Sb. zpracovává a navazuje na předpisy Evropské unie.

- Směrnice Evropského parlamentu a Rady 2013/36/EU ze dne 26. června 2013 o přístupu k činnosti úvěrových institucí a o obezřetnostním dohledu nad úvěrovými institucemi a investičními podniky, o změně směrnice 2002/87/ES a zrušení směrnic 2006/48/ES a 2006/49/ES, v platném znění.
- Nařízení Evropského parlamentu a Rady (EU) č. 575/2013 ze dne 26. června 2013 o obezřetnostních požadavcích na úvěrové instituce a investiční podniky a o změně nařízení (EU) č. 648/2012.

Tato vyhláška mimo jiné upravuje požadavky na řídicí a kontrolní systém banky a dále pravidla pro krytí a omezení rizik. Toto jsou 2 základní oblasti, které souvisí s problematikou obsaženou v této diplomové práci.

Požadavky na informace a komunikace dle § 23

„(5) Povinná osoba

a) stanoví podmínky přístupu pracovníků k informačním a komunikačním systémům a údajům v nich zaznamenaným, rozsah přístupových práv a proces jejich stanovení, včetně způsobu rozhodování o rozsahu přístupových práv jednotlivých pracovníků a rozhodování o jejich změnách,

b) stanoví způsob zajištění a podmínky, za kterých budou do informačních a komunikačních systémů ukládána data související s prováděnými obchody a poskytovanými službami a prováděny jejich dovozené úpravy, podmínky nakládání s těmito daty a zajištění snadné zjistitelnosti jejich původního obsahu a provedených úprav a

c) zabezpečuje ochranu informačních a komunikačních systémů před přístupem a zásahy ze strany neoprávněných osob a před poškozením a možnost zpětně získat stanovené informace i v případě, že k poškození došlo.“ [14]

5.1 Požadavky na informační systémy a technologie

- Vytvoření bezpečnostních zásad informačních systémů, jejichž obsahem jsou:

- a) cíle bezpečnosti informačních systémů;
- b) hlavní zásady a postupy pro zajištění integrity, dostupnosti a důvěrnosti informací;
- c) definování působnosti a pravomocí v oblasti ochrany aktiv a zajištění plnění bezpečnostních zásad informačních systémů.
- Zajištění dodržování bezpečnostních zásad v jednotlivých informačních systémech.
- Pravidelné provádění analýzy rizik informačních systémů s definovanými:
 - a) aktivy;
 - b) hrozbami;
 - c) pravděpodobností realizace hrozeb;
 - d) odhad následků působení hrozeb a protiopatření.
- V oblasti zajištění bezpečnosti přístupu k informacím má provozovatel banky povinnost:
 - a) přidělení přístupových práv uživatelům informačních systémů;
 - b) ochrany důvěrnosti a integrity autentizačních údajů;
 - c) zajistit jednoznačnou autentizaci uživatele v systémech;
 - d) zajistit přístup k informacím v informačních systémech uživatelům, kteří byli pro tento přístup autorizováni;
 - e) zaznamenávání událostí auditních záznamů systémů – logů, jejich ochranu před neautorizovaným přístupem, modifikací nebo zničením;
 - f) uchovávání a vyhodnocování bezpečnostních auditních záznamů pracovníkem, který má přístup k těmto logům pouze s oprávněním čtení těchto záznamů.
- V oblasti bezpečnosti komunikačních sítí provozovatel banky zajišťuje:
 - a) opatření minimalizace průniku do její vnitřní sítě a zajištění tak bezpečnosti informačních systémů ve vnitřní síti;
 - b) v případě přenosu informací v prostředí internetu musí být zajištěna důvěrnost a integrity informací a zvolena spolehlivá autentizace komunikačních stran včetně ochrany autentizačních údajů.

- V oblasti fyzické bezpečnosti musí být zavedeny a udržovány opatření zajištění fyzické ochrany aktiv informačních systémů.
- Při provozování informačních systémů je krom jiných požadavků kladen důraz na pravidelné provádění a vyhodnocování bezpečnosti informačních systémů. [14]

II. PRAKTICKÁ ČÁST

6 POPIS ORGANIZACE

6.1 Charakteristika

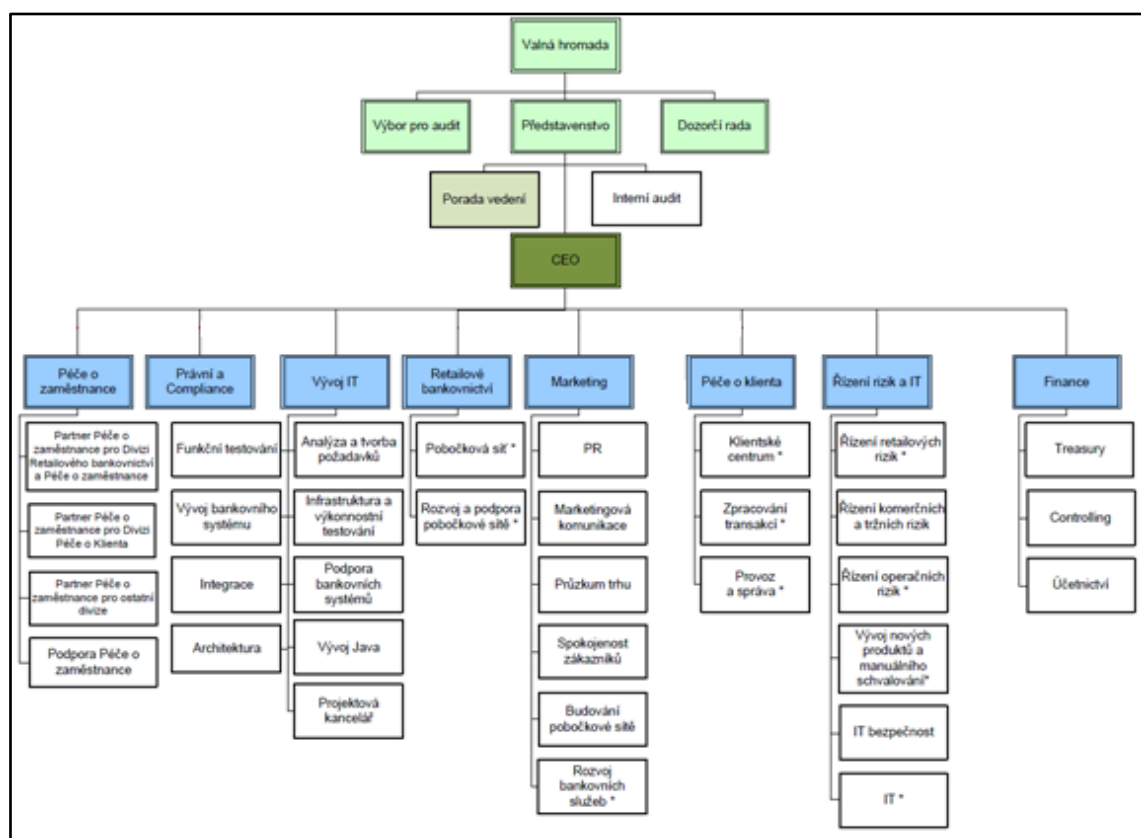
V rámci mé diplomové práce je předmětem analýzy systémů společnost působící v bankovní sféře. Velice oceňuji ochotu vedení této společnosti, že mi umožnila provést analýzu systémů a ctím její požadavky:

- anonymizace názvu společnosti, dále jen „Společnost a. s.“;
- záměrně zkreslené hodnoty při hodnocení komponent a aktiv;
- nezveřejňovat výsledky hospodaření společnosti.

To vše s ohledem na zajištění bezpečnosti systémů a ochrany informací a dat jak interních, tak klientských. Předmětem analýzy rizik jsou tedy všechny klíčové procesy organizace, potažmo komponenty celkového informačního systému.

Společnost a.s. působí na českém trhu od roku 2010 a její hlavní sídlo je v Praze. Provozuje řádově desítky poboček po celé České Republice.

6.2 Organizační struktura organizace



Obr. 2 Organizační struktura Společnost a. s. [vlastní]

7 BEZPEČNOSTNÍ SITUACE ORGANIZACE

7.1 Analýza rizik informačního systému

Společnost nemá implementován a formálně zaveden systém řízení bezpečnosti informací dle standardů řady ČSN ISO/IEC 2700x – Information Security management system (dále též jen ISMS), nicméně s ohledem k požadavkům regulatorních opatření (zejména regulace v oblasti ochrany osobních údajů) je pro oblast řízení bezpečnosti informací jednoznačně efektivní přidržet se postupů a doporučení ISMS.

7.1.1 Identifikace komponent (model informačního systému)

Informačním systémem rozumíme systém zpracování informací, včetně souvisejících organizačních, technických a finančních prostředků a lidských zdrojů, který opatřuje a distribuuje informace.

Hlavní prvky celkového informačního systému Společnost a.s. tvoří malé množství, relativně samostatných informačních systémů, mezi hlavní patří následující:

- servery a datová úložiště;
- AD, doménová struktura;
- telefonní ústředna (HW+SW);
- serverovna (zabezpečené zóny);
- internetové bankovníctví;
- mobilní bankovníctví;
- klientská data;
- PZTS, EPS;
- elektronická pošta;
- účetnictví;
- IDM (řízení přístupových práv);
- archív;
- infrastruktura;
- aktivní síťové prvky;

- personální IS;
- mzdový IS;
- podatelna + datové schránky;
- docházkový systém;
- helpdesk.

7.1.1.1 Analýza dopadů incidentu (BIA)

Za účelem provedení BIA analýzy byl informační systém dekomponován na komponenty systému, či služby koncovému uživateli. Cílem tohoto hodnocení je určit důležitost pro společnost. Jednalo se o dotazování vlastníků procesů, kteří měli hodnověrně vysvětlit způsoby, kterými jsou data využívána. Tito pracovníci byli dotazováni na nastínění realistického scénáře nejhoršího případu, který by mohl vyplývat z následujících dopadů:

- nedostupnost dat;
- poškození dat (integrita dat);
- prozrazení dat (důvěrnost dat).

Jako vodítko byla vytvořena hodnotící tabulka, která je zmíněna v kapitole Metodika analýzy rizik a je součástí přílohy této diplomové práce.

Celkový přehled hodnocení dopadů jednotlivých procesů:

Tab. 1 Výsledky hodnocení BIA Společnost

a. s. [vlastní]

Servery a datová úložiště	9
AD, doménová struktura	9
Telefonní ústředna (HW+SW)	9
Serverovna (zabezpečené zóny)	9
Internetové bankovníctví	9
Mobilní bankovníctví	9
Klientská data	9
PZTS, EPS	9
Elektronická pošta	8
Účetnictví	8
IDM (řízení přístupových práv)	8

Archív	8
Infrastruktura	7
Aktivní síťové prvky	7
Personální IS	7
Mzdový IS	7
Podatelna + datové schránky	6
Docházkový systém	4
HelpDesk	4

7.1.2 Identifikace aktiv

Na základě následného zpracování zjištění hodnocení dopadů incidentu jsou identifikována jednotlivá aktiva. Současně s identifikací aktiv jsou určeni vlastníci jednotlivých aktiv.

Aktiva jsou seskupena podle bezpečnostních nároků a případně dalších požadavků na kritičnost zpracovávaných informací.

Aktivum lidské zdroje je zahrnuto do jednotlivých identifikovaných aktiv, jeho působení na jiné aktivum je hodnoceno v hrozbě „Chyba provozních zaměstnanců“ a „Chyby uživatele“.

Aktivum HW (pracovní stanice, notebooky) je vzhledem k jeho hodnotě integrováno do aktiva Servery a datová úložiště.

Následující tabulka popisuje identifikovaná informační aktiva a jejich vlastníky.

Tab. 2 Vlastníci informační aktiva Společnost a. s. [vlastní]

Aktivum	Vlastník
1. Infrastruktura	Oddělení IT
2. Aktivní síťové prvky	Oddělení IT
3. Servery a datová úložiště	Oddělení IT
4. Firewall	Oddělení IT
5. El.pošta	Oddělení IT
6. AD, Doménová struktura	Oddělení IT
7. Telefonní ústředna	Oddělení IT
8. SW telefonní ústředny	Oddělení IT
9. Serverovna (zabezpečené zóny)	oddělení IT bezpečnost
10. Informace o uživateli	oddělení IT bezpečnost
11. Bankovní IS	divize Řízení rizik a IT

Aktivum	Vlastník
12. Data o klientech	divize Retailové bankovníctví
13. Data o účtech	divize Retailové bankovníctví
14. Personální IS	divize HR
15. Mzdový IS	divize HR
16. Účetnictví	divize Finance
17. Majetek	divize Klientské služby
18. Kamerový systém	oddělení Řízení operačních rizik
19. Docházkový systém	divize HR
20. Komunikace mimo banku (ČNB, ...)	divize Finance
21. Help desk	oddělení IT
22. Bankomaty	oddělení Kartové centrum
23. ATM systém (podpora bankomatů)	oddělení Kartové centrum
24. CA (certifikační autorita)	oddělení IT bezpečnost
25. Poplachový systém (popl.tl.)	oddělení Řízení operačních rizik
26. EZS, EPS	oddělení Řízení operačních rizik
27. Evidence uživatelských práv (Práva)	oddělení IT bezpečnost
28. IS auditu (SIEM)	oddělení IT bezpečnost
29. Klimatizace + UPS	oddělení IT
30. Podatelna + dat.schr.	divize Klientské služby
31. Archiv	divize Klientské služby
32. Datové schránky	divize Klientské služby
33. Síťové tiskárny	oddělení IT
34. Sklad zálohovacích médií	oddělení IT bezpečnost

7.1.3 Hodnocení aktiv

Hodnota aktiv je stanovována vlastníkem v relativní stupnici s využitím hodnotící stupnice. Byla vybrána a odsouhlasena třístupňová škála hodnocení aktiv. Důvěrnost, integrita a dostupnost je hodnocena jako vysoká, střední nebo nízká.

Tab. 3 Škála hodnocení aktiv [vlastní]

Vlastnost	Požadavek	Popis
Důvěrnost	Vysoká (V)	Ztráta důvěrnosti aktiva může způsobit ohrožení hlavních činností banky, vážnou ztrátu důvěryhodnosti banky, rozsáhlou negativní publicitu, sankce ve výši milionů korun
	Střední (S)	Ztráta důvěrnosti aktiva může způsobit ohrožení vedlejších činností banky, narušení důvěryhodnosti banky, občasnou negativní publicitu, sankce ve výši až jednotek milionů korun
	Nízká (N)	Ztráta důvěrnosti aktiva nenaruší činnosti banky, může způsobit ojedinělé stížnosti nebo sankce ve výši nejvýše řádů stovek tisíc korun.
Dostupnost	Vysoká (V)	Aktivum musí být dostupné trvale, je možno tolerovat dobu nedostupnosti v řádu minut
	Střední (S)	Aktivum musí být dostupné v pracovní době, je možno tolerovat dobu nedostupnosti v řádu hodin
	Nízká (N)	Aktivum nemusí být trvale dostupné, je možno tolerovat dobu nedostupnosti v řádu dnů
Integrita	Vysoká (V)	Ztráta integrity může způsobit ohrožení hlavních činností banky, nároky na vícepráci nebo hmotné ztráty v řádu milionů korun a více
	Střední (S)	Ztráta integrity může způsobit ohrožení vedlejších nebo omezení hlavních činností organizace, nároky na vícepráci nebo hmotné ztráty v řádu až jednotek milionů korun.
	Nízká (N)	Ztráta integrity aktiva může způsobit omezení vedlejších činností organizace, nároky na vícepráci nebo hmotné ztráty nejvýše v řádu stovek tisíc korun

Skupina aktiv	Infrastruktura	Aktivní síťové prvky	Servery a datová úložiště	Elektronická pošta	AD, doménová struktura
Hrozby					
Dostupnost	V	V	V	S	V
Důvěrnost	S	S	V	V	V
Integrita	S	S	V	V	V

Obr. 3 Vzorek hodnocení aktiv Společnost a.s. [vlastní]

7.1.4 Odhad a hodnocení hrozeb

Hodnocení hrozeb a zranitelností je založeno zejména na informacích získaných v pohovorech s vlastníky aktiv. Na jejich základě byla stanovena úroveň jednotlivých hrozeb a zranitelností u jednotlivých aktiv. Detailní dokumentace o přehledu hrozeb a zranitelností je součástí výstupů SW nástroje ARIS.xls.

7.1.4.1 Odhad frekvence hrozeb, úrovně zranitelnosti a stávající opatření

K celkovému posouzení hrozby je nutné znát její úroveň (pravděpodobnost výskytu hrozby), ale také úroveň zranitelnosti systémů. Proto je u každé hrozby uvedena i úroveň zranitelnosti. Podle toho je možno posoudit, zda má hrozba s vysokou úrovní šanci na úspěch (realizaci).

Odhad četnosti výskytu hrozby

Tab. 4 Odhad četnosti hrozby [vlastní]

Stupeň	Slovní popis	Četnost výskytu
1	Velmi nízká	jednou za více let
2	Nízká	asi jednou ročně
3	Střední	asi jednou měsíčně
4	Vysoká	asi jednou za několik dnů
5	Mimořádně vysoká	denně až trvale

Například:

Vždy když se vrátím z oběda	= 5	Když přijde velká voda	= 1
Vždy ve výplatní termín	= 3	Viry, spyware, hackeři	= 5
Jednou za půl roku	= 2	Porucha PC typicky	= 2
Jednou za čtvrt roku	= 3	Porucha serveru typicky	= 1
Při každé bouřce	= 3		

Odhad dopadu hrozby*Tab. 5 Odhad dopadu hrozby [vlastní]*

Stupeň	Dopad hrozby	Vodítka pro odhad z hlediska			
		organizačního	poškození aktiva	výpadku služby	finančního
1	Zanedbatelný	nevýznamný	do 1%	do 1 hodina	do 5 tis. Kč
2	Nízký	znatelný	do 5%	do 4 hodin	do 50 tis. Kč
3	Střední	přechodné problémy	do 10%	do 1 dne	do 1 mil. Kč
4	Vysoký	krátkodobé vážné problémy	do 50%	do 1 týdne	do 10 mil. Kč
5	Mimořádně vysoký	dlouhodobé vážné problémy	> 50%	> 1 týden	> 10 mil. Kč

K odhadu se použije ten sloupec, který nejlépe odpovídá charakteru aktiva a typu hrozby.

Odhad účinnosti stávajících opatření*Tab. 6 Odhad účinnosti opatření [vlastní]*

Stupeň	Slovní popis	Účinnost asi
1	Mimořádně vysoká	>95%
2	Dostatečná	80%
3	Částečná	50%
4	Nízká	20%
5	Zanedbatelná	<5%

Například opatření na ochranu proti škodlivým programům:

Pravidelně aktualizovaný, centrálně instalovaný a administrovaný antivirový SW = 1

Lokálně instalovaný antivirový SW s automatickou aktualizací, poučení uživatelé = 2

Lokálně instalovaný antivirový SW, bez pravidelné aktualizace, neznalí uživatelé = 4

Skupina aktiv	Infrastruktura			Aktivní síťové prvky			Servery a datová úložiště		
Hrozby									
Dostupnost	V			V			V		
Důvěrnost	S			S			V		
Integrita	S			S			V		
	Č	D	O	Č	D	O	Č	D	O
Zemětřesení									
Povodně									
Hurikán	1	5	3	1	5	3	1	5	3
Blesk	1	3	3	1	3	3	1	3	3
Průmyslová akce									
Bombový útok									
Použití zbraní									
Požár	1	5	2	1	5	2	1	4	2
Úmyslná škoda	1	2	1	1	2	2	1	3	2
Selhání dodávky energie	2	2	2	2	3	2	2	3	2
Selhání dodávky vody									
Selhání klimatizace				2	3	3	2	3	2
Selhání HW				1	3	1	1	3	2
Kolísání proudu (energie)	1	2	2	1	3	1	2	2	2

Obr. 4 Vzorek hodnocení hrozeb Společnost a. s. [vlastní]

7.1.5 Stanovení míry rizika

Míra rizika (bezrozměrné číslo) je určena jako součin číselných parametrů hodnoty aktiva, četnosti hrozby, dopadu hrozby, koeficientu účinnosti stávajících opatření.

Kalkulace probíhá dle vzorce:

$$R = (V_C + V_I + V_A) * O * I * C$$

(1)

kde:

R = míra rizika,

V_C = hodnota aktiva z pohledu ohrožení jeho důvěrnosti,

V_I = hodnota aktiva z pohledu ohrožení jeho integrity,

V_A = hodnota aktiva z pohledu ohrožení jeho dostupnosti,

O = četnost hrozby,

I = dopad hrozby,

C = koeficient účinnosti existujících protiopatření.

Míra rizika bez uvažování stávajících opatření

Výpočet vychází ze stávajícího vzorce za předpokladu, že uvažujeme neexistenci opatření. Neexistence opatření je v tomto případě vyjádřena hodnotou koeficientu $C = 5$. Kompletní hodnocení rizik jednotlivých aktiv Společnost a. s. je součástí ARIS.xls. V Příloze P IX je uveden přehled hodnocení rizik bez uvažování stávajících opatření.

Míra rizika se stávajícími opatřeními

Přehled výsledků hodnocení rizik s uvažováním stávajících opatření je součástí Přílohy P X. Kompletní hodnocení rizik je součástí ARIS.xls.

7.2 Popis SW nástroje ARIS.xls

Softwarový nástroj pro podporu zpracování analýzy rizik byl vytvořen pro vnitřní potřebu společnosti samotné. Skládá se ze soustavy tabulek a vzorců v aplikaci Microsoft Excel a programových bloků v jazyce Visual Basic for Applications. Tento nástroj mi byl po dobu tvorby mé diplomové práce zpřístupněn pod odborným vedením vedoucího oddělení IT bezpečnosti.

7.2.1 Podklady

Údaje zjištěné při pohovorech s respondenty (vlastníky aktiv) jsou vkládány do listu Podklady.

7.2.1.1 Aktiva

- Každému aktivu jsou určeny tři sloupce, v horní části sloučené. Aktiva lze přidávat vložením sloupců na pravou stranu tabulky nebo i mezi existující aktiva, je však nutné zachovat existující uspořádání.
- Do řádku 1 je vkládán název aktiva.

- Do řádků 2, 3, 4 jsou vkládány hodnoty nároků aktiva na zachování dostupnosti, důvěrnosti a integrity, ve formě znaků N, S, V pro hodnoty Nízká, Střední, Vysoká.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1		Aktiva																
2		Dostupnost		V		S			S			V		S				
3		Důvěrnost		V		S			N			V		N				
4		Integrita		S		N			N			S		V				
5			Č	D	P	Č	D	P	Č	D	P	Č	D	P	Č	D	P	Č
6	1.1	Hrozba 1.1	1	5	1	1	4	2	1	3	2	1	4	1	1	5	1	1
7	1.2	Hrozba 1.2	1	5	1	1	4	2	1	3	2	1	4	1	1	3	1	1
8	1.3	Hrozba 1.3	1	5	1	1	4	2	1	3	2	1	4	1				1
9	1.4	Hrozba 1.4	1	5	1	1	4	2	1	3	2	1	4	1				1
10	1.5	Hrozba 1.5	1	5	1	1	4	2	1	3	2	1	4	1				1
11	1.6	Hrozba 1.6	1	5	1	1	4	2	1	3	2	1	4	1	3	3	2	1
12	1.7	Hrozba 1.7	1	5	1	1	4	2	1	3	2	1	4	1				1
13	2.1	Hrozba 2.1	2	4	2	1	3	2	1	2	2	2	3	2				1
14	2.2	Hrozba 2.2	2	3	2	2	2	2	2	2	2	2	3	2	2	5	2	1
15	2.3	Hrozba 2.3	1	3	2	1	2	2	3	2	3	1	3	2				1
16	2.4	Hrozba 2.4	1	2	1	1	2	1	3	2	3	1	2	1				1
17	2.5	Hrozba 2.5	3	2	2	3	3	3	4	3	3	3	2	2	3	2	2	2
18	2.6	Hrozba 2.6	3	3	2	3	3	3	5	3	4	3	3	2	2	2	3	5
19	2.7	Hrozba 2.7	4	4	3	3	3	3	3	2	3	4	4	3	3	3	2	1
20	3.1	Hrozba 3.1	3	4	2	3	4	2	3	4	2	3	4	2	1	4	1	2
21	3.2	Hrozba 3.2	3	3	1	3	3	1	3	3	1	3	3	1				1
22	3.3	Hrozba 3.3	5	2	2	5	2	2	5	2	2	5	2	2				1
23	3.4	Hrozba 3.4	3	3	3	3	3	3	3	3	3	3	3	3	1	4	2	1

Obr. 5 List Podklady – Aktiva [vlastní]

7.2.1.2 Katalog hrozeb

- Katalog (seznam) hrozeb, stanovený v úvodu analýzy, je vložen v řádcích 6 a dále, sloupcích 1 (číslo hrozby) a 2 (název hrozby). Hrozby je možno přidávat nebo odebrat přidáním nebo odebráním řádku, se zachováním existujícího uspořádání.
- Při přidání nebo odebrání hrozby je nutno provést také:
 - přidání nebo odebrání příslušného sloupce hrozby ve vzorovém listu 0. Přitom je třeba dbát na zachování vzorců a formátů, např. je zkopírovat ze sousedního sloupce;
 - přidání nebo odebrání příslušného sloupce hrozby v listu Hrozby. V případě přidání hrozby je nutno provést mapování opatření, které danou hrozbu pokrývají – do průsečíku hrozby a opatření se vkládá hodnota 1.

Microsoft Excel - Triangl.xls																		
Soubor Úpravy Zobrazit Vložit Formát Nástroje Data Okno Nápověda																		
Vložit jinak...																		
100%																		
Arial 10 B I																		
Aktiva																		
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
	Aktiva																	
1																		
2	Dostupnost		V			S			S			V			S			
3	Důvěrnost		V			S			N			V			N			
4	Integrita		S			N			N			S			V			
5																		
6	1.1 Hrozba 1.1	Č	D	P	Č	D	P	Č	D	P	Č	D	P	Č	D	P	Č	D
7	1.2 Hrozba 1.2	1	5	1	1	4	2	1	3	2	1	4	1	1	5	1	1	5
8	1.3 Hrozba 1.3	1	5	1	1	4	2	1	3	2	1	4	1					
9	1.4 Hrozba 1.4	1	5	1	1	4	2	1	3	2	1	4	1					
10	1.5 Hrozba 1.5	1	5	1	1	4	2	1	3	2	1	4	1					
11	1.6 Hrozba 1.6	1	5	1	1	4	2	1	3	2	1	4	1	3	3	2		
12	1.7 Hrozba 1.7	1	5	1	1	4	2	1	3	2	1	4	1					
13	2.1 Hrozba 2.1	2	4	2	1	3	2	1	2	2	2	3	2					
14	2.2 Hrozba 2.2	2	3	2	2	2	2	2	2	2	2	3	2	2	5	2		
15	2.3 Hrozba 2.3	1	3	2	1	2	2	3	2	3	1	3	2					
16	2.4 Hrozba 2.4	1	2	1	1	2	1	3	2	3	1	2	1					
17	2.5 Hrozba 2.5	3	2	2	3	3	3	4	3	3	3	2	2	3	2	2		
18	2.6 Hrozba 2.6	3	3	2	3	3	3	5	3	4	3	3	2	2	2	3		
19	2.7 Hrozba 2.7	4	4	3	3	3	3	3	2	3	4	4	3	3	3	2		
20	3.1 Hrozba 3.1	3	4	2	3	4	2	3	4	2	3	4	2	1	4	1		
21	3.2 Hrozba 3.2	3	3	1	3	3	1	3	3	1	3	3	1					
22	3.3 Hrozba 3.3	5	2	2	5	2	2	5	2	2	5	2	2					
23	3.4 Hrozba 3.4	3	3	3	3	3	3	3	3	3	3	3	3	1	4	2		

Obr. 6 Seznam hrozeb [vlastní]

Microsoft Excel - Triangl.xls												
Soubor Úpravy Zobrazit Vložit Formát Nástroje Data Okno Nápověda												
E3 fx Arial 10 B I U												
	A	B	C	D	E	F	G	H	I	J	K	
1					Hrozba	Hrozba 1.1	Hrozba 1.2	Hrozba 1.3	Hrozba 1.4	Hrozba 1.5	Hrozba 1.6	Hrozba 1.7
2				Relevantní	ne	ne	ne	ne	ne	ne	ne	ne
3		Hodnota aktiva	Původní rizika	Četnost								
4				Dopad								
5				Celkové riziko								
6			Redukovaná rizika	Protipatření								
7				Celkové riziko								
8				Vybráno								
9	5.1.1	Dokument bezpečnostní politiky informací		0	0	0	0	0	0	0	0	0
10	5.1.2	Přezkoumání bezpečnostní politiky informací		0	0	0	0	0	0	0	0	0
11	6.1.1	Závazek vedení směrem k bezpečnosti informací		0	0	0	0	0	0	0	0	0
12	6.1.2	Koordinace bezpečnosti informací		0	0	0	0	0	0	0	0	0
13	6.1.3	Přidělení odpovědnosti v oblasti informační bezpečnosti		0	0	0	0	0	0	0	0	0
14	6.1.4	Schvalovací proces prostředků zpracování informací		0	0	0	0	0	0	0	0	0
15	6.1.5	Dohody o ochraně důvěrných informací		0	0	0	0	0	0	0	0	0
16	6.1.6	Kontakt s orgány veřejné správy		0	0	0	0	0	0	0	0	0
17	6.1.7	Kontakt se zájmovými skupinami		0	0	0	0	0	0	0	0	0
18	6.1.8	Nezávislá přezkoumání bezpečnosti informací		0	0	0	0	0	0	0	0	0
19	6.2.1	Identifikace rizik vyplývajících z přístupu externích subjektů		0	0	0	0	0	0	0	0	0
20	6.2.2	Bezpečnostní požadavky pro přístup klientů		0	0	0	0	0	0	0	0	0
21	6.2.3	Bezpečnostní požadavky v dohodách se třetí stranou		0	0	0	0	0	0	0	0	0
22	7.1.1	Evidence aktiv		0	0	0	0	0	0	0	0	0
23	7.1.2	Vlastnictví aktiv		0	0	0	0	0	0	0	0	0
24	7.1.3	Přípustné použití aktiv		0	0	0	0	0	0	0	0	0
25	7.2.1	Doporučení pro klasifikaci		0	0	0	0	0	0	0	0	0
26	7.2.2	Označování a zacházení s informacemi		0	0	0	0	0	0	0	0	0
27	8.1.1	Role a odpovědnosti		0	0	0	0	0	0	0	0	0
28	8.1.2	Prověřování		0	0	0	0	0	0	0	0	0
29	8.1.3	Podmínky výkonu pracovní činnosti		0	0	0	0	0	0	0	0	0

Obr. 7 Vzorový list - sloupce hrozby [vlastní]

Přehled hrozeb a relevantních opatření

		Hrozby	J	K	L	M	N	O	P	Q	R	S	T	U
			1.7	2.1	2.2	2.3	2.4	2.5	2.6	2.7	3.1	3.2	3.3	3.4
1	Opatření													
2	5.1.1 Dokument bezpečnostní politiky informací							1	1					
3	5.1.2 Přezkoumání bezpečnostní politiky informací							1	1					
4	6.1.1 Závazek vedení směrem k bezpečnosti informací							1	1	1				
5	6.1.2 Koordinace bezpečnosti informací							1	1					
6	6.1.3 Přidělení odpovědnosti v oblasti informační bezpečnosti							1	1	1	1	1	1	
7	6.1.4 Schvalovací proces prostředků zpracování informací							1						
8	6.1.5 Dohody o ochraně důvěrných informací			1										
9	6.1.6 Kontakt s orgány veřejné správy		1						1					
10	6.1.7 Kontakt se zájmovými skupinami			1					1					
11	6.1.8 Nezávislá přezkoumání bezpečnosti informací							1	1	1				
12	6.2.1 Identifikace rizik vyplývajících z přístupu externích subjektů													
13	6.2.2 Bezpečnostní požadavky pro přístup klientů			1				1						
14	6.2.3 Bezpečnostní požadavky v dohodách se třetí stranou			1				1						
15	7.1.1 Evidence aktiv						1						1	
16	7.1.2 Vlastnictví aktiv			1			1						1	
17	7.1.3 Přípustné použití aktiv					1	1						1	
18	7.2.1 Doporučení pro klasifikaci						1							

Obr. 8 List Hrozby – sloupce hrozby [vlastní]

7.2.1.3 Hrozby

Do řádků listu Podklady, počínaje řádkem 6, jsou vkládány hodnoty jednotlivých hrozeb pro každé aktivum. Do prvního sloupce ve skupině, nadepsaného Č, je vkládána hodnota četnosti hrozby v rozsahu 1 – 5. Do druhého sloupce ve skupině, nadepsaného D, je vkládána hodnota dopadu hrozby v rozsahu 1 – 5.

Microsoft Excel - Triangl.xls																			
Soubor Úpravy Zobrazit Vložit Formát Nástroje Data Okno Nápověda																			
Vložit jinak...																			
100%																			
Arial																			
B I																			
Aktiva																			
A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
	Aktiva																		
1																			
2	Dostupnost		V			S			S			V			S				
3	Důvěrnost		V			S			N			V			N				
4	Integrita		D			N			N			S			V				
5		Č	D	P	Č	D	P	Č	D	P	Č	D	P	Č	D	P	Č	D	P
6	1.1 Hrozba 1.1	1	5	1	1	4	2	1	3	2	1	4	1	1	5	1			
7	1.2 Hrozba 1.2	1	5	1	1	4	2	1	3	2	1	4	1	1	3	1			
8	1.3 Hrozba 1.3	1	5	1	1	4	2	1	3	2	1	4	1						
9	1.4 Hrozba 1.4	1	5	1	1	4	2	1	3	2	1	4	1						
10	1.5 Hrozba 1.5	1	5	1	1	4	2	1	3	2	1	4	1						
11	1.6 Hrozba 1.6	1	5	1	1	4	2	1	3	2	1	4	1	3	3	2			
12	1.7 Hrozba 1.7	1	5	1	1	4	2	1	3	2	1	4	1						
13	2.1 Hrozba 2.1	2	4	2	1	3	2	1	2	2	2	3	2						
14	2.2 Hrozba 2.2	2	3	2	2	2	2	2	2	2	2	3	2	2	5	2			
15	2.3 Hrozba 2.3	1	3	2	1	2	2	3	2	3	1	3	2						
16	2.4 Hrozba 2.4	1	2	1	1	2	1	3	2	3	1	2	1						
17	2.5 Hrozba 2.5	3	2	2	3	3	3	4	3	3	3	2	2	3	2	2			
18	2.6 Hrozba 2.6	3	3	2	3	3	3	5	3	4	3	3	2	2	2	3			
19	2.7 Hrozba 2.7	4	4	3	3	3	3	3	2	3	4	4	3	3	3	2			
20	3.1 Hrozba 3.1	3	4	2	3	4	2	3	4	2	3	4	2	1	4	1			
21	3.2 Hrozba 3.2	3	3	1	3	3	1	3	3	1	3	3	1						
22	3.3 Hrozba 3.3	5	2	2	5	2	2	5	2	2	5	2	2						
23	3.4 Hrozba 3.4	3	3	3	3	3	3	3	3	3	3	3	3	1	4	2			

Obr. 9 List Podklady – vkládání hodnot četnost a dopad [vlastní]

7.2.1.4 Zranitelnost a protiopatření

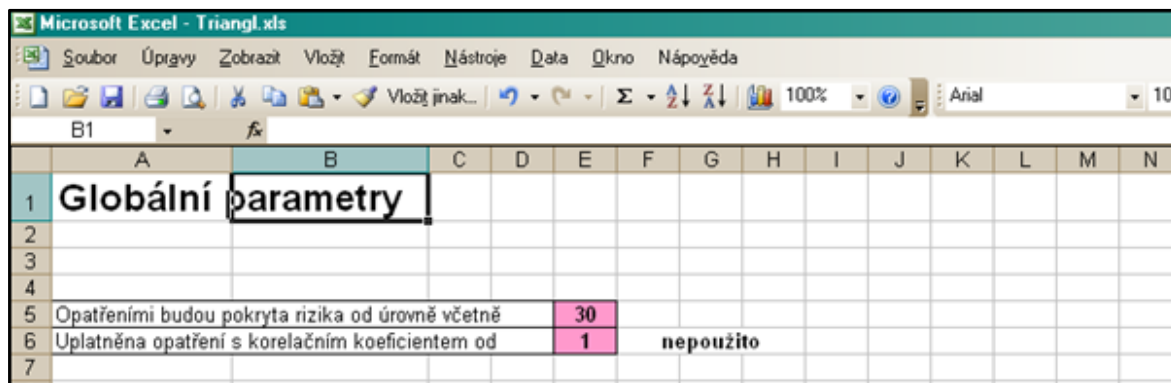
Do třetího sloupce ve skupině pro každé aktivum je vkládána hodnota účinnosti protiopatření v rozsahu 1 – 5.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
		Aktiva	Aktivum 1			Aktivum 2			Aktivum 3			Aktivum 4			Aktivum 5			
1																		
2		Dostupnost		V			S			S			V			S		
3		Důvěrnost		V			S			N			V			N		
4		Integrita		S			N			N			S			V		
5			Č	D	P	Č	D	P	Č	D	P	Č	D	P	Č	D	P	Č
6	1.1	Hrozba 1.1	1	5	1	1	4	2	1	3	2	1	4	1	1	5	1	
7	1.2	Hrozba 1.2	1	5	1	1	4	2	1	3	2	1	4	1	1	3	1	
8	1.3	Hrozba 1.3	1	5	1	1	4	2	1	3	2	1	4	1				
9	1.4	Hrozba 1.4	1	5	1	1	4	2	1	3	2	1	4	1				
10	1.5	Hrozba 1.5	1	5	1	1	4	2	1	3	2	1	4	1				
11	1.6	Hrozba 1.6	1	5	1	1	4	2	1	3	2	1	4	1	3	3	2	
12	1.7	Hrozba 1.7	1	5	1	1	4	2	1	3	2	1	4	1				
13	2.1	Hrozba 2.1	2	4	2	1	3	2	1	2	2	2	3	2				
14	2.2	Hrozba 2.2	2	3	2	2	2	2	2	2	2	2	3	2	2	5	2	
15	2.3	Hrozba 2.3	1	3	2	1	2	2	3	2	3	1	3	2				
16	2.4	Hrozba 2.4	1	2	1	1	2	1	3	2	3	1	2	1				
17	2.5	Hrozba 2.5	3	2	2	3	3	3	4	3	3	3	2	2	3	2	2	
18	2.6	Hrozba 2.6	3	3	2	3	3	3	5	3	4	3	3	2	2	2	3	
19	2.7	Hrozba 2.7	4	4	3	3	3	3	3	2	3	4	4	3	3	3	2	
20	3.1	Hrozba 3.1	3	4	2	3	4	2	3	4	2	3	4	2	1	4	1	
21	3.2	Hrozba 3.2	3	3	1	3	3	1	3	3	1	3	3	1				
22	3.3	Hrozba 3.3	5	2	2	5	2	2	5	2	2	5	2	2				
23	3.4	Hrozba 3.4	3	3	3	3	3	3	3	3	3	3	3	3	1	4	2	

Obr. 10 List Podklady – vkládání hodnot protiopatření [vlastní]

7.2.2 Stanovení prahové hodnoty

Klíčovým parametrem pro výběr opatření k pokrytí rizik je prahová hodnota, uvedená na listu Parametry. Pouze rizika vyšší nebo rovná této hodnotě budou pokrývána opatřeními. Nižší rizika jsou považována za zbytková a nejsou jim přiřazována opatření.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	Globální parametry													
2														
3														
4														
5	Opatřeními budou pokryta rizika od úrovně včetně				30									
6	Uplatněna opatření s korelačním koeficientem od				1	nepoužito								
7														

Obr. 11 List Parametry – stanovení úrovně pokrytí rizik [vlastní]

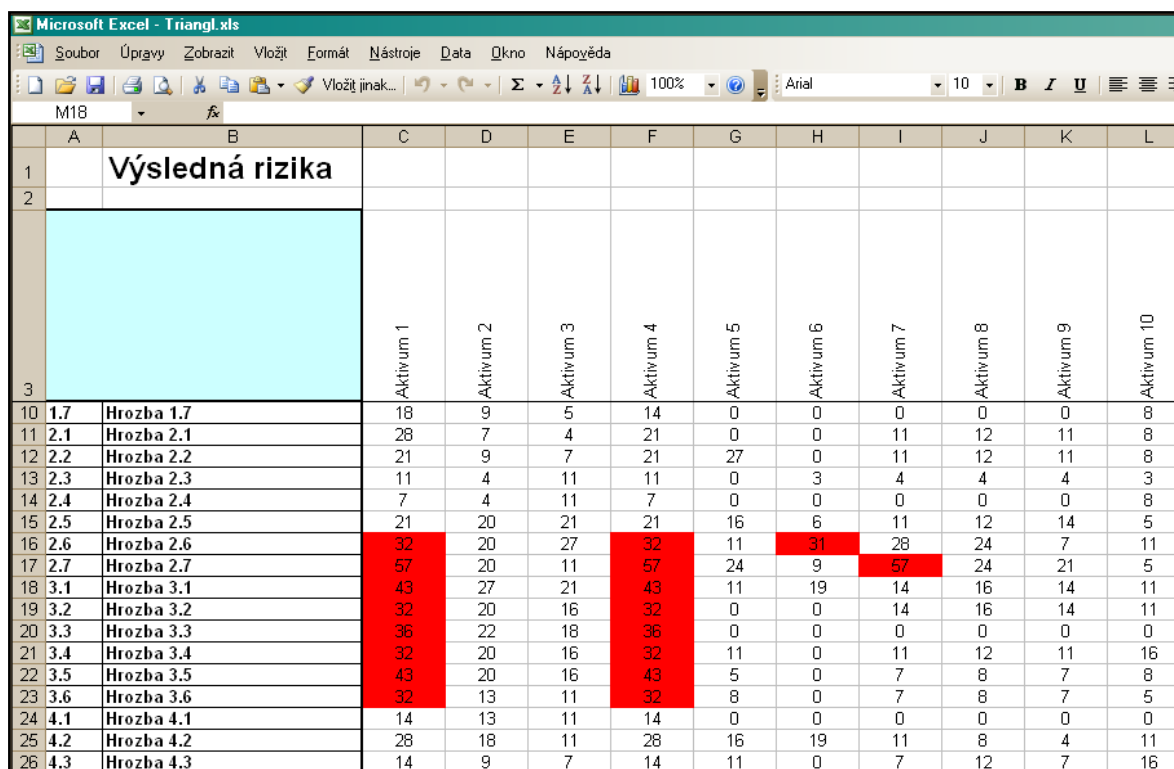
7.2.3 Zpracování

Míru rizika spočítá softwarový nástroj pro všechny kombinace aktiv a hrozeb při běhu programového modulu, spuštěného tlačítkem Vytvoří se listy aktiv na listu Podklady. Při tomto běhu je pro každé aktivum vytvořen samostatný list, obsahující v řádcích 3, 4 zjištěné hodnoty, v řádku 6 spočtenou míru rizika. Ve sloupci D (Vybráno) je kumulativní údaj, který popisuje váhu opatření. Aktivací automatického filtru v buňce D8 lze zobrazit jen vybraná nebo jen nevybraná opatření. Tyto údaje jsou dále používány v procesu výběru opatření.

	A	B	C	D	E	F	G	H	I	J
1	Infrastruktura			Hrozba	Zemětřesení	Povodně	Hurkán	Blesk	Průmyslová akce	Bombový útok
2				Relevantní	ne	ne	ano	ano	ne	ne
3				Četnost			1	1		
4				Dopad			5	3		
5				Protiopatření			3	3		
6				Celkové riziko			105	63		
7				Vybráno						
8	5.1.1	Dokument bezpečnostní politiky informací		175	0	0	105	0	0	0
9	5.1.2	Přezkoumání bezpečnostní politiky informací		0	0	0	0	0	0	0
10	6.1.1	Závazek vedení směrem k bezpečnosti informací		0	0	0	0	0	0	0
11	6.1.2	Koordinace bezpečnosti informací		56	0	0	0	0	0	0
12	6.1.3	Přidělení odpovědnosti v oblasti informační bezpečnosti		0	0	0	0	0	0	0
13	6.1.4	Schvalovací proces prostředků zpracování		147	0	0	0	0	0	0
14	6.1.5	Dohody o ochraně důvěrných informací		0	0	0	0	0	0	0
15	6.1.6	Kontakt s orgány veřejné správy		161	0	0	105	0	0	0
16	6.1.7	Kontakt se zájmovými skupinami		0	0	0	0	0	0	0
17	6.1.8	Nezávislá přezkoumání bezpečnosti informací		0	0	0	0	0	0	0
18	6.2.1	Identifikace rizik plynoucích z přístupu externích subjektů		203	0	0	0	0	0	0
19	6.2.2	Bezpečnostní požadavky pro přístup klientů		0	0	0	0	0	0	0
20	6.2.3	Bezpečnostní požadavky v dohodách se třetí		0	0	0	0	0	0	0
21	7.1.1	Evidence aktiv		133	0	0	0	63	0	0
22	7.1.2	Vlastnictví aktiv		133	0	0	0	63	0	0
23	7.1.3	Přípustné použití aktiv		0	0	0	0	0	0	0
24	7.2.1	Doporučení pro klasifikaci		0	0	0	0	0	0	0
25	7.2.2	Označování a zacházení s informacemi		0	0	0	0	0	0	0
26	8.1.1	Role a odpovědnosti		0	0	0	0	0	0	0
27	8.1.2	Prověřování		0	0	0	0	0	0	0
28	8.1.3	Podmínky výkonu pracovní činnosti		0	0	0	0	0	0	0
29	8.2.1	Odpovědnosti vedoucích zaměstnanců		0	0	0	0	0	0	0
30	8.2.2	Informovanost, vzdělávání a školení v oblasti bezpečnosti informací		0	0	0	0	0	0	0
31	8.2.3	Disciplinární řízení		70	0	0	0	0	0	0
32	8.3.1	Odpovědnosti při ukončení pracovního vztahu		0	0	0	0	0	0	0
33	8.3.2	Navrácení zapůjčených prostředků		0	0	0	0	0	0	0
34	8.3.3	Odebrání přístupových práv		0	0	0	0	0	0	0
35	9.1.1	Fyzický bezpečnostní perimetr		147	0	0	0	0	0	0
36	9.1.2	Fyzické kontroly vstupu osob		70	0	0	0	0	0	0

Obr. 12 List Aktiva [vlastní]

Výsledná rizika jsou přehledně zobrazena na listu Rizika, přičemž rizika rovná nebo vyšší než stanovená úroveň jsou barevně zvýrazněna. Červenou barvou jsou zvýrazněna rizika, která i po snížení opatřeními přesahují prahovou hodnotu.



	A	B	C	D	E	F	G	H	I	J	K	L
1		Výsledná rizika										
2												
3												
			Aktivum 1	Aktivum 2	Aktivum 3	Aktivum 4	Aktivum 5	Aktivum 6	Aktivum 7	Aktivum 8	Aktivum 9	Aktivum 10
10	1.7	Hrozba 1.7	18	9	5	14	0	0	0	0	0	8
11	2.1	Hrozba 2.1	28	7	4	21	0	0	11	12	11	8
12	2.2	Hrozba 2.2	21	9	7	21	27	0	11	12	11	8
13	2.3	Hrozba 2.3	11	4	11	11	0	3	4	4	4	3
14	2.4	Hrozba 2.4	7	4	11	7	0	0	0	0	0	8
15	2.5	Hrozba 2.5	21	20	21	21	16	6	11	12	14	5
16	2.6	Hrozba 2.6	32	20	27	32	11	31	28	24	7	11
17	2.7	Hrozba 2.7	57	20	11	57	24	9	57	24	21	5
18	3.1	Hrozba 3.1	43	27	21	43	11	19	14	16	14	11
19	3.2	Hrozba 3.2	32	20	16	32	0	0	14	16	14	11
20	3.3	Hrozba 3.3	36	22	18	36	0	0	0	0	0	0
21	3.4	Hrozba 3.4	32	20	16	32	11	0	11	12	11	16
22	3.5	Hrozba 3.5	43	20	16	43	5	0	7	8	7	8
23	3.6	Hrozba 3.6	32	13	11	32	8	0	7	8	7	5
24	4.1	Hrozba 4.1	14	13	11	14	0	0	0	0	0	0
25	4.2	Hrozba 4.2	28	18	11	28	16	19	11	8	4	11
26	4.3	Hrozba 4.3	14	9	7	14	11	0	7	12	7	16

Obr. 13 List Rizika [vlastní]

Vybraná opatření pro všechna aktiva jsou shrnuta v listu Vybraná opatření. Ve sloupci C je kumulativní údaj, zda bylo opatření vybráno a jeho váha. Tento údaj lze tam, kde je to praktické, použít jako podklad k rozhodnutí o aplikaci opatření pouze na některá aktiva. Pokud opatření nebylo vybráno, obsahuje příslušná buňka text „ne“.

Microsoft Excel - Triangl.xls								
Soubor Úpravy Zobrazení Vložit Formát Nástroje Data Okno Nápověda								
Vložit jinak...								
100%								
Arial								
B I U								
A1								
A	B	C	D	E	F	G	H	I
1	Vybraná opatření							
2								
3			Vybraná opatření					
4	5.1.1	Dokument bezpečnostní politiky informací	19	Aktivum 1	Aktivum 2	Aktivum 3	Aktivum 4	Aktivum 5
5	5.1.2	Přezkoumání bezpečnostní politiky informací	19	4	2	0	4	0
6	6.1.1	Závazek vedení směrem k bezpečnosti informací	6	2	0	0	2	0
7	6.1.2	Koordinace bezpečnosti informací	10	2	1	0	2	0
8	6.1.3	Přidělení odpovědnosti v oblasti informační bezpečnosti	19	8	1	0	8	0
9	6.1.4	Schvalovací proces prostředků zpracování informací	12	3	1	1	3	0
10	6.1.5	Dohody o ochraně důvěrných informací	12	3	2	0	3	0
11	6.1.6	Kontakt s orgány veřejné správy	3	1	0	0	1	0
12	6.1.7	Kontakt se zájmovými skupinami	9	4	0	0	4	0
13	6.1.8	Nezávislá přezkoumání bezpečnosti informací	14	5	0	0	5	0
14	6.2.1	Identifikace rizik vyplývajících z přístupu externích subjektů	19	4	2	1	4	0
15	6.2.2	Bezpečnostní požadavky pro přístup klientů	7	1	1	0	1	0
16	6.2.3	Bezpečnostní požadavky v dohodách se třetí stranou	18	4	2	1	4	0
17	7.1.1	Evidence aktiv	18	5	2	0	5	0
18	7.1.2	Vlastnictví aktiv	18	5	2	0	5	0
19	7.1.3	Přípustné použití aktiv	18	5	2	0	5	0
20	7.2.1	Doporučení pro klasifikaci	13	3	1	0	3	0

Obr. 14 List Vybraná opatření [vlastní]

7.2.4 Příprava prohlášení o aplikovatelnosti

Po vyhodnocení rizik a doporučení opatření nástroj vytvoří na listu Prohlášení o aplikovatelnosti textové podklady pro přípravu Prohlášení o aplikovatelnosti a Plánu zvládání rizik.

Prohlášení o aplikovatelnosti			
Skupina / Cíl / Opatření	Vybrán	Pokryvá rizika plynoucí z:	Redukuje působení hrozby:
5.1 Bezpečnostní politika informací	ano		
5.1.1 Dokument bezpečnostní politiky informací	ano	hrozby Hrozba 2.6 vůči aktivu Aktivum 1; hrozby Hrozba 5.1 vůči aktivu Aktivum 1; hrozby Hrozba 5.2 vůči aktivu Aktivum 1; hrozby Hrozba 5.13 vůči aktivu Aktivum 1; hrozby Hrozba 5.1 vůči aktivu Aktivum 2; hrozby Hrozba 5.2 vůči aktivu Aktivum 2; hrozby Hrozba 2.6 vůči aktivu Aktivum 4; hrozby Hrozba 5.1 vůči aktivu Aktivum 4; hrozby Hrozba 5.2 vůči aktivu Aktivum 4; hrozby Hrozba 5.13 vůči aktivu Aktivum 4; hrozby Hrozba 2.6 vůči aktivu Aktivum 6; hrozby Hrozba 5.1 vůči aktivu Aktivum 6; hrozby Hrozba 5.2 vůči aktivu Aktivum 6; hrozby Hrozba 5.1 vůči aktivu Aktivum 7; hrozby Hrozba 5.2 vůči aktivu Aktivum 7; hrozby Hrozba 5.1 vůči aktivu Aktivum 8; hrozby Hrozba 5.2 vůči aktivu Aktivum 8; hrozby Hrozba 5.1 vůči aktivu Aktivum 9; hrozby Hrozba 5.2 vůči aktivu Aktivum 9	Hrozba 2.6 vůči aktivu Aktivum 1, Aktivum 4, Aktivum 6; Hrozba 5.1 vůči aktivu Aktivum 1, Aktivum 2, Aktivum 4, Aktivum 6, Aktivum 7, Aktivum 8, Aktivum 9; Hrozba 5.2 vůči aktivu Aktivum 1, Aktivum 2, Aktivum 4, Aktivum 6, Aktivum 7, Aktivum 8, Aktivum 9; Hrozba 5.13 vůči aktivu Aktivum 1, Aktivum 4
5.1.2 Přezkoumání bezpečnostní politiky informací	ano	hrozby Hrozba 2.6 vůči aktivu Aktivum 1; hrozby Hrozba 2.7 vůči aktivu Aktivum 1; hrozby Hrozba 2.6 vůči aktivu Aktivum 4; hrozby Hrozba 2.7 vůči aktivu Aktivum 4; hrozby Hrozba 2.6 vůči aktivu Aktivum 6; hrozby Hrozba 2.7 vůči aktivu Aktivum 7	Hrozba 2.6 vůči aktivu Aktivum 1, Aktivum 4, Aktivum 6; Hrozba 2.7 vůči aktivu Aktivum 1, Aktivum 4, Aktivum 7
6 Organizace bezpečnosti informací	ano		
6.1 Interní organizace	ano		
6.1.1 Závazek vedení směrem k bezpečnosti informací	ano	hrozby Hrozba 2.6 vůči aktivu Aktivum 1; hrozby Hrozba 5.1 vůči aktivu Aktivum 1; hrozby Hrozba 5.1 vůči aktivu Aktivum 2; hrozby Hrozba 2.6 vůči aktivu Aktivum 4; hrozby Hrozba 5.1 vůči aktivu Aktivum 4; hrozby Hrozba 2.6 vůči aktivu Aktivum 6; hrozby Hrozba 5.1 vůči aktivu Aktivum 7; hrozby Hrozba 5.1 vůči aktivu Aktivum 8; hrozby Hrozba 5.1 vůči aktivu Aktivum 9	Hrozba 2.6 vůči aktivu Aktivum 1, Aktivum 4, Aktivum 6; Hrozba 5.1 vůči aktivu Aktivum 1, Aktivum 2, Aktivum 4, Aktivum 6, Aktivum 7, Aktivum 8, Aktivum 9
6.1.2 Koordinace bezpečnosti informací	ano	hrozby Hrozba 2.6 vůči aktivu Aktivum 1; hrozby Hrozba 2.7 vůči aktivu Aktivum 1; hrozby Hrozba 3.1 vůči aktivu Aktivum 1; hrozby Hrozba 3.2 vůči aktivu Aktivum 1; hrozby Hrozba 3.3 vůči aktivu Aktivum 1; hrozby Hrozba 5.3 vůči aktivu Aktivum 1; hrozby Hrozba 5.12 vůči aktivu Aktivum 1; hrozby Hrozba 5.13 vůči aktivu Aktivum 1; hrozby Hrozba 5.3 vůči aktivu Aktivum 2; hrozby Hrozba 2.6 vůči aktivu Aktivum 4; hrozby Hrozba 2.7 vůči aktivu Aktivum 4; hrozby Hrozba 3.1 vůči aktivu Aktivum 4; hrozby Hrozba 3.2 vůči aktivu Aktivum 4; hrozby Hrozba 3.3 vůči aktivu Aktivum 4; hrozby Hrozba 5.3 vůči aktivu Aktivum 4; hrozby Hrozba 5.12 vůči aktivu Aktivum 4; hrozby Hrozba 5.13 vůči aktivu Aktivum 4; hrozby Hrozba 2.6 vůči aktivu Aktivum 6; hrozby Hrozba 2.7 vůči aktivu Aktivum 7	Hrozba 2.6 vůči aktivu Aktivum 1, Aktivum 4, Aktivum 6; Hrozba 2.7 vůči aktivu Aktivum 1, Aktivum 4, Aktivum 7; Hrozba 3.1 vůči aktivu Aktivum 1, Aktivum 4; Hrozba 3.2 vůči aktivu Aktivum 1, Aktivum 4; Hrozba 3.3 vůči aktivu Aktivum 1, Aktivum 4; Hrozba 5.3 vůči aktivu Aktivum 1, Aktivum 2, Aktivum 4; Hrozba 5.12 vůči aktivu Aktivum 1, Aktivum 4; Hrozba 5.13 vůči aktivu Aktivum 1, Aktivum 4
6.1.3 Přidělení odpovědnosti v oblasti informační bezpečnosti	ano	hrozby Hrozba 4.6 vůči aktivu Aktivum 1; hrozby Hrozba 5.14 vůči aktivu Aktivum 1; hrozby Hrozba 5.15 vůči aktivu Aktivum 1; hrozby Hrozba 5.14 vůči aktivu Aktivum 2; hrozby Hrozba 5.14 vůči aktivu Aktivum 3; hrozby Hrozba 4.6 vůči aktivu Aktivum 4; hrozby Hrozba 5.14 vůči aktivu Aktivum 4; hrozby Hrozba 5.15 vůči aktivu Aktivum 4; hrozby Hrozba 5.14 vůči aktivu Aktivum 7; hrozby Hrozba 5.15 vůči aktivu Aktivum 7; hrozby Hrozba 5.14 vůči aktivu Aktivum 8; hrozby Hrozba 5.15 vůči aktivu Aktivum 8	Hrozba 4.6 vůči aktivu Aktivum 1, Aktivum 4; Hrozba 5.14 vůči aktivu Aktivum 1, Aktivum 2, Aktivum 3, Aktivum 4, Aktivum 7, Aktivum 8; Hrozba 5.15 vůči aktivu Aktivum 1, Aktivum 4, Aktivum 7, Aktivum 8

Obr. 15 List Prohlášení o aplikovatelnosti [vlastní]

8 METODIKA ANALÝZY RIZIK

8.1 Úvodní ustanovení

8.1.1 Účel

Tato kapitola popisuje návrh metodiky procesu řízení rizik pro Společnost a.s.

8.1.2 Metodika

Požadavky na metodiku procesu řízení rizik vyplývají zejména z vyhlášky ČNB č. 163/2014 Sb. a relevantních technických standardů - ČSN ISO/IEC 27001, 27002, 27005.

8.1.3 Hranice analýzy rizik

Metodika procesu řízení rizik bude aplikována pro Společnost a. s.. Hranice analýzy rizik mohou být upřesněny takto:

1. Z hlediska organizační struktury.
 - Všechny organizační jednotky společnosti.
2. Z hlediska hlavních procesů (činností).
 - Všechny procesy společnosti.
3. Z hlediska místa dislokace (lokality).
 - Dle sídla společnosti a všech ostatních lokalit.
4. Z hlediska informačních technologií.
 - Veškeré technologie ICT využívané ve společnosti.
5. Z hlediska služeb externích subjektů.
 - Dodavatelé ICT služeb a technologií.
6. Z hlediska informačních systémů (tj. služeb koncovému uživateli).
 - Všechny komponenty informačního systému společnosti.

8.2 Provedení analýzy rizik s využitím metodiky řízení rizik

8.2.1 Proces analýzy rizik

Proces analýzy rizik (dále též jen AR) je součástí managementu rizik jako jednoho z důležitých procesů systému řízení bezpečnosti informací ISMS.

Proces analýzy rizik v oblasti informační bezpečnosti je nutno chápat jako základní analytický podklad ke všem návazným analýzám a návrhům týkajících se dané oblasti.

8.2.2 Vstupy do procesu AR v oblasti ISMS

Vstupy do procesu AR jsou především:

- informace od vlastníků komponent a aktiv;
- hranice analýzy aktiv;
- obecné definice politik a strategií.

8.2.3 Výstupy procesu AR v oblasti ISMS

Výstupy procesu AR jsou:

- model informačního systému;
- seznam komponent zahrnující identifikaci vlastníků komponent;
- seznam aktiv (inventura aktiv) zahrnující identifikaci vlastníků aktiv a jejich hodnocení;
- seznam relevantních hrozeb, jejich hodnocení, včetně identifikace protipatření a hodnocení míry rizika;
- definice kritérií pro akceptaci rizik a variant pro zvládání rizik.

8.2.4 Role AR v oblasti ISMS

Vlastník komponenty: Osoba, která je odpovědná za komponentu v rámci procesu analýzy aktiv. Vlastník musí být schopen posuzovat relevantně komponentu, nemusí být fyzickým či organizačním vlastníkem aktiv komponenty. Vlastník komponenty odpovídá zejména za:

- hodnocení dopadů incidentu v rámci analýzy dopadů incidentu.

V procesu AR bude vlastníkem komponenty typicky vedoucí příslušné organizační jednotky nebo jím pověřený pracovník, případně příslušný (aplikační, či systémový) správce.

Identifikaci relevantních aktiv, určení vlastníků aktiv a především hodnocení v rámci analýzy dopadů bude provádět vlastník komponenty s využitím podkladů od identifikovaných odpovědných pracovníků.

Vlastník aktiva: Osoba, která je odpovědná za aktivum v rámci procesu analýzy aktiv. Vlastník musí být schopen posuzovat relevantně aktivum, nemusí být fyzickým či organizačním vlastníkem aktiva. Vlastník aktiva odpovídá zejména za:

- hodnocení aktiva,
- odhad hrozeb příslušných k danému aktivu,
- odhad frekvence hrozeb,
- odhad zranitelnosti aktiva,
- identifikaci stávajících protiopatření,
- odhad účinnosti protiopatření.

8.3 Analýza rizik

Analýza aktiv

8.3.1 Stanovení hranic analýzy aktiv

Vlastní analýze aktiv musí předcházet stanovení hranic analýzy aktiv. Pečlivá definice hranic v tomto stádiu znamená, že se vyhneme zbytečné práci a zvýšíme kvalitu analýzy aktiv. Popis hranic jasně určí, co je nezbytné při provádění analýzy aktiv z dále uvedených prvků zohlednit.

8.3.2 Identifikace komponent a stanovení hranic analýzy aktiv

Identifikace a hodnocení komponent vyžaduje nalézt a určit hranice komponent a organizační odpovědnost. Určit hranice komponent - komplexních systémů, systémů propojených sítěmi a podobně je relativně komplikované.

Komponentu identifikujeme tak, že definujeme hranice okolo skupiny procesů, komunikací, datových úložišť a příslušejících zdrojů. Elementy uvnitř těchto hranic vytvářejí jednotlivý systém, vyžadující samostatná systémová bezpečnostní pravidla a nové vyhodnocení bezpečnosti, jakmile dojde k větší modifikaci systému. Každý element systému by měl být:

- být pod tímtož přímým řízením;
- mít tutéž funkčnost nebo účel činnosti;
- mít v podstatě tytéž funkční charakteristiky a bezpečnostní potřeby;
- být umístěn v tomtéž obecném provozním prostředí.

8.3.2.1 Model informačního systému – identifikace komponent

Systém zpracování informací od jejich vzniku až po jejich likvidaci, či předání (dále též jen **informační systém**) bude v tomto kroku rozdělen na komponenty. Pozn.: Informační systém v tomto smyslu zahrnuje všechna zpracování informací - nejen zpracování informací v elektronické podobě, ale také např. zpracování informací v listinné podobě a podobně.

Komponenta vyjadřuje procesní pohled na informační systém. Pojem komponenta zahrnuje i tzv. aktivum primární. Komponentami jsou obvykle hlavní procesy a informace.

V rámci AR budou identifikovány zejména následující typy komponent:

1. Informační aktiva – informace a související datové zdroje.
2. Služby IT – informační a komunikační služby pro podporu činností koncových uživatelů.
3. Znalosti.

I. krok AR – Identifikace komponent

Informační systém organizace (včetně informačních a komunikačních technologií a sw aplikací) je na základě stanovení hranic analýzy aktiv rozdělen na komponenty – je vytvořen tzv. model informačního systému organizace.

Každé komponentě je přiřazen vlastník komponenty.

V procesu AR bude vlastníkem komponenty typicky vedoucí příslušné organizační jednotky, nebo jím pověřený pracovník, případně příslušný (aplikační, či systémový) správce. Identifikaci relevantních aktiv, určení vlastníků aktiv a především hodnocení v rámci analýzy dopadů bude provádět vlastník komponenty s využitím podkladů od identifikovaných odpovědných pracovníků.

8.3.2.2 Analýza dopadů incidentu (*Business Impact Analysis, BIA*)

Analýza dopadů incidentu (Business Impact Analysis, BIA) je hodnocením dopadů bezpečnostních incidentů, které se projeví ztrátou dostupnosti, integrity či důvěrnosti do fungování organizace. Tato analýza je součástí analýzy aktiv.

I. 1. krok AR - Analýza dopadů incidentu

Vlastník komponenty hodnotí dopady incidentů důvěrnosti, dostupnosti a integrity dat.

Hodnocení incidentu vlastník komponenty provede přiřazením stupně z číselníku uvedeného v Příloze P V.

Při hodnocení dopadů incidentu je potřeba mj. posoudit následující klíčové atributy:

1. Míra podílu osobních údajů nebo obchodního tajemství,
2. Rozsah dotčených právních povinností či jiných závazků,
3. Rozsah narušení vnitřních řídicích a kontrolních činností,
4. Poškození veřejných, obchodních či ekonomických zájmů,
5. Možné finanční ztráty,
6. Rozsah narušení běžných činností povinné osoby,
7. Dopady na ztrátu dobrého jména či dobré pověsti.

8.3.3 Identifikace a hodnocení aktiv

Aktivum

Je část celkového systému, které organizace přímo přiřazuje hodnotu a pro kterou tudíž organizace požaduje ochranu. Při identifikaci aktiv by mělo být vzato v úvahu, že informační systém organizace tvoří jen hardware a software. Informační systém se skládá z aktiv.

Všechna aktiva uvnitř stanovených hranic analýzy aktiv musí být identifikována. Hranici analýzy stanovuje vedení společnosti prostřednictvím BIA analýzy.

Cílem identifikace aktiv je vytvoření úplného seznamu aktiv. Následně by měly být těmto aktivům přiřazeny hodnoty. Tyto hodnoty reprezentují význam aktiv pro činnost organizace. To je možné vyjádřit ve smyslu bezpečnostních problémů, jako jsou potenciální nepříznivé dopady na činnost organizace plynoucí ze zpřístupnění, modifikace, nedostupnosti a/nebo zničení informací a dalších aktiv informačního systému. Tak se identifikace a ohodnocení aktiv založené na potřebách činnosti organizace stává hlavním faktorem

při determinaci rizik. Pozn. analýza aktiv je předpokladem pro provedení tzv. analýzy rizik.

Hodnocení aktiv

Vstupní údaje pro hodnocení aktiv by měly být zajištěny vlastníky a uživateli aktiv. Přiřazené hodnoty by se měly vztahovat k nákladům na pořízení a udržování aktiva, na potenciální nepříznivé dopady na činnost organizace plynoucí ze ztráty důvěrnosti, integrity, dostupnosti, individuální odpovědnosti, autenticity a spolehlivosti. Každé z identifikovaných aktiv by mělo mít pro organizaci určitou hodnotu.

V procesu AR bude vlastníkem aktiva typicky příslušný (aplikační, či systémový) správce. Ocenění aktiva a další hodnocení bude provádět vlastník aktiva s využitím podkladů od identifikovaných odpovědných pracovníků.

Při hodnocení aktiv je potřeba posoudit následující klíčové atributy:

1. Míra podílu osobních údajů nebo obchodního tajemství.
2. Rozsah dotčených právních povinností či jiných závazků.
3. Rozsah narušení vnitřních řídicích a kontrolních činností.
4. Poškození veřejných, obchodních či ekonomických zájmů.
5. Možné finanční ztráty.
6. Rozsah narušení běžných činností povinné osoby.
7. Dopady na ztrátu dobrého jména či dobré pověsti.

II. krok AR – Identifikace aktiv

V tomto kroku jsou identifikována aktiva, jejich příslušnost ke komponentám, jejich typ a jejich vlastníci.

Typologie aktiv je uvedena v Příloze P I.

III. krok AR – Hodnocení aktiv

Hodnota aktiv je stanovována vlastníkem v relativní stupnici s využitím číselníku hodnot aktiv, který je uveden v Příloze P II.

Pro stanovení hodnoty aktiva lze využít doporučení pro hodnocení jednotlivých typů aktiv uvedené v Příloze P III.

Analýza rizik

8.3.4 Odhad hrozeb

Hrozba představuje možnost poškodit zkoumaný IS a jeho aktiva. V případě jejího výskytu působí na IS v tom smyslu, že je příčinou nežádoucích incidentů a tudíž nepříznivých dopadů.

Hrozba je síla, událost nebo aktivita osoby, která má nežádoucí vliv na bezpečnost organizace nebo může způsobit škodu na jejích aktivech. Hrozby mohou být přírodního, technického nebo lidského původu, a mohou být náhodné nebo úmyslné (hrozbou může být např. požár, přírodní katastrofa, krádež zařízení, získání přístupu k informacím neo-právněnou osobou, chyba obsluhy apod.). Měly by být identifikovány zdroje jak náhodných tak úmyslných hrozeb a měla by být odhadnuta pravděpodobnost jejich výskytu. Podstatné je, aby nebyla přehlédnuta žádná relevantní hrozba, protože by to mohlo mít za následek selhání nebo oslabení bezpečnosti IS.

Po identifikaci zdroje hrozby (kdo a co bylo příčinou hrozby) a cíle hrozby (tj. které prvky IS mohou být hrozbou ovlivněny), je nutné odhadnout parametry hrozby. Přitom by se mělo přihlídnout k:

- motivaci - vědomým a nutným možnostem, zdrojům, které jsou dostupné pro možné útočníky;
- atraktivnosti a zranitelnosti aktiv IS pro možné útočníky, jako zdroji záměrných hrozeb;
- možným následkům (dopadům) v případě výskytu hrozby;
- geografickým faktorům jako je blízkost chemických továren nebo továren na zpracování nafty, možnosti extrémních povětrnostních podmínek a faktorům, které by mohly ovlivnit lidské chyby a chybné funkce zařízení, jako zdroji náhodných hrozeb.

Po dokončení odhadu existuje seznam identifikovaných hrozeb, aktiv nebo skupiny aktiv, které mohou tyto hrozby ovlivnit a míra závažnosti hrozeb.

IV. krok AR

Odhad hrozeb a jejich hodnocení je realizováno prostřednictvím interně vyvinutého hodnotícího SW nástroje ARIS.xls. Číselník hrozeb vychází ze standardů ČSN ISO/IEC 27005.

8.3.5 Odhad frekvence hrozeb

V tomto kroku je nutno provést odhad frekvence výskytu hrozeb. Odhad frekvence hrozby je dle typu hrozby proveden na základě zkušeností, statistik, atd.

V. krok AR

Odhad frekvence hrozeb je stanoven.

Frekvence hrozeb jsou vybírány z číselníku, uvedeného v Příloze P VI.

8.3.6 Odhad zranitelnosti (dopadů)

Zranitelnost je nedostatek, slabina nebo stav analyzovaného aktiva, kterého může být využito hrozbou pro uplatnění jejího nežádoucího vlivu. Tato veličina je vlastností aktiva a vyjadřuje, jak citlivé je aktivum na působení dané hrozby. Zranitelnost vznikne všude tam, kde dochází k interakci mezi hrozbou a aktivem.

Základní charakteristikou zranitelnosti je její úroveň. Úroveň zranitelnosti aktiva se hodnotí podle citlivosti (náchylnost aktiva být poškozeno danou hrozbou) a kritičnosti (důležitost aktiva pro organizaci).

Tento odhad identifikuje zranitelnosti, které mohou být využity hrozbami a odhaduje pravděpodobný stupeň slabých míst, tj. snadnosti jejich využití. Např. některá aktiva jsou snadno manipulovatelná, snadno ukryta nebo přepravena - všechny tyto vlastnosti se mohou týkat zranitelností. Příklady zranitelností jsou:

- pravidla práce v bezpečnostních zónách nejsou definována;
- včasné údržby a opravy technicky se neprovádí;
- zálohování dat se neprovádí;
- postupy pro kontrolu použití hesel chybí.

Je důležité reálně odhadnout, jak vážné jsou zranitelnosti, jinými slovy, jak snadno mohou být tato zranitelnosti využity. Měla by být odhadnuta zranitelnost ve vztahu ke každé hrozbě, která by mohla tuto zranitelnost IS ve specifické situaci využít. Například IS může obsahovat zranitelnost vůči hrozbě předstírání identity uživatele a zneužití zdrojů. Zranitelnost na předstírání identity může být vysoká jako důsledek absence autentizace uživatele. Na druhé straně zranitelnost týkající se zneužití zdrojů může být nízká, protože dokonce

i v případě chybějící autentizace uživatele jsou prostředky, pomocí kterých mohou být zdroje zneužity, limitovány.

VI. krok AR

Odhad úrovně zranitelností je stanoven.

Zranitelnosti mohou být vybírány z daných číselníků.

Úrovně zranitelnosti jsou vybírány z číselníku, uvedeného v Příloze P VII.

8.3.7 Odhad účinnosti protiopatření

Ochranná opatření nebo protiopatření jsou praktiky, postupy nebo mechanismy, které mohou poskytnout ochranu před hrozbou, snížit zranitelnost, omezit dopad nežádoucího incidentu, detekovat nežádoucí incidenty a usnadnit obnovu. Účinná bezpečnost obvykle vyžaduje kombinaci různých ochranných opatření, aby poskytla aktivům různé stupně bezpečnosti. Například mechanismus řízení přístupu aplikovaný na počítače by měl být podporován auditními kontrolami, personálními procedurami, školením a fyzickou bezpečností. Některá ochranná opatření mohou existovat již jako součást prostředí, nebo jako inherentní aspekt aktiv nebo mohou být v IS nebo v organizaci již uplatněna.

Ochranná opatření mohou vykonávat jednu nebo více následujících funkcí: detekci, odstrašovací funkci, prevenci, omezení, korekci, obnovu, monitorování a povědomí o problému. Pro korektně implementovaný bezpečnostní program je podstatný vhodný výběr ochranných opatření. Mnoho ochranných opatření může plnit vícenásobné funkce.

Příklady ochranných opatření jsou:

- pracovní smlouvy,
- prověřování pracovníků,
- zabezpečení proti požáru a násilnému vniknutí do budov,
- havarijní plány,
- školení,
- síťové firewally,
- monitorování a analýza sítě,
- šifrování k zajištění důvěrnosti,
- digitální podpisy,
- antivirový software,
- záložní kopie informací,
- rezervní zdroje energie,

- mechanismy řízení přístupu.

Součástí hodnocení je jednak identifikace existujících protiopatření, jednak odhad jejich účinnosti jako funkce snižující míru zranitelnosti aktiva.

Po dokončení odhadu existuje seznam identifikovaných protiopatření, které mohou ovlivnit (snížit) zranitelnost danou hroznou a míra předpokládané účinnosti protiopatření.

VII. krok AR

Identifikace protiopatření a odhad jejich účinnosti je realizován prostřednictvím SW nástroje ARIS.xls

Protiopatření jsou vybírána z číselníků, které jsou součástí tohoto nástroje.

Účinnost protiopatření je vybírána z číselníku, uvedeného v Příloze P VIII.

Číselník protiopatření je vypracován dle standardu ČSN ISO/IEC 27001.

8.3.8 Hodnocení míry rizika

Tato kapitola je zaměřena na poslední etapu, což je vyhodnocení celkových rizik. Jak již bylo dříve uvedeno, aktiva, která mají hodnotu a určitý stupeň zranitelnosti, jsou v riziku vždy, když existuje nějaká hrozba. Vyhodnocení rizik je kombinací potenciálních nepříznivých dopadů nežádoucích incidentů na činnost organizace a stupně odhadnutých hrozeb a zranitelností. Rizika představují míru vystavení se hrozbě, jehož subjektem může být IS a příslušná organizace. Míry rizika jsou výsledkem matematické funkce:

- hodnot aktiv;
- hrozeb;
- snadnosti využití zranitelností hrozbami, které vyvolají nežádoucí dopady;
- četnosti hrozeb;
- existujících a plánovaných ochranných opatření, která mohou snížit závažnost zranitelností, hrozeb a dopadů.

Cílem analýzy rizik je identifikovat a odhadnout rizika, kterým je IS a jeho aktiva vystaven, aby mohla být identifikována a vybrána vhodná a oprávněná bezpečnostní ochranná opatření. Při odhadování rizik je zvažováno několik aspektů včetně jejich dopadu a pravděpodobnosti.

Výsledkem tohoto kroku je seznam naměřených rizik pro každý z dopadů, který je důsledkem zpřístupnění, modifikace, nedostupnosti nebo zničení posuzovaného IS. Míry

rizika pomáhají také identifikovat, která rizika by měla být při výběru ochranných opatření řešena jako první.

VIII. krok AR

Míra rizika (bezrozměrné číslo) je určena jako součin číselných parametrů hodnoty aktiva, četnosti hrozby, dopadu hrozby, koeficientu účinnosti stávajících opatření.

Kalkulace probíhá dle vzorce:

$$R = (V_C + V_I + V_A) * O * I * C \quad (1)$$

kde:

R = míra rizika,

V_C = hodnota aktiva z pohledu ohrožení jeho důvěrnosti,

V_I = hodnota aktiva z pohledu ohrožení jeho integrity,

V_A = hodnota aktiva z pohledu ohrožení jeho dostupnosti,

O = četnost hrozby,

I = dopad hrozby,

C = koeficient účinnosti existujících protiopatření.

8.3.9 Akceptace rizik, varianty zvládání rizik

8.3.9.1 Kritéria pro hodnocení rizik - obecná definice

- Stanovení hodnot informačních aktiv z hlediska požadavků na jejich dostupnost, důvěrnost a integritu.
- Určení požadavků relevantní legislativy a požadavků vyplývajících z uzavřených smluvních vztahů.
- Určení možných dopadů identifikovaných hrozeb, reálných pravděpodobností jejich uskutečnění a určení úrovně rizik pro informační aktiva.
- Určení akceptovatelné úrovně rizika pro informační aktiva.
- Snížení či likvidace rizik prostřednictvím pokrytí hrozeb doporučenými protiopatřeními dle ČSN ISO/IEC 27001.

8.3.9.2 Kritéria pro akceptaci rizik

IX. krok AR

Rozhodnutí o kritériích pro akceptaci rizik a akceptovatelnou úroveň stanovuje svým rozhodnutím vedení organizace jako jeden z nezbytných důkazů o vůli vedení organizace managementu rizik.

Kritéria pro akceptaci rizik navrhuje vedoucí oddělení IT bezpečnosti a navrhuje maximální míru akceptovatelného rizika.

8.3.9.3 Varianty pro zvládání rizik

Obsahem této etapy risk managementu je návrh variant pro zvládání rizik, resp. návrh doporučených protiopatření

Podkladem pro identifikaci a vyhodnocení variant pro zvládání rizik jsou politiky organizace a kritéria akceptaci rizik.

X. krok AR

Za identifikaci a vyhodnocení variant pro zvládání rizik odpovídá vedoucí oddělení IT bezpečností. Identifikací a vyhodnocením variant pro zvládání rizik se rozumí uvedené možné činnosti:

- *aplikování vhodných opatření;*
- *vědomé a objektivní akceptování rizik za předpokladu, že zřetelně naplňují politiky organizace a kritéria pro akceptaci rizik;*
- *vyhnutí se rizikům;*
- *přenesení rizik spojených s činností organizace na třetí strany, např. na pojišťovny, dodavatele.*

8.3.10 Zpráva z analýzy rizik

O provedení analýzy rizik je zpracována zpráva, která je předložena nadřízeným k odsouhlasení.

8.4 Údržba analýzy rizik

Za aktualizaci analýzy rizik zodpovídá vedoucí oddělení IT bezpečnosti v součinnosti s vlastníky komponent a aktiv.

Analýza rizik je kontinuálním procesem minimálně v tom smyslu, že je stanoven interval pro revizi analýzy. **Revize analýzy rizik je prováděna „Minimálně jednou za dva roky a při každé podstatné změně systému“.**

9 NÁVRH IMPLEMENTACE BEZPEČNOSTNÍ POLITIKY

9.1 Bezpečnostní politika

Cíl: Definovat směr a vyjádřit ochotu vedení společnosti naplňovat bezpečnost informací s požadavky organizace, vnitřními směrnicemi a příslušnými zákony.

Zjištění: Je vypracována Strategie bezpečnosti informací, definující základní oblasti s odkazem na samostatnou směrnici Bezpečnostní politika informací. V nedávné době byla aktualizována.

Doporučení: Směrnice Bezpečnostní politika informací je klíčovým dokumentem organizace v rámci systému řízení bezpečnosti informací. Ač byla v nedávné době aktualizována, je potřeba důsledně revidovat a aktualizovat na základě periodických aktivit. Doporučuji dále důsledně kontrolovat dodržování bezpečnostní politiky zaměstnanci organizace na všech úrovních.

9.2 Organizace bezpečnosti informací

Cíl: Bezpečnost informací ve společnosti musí být řízena odpovědnými pracovníky organizace vedená managementem, které by schvalovalo politiku bezpečnosti, definovalo odpovědnosti v oblasti bezpečnosti informací a koordinovalo implementaci bezpečnosti. Zároveň je třeba zachovat bezpečnost zařízení zpracovávající informace, bezpečnost aktiv, které jsou přístupné třetím stranám a to i v případech, kdy je odpovědnost přenesena formou outsourcingu přenesena na jinou organizaci.

Zjištění: Společnost a. s. má dle požadavků ČNB zřízeno oddělení IT bezpečnosti, definovanou roli vedoucího IT bezpečnosti s určenou odpovědností za bezpečnost informací v organizaci. Vztahy s externími subjekty jsou definovanými smluvními vztahy. V případě nutnosti přístupu třetích stran do provozovaných informačních systémů jsou s těmito subjekty uzavírány NDA dohody s jasně definovanými podmínkami pro zajištění bezpečnosti informací.

Doporučení: Požadavky na přístup třetích stran (dodavatelů) do systémů jsou řízeny ad-hoc a je potřeba zajistit/zefektivnit proces pro schvalování přístupů do systémů externistům až po zajištění smluvních dokumentů NDA.

9.3 Řízení aktiv

Cíl: Zajistit a udržovat přiměřenou ochranu aktiv společnosti vedením evidence aktiv.

Zjištění: Jsou definováni vlastníci a správci jednotlivých aktiv dle platných interních směrnic oddělení IT – Řízení IS/IT a IT bezpečnosti – Analýza rizik systému řízení informací, Klasifikace informací. Z pohledu směrnice Analýzy rizik systému řízení informací není zpracována konkrétní metodika analýzy rizik. Z pohledu změny vlastníků aktiv prakticky neprobíhá jednoznačné určení vlastníka aktiva vedením společnosti. Někteří vlastníci si nejsou vědomi určením odpovědností za aktiva

Doporučení: Vedení společnosti musí jednoznačně jmenovat vlastníka aktiva a periodicky informovat vlastníky o případných změnách.

9.4 Bezpečnost lidských zdrojů

Cíl: Snížení rizika chyby lidského faktoru, podvodu, krádeže, zneužití prostředků. Zajištění povědomí zaměstnanců, dodavatelů o bezpečnostních hrozbách. Připravenost podílet se na dodržování bezpečnostní politiky v průběhu výkonu práce.

Zjištění: V interních směrnicích jsou definovány role a odpovědnosti v oblasti bezpečnosti informací. Součástí úvodních i periodických školení je i školení v oblasti IT bezpečnosti prováděné formou elearningu. Jsou popsány pravidla bezpečnosti informačních systémů pro uživatele s povinnostmi a odpovědnostmi, dále existuje interní směrnice Požadavky na bezpečnost poboček. Soubor směrnic v této oblasti je dostatečně popsán.

Doporučení: Udržet soubor předpisů aktualizovaný a průběžně jej revidovat. Doporučuji provádět školení v oblasti bezpečnosti informací formou meetingů a informovat zaměstnance o aktuálních hrozbách v této oblasti.

9.5 Fyzická bezpečnost a bezpečnost prostředí

Cíl: Zabránit neoprávněnému přístupu do vymezených prostor organizace. Zamezit ztrátě, poškození či odcizení prostředků pro zpracování informací a dat.

Zjištění: Společnost a. s. má řízený přístup pomocí elektronických přístupových systémů jak v prostorách administrativní budovy, tak na pobočkách. Jsou vybudovány serverovny a přístup do těchto prostor je řízen. Serverovny v centrále společnosti jsou vybaveny sys-

témy PZTS, EPS doplněny SHZ. Serverovny na pobočkách jsou konstrukčně odděleny od prostor pro veřejnost a jsou zabezpečeny systémy PZTS. Společnost má pronajaty samostatné uzavřené prostory v rozsahu dvou pater. Ač přístup do těchto prostor je řízen pomocí systémů EKV postrádám existenci prostoru recepce pro evidenci a řízení návštěv. Fyzická bezpečnost organizace je v kompetenci samostatného oddělení Fyzické bezpečnosti

Doporučení: Zajisti prostor recepce a tím pádem posílit režimová opatření pro návštěvy.

9.6 Řízení komunikací a řízení provozu

Cíl: Zajištění bezchybného a bezpečného provozu prostředků pro zpracování informací, minimalizace selhání prostředků, zajištění dostupnosti služeb. Zamezit ztrátě, změně či zneužití informací.

Zjištění: Společnost a. s. má fakticky rozdělen provoz systémů na produkční a neprodukční systémy. Veškeré produkční systémy jsou zajištěny formou outsourcingové smlouvy s externím dodavatelem a definovanými požadavky na SLA. Z pohledu neprodukčních systémů jsou tyto ve správě IT oddělení podloženy interními směnicemi popisující celý provoz dostatečně. Z pohledu IT bezpečnosti jsou zajišťovány a vyhodnocovány auditní logy všech produkčních systémů a většiny neprodukčních systémů. Dále je řízen, monitorován a vyhodnocován síťový provoz.

Doporučení: nejsou

9.7 Řízení přístupu

Cíl: Zajištění řízeného přístupu k informacím, bránit neoprávněným přístupům do systémů, koncových stanic, sítí. Zajistit bezpečnost mobilní výpočetní techniky a prostředků v případě vzdáleného přístupu.

Zjištění: Pro řízení přístupových práv je provozován interně vyvinutý identity management systém (IDM) ve správě IT oddělení a pod kontrolou oddělení IT bezpečnosti. Jsou zavedeny procesy: podání požadavků, schvalování a následná realizace požadovaných přístupů, případně procesy pro zrušení stávajících přístupů do systémů. Jsou prováděny

audity přístupových oprávnění v pravidelných intervalech. Nedostatky jsou ve spolupráci se správci daných systémů odstraňovány. Pomocí interních směrnic jsou popsány oblasti řešící: řízení přístupů k IS a vzdálený VPN přístup, politiku hesel, šifrování koncových mobilních zařízení (notebooky, mobilní telefony, tablety), klasifikace informací popisující pravidla nakládání s těmito informacemi a možné metody jejich zajištění. Strategie bezpečnosti informací jednoznačně definuje politiku přidělování nezbytných oprávnění. Není dostatečně prováděna kontrola neslučitelnosti rolí.

Doporučení: V rámci systému IDM specifikovat oblasti slučitelných a neslučitelných rolí.

9.8 Akvizice, vývoj a údržba informačních systémů

Cíl: Implementace bezpečnostních opatření při vývoji IS a zajištění tak integrity, dostupnosti a důvěrnosti informací.

Zjištění: Společnost má zajištěn vývoj aplikací odděleně od provozování ostatních systémů. Oblast vývoje nebyla součástí této analýzy.

Doporučení: Provést samostatnou analýzu této oblasti.

9.9 Zvládání bezpečnostních incidentů

Cíl: Minimalizace škod způsobených selháním a bezpečnostními incidenty. Monitoring incidentů, vyhodnocování, poučení se závěrů.

Zjištění: Ve Společnost a. s. je nastaven proces pro zvládání bezpečnostních incidentů se zpracovanou směrnicí. Řešení bezpečnostních incidentů, dle které probíhá i vyhodnocování bezpečnostních incidentů. Pro evidenci bezpečnostních incidentů slouží systémový ticketovací nástroj bez možností provádění statistik apod. Proces vyhodnocování je dostačující. V kompetenci oddělení IT bezpečnosti jsou provozovány SIEM nástroje, které vyhodnocují systémové logy produkčních i některých neprodukčních systémů, které to umožňují. Je zajištěno archivování systémových logů. V případě pořizování nových či náhrada stávajících systémů jsou prováděny výběrová řízení s ohledem na bezpečnostní požadavky a možnosti logování.

Doporučení: pořízení nového ticketovacího nástroje pro jednotnou správu a evidenci bezpečnostních incidentů. Stávající řešení neodpovídá plně požadavkům pro jednotný systém evidence a vyhodnocování bezpečnostních incidentů.

9.10 Řízení kontinuity činností organizace

Cíl: Organizační a technické zajištění klíčových procesů organizace v případě havárií, selhání či živelných pohrom s ohledem na zhodnocení dopadu v případě přerušení činnosti společnosti. Schopnost efektivně fungovat v případě narušení provozu. Organizačně a technicky zajistit obnovu kritických procesů organizace v případě většího selhání nebo havárie, včetně rámcového zhodnocení dopadu při přerušení činnosti podniku. Jedná se zde především o otázky zálohování dat, reakce na zcizení prostředků VT, živelné katastrofy, výpadku elektrického napájení apod.

Zjištění: Společnost a. s. vypracovala a postupuje dle směrnice Kontinuita podnikání. Jsou vypracovány havarijní plány jednotlivých oddělení. Existují havarijní plány systémů. Z pohledu zálohování dat probíhají testy záloh produkčních systémů dle pravidelných předpisů a jsou dokumentovány – zajištěno outsourcingem. Testy záloh neprodukčních systémů probíhají v reálu neplánovaně bez dokumentace.

Doporučení: Dodržovat formálně popsané postupy zálohování dat neprodukčních systémů. Poučit odpovědné zaměstnance o vytváření záznamů provedených záloh.

9.11 Soulad s požadavky

Cíl: Soulad veškerých postupů s definovanou bezpečnostní politikou a dílčími směnicemi. Předejít porušení norem, zákonných nebo smluvních povinností či bezpečnostních požadavků. Soulad musí být zajištěn prováděním pravidelných auditů buď vlastními silami organizace či externím auditorem s odpovídající kvalifikací.

Zjištění: Společnost a. s. zajišťuje soulad s požadavky jak vlastními silami oddělením interního auditu, tak pomocí externích auditorů. Revize postupů dle interních směrnic probíhají pravidelně. Externí audity jsou prováděny i s ohledem na srovnání výstupů interních auditů a liniových kontrol. Plány liniových kontrol jsou nastaveny.

Doporučení: nejsou

ZÁVĚR

Cílem této diplomové práce bylo provedení literární rešerše teoretických podkladů v problematice bezpečnostní politiky organizace, analýza modelu informačního a komunikačního systému zvolené organizace, návrh implementace a zpracování metodiky analýzy rizik použitelné i pro obdobné subjekty. Tato metodika je nutnou součástí portfolia dílčích směrnic organizací působících v bankovní sféře.

S ohledem na společnost, na citlivost informací a dat, které zpracovává její informační systém, byla vypracovaná analýza v této diplomové práci částečně anonymizovaná s ohledem na kritičnost některých systémů a zajištění bezpečnosti klientských dat. Vzhledem k těmto skutečnostem je následná implementace bezpečnostních opatření popsána formou dílčích kroků, které je nutno prezentovat vrcholovému managementu organizace. Jsou navrženy dílčí rizika k eliminaci, snížení či akceptaci vedením. Následně jsou popsány kroky dlouhodobého udržení systému řízení bezpečnosti informací.

Metodika analýzy rizik byla koncipována formou samostatného dokumentu, jenž v organizaci dosud nebyl zpracován a pomocí dílčích kroků je pomocníkem zpracovatele budoucích analýz. Mým přáním je praktické využití dané metodiky organizací, která danou směrnicí akceptovala a uvedla v užívání.

Dále doufám, že tato práce pomohla čtenáři k vytvoření uceleného pohledu na problematiku analýzy rizik informačních systémů, bezpečnostní politiky a jejího významu pro organizace obdobného charakteru.

SEZNAM POUŽITÉ LITERATURY

- [1] LEE, Bruce. *Bruce Lee, umělec života*. Editor John R Little. Překlad Jana Novotná. Praha: Pragma, 2002, 279 s. ISBN 80-720-5868-1.
- [2] ČSN ISO/IEC 27005. *Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013. Třídící znak 36 9790.
- [3] MAISNER, Martin, 2015. *Zákon o kybernetické bezpečnosti: komentář*. Vydání první. Praha: Wolters Kluwer. Komentáře (Wolters Kluwer ČR). ISBN 9788074788178. [13] *Zákon o ochraně osobních údajů: komentář*, 2012. 1. vyd. V Praze: C.H. Beck. Beckova edice komentované zákony. ISBN 9788071792260.
- [4] ČSN ISO/IEC 27000. *Informační technologie – Bezpečnostní techniky - Systém řízení bezpečnosti informací – Přehled a slovník*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Třídící znak 36 9790.
- [5] NOVÁK, Daniel, 2014. *Zákon o ochraně osobních údajů a předpisy související: komentář*. Vyd. 1. Praha: Wolters Kluwer. Komentáře (Wolters Kluwer ČR). ISBN 9788074786655.
- [6] POŽÁR, Josef, 2005. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 8086898385.
- [7] BENDA, Radek. *Zásady tvorby bezpečnostního projektu. Sborník konference "Internet a bezpečnost organizací", 2006*.
- [8] PAULIČKOVÁ, Anna. *Ochrana informací coby součást bezpečnostní politiky organizace*. Brno, 2008. Diplomová práce. Masarykova universita, Filozofická fakulta, Ústav české literatury a knihovnictví.
- [9] ČSN ISO/IEC 27001. *Informační technologie – Bezpečnostní techniky - Systém řízení bezpečnosti informací - Požadavky*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014. Třídící znak 36 9797.
- [10] JAŠEK, Roman, 2006. *Informační a datová bezpečnost*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně. ISBN 8073184567.

- [11] LUDVÍK, Miroslav a Bohumír ŠTĚDRŮ, 2008. *Teorie bezpečnosti počítačových sítí*. Vyd. 1. Kralice na Hané: Computer Media. ISBN 9788086686356.
- [12] JAŠEK, Roman a Martin LUKÁŠ, 2003. *Informatika ve veřejné správě*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně. ISBN 8073181479.
- [13] SULEK, Martin. Organizační a režimové opatření: Slezská univerzita v Opavě [online]. 2013 [cit. 2016-04-20]. Dostupné z: <http://www.slu.cz/math/cz/knihovna/ucebni-texty/Ochrana-osob-a-majetku/Organizacni-a-rezimove-opatreni-a-fyzicka-ochrana.pdf>
- [14] *Sbírka zákonů Česká republika*, 2014. Břeclav: Moraviapress. ISSN 12111244.
- [15] ICT (Information and Communication Technologies) - ManagementMania.com. *Sociální síť pro business - ManagementMania.com* [online]. [cit. 2016-04-22]. Dostupné z: <https://managementmania.com/cs/informacni-a-komunikacni-technologie>
- [16] NDA (Non-disclosure agreement) Dohoda o mlčenlivosti - ManagementMania.com. *Sociální síť pro business - ManagementMania.com* [online]. [cit. 2016-04-22]. Dostupné z: <https://managementmania.com/cs/nda-non-disclosure-agreement>
- [17] Identity management – centrální správa uživatelských účtů | Computerworld.cz. *Computerworld.cz | Deník pro IT profesionály* [online]. [cit. 2016-04-22]. Dostupné z: <http://computerworld.cz/securityworld/identity-management-centralni-sprava-uzivatelskych-uctu-47568>

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AD	Active Directory – autentizační a autorizační adresářová služba
AR	Analýza rizik
BIA	Business Impact Analysis – metoda analýzy dopadů
ČNB	Česká národní banka
ČSN	Česká státní norma
DA	Datová aktiva
EKV	Elektronická kontrola vstupu
EPS	Elektrická požární signalizace
HW	Hardware
ICT	Information and Communication Technologies – informační a komunikační technologie
IDM	Identity Management – informační systém, který dokáže z jednoho místa ovládat životní cyklus všech uživatelských účtů a audit
IS	Informační systém
ISMS	Information Security Management System – dokumentovaný systém řízení informační bezpečnosti
ISO	International Organization for Standardization – mezinárodní organizace zabývající se tvorbou norem
ISP	Internet Service Provider, poskytovatel internetového připojení
IT	Informační technologie
LAN	Local Area Network – místní síť
Loc	Lokality
MD	Datová média
NDA	Non-disclosure Agreement – dohoda o mlčenlivosti
OÚ	Osobní údaj
PBX	Telefonní ústředna

PC	Osobní počítač
Per	Periferní zařízení
PZTS	Poplachové, zabezpečovací a tísňové systémy
SIEM	Security Information and Event Management – monitoring korelovaných bezpečnostních událostí a reporting
SKU	Služba koncovému uživateli
SLA	Service Level Agreement – dohoda o úrovni poskytovaných služeb
Srv	Server
SW	Software
UPS	Uninterruptible Power Supply – záložní zdroj energie
VT	Výpočetní technika

SEZNAM OBRÁZKŮ

<i>Obr. 1 Vztah mezi normami řady ISMS [4]</i>	<i>29</i>
<i>Obr. 2 Organizační struktura Společnost a. s. [vlastní]</i>	<i>37</i>
<i>Obr. 3 Vzorek hodnocení aktiv Společnost a.s. [vlastní]</i>	<i>42</i>
<i>Obr. 4 Vzorek hodnocení hrozeb Společnost a. s. [vlastní]</i>	<i>46</i>
<i>Obr. 5 List Podklady – Aktiva [vlastní]</i>	<i>48</i>
<i>Obr. 6 Seznam hrozeb [vlastní].....</i>	<i>49</i>
<i>Obr. 7 Vzorový list - sloupce hrozby [vlastní]</i>	<i>50</i>
<i>Obr. 8 List Hrozby – sloupce hrozby [vlastní].....</i>	<i>51</i>
<i>Obr. 9 List Podklady – vkládání hodnot četnost a dopad [vlastní]</i>	<i>52</i>
<i>Obr. 10 List Podklady – vkládání hodnot protiopatření [vlastní]</i>	<i>53</i>
<i>Obr. 11 List Parametry – stanovení úrovně pokrytí rizik [vlastní].....</i>	<i>54</i>
<i>Obr. 12 List Aktiva [vlastní]</i>	<i>55</i>
<i>Obr. 13 List Rizika [vlastní].....</i>	<i>56</i>
<i>Obr. 14 List Vybraná opatření [vlastní]</i>	<i>57</i>
<i>Obr. 15 List Prohlášení o aplikovatelnosti [vlastní].....</i>	<i>58</i>

SEZNAM TABULEK

<i>Tab. 1 Výsledky hodnocení BIA Společnost a. s. [vlastní]</i>	39
<i>Tab. 2 Vlastníci informační aktiva Společnost a. s. [vlastní]</i>	40
<i>Tab. 3 Škála hodnocení aktiv [vlastní]</i>	42
<i>Tab. 4 Odhad četnosti hrozby [vlastní]</i>	43
<i>Tab. 5 Odhad dopadu hrozby [vlastní]</i>	44
<i>Tab. 6 Odhad účinnosti opatření [vlastní]</i>	45

SEZNAM ROVNIC

- (1) Stanovení míry rizika

SEZNAM PŘÍLOH

- P I Typ aktiva
- P II Hodnota aktiva
- P III Doporučení pro hodnocení jednotlivých typů aktiv
- P IV Katalog možných incidentů
- P V Hodnotící kritéria dopadu bezpečnostního incidentu
- P VI Frekvence hrozeb
- P VII Úroveň zranitelnosti
- P VIII Účinnost protiopatření
- P IX Výsledky hodnocení rizik bez opatření Společnost a. s.
- P X Výsledky hodnocení rizik včetně opatření Společnost a. s.

PŘÍLOHA P I: TYP AKTIVA

Služba koncovému uživateli (SKU)	SKU-Mailová komunikace
	SKU-Dávkové zpracování
	SKU-Práce uživatele s aplikací
	SKU-Služby dodavatelů
	SKU-Hlasové služby
	SKU-Přístup na Internet
Software (SW)	SW-Aplikace
	SW-Finanční aplikace
	SW-Bezpečnostní aplikace
	SW-Personální aplikace
	SW-Obecná aplikace/Aplikace na zakázku
	SW-EDI
Datová aktiva (DA)	DA-Datová aktiva
	DA-Datová aktiva - Osobní
Datová média (MD)	MD-Elektronické médium
	MD-Neelektronické médium
Server (Srv)	Srv-Paměťové zařízení
	Srv-Server
LAN	LAN-ISP
	LAN-Firewall/proxy
Telefonní ústředna (PBX)	PBX
Periferní zařízení (Per)	Per-Fax
	Per-Tiskárny

PC	PC/NTB
	PC/NTB-PC
	PC/NTB-Terminál
Lokality (Loc)	Loc-Společnost
	Loc-Budova
	Loc-Místnost
Zpracování osobních údajů	Zpracování OÚ

PŘÍLOHA P II: HODNOTA AKTIVA

1	Žádná, hodnota do 1 tis. Kč
2	Zanedbatelná, hodnota do 10 tis. Kč
3	Malá, hodnota 10 - 100 tis. Kč
4	Nízká, hodnota 100 - 300 tis. Kč
5	Nízká až střední, hodnota 300 tis. – 1 mil. Kč
6	Střední, hodnota 1 mil. – 3 mil. Kč
7	Střední až vysoká hodnota 3 mil. – 10 mil. Kč
8	Vysoká hodnota 10 mil. Kč - 30 mil. Kč
9	Velmi vysoká hodnota 30 mil. Kč - 100 mil. Kč

PŘÍLOHA P III: DOPORUČENÍ PRO HODNOCENÍ JEDNOTLIVÝCH TYPŮ AKTIV

Služba koncovému uživateli	Hodnota dopadu nedostupnosti služby pro organizaci, pokud nelze úhrnné náklady na službu za časovou jednotku (obvykle 1 rok)
Software	Pořizovací náklady (náklady vlastnictví zahrnující náklady na licence, implementaci, maintenance, ...)
Datová aktiva	Převažující z následujících možností – hodnota dopadu: <ul style="list-style-type: none">- ztráty dostupnosti,- ztráty důvěrnosti,- ztráty integrity
Datová média	Aktuální tržní cena adekvátní náhrady
Server	Aktuální tržní cena adekvátní náhrady
LAN	Aktuální tržní cena adekvátní náhrady
Telefonní ústředna (PBX)	Aktuální tržní cena adekvátní náhrady
Periferní zařízení (Per)	Aktuální tržní cena adekvátní náhrady
PC	Aktuální tržní cena adekvátní náhrady
Lokalita	Hodnota majetku v lokalitě
Zpracování osobních údajů	Převažující z následujících možností – dopad ztráty dostupnosti, dopad ztráty důvěrnosti, dopad ztráty integrity.

PŘÍLOHA P IV: KATALOG MOŽNÝCH INCIDENTŮ

Vlastnost	Požadavek	Popis
Důvěrnost	Vysoká (V)	Ztráta důvěrnosti aktiva může způsobit ohrožení hlavních činností banky, vážnou ztrátu důvěryhodnosti banky, rozsáhlou negativní publicitu, sankce ve výši milionů korun
	Střední (S)	Ztráta důvěrnosti aktiva může způsobit ohrožení vedlejších činností banky, narušení důvěryhodnosti banky, občasnou negativní publicitu, sankce ve výši až statisíců korun
	Nízká (N)	Ztráta důvěrnosti aktiva nenaruší činnosti banky, může způsobit ojedinělé stížnosti nebo sankce ve výši nejvýše desetitisíců korun
Dostupnost	Vysoká (V)	Aktivum musí být dostupné trvale, je možno tolerovat dobu nedostupnosti v řádu minut
	Střední (S)	Aktivum musí být dostupné v pracovní době, je možno tolerovat dobu nedostupnosti v řádu hodin
	Nízká (N)	Aktivum nemusí být trvale dostupné, je možno tolerovat dobu nedostupnosti v řádu dnů
Integrita	Vysoká (V)	Ztráta integrity může způsobit ohrožení hlavních činností banky, nároky na vícepráci nebo hmotné ztráty v řádu milionů korun a více
	Střední (S)	Ztráta integrity může způsobit ohrožení vedlejších nebo omezení hlavních činností organizace, nároky na vícepráci nebo hmotné ztráty v řádu až statisíců korun
	Nízká (N)	Ztráta integrity aktiva může způsobit omezení vedlejších činností organizace, nároky na vícepráci nebo hmotné ztráty nejvýše v řádu desetitisíců korun

PŘÍLOHA P V: HODNOTÍCÍ KRITÉRIA DOPADU BEZPEČNOSTNÍHO INCIDENTU

Hodnocení dopadu bezpečnostního incidentu. Bezpečnostní incident je každá ne-standardní bezpečnostní situace, při které došlo nebo mohlo dojít k ohrožení bezpečnosti (dostupnosti, integrity a/nebo důvěrnosti) dat.

Stupeň	Slovní popis	Dopad – Řízení organizace	Hodnota ve škále
1	Zanedbatelný	Obtěžující, komplikující práci v rámci jednotlivých oddělení, snižující efektivitu.	1-10 tis.
1	Malý	Snižující efektivitu práce na více odděleních, možný nárůst nekoordinace a prostojů.	10-100 tis.
1	Nízký	Narušující práci v organizaci, výrazně snižující efektivitu vykonávaných činností jednotlivých oddělení a odborů. Možnost komplikací se smluvními subjekty a klienty.	100-300 tis.
2	Nízký až střední	Zastavující některé činnosti a poskytování služeb. Přerůstající rámec organizace, možnost medializace problémů, snížení kreditu organizace. Organizace takřka nevykonává běžnou agendu, poškození zájmů klientů.	300 tis. – 1 mil.
2	Střední	Zastavující některé činnosti a poskytování služeb. Přerůstající rámec organizace, možnost medializace problémů, snížení kreditu organizace. Organizace fakticky nevykonává běžnou agendu, poškození zájmů klientů.	1-3 mil.
3	Střední až vysoký	Zastavující většinu činnosti a poskytování služeb. Přerůstající rámec organizace, medializace problémů, výrazné snížení kreditu organizace.	3-10 mil.
3	Vysoký	Zastavující většinu činnosti a poskytování služeb. Přerůstající rámec organizace, medializace problémů, výrazné snížení kreditu organizace.	10-30 mil.
3	Velmi vysoký	Velmi vysoké dopady na poskytování služeb organizace. Přerůstající rámec organizace, medializace problémů, výrazné snížení kreditu organizace.	30-100 mil.

PŘÍLOHA P VI: FREKVENCE HROZEB

Stupeň	Slovní popis	Četnost výskytu
1	Velmi nízká	jednou za více let
2	Nízká	asi jednou ročně
3	Střední	asi jednou měsíčně
4	Vysoká	asi jednou za několik dnů
5	Mimořádně vysoká	denně až trvale

PŘÍLOHA P VII: ÚROVEŇ ZRANITELNOSTI

Stupeň	Dopad hrozby	Vodítka pro odhad z hlediska			
		organizačního	poškození aktiva	výpadku služby	finančního
1	Zanedbatelný	nevýznamný	do 1%	do 1 hodina	do 5 tis. Kč
2	Nízký	znatelný	do 5%	do 4 hodin	do 50 tis. Kč
3	Střední	přechodné problémy	do 10%	do 1 dne	do 1 mil. Kč
4	Vysoký	krátkodobé vážné problémy	do 50%	do 1 týdne	do 10 mil. Kč
5	Mimořádně vysoký	dlouhodobé vážné problémy	> 50%	> 1 týden	> 10 mil. Kč

PŘÍLOHA P VIII: ÚČINNOST PROTIOPATŘENÍ

Stupeň	Slovní popis	Účinnost asi
1	Mimořádně vysoká	>95%
2	Dostatečná	80%
3	Částečná	50%
4	Nízká	20%
5	Zanedbatelná	<5%

PŘÍLOHA P IX: VÝSLEDKY HODNOCENÍ RIZIK BEZ OPATŘENÍ

		Infrastruktura	Aktivní síťové pokry	Severny a datová uložení	Elektronická pošta	AD, doménová struktura	Telefonní ústředna (HW+ SW)	Severovna (zabezpečení zóny)	Internetové bankovníčví	Mobilní bankovníčví	Klientská data	Personální IS	Mzdový IS	Účetníčví	Dochazkový systém	HelpDesk	PZTS, EPS	IDM (řízení přístupových práv)	Podatelna + datové schránky	Archív
1	Zemětřesení	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	Povodně	175	175	225	180	225	225	180	0	0	0	105	105	120	60	0	0	0	90	160
3	Hurikán	105	105	135	80	135	225	450	0	0	0	210	210	240	80	0	360	0	0	0
4	Blesk	0	0	0	0	0	0	135	0	0	0	0	0	0	40	0	180	0	0	120
5	Průmyslová akce	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	Bombový útok	0	0	0	0	0	0	225	0	0	0	0	0	0	0	0	270	0	0	0
7	Použití zbraní	175	175	180	120	180	225	180	225	225	0	140	140	160	60	60	135	120	120	200
8	Požár	70	70	135	120	135	180	270	180	180	360	140	140	160	80	20	135	120	120	160
9	Úmyslná škoda	140	210	270	160	270	270	0	0	0	0	0	0	0	80	80	135	0	120	0
10	Selhání dodávky energie	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	Selhání dodávky vody	0	210	270	160	270	360	180	0	0	0	0	0	0	0	40	0	0	0	0
12	Selhání klimatizace	0	105	135	80	135	180	0	180	180	0	70	70	120	60	40	135	80	90	0
13	Selhání HW	70	105	180	160	180	270	180	0	0	0	0	0	0	0	80	0	0	0	0
14	Kolísání proudu (energie)	35	105	270	160	270	270	180	0	0	0	0	0	0	0	0	0	0	0	0
15	Extrémní teplota a vlhkost	0	70	90	80	90	90	135	0	0	0	0	0	0	0	0	0	0	0	0
16	Prach	140	140	180	120	180	225	0	0	0	0	0	0	0	0	40	0	0	0	0
17	Elektromagnetická radiace	105	140	135	80	135	225	0	0	0	0	0	0	0	0	40	0	0	0	0
18	Elektrostatický náboj	70	105	90	120	180	135	0	225	225	180	140	140	160	40	20	90	120	90	160
19	Krádež	0	0	135	160	180	0	0	225	225	0	140	140	160	0	40	0	80	180	160
20	Neoprávněné použití pamětového média	0	0	180	160	180	0	0	135	135	0	140	140	160	0	20	0	80	180	160
21	Poškození pamětového média	70	105	135	120	180	180	135	135	180	315	315	360	40	20	270	80	120	120	0
22	Chyba provozních zaměstnanců	70	70	90	80	135	135	0	135	135	0	210	210	240	0	20	270	80	0	120
23	Chyba údržby	0	0	135	120	180	180	0	135	135	0	210	210	240	60	40	0	80	90	120
24	Selhání SW	0	0	135	120	180	180	0	180	180	0	140	140	160	0	40	0	120	60	0
25	Použití SW neautorizovanými uživateli	0	0	135	120	180	135	0	135	135	0	105	105	120	0	20	0	120	180	0
26	Použití SW neautorizovaným způsobem	0	140	135	160	180	180	90	675	675	405	140	140	160	120	20	0	120	60	0
27	Předstírání identity uživatele	0	0	90	0	135	0	0	0	0	0	0	0	0	0	0	0	0	0	0
28	Nelegální používání SW	0	0	675	400	900	0	0	900	900	0	525	525	600	0	0	0	400	300	0
29	Škodlivý SW	0	0	180	160	180	0	0	225	225	270	140	140	200	0	20	0	120	150	200
30	Nelegální import/export SW	105	105	135	120	180	135	0	0	0	0	0	0	0	0	0	0	0	0	0
31	Přístup k síti neautorizovanými uživateli	105	105	135	0	135	135	0	0	0	0	0	0	0	0	0	0	0	0	0
32	Použití síťového vybavení neautorizovaným způsobem	0	105	135	0	180	225	0	0	0	0	0	0	0	0	20	0	0	0	0
33	Technické selhání síťových komponent	0	70	0	0	0	0	0	45	45	0	0	0	0	0	20	0	80	0	0
34	Chyba přenosu	105	0	0	0	0	180	0	0	0	0	0	0	0	0	20	180	80	0	0
35	Poškození vedení	0	70	135	0	180	225	0	405	405	0	0	0	0	0	20	0	0	0	0
36	Přetížení provozu	105	105	0	0	0	180	0	270	270	0	0	0	0	0	0	0	0	0	0
37	Odposlech	105	105	0	0	0	135	0	135	135	0	0	0	0	0	0	0	0	0	0
38	Infiltrace komunikací	105	105	0	0	0	0	0	180	180	0	0	0	0	0	0	0	0	0	0
39	Analýza provozu	0	105	90	120	180	135	0	135	135	0	0	0	0	0	20	0	0	0	0
40	Chybné směrování zpráv	0	140	135	160	180	180	0	180	180	0	0	0	0	0	20	0	0	0	0
41	Přesměrování zpráv	0	105	135	120	180	135	0	540	540	405	105	105	120	0	40	0	80	120	200
42	Popření	0	105	0	0	135	225	0	0	0	0	0	0	0	0	0	0	0	0	0
43	Selhání komunikačních služeb (síťových služeb)	0	105	135	120	135	180	0	90	90	135	0	0	0	0	60	0	0	90	120
44	Nedostatek zaměstnanců	105	0	90	120	135	180	0	135	135	360	105	105	120	0	0	0	240	0	0
45	Chyby uživatele	0	70	90	80	90	135	0	135	135	0	0	0	0	0	0	0	0	0	0
46	Nesprávné použití zdrojů																			

PŘÍLOHA P X: VÝSLEDKY HODNOCENÍ RIZIK SE STÁVAJÍCÍMI OPATŘENÍMI

		Infrastruktura	Aktivní síťové prvky	Servery a datová úložiště	Elektronická pošta	AD, doménová struktura	Telefonní ústředna (HW+ SW)	Serverovna (zabezpečené zóny)	Internetové bankovníčnictví	Mobilní bankovníčnictví	Klientská data	Personální IS	Mediový IS	Účetnictví	Docházkový systém	HelpDesk	PZTS, EPS	IDM (řízení přístupových práv)	Podatelna + datové schránky	Archiv
1	Zemětřesení	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	Povodně	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	Hurikán	105	105	135	96	135	135	72	0	0	0	42	42	48	24	0	0	0	54	64
4	Blesk	63	63	81	48	81	90	90	0	0	0	84	84	96	24	0	144	0	0	0
5	Průmyslová akce	0	0	0	0	0	0	54	0	0	0	0	0	0	16	0	72	0	0	72
6	Bombový útok	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	Použití zbraní	0	0	0	0	0	0	90	0	0	0	0	0	0	0	0	162	0	0	0
8	Požár	70	70	72	48	72	90	72	90	90	0	56	56	64	24	24	54	48	48	80
9	Úmyslná škoda	14	28	54	48	54	72	108	108	108	144	28	28	32	24	8	54	48	48	64
10	Selhání dodávky energie	56	84	108	64	108	108	0	0	0	0	0	0	0	48	32	54	0	48	0
11	Selhání dodávky vody	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	Selhání klimatizace	0	126	108	54	108	144	72	0	0	0	0	0	0	0	16	0	0	0	0
13	Selhání HW	0	21	54	32	54	72	0	108	108	0	28	28	48	24	16	81	32	54	0
14	Kolísání proudu (energie)	28	21	72	64	72	108	36	0	0	0	0	0	0	0	32	0	0	0	0
15	Extrémní teplota a vlhkost	21	42	108	64	108	108	72	0	0	0	0	0	0	0	0	0	0	0	0
16	Prach	0	28	36	32	36	36	54	0	0	0	0	0	0	0	0	0	0	0	0
17	Elektromagnetická radiace	84	56	108	72	72	135	0	0	0	0	0	0	0	0	0	0	0	0	0
18	Elektrostatický náboj	63	56	81	48	54	135	0	0	0	0	0	0	0	0	16	0	0	0	0
19	Krádež	28	42	18	24	72	27	0	90	90	72	84	84	96	24	8	54	48	54	96
20	Neoprávněné použití pamětového média	0	0	54	64	72	0	0	90	90	0	56	56	64	0	16	0	32	108	96
21	Poškození pamětového média	0	0	72	64	72	0	0	54	54	0	56	56	64	0	8	0	32	108	96
22	Chyba provozních zaměstnanců	42	42	54	48	72	72	72	54	54	72	189	189	216	24	8	108	32	48	72
23	Chyba údržby	42	28	36	32	54	54	0	54	54	0	126	126	144	0	8	108	32	0	72
24	Selhání SW	0	0	54	48	72	72	0	81	81	0	126	126	144	24	16	0	32	36	72
25	Použití SW neautorizovanými uživateli	0	0	72	64	72	72	0	72	72	0	56	56	64	0	16	0	48	24	0
26	Použití SW neautorizovaným způsobem	0	0	54	48	72	54	0	54	54	0	42	42	48	0	8	0	48	72	0
27	Předstírání identity uživatele	0	56	54	64	72	72	36	270	270	81	56	56	64	48	8	0	48	24	0
28	Nelegální používání SW	0	0	36	0	54	0	0	0	0	0	0	0	0	0	0	0	0	0	0
29	Škodlivý SW	0	0	135	80	180	0	0	180	180	0	105	105	120	0	0	0	80	80	0
30	Nelegální import/export SW	0	0	72	64	72	0	0	90	90	108	84	84	120	0	8	0	48	80	80
31	Přístup k síti neautorizovanými uživateli	42	42	54	48	72	54	0	0	0	0	0	0	0	0	0	0	0	0	0
32	Použití síťového vybavení neautorizovaným způsobem	42	42	54	0	54	54	0	0	0	0	0	0	0	0	0	0	0	0	0
33	Technické selhání síťových komponent	0	42	54	0	72	90	0	0	0	0	0	0	0	0	8	0	0	0	0
34	Chyba přenosu	0	28	0	0	0	0	0	18	18	0	0	0	0	0	8	0	32	0	0
35	Poškození vedení	42	0	0	0	0	72	0	0	0	0	0	0	0	0	8	72	32	0	0
36	Přetížení provozu	0	28	54	0	72	90	0	162	162	0	0	0	0	0	8	0	0	0	0
37	Odposlech	42	42	0	0	0	72	0	108	108	0	0	0	0	0	0	0	0	0	0
38	Infiltrace komunikací	42	42	0	0	0	54	0	54	54	0	0	0	0	0	0	0	0	0	0
39	Analýza provozu	42	42	0	0	0	0	0	72	72	0	0	0	0	0	0	0	0	0	0
40	Chybné směrování zpráv	0	42	36	48	72	54	0	54	54	0	0	0	0	0	8	0	0	0	0
41	Přesměrování zpráv	0	56	54	64	72	72	0	72	72	0	0	0	0	0	8	0	0	0	0
42	Popření	0	42	54	48	72	54	0	108	108	162	42	42	48	0	16	0	32	48	80
43	Selhání komunikačních služeb (síťových služeb)	0	42	0	0	54	90	0	0	0	0	0	0	0	0	0	0	0	0	0
44	Nedostatek zaměstnanců	0	63	81	72	81	108	0	36	36	81	0	0	0	0	24	0	0	36	48
45	Chyby uživatele	42	0	36	48	54	108	0	27	27	144	42	42	48	0	0	0	96	0	0
46	Nesprávné použití zdrojů	0	28	36	32	36	54	0	54	54	0	0	0	0	0	0	0	0	0	0