Aplikace procesu managementu kontinuity činností organizace v průmyslu komerční bezpečnosti

Application of Process of Business Continuity Management in the Commercial Security Industry

Bc. Blanka Bilová

Diplomová práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

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

Jméno a příjmení:	**Bc. Blanka BILOVÁ**
Osobní číslo:	**A11366**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Aplikace procesu managementu kontinuity činností organizace v průmyslu komerční bezpečnosti**

Zásady pro vypracování:

1. **Popište základní principy procesu managementu kontinuity činností.**
2. **Analyzujte požadavky na obsah dokumentace managementu kontinuity činností.**
3. **Navrhněte a zdůvodněte oblasti aplikace managementu kontinuity činností v průmyslu komerční bezpečnosti.**
4. **Na modelovém příkladu obchodní společnosti zpracujte plán kontinuity činností.**
5. **Navrhněte kriteria hodnocení managementu kontinuity činností organizace.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **HILES, Andrew. The Definitive Handbook of Business Continuity Management. 3. vyd. 2011. ISBN 9780470670149.**
2. **ENGEMANN, Kurt J. a Douglas M HENDERSON. Business Continuity and Risk Management: Essentials of Organizational Resilience. Rothstein Associates, Inc, 2012. ISBN 978-1-931332-54-5.**
3. **ČSN BS 25999-1. Management kontinuity činností organizace - Část 1: Soubor zásad. Praha: ČNI: 2009. 52 s. Třídící znak 010370.**
4. **ČSN ISO/IEC 27001. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky. Praha: ÚNMZ, 2006. 36 s. Třídící znak 369790.**
5. **ESTALL, Hilary. Business Continuity Management Systems. British Computer Society, 2012. 128 p. ISBN 1780171463.**

Vedoucí diplomové práce: **Ing. Jan Valouch, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **8. února 2013**

Termín odevzdání diplomové práce: **3. června 2013**

Ve Zlíně dne 8. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce je zaměřena na možnosti aplikace procesu managementu kontinuity činností organizace v průmyslu komerční bezpečnosti. Úvodní část obsahuje základní principy procesu kontinuity činnosti v souvislosti se základními technickými normami v dané oblasti. Po uvedení norem, je provedena analýza požadavků, podle kterých se postupuje v případě zavedení procesu kontinuity činnosti organizace do obchodní společnosti, a jsou rozebrány jednotlivé fáze plánu kontinuity činností. Dále je řešena otázka požadavků na dokumentaci pro proces kontinuity činností organizace. Výstupem práce je pak, na základě získaných teoretických poznatků, objasnit problematiku kontinuity činnosti z hlediska využití v průmyslu komerční bezpečnosti a následně na modelovém příkladu provést analýzu hrozeb, spolu se zpracováním strategií směřujících k eliminaci, popř. vyloučení případných rizik. Závěr práce popisuje plán kontinuity činností a prezentuje zpracovaný návrh kritérií hodnocení managementu kontinuity činností organizace.

Klíčová slova: management kontinuity činností, analýza, riziko, hrozba, plán kontinuity činností organizace.

ABSTRACT

The thesis is focused on the possibility of application of the process of business continuity management in the commercial security industry. The introductory part contains the basic principles of the process of business continuity in the context of basic technical standards in the field. After putting standards, the analysis requirements that shall be applied to the process of introducing business continuity in the company and is focused on different phases of the business continuity plan. It is also addressed in the documentation requirements for business continuity process. The output of the work is based on theoretical knowledge, clarify issues BCM of terms used in the commercial security industry and consequently the model example to analyze threats, together with the processing strategies to eliminate or avoid possible risks. The conclusion describes the business continuity plan and presents prepared proposal evaluation criteria of business continuity management.

Keywords: business continuity management, analysis, risk, threat, business continuity plan.

Na tomto místě bych velmi ráda poděkovala mému vedoucímu diplomové práce panu Ing. Janu Valouchovi, Ph.D. za vstřícný přístup a cenné podněty a připomínky, kterými významně přispěl ke konečné podobě této diplomové práce.

Poděkování patří také mé rodině za jejich podporu po celou dobu studia a v neposlední řadě můj dík patří mým přátelům, kteří mi vědomě a často i nevědomě dodávali optimismus a sílu.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové 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 práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byla jsem seznámena s tím, že na moji diplomovou 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 práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové 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 práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Obchodní společnosti, které chtějí být v dnešní době úspěšné na trhu, musí být vždy připraveny na plynulý chod činnosti společnosti. Za hlavní cíl každé obchodní společnosti se považuje úspěch na trhu, kterého lze dosáhnout právě tím, že si společnost stanoví priority, představu o vývoji budoucnosti a jasný cíl, kterého chce dosáhnout. V dnešní ekonomické situaci není pro žádnou společnost jednoduché udržet se v konkurenčním boji na předních místech za zcela běžných podmínek. Proto každá společnost, která chce být o krok napřed, by měla zvážit a zajistit plynulý chod svých činností i v případě nečekané události, která může ohrozit činnost jejich hlavních procesů. Nikdo z nás nedokáže odhadnout, co se v budoucnosti stane a jaké následky vyvstanou v případě nečekané události. Pokud ale tyto situace nastanou, měla by být společnost na tyto hrozby připravena. Není-li společnost připravena na nenadálé události, dá se předpokládat, že riziko ztrát při vzniku nečekané události způsobí spíše negativní dopad a to téměř na celý chod společnosti.

Právě prostřednictvím řízení kontinuity činností (BCM - Business Continuity Management) lze toto riziko ztrát snížit. Mohlo by se zdát, že plán kontinuity činnosti je součástí managementu pouze u větších společností, ale dle mého názoru i malé společnosti by měly zvážit tuto možnost, protože nejen u velkých společností nastávají nečekané události, na které by měly být společnosti připraveny. Není pravidlem, že větší společnosti mají vyšší pravděpodobnost vzniku nečekané události a menší společnosti pravděpodobnost vzniku malou. Riziko vzniku této nečekané události nelze nijak předvídat, důležitější je, jak je společnost na riziko připravena. Další otázkou je pak riziko ztrát. I v tomto případě nemůžeme spoléhat na to, že velké společnosti mají velké ztráty a malé společnosti ztráty malé. Z hlediska možností vytvoření plánu kontinuity činnosti (BCP - Business Continuity Plan) jsou větší společnosti na tom lépe, ať už z finančního hlediska, tak i personálního a to z důvodu toho, že na vytvoření plánu se podílí větší množství lidí, tím pádem, i z finančního hlediska bude vytvoření plánu náročnější. První impuls k zavedení kontinuity činnosti organizace by měl být v rukou vedení společnosti, má-li zájem a snahu o to, aby se jejich společnost stala společností moderní, a tím pádem žádanější na trhu. Správný management každé moderní společnosti by se měl soustředit na známé pořekadlo: „Kdo je připraven, není zaskočen“. Není na místě vytvářet plán až v případě, kdy nečekaná událost

nastane, ale mít ho již prostřednictvím řízení kontinuity činnosti vytvořen a tím zachovat celý chod společnosti s minimálními ztrátami.

Hlavním přínosem této práce je seznámení s problematikou tvorby BCP a na modelovém příkladu obchodní společnosti představit možnosti aplikace BCM v průmyslu komerční bezpečnosti.

I. TEORETICKÁ ČÁST

1 PRINCIPY MANAGEMENTU KONTINUITY ČINNOSTÍ

Proces řízení kontinuity činnosti organizace není v naší republice pro žádnou obchodní společnost povinností. V současné době neexistuje zákonná úprava, která by řešila problematiku týkající se kontinuity činnosti organizace. Pro řídící proces, který má za hlavní cíl zajistit plynulost klíčových procesů byl vytvořen standard ČSN BS 25999. Jedná se o normu, která je pro společnosti doporučující v případě zavedení kontinuity činnosti organizace. Z hlediska bezpečnosti společnosti, se ale setkáváme i s dalšími normami, které jsou z hlediska bezpečnosti společnosti více používané a tím známější.

Z tohoto důvodu se v této kapitole zaměřím na požadavky, pokyny a doporučení relevantních technických norem, které souvisí s pojmem bezpečnost. Jedná se především o nejpoužívanější normu ISO/IEC 27000. Řada této normy se zabývá především systémem řízení bezpečnosti informací.

1.1 Význam BCM

Management kontinuity činností organizací (BCM) představuje proces, který zavádí obchodní společnosti, které mají snahu fungovat na trhu, a to aniž by došlo k jakémukoli přerušení činnosti organizace při vzniku nenadálé situace. Podle normy ČSN BS 25999-1 je definice BCM organizací vlastněný a řízený proces, který zakládá pro svůj účel vhodné strategie a operační rámec, který:

- proaktivně[1] zvyšuje odolnost organizace proti narušení její schopnosti dosahovat klíčových cílů,
- poskytuje vyzkoušenou metodu obnovení její schopnosti realizovat klíčové produkty a služby na stanovené úrovni a ve stanovený čas po přerušení,
- přináší prokazatelnou způsobilost zvládat přerušení činností organizace a chránit reputaci a jméno organizace. [1]

[1] Proaktivně řídit znamená efektivně vyhledávat možná rizika a tím jim účelně předcházet. K zabezpečení kontinuity činností nestačí pouze reagovat na vznik incidentů.

1.2 Důvody pro aplikaci BCM v obchodní společnosti

Obchodní společnosti, které chtějí být na trhu úspěšné, musí mít zpracované plány, které obsahují záměry a cíle, kterých chce společnost dosáhnout. Jedná se o dosažení krátkodobých, střednědobých a dlouhodobých cílů společnosti. Prostřednictvím BCM plánu lze těchto záměrů a cílů dosáhnout i v případě, že by došlo k neočekávanému přerušení chodu společnosti. V případě neočekávané události nelze veškerá rizika eliminovat úplně, ale lze jejich dopady zmírnit. Mezi hlavní následky patří zejména ztráty na životě, majetku nebo neschopnost dodávání produktů. Ve své podstatě, jde o soustředění se na dopady přerušení, které prostřednictvím BCM identifikuje činnosti, na kterých závisí přežití organizace. BCM vytváří plán, prostřednictvím kterého lze přiměřeně reagovat na přerušení provozu. Tím se tento proces plánování stává významným kladným krokem každé obchodní společnosti, nikoliv záporným.

1.3 Terminologie v oblasti řízení kontinuity činnosti organizace

V úvodní části je potřeba uvést základní pojmy v oblasti řízení kontinuity činnosti organizace. Je to z důvodu rychlejší orientace a správného pochopení výrazů a pojmů, se kterými se v práci často setkám. Tím se minimalizuje možnost špatného porozumění celé problematiky řízení kontinuity činností.

Terminologii je vytvořena na základě normy BS 25999-1 (Řízení kontinuity činností organizace - Část 1:Soubor zásad) je českou verzí britské normy a rozhodla jsem ji seřadit abecedně pro lepší orientaci.

Analýza dopadů - Business Impact Analysis (BIA)

Jedná se o nejdůležitější část řízení kontinuity činností. Jde o proces, při kterém společnost analyzuje veškeré své procesy a zjišťuje v případě jejich přerušení dopad na celý chod společnosti. Na základě této analýzy se zkoumá jak finanční dopady (zisk, ztráta) tak i nefinanční dopady (zachování dobrého jména společnosti).

Cíl obnovy činnosti - Recovery Point Objective (RPO)

Tato činnost představuje dobu, po kterou lze akceptovat ztrátu údajů, přerušení činnosti, služeb a dále pak jak dlouho dokáže existovat bez přístupu k těmto údajům, činnostem.

Snahou je, aby se neztratilo více dat, než je maximum pro každou činnost (Maximum Tolerable Data Loss - MTDL).

Maximální přijatelná ztráta údajů - Maximum tolerable data loss (MTDL)

V případě vzniku nečekané události dochází ke ztrátě údajů. Jde o ztráty dat, které mají vliv na klíčové procesy společnosti. Z tohoto důvodu existuje pojem maximální přijatelná ztráta údajů což je ztráta údajů, kde ztrátu těchto údajů lze akceptovat, aby byl zachován celý chod společnosti.

Činnost - Activity

Soubor veškerých procesů obchodní společnosti, vlastním jménem za účelem tvorby produktů nebo poskytování služeb.

Doba obnovy činnosti - Recovery Time Objective (RTO)

Představuje ideální čas, do kterého je potřeba obnovit funkci kritického procesu po nečekaném přerušení. Jedná se o obnovu klíčových procesů společnosti. Nesmí být ale překročen maximální interval výpadku pro jednotlivé činnosti (Maximum Tolerable Period of Disruption MTPD).

Maximální přijatelný interval výpadku - Maximum Tolerable Outage (MTO)

Interval výpadku, vyjádřený časově. Maximálně přijatelný výpadek činnosti společnosti, ve kterém nedojde k ohrožení činnosti společnosti.

Minimální úroveň poskytování služeb - Minimal Required Service Level (MRSL)

Stanovení minimální úrovně poskytování služeb, výroby, při které je zajištěno dosažení stanovených cílů společnosti.

Dopad - Impact

Jedná se o vyhodnocený následek konkrétního výsledku.

Havárie

Havárie dělíme do dvou skupin a to na nepředvídatelnou událost (výpadek el. energie) a předvídatelnou událost (povodně, sněhová kalamita). Jde o činnost, která má vážný dopad na činnost společnosti a díky této havárii dochází k přerušení činnosti nebo ukončení činnosti.

Incident

Představuje nečekanou a nestandardní událost, která způsobuje problémy, přerušení činnosti organizace nebo dokonce až nečekanou krizi.

Kontinuita činnosti organizace - Business Continuity

Úkolem kontinuity činnosti organizace je zabezpečení plynulého chodu klíčových procesů obchodní společnosti (vhodným plánováním a následnou reakcí na incidenty) v případě nečekané události a to zejména zachování provozu na předem stanovené úrovni.

Management kontinuity činnosti organizace - Business Continuity Management (BCM)

Jedná se o dynamický, holistický[2] proces managementu, který pracuje s různorodými proměnnými, které identifikují potenciální hrozby s jejich následným dopadem. Zabývá se tím, aby v případě naplnění těchto hrozeb byla obchodní společnost schopna reagovat a být odolná vůči těmto hrozbám. Hlavním cílem je zabezpečení a zachování klíčových zájmů společnosti, zúčastněných stran a udržení dobré pověsti.

Plán kontinuity činnosti - Business Continuity Plan (BCP)

V případě vzniku havárie má obchodní společnost vytvořen soubor, ve kterém jsou uloženy sestavené plány, které se využijí právě v případě vzniku nečekané události, aby byl zachován nepřetržitý chod společnosti.

Plán managementu incidentů - Incident Management Plan (IMP)

Při vzniku incidentu je vytvořen striktní plán činností, které obsahuje souhrnný popis, kdo, co, kdy, za jakých podmínek bude konat. Jeho obsahem jsou především určeni klíčoví zaměstnanci, zdroje, činnosti, služby, které jsou potřebné ke zvládání nečekané události.

---

[2] **Holismus** (z řeckého to holon, celek) je filosofický názor nebo směr, který zdůrazňuje, že všechny vlastnosti nějakého systému nelze určit nebo vysvětlit pouze zkoumáním jeho částí. Naopak celek podstatně ovlivňuje i fungování nebo podobu svých částí. Tuto zásadu vyslovil poprvé Aristotelés v Metafysice: „Celek je víc než souhrn jeho částí.“

Plán obnovy - Disaster Recovery Plan (DRP)

Dokument, který lze označit jako havarijní plán. Popisuje zdroje, činnosti, úkoly, které je potřeba zajistit na obnovu technických prostředků společnosti. Plány obnovy jsou při zavádění kontinuity činnosti podmnožinou plánu kontinuity činnosti (BCP) a zabývají se především klíčovými procesy společnosti.

Program managementu kontinuity činnosti organizace - Business continuity management programme

Za podpory vedení společnosti a managementu je zaveden tento řídící a nepřetržitý proces, který je vybaven prostředky, které mají za úkol identifikaci hrozeb, jejich potenciálních ztrát a udržování navržených strategií obnovy plánů za účelem zajištění kontinuity služeb prostřednictvím školení, výcviku, přezkoumávání.

Přerušení - Disruption

Situace, která je buď očekávaná, nebo neočekávaná a její vznik způsobí narušení běžné činnosti společnosti. Při vzniku většího přerušení se pak již jedná o havárii.

Strategie obnovy - Recovery strateg

V případě vzniku nečekané události (havárie) jsou z hlediska strategie určeny a vybrány činnosti, které mají za úkol obnovit činnost společnosti na předem stanovenou úroveň.

Testování - Exercise

Činnost, která slouží ke zkoušení celého nebo jen některé z částí plánu kontinuity činnosti organizace, ať už z hlediska obsahu informací nebo dosažení stanoveného výsledku. Možností testování je simulace incidentu, při němž se testují jednotlivé role zaměstnanců a jejich zvládnutí.

Životní cyklus managementu kontinuity činností organizace - Business continuity management lifecycle

Souhrn činností z hlediska jednotlivých fází programu managementu kontinuity činností organizace.

1.4 Legislativní požadavky na BCM

1.4.1 Systém řízení bezpečnosti informací

Mezinárodní normy pod označením ISO vydává Mezinárodní organizace pro standardizaci ISO (International Organization for Standardization). Jedná se o světovou federaci národních normalizačních organizací se sídlem v Ženevě, která byla založena v roce 1947. Normy ISO mají celosvětovou působnost, ale nejvíce jsou rozšířeny v Evropských zemích.

ISO/IEC 27000 (Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník), zabývající se bezpečností informací má za úkol sjednotit doporučení a požadavky, které se vyskytují v různých normách. Jedná se o určitý postup, návod jak by měly společnosti v této oblasti postupovat. [2]

Norma ISO/IEC 27000 upravuje:

- základní terminologii,
- definice pravidel v oblasti ISMS (Information Safety Management System).

Tato norma je pouze úvodem do oblasti bezpečnosti informací a obchodní společnosti si musí vybrat konkrétní normu, prostřednictvím které vyřeší své konkrétní potřeby.

Na tuto úvodní normu pak navazuje řada dalších norem.

Z hlediska tématu práce se zaměřím na tyto normy:

- ISO/IEC 27001 - Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky,
- ISO/IEC 27002 - Informační technologie - Bezpečnostní techniky - Soubor postupů pro řízení informační bezpečnosti.

1.4.2 Systém managementu bezpečnosti informací

Pro zlepšování a udržování systému managementu bezpečnosti informací vznikla norma *ISO/IEC 27001:2005 (Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky).* Tato norma se považuje za hlavní normu rodiny ISO 27000 a na základě této normy se provádí certifikace. Dále se používá k nezávislému posouzení, zdali je organizace schopna vytvořit a udržovat celkový systém

informační bezpečnosti. ISO 27001 se stala nástupcem normy BS 7799-2:2002. Hlavním úkolem této normy je plynulý proces zlepšování, implementace a zdokonalování veškerého systému řízení informační bezpečnosti prostřednictvím modelu PDCA. Zkratka PDCA je složena ze čtyř anglických slov (Plan - Do - Check - Act) - (Plánuj - Dělej - Kontroluj - Jednej). Modelu PDCA se budu více zabývat v kapitole 2.1.

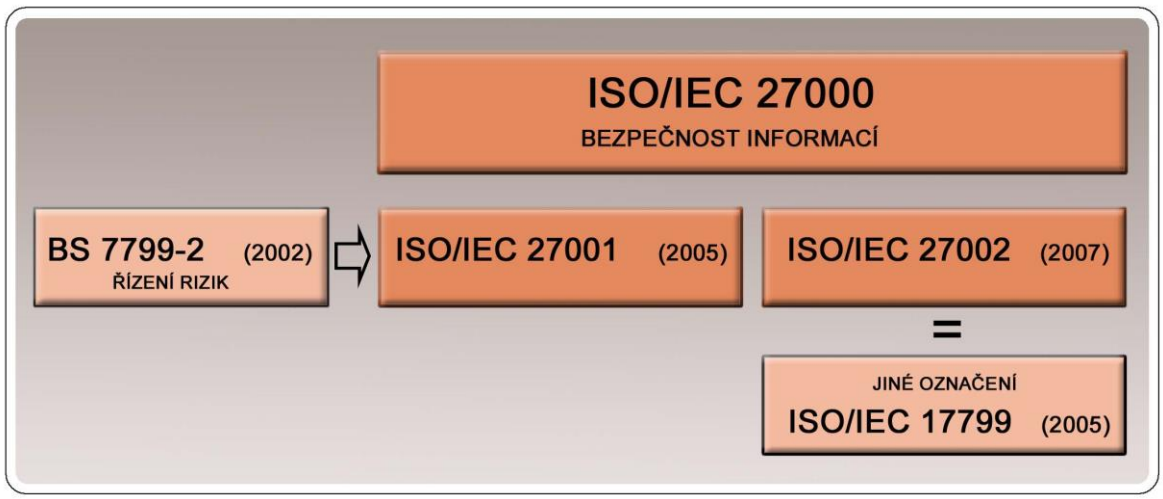
Norma stanoví základní požadavky pro ustavení, zavedení, provozování, monitorování, udržování a zlepšování systému managementu bezpečnosti informací (ISMS). Organizace musí:

- určit rozsah a hranice ISMS na základě posouzení specifických rysů činností organizace, jejího uspořádání, struktury, umístění (lokality), aktiv a technologií,
- definovat politiku ISMS,
- stanovit přístup k hodnocení rizik (identifikovat metodiku, vytvořit kritéria),
- identifikovat rizika (identifikovat aktiva, hrozby pro tato aktiva, zranitelnost, dopady),
- analyzovat a vyhodnocovat rizika (posoudit dopady na činnost organizace, posoudit reálnou pravděpodobnost hrozeb),
- identifikovat a vyhodnotit varianty pro zvládání rizik (aplikace vhodných opatření, vyhnutí se rizikům, přenesení rizik na třetí strany např. pojišťovny),
- formulovat plán zvládání rizik, který vymezí činnost vedení, zdroje, odpovědnosti a priority,
- provádět interní audity ISMS v plánovaných intervalech,
- provádět odpovídající opravné a preventivní činnosti (aplikace výsledků auditů),
- dokumenty musí obsahovat prohlášení politiky a cílů ISMS, rozsah ISMS, postupy a opatření, popis použitých metodik, plán zvládání rizik, prohlášení o aplikovatelnosti,
- dokumenty musí být chráněny a řízeny. [3]

1.4.3 Soubor postupů pro řízení informační bezpečnosti

Norma *ISO/IEC 27002:2007 (Informační technologie - Bezpečnostní techniky - Soubor postupů pro řízení informační bezpečnosti)* nahradila v roce 2007 původní normu BS 17799:2005. Kromě názvu se v normě nic nezměnilo, tudíž se můžeme setkat s použitím obou variant. Jedná se o soubor nejlepších postupů, které slouží jako kontrolní seznam bezpečnosti informací. Není nikde definováno, která opatření mají být aplikována, rozhodnutí o aplikaci je již na každé obchodní společnosti. Podstatou je, že vhodná opatření vybírají společnosti na základě výsledků analýzy rizik s následnou realizací při konkrétní situaci. K využití mé práce je nejzajímavější část Řízení kontinuity činností organizace, která je právě věnována řízení kontinuity činností organizace z hlediska bezpečnosti informací. Stanoví zejména:

- hlavní cíl, kterým je ochrana procesů organizace před následky závažných selhání informačních systémů nebo katastrof a co nejdříve zajistit obnovu činnosti,
- zpracování řízení kontinuity činnosti v méně rozsáhlé podobě, než je v normě BS 25999,
- opatření k identifikaci a minimalizaci rizik,
- opatření k omezení důsledků škodlivých incidentů,
- opatření k včasné dostupnosti informací potřebných pro obnovení nezbytných činností. [4]



Obr. 1: Struktura normy ISO/IEC 27000 [2], upravila Bilová, 2013

1.4.4 Veřejně dostupná specifikace pro řízení kontinuity

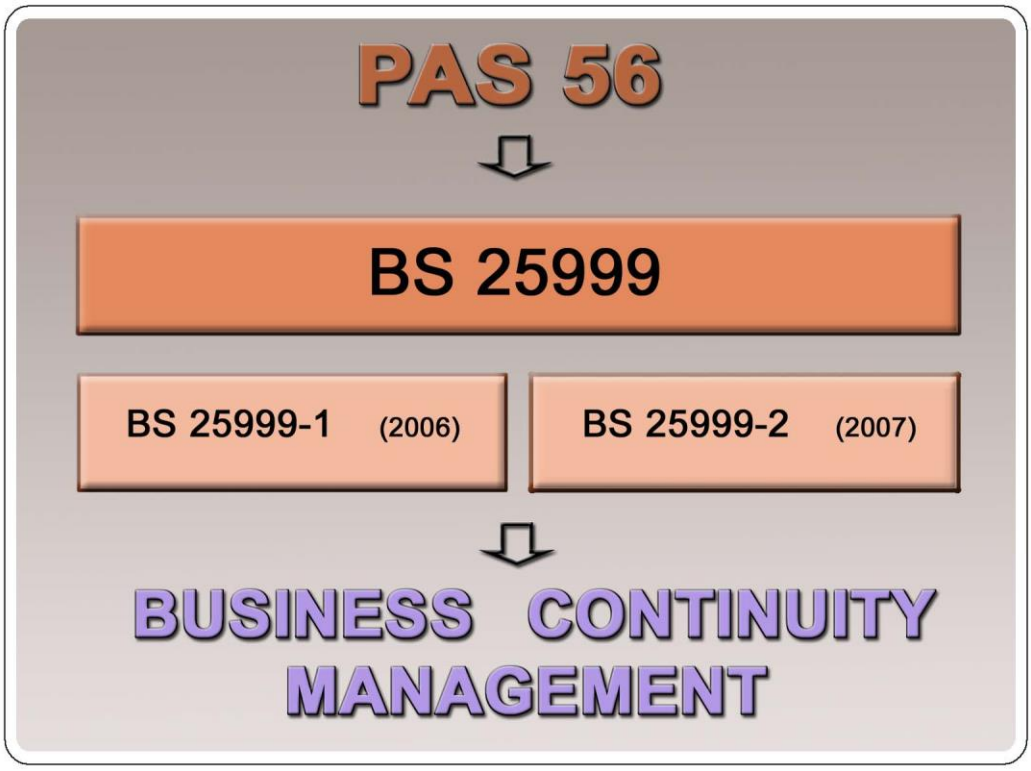
PAS 56 - Veřejně dostupná specifikace pro řízení kontinuity podnikání (Publicly Available Specification) „Guide to Business Continuity Management“ vydána britským normalizačním institutem British Standards Institute, BSI v roce 2003. Tento dokument vznikl jako průvodce pro zavedení procesu, principů a terminologie v oblasti řízení kontinuity činností organizace. Hlavním obsahem je identifikace potenciálních dopadů, které ohrožují organizace a poskytují rámec pro zvyšování odolnosti a schopnosti pro účinnou reakci. V definici byly také stanoveny postupy pro ochranu zájmů klíčových zainteresovaných subjektů, pověst a značku společnosti. Není zde popisován jen pohled z hlediska účinné reakce a snížení zrát, ale je zde poukázáno na možnosti strategií pro maximalizaci zisku. Toho lze dosáhnout pouze tehdy, když organizace účinně reaguje na rizika, které jí hrozí a musí mít za cíl obnovení obchodních činností zejména z pohledu zákazníka, tím se sníží ztráty. Hlavní část tohoto dokumentu je ale věnována právě životnímu cyklu, který představuje kontinuální cyklický proces podporující činnost podnikání. Tento životní cyklus je nastaven tak, aby prostřednictvím kontinuálního procesu, v němž obchodní společnosti vykonávají svoji činnost, byly vylepšovány jejich plány, procesy a pohotovostní reakce na kritické události. PAS 56 představuje základ pro normu, která právě PAS 56 nahradila. Jedná se o normu BS 25999, která je pro řízení kontinuity činnosti organizace doporučující a v současné době aktuální. [5]

1.4.5 Řízení kontinuity činností organizace

Norma *ČSN BS 25999-1:2006 - Řízení kontinuity činností organizace - Část 1:Soubor zásad* [1] je českou verzí britské normy. V této části normy je definována základní terminologie managementu kontinuity činností organizace a dále jsou popsány jednotlivé fáze k zavedení procesu kontinuity činností. Hlavním obsahem normy je popis postupů pro zavedení kontinuity činností a vytvoření analýzy společnosti, stanovení rizik, jejich dopadů a návrh strategií s následným testováním plánů kontinuity. Tuto normu mohou používat jakékoliv společnosti, které mají zájem zjistit a zhodnotit schopnost organizace ve splňování požadavků zákazníků, ale i požadavků samotné společnosti.

Další část této normy je pouze v anglické verzi a není prozatím proveden překlad do české verze Úřadem pro technickou normalizaci. Jedná se o *BS 25999-2:2007 - Řízení kontinuity činností organizace - Část 2: Specifikace.* Tato část již konkrétně stanovuje, co musí

společnost udělat pro zavedení systému řízení kontinuity činností. Jedná se o požadavky, které mohou být objektivně kontrolovány. Jedině tak může společnost uvádět pro další společnosti, že má úspěšně vytvořen systém řízení kontinuity činností. Na základě normy BS 25999-2 se provádí certifikace systémů řízení kontinuity činností.



Obr. 2: Standard BCM

1.4.6 Zákony v rámci havarijního a krizového plánovaní

Jak již bylo uvedeno, tak v České republice není v žádné zákonné úpravě povinnost zavádění procesu řízení kontinuity činnosti organizace. Z hlediska zákonné úpravy existují zákony, vyhlášky, nařízení vlády, které vyžadují plánování a přípravu havarijních a krizových plánů, které jsou velmi podobné plánům spojených s řízením kontinuity činnosti organizace. Jelikož je plán kontinuity činnosti velmi podobný havarijnímu a krizovému plánu, v této kapitole uvedu zákony spojené s havarijním a krizovým plánováním. Rozdíl mezi havarijním a krizovým plánem a plánem kontinuity činnosti je ten, že havarijní a krizové plány mají některé organizace ze zákona povinné. Havarijní plány mají na základě § 32 zákona č. 59/2006 Sb., o prevenci závažných havárií mít vypracovány objekty a zařízení, v nichž je umístěna vybraná nebezpečná chemická látka nebo chemický přípravek.

Cílem je snížit pravděpodobnost vzniku a omezit následky závažných havárií na zdraví a životy lidí, hospodářských zvířat, životního prostředí a majetku.
Na základě § 3 zákona č. 59/2006 Sb., organizace jsou povinné vytvořit plán a bezpečnostní dokumentaci dle skupiny, kam jsou zařazeny. Skupiny dělíme:

- skupina A - bezpečnostní program prevence závažné havárie a plán fyzické ochrany,
- skupina B - bezpečnostní zpráva, vnitřní havarijní plán, podklady pro stanovení zóny havarijního plánování a zpracování vnějšího havarijního plánu a plán fyzické ochrany. [6]

Z hlediska krizového plánování ukládá nařízení vlády č. 462/2000 Sb. krizového zákona, zpracovat krizové plány pro ochranu veřejného zájmu orgánům veřejné správy. Pokud se jedná o plány krizové připravenosti, ty zpracovávají právnické osoby a subjekty v souvislosti s územním krizovým plánem. Obsahem krizového plánu (kraje, obce s rozšířenou působností) je souhrnný postup při vzniku mimořádné události, při níž je vyhlášen jeden z krizových stavů: stav nebezpečí, nouzový stav, stav ohrožení státu, válečný stav.

Havarijní plán

Je vytvořen pro případ vzniku mimořádné události, při které je vyhlášen třetí nebo zvláštní stupeň poplachu a je přílohou Krizového plánu. Obsahem plánu je informační část, operativní část a druhy jednotlivých plánů pro konkrétní činnosti.

Krizový plán

V případě vzniku krizové situace je vytvořen souhrn krizových opatření a postupů. V základní části je vymezena působnost, odpovědnost a úkoly správních úřadů a ostatních státních orgánů, orgánů samosprávy, které mají povinnost zpracovat krizový plán, stanovení a hodnocení možných krizových rizik, jejich dopad na území a činnost jednotlivých organizačních složek státu. V příloze je pak přehled prostředků a osob k eliminaci krizových situací, typové plány, katalog krizových opatření a operační plány.

Přehled zákonů souvisejících s havarijním a krizovým plánem:

- Zákon č. 59/2006 Sb., o prevenci závažných havárií,
- Zákon č. 238/2000 Sb., o hasičském záchranném sboru České republiky a o změně

některých zákonů,

- Zákon č. 239/2000 Sb., o integrovaném záchranném systému a změně některých zákonů,
- Zákon č. 240/2000 Sb., o krizovém řízení a změně některých zákonů (krizový zákon),
- Zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů.

Dílčí závěr

První kapitola byla úvodem z hlediska legislativy do procesu řízení kontinuity činnosti organizace. Proces řízení kontinuity činnosti je spjat s pojmem bezpečnosti, proto bylo důležité uvést normu zabývající se právě bezpečností - ISO/IEC 27001. Z důvodu méně známé formy řízení procesu managementu společnosti bylo nutné uvedení základní legislativy z této oblasti a to zejména popis normy BS 25999, která je stěžejní pro další kapitoly. Hlavním výstupem procesu řízení kontinuity činnosti organizace je vytvoření plánu kontinuity činnosti organizace a tento plán je velmi podobný havarijnímu a krizovému plánu, proto je v této části uvedeno několik základních zákonných úprav, které souvisí právě s havarijními a krizovými plány. Aby nedocházelo k nesrovnalostem významu některých pojmů, součástí této kapitoly je základní terminologie z řízení kontinuity činnosti. Legislativa pro oblast řízení kontinuity činnosti není až tak obsáhlá, hlavním úkolem je správné pochopení základní normy BS 25999, která bude podrobněji rozebrána v následující části.

2 ANALÝZA POŽADAVKŮ NA OBSAH DOKUMENTACE BCM

K analýze požadavků na obsah dokumentace k zavedení kontinuity činnosti organizace je nutné představit normu, která je pro tuto činnost zásadní. Z tohoto důvodu je tato kapitola zaměřena na analýzu normy *ČSN BS 25999-1:2006 Řízení kontinuity činností organizace - Část 1: Soubor zásad (Code of practice for business continuity management).*

Obsahem normy je soubor zásad, které musí management obchodní společnosti dodržovat v případě aplikace řízení kontinuity činností organizace do obchodní společnosti. Jde o podrobný popis požadavků pro zavedení praktik, kterými lze dosáhnout účinného řízení kontinuity činností.

Neméně významná je i druhá část normy *BS 25999-2:2007 Řízení kontinuity činností organizace - Část 2: Specifikace (Specification for business kontinuity management)*, která se zabývá požadavky na implementaci, provozování a zlepšení kontinuity činnosti organizace. Vzhledem k tomu, že je tato část normy prozatím v anglické verzi, budu se v práci zabývat první částí uvedené normy. Je ale nutné uvést to, že na základě této normy se v zahraničí provádí certifikace pro zavedení systému kontinuity činností organizace. [7]

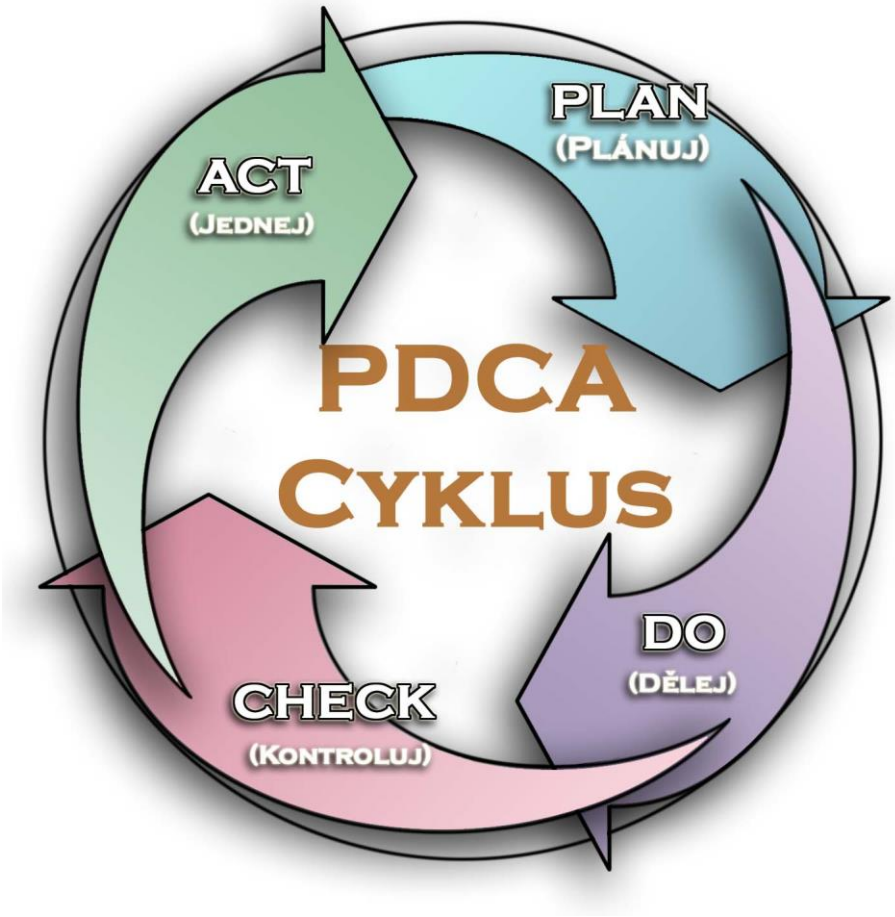
Protože je tato norma pro většinu organizací neznámá, je důležité si uvést základy, které tato norma tvoří. Zaměřuje se nejen na tvorbu plánů, pravidel, prevenci a snížení následků, ale také na provozní procesy, které tyto činnosti realizují. Jedná se o činnost, která je začleněna do činnosti managementu organizace, který se zabývá především plynulým chodem činnosti společnosti. V normě jsou uvedeny požadavky na dokumentaci, které jsou nutné při zavedení řízení kontinuity činností organizace.

2.1 Životní cyklus managementu kontinuity činností (PDCA)

2.1.1 Cyklus PDCA

Důležitým procesem pro zachování kontinuity činností při zavedení BCM je postup činností, tzv. PDCA cyklus. Jedná se o systémový přístup k řízení, který je založen na práci Waltera A. Shewharta, který ve 30. letech dvacátého století vyvinul ve Spojených státech řízení statistického procesu. Tu převzal a od 50. let dvacátého století dále velmi úspěšně propagoval proslulý odborník v oblasti řízení jakosti W. Edwards Deming, a stále se ve velkém měřítku používá k dosahování kontinuálního zlepšování systémů řízení.

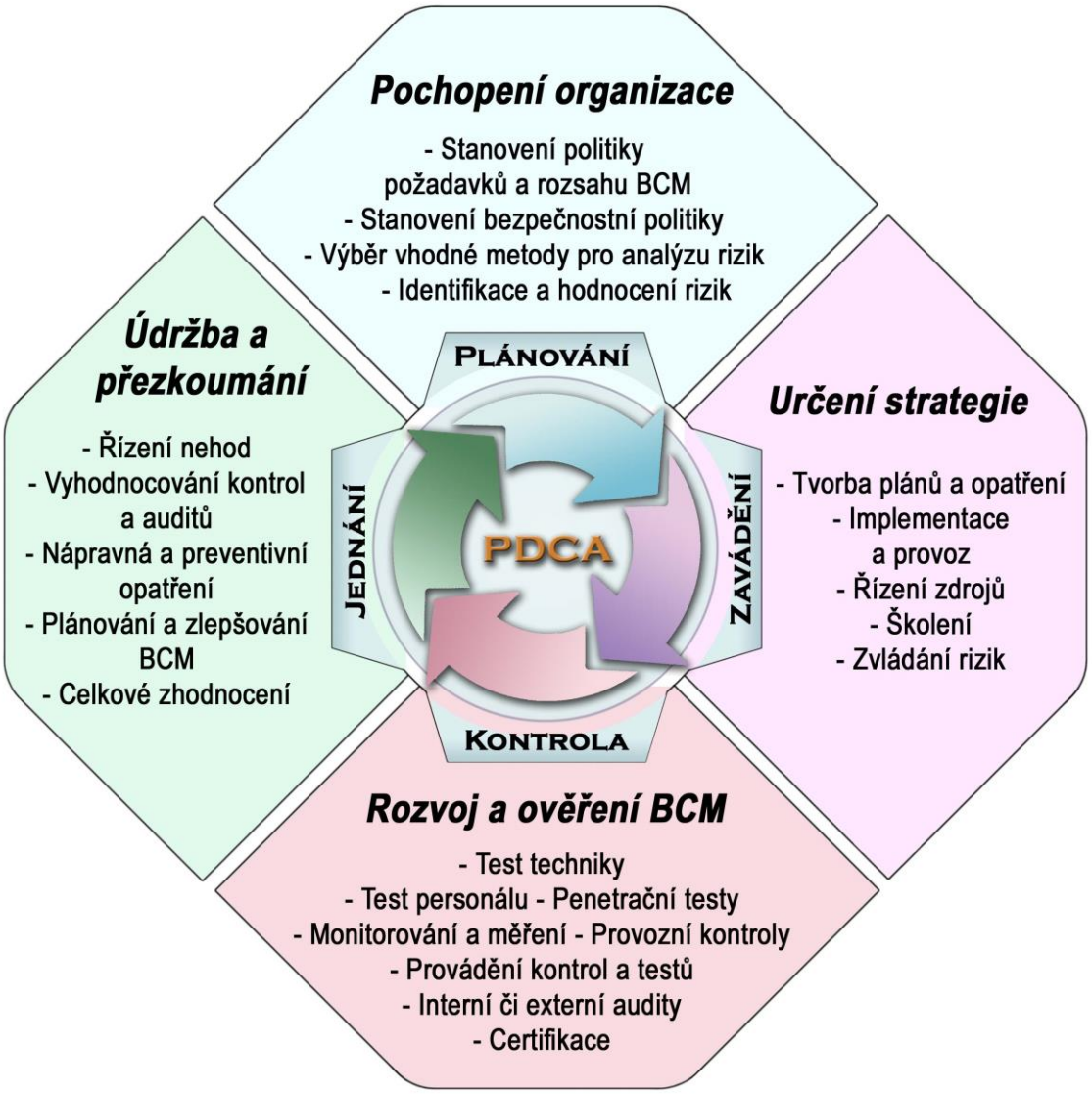
Demmingův cyklus je metoda postupného zlepšování kvality výrobků, procesů a služeb probíhajících formou opakovaného cyklu - Plánuj, Dělej, Kontroluj, Jednej (Plan - Do - Check - Act). Jde tedy o proces, který je ve své podstatě nekonečný. Základ tohoto procesu je obsahem normy ČSN ISO/IEC 27001. [8]



Obr. 3: Princip PDCA cyklu

2.1.2 Životní cyklus řízení kontinuity činností organizace

Zavedení BCM systému v organizaci je krok, který musí vzejít od vedení společnosti. Z důvodu toho, že se jedná o vytvoření firemní kultury BCM a její začlenění do veškerého systému řízení, je žádoucí, aby tento krok znamenal pro společnost úspěch. Toho lze dosáhnout pomocí životního cyklu řízení kontinuity činností organizace. Samotný cyklus řízení kontinuity činností je opakující se proces, který plynule navazuje na jednotlivé části, které jsou znázorněny na obrázku č. 4. [7]



Obr. 4: Životní cyklus řízení kontinuity činností [7]

2.1.2.1 Plánuj - Plan

Etapa plánování je prvotním krokem k zavedení kontinuity činnosti organizace. Hlavním úkolem tohoto procesu je pochopení činnosti organizace a identifikace cílů, zdrojů, závazků, které společnost má. Na základě podrobného seznámení s celkovou politikou společnosti se stanovují potupy, které vedou k řízení rizik a zvyšování bezpečnosti. Dále se přistupuje k provedení analýzy rizik a identifikaci hrozeb. Na základě těchto analýz je pak vytvořen plán obnovy, který obsahuje připravenost na tyto hrozby, reakce a kontinuitu k

dosažení stanovených cílů společnosti. V této etapě jde o stanovení problému, situace s jeho následným stanovením plánu, jak tento problém řešit.

2.1.2.2 Dělej - Do

Po etapě plánování, ve které byly provedeny veškeré procesy k identifikaci rizik, a hrozeb společnosti nastává etapa zavádění plánu do společnosti. Je na společnosti, jakou si zvolí strategii pro implementaci plánu do společnosti. V této části se zpracuje plán rizik, plán obnovy a zavádějí se preventivní opatření ke snížení vzniku nečekané události.

2.1.2.3 Kontroluj - Check

Po zavedení plánu do společnosti je nutná kontrola zavedeného plánu. V této etapě se sledují dosažené výsledky a porovnávají se s plánem. Jde především o kontrolu požadavku, který byl v první etapě plánu uveden jako problém a měl být řešen. Provádí se testování, aktualizace a v neposlední řadě audit.

2.1.2.4 Jednej - Act

Poslední etapou je ověření výsledku. V případě, že plnění stanoveného plánu není dle očekávání, je nutné dohledat příčinu, z jakého důvodu se plán neplní. To vyžaduje vytvoření nového plánu, který je zaměřen na odstranění příčiny neplnění požadavku dle plánu. Po odstranění tohoto problému je nutné udělat závěrečný krok, který představuje zavedení těchto změn do daného procesu. Mezi poslední krok patří kontrola, zda stanovené změny jsou uplatňovány dle plánu.

2.2 Požadavky na dokumentaci

Zavedení systému je velmi složitý proces, který je provázen několika fázemi. Aby bylo řízení kontinuity činností organizace zavedeno správně, je nutné pečlivé dodržování těchto jednotlivých fází. Každá fáze obsahuje několik dokumentů, které jsou pro správnou účinnost procesu kontinuity činnosti organizace závazné.

Z tohoto důvodu se budu v této části práce zabývat jednotlivými procesními postupy při tvorbě BCP, s cílem vymezení požadavků na dokumenty, které ke každé části fáze patří.

Přehled fází:

1. zavedení BCM,
2. analýza a strategie,
3. plánování,
4. implementace,
5. testování,
6. operativní řízení. [1]

2.2.1 Zavedení BCM

Pro zavedení BCM je rozhodující souhlas a přesvědčení vedení společnosti. Aby mohlo být zavedení procesu kontinuity činnosti úspěšné, je na samém začátku důležité zpracovat následující dokumenty, které obsahují několik důležitých bodů:

Dokument politiky BCM

- identifikace cílů organizace, způsob jakými je těchto cílů dosaženo,
- vytýčení směru, jakým společnost směřuje,
- identifikace zákonných povinností a prostředí, ve kterém organizace působí.

Dokument analýzy společnosti

- stanovení vzájemných závislostí svých činností a závislostí na externí organizace,
- identifikace činností, majetku a zdrojů, včetně těch, které pocházejí z vnějšku organizace a které podporují dodávání produktů,
- identifikace závazků vůči zainteresovaným stranám (vztahy k obchodním partnerům).

2.2.2 Analýza a strategie

Na základě předchozí analýzy společnosti, jejich jednotlivých procesů a vzájemného propojení těchto procesů nastupuje další fáze, která musí být provedena velice důkladně, protože se jedná o základ, ze kterého se vychází při tvorbě plánu kontinuity činností organizace. Výstupem jsou následující dokumenty:

Analýza rizik a hrozeb

- stanovení zranitelných míst, které jsou pro společnost nejvíce nebezpečné,
- identifikace procesů, při jejichž výpadku dochází k narušení chodu společnosti,
- třídění své činnosti na základě jejich důležitosti při obnovování,
- určení směru dopadu hrozeb, zda na lidské zdroje, technické prostředky, popř. okolí společnosti.

Analýza dopadů

- posouzení dopadu a následků během doby poruchy klíčových činností (BIA),
- identifikace a odhad vnímaných hrozeb, které mohou narušit klíčové produkty,
- stanovení pravděpodobnosti, s jakou společnosti vznik nečekané události - hrozby,
- stanovení maximální tolerované doby přerušení každé činnosti,
- stanovení nejdůležitějších oblastí společnosti pro zachování kontinuity společnosti,
- finanční dopady spojené s obnovou činnosti společnosti.

Strategie

- návrh opatření ke snížení pravděpodobnosti výskytu incidentů nebo redukci možných účinků,
- vymezení navrhovaných opatření pro následující oblasti:
  - lidské zdroje (školení a výcvik personálu),
  - prostory (alternativní prostory uvnitř organizace, popř. externí),
  - technologie (vazby technologií na kritické oblasti),
  - informace (zajištění informací životně důležitých pro výkon organizace),
  - dodávky (seznam kritických dodávek, odklon dodávek do jiných míst),
  - zainteresované strany (ochrana zájmů klíčových zainteresovaných stran).

2.2.3 Plánování

Tato fáze následuje po důkladné analýze veškerých hrozeb a jejich dopadů a vychází z navržených strategií. V této fázi se tvoří konkrétní plány na nečekané události, které by mohly ohrozit chod společnosti. Úkolem tohoto plánovaní je určení postupů, prostřednictvím kterých dojde k zotavení společnosti a jakým způsobem budou obnoveny narušené klíčové procesy. BCP musí zajistit, že v případě vzniku mimořádné události jsou činnosti organizační jednotky obnoveny v čase RTO, stanoveném v rámci provedené analýzy dopadů. Celá fáze plánování je obsahem následujících dokumentů:

Plán zvládání (managementu) incidentů

- obsahuje seznam úkolů a checklist činností k řízení okamžitých následků přerušení činnosti organizace,
- popis za jakých okolností a jakým způsobem bude organizace komunikovat s personálem, jejich příbuznými, přáteli a kontakty pro případ stavu nouze,
- identifikace personálu s příslušnými pravomocemi pro spojení s pohotovostními službami,
- stanovení komunikační strategie při incidentu (způsob spojení s médii, směrnice nebo vzor pro návrh stanovisek pro média).

Plán kontinuity činností

- způsob vyvolání BCP,
- stanovení osoby (osob) odpovědných za rozhodnutí o vyvolání plánu kontinuity činností organizace,
- postupy, které by měly tyto osoby podstoupit při tomto rozhodnutí,
- určení osoby, která musí být informována v případě učinění rozhodnutí vyvolat BCP,
- určení ostatních rolí (kdo jde kam a kdy),
- které služby jsou kde a kdy dostupné, včetně toho jak organizace mobilizuje externí zdroje.

Plán obnovy činností

- popisy konkrétních činností jednotlivých osob, oddělení (týkají se prostor, technologií, informací, dodávek a zainteresovaných stran, které byly identifikovány ve strategické fázi),
- stanovení zdrojů nutných pro obnovu činností organizace v různých časových bodech:
  - finanční detaily (např. výplaty),
  - záznamy zákaznických účtů,
  - detaily o dodavatelích a zainteresovaných stranách,
  - právní dokumenty (smlouvy, pojistné smlouvy, právní listiny),
- identifikace a jmenování osob určených pro řízení fázi kontinuity činností a fázi obnovy činností organizace po přerušení (v mnoha případech to mohou být osoby, které jsou uvedeny v plánu managementu incidentu),
- stanovení časového harmonogramu pro aktualizace plánů.

Všechny plány by měly být stručné a přístupné pro ty, kdo mají odpovědnosti stanovené v plánech. Musí mít podporu vrcholového vedení a musí být podpořeny příslušným rozpočtem pro vývoj, udržování a školení nebo výcvik.

Vytvořené plány by se měly testovat z důvodu jejich funkčností.

2.2.4 Implementace

Po vytvoření plánu je následujícím krokem implementace navržených opatření a finální zavedení BCM do kultury obchodní společnosti. Při realizaci navrženého plánu, může dojít ke zjištění posledních nedostatků, které musí být odstraněny. Realizace zavedení BCM je pro společnost velkou změnou, proto musí být s touto skutečností seznámeni všichni zaměstnanci tak, aby mohl být BCM ve společnosti co nejefektivnější. Je nutné ověření, zdali všichni pověření zaměstnanci znají dostatečně své role a jsou schopni plnit povinnosti vyplývajících z jejich funkcí. Jedině takto může být BCM úspěšně realizován do každodenních činností společnosti. Dokumenty této fáze jsou:

Rozpočet

- návrh rozpočtu na realizaci implementace navržených opatření do struktury společnosti (náklady na osoby, techniku a vybavení).

Lidské zdroje

- obsahuje celkový seznam osob podílejících se na implementaci BCM s určenými rolemi.

Seznam oddělení zapojených do BCM

- obsahuje úplný seznam oddělení zapojených do implementace BCM, popř. všech poboček společnosti.

Časový harmonogram

- obsahuje úplný časový harmonogram zavádění BCM.

2.2.5 Testování

Proces testování zahrnuje pravidelné testy plánů, které se konají v pravidelných intervalech stanovených vedoucím BCM. Účelem testů je ověření efektivity zavedeného BCM a ověření, zdali klíčové procesy budou obnoveny, tak jak je uvedeno v plánech. Je vytvořeno několik testů za účelem zjištění funkčnosti BCM jako celku. Hlavním úkolem testování je identifikace slabých míst, které je potřeba odstranit a zlepšit. Jedině tak můžeme zajistit dobrou kontinuitu společnosti.

Obsahem testů by mělo být:

- ověření navržených strategií,
- ověření znalostí všech členů týmu, veškerých kontaktních údajů,
- ověření navrhnutých postupů, odhalení nedostatků plánu, aktuálnost plánů.

Základní typy testování představují zároveň dokumenty této fáze. Jsou to:

Test úplnosti plánů

- jedná se o nejzákladnější test, představující kontrolu úplnosti plánů. Zahrnuje teoretické přezkoumání kompletnosti informací obsažených v plánech, provádí se ověření správnosti, úplnosti a aktuálnosti uvedených údajů, jako jsou např.

kontaktní informace na členy týmu, umístění záložních prostor a seznam technických prostředků.

Teoretický průchod plánem

- kontrola úplnosti plánů rozšířená o teoretické prověření konkrétních postupů obnovy, ověření znalostí rolí jednotlivých členů týmu a jejich vzájemné komunikace (vysvětlují co by v dané situaci dělali, jak by postupovali, koho by kontaktovali). Cílem testů je odhalit nedostatky v navržených postupech obnovy jednotlivých procesů. Může to být také dobrý způsob jak zaškolit nové členy týmu, ale také periodické školení stávajících členů týmu.

Simulační testy

- praktické nacvičování a prověření jednotlivých postupů a týmové interakce podle předem připravených scénářů. Součástí testů je prověření funkčnosti komunikačních linek, otestování komunikace s dodavateli, zákazníky, médii a záchrannými složkami. Příkladem simulačních testů může být např. nácvik požáru budovy.

Test úplného přerušení

- jedná se o komplexní testování. Toto testování se považuje za maximum v rámci prověření funkčnosti daného plánu. Jeho součástí je přerušení klíčového procesu za plného provozu, bezprostřední reakce na situaci a obnovení činnosti na základě aktuálních zdrojů. Tímto se prověří veškeré části plánů a reakcí všech zúčastněných osob. I když na základě tohoto testu dojde nejvíce k prověření všech plánů, je na zvážení každé společnosti, zda tento test podstoupit a to z důvodu rizika vzniku nečekané události, která by mohla při testování nastat.

Paralelní test

- z hlediska testování se taktéž jedná o komplexní test. Tento test je pro společnosti sice technicky náročný, ale z hlediska rizik je přijatelnější než test úplného přerušení. Testování je prováděno za běžného provozu, s tím že dojde k přerušení klíčového procesu, ale ne ve skutečně požadované lokalitě. Obnova tohoto procesu musí být provedena v požadovaném čase a na požadované úrovni. Hlavním cílem testování je ověření chodu společnosti a jejich reakci při vzniku nečekané události.

2.2.6 Operativní řízení

Jedná se o poslední fází při zavádění procesu kontinuity činnosti organizace. Představuje neustále opakující se proces činností zahrnující informovanost o procesu BCM ve společnosti, soubor testování plánů a osob, audit systému, aktualizaci plánů a školení všech zúčastněných osob. Tyto stále opakující se činnosti mají za úkol udržování BCM v celé společnosti. V průběhu této fáze vznikají dokumenty, jejichž obsahem bývá:

Informovanost o BCM ve společnosti

Tento proces je ve společnosti základem pro úspěšné vedení procesu kontinuity činnosti organizace. Jelikož na činnosti BCM se podílí velký počet zaměstnanců, je prioritou vedení společnosti informovat o tomto zavedeném procesu všechny zúčastněné osoby. Jedině tak může být reakce na nečekané události co nejrychlejší. Samozřejmostí této části je přehledné vedení veškeré dokumentace, se kterou musí být všichni zaměstnanci seznámeni.

Testování plánů a osob

Tato část se zabývá především testy v předem stanovených intervalech a to na nejrizikovější kritické procesy, které mohou být ohroženy a jsou pro společnost klíčové. Testování má za úkol prověřit stanovený plán a jeho funkčnost, případně odhalit nedostatky BCM systému.

Audit společnosti

Pro ověření správně vypracovaného BCM je nejúčinnější metodou provedení auditu. Audit je prováděn externí společností, která provede kontrolu nastaveného BCP, jeho vhodnost a účelnost pro danou společnost, začlenění činnosti kontinuity do všech klíčových procesů společnosti. Hlavním úkolem auditu je zkoumání úplnosti a aktuálnosti dokumentace spojené s procesem BCM, vhodnost navržených opatření k minimalizaci ztrát, pravidelnost testování. Výsledkem je nezávislé vymezení nedostatků a příčin, kterým se musí společnost v rámci BCM věnovat a odstranit.

Aktualizace plánů

Dalším úkolem operativního řízení je sledování celého chodu společnosti a zaznamenávání případné aktualizace chodu společnosti do stanovených plánů. Jelikož se chod společnosti vyvíjí každým dnem je důležité tyto změny zaznamenávat, jelikož může dojít ke změně strategie a cíle společnosti a může dojít ke změně klíčových procesů. Změny se nemusí

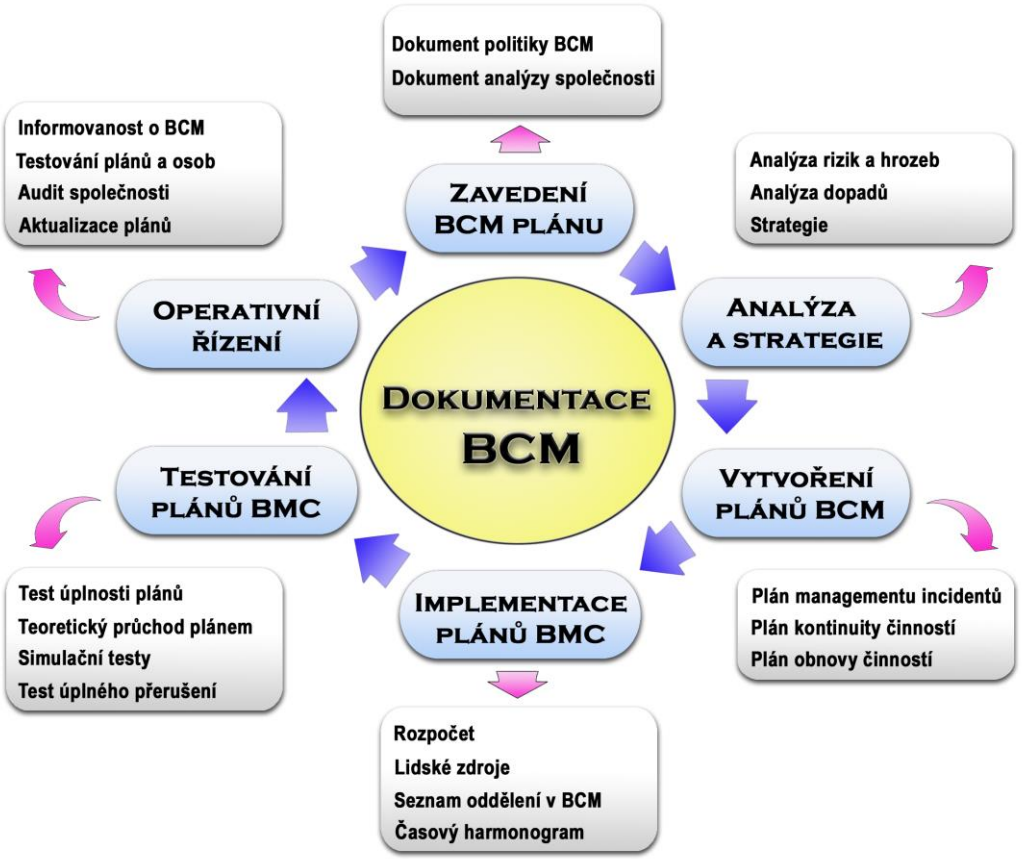
týkat pouze stanovení cíle společnosti, ale může jít o změny organizační, personální, technologickými a v neposlední řadě legislativě v oblasti BCM.

Školení

Informovanost všech zúčastněných osob je pro proces zachování kontinuity činnosti společnosti zásadní. Z tohoto důvodu je vhodné při změně v navržených plánech provést patřičné proškolení osob, tak aby byla zachována informovanost.

Dílčí závěr

Cílem této kapitoly bylo provést analýzu požadavků na dokumentaci, která je nutná pro zavedení BCM do kultury společnosti. Tyto dokumenty přesně kopírují jednotlivé fáze, ze kterých se skládá celý proces BCM. Tyto fáze jsou spojeny s modelem PDCA, což představuje nekonečně opakující se proces pro zachování kontinuity činností společnosti. Je to proces řízení, při kterém dochází k neustálému zlepšování zavedeného systému. Následující obrázek znázorňuje souhrnný přehled dokumentace u jednotlivých fází při tvorbě BCP.



Obr. 5: Přehled dokumentů požadovaných BCM

II. PRAKTICKÁ ČÁST

3 ANALÝZA SPOLEČNOSTÍ PRO APLIKACI BCM V PRŮMYSLU KOMERČNÍ BEZPEČNOSTI

3.1 Obchodní společnosti v průmyslu komerční bezpečnosti

Třetí část práce je zaměřena na návrh společností a oblastí pro aplikaci BCM v průmyslu komerční bezpečnosti. Prvním krokem k vytvoření návrhu, je nutná analýza obchodních společností vyskytujících se v průmyslu komerční bezpečnosti.

Obchodní společnosti v průmyslu komerční bezpečnosti představují soukromé subjekty, podnikající na základě živnostenského oprávnění pro konkrétní druh činnosti. Pro tuto oblast podnikání je podle zákona č. 455/1991 Sb., zapotřebí koncesovaná živnost - dle § 26, příloha č. 3. Předmětem podnikání na základě koncese v průmyslu komerční bezpečnosti je:

- ostraha majetku a osob,
- služby soukromých detektivů,
- poskytování technických služeb k ochraně majetku a osob.

Hlavním úkolem u veškerých obchodních činností je vykonávání soustavné činnosti, vlastním jménem, na vlastní odpovědnost, za účelem dosažení zisku. U každého předmětu podnikání jsou stanoveny podmínky, za kterých je vydáno živnostenské oprávnění a u každého předmětu podnikání je dále stanoveno, že společnost zajišťuje výkon činnosti pouze fyzickými osobami, které splňují požadavky odborné způsobilosti, které jsou uvedeny v příloze č. 5 živnostenského zákona. [9]

Všeobecně lze říci, že úkolem společností v průmyslu komerční bezpečnosti je ochrana a ostraha osob a majetku. O bezpečnost osob uvnitř státu se stará zejména v ČR státní orgán - Policie ČR. Z důvodu narůstajících požadavků na vyšší bezpečnost fyzických i právnických osob a ochranu jejich majetku před násilím, nebezpečím či vandalismem vzrůstají požadavky po společnostech soukromých bezpečnostních služeb.

Z důvodu toho, že bezpečnost je pro každého z nás důležitým faktorem, je žádoucí aby společnosti podnikající v oblasti průmyslu komerční bezpečnosti byly ve své činnosti co nejvíce připraveny nabídnout co nejkvalitnější služby pro své zákazníky. V dnešní době, kdy narůstá počet násilí ve společnosti, se stávají obchodní společnosti v průmyslu

komerční bezpečnosti žádanější a tím pádem je téma kontinuity činnosti organizace v průmyslu komerční bezpečnosti aktuální.

V oblasti průmyslu komerční bezpečnosti se můžeme dále setkat se subjekty, které nepodléhají koncesované živnosti. Jedná se o společnosti, jejichž předměty působení jsou zejména:

- výroba a prodej zabezpečovací techniky,
- vzdělávání v oblasti bezpečnostního inženýrství (bezpečnostní školství),
- bezpečnostní projekty,
- bezpečnostní poradenství, analýzy a audity,
- zkušebnictví a normo-tvorba. [10]

3.1.1 Ostraha majetku a osob

Společnosti, které mají za hlavní činnost podnikání a poskytování služeb v oblasti ochrany osob a ostrahy majetku, patří v rámci trhu práce mezi nejžádanější. Ostraha osob souvisí především s ochranou života a zdraví a proto má vždy přednost před ostrahou majetku, která souvisí především s ostrahou movitých a nemovitých věcí. V tomto předmětu podnikání poskytují společnosti i ostrahu při přepravě peněž a cenností, zajišťují dohled a pořádek v místech konání sportovních akcí, veřejných shromáždění, společenských akcí apod.

Ochranu osob a majetku lze poskytovat těmito formami:

1. fyzická ochrana,
2. technická ochrana - mechanická, elektronická, smíšená a speciální,
3. kombinovaná ochrana. [11]

Společnosti, které vykonávají ochranu osob, a ostrahu majetku nazýváme hlídací služby. Jelikož jsou tyto společnosti v dnešní době velmi žádané na trhu, je důležité, aby společnost měla dobré jméno a mohla nabídnout velmi kvalitní služby.

Hlídací služby poskytují:

- ochranu osob,
- ostrahu majetku,
- služby přepravy peněz a cenností a zpracování peněžní hotovosti,
- zajišťování pořádku v místě soustředění osob, zejména při pořádání veřejného shromáždění, slavnosti nebo společenského, kulturního, sportovního anebo jiného podniku,
- provozování zabezpečovacího anebo poplachového systému, provozování jejich částí nebo vyhodnocování narušení chráněného objektu anebo místa. [12]

Činnosti obchodních společností poskytujících hlídací služby:

- objektová bezpečnost a režimová opatření,
- fyzická ochrana a ostraha (pochůzkáři, vrátní, recepční, klíčová služba, psovodi, patrol systém apod.),
- osobní ochrana (bodyguarding),
- zásahové jednotky PPC,
- statická ochrana objektů,
- pohyblivá ochrana objektů,
- monitorovací ochrana objektů,
- bezpečnostní doprovody osob,
- bezpečnostní doprovody vozidel. [10]

3.1.2 Služby soukromých detektivů

Mezi další obchodní společnosti vykonávající obchodní činnost v průmyslu komerční bezpečnosti řadíme služby soukromých detektivů. Tato služba je poskytována za úplatu, na základě smluvního vztahu mezi zákazníkem a společností.

Tyto společnosti mají za hlavní předmět podnikání získávání, pátrání, hledání a seskupování informací o konkrétních fyzických nebo právnických osobách dle požadavku

jiné fyzické či právnické osoby. Nejedná se pouze o získávání informací o osobách, ale jde i o hledání majetku, zejména v návaznosti na majetkové poměry v souvislosti s vymáháním pohledávek.

Výsledky činnosti soukromých detektivů slouží jako důkazní materiály při řízení před soudem.

Služby soukromých detektivů poskytují:

- detektivní služby,
- ochranné detektivní služby,
- klasické detektivní služby,
- detektivní služby ochrany ekonomických zájmů,
- podnikatelské zpravodajství. [10]

Činnosti obchodních společností poskytujících služby soukromých detektivů:

- hledání majetku,
- hledání osob majetku,
- pozorování činnosti osoby,
- zjišťování skutečností, které mohou sloužit jako důkaz v řízení před soudem nebo správním orgánem,
- získávání informací o osobním stavu fyzické osoby, o jednání osoby nebo o jejích majetkových poměrech,
- získávání informací v souvislosti s vymáháním pohledávek,
- získávání informací o protiprávním jednání osob ohrožujících obchodní tajemství. [13]

3.1.3 Poskytování technických služeb k ochraně majetku a osob

Mezi poslední předmět podnikání v průmyslu komerční bezpečnosti řadíme poskytování technických služeb k ochraně majetku a osob. Tato oblast, jak je možné již z názvu odvodit, představuje veškeré technické služby spojené s ochranou majetku a osob.

Technické služby k ochraně majetku a osob poskytují:

- projektování,
- montáž,
- údržbu,
- opravy.

Činností obchodních společností poskytujících technické služby ochrany osob a majetku:

- monitoring statických objektů (technická část),
- monitoring pohyblivých objektů (technická část),
- obsluha PPC (telefonních, radiových a GSM),
- dispečerská pracoviště PPC (technická část),
- dodávka a montáž EZS,
- dodávka a montáž CCTV,
- dodávka a montáž EPS,
- dodávka a montáž ACS,
- dodávka a montáž systému zajišťujících ochranu zboží,
- dodávka a montáž integrovaných systémů,
- datová bezpečnost,
- kontrolní a dozorové systémy,
- dodávka a montáž ostatních systémů mechanických zábranných systémů a prostředků (mříže, rolety, fólie, bezpečnostní skla),
- speciální technické systémy a prostředky,
- mechanické a elektronické zabezpečení vozidel,
- přenos bezdrátových signálů a dat,
- venkovní perimetrie. [10]

3.1.4 Výroba a prodej zabezpečovací techniky

Výrobu a prodej zabezpečovací techniky řadíme mezi nejvýznamnější způsob podnikání v průmyslu komerční bezpečnosti, neboť aby bylo možné provádět ochranu majetku, musí být vyrobeny prostředky určené právě k tomuto účelu. Jedná se převážně o firmy, které se zabývají výrobou a prodejem prvků mechanických zábranných systémů jako jsou různé typy bezpečnostních mříží, dveří, zámků, fólií, garážových a průmyslových vrat, bran, předokenních roleta apod. Dále je to výroba trezorů, sejfů, trezorů na zbraně, přístupových a parkovacích systémů (turnikety, závory) a výroba protipožárního zabezpečení. Zabezpečovací systémy by měly představovat spolehlivé produkty, proto musí být výroba probíhat na základě stanovaných norem např. ČSN EN 50131, případně schválení Českou asociací pojišťoven. V případě distribuce těchto výrobků by měla firma dbát na proškolení zákazníka dodavatelem ohledně vlastností, způsobu použití a instalaci daného výrobku nebo produktu. Aby byla zachována funkčnost jednotlivých systémů ochrany, mělo by být předností společnosti poskytovat pravidelný servis.

3.1.5 Vzdělávání v oblasti bezpečnostního inženýrství

Každý z nás by se měl neustále vzdělávat. Jelikož vzdělání je pro člověka nezbytnou součástí každodenního života, není tomu jinak ani v oblasti bezpečnostního inženýrství. Pro tuto činnost je obzvlášť nezbytné odborné vzdělání, neboť poptávka po odbornících z bezpečnostní oblasti v současnosti stále narůstá. Technika a způsoby ochrany se neustále vyvíjí, proto v dnešní době narůstají požadavky na vzdělané a kvalifikované lidi v oblasti bezpečnostního inženýrství. Takto vzdělaní lidé se stávají bezpečnostními manažery, specialisty, auditory, atd.

V současné době je možné vzdělávat se v oblasti bezpečnostního inženýrství např. na UTB ve Zlíně - fakultě aplikované informatiky v oboru Bezpečnostní technologie, systémy a management a dále se jedná o fakultu bezpečnostního inženýrství na VŠB - technické univerzitě, která nabízí vzdělání v oborech požární ochrany, ochrany obyvatelstva, bezpečnostního managementu a bezpečnostních služeb.

3.1.6 Bezpečnostní projekty

K další činnosti v oblasti průmyslu komerční bezpečnosti řadíme samotné bezpečnostní projekty. Společnosti poskytující tyto služby se zabývají zhotovením bezpečnostních

projektů a analýz průmyslových či komerčních objektů. Provádí bezpečnostní prohlídky budov a areálů, vyhodnocují rizika a připravují nabídku k jejich řešení či eliminaci. Společnosti by měly k bezpečnostním projektům přistupovat na základě odborných znalostí, efektivních prostředků, zkušeností a znalostí místních poměrů.

Bezpečnostní projekt je zaměřen na realizaci bezpečnostních opatření v oblasti administrativy, personální, informačních systémů, fyzické bezpečnosti. Veškeré činnosti vychází ze stanoveného cíle společnosti a musí být dodrženy veškeré platné normy, vyhlášky a další legislativní požadavky.

3.1.7 Bezpečnostní poradenství, analýzy a audity

Každá společnost, která nemá odborníky vzdělané v oblasti bezpečnosti, má možnost získat znalosti prostřednictvím bezpečnostního poradenství. Tuto činnost vykonávají společnosti, které mají speciálně vyškolené pracovníky s patřičným vzděláním, kteří jsou schopni na základě svých znalostí poskytnout poradenství v této oblasti.

Poradenství vychází z provedené bezpečnostní analýzy, na základě které jsou navrženy konkrétní bezpečnostní opatření. Zpracovává se dokument, který obsahuje vyhodnocení vnějších a vnitřních rizik, a to na základě správného porozumění cílů společnosti.

Každá společnost, která si chce ověřit aktuální stav bezpečnosti vlastní společnosti má možnost získání této informace prostřednictvím bezpečnostního auditu. Úkolem auditu je redukování bezpečnostních rizik a zjištění zranitelných míst nejen uvnitř společnosti.

3.1.8 Zkušebnictví a normotvorba

Společnosti, které se pohybují v této oblasti, mají poněkud odlišné druhy činností, ale do průmyslu komerční bezpečnosti rozhodně patří. Nezabývají se přímo poskytováním fyzické nebo technické bezpečnosti, ale podílí se spíše na vývoji techniky, certifikacích, sdružování společností a tvorbě legislativy. Poskytují rovněž konzultační činnost v oblasti bezpečnosti strojů a bezpečnosti elektrických zařízení, posuzují uvedená zařízení, spolupracují při kompletaci potřebné dokumentace a vydání prohlášení o shodě.

Příkladem může být profesní sdružení GRÉMIUM ALARM. Tato asociace se během několika let stala významným partnerem Hospodářské komory ČR - autorizovaným živnostenským společenstvem pro technické služby k ochraně majetku a osob a stala se

partnerem Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví. Asociace tak má rozhodující vliv na zavádění evropských norem a technických specifikací do soustavy českých technických norem a je spoluautorem technických národních specifikací.

3.2 Návrh společností v průmyslu komerční bezpečnosti pro aplikaci BCM

Na základě analýzy činností obchodních společností poskytujících služby v průmyslu komerční bezpečnosti je zřejmé, že u každého typu společnosti, snad s výjimkou školství, by nenadálé události mohly ohrozit jejich chod, prosperitu, popř. dobré jméno na trhu. Vzhledem k tomu, že snahou je vždy provozovat důvěryhodnou firmu, která se snaží uspokojit zákazníka a vytvářet zisk, hrozba poklesu výroby, nedodání konkrétní služby, apod. by mělo tyto firmy přimět k zavádění plánů na řešení mimořádných situací.

Zavedení BCM však bude více či méně užitečné vzhledem k tomu, v jaké oblasti podnikání se daná firma pohybuje.

Pokud se jedná o společnosti provozující činnost na základě koncesované živnosti je vhodnost zavedení BCM u těchto koncesí:

- poskytování technických služeb k ochraně majetku a osob,
- ochrana osob a ostraha majetku (hlídací služby).

Pokud se jedná o další typy společností, nepodnikající na základě koncesované živnosti, má rozhodně větší význam a přínos zavedení BCM u společností zabývajících se výrobou a dodávkou zabezpečovací techniky než u společnosti poskytující bezpečnostní analýzu nebo audit.

Z hlediska možných dopadů na jednotlivé typy společnosti navrhuji zavedení BCM u těchto oblastí podnikání:

- výroba a dodávka zabezpečovací techniky,
- bezpečnostní projekty.

3.2.1 Poskytování technických služeb k ochraně majetku a osob

Co se týká koncesované živnosti poskytování technických služeb, řadíme tuto činnost mezi rizikovější, protože na bezproblémovém chodu společnosti závisí spousta dalších osob a

podniků, kterým je služba technické ochrany poskytována. Příkladem může být selhání zařízení nebo obsluhy PPC, které v případě absence záložní techniky může znamenat velké problémy. Proto bych doporučovala zavedení BCM v této oblasti jako za nejdůležitější.

3.2.2 Ochrana osob a ostraha majetku (hlídací služby)

Pokud se jedná o společnosti provozující hlídací služby, je vhodné zavedení BCM v této bezpečnostní oblasti proto, že tato činnost spočívá v ochraně osob a ostraze majetku, kde je nejvýznamnější ochrana zdraví a života. Z tohoto důvodu by měly být společnosti opět připraveny na nečekané události spojené s technikou, personálem a jinými hrozbami, které by jejich činnost mohly narušit.

Poslední typ koncesované živnosti je ve svém oboru taktéž důležitý, ale služby soukromých detektivů v případě mimořádné události nepředstavují tak velké riziko ztrát jako u poskytování technický prostředků a ochrany osob a ostrahy majetku.

3.2.3 Výroba a dodávka zabezpečovací techniky

Vzhledem k tomu, že výroba zabezpečovací techniky je závislá na použitých technologiích, materiálech, zařízeních a energii, představuje výpadek ve výrobě pro společnost velká rizika ztrát. Zavedení BCM proto u těchto typů společností považuji za téměř nutné, protože nepřipravenost na nenadálé události může způsobit velké časové prodlení v návratu k normálnímu stavu.

3.2.4 Bezpečnostní projekty

Společnosti zabývající se zpracováním bezpečnostních projektů nejsou tak závislé na technologických zdrojích jako výrobní firmy, zato mohou disponovat velkým množstvím dat a informací o svých zákaznících, společnostech, objektech apod. Je u nich tedy především nutné zavedení informační bezpečnosti. Ztráta důvěrných informací může v tomto případě totiž znamenat ohrožení jednak společnosti, která bezpečnostní analýzu a projekt zpracovává a jednak samotného zákazníka.

3.3 Oblasti pro zavedení BCM do obchodních společností v průmyslu komerční bezpečnosti

Z provedené analýzy činností obchodních společností poskytujících služby v průmyslu komerční bezpečnosti vyplývá jednoznačně několik oblastí, ve kterých je zavedení BCM velice vhodné a účelné. A to zejména z toho důvodu, že připravenost na nečekané události v těchto oblastech může významným způsobem ochránit společnost před ztrátou dobrého jména a postavení na trhu. Třebaže tyto společnosti provozují odlišné služby, ohrožené oblasti se navzájem prolínají ve všech typech podnikání a z toho důvodu je možné BCM aplikovat s menšími rozdíly u všech společností v průmyslu komerční bezpečnosti.

I přesto, že se BCM zavádí do společnosti jako celku, snažila jsem se v práci uvést oblasti, které považuji za klíčové a které při vzniku mimořádné události musí být pro zachování plynulého chodu společnosti obnoveny co nejdříve. Těmto oblastem by se mělo při tvorbě BCP věnovat důkladně. Jedná se o tyto oblasti:

- oblast personalistiky,
- oblast informačních technologií,
- oblast technického zabezpečení,
- oblast objektové bezpečnosti.

V následujících kapitolách uvedu problematiku těchto oblastí vzhledem ke kontinuitě činností společností v průmyslu komerční bezpečnosti.

3.3.1 Oblast personalistiky

Tato oblast je pro společnost velmi důležitá, neboť přístup zaměstnanců a osob, které s ní přichází do styku, může chod podniku ovlivnit mnoha způsoby. Ať už se jedná o hlídací služby, které jsou obzvlášť závislé na lidském potencionálu, tak i ostatní společnosti, které se zabývají poskytováním technických služeb. Možné ohrožení kontinuity činností může způsobit jednak absence osob na klíčových pozicích a jednak negativní morálka zaměstnanců. Tou může být např. neplnění svých povinností, neznalost dané problematiky, zneužití informací atd. Důraz by měl být kladen také na osoby, které přichází do prostor společnosti za jakýmkoliv účelem. Zavedení BCM by mělo na tyto problémy reagovat stanovením zastupitelnosti na různých pozicích, pravidelným školením, prověřováním

osobních i kvalifikačních předpokladů, motivačními programy a dodržováním přístupového režimu.

3.3.2 Oblast informačních technologií

Pro tuto oblast existují zvláštní pravidla a postupy, neboť ochrana informací v současné době představuje pro společnosti úkol velmi vážného významu. Ztráta, poškození nebo krádež cenných dat může v mnoha případech znamenat až existenční problémy. Společnosti průmyslu komerční bezpečnosti pracují totiž s citlivými údaji svých zákazníků, údaji o objektech, ve kterých zabezpečují své služby, vlastní rozsáhlé databáze zákazníků a dodavatelů, množství realizačních projektů, údaje o trasách, po kterých se pohybují v případě poskytování ochranných doprovodů, technické údaje o zařízení instalovaných v zabezpečovaných objektech, informace o zaměstnancích a obchodních partnerech a spoustu dalších informací, které mohou být pro konkurenci velmi zajímavé. Zavedením BMC je třeba určit kritická místa, míru rizika a zabezpečit je tak, aby nebylo možné tyto informace zneužít jak uvnitř společnosti, ale zejména pak zvenčí po datových linkách, neboť veřejná internetová síť představuje v současnosti nejfrekventovanější a nejdůležitější komunikační prostředek a tím velmi ohrožený přístup.

3.3.3 Oblast technického zabezpečení

Tato oblast je kritická zejména ve společnostech poskytujících technické prostředky ochrany, ale stejně tak jiné služby. Ke svým činnostem firmy používají množství komunikačních zařízení, dopravních prostředků, montážních nářadí a zařízení, na jejichž funkčnosti jsou firmy závislé vzhledem ke kvalitním, včasným a spolehlivým dodávkám svých služeb. Například na bezporuchovém chodu PPC závisí zabezpečení ochrany mnoha objektů, ve kterých společnost provozuje hlídací služby. Stejně tak spolehlivost kamerového systému v rozsáhlém objektu může znamenat zvýšení anebo úpadek prestiže dané firmy. V případě zásahových jednotek, které se potřebují včas dopravit k ohroženému objektu nebo v případě dodávek zboží nebo systémů k zákazníkům, je společnost závislá na spolehlivosti vozového parku. I třeba banální nedostatek pohonných hmot může znamenat velký problém Do technického zabezpečení je nutné zahrnout rovněž zajištění zdroje elektrické energie, bez které je provoz společnosti téměř nemožný. Z těchto důvodů

je v případě zavedení BCM ve firmě třeba pamatovat při zpracování plánu k zachování kontinuity činnosti, i na tuto oblast.

3.3.4 Oblast objektové bezpečnosti

Poslední oblast je neméně důležitá, protože představuje pro společnost hlavní jádro jejího působení. Objekty, ve kterých se společnost nachází, popř. je používá k jiným účelům, spojenými se svými aktivitami, představují velký zdroj možných problémů. Může to být např. poškození objektu a zařízení v případě vzniku požáru anebo důsledkem povodně zatopení nízkopodlažních prostor. Nebezpečím ale nemusí být pouze živelní události. Poškození budov, skladů, kanceláří a jiných objektů může být způsobeno vandaly, pokusy o vloupání nebo poruchami technologických zařízení, např. prasklé vodovodní potrubí či topení. I na tyto havárie je nutné v plánu BCM klást důraz, aby bylo možné krizovým událostem včas předcházet. V případě jejich vzniku pak musí být připravena řešení k zajištění včasné nápravy, popř. postupy na přestěhování konkrétního pracoviště do jiných objektů. Jen tak lze zachovat kontinuitu činností společnosti.

Dílčí závěr

Tato kapitola byla věnována návrhu společností a oblastí k zavedení BCM pro zachování kontinuity činností u společností podnikajících v průmyslu komerční bezpečnosti. Protože se v této problematice pohybuje mnoho subjektů s různým zaměřením, byla k tomuto účelu provedena analýza společností a jejich činností, které se tímto druhem podnikání zabývají. Mezi předmět podnikání v průmyslu komerční bezpečnosti řadíme:

- ostraha majetku a osob,
- služby soukromých detektivů,
- poskytování technických služeb k ochraně majetku a osob,
- výroba a dodávka zabezpečovací techniky,
- bezpečnostní projekty,
- bezpečnostní poradenství, analýzy a audity,
- zkušebnictví a normotvorba.

Třebaže se jedná o různé typy podnikání s odlišným zaměřením, na základě provedené analýzy činností považuji za účelnější zavedení u společností zabývající se činnostmi:

- poskytování technických služeb k ochraně majetku a osob,
- ochrana osob a ostraha majetku (hlídací služby),
- výroba a dodávka zabezpečovací techniky,
- bezpečnostní projekty.

V různých společnostech může být kladen důraz na jinou oblast, ale dle mého názoru je vhodné mít plány připravenosti ve všech, protože oblasti, které mohou být zdrojem narušení kontinuity činností, se nachází ve všech typech společností. V tabulce č. 1 představuji společnosti, oblasti a přehled kritických míst, ve kterých navrhuji zavedení BCM.

Tab. 1: Návrh společností a oblastí k zavedení BCM

Obchodní společnosti v PKB	Oblast	Kritické místo
Ostraha majetku a osob	Personalistika	Kvalita zaměstnanců
		Absence
		Zneužití informací
		Pohyb osob
Výroba a dodávka zabezpečovací techniky	Informační technologie	Databáze zákazníků
		Projekty
		Finance
		Know- How
		Interní síť
Poskytování technických služeb k ochraně majetku a osob	Technické zabezpečení	Elektrická energie
		Komunikace
		Autopark
		Zařízení PPC, CCTV, poplachové systémy
Bezpečnostní Projekty	Objektová bezpečnost	Požár
		Vloupání
		Zaplavení
		Přístup osob

4 PLÁN KONINUTITY ČINNOSTÍ PRO OBCHODNÍ SPOLEČNOST V PRŮMYSLU KOMERČNÍ BEZPEČNOSTI

Tato kapitola se bude zabývat aplikací BCM na vybranou obchodní společnost, podnikající v průmyslu komerční bezpečnosti. Na základě získaných teoretických znalostí dané problematiky provedu analýzu její činnosti spolu s vlivy, které mohou její postavení na trhu různým způsobem ovlivnit a způsobit jí v mnoha případech existenční problémy. Následně se budu snažit tyto negativní faktory vyhodnotit a implementací BCM představit konkrétní plán na zachování kontinuity.

Na základě výsledku provedené analýze obchodních společností v předcházející kapitole jsem se rozhodla vytvoření BCP pro společnost zabývající se jak výrobou, tak i montáží zabezpečovacího zařízení. Bude se jednat o fiktivní společnost, kterou jsem si vytvořila na základě svého uvážení.

V této části práce budu postupovat dle jednotlivých částí normy BS 25999-1, tak jak by to mělo vždy být v případě, že se společnost pro zavedení BCM rozhodne.

Jak bylo uvedeno v teoretické části při zavedení procesu kontinuity činností, je důležité dodržení jednotlivých fází a dokumentů, aby BCM bylo co nejúčinnější.

4.1 Fáze 1 : Zavedení BCM

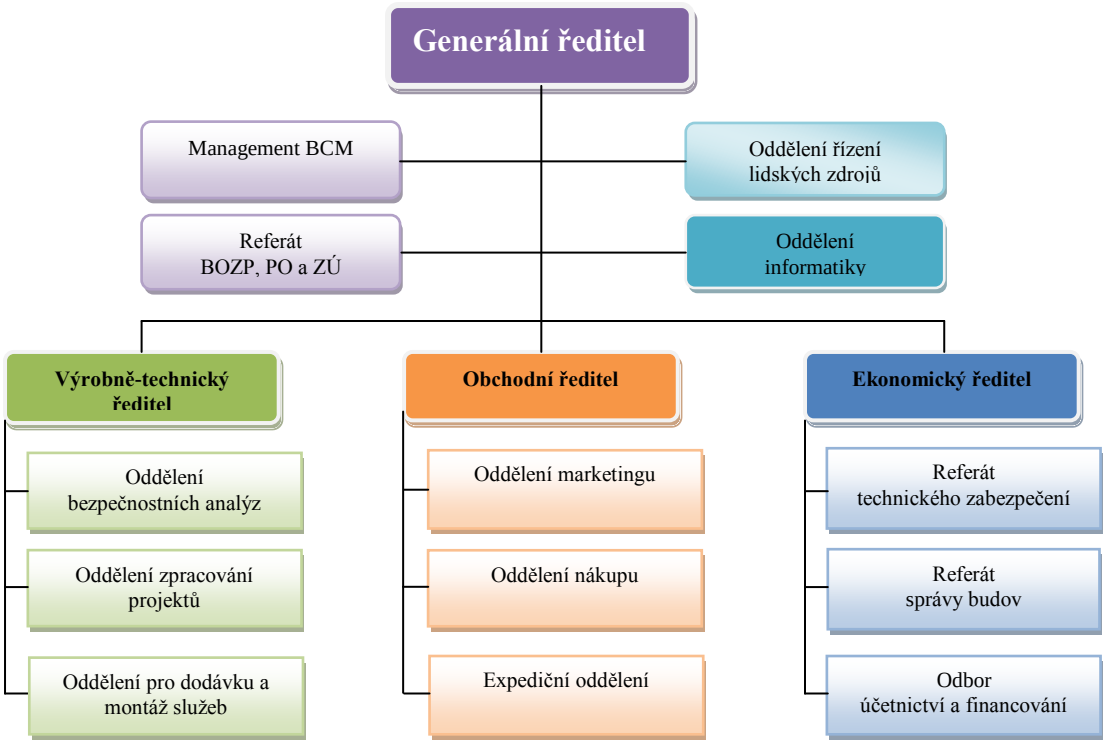
Jak již víme, v této fázi dochází k získání důležitých informací o společnosti, která má zájem o zavedení BCM. Jde především o identifikaci cílů společnosti, směr jakým společnost směřuje a rozbor všech činností, kterými se společnost zabývá. Popisem činností se myslí nejenom interní činnost, ale také vzájemné působení a vazby na externí společnosti.

4.1.1 Analýza obchodní společnosti

Obchodní společnost sídlí v Brně a její hlavní činností je podnikání v oblasti zabezpečení bytů, rodinných domů, výrobních prostor, administrativních budov nebo skladů. Jedná se o společnost, která sídlí na okraji města, na vlastním pozemku o rozloze 5000 m^2. V Brně je hlavní sídlo společnosti, ale má i tři pobočky a to: Zlín, Praha, České Budějovice. Celkový počet zaměstnanců ve společnosti je 400 a to včetně poboček. Jelikož hlavní sídlo je

v Brně, je zde i největší počet zaměstnanců a to 250, na každé pobočce je pak 50 zaměstnanců.

V následujícím obrázku představím organizační strukturu společnosti a to pro lepší orientaci při tvorbě samotných plánů kontinuity činností a stanovení jednotlivých rolích.



Obr. 6: Organizační struktura společnosti

Jak už bylo řečeno, mezi hlavní aktivity společnosti patří navrhování zabezpečovací techniky, zpracování nabídek, montáž zařízení a prodej jednak formou maloobchodu ve vlastní prodejně nebo prostřednictvím e-shopu a zároveň formou velkoobchodu pro další firmy, zabývající se poskytováním zabezpečovací techniky. Své služby společnost dodává jak malým zákazníkům, tak i větším společnostem jakou jsou středně velké výrobní podniky nebo supermarkety.

Hlavní činnost můžeme tedy rozdělit na tyto části:

1. **Návrh zabezpečovacích systémů.**
2. **Zpracování nabídek.**
3. **Montáž.**
4. **Prodej.**

Tyto činnosti musí na sebe vzájemně navazovat, aby byl zachován plynulý chod společnosti. V současné době jde o společnost, která se velmi dynamicky rozvíjí a z důvodu toho, že počet zákazníků narůstá, v případě výpadku nebo přerušení plynulého chodu činností by mohly vzniknout pro společnost ztráty, které by měly velmi negativní vliv na dobré jméno, které si společnost vybudovala.

Jelikož se jedná o společnost, která má v ČR dobré postavení a chce být nadále na trhu úspěšná, rozhodla se přistoupit na zavedení BCM do společnosti. Z důvodu velkých, důležitých zákazníků vyplynula potřeba připravit se aplikací BCM na řešení krizových situací, které mohou nastat, v případě nečekané události.

Hlavním cílem společnosti je totiž udržení svého dobrého jména na trhu, nabízení kvalitních služeb pro své stávající, ale i nové zákazníky. Kvalitních služeb je dosahováno především kladným přístupem vedením společnosti, které podporuje nápady a vytváří vzdělávací aktivity pro své zaměstnance. Jelikož vedení společnosti podporuje veškeré činnosti pro zlepšení svých nabízených služeb, je vstřícné ke změnám rozhodla se přistoupit k zavedení BCM do společnosti. Společnost vyčlenila dostatek financí na celý projekt BCM, ale také na případné nutné změny, úpravy, které na základě BCM vyvstanou.

Vytvořením plánu BCM bude mít společnost náskok před konkurencí, která v této oblasti stále narůstá.

4.2 Fáze 2 : Analýza a strategie

Po představení obchodní společnosti a pochopení činností společnosti přichází na řadu fáze, která je pro úspěšné zavedení BCM stěžejní. Jde o velmi důležitou fázi, při které se právě analyzují rizika, které společnosti hrozí, což představuje základ pro vytvoření plánu pro zachování kontinuity činností společnosti.

4.2.1 Analýza rizik

Aby bylo možné provést analýzu rizik, je třeba uvědomit si jednotlivé procesy ve společnosti a brát v úvahu veškeré činnosti jasně zřetelné, ale i ty, které nejsou na první pohled zřejmé. Je důležité pochopit cíle, které má společnost stanovené a kterých chce dosáhnout. Na základě předcházející analýzy společnosti pak můžeme identifikovat hrozby a provést analýzu rizik, které mohou společnost ohrozit v případě, že nastanou. Musíme se

zaměřit zejména na hlavní činnosti organizace, které jsou pro ni klíčové a na jejich vzájemné vazby.

Jelikož aktivity firmy můžeme rozložit na různé směry, budeme nyní tyto části analyzovat z hlediska propojenosti a z hlediska působení možných hrozeb.

Část první - Návrhy zabezpečovacích systémů. Tato činnost je pro firmu z hlediska zisku nejdůležitější, neboť se jedná převážně o velké zakázky. Z tohoto důvodu budeme považovat tuto činnost za klíčovou, na které záleží veškerý úspěch společnosti. Od samého počátku jsou všechny aktivity spojené s touto částí závislé na dobrém jméně společnosti, kvalifikovaných zaměstnancích, a to nejen v oboru zabezpečovacích systémů, ale také těch, kteří se zabývají managementem společnosti, marketingem, obchodními činnostmi a současně na zaměstnancích, kteří nepřímo souvisí s hlavním předmětem podnikání dané společnosti, tzn. veškeré personální obsazení. Profit společnosti závisí zejména na kvalitním marketingu, propagaci, kvalitních manažerů a obchodníků, apod. Jakmile o nabízené služby projeví zákazník zájem, musí mít společnost v obchodnících profesionály, kteří budou mít znalosti, zkušenosti, praxi v oblasti problematiky zabezpečovacích systémů.

Část druhá - Zpracování nabídek. Tato část se opět odvíjí od kvalitního personálu, ale není zde sledován pouze lidský faktor. Zpracování nabídek, vyřizování obchodních zakázek, komunikace s pobočkami nebo zákazníky jsou činnosti zcela závislé na veškerých technických komponentech společnosti a to zejména na vybavení IT technologiemi, které zahrnují hardware, software, datové přenosy, atd. Aby mohly být zpracovány nabídky, potřebují zaměstnanci k tomuto spolehlivé technické vybavení.

Část třetí - Montáž. Další důležitou částí je montáž navržených systémů u zákazníka. Je opět závislá jak na lidském faktoru tak i technickém vybavení. Je třeba mít spolehlivé, dobře vyškolené zaměstnance, kteří montáž provedou odborným způsobem. Jedná se totiž o finální krok, kterým je zakázka dokončena.

Část čtvrtá - Prodej. Poslední část se zabývá samotným prodejem jednotlivých výrobků a komponentů, které společnost prostřednictví svých zakázek poskytuje. Jelikož společnost spolupracuje výhradně s dodavateli, kteří mají pro své výrobky potřebné certifikace, řadíme činnost prodeje za seriózní. Hlavním úkolem prodeje je mít nabízené zboží v dostatečném množství pro své zákazníky a v neposlední řadě dodržování dodacích lhůt. V této části je

činnost opět závislá na lidském faktoru ať už z hlediska znalostí výrobků, tak i znalostí souvisejících s prodejem, skladovou evidencí, atd. Neméně důležitou součástí je i plně funkční technické vybavení, na kterém je závislý proces zpracování veškerých objednávek.

Maloobchodní prodej je uskutečňován prostřednictvím svého kamenného obchodu, který sídlí v Brně, kde je zaměstnána jedna osoba jako prodejce, a dále jsou zde skladníci. Z důvodu velkého množství sortimentu provozuje společnosti i velkoobchod, kde nabízí vybrané zboží ve větším množství, prostory pro velkoobchod sídlí opět v Brně. Současně probíhá prodej i přes e-shop, který je pro společnost téměř nutností, jelikož tento způsob objednávání zboží a prodeje je v dnešní době považován za nejrychlejší.

Veškeré uvedené části musí být navzájem propojeny, musí mít plynulý chod, neboť jen tak lze dosáhnout úspěchu společnosti. Jedině tak může společnost dosáhnout dobrých výsledků a tím plnit stanovené cíle.

4.2.2 Stanovení potenciálních hrozeb

Na základě analýzy jednotlivých částí, jsem stanovila hrozby, které mohou plynulý chod společnosti více či méně narušit. Jde především o technické výpadky, které zasahují do všech částí, kterými se společnost zabývá. Může to být přerušení dodávky energie nebo funkčnost technického a programového vybavení IT technologií. Dále jde o hrozby, které nesouvisí přímo s technickými vlastnostmi, ale spíše s nečekanými jevy, jako jsou přírodní živly, selhání lidského faktoru, kriminální činnost, atd. V následující tabulce je zobrazen přehled možných rizik spolu s oceněním z hlediska dopadů na chod společnosti.

Tab. 2: Přehled a ocenění hrozeb

Hrozba		***Ocenění***	***Popis***
Dodávka energie	Elektřina	***10***	Hlavní zdroj pro činnost společnosti
	Plyn (topení)	***3***	Při poruše topení, možnost zvýšení absence zaměstnanců
	Voda	***5***	Při přerušení dodávky vody - omezený provoz společnosti
Technika IT	HW	***10***	Omezené možnosti zpracování zakázek
	SW	***10***	Ztráta nebo poškození dat
	Datové přenosy	***10***	Výpadky v komunikaci uvnitř i vně společnosti

Přírodní živly	Povodeň	***5***	Ohrožení provozu v nižších patrech
	Požár	***10***	Možnost poškození objektu, vybavení, ztráta důležitých dokumentů, zboží
Kriminální činnost	Vloupání	***10***	Možnost ztráty technického vybavení, zboží, dat prostředků
	Vandalismus	***5***	Zničení zabezpečovacího zařízení, pláště budovy
Lidský faktor	Nemoci	***8***	Absence zaměstnanců
	Krádeže	***5***	Nečekané odcizení majetku, dat, finančních prostředků
	Špatné znalosti	***10***	Možné poškození dobrého jména společnosti, reklamace
Technické prostředky	Vozový park	***8***	Možné zpoždění dodávek zboží nebo komponent zakázek
Ekonomická rizika	Smlouvy	***8***	Možné vypovězení smluv o dodávkách, ztráta zákazníka
	Platební neschopnost	***10***	Platební neschopnost za poskytnuté služby, zboží

4.2.3 Návrh opatření

Dodávka energie - výpadek elektrické energie lze eliminovat pouze s použitím záložního zdroje. Primárně je dodávka elektřiny realizována prostřednictvím veřejné rozvodné sítě od dodavatele e-on. Za sekundární (záložní) zdroj se nabízí nejjednodušší použití UPS, ale jeho kapacita v případě dlouhodobého výpadku nemusí být zcela dostačující. Proto je vhodné instalovat ještě dieselovou elektrocentrálu, která zajistí chod všech zařízení, z nichž nejdůležitější je samozřejmě výpočetní technika. Je třeba podotknout, že v případě výpadku nebo jakékoli havárie veřejné distribuční sítě, je v daném okamžiku prakticky bez proudu celá příslušná aglomerace, ale v případě naší společnosti je třeba zachování kontinuity všech interních procesů, jako je zejména zpracování dat, interní komunikace, tvorba podkladů, příprava zakázek pro maloobchod i velkoobchod, atd.

Technika IT - pro případy poruchy výpočetní techniky je třeba mít k dispozici dostatečný počet záložních počítačů a jiného nutného hardwaru, který musí být připraven pro okamžité použití. Tedy s nainstalovaným softwarem a jiným potřebným vybavením. To vše se týká tiskáren, komunikačních prostředků, serverů, atd. Dá se předpokládat, že výpadek výpočetní techniky nemusí být vždy převratně velkého rozsahu, není proto třeba každé

zařízení zvlášť dublovat. Je třeba ale zajistit např. vhodnou organizací pracovníků sloučení dvou nebo několika pracovišť do jednoho a podřídit tak činnost konkrétního oddělení k zabezpečení těch procesů, které jsou v daném okamžiku nejdůležitější.

Přírodní živly - pro případy hrozeb této kategorie je třeba vypracovat speciální havarijní plány, což je dokonce právnickým osobám nařízeno přímo příslušnými zákony. V našem případě (ve vztahu k BCM) je ale nutné mít k dispozici plány, podle nichž bude firma schopná v dostatečném časovém úseku obnovit všechny klíčové procesy, potřebné k zajištění produkce. Např. v případě povodně, nebo rozsáhlé havárie vodovodního řádu je třeba zpracovat plán pro přesun pracovišť (techniky, dokumentace, zboží) z nízkých, ohrožených pater do vyšších, aby bylo možné opět zahájit činnost. Dle rozsahu havárie je ale nutné přihlédnout k problematice obsazení pracovišť příslušným personálem. Zorganizovat jejich dopravu tak, aby nedošlo k ohrožení zdraví nebo života.

Jinou závažnou záležitostí je havárie v důsledku požáru. Není třeba se zde zabývat problematikou nutnosti instalace EPS, ale zpracováním postupů k záchraně osob, materiálu a veškerého vybavení v případě zasažení příslušného objektu požárem. Stejně jako v případě zatopení provozů je nutné podle předem připraveného plánu zorganizovat obnovu pracovišť na předem stanovené místa, např. do smluvně pronajatých náhradních prostor.

V souvislosti s připraveností na tento typ hrozeb je třeba klást důraz na preventivní opatření, které zahrnují zejména provádění preventivních prohlídek a údržby protipovodňových opatření, pravidelné školení personálu, kontrolu stavu požárně-bezpečnostních řešení objektů, provádění pravidelné údržby a revize EPS a dalších vyhrazených zařízení. Pokud to je ekonomicky a technicky únosné, je nutné volit umístění důležitých technologických zařízení tak, aby nemohlo dojít k jejich poškození jak vodou, tak požárem.

Kriminální činnost - jedná se převážně o pokusy pachatelů vniknout do areálu, které mohou většinou vést k poškození pláště budov a následně odcizení techniky, zboží, dokumentace a jiného majetku společnosti. K eliminaci těchto rizik je nutná instalace zabezpečovacích prvků a systémů jak k ochraně perimetru, tak pláště objektů jako jsou PZTS, CCTV, oplocení areálu, ACS, hlídací služba pro fyzickou kontrolu návštěv, klíčový

režim atd. Důsledná režimová opatření umožňují realizovat moderní systémy přístupových systémů ACS.

Lidský faktor - hrozby, které vyplívají z této příčiny, jsou velmi rozmanité a těžko předvídatelné. Příkladně i dlouholetý kvalitní, loajální pracovník může někdy podlehnout např. nabídce konkurence a vzápětí společnost určitým způsobem poškodit. Na místě je tedy klást velký důraz na personalistiku podniku, která musí zajistit výběr co nejkvalitnějších pracovníků. Na klíčových pozicích pak musí být osoby, na něž je spolehnutí a s dostatečnými odbornými předpoklady. V souvislosti s BCM ale nelze řešit pouze loajalitu pracovníků, ale celkové obsazení všech pozic firmy odpovídajícím personálem. Je nutné v rámci jednotlivých oddělení a pozic provádět periodická školení, pořádat vzdělávací kurzy (z důvodu nových technologií) a samozřejmě nastavit odpovídající mzdovou politiku. K eliminaci rizika dlouhodobých absencí na klíčových pozicích z důvodu nemocí je třeba zajistit vhodnou zastupitelnost pracovníků. V takových případech je pak nutné organizovat pracovní náplně tak, aby nemohlo dojít k výraznému snížení výkonu některého oddělení. To se týká jak pracovníků administrativy, tak oddělení příjmu a zpracování zakázek anebo montážních pracovníků. K tomuto účelu je vhodné osoby, které je možné použít ke konkrétní zastupitelnosti vhodně ohodnotit. V souvislosti s předcházením onemocnění zaměstnanců je třeba dbát hygienických zásad, umožnit jednotlivcům potřebná lékařská vyšetření a v případě nemoci patřičnou léčbu. Jen tak lze pracovníky spolehlivě chránit před propuknutím nežádoucích nákaz a snížit tak riziko oslabení pracovního kolektivu.

Technické prostředky - ke snížení rizika je nutná připravenost náhradních vozů, vzhledem k množství zakázek a rozsahu jednotlivých dodávek doporučuji zajistit na každé pobočce min. 2 náhradní vozidla. Tato vozidla mohou být přiměřeným způsobem používána k různým účelům a potřebám společnosti, ale prioritně musí být k dispozici oddělení zabezpečující dodávku zboží a služeb. V krajních případech je vhodné, aby byla zajištěna náhradní doprava prostřednictvím předem domluvené přepravní společnosti.

K předcházení poruch vozového parku je nutné zabezpečit pravidelný servis, technické kontroly, vést dokumentaci provozu a upozorňovat na vznikající závady.

Ekonomická rizika - ke snížení rizika je zapotřebí mít kvalifikované zaměstnance na ekonomických odděleních. Musí dbát na řádné podmínky jak ve smlouvách týkajících se

nájmu, zakázek, projektů, tak i na dodržování termínů splatnosti na vystavených fakturách. V případě nedodržení stanovených podmínek nastavit vysoké sankce. Dále je nutné sledování aktuální ekonomické situace, konkurence na trhu, vybírání vhodných, spolehlivých dodavatelů. Musí být zajištěna vždy finanční rezerva v případě platební neschopnosti zákazníka, tak aby společnosti nevznikala potřeba se zadlužovat. V případě vypovězení smluv, hledat co nejvhodnější řešení pro klienta, snaha udržení klienta např. formou lepších cen, bonusů, služeb.

4.3 Fáze 3 : Plánování

Po důkladné analýze veškerých hrozeb a jejich dopadů přichází na řadu plány, kterými se budou zaměstnanci v případě vzniku mimořádné události řídit. Přednostně budou vytvořeny plány na hrozby, které nejvíce ohrožují chod společnosti. Z mého pohledu se mi jeví jako nejkritičtější dopad na činnost - **Návrh zabezpečovacích systémů**, jelikož tato činnost je pro společnost nejziskovější.

V následujících kapitolách uvedu, jak by mělo v praxi vytvoření plánů vypadat a co všechno by měly obsahovat.

4.3.1 Plán zvládání (managementu) incidentu:

V rámci tvorby BCM do společnosti je nedílnou součástí plánování vytvoření dokumentu, který má za úkol řídit a organizovat postup při vzniku incidentu. Obsahem plánu by měl být přehledný seznam úkolů, které mají být při vzniku mimořádné události provedeny. Na prvním místě je vždy zajištění bezpečnosti osob, což je pro společnost nejdůležitější. Dále navazují další činnosti, které mají za úkol zvládnout incident v co nejpřijatelnějším způsobu řešení.

V následujících kapitolách jednotlivé kroky popíšu a na obrázku č. 7 pak graficky zobrazím jejich sled. Jedná se o postup, který musí být zachován od samotného vzniku incidentu až po jeho úplné zvládnutí.

4.3.1.1 Hlášení mimořádné události

V případě jakéhokoliv podezření na ohrožení života či provozu je nutné zachování tohoto postupu:

a) vznik přírodních hrozeb - postupovat v souladu s pravidly BOZP a dle stanoveného evakuačního plánu,

b) vznik ostatních hrozeb - jakýkoliv vznik mimořádné události je zaměstnanec povinen hlásit svému přímému nadřízenému (vedoucí oddělení), případně jeho zástupci.

U obou typů hrozeb je provedeno vedoucím oddělení (krizového týmu) prvotní posouzení mimořádné události a na základě vyhodnocení aktivuje příslušnou část BCP.

Vedoucí krizového týmu v prvé řadě chrání zdraví a životy zaměstnanců a postupuje v souladu s pravidly požární ochrany, BOZP, dle evakuačního plánu. Jeho povinností je vždy provést důkladnou kontrolu a mít přehled o počtu všech evakuovaných zaměstnanců, a jakmile budou všichni zaměstnanci v bezpečí, opouští jako poslední místo vzniku mimořádné události.

Následně vedoucí krizového týmu řídí obnovu procesů podle zpracovaného BCP a zajišťuje informování a komunikaci s veškerými členy krizového týmu. Při vzniku 2. stupně a vyššího je povinnost informovat manažera BCM o vzniklé situaci. V případě, že se jedná o 1. stupeň, není podmínkou informovat o vzniklé situaci manažera BCM, veškerou odpovědnost při vzniku tohoto stupně přebírá vedoucí krizového týmu.

4.3.1.2 Vyhlášení a ukončení mimořádného stavu

Pokud ve společnosti vznikne mimořádná událost na 1. stupni, není nutnost svolávat krizový tým. Je na posouzení vedoucího krizového týmu, zdali je nutné svolat všechny členy krizového týmu nebo je možné vznik incidentu řešit běžnými operativy. Od vzniku 2. stupně mimořádné události je bezpodmínečné svolání všech členů krizového týmu.

Při zjištění mimořádných stavů, které jsou očekávány např. 1 denní výpadek klíčových systémů nebo zjištění jakékoliv nečekané události na úrovni 1. stupně, je bezpodmínečně nutné včasně reagovat na vzniklou situaci a informovat o ní veškeré členy týmu, aby byli srozuměni o možném vzniku vyššího stupně mimořádné události.

Ukončení mimořádného stavu je vyhlášeno vedoucím krizového týmu.

4.3.1.3 Místo setkání krizového týmu

V případě, kdy mimořádná událost dosahuje 2. stupně dochází ke svolání všech členů krizového týmu. Tito členové se schází na předem určeném místě a to z důvodu posouzení vzniklé situace, jejího rozsahu, dopadu tak, aby byla přijata příslušná opatření. Pokud nastane situace, že je vznikem mimořádné události zasažen celý objekt společnosti, schází se členové krizového týmu na předem určené budově v okolí společnosti, jedná se o náhradní místo setkání. Při vzniku mimořádné události je povinností zástupce krizového týmu na ověření prostorů pro setkání krizového týmu.

4.3.1.4 Komunikační strategie

Interní komunikace - vedoucí krizového týmu o vyhlášeném mimořádném stavu od stupně 2. informuje svého přímého nadřízeného, který zajistí informovanost ostatních organizačních jednotek, na které má událost dopad. Zaměstnanci jsou o mimořádném stavu, postupu jeho zvládání, pracovní náplni v následujících dnech, apod. informováni svým přímým nadřízeným.

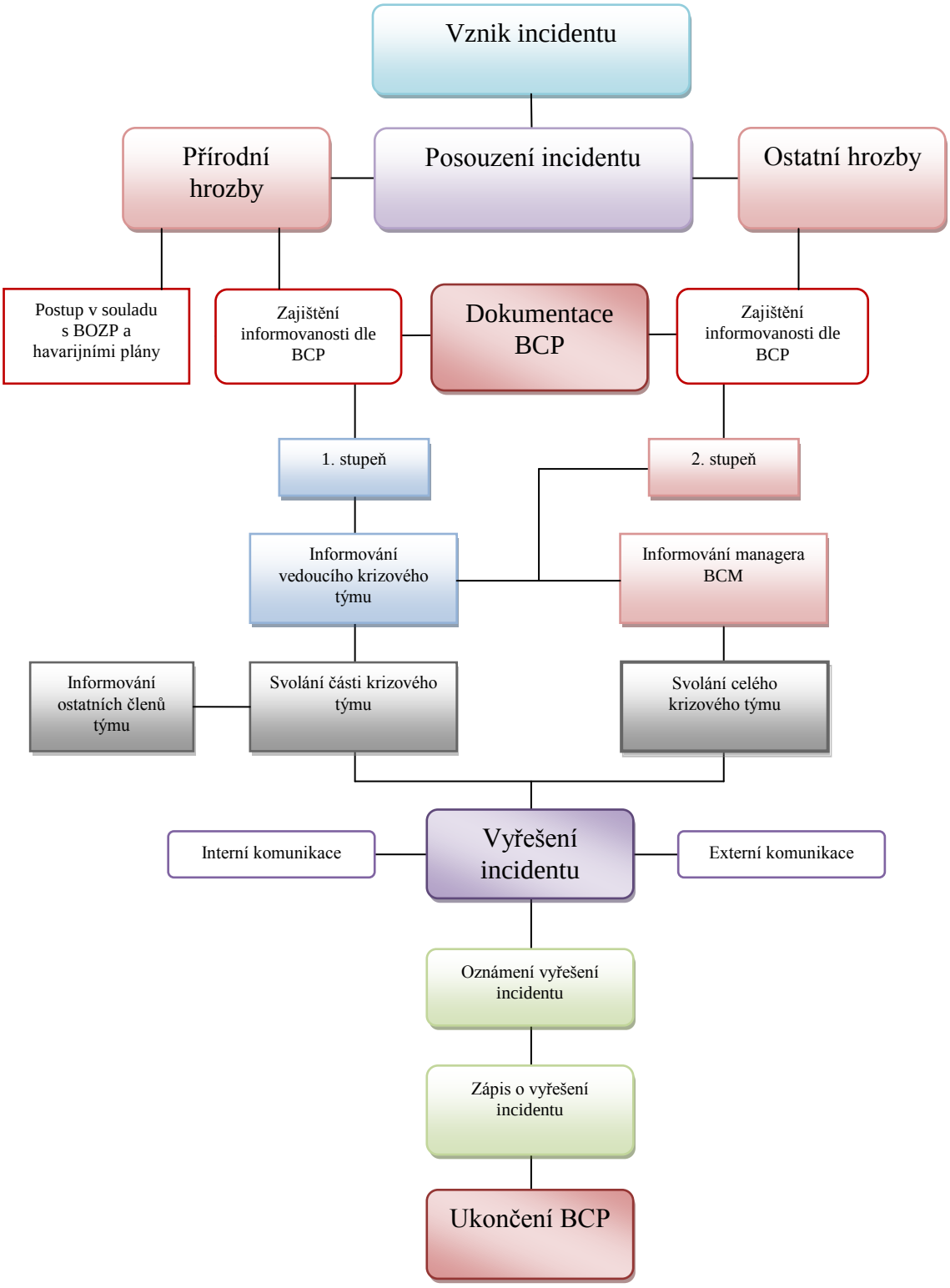
Externí komunikace - žádný zaměstnanec nemá povolení k poskytování jakýchkoliv informací o vzniku mimořádné události. Poskytování těchto informací všem externím osobám (klienti, rodinní příslušníci, složky IZS) je plně v kompetenci tiskového mluvčího, případně v jeho nepřítomnosti ředitelem společnosti. Komunikaci s veřejností a médii má taktéž na starosti tiskový mluvčí společnosti. Kromě tiskového mluvčího nesmí s médii nikdo jiný komunikovat a podávat informace o nastalé situaci - zaměstnanci se vždy odkazují na tiskového mluvčího společnosti.

4.3.1.5 Záznamy o důležitých informacích o incidentu

Jedná se o dokument, který obsahuje záznamy o rozhodnutích a činnostech týmu, jako je časový přehled incidentu, detaily ztrát a veškeré další činnosti provedené v souvislosti se vznikem mimořádné události. Tyto údaje provádí vedoucí krizového týmu, popřípadě osoba z týmu, která je na vzniklém místě události jako první.

Záznamy by měly být co nejpodrobnější, aby mohl být následně zmapován celý průběh zvládání události a případně přijata nápravná opatření.

V případě nutnosti je možné přistoupit na alternativní postupy při vzniku incidentu, avšak tyto postupy musí být pečlivě zaznamenány, aby mohly být následně zapracovány do plánu, a tímto by byla provedena aktualizace plánu.



Obr. 7: Schéma procesu zvládnutí incidentu

4.3.2 Plán kontinuity činností pro návrh zabezpečovacích systémů

V této části práce provedu vytvoření BCP formou tabulek s uvedením klíčových hrozeb, jejich popisem a návrhem řešení, aby v případě jejich vzniku všechny zainteresované osoby věděly, jakým způsobem mají postupovat. Jelikož vytvoření kompletního BCP pro společnost by představovalo obsáhlý dokument, vybrala jsem pouze jednu činnost společnosti a to **Návrh zabezpečovacích systémů**.

4.3.2.1 BCP pro činnost - návrh zabezpečovacích systémů

Plán vychází z předcházející analýzy, která identifikovala hrozby, jež v případě, že nastanou, mohou významným způsobem narušit plynulý chod společnosti. Jak jsem již uvedla, z důvodu obsáhlosti, jsem vybrala hrozby, které jsem ocenila v předcházející analýze jako nejrizikovější.

Z vybraných hrozeb jsem vytvořila tabulky, které uvádí popis hrozeb s dopadem na daný proces, pravděpodobnost jejich vzniku a návrhy opatření. Z důvodu obsáhlosti tématu, je opět navrženo opatření pouze při kritické míře dopadu na chod společnosti.

Tab. 3: BCP pro hrozbu - Dodávka elektrické energie

Plán kontinuity činností (BCP)	
Návrh BCP pro činnost - Návrh zabezpečovacích systémů	
Název hrozby:	**Dodávka energie - Elektřina**
Pravděpodobnost vzniku:	**nízká**
Popis hrozby:	**Výpadek veřejné distr. sítě nebo závada na hl. přívodu**
Významnost (ocenění):	**10**
Opatření:	
Prevence: 1. Instalace náhradních zdrojů el. energie (UPS, elektrocentrála) s potřebným výkonem. **Činnosti v případě trvání hrozby:** 1. Uvést do provozu náhradní zdroj el. energie. 2. V případě, že porucha je na zařízení veřejné rozvodné sítě kontaktovat havarijní službu dodavatele. 3. V případě, že porucha je na vlastním zařízení, povolat smluvní elektro servis.	

Tab. 4: BCP pro hrozbu - Požár

Plán kontinuity činností (BCP)	
Návrh BCP pro činnost - Návrh zabezpečovacích systémů	
Název hrozby:	**Požár**
Pravděpodobnost vzniku:	**vysoká**
Popis hrozby	**Poškození objektu vznikem požáru**
Významnost (ocenění):	**10**
Opatření:	
Prevence: 1. Kontrolovat dodržování opatření dle existujících požárně-bezpečnostních řešení stavebních objektů. 2. Provádět pravidelnou údržbu a revize vyhrazených zařízení. 3. Dodržovat předpisy pro skladování hořlavin. 4. Provádět pravidelné kontroly zařízení EPS. **Činnosti v případě trvání hrozby:** 1. Provádět činnosti v souladu s požárními a poplachovými směrnicemi společnosti oznámení požáru nadřízenému, v případě, že je požár možno eliminovat pomocí PPH, neprodleně zahájit hašení. V případě potřeby telefonicky zajistit zásah HZS. 2. Odhadnout možné důsledky z hlediska omezení provozu objektu, v případě, že ohrožení neumožní bezpečný chod společnosti, zajistit jeho bezpečné odstavení. 3. V případě, že požár neohrožuje provoz objektu, provádět preventivní opatření, které zabrání rozšíření požáru a ohrození provozu okolních jednotek. Dále viz HAVARIJNÍ PLÁN SPOLEČNOSTI, Požární a poplachové směrnice a požární řády.	

Tab. 5: BCP pro hrozbu - Výpadek HW a SW

Plán kontinuity činností (BCP)	
Návrh BCP pro činnost - Návrh zabezpečovacích systémů	
Název hrozby:	**Technika IT - HW, SW**
Pravděpodobnost vzniku:	**vysoká**
Popis hrozby:	**Porucha potřebného IT vybavení**
Významnost (ocenění):	**10**

Opatření:
Prevence: 1. Dodávku a pravidelné obnovu hardware a potřebného IT vybavení realizovat smluvně formou outsourcingu. 2. Zabezpečit pravidelné zálohování dat a dostatečný počet náhradní techniky. **Činnosti v případě trvání hrozby:** 1. Kontaktovat firmu, která zajišťuje správu IT vybavení. 2. Uvést do provozu potřebnou záložní techniku, popř. přesunout konkrétní činnost do jiného oddělení.

Tab. 6: BCP pro hrozbu - Výpadek datových přenosů

Plán kontinuity činností (BCP)	
Návrh BCP pro činnost - Návrh zabezpečovacích systémů	
Název hrozby:	**Technika IT - Datové přenosy**
Pravděpodobnost vzniku:	**střední**
Popis hrozby	**Porucha počítačové sítě a komunikačních kanálů**
Významnost (ocenění):	**10**
Opatření:	
Prevence: 1. Služby v oblasti správy počítačové sítě realizovat smluvně formou outsourcingu. 2. Zajištění služeb mobilního operátora, popř. zřízení pevné linky. **Činnosti v případě trvání hrozby:** 1. Kontaktovat firmu, která zajišťuje správu počítačové sítě. 2. V případě poruchy telefonického spojení po mobilní síti použít komunikační prostředky pevné linky.	

Tab. 7: BCP pro hrozbu - Vloupání

Plán kontinuity činností (BCP)	
Návrh BCP pro činnost - Návrh zabezpečovacích systémů	
Název hrozby:	**Kriminální činnost - Vloupání**

Pravděpodobnost vzniku:	**vysoká**
Popis hrozby:	**Pokus o narušení objektu, nepovolané osoby**
Významnost (ocenění):	**10**
Opatření:	
Prevence: 1. Areál objektu je oplocen, vybaven PZS a střežen hlídací službou. 2. Průchod přes vrátnici je možný pouze po zapsání do knihy návštěv a předložení průkazu totožnosti. Návštěvy si musí zaměstnanci vyzvednout osobně na vrátnici. **Činnosti v případě trvání hrozby:** 1. Ihned informovat o vzniklé situaci nadřízeného, dále pracovníka hlídací služby na vrátnici a Policii ČR. 2. Vyčkat na pokyny nadřízeného. V případě ohrožení provozu objektu provést úkony k ochraně osob a majetku.	

Tab. 8: BCP pro hrozbu - Lidský faktor

Plán kontinuity činností (BCP)	
Návrh BCP pro činnost - Návrh zabezpečovacích systémů	
Název hrozby:	**Lidský faktor - Znalosti**
Pravděpodobnost vzniku:	**střední**
Popis hrozby	**Způsobení závažných pochybení**
Významnost (ocenění):	**10**
Opatření:	
Prevence: 1. Provádět účinnou personalistiku společně s personálním auditem důrazem na přezkoušení z potřebných znalostí. 2. Organizovat pravidelné školení personálu na všech úrovních a ve všech profesích. **Činnosti v případě trvání hrozby:** 1. V případě zjištění pochybení zaměstnance přistoupit k různým formám osobního postihu. 2. Při opakovaném nebo vážném pochybení zavést kroky k rozvázání pracovního poměru.	

Tab. 9: BCP pro hrozbu - Kybernetický útok

Plán kontinuity činností (BCP)	
Návrh BCP pro činnost - Návrh zabezpečovacích systémů	
Název hrozby:	**Kybernetický útok velkého rozsahu**
Pravděpodobnost vzniku:	**Velmi vysoká**
Popis hrozby	**Virová nákaza SW, útok z veřejné datové sítě**
Významnost (ocenění):	**10**
Opatření:	
Prevence: 1. Všechny systémy chránit aktualizovaným antivirovým softwarem. Virová nákaza je možná pouze přenosem pomocí přenosných médií (USB disky, CD-ROM, SD karty,…). 2. Zaměstnanci společnosti na všech pobočkách jsou povinni dodržovat základní zásady práce s přenosnými datovými médii a emailovou poštou. **Činnosti v případě trvání hrozby:** 1. V případě zjištění hrozby vyřadit zařízení z provozu a kontaktovat firmu zajišťující správu IT technologií.	

Tab. 10: BCP pro hrozbu - Platební neschopnost

Plán kontinuity činností (BCP)	
Návrh BCP pro činnost - Návrh zabezpečovacích systémů	
Název hrozby:	**Ekonomické riziko - Platební neschopnost**
Pravděpodobnost vzniku:	**vysoká**
Popis hrozby	**Nezaplacené faktury**
Významnost (ocenění):	**10**
Opatření:	
Prevence: 1. Uzavřené zakázky pečlivě připravit, zvýraznění dodacích podmínek, splatností. 2. Dostatečně vysoká sankce za zpoždění plateb, sledovat termíny splatností. **Činnosti v případě trvání hrozby:** 1. Poslední den splatnosti zaslat upozornění na tento termín, následně v případě zjištění nezaplacené platby ihned kontaktovat zákazníka a požadovat úhradu včetně sankce.	

Následující tabulka představuje stupně, při kterých dochází k aktivaci samotného BCP. V tabulce je uveden stupeň mimořádné události v časové hodnotě, který představuje dobu výpadku klíčových aplikací, systémů. Dále je zde pro představu uvedena míra dopadu, což je ve skutečnosti dopad na chod společnosti při konkrétním stupni mimořádné události. Jsou zde uvedeny příklady, o jaké narušení se jedná. Z praktického hlediska se považuje aktivace samotného BCP v případě druhého stupně a výš, první stupeň mimořádné události se řeší prostřednictvím odpovědných osob.

Tab. 11: Hodnocení stupňů mimořádné události

Stupeň MU- (čas) - Míra dopadu	
1. stupeň - (8hodin) - Žádný (Ž)	**2. stupeň - (1den) - Malý (M)**
Menší výpadky hlavních systémů, nefunkčnost programů, absence zaměstnanců, omezený provoz, nečekané havárie.(vždy v řádech hodin, zaměstnanci do 10%)	Výpadky hlavních systémů, nefunkčnost programů, absence zaměstnanců, omezený provoz, nečekané havárie.(vždy v řádech dnů, zaměstnanci do 40%)
3. stupeň - (5dní) - Velký (V)	**4. stupeň - (>10dní) - Kritický (K)**
Větší výpadky hlavních systémů, nefunkčnost programů, absence zaměstnanců, omezený provoz, nečekané závažné havárie.(vždy v řádech několika dnů, zaměstnanci do 70%)	Rozsáhlé výpadky hlavních systémů, nefunkčnost programů, dlouhodobé výpadky procesů, aplikací, absence zaměstnanců - celá oddělení, min. provoz, nečekané kritické havárie - kritický dopad na celý chod společnosti (vždy nad 10 dnů, zaměstnanci nad 90%)

4.3.2.2 Role a odpovědnost při vzniku incidentu

Ve společnosti je vytvořen krizový tým pro případ vzniku incidentu v procesu **Návrh zabezpečovacích systémů**. Jeho složení je tvořeno členy jednotlivých oddělení, které jsou v případě vzniku incidentu ohroženy, zároveň je v tabulce uveden stupeň, při kterém je nutné danou osobu kontaktovat. Struktura krizového týmu je v tabulce č. 12.

Dále je nutné v plánu uvést ostatní důležité kontakty na organizace a osoby, které je třeba v případě vzniku nečekané události informovat, protože na jejich činnosti také závisí rychlost a průběh zvládnutí incidentu. Jedná se zejména o kontakty na jednotlivé složky IZS, majitele společnosti, servisní společnosti, atd. viz tab. 13.

Tab. 12: Struktura krizového týmu

Struktura krizového týmu - NÁVRH ZABEZPEČOVACÍCH SYSTÉMŮ				
Role	**Funkce/oddělení**	**Jméno, příjmení**	**Kontaktní údaje**	**Stupeň**
Hlavní osoby	Vedoucí krizového týmu	Petr Svoboda	+420 774234897 svoboda@abab.cz	1,2,3,4 stupeň
	Zástupce krizového týmu	Jan Nový	+420 774657212 novy@abab.cz	2,3,4 stupeň
	Manažer BCM	Adam Eben	+420 774234590 eben@abab.cz	2,3,4 stupeň
	Ekonomický ředitel	Pavel Straka	+420774 654387 straka@abab.cz	2,3,4 stupeň
	Obchodní ředitel	Dana Jamná	+420774 356721 jamna@abab.cz	2,3,4 stupeň
	Výrobně-technický Ředitel	Jiří Adamec	+420774 908790 adamec@abab.cz	2,3,4 stupeň
	Generální ředitel	Ing. Marek Jurček	+420774 345786 jurcek@abab.cz	3,4, stupeň
Členové	Oddělení informatiky	Radek Horký	+420774876564 horky@abab.cz	2,3,4 stupeň
	Oddělení bezpečnostních analýz	Petr Matuška	+420774376908 matuska@abab.cz	2,3,4 stupeň
	Oddělení zpracování projektů	Eva Polachová	+420774125453 polachova@abab.cz	2,3,4 stupeň
	Oddělení pro dodávku a montáž služeb	Tomáš Hamánek	+420774967431 hamanek@abab.cz	2,3,4 stupeň

Tab. 13: Seznam kontaktů v případě vzniku incidentu

Důležité kontakty pro vznik incidentu		
	Kontakt	**Telefonní číslo**
Složky IZS	HZS	150
	ZZS	155
	Policie ČR	158
Vedení společnosti	Generální ředitel Ing. Marek Jurček	+420 774345786
	Zástupce ředitele Mgr. Jiří Novotný	+420 774231975

	Tisková mluvčí Mgr. Eva Slabá	+420 774098675
Servisní společnosti	Servis pro správu budov, vodo-topo, plyn	+420 607443876
	Servis IT	+420775342765
	Dispečink veřejné rozvodné sítě el. energie	+420 773890654

Při tvorbě BCP je důležité mít údaje o místě setkání krizového týmu s případným náhradním místem, pokud není možné se sejít v místě určeném v objektu společnosti.

Tab. 14: Kontaktní údaje na místo krizového týmu

Místo setkání krizového týmu			
Hlavní místo setkání:	**Abab, spol. s.r.o., Heršpická 29, Brno - Královo Pole, 612 00**	**Podlaží:**	**1**
Kancelář:	**Kancelář výrobně technického-ředitele**	**Číslo kanceláře**	**43**
Náhradní místo setkání:	**STAVOMAX, spol. s.r.o., Košínova 31, Brno - Královo Pole, 612 00**	**Podlaží:**	**1**
Kancelář:	**Kancelář ředitele společnosti**	**Číslo kanceláře**	**128**
Poznámky:			

4.3.2.3 Systém kontroly verze plánu

Součástí tvorby BCP je dokument, který obsahuje údaje o jakékoliv aktualizaci a změně provedené v plánu, které musí být pravdivě zaznamenány, co, kdo a kdy zaznamenal. Po každé aktualizaci nastává změna v čísle verze plánu, kterou musí obdržet všechny oprávněné osoby. Všichni členové musí mít vždy aktuální verzi plánu, včetně zaznamenaných změn.

Tab. 15: Seznam držitelů plánu

Přehled držitelů plánu			
Jméno, příjmení	**Forma plánu Tištěná/elektronicky**	**Verze plánu**	**Datum, podpis**
Petr Svoboda	T&E	1.00	
Jan Nový	T&E	1.00	
Adam Eben	T&E	1.00	
Pavel Straka	T&E	1.00	
Dana Jamná	T&E	1.00	
Jiří Adamec	T&E	1.00	
Ing. Marek Jurček	T&E	1.00	
Radek Horký	T	1.00	
Petr Matuška	T	1.00	
Eva Polachová	T	1.00	
Tomáš Hamánek	T	1.00	
Změny v plánech			
Verze plánu	Uskutečněná změna	Provedl	Datum, podpis
1.00	Aktualizace tel. čísel	Petr Svoboda	1. 5. 2013
1.01			

4.3.2.4 Záznamy o průběhu incidentu

V případě vzniku incidentu je v rámci BCP vytvořen dokument, který zaznamenává celý průběh jednotlivých kroků celého krizového týmu a všech zúčastněných osob. Záznam vytváří zpravidla vedoucí krizového týmu, případně osoba, která byla na místě vzniku incidentu jako první, která po příchodu vedoucího krizového týmu mu předá tuto činnost. Je nutné zaznamenání detailního průběhu zvládání události, zejména pak všech odlišných postupů stanovených v plánech. Na základě tohoto záznamu, se pak vytvoří závěr, který bude v případě změn implementován do plánu, tzn., že bude provedena aktualizace.

Tab. 16: Formulář na popis incidentu

Průběh činností při vzniku incidentu

Vznik incidentu		Průběh zásahu
Datum:	Čas:	
První osoba na místě vzniku incidentu		
Další zúčastněné osoby		

4.3.3 Plán obnovy činností

Plán obnovy činností představuje dokument, který se zabývá zajištěním kontinuity a obnovy klíčových procesů společnosti. Pro obnovu těchto procesů se využívají jak interních, tak i externích zdrojů. Hlavním úkolem tohoto plánu je dostupnost veškerých procesů, v případě vzniku mimořádné události, což je závislé jak na lidských, technických, informačních a finančních zdrojích.

4.3.3.1 Procesní činnosti pro návrh zabezpečovacích systémů

Pro znázornění plánu obnovy činností pokračuji v činnosti - návrh zabezpečovacích systémů. Z hlediska obnovy procesů a činností jsem stanovila pro vybranou činnost konkrétní procesní činnosti, které mají na společnost při vzniku mimořádné události největší vliv. Priorita těchto činností byla vybrána pro případy nefunkčnosti klíčových aplikací nebo větší absence zaměstnanců.

V následující tabulce jsou uvedeny vybrané procesní činnosti, které by měly být co nejdříve obnoveny: zpracování zakázky, uskutečňování plateb, vedení dokumentace.

Tab. 17: Vybrané procesní činnosti

Procesní činnosti	MTO	RTO	MRSL
Zpracování zakázky	2dny	12hod.	Alternativní zpracování (papír, off-line aplikace), komunikace s klientem
Uskutečňování plateb	3dny	1den	První budou hrazeny platby a přeplatky přesahující částku 12.000,- Kč u všech klientů a závazků
Vedení dokumentace	10 dní	5dní	Zajistit dokumenty dle výsledku posouzeného objektu, vždy řešit dokumenty dle priority zakázky

MTO - představuje maximálně akceptovatelnou dobu výpadku procesů.

RTO - (čas efektivní obnovy procesu) - jedná se o časovou hodnotu, která stanovuje požadavek na rychlost obnovy procesů při vzniku jejich přerušení.

MRSL - minimální úroveň funkčnosti procesů.

4.3.3.2 Stanovení zdrojů pro zachování kontinuity činností

U procesních činností jsem vyhodnotila jako nejdůležitější zdroje pro zachování kontinuity činností: zaměstnance, technické vybavení a aplikace pro činnosti související s navrhováním zabezpečovacích systémů. Následující tabulka pak znázorňuje jednotlivé zdroje, které je potřeba zajistit pro obnovu činností.

Tab. 18: Seznam použitých zdrojů

Seznam zdrojů pro zachování kontinuity činností					
Procesní činnosti	**Zdroje**				**Odpovědnost za dodání zdrojů**
	Zaměstnanci	**Aplikace**	**Technické vybavení**		
Zpracování zakázky	3	Program pro zpracování zakázky	PC	2ks	Oddělení informatiky
			Telefon	2ks	
			Tiskárna	2ks	
Provádění plateb	2	Bankovní aplikace	PC	2ks	Oddělení účetnictví a financování
		Účetní program	Kalkulátor	2ks	
			Telefon	2ks	
Vedení dokumentace	3	Program pro vedení dokumentace	PC	2ks	Oddělení zpracování projektů
			Tiskárna	2ks	
			Telefon	2ks	

4.3.3.3 Obsah plánu obnovy

Pro tuto kapitolu jsem si zvolila plán obnovy při hrozbě zatopení objektu společnosti v důsledku závady na vodovodním potrubí. Tato hrozba způsobí vyřazení klíčových aplikací, na kterých je zpracovávání návrhů zabezpečovacích systémů závislé. Tento výpadek má vliv na všechny procesní činnosti uvedené v tabulce č. 4.

Tab. 19: Časový harmonogram činností

Rozpis činností a časový harmonogram	
Doba trvání hrozby	**Činnost**
0-6 hod	– identifikace zdroje incidentu – uzavření hlavního přívodu vody – vypnutí všech energií (elektrické vedení, plyn), – ohlášení havárie nadřízenému – oznámení události na HZS – vyhodnocení události, svolání krizového týmu – zajištění personálu, který se bude podílet na obnově – zajištění potřebných zdrojů (materiál, technika) – záchrana datových médií a dokumentace – kontaktovat servis na opravu zasaženého místa – identifikace a odstranění chemických látek
6-12 hod	– přesun zařízení a materiálů do nezasažených objektů – zajištění dokumentace pro pojišťovnu (záznamy o průběhu incidentu, fotodokumentace) – zprovoznění zdroje el.energie – zprovoznění náhradních komunikačních zdrojů
>12 hod	– informování zákazníků – komunikace s externími dodavateli – zprovoznění klíčových aplikací v náhradním objektu – **viz tab. 20**. – úklid zasaženého objektu po odčerpání vody – obnova objektu (oprava podlah, vymalování) – vybavení objektu kancelářským nábytkem – obnova technického vybavení – vyhodnocení zvládnutí situace – vyčíslení materiálních a finančních škod

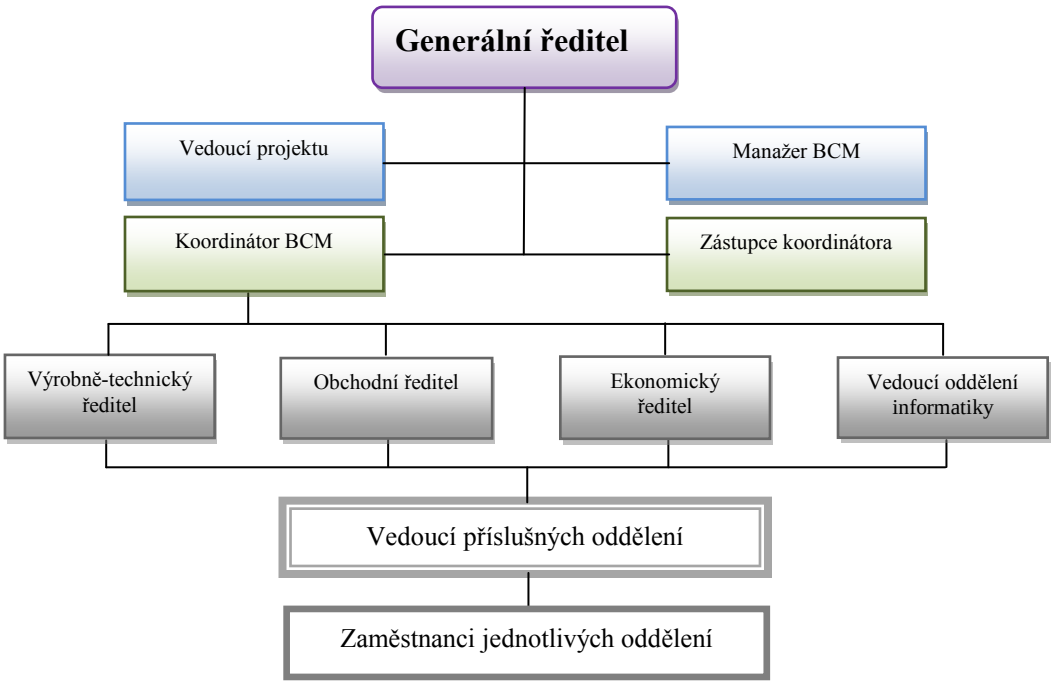
Součástí plánu obnovy musí být v případě nutnosti náhradního objektu potřebné údaje o tomto objektu.

Tab. 20: Údaje o náhradním objektu

Alternativní objekt			
Název zařízení:	**STAVOMAX, spol. s.r.o.**	**Podlaží:**	**2**
Adresa:	**Košínova 31, Brno - Královo Pole, 612 00**		
Telefon:	**604 623 271**	**Fax:**	**541 219 606**
Kontaktní osoba:	**Ing. David Procházka**	**Telefon:**	**604 844 744**
Alternativní osoba:	**p. Roman Čihák**		
Důležité údaje			

4.4 Fáze 4 : Implementace

Ve fázi implementace se uskutečňuje realizace samotného BCM do celého chodu společnosti. Aby zavedení BCM do společnosti, bylo co nejúčinnější, je důležité mít pro tento proces seznam osob, které se podílí na implementaci BCM do společnosti. Proto je vytvořena organizační struktura, podílející se na celém BCM v návaznosti na důležitost konkrétních rolích.



Obr. 8: Organizační struktura při implementaci BCM

Povinnosti členů

1. Vedoucí projektu

Řídí a koordinuje veškeré činnosti a aktivity související s ustavením, zaváděním, realizací a rozvoje funkčního systému řízení kontinuity činností. V jeho kompetenci je vypracování a schvalování strategií společnosti včetně jejích aktualizací.

2. Manažer BCM

Vytváří odbornou metodiku pro účinnost BCM ve společnosti, pravidelné revize analýzy dopadů a hodnocení rizik. Jeho osoba je odpovědná za správně vytvořených BCP, s tímto má další povinnost vytvořit strategii BCM a veškeré činnosti ve fázi zpracování a aktualizací dokumentů. Musí mít veškerý přehled o všech aktualizacích a změn uvnitř společnosti. V případě vzniku mimořádného 2. stupně je informován od vedoucí krizového týmu o nastalé situaci.

3. Koordinátor BCM za oddělení

Jeho činností je zachování kontinuity a obnovy procesů na jeho oddělení, za které je odpovědný. Podílí se aktivním způsobem při implementaci na BCM na jeho oddělení, musí dodržovat předem stanovené pravidelné testování jeho plánů. V rámci oddělení si musí zvolit svého zástupce, který bude odpovídat za platnost BCP v jeho nepřítomnosti.

4. Zástupce koordinátora

Plní veškeré pokyny svého koordinátora, poskytuje spolupráci v přípravě veškerých dokumentů, podkladů pro školení. Je zodpovědný za správnost, zaznamenávání změn, údajů, verzí.

5. Zaměstnanci

Všichni zaměstnanci musí být prokazatelně seznámení s procesem zavedení BCM do společnosti, účastní se pravidelných školení, testování BCM. V případě vzniku mimořádné události hlásí svému přímému nadřízenému tuto skutečnost a vyčkají na další pokyny od vedoucí krizového týmu. Jsou nápomocni při řešení a obnovy následků mimořádné události.

4.5 Fáze 5 : Testování a operativní řízení

V poslední fázi testování se společnost rozhodla pro zvolení testování formou simulačního testu. Jedná se o nacvičování a prověření postupů společně se schopností týmové práce dle předem připravených scénářů vždy pro konkrétní typ hrozby.

4.5.1 Simulační test

Simulační testy budou probíhat na základě předem stanoveného časového harmonogramu a předem stanovených hrozeb. Ty pro simulační test stanoví vždy manažer BCM a je jen na něm, který typ hrozby zvolí. Tato forma testu bude prováděna v pravidelných intervalech a to:

- jedenkrát za 6 měsíců (při běžném provozu společnosti),
- do 2 měsíců po vzniku incidentu (při omezeném provozu společnosti).

Tab. 21: Formulář simulačního testu

Simulační test pro vznik hrozby - zatopení objektu	
Datum zahájení testu: 1. 7. 2013	Zahájení testu (čas): 10:05 hod.
Datum ukončení testu: 1. 7. 2013	Konec testu (čas): 13:00 hod.
Popis hrozby: Po příchodu do zaměstnání pracovník oddělení zpracování zakázek zjistil zatopení objektu v celé jeho ploše do výšky zhruba 30 cm z důvodu závady na vodovodním potrubí.	
Vytvořil: Adam Eben - manažer BCM	Zaznamenal: Petr Svoboda - vedoucí krizového týmu
Provoz společnosti:	běžný
Seznam osob testování:	Petr Svoboda, Jan Nový, Adam Eben, Pavel Straka, Dana Jamná, Jiří Adamec, Ing. Marek Jurček, Radek Horký, Petr Matuška, Eva Polachová, Tomáš Hamánek
Záznamy o průběhu testování: O incidentu byly informovány všechny osoby uvedené v seznamu krizového týmu. Ten se sešel na předem určeném stanovišti. Následně byla zhodnocena míra incidentu a byly zahájeny práce v souladu s plánem obnovy. Byl učiněn pokus o kontaktování firmy zajišťující servis vodovodního potrubí, ale spojení nebylo navázáno z důvodu neexistujícího tel. čísla. Dále byla zjištěna závada na sekčním ventilu potrubí vody.	

Záznamy provedl:		Petr Svoboda - vedoucí krizového týmu
Vyhodnocení testování - nedostatky:		Lhůta pro odstranění nedostatků:
1. Zjištění nového tel. kontaktu na servisní organizaci		1 den
2. Vadný ventil na potrubí		3 dny
Implementace zjištěných nedostatků do BCP	Termín: Ihned	Provede: Petr Svoboda - vedoucí krizového týmu

Dílčí závěr

Cílem této části práce bylo popsat společnost z oblasti průmyslu komerční bezpečnosti, která se zabývá navrhováním zabezpečovacích systémů, jejich dodávkou a montáží. Na základě teoretických znalostí, jsem vytvořila příklad, jak by měla společnost v případě vytváření plánu kontinuity činností postupovat. Byla provedena analýza společnosti, pochopení jejich základních činností, stanovení hrozeb a na základě těchto výsledků jsem navrhla opatření, která by měla společnost aplikovat, aby byl zachován její plynulý chod v případě nečekané události.

Nejdůležitější fázi 3: Plánování, jsem zpracovala podrobněji, jelikož jejím výstupem je právě samotný plán kontinuity činnosti, který byl hlavním úkolem této diplomové práce. Součástí BCP je plán obnovy, který je pro zachování kontinuity činností důležitý, vzhledem k obnově klíčových procesů po vzniku incidentu.

Následující fáze implementace a testování jsem zpracovala již v menším rozsahu a to z důvodu velké obsáhlosti a složitosti tématu. I přesto jsem naplnila veškeré kroky dle normy BS 25999, které jsou závazné pro zavedení BCM do společnosti. Jedině při jejich dodržení vznikne materiál, který je pro společnost stěžejní a v případě vzniku mimořádné události účinný.

5 KRITERIA HODNOCENÍ MANAGEMENTU KONTINUITY ČINNOSTÍ ORGANIZACE

V poslední části této diplomové práce se zaměřím na způsob hodnocení zavedeného managementu kontinuity činností. Aby toto hodnocení bylo možné provádět kvalitně a objektivně, je třeba stanovit kritéria, na základě kterých se bude provádět audit zaměřený na veškerou činnost managementu kontinuity činností. Tato kritéria musí být odpovídat požadavkům příslušných norem, zejména BS 25999.

Vlastní hodnocení společnosti může být prováděno různými způsoby, já jsem ve své práci zvolila kontrolu zavedení BCM formou checklistu. Jedná se o dokument, ve kterém odpovídáme na otázky sestavené na základě předem stanovených kritérií. V případě, že dojde ke zjištění nějakých nedostatků, uvedou se formou záznamu spolu s časovým harmonogramem jejich odstranění.

5.1 Stanovení kritérií

Pro stanovení jednolitých kritérií pro hodnocení managementu kontinuity činností jsem rozdělila oblasti hodnocení na dvě části. Jednotlivé oblasti těchto částí jsou pak součástí checklistu.

1. **Část obsahující dokumenty**

Co se týká kritérií pro hodnocení oblastí, ve kterých jsou vytvořeny dokumenty (dokumentace, školení, testování, začlenění BCP do společnosti, právní předpisy, rozpočet) považuji za nutnost provedení kontroly:

- jmenný seznam osob vlastnících plány BCP,
- seznam s kontaktními údaji,
- značení a číslování plánů,
- úplnosti dokumentů,
- aktuálnost dokumentů,
- harmonogram aktualizací,
- seznam hrozeb,

- seznam cílů společnosti,
- přehledy o změnách v dokumentech,
- archivace všech dokumentů,
- záznamy o průběhu incidentu,
- finanční náklady.

V případě zjištěného nedostatku v oblasti spojené s dokumenty je navrženo opatření spočívající v doplnění dokumentů, aktualizace dokumentů, případně návrh na nové vypracování dokumentu. Vždy je stanovena lhůta, do které je požadována náprava.

2. **Část neobsahující dokumenty**

Jedná se o hodnocení oblasti, která není reprezentována konkrétními dokumenty a ve které nelze na první pohled určit jednoznačnou odpověď a to znalosti personálu. Pro tuto oblast navrhuji tato kritéria:

- test zaměstnanců o povědomí BCM,
- test členů krizového týmu.

K prokázání provedených školení a testů je třeba zkontrolovat:

- harmonogram školení,
- obsah školení,
- presenční listina zúčastněných.

Na základě vytvořených testů je provedena kontrola znalostí o celém BCM ve společnosti. V případě zjištění nedostatků navrhuji jako vhodný způsob odstranění tohoto nedostatku zvýšení četnosti porad a školení, ve kterých bude věnována pozornost právě BCM tak, aby byli jednotliví zaměstnanci o tomto procesu častěji informování a tímto způsobem se zavedení BCM jistě dostane do povědomí všech osob.

5.2 Průběh hodnocení

V předchozí kapitole jsem navrhla hodnotící kritéria pro hodnocení zavedení BCM do společnosti. Tato kritéria nyní budou posuzována metodou checklistu, prostřednictvím kterého se bude zjišťovat splnění požadavků dle normy BS 25999.

Obsah checklistu je sestaven tak, aby byly zhodnoceny důležité kroky, které musí být při zavedení BCM do společnosti provedeny a dodrženy. Z tohoto důvodu je vždy hodnocena oblast, ve které jsou uvedeny otázky vztahující se právě k dané oblasti hodnocení. Na jednotlivé otázky se v průběhu hodnocení bude odpovídat dle zjištěného stavu možností ano – ne. V případě odpovědi ne, je vyžadováno písemné zdůvodnění zjištěného nedostatku, případně důvod nesplnění daného kroku. Tímto způsobem je vyplněn celý dokument a na základě zjištěných odpovědí je provedeno navrhované opatření pro zjištěné nedostatky. Výsledky hodnocení jsou vždy stanoveny pro jednotlivé oblasti. Jelikož se BCM zavádí do společnosti jako celku, jsou kritéria hodnocení opět sestavena tak, aby zkontrolovaly skutečně dodržení jednotlivých kroků.

Tab. 22: Seznam kritérií pro hodnocení BCM

Oblast hodnocení	Kritérium	ANO	NE	Nedostatek - důvod
Dokumentace	Mají všechny určené osoby u sebe poslední verzi plánů?			
	Jsou uvedeny aktuální kontakty na všechny osoby v plánu?			
	Jsou všechny plány aktuální?			
	Zavedli se všechny identifikované kritické činnosti do plánů?			
	Jsou popsány všechny činnosti společnosti?			
	Jsou stanoveny veškeré hrozby?			
	Byly dodrženy cíle společnosti?			
	Jsou vytvořeny plány obnovy pro vznik konkrétního incidentu?			
	Existují všechny zápisy ze vzniku incidentu?			
	Jsou veškeré verze plánů, zápisy z incidentů archivovány?			
Příprava personálu (školení)	Má společnost přehled absolvovaných školení zaměstnanců?			
	Existuje jmenný seznam proškolených zaměstnanců?			

	Je vytvořen harmonogram pro navazující školení pro zaměstnance?			
	Je obsah školení dostatečně obsáhlý?			
Znalosti personálu	Znají všichni zaměstnanci jednotlivé kroky zavedeného BCM?			
	Jsou zaměstnanci informování o změnách v BCM?			
Testování	Existují zápisy z průběhu testovaní zavedeného BCM?			
	Je dostatečná četnost testování?			
	Existují záznamy o výsledcích a závěrech z testování?			
	Jsou zjištěné závěry aplikované a začleněné do plánů?			
Začlenění BCP do vnitřních dokumentů	Byly plány v rámci BCM začleněny do směrnic společnosti?			
	Vznikly navazující dokumenty při zavedení BCM?			
Právní předpisy	Je BCM zaveden v souladu s právními předpisy vztahující se k činnosti společnosti?			
Rozpočet	Byl dodržen finanční rozpočet?			
	Byly správně čerpány finanční prostředky z rozpočtu?			
	Jsou doloženy veškeré doklady spojené s náklady na BCM?			
	Je dodržena výše mzdových nákladů?			
	Je dodržena výše finančních nákladů na technické vybavení?			
Zjištěný nedostatek - navrhované opatření: **1.** **2.**		**Termín pro odstranění nedostatků:**		

Závěr z výsledku kontroly zavedení BCM do společnosti:			
Schválení zavedeného BCM	**ANO** **(bez výhrad)**	**ANO** **(po odstranění zjištěných nedostatků)**	**NE**
Kontrolu provedl:		**Dne:**	

Hodnocení společnosti je prováděno prostřednictvím auditu externí společností. Výsledkem checklistu je závěr z provedené kontroly, který má tři varianty schválení. O provedeném auditu se musí vypracovat zpráva, jejíž závěry je nutné zapracovat do konkrétních dokumentů.

Dílčí závěr

Poslední část diplomové práce je zaměřena na stanovení jednotlivých kritérií pro zavedení managementu kontinuity činností do společnosti. Hodnotící kritéria jsem stanovila na základě požadavků příslušné normy BS 25999. Následně jsem navrhla provedení kontroly formou checklistu. Součástí tohoto dokumentu jsou otázky směřující ke kontrole dodržení jednotlivých kroků při aplikaci normy BS 25999. Je zde uveden celý průběh hodnocení včetně kritérií, které jsem rozdělila na ty, které obsahují dokumenty, a které jsou pouze vědomostní. Je zde řešena i otázka případného návrhu opatření pro zjištěný nedostatek, popř. způsob ověření znalostí zaměstnanců. Dokument checklistu je výstupem této poslední části a v případě aplikovatelnosti v reálné společnosti by představoval pro společnost závěr z výsledku kontroly.

ZÁVĚR

Vzhledem k tomu, že je proces managementu kontinuity činností pro mnohé společnosti v ČR dosud málo známý, bylo vhodné tuto problematiku v diplomové práci podrobněji přiblížit. Je to především proto, že se společnosti v průmyslu komerční bezpečnosti stávají v dnešní době čím dál víc žádanější na trhu, a zachování kontinuity činností je z tohoto důvodu více než nutností.

První část práce je zaměřena na legislativní požadavky související právě s touto problematikou. Byl vytvořen přehled základní terminologie, aby nedocházelo k nesrovnalostem při výkladu neznámých pojmů. Součástí této kapitoly jsem vytvořila přehled veškerých norem a zákonů v souvislosti s tématem práce. Jelikož pro proces kontinuity činností existuje pouze doporučující norma BS 25999, uvedla jsem vývoj této normy a dále jsem uvedla i normy, které jsou spjaty s pojmem bezpečnosti, a tudíž pro tuto práci vhodné. Jedná se zejména o normy řady ISO 27000, které představují pro společnosti postupy v případě řízení systému bezpečnosti informací. Na tyto normy pak navazují zákony, které nepřímo souvisí s procesem zachování kontinuity činností. Je to především z toho důvodu, že výstupem je plán, který je velmi podobný krizovým a havarijním plánům.

Pro aplikaci procesu kontinuity činností do společnosti je na prvním místě seznámení se s teoretickými znalostmi, jak celý proces zachování kontinuity činností funguje, proto jsem v další části práce podrobně rozebrala normu, která je jako jediná doporučující pro tuto činnost. Jelikož výsledkem zavedeného procesu BCM je nekonečně opakující se proces, jsou v této části práce rozebrány jednotlivé fáze společně s požadovanou dokumentací.

Za stěžejní výstup práce považuji část 4, ve které v souladu se zadáním aplikuji zavedení BCM do obchodní společnosti podnikající v průmyslu komerční bezpečnosti. Pro vybranou společnost jsem zpracovala plán, který je nutné dodržet v případě, že se společnost rozhodne zavést BCM do své bezpečnostní politiky. Na základě získaných teoretických znalostí jsem představila jednotlivé fáze a s nimi spojené kroky, které musí být pro společnost závazné, aby bylo zavedení BCM účinné. Výstupem práce jsou BCP a plán obnovy, který určuje, jak se mají určení zaměstnanci zachovat v případě vzniku incidentu. Tato část rovněž zahrnuje veškeré činnosti, dokumenty, postupy a role jednotlivých osob začleněných do BCM, které jsou v případě plánování a implementace BCM potřebné.

Závěr práce je věnován stanovení kritérií pro hodnocení managementu kontinuity činností. Jednotlivá kritéria představují oblasti, které je nutné podrobit kontrole, na základě které pak dojde k celkovému hodnocení fungování BCM, zjištění nedostatků a následně jejich nápravy. Na základě požadavků normy BS 25999 jsem stanovila oblasti hodnocení, které dělím na ty, které jsou představovány zejména konkrétními dokumenty a na ty, které představují převážně vědomosti a znalosti všech osob. Výstupem této části je vytvoření checklistu, prostřednictvím kterého dojde k hodnocení dodržení všech jednotlivých kroků a cílů BCM.

Zpracování problematiky BCM bylo pro mne velkým přínosem, protože jsem si na konkrétním modelu společnosti vyzkoušela práci bezpečnostního manažera v praxi. V průběhu studia materiálů k danému tématu jsem zjistila, že je mnoho společností, které případný vznik incidentů berou na lehkou váhu a neuvědomují si všechna rizika spojená s výpadky procesů a činností, na kterých jsou závislí. Je to dáno především nezájmem investovat do bezpečnostní politiky, protože dopady hrozeb si připouští jen okrajově. V případě narušení chodu společnosti pak dochází k situaci, kdy žádný zaměstnanec neví, jak se má chovat a odstranění případného incidentu trvá mnohem déle.

Svou prací bych chtěla tuto problematiku přiblížit právě těm, kteří o ni dosud nejevili zájem a neuvědomují si, že právě otázka bezpečnosti a připravenosti na nečekané události je v současné době obrovské konkurence jeden z klíčových momentů pro upevnění dobrého postavení na trhu.

Závěrem je třeba zdůraznit, že management kontinuity činností je neustále opakující se proces, proto by mělo být vždy snahou společnosti tento proces neustále sledovat a aktualizovat vždy s ohledem na dosažení stanovených cílů společnosti.

ZÁVĚR V ANGLIČTINĚ

Since it is the business continuity management process for many companies in the Czech Republic yet little known, it was appropriate to issue the thesis in more detail closer. It is mainly because of the commercial security industry nowadays becomes increasingly more demanding in the market, and business continuity is therefore more than a necessity.

The first part focuses on the legislative requirements associated specifically with this issue. It was created overview of the basic terminology in order to avoid inconsistencies in the interpretation of terms. Part of this chapter, I created a list of all the standards and laws in relation to the topic of this work. As for the process of business continuity exists only recommendatory standard BS 25999, I introduced the development of this standard and I said and standards that are associated with the concept of security, and therefore suitable for the job. In particular, the ISO 27000 series of standards, which represent the company's procedures for information security management system. These standards are followed by laws that indirectly related to the process of business continuity. It is mainly because the output is a plan that is very similar to crisis and emergency plans.

The application process continuity in society is the first introduction to the theoretical knowledge of how the whole process of business continuity works, because I work in another part of the standard analyzed in detail, which is the only recommendation for this activity. As a result of the established process BCM is endlessly repetitive process in this part of the work focused on different stages along with the required documentation.

The fundamental output of work consists of 4, in which, in accordance with the specifications apply the BCM introduction to a company operating in the commercial security industry. For the selected company I worked up a plan to be followed in the event that the company decides to introduce BCM into its security policy. On the basis of theoretical knowledge I presented the different phases and related steps that must be binding for the company that the introduction of an effective BCM. Outcome of this work are BCP and recovery plan that specifies how to determine the employees do in the event of an incident. This section also includes all activities, documents, procedures and role of individuals included in the BCM that are in the planning and implementation of BCM needed.

The conclusion is devoted to establishing criteria for assessing business continuity management. The individual criteria are areas that need to be audited, based on that then the overall evaluation of the functioning BCM, identify deficiencies and consequently their axles. Based on the requirements of BS 25999 I set evaluation, which are divided into those that are represented mainly by specific documents and those that are mainly knowledge and understanding of all people. The output of this section is a checklist through which will review compliance of individual steps and objectives of the BCM.

Processing issues BCM has been a great help for me, because I have the specific model of job security manager tried out in practice. During the study materials on the topic, I found that there are many companies that may have arisen incidents take lightly and do not realize all the risks associated with failures of processes and activities on which they depend. It is primarily due to the lack of interest to invest in security policy, because the effects of threats, admits only marginally. In the event of disruption of then leads to a situation where no employee knows how to behave and to remove any incident takes much longer.

With my work I would like to approach this issue very people who so far showed no interest and do not realize that it was a question of safety and preparedness for unexpected events is currently a huge competition one of the keys to maintaining good reputation in the market.

Finally, it should be emphasized that business continuity management is constantly repeating the process, so it should always be the aim of this process is constantly monitored and updated always with a view to achieving the objectives of the company.

SEZNAM POUŽITÉ LITERATURY

[1] BS 25999-1. *Management kontinuity činností organizace - Část 1: Soubor zásad*. Praha: CNI: 2009. 52 s. Třídící znak 010370.

[2] ČSN ISO/IEC 27000 *Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník*. Praha: ÚNMZ, 2009. 42 s. Třídící znak 369790.

[3] ČSN ISO/IEC 27001. *Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky*. Praha: ÚNMZ, 2006. 36 s. Třídící znak 369790.

[4] ČSN ISO/IEC 17799. *Informační technologie - Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací*. 2.vyd. Praha: Český normalizační institut, 2005. 102 s. Třídící znak 369790.

[5] Risk Analysis Consultant [online]. 2012 [cit. 2013-02-15]. Dostupné z WWW: <http://www.rac.cz/rac/homepage.nsf/CZ/PAS56>.

[6] Česká republika. Zákon č. 59/2006 Sb. o prevenci závažných havárií, ve znění pozdějších předpisů. In *Sbírka zákonů*. 2006, 25, s. 59-60.

[7] HILES, Andrew. *The Definitive Handbook of Business Continuity Management*. 3. vyd. Hoboken, N. J.: Wiley, 2011, 798 s. ISBN 978-047-0670-149.

[8] Risk Analysis Consultant [online]. 2012 [cit. 2013-02-15]. Dostupné z WWW: <http://www.rac.cz/rac/homepage.nsf/CZ/RM2BCM/$FILE/Druha%20kapitola.pdf >.

[9] Česká republika. Zákon č. 455/1991 Sb. o živnostenském podnikání (živnostenský zákon). In *Sbírka zákonů*. 1991, 87, s. 455.

[10] LAUCKÝ, JUDr. Vladimír: *Řízení technologických procesů v PKB*. 2. vyd. Zlín: Univerzita Tomáše Bati, 2005. 101 s. ISBN 80-7318-329-3.

[11] LAUCKÝ, JUDr. Vladimír: Technologie komerční bezpečnosti II. Zlín: Univerzita Tomáše Bati, 2004, 122 s. ISBN 80-7318-231-9.

[12] LAUCKÝ, JUDr. Vladimír: Technologie komerční bezpečnosti I. Zlín: Univerzita Tomáše Bati, 2003, 64 s. ISBN 80-7318-119-3.

[13] Česká komora detektivních služeb [online]. 2013 [cit. 2013-02-15]. Dostupné z WWW: <http://www.ckds.cz/index.php?nid=3729&lid=CS&oid=458887>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACS	Přístupový systém
BCM	Management kontinuity činnosti organizace
BCP	Plán kontinuity činností
BIA	Analýza dopadů
BOZP	Bezpečnost a ochrana zdraví při práci
BSI	Britský normalizační institut
CCTV	Uzavřený kamerový systém
CDROM	Kompaktní disk pouze pro čtení paměti
ČR	Česká republika
ČSN-BS	Česká technická norma – Britské národní normy
ČSN-EN	Česká technická norma – Evropská norma
DRP	Plán obnovy
EPS	Elektrická požární signalizace
EZS	Elektronický zabezpečovací systém
GSM	Globální systém pro mobilní komunikaci
HW	Hardware
HZS	Hasičský záchranný sbor
ISMS	Systém řízení bezpečnosti informací
ISO/IEC	Mezinárodní norma
IT	Informační technologie
IZS	Integrovaný záchranný systém
MRSL	Minimální úroveň poskytování služeb
MTDL	Maximální přijatelná ztráta údajů
MTO	Maximální přijatelný interval výpadku

PAS	Veřejně dostupná specifikace
PC	Osobní počítač
PPH	Preventivní požární hlídka
PDCA	Demingův cyklus zlepšování
PO	Požární ochrana
PPC	Poplachové přijímací centrum
PZTS	Poplachové zabezpečovací a tísňové systémy
RPO	Cíl obnovy činnosti
RTO	Doba obnovy činnosti
SD	Secure digital
SW	Software
UPS	Nepřerušitelný zdroj energie
USB	Univerzální sériová sběrnice
ZU	Zvláštní úkoly
ZZS	Zdravotnická záchranná služba

SEZNAM OBRÁZKŮ

SEZNAM TABULEK