Projekt implementace managementu bezpečnosti informací v rámci realizace ISO 20000 ve firmě Synot ICT Services a.s.

The project of implementation of security management within the framework of ISO 20000 realization in the Synot ICT service a.s.

Bc. Lukáš Svozil

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

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

Jméno a příjmení:	**Bc. Lukáš SVOZIL**
Osobní číslo:	**A10531**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Projekt implementace managementu bezpečnosti informací v rámci realizace ISO 20000 ve firmě Synot ICT Services a.s**

Zásady pro vypracování:

1. **Proveďte literární rešerši s problematikou ISMS.**
2. **Analyzujte současný stav řízení informací a úroveň bezpečnosti procesů ve zvolené organizaci.**
3. **Navrhněte optimalizaci procesů řízení bezpečnosti informací s následnou implementací ISMS.**
4. **Proveďte diskusi nad řešením celého projektu.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **PUŽMANOVÁ, Rita. Moderní komunikační sítě od A do Z : Technologie pro datovou,hlasovou i multimediální komunikaci. 2. aktualizované vydání. Brno : Computer Press, a.s., 2006. 430 s. ISBN 80-251-1278-0.**
2. **STREBE, Matthew ; PERKINS, Charles. Firewally a proxy-servery : Praktický průvodce. Vydání první. Brno : Computer Press, a.s., 2003. 450 s. ISBN 80-7226-983-6.**
3. **HORÁK, Jaroslav. Bezpečnost malých počítačových sítí : praktické rady a návody. První vydání. Praha : Grada Publishing, a.s., 2003. 200 s. ISBN 80-247-0663-6.**
4. **NORTCUTT, Stephen, et al. Bezpečnost sítí : Velká kniha. Vydání první. Brno : CP Books, 2005. 589 s. ISBN 80-251-0697-7.**
5. **LOCKHART, Andrew. Bezpečnost sítí na maximum. Vydání první. Brno : CP Books, 2005. 276 s. ISBN 80-251-0805-8.**
6. **KABELOVÁ, Alena, et al. Velký průvodce protokoly TCP/IP a systémem DNS : 3. aktualizované a rozšířené vydání. První dotisk 3. aktualizovaného vydání. Brno : CP Books, 2005. 542 s. ISBN 80-7226-675-6.**

Vedoucí diplomové práce: **doc. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **25. února 2011**

Termín odevzdání diplomové práce: **27. května 2011**

Ve Zlíně dne 25. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce bude řešit problematiku informační bezpečnosti v organizacích poskytujících ICT služby. Řešeny budou jednotlivé možnosti přístupu k informační bezpečnosti. V závěru se práce zaměří na implementaci informační bezpečnosti v organizaci poskytující ICT služby.

Klíčová slova: bezpečnost informací, informace, ICT, bezpečnost, řízení informační bezpečnosti, proces

ABSTRACT

This diploma thesis deals with the issue of information security in companies providing ICT services. Individual possibilities of the information security will be solved. At the end of this work I will focus on implementation of the information security in the company providing ICT services.

Keywords: Information security, Information security management, information, ICT, safety, process

Na tomto místě bych rád poděkoval svému vedoucímu diplomové práce panu doc. Mgr. Romanovi Jaškovi, Ph.D. za jeho odborné rady, připomínky a konzultace. Dále bych chtěl poděkovat své rodině a přítelkyni za výraznou podporu po celou dobu během mých studií.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Bezpečnost, pojem v posledních letech používaný s rostoucí frekvencí a prioritou, slýcháme ze všech oblastí lidské činnosti a stále nachází nové pole působnosti. Ne jinak tomu je i ve sféře ICT, kde se tento termín zařadil mezi nejožehavější témata současnosti.

Skutečnost, že každá firma zpracovává, uchovává a využívá informace, na nichž závisí prosperita celé společnosti, je nám všem dobře známá. Existují však oblasti podnikání, pro které je správné zacházení s informacemi naprosto zásadní. Zcizení, nedostupnost, poškození či zneužití těchto dat může mít nemalý dopad na chod celé společnosti. Ztráta dobrého jména, oslabení pozice na trhu, finanční ztráta, nebo úplný zánik podnikatelského subjektu jsou důsledky špatného zacházení s informacemi. O to více je zarážející, že řízení bezpečnosti informací byla ve spoustě organizací, a někde stále je, opomíjena. V posledních letech však nastává obrat ve vnímání této problematiky. Vrcholný management si začíná uvědomovat význam této oblasti.

Diplomová práce řeší problematiku bezpečnosti informací v organizacích, které působí v oblasti poskytování ICT služeb. Na úvod zjistíme, z jakého důvodu je nezbytné věnovat se řízení informační bezpečnosti. Dále přistoupíme k definování pojmu informace, přiblížíme si její životní cyklus a proberme metody vedoucí k zajištění její ochrany.

V následující kapitole budou přiblíženy jednotlivé aktivity, kterými je nutné se zabývat při zavádění procesu řízení informační bezpečnosti.

Praktická část se zabývá problematikou zavádění managementu informační bezpečnosti v rámci implementace normy ISO/IEC 20000.

I. TEORETICKÁ ČÁST

1 BEZPEČNOST V ICT

Současná integrace ICT do našeho života přináší spolu s výhodami, také jistou závislost na službách poskytovaných informačními technologiemi. Dlouhodobá nedostupnost způsobuje problémy nejen v osobním životě, ale především na straně komerčních subjektů. Zejména závislost ve smyslu obchodního vztahu mezi společnostmi, zavádí požadavek na úroveň kvality smluvené služby. Nedostupnost námi poskytované služby je důsledkem bezpečnostního incidentu. Bezpečnostní problematika se vyvíjí stejně rychle jako samotné ICT. Incidenty se stávají běžnou součástí našeho podnikání. Nejedná se o nahodilé jevy, jako tomu mohlo být před deseti a více lety, kdy infrastruktury našich systémů byly mnohonásobně menší, jednodušší a spousta z nich neměla přístup do internetu. Hlavním požadavkem bylo převážně vybudování sítě a zajistit její funkční chod. Bezpečnost nebyla jen časovou či finanční překážkou, ale mnohdy i termínem, který si vedení společností nespojovalo právě s oblastí ICT.

Současný trend a inovativní pohled na ICT vyžaduje pravý opak, což si začíná uvědomovat i vrcholný management. Informační bezpečnost se stává jedním ze stěžejních bodů, ne-li přímo základním pilířem pro vybudování kvalitních ICT struktur.

1.1 Je nutné zabývat se bezpečností informací?

Jestliže si vrcholný management klade otázku, zdali se má zabývat řízením informačních rizik, odpověď je jednoznačně ANO. Každý podnikatelský subjekt vlastní majetek nemalých hodnot. Jedná se o nemovitosti, ICT zařízení, vozový park, atd., o něž se adekvátně stará a chrání je. Stejným aktivem konkrétní finanční hodnoty je informace, na níž stojí nebo padá naše podnikání. Každá organizace, působící v různorodých oblastech, zpracovává, shromažďuje a využívá data, jež jsou pro její činnost nepostradatelné. Ve většině případů právě nedostupnost informací má na podnik nejvíce devastující dopad.

Informační bezpečnost je jasným znakem jakosti služby a má zásadní význam zejména pro společnosti, které informace prodávají jakou svůj hlavní produkt. Z těchto vět logicky vyplývá, že IS je třeba chránit, protože se jedná nejen o ochranu investic, neboť informace je zboží, ale také k tomu nutí právní nebo morální pravidla, činnost konkurence a zákonné úpravy pro ochranu dat [16]. Podstatný je také fakt, že informace musejí být řízeny a není důležité, zda organizace má 50, 500, nebo 5000 zaměstnanců.

1.2 Vysvětlení pojmů

Z důvodu porozumění textu a pochopení dané problematiky si úvodem objasníme pojmy, které se budou v diplomové práci objevovat.

- IS – Informační systém
- ICT - Původně používaná zkratka informačních technologií IT (z anglického výrazu Information Technologies) se rozrostla na dnešní tvar ICT. Termín byl doplněn o slovíčko komunikace (Information and Communication Technologies). ICT je pojem užívaný přeneseně, bavíme-li se o hardwaru, softwaru, nebo o dalších oblastech týkajících se informačních technologií.
- Bezpečnostní politika – Základní dokument, ve kterém jsou shrnuty zásady a požadavky společnosti na řízení bezpečnosti informací.
- Bezpečnostní incident – Událost, při které dochází, nebo která může vést k narušení dostupnosti, integrity a důvěrnosti informací.
- Aktiva – Vše co má pro společnost hodnotu. Nejedná se jen o fyzický majetek, ale také o informace, jimiž podnik disponuje.

1.3 Bezpečnost informací

Obecný pojem bezpečnost můžeme definovat jako žádoucí stav, při kterém jsou veškerá rizika snížena na přijatelnou mez. Pokud termín zasadíme do oblasti ICT, tak bezpečností máme na mysli ochranu informačních systémů a informací, které jsou zde uloženy, zpracovávány a transportovány. Mezinárodní normalizační organizace ISO ve svých normách definuje bezpečnost jako zajištěnost proti nebezpečím, minimalizaci rizik a jako komplex administrativních, logických, technických a fyzických opatření pro prevenci, detekci a opravu nesprávného použití IS. Bezpečným nazýváme IS v případě, jestliže je zajištěn fyzicky, administrativně, logicky i technicky [16].

Každá z výše zmíněných definic se dívá na problematiku z jiné stránky. Můžeme říci, že těmito tvrzeními chodíme kolem horké kaše, kterou v tomto případě je bezpečnost informace. Dříve publikované definice nám nastiňují možnosti, jak přistupovat k ochraně dat a jaké procesy jsou k jejímu zajištění nutné. Nejdůležitější myšlenka ovšem ještě nezazněla. Bavíme-li se o bezpečnosti informací, první co nás napadne, musí být zajištění

proti narušení dostupnosti, integrity a důvěrnosti informace. Pouze dostupná informace, u níž je zachována integrita a důvěrnost je zabezpečená.

V další podkapitole se dozvíme, jaké hrozby ohrožují naše informační systémy a v nich se nacházející, pro nás tolik důležité informace.

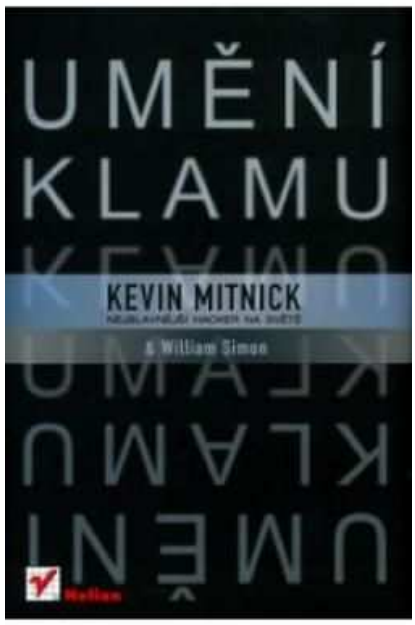
1.4 IT Hrozby

Hrozeb, které mohou působit na náš informační systém, jsou obrovské množství. Rizika, určující s jakou pravděpodobností daná hrozba skutečně nastane, jsou odlišná u každé organizace. Potenciální nebezpečí se liší nejen oblastí působnosti dané organizace, ale také podle geografické polohy. Zajímat se budeme jen o hrozby, které se týkají naší organizace a řízení rizik k těmto hrozbám má pro nás význam.

Obecně lze nebezpečí rozdělit na hrozby přírodního původu (povodně, hurikány, zemětřesení, sopečná činnost atd.), technické selhání HW a působení člověka. Na první pohled to může znít paradoxně, ale nejvíce bezpečnostních incidentů mají na starosti právě vlastní zaměstnanci. Pokud je cílený útok vedený z vnějšího prostředí organizace, jedná se převážně o hackery, špionáž, konkurenční boj. Zaměstnanci z vlastních řad bezpečnostní incident mohou způsobit úmyslně nebo neúmyslně. Neúmyslné počínání vede z nedbalosti, neopatrnosti, či nízké odborné způsobilosti pracovníka. Úmyslné poškození organizace vedoucí z řad vlastních zaměstnanců bývá motivováno např. křivdou vůči společnosti, dostáním výpovědi, podplácením, vydíráním ze třetí strany. Udává se, že z celkového počtu bezpečnostních incidentů jich způsobí vlastní zaměstnanci až 80%.

Z výše uvedených řádků plyne, že bezpečnost informací je nejen technickou záležitostí, ale že výrazná část připadá právě na lidský faktor. I přes zabezpečení na vysoké technické úrovni je zde stále člověk, u kterého nemůžeme garantovat jeho chování a rizikům z toho plynoucích nemůžeme nikdy zcela zabránit. Sociální inženýrství je velmi zajímavý obor zabývající se právě získáváním informací od lidí, zneužívající nepozornost, únavu, emoce, zvědavost či naivitu obelhané osoby. Sociotechniky jsou metody vedoucí k přesvědčování a ovlivňování lidí, přičemž cílem je vyzvědět od nich potřebnou informaci, nebo je přesvědčit k provedení určitých činů. Útočník se vydává za někoho jiného, má nastudované informace o organizaci, o osobách zde pracujících, např. ze sociálních sítí, z internetových stránek. Tyto informace umí útočníci použít tak efektivně a přesvědčivě, že jsou schopni z osob vyzvědět další doplňkové informace, či přímo cílené informace. Čím je organizace

větší, tím snadněji se sociotechnikovi povede vyzvědět tížená data. Lidé se v takové společnosti vzájemně většinou ani neznají. Zdárný příklad je, pokud řadovému pracovníkovi zavolá útočník a představí se jako IT specialista starající se o jeho PC. S vhodnými argumenty, kterými může být zlepšení poskytování služeb, či jakákoliv úprava připadající oběti velmi výhodná a užitečná prozradí klidně i své přístupové hesla, systémy do kterých má přístup atd.



Obrázek 1. Sociální inženýrství[29]

Problematiku řízení hrozeb podrobněji probereme v kapitole Analýza hrozeb.

K vysvětlení dalších významných částí problematiky informační bezpečnosti se dostaneme dále v práci. Nejprve definujeme informaci, její životní cyklus a charakteristické vlastnosti a druhy přístupů k jejímu zabezpečení.

2 INFORMACE

Informace je termín používaný v mnoha oblastech, avšak vyskytující se v odlišných formách. Může se nacházet v podobě verbální, jako mluvené slovo, podobě fyzické, např. na papíře, nebo v podobě elektronické, ve formě dat uložených v IS. I přes tyto odlišnosti vykazují informace stejné, charakteristické vlastnosti. První je fakt, že užitečná je pouze ta informace, která snižuje míru neurčitosti, zvyšuje míru vědění, jinými slovy je pro nás přínosná. De-facto každá informace snižuje míru nevědění, ovšem ne každá je pro nás přínosná. My se zaměřujeme pouze na takové, které jsou pro nás využitelné například ve vědecké či podnikatelské činnosti. Přínosná informace má určitou hodnotu a stává se pro vlastníka aktivem. Záleží také samozřejmě na její aktuálnosti. Každá informace je aktuální a užitečná pouze po určitý časový úsek, který je v jednotlivých případech odlišný. Z tohoto vyplývá, že informace prochází jistým životním cyklem.

2.1 Životní cyklus informace

Na obrázku č. 2 je popsán životní cyklus informace IL (information lifecycle). Informace vznikne v určitém bodě na časové ose, po které se pohybuje až po svůj zánik. V tomto časovém období prochází různými změnami. Jsou modifikovány tak, aby si udržely, nebo zvýšili svou užitečnost, jsou transportovány k jiným uživatelům, nebo jsou určeny pouze ke čtení a jejich podoba zůstává neměnná. Přestože variant je spousta, je zde jeden stěžejní, společný bod. Mezi těmito aktivitami musejí být informace někde uloženy.

Obrázek 2. Životní cyklus informace[17]

Jelikož se zabýváme tématikou ochrany informací, budeme se na životní cyklus informací dívat především bezpečnostní optikou. Z toho vyplývají povinnosti jak s daty zacházet od jejich vzniku až po jejich zničení. Jak je znázorněno na obrázku č. 2, informace je potřeba chránit v úložišti, při přenosu a během uživatelské manipulace. Tyto aktivity provádíme za účelem zajištění a zachování jejich dostupnosti, důvěryhodnosti a integrity. Stejně důležitý je také proces likvidace informací, kdy nedohlížíme na dodržení tří výše zmíněných bodů, naopak se snažíme, aby již s daty nebylo možné jakkoliv nakládat. Jejich zneužitím by mohlo dojít ke způsobení újmy bývalému vlastníkovi. Prozrazení výrobního know-how, obchodních informací, získání kontaktů na zákazníky do rukou konkurence. To je jen malý zlomek možných scénářů.

2.1.1 Informace v úložišti

Je třeba mít na mysli, že se může jednat o jakýkoliv druh média. HDD, DVD, CD, flash disk a také papír jsou pro data úložištěm. Integrita, dostupnost a důvěrnost v tomto životním cyklu bývá zpravidla zajištěna fyzickou, logickou a personální ochranou. Data je potřeba zálohovat a archivovat na jiné fyzické médium nejlépe umístěné v geografické lokalitě vzdálené od originálních dat. Vzdálený i fyzický přístup je potřeba řídit na úrovni personální bezpečnosti udělením práv a oprávnění k těmto činnostem pouze vybraným osobám.

2.1.2 Informace během přenosu

IS si v rámci komunikace vyměňují informace. Může se jednat o spojení v rámci vnitřní sítě (LAN), ale také skrze veřejné sítě (WAN, MAN) v případě že každé zařízení se nachází v jiném autonomním systému. Z těchto důvodu je nutné linku, po které jsou data přenášena, šifrovat, obzvláště když se jedná o přenos dat přes veřejnou síť, kterou je internet. Dále je vhodné jednotlivé zprávy číslovat, aby bylo zřejmé, zda dorazily ve správném pořadí nebo zda se někdo nepokusil o tzv. replay attack. Jako ochranu před nežádoucí modifikací je možné data podepsat a tím podvrženou nebo pozměněnou zprávu snadno odhalit.[17]

2.1.3 Likvidace informace

Tak jako je nezbytné dbát na bezpečnost informací během celého životního cyklu dat, tak stejně důležité je zaměřit se na likvidaci těchto informací. Tato poslední část cyklu, je stále většinou společností ignorována. Přitom se jedná o důležitou součást informační

bezpečnosti. Přenecháním PC jinému uživateli v rámci podniku můžeme poskytnout informace osobě, jež k tomuto druhu dat nemá mít přístup. Ve spoustě firem se staré PC, notebooky a jiné zařízení po nahrazení modernější technikou vyřadí z provozu a nikdo se nezajímá, zda neobsahují důvěrné informace. Zařízení končí většinou ve skladech a je možno z něj získat velké množství dat, které při zneužití, např. konkurencí, mohou způsobit firmě nemalou škodu. Zcizení mohou způsobit sami zaměstnanci, od kterých, jak se později dozvíme, hrozí převážná míra rizika. Případný zásah do bezpečnosti dat v průběhu jejich životního cyklu bude, za předpokladu správného řízení informační bezpečnosti, s největší pravděpodobností odhalen. Kdo ale bude mít přehled, zda se na vyřazené PC stanici nachází citlivé informace, či zda si někdo jejich kopii odnesl domů na přenosném médiu. Jistě bude snazší odhalit narušení integrity, dostupnosti, či důvěrnosti dat v průběhu jejich životnosti, než odhalení zneužití informací, kterým již nikdo žádnou pozornost nevěnuje.

Největším vynaloženým úsilím bývá zpravidla zformátování disků. Získat data z takového disku dnes není žádný velký problém. Na Internetu je množství programů, které nám takovou službu poskytnou. Nyní si představíme několik možností jak data bezpečně likvidovat.

2.1.3.1 Fyzická likvidace

Firmy by měly přijmout zásadu, že v okamžiku, kdy jakýkoliv nosič informací definitivně opouští prostory jejich firmy, tak musí být fyzicky zlikvidován nebo data na něm uložená, musí být bezpečným způsobem odstraněna. S likvidací optických medií a disket firmy obvykle nemívají problém a proces likvidace zapracovaly do svých interních instrukcí, neboť je v celku prostý. Takové médium stačí vhodit do skartovačky nebo zlomit. S HDD je to bohužel horší, ale i zde existují jednoduchá řešení. Pokud nechcete likvidaci provádět sami, tak na trhu je dost firem, které vaše média za úplatu rádi zlikvidují, mnohdy i ekologicky. Taková likvidace pak spočívá v rozebrání HDD na jednotlivé díly, sešrotování a roztavení. Pravda, některé z těchto firem se s nějakým rozebíráním nezdržují a na drcení HDD používají několika tunový skartovací stroj a vzniklou drť pak roztaví v peci a vydají o celém procesu likvidace, kterému může přihlížet i zákazník, certifikát.[17]

2.1.3.2 Přepsání náhodnými daty

Klasické zformátování disku obvykle není dostatečné, jelikož existují možnosti, jak tyto soubory obnovit. Windows například pouze přepisují hlavičku souboru a označí příslušné místo jako volné. Nabízí se nám možnost celý disk přepsat náhodnými daty. V Internetu lze najít programy, které přepíší disk náhodnými soubory. Původně bylo třeba zmíněné přepsání provádět několikrát a přitom jedno přepsání trvalo několik hodin. Gutmannova metoda vyžaduje 35 násobný přepis. Ten mohl trvat i několik dní, což mnoho organizací odrazovalo. Nyní NIST (The National Institute of Standards and Technology) prohlásil, že většinu současných HDD stačí přepsat pouze jednou. Toto tvrzení bylo nezávisle potvrzeno i několika dalšími experty [17].

2.1.3.3 Demagnetizace

Kromě fyzické likvidace médií nebo bezpečného přepsání obsahu náhodnými daty je možné použít i demagnetizátor (degausser). Jedná se o nejrychlejší metodu, jak data z HDD spolehlivě odstranit. Je třeba si však uvědomit, že HDD se poté stává prakticky nepoužitelným, protože kromě dat dojde i ke zničení informací, které byly na disk zapsány v továrně při nízko-úrovňovém formátování.[17]

2.2 Požadavky na informaci

2.2.1 Dostupnost

Narušení dostupnosti mohou způsobit různé druhy incidentů, jako jsou porucha HW, OS, aplikace, problém v komunikační síti, fyzický útok na systém atd. Dostupnost systémů udáváme v procentech. Slouží nám jako měrná jednotka k měření funkčnosti systému. Touto jednotkou poskytovatel služby deklaruje schopnost dodržet dostupnost služby. Pokud nedodrží SLA má to pro něj nejen jednorázový finanční dopad, ale také možný odchod klientů ke konkurenci.

Ač je populární uvádět dostupnost systému v % za rok, je mnohem přesnější a praktičtější uvádět RTO (Recovery Time Objective) a RPO (Recovery Point Objective).[19]

- RTO vyjadřuje, za jak dlouho po výpadku musí být systém funkční, resp. jak dlouhý výpadek může být tolerován. Pro RTO rovno nule by to znamenalo vybudovat zcela redundantní infrastrukturu.[19]

- RPO vyjadřuje, kolik práce resp. jaké množství dat může být ztraceno. Jde o to, že záloha je dejme tomu např. naplánována na 03:00 a v 09:00 dojde k havárii diskového pole. Změněny, které byly provedeny mezi 03:00 a 09:00 jsou tedy nenávratně ztraceny.[19]

Dobu nedostupnosti (RTO) a ztrátu dat (RPO) je třeba od sebe odlišovat, když se provádí business impact analýza, od které se odvíjí návrh celé architektury řešení. Častou chybou je, že se uvažuje jen o RTO a na RPO se zcela zapomíná.[19]

Obrázek 3. Dostupnost[19]

Z tohoto důvodu je nutné vybudovat kvalitní a odolnou infrastrukturu. Důležitá je samozřejmě fyzická a personální bezpečnost. Při budování systémů je velmi důležité brát v potaz poruchu jednotlivých technických zařízení a komunikačních tras. Jestliže jsme vázáni SLA vůči klientovi, je nutné být na takové výpadky připraven. Zajištění redundance hraničních routerů, FW, komunikačních cest, aktivních prvků, serverů by mělo být samozřejmostí. Pokud některé ze zařízení přestane fungovat, provoz bude překlopen na záložní trasu.

2.2.2 Důvěrnost

Důvěrností máme na mysli poskytnutí přístupu k informaci pouze oprávněné osobě. V praxi, zejména ve větších organizacích čítající stovky zaměstnanců, není snadné bez řízení oprávnění přístupu k datům poskytovat tyto privilegia. Společnost pracuje s daty

různé úrovně důležitosti a každý pracovník má mít přístup pouze k těm informacím, které potřebuje ke své pracovní činnosti. Je nutné definovat klasifikační skupiny a přiřadit k nim data dle důležitosti. Skupiny musejí být přehledné a srozumitelné tak, aby přiřazení informace do určité skupiny bylo jednoznačné.

Obrázek 4. Důvěrnost[18]

Státní sektor používá následující klasifikační schémata:

- Přísně tajné (Top Secret)
- Tajné (Secret)
- Důvěrné (Confidential)
- Citlivé, ale neklasifikované (Sensitive, but unclassified)
- Neklasifikované (Unclassified)

Klasifikační schéma v soukromém sektoru může vypadat následovně:

- Důvěrná data
- Citlivá data
- Interní data
- Veřejná data

Je zřejmé, že pro zajištění důvěrnosti je nezbytné implementovat vhodná opatření na úrovni fyzické, logické a organizační bezpečnosti, např. že média musí být uložena pod zámkem a stejně tak i dokumenty nesmí být ponechány po odchodu z pracoviště volně na stole, ale musí být uzamčeny. Jedná se o tzv. zásadu prázdného stolu (clear desk policy). Dále také, že přísně důvěrné informace v elektronické podobě musí být šifrovány. Další obecnou zásadou bez ohledu na klasifikační stupeň by mělo být, že na dokumentu bude vždy uveden jeho autor, datum vytvoření a na každé straně bude uvedeno číslo stránky a celkový počet stran[18].

2.2.3 Integrita

Zachování správné a úplné hodnoty informace nazýváme integrita. K narušení integrity může dojít úmyslně, nebo neúmyslně. Neúmyslné narušení původního stavu dat má na svědomí technická závada. Úmyslnou nežádoucí modifikaci dat má na svědomí cílený útok se záměrem poškodit hodnotu informace. V obou případech je velmi důležité včasné rozpoznání narušení integrity, což není vůbec snadné. Můžete namítnout, že prevencí bude zálohování dat a máte určitě pravdu. Ovšem narážíme opět na problém vystopování okamžiku, ve kterém došlo ke znehodnocení informace, tak abychom mohli použít poslední správnou záloh. K identifikaci hledaného časového okamžiku nám mohou pomoci logy, avšak monitoring je nutno provádět pravidelně, jinak nás čeká nelehký úkol, pokud vůbec narušení integrity objevíme.

Obrázek 5. Integrita[30]

2.3 Druhy přístupů k informační bezpečnosti

Zajištění dostupnosti, integrity a důvěrností informací je proces složený z jednotlivých aktivit. Důležité je analyzovat vše co se podílí, či má vliv, na informační bezpečnost. V první řadě je třeba definovat aktiva. Patří zde samozřejmě data, jež jsou uložena na HW či jiných médiích, na HW běží jistý SW, komunikace probíhá po síti. Všechna tato zařízení se nachází v objektu a spravují je lidé. Zjištěná aktiva jsou:

- HW
- SW
- Data
- Síť
- Objekt
- Lidské zdroje
- Image společnosti

Všechny tyto aktiva jsou součástí informační bezpečnosti, tudíž je třeba je chránit. Ochrana těchto hodnot bude požadovat rozdílné bezpečnostní metody.

2.3.1 Fyzická bezpečnost

Jak již z názvu vyplývá, jedná se o zajištění fyzické bezpečnosti, kterou rozumíme zaopatření celého objektu a v něm se nacházejících lidí a techniky. Hlavní hrozby v této oblasti jsou:

- Fyzický útok
- Přírodní katastrofa

Fyzický atak přichází nejen od útočníků z vnějšího prostředí, ale také z řad vlastních zaměstnanců. Patří sem fyzická ostraha, režimová opatření, zabezpečení objektu prvky technické ochrany (EZS, CCTV, ACS).

Přírodní katastrofy se liší podle geografické polohy. Odlišné hrozby budou na ostrově v Tichém oceáně, jiné v povodí Vltavy a na Antarktidě. V naší geografické poloze se snažíme snížit rizika plynoucí ze strany ohně, vody a větru.

2.3.2 Personální bezpečnost

Průzkumy uvádí, že téměř až 80% všech bezpečnostních incidentů zapříčiní interní zaměstnanci. Zprvu se to může zdát divné, ale opak je pravdou. Tito lidé přichází každodenně do styku s informacemi různých kvalifikačních stupňů a tudíž je na místě vnímat rizika vznikající v této úrovni. Zaměstnanci mají mnohem více informací a možností, než kterýkoliv útočník pocházející zvenčí. Může jít o neúmyslně vzniklý incident, ale mnohdy se jedná o úmyslné počínání. Nespokojený pracovník, který si chce vyřídit účty s kolegy či vedoucím, může zneužít svého přístupu k jistým informacím. Propuštěný, ale i dobrovolně odcházející člověk může zcizit data, které se mu budou přínosem v dalším povolání, či prostá krádež informací pro třetí osobu. Ať už bude mít bezpečností incident námi přednesený scénář, či zcela jiný, jedna věc bude vždy jistá. Nastane bezpečnostní incident znamenající pro organizaci finanční ztrátu.

Jak se proti tomuto druhu hrozeb bránit? Zavedení procesů a směrnic, dle kterých budou zaměstnanci postupovat, nám pomůže jako rámec, který stanoví povinnosti, možnosti a postupy v předem definovaných situacích. Osobnost a schopnosti lidí nejsou bezvýznamné, ovšem my si musíme umět každého člověka odborně vychovat dle potřeb organizace. Chybné je, pokud tento proces zúžíme na pouhé přijetí/propuštění zaměstnance. Vztah zaměstnavatel – zaměstnanec by se měl skládat přinejmenším z těchto aktivit:

- Výběr zaměstnance
- Výchova zaměstnance
- Školení zaměstnance
- Motivace zaměstnance
- Ukončení pracovního poměru zaměstnance

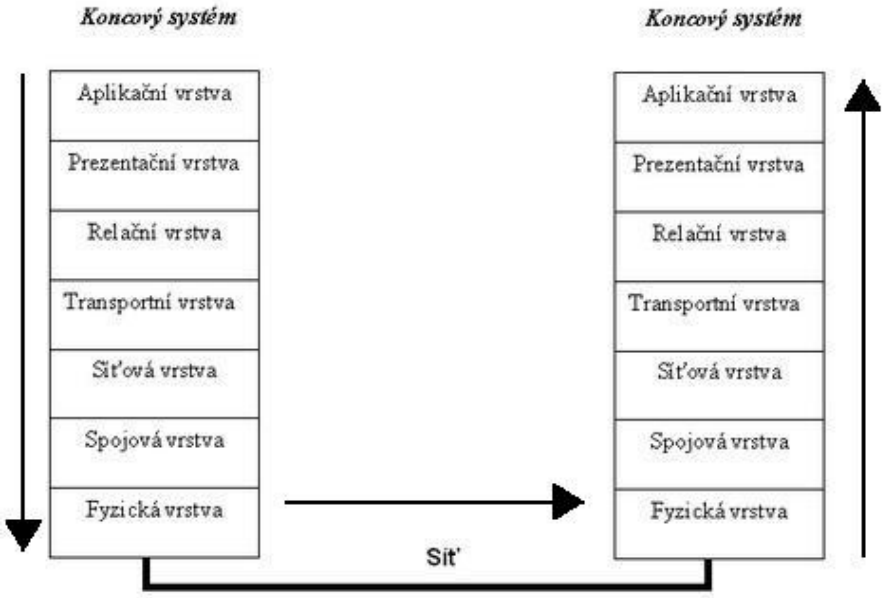
Celý systém je tak silný, jak je silný jeho nejslabší článek. Pořízení technologií za miliony nám nezaručí jistý úspěch. Tuto koupi můžeme považovat za zbytečnou, pokud systémy obsluhují nekvalifikovaní pracovníci.

2.3.3 Komunikační bezpečnost

Komunikační bezpečnosti byla zmíněna již v kapitole Životní cyklus informace. Jedná se o tutéž problematiku. Nyní si ji po obecném seznámení, ve výše zmíněné kapitole, rozvedeme podrobněji.

Dozvěděli jsme se, že komunikační bezpečnost zajišťuje bezpečný přenos dat v lokálních i veřejných sítích architektury TCP/IP. Našim cílem je zajištění bezpečného přenosu dat.

K názorné představě nám poslouží vrstvové uspořádání architektury OSI.



Obrázek 6. Model OSI [21]

Zabezpečením vybraných vrstev modelu OSI dosáhneme ochrany přenosu dat. Model OSI se skládá z těchto vrstev:

- Fyzická vrstva
- Spojová vrstva
- Síťová vrstva
- Transportní vrstva
- Relační vrstva
- Prezentační vrstva
- Aplikační vrstva

Zabezpečením fyzické vrstvy máme na mysli ochranu proti přerušení vodičů, odposlechu a rušení signálu. Zabýváme se tedy technickými hrozbami.

Spojová vrstva zajišťuje přenos datových rámců. Provádí kontrolní součty, kterými zjišťuje případné technické selhání. Dále provádí ochranu proti úmyslným útokům. Jedná se například o protokol PPP (Point-to-Point Protocol), který zapouzdřuje rámce přenosových technologií za účelem zabezpečení autenticity a důvěrnosti spojení[32].

Na úrovni síťové vrstvy můžeme implementovat velmi významné bezpečnostní opatření. Tímto opatřením je firewall, který chrání přístup do vnitřní sítě před okolním světem. Na FW máme možnost nastavit spoustu pravidel, která ochrání naši interní síť. Může nám také sloužit jako rozhraní ve vnitřní sítě, kde máme podsítě. Některé jsou určeny pro uživatele, jiné pro systémy. Na FW můžeme nastavit pravidla pro přístup koncových uživatelů do jednotlivých systémů.

Nejznámějším protokolem pro zajištění bezpečného přenosu dat je protokol SSL (Secure Socket Layer). Zajišťuje nám ochranu na transportní vrstvě. Zaměřuje se na zabezpečení aplikačních protokolů pomocí komunikační architektury klient-server.

2.3.4 Logická bezpečnost

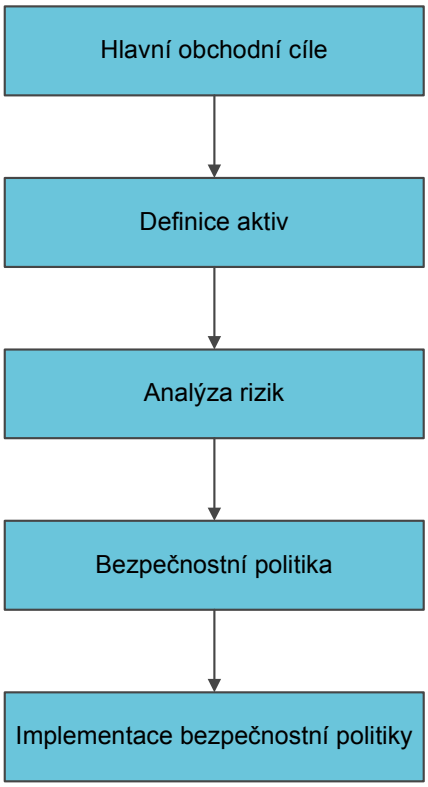
Operační systém, databáze, aplikace, obecně můžeme říci software je potřebný ke zpracování dat v elektronické podobě. Přístup k systémům je potřeba řídit, tímto se zabývá právě oblast logické bezpečnosti.

2.3.5 Organizační bezpečnost

Občas je prezentována také jako administrativní bezpečnost. Vedení společnosti, nebo osoby, jímž byla udělena odpovědnost za oblast ochrany informací, mají na starosti organizační bezpečnost. Dalo by se říci, že se jedná o první štaci, kterou začínáme nekonečný koloběh řízení bezpečnosti informací. V tomto úseku je potřeba definovat bezpečnostní politiku organizace. Z té budeme vycházet nejen při stanovování směrnic, z níž budou jasně definovány povinnosti zaměstnanců v otázce ochrany informací. V souhrnu tedy můžeme říci, že organizační bezpečnost se zabývá řízením bezpečnosti informací, stanovením odpovědnosti jednotlivých osob. Z těchto řádků může plynout trochu zkreslená představa, že se jedná pouze o jednorázovou činnost. Opak je však pravdou. Bezpečnostní politika musí být aktuální a odrážet potřeby společnosti a trhu. Dochází také k fluktuaci zaměstnanců, předelegování odpovědnosti atd. Z toho je zřejmé, že tato oblast, stejně jako ostatní, je neustávajícím procesem. Pokud tomu tak není, nemůžeme mluvit o řízení ochrany informací.

3 ZAVEDENÍ ŘÍZENÍ INFORMAČNÍ BEZPEČNOSTI

Zopakujme si velmi důležitou myšlenku, která zazněla již výše v textu. K zavedení řízení bezpečnosti informací je potřeba mít plnou podporu vedení organizace. V ideálním případě vrcholný management společnosti je sám přesvědčen o nutnosti implementace informační bezpečnosti, která se řeší na základě jeho nařízení.



Obrázek 7. Proces implementace

Informační bezpečnosti

Spolupráce vedení podniku je potřebná samozřejmě i dále během budování a řízení Security Managementu. Hned na začátku je potřeba, aby byly definovány hlavní obchodní cíle organizace. Poté můžeme přejít k definování aktiv, které je nutné chránit. Analýza rizik je posledním krokem, po němž může být sestavena bezpečnostní politika organizace. Jedná se o zastřešující dokument celé informační bezpečnosti, pod nímž jsou ostatní interní dokumenty, kterými jsou směrnice, pracovní pokyny, nařízení atd. Další fází je implementace bezpečnostní politiky do praxe. Záměrně říkám další, nikoliv poslední, jelikož řízení informační bezpečnosti nekončí implementováním BP, či auditem. Tento

proces musí stále pokračovat, aktualizovat a neustále reagovat na impulsy přicházející jak z vnějšího, tak vnitřního prostředí firmy.

Audit na obr. 7 není uveden záměrně, jelikož není nezbytně nutnou částí. Většina firem však v dnešní době audit podstupují, jelikož je zárukou kvality poskytovaných služeb, lépe mohou obstát v konkurenčním boji a zvyšuje se jejich postavení na trhu. Mnohdy je právě získání certifikace hlavním důvodem k zavedení informační bezpečnosti.

K dispozici jsou standardy, které jsou lety praxe odzkoušené. Možnost je samozřejmě vytvoření vlastních praktik, to se však nedoporučuje, jelikož hrozí riziko opomenutí důležitých oblastí a především vymýšlet již vymyšlené a praxí prověřené metody je ztráta času. Jistě není nutno připomínat známé rčení, že čas jsou peníze. Efektivnější bude věnování času a energie k zavedení jednoho z používaných standardů.

3.1 Normy

Pro následný výběr strategie nasazení bezpečnostních pravidel máme několik možností. Tou nejméně vhodnou alternativou je pokus o vytvoření vlastního standardu. Je zde riziko, že tvůrci nových pravidel nebudou natolik zkušení, aby zahrnuli všechny důležité oblasti a správně je zpracovali.

3.1.1 BS 17799-2

Britský standard pro informační bezpečnost, BS 7799, uvedly v roce 1995 v život přední ekonomické organizace. Vznikl tak efektivní nástroj k hodnocení systémů řízení informační bezpečnosti (ISMS), který se rychle rozšířil po celém světě a dnes je k dostání ve více než 11 jazycích. V roce 1998 byla norma přizpůsobena požadavkům nových trendů a v roce 2000 schválena jako standard ISO. V roce 2005 byl uveden v platnost nejnovější standard, zahrnující ty nejaktuálnější poznatky z oblasti komplexní informační bezpečnosti - ISO 27001, který je postaven na základech BS 7799/ISO 17799. [1]

Norma sestává ze dvou částí: Příručka k řízení informační bezpečnosti a Specifikace pro ISMS. V současné době je plně nahrazena normou ISO/IEC 27001 ISMS. [2]

3.1.2 ISO/IEC 27001 ISMS

Tato norma je známa také pod zkratkou ISMS (Information Security Management Systém). Jak bylo zmíněno v předešlém textu, norma ISO 27001 navazuje na standard BS 17799-2.

ISO/IEC 27001 si klade za cíl poskytnout doporučení, jak aplikovat ISO/IEC 27002 v rámci procesu ustavení, provozu, údržby a zlepšování systému řízení bezpečnosti informací (ISMS) v organizaci v souladu se systémy řízení kvality nebo bezpečnosti prostředí. [28]

Norma popisuje vhodný systém řízení, strukturu a procesy pro řízení bezpečnosti informací podle opatření definovaných v ISO/IEC 27002. Organizace mohou na základě hodnocení rizik z ISO/IEC 27002 vybrat přesně ta opatření, která jsou aplikovatelná v jejich prostředí. Z tohoto důvodu jsou také hlavní části ISO/IEC 27002 uvedeny také v příloze ISO/IEC 27001. Podle ISO/IEC 27001 mohou organizace definovat rozsah certifikovaného systému. Správná definice ISMS je kritickým krokem při jeho zavádění v organizaci. Pokud je systém řízení bezpečnosti informací zaveden pouze v určité části organizace, vydaný certifikát je platný právě pro tuto část nikoli pro celou organizaci. [28]

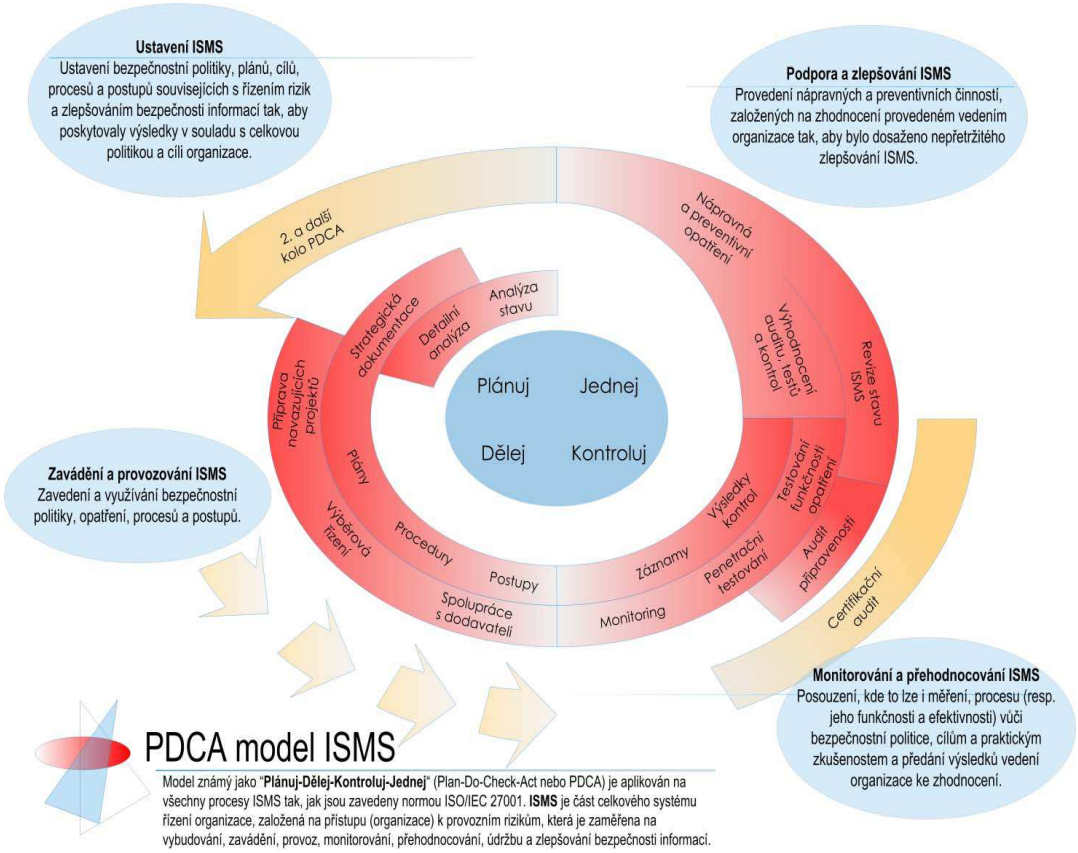
Mezi hlavní aspekty této části normy, které pokrývá, patří:

- harmonizace s normami pro další systémy řízení
- kontinuální zajištění procesu zlepšování řízení bezpečnosti informací
- celopodnikové řízení
- zajištění souladu s právními a regulatorními předpisy
- záruky za bezpečnost informací
- zavedení principů OECD pro oblast bezpečnosti informačních systémů a sítí [28]

ISMS zavádí procesní přístup k řízení podle Demingova modelu PDCA. PDCA je zkratkou z anglického slovního spojení Plan-Do-Check-Act, neboli Plánuj- Dělej – Kontroluj – Jednej. Jedná se o přístup k řízení procesů zaměřený na kontinuální zlepšování. Zaručuje tedy, že pokud je bezpečnost řízena tímto modelem, nejedná se o jednorázovou aktivitu, ale o kontinuální, stále se zdokonalující proces. Standard striktně definuje postup implementace ISMS a definuje cíle, které musejí být splněny. Čtyři kroky dle Demingova modelu PDCA jsou:

- Plánuj (Plan)
- Dělej (Do)
- Kontroluj (Check)

- Jednej (Act)



Obrázek 8. PDCA [28]

3.1.2.1 Plánuj

Cílem prvního kroku Plánuj je zanalyzovat současný stav procesu řízení bezpečnosti informací, zjistit problémy, slabiny procesů. Je nutné shromáždit veškeré možné informace o řízení rizik. Budou nás zajímat všechny procesy a činnosti prováděné v rámci ISMS, stejně jako implementované opatření.

Pokud tomu tak ještě není, je třeba definovat bezpečnostní politiku organizace, dále jednotlivé procesy a procedury pro tuto oblast.

3.1.2.2 Dělej

Sám název nám napovídá, že v tomto kroku se budeme zabývat implementací navrhnutých projektů a opatření v bodě Plánuj. Nemusí se vždy jednat pouze o implementaci

nápravných opatření, ale také o kompletně nově nasazené procesy, jež ISMS vyžaduje. Mezi základní implementované oblasti patří:

- Bezpečnostní politika
- Bezpečnostní standardy, postupy
- Proces řízení rizik
- Proces řízení bezpečnostních incidentů
- Odborné školení
- Řízení provozu
- Řízení zdrojů

Jednotlivé procesy je třeba testovat a zajistit výstupy pro další krok, jímž je „Check“ (Kontrola).

3.1.2.3 Kontroluj

Pro procesy a aktivity, jež jsme naplánovali a nasadili do ostrého, či testovacího provozu je nutné zhodnotit úroveň plnění požadavků. Ověřujeme jejich účinnost vůči bezpečnostní politice a vytvořeným standardům.

3.1.2.4 Jednej

Využití nápravných a preventivních činností, založených na výsledcích analýzy řízení tak, aby bylo dosaženo nepřetržitého zlepšování ISMS. Jedná se o implementace identifikovaných zlepšení, provedení nápravných a preventivních akcí, projednání výsledků a návrhů na zlepšení se zainteresovanými stranami, zajištění zlepšování dosažených cílů.[28]

3.1.3 ISO/IEC 20000

Norma ISO/IEC 20000 vzešla z původně britských norem BS 15000-1 a BS 15000-2. Tento standard se zaměřuje, ovšem není omezen pouze, na služby produkované ICT organizacemi. Cílem normy je nejen zvyšování kvality, ale také související zvyšování efektivity a snižování nákladů. Jelikož služby ICT jsou poměrně sofistikovanou oblastí, je nezbytné kvalitní a přesné nastavení pravidel pro řízení procesů. Norma ISO 20000 vychází z dlouholetých zkušeností odborníků a podniků zaměřených na ICT. Tyto

zkušenosti byly shrnuty do ITIL (Information Technology Infrastructure Library), z které standard ISO 20000 vychází. Rámec přístupů ITIL probereme níže.

Mezi základní vlastnosti normy patří již zmíněná, striktně definovaná pravidla pro poskytovatele služeb v oblasti ICT. Jsou stanoveny:

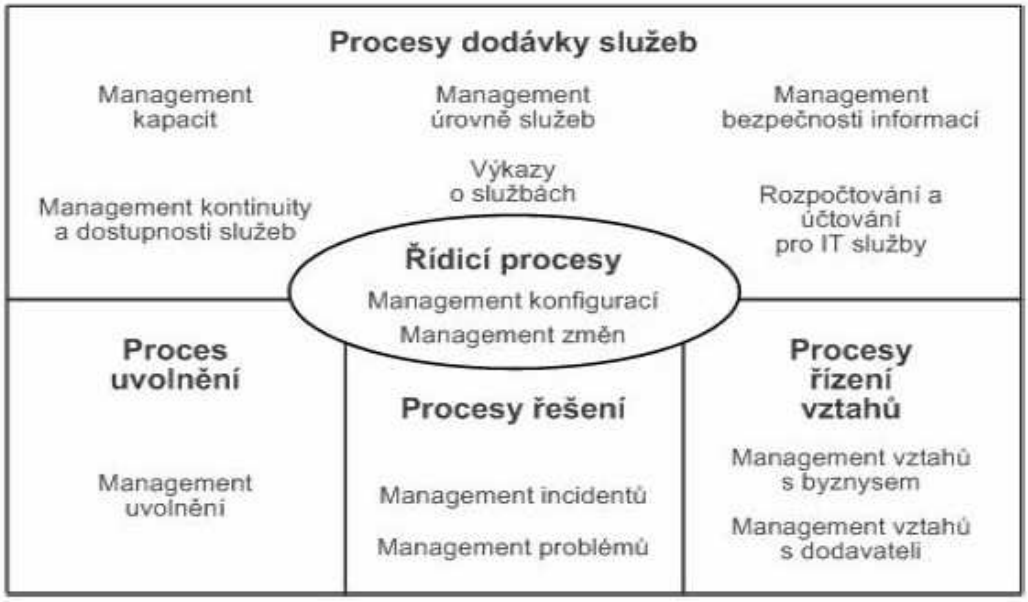
- Požadavky na odpovědnost vedení
    - Stanovení politiky managementu služeb, cíle, plány
    - Řízení rizik v organizaci
    - Stanovit odpovědného člena pro jednotlivé role managementu služeb
    - Definování zdrojů pro monitorování, plánování, implementaci, zlepšování služeb
- Požadavky na dokumentaci
    - Dokumentace politik poskytovaných služeb
    - Dokumentace o úrovni poskytovaných služeb
    - Dokumentace jednotlivých procesů
    - Záznamy vyplývající z normy ISO 20000
- Požadavky na kvalifikaci, povědomí a školení

Norma ISO/IEC 20000 se zabývá oblastmi:

- Procesy dodávky služeb
    - Management kapacit
    - Management úrovně služeb
    - **Management bezpečnosti informací**
    - Management kontinuity a dostupnosti služeb
    - Management Výkazy o službách
    - Management rozpočtování a účtování pro IT služby
- Řídící procesy
    - Management konfigurací

- Management změn

- Proces uvolnění
  - Management uvolnění
- Proces řešení
  - Management problémů
  - Management incidentů
- Procesy řízení vztahů
  - Management vztahů s byznysem
  - Management vztahů s dodavateli



Obrázek 9. ISO 20000 [31]

V rámci ISO 20000 si více přiblížíme pouze Management bezpečnosti informací.

3.1.3.1 Management bezpečnosti informací

ISO 20000 v oblasti bezpečnosti informací se zaměřuje především na dva nezbytné procesy:

- Proces řešení bezpečnostních incidentů
- Proces řízení rizik

V návaznosti na provedenou analýzu rizik je třeba stanovit bezpečnostní politiku organizace. Ta musí vycházet z obecné politiky společnosti. Bezpečnostní politika je dále rozpracovaná do interních bezpečnostních směrnic.

ISO 20000 klade důraz na vedenou dokumentaci, tudíž i řízení bezpečnosti informací musí být řádně dokumentováno. Z toho vyplývá, že procesy řízení bezpečnostních incidentů a řízení rizik spadají do této oblasti. Nejen základní popis celého procesu, ale také prováděné změny, stavy a výstupy z procesů je třeba dokumentovat.

Řízení procesu bezpečnostních incidentů je v rámci security managementu nezbytné. Za bezpečnostní incident můžeme považovat porušení bezpečnostní politiky, bezpečnostních standardů, či jiné jednání, které může mít za následek narušení dostupnosti, kontinuity a integrity informací. Co je v dané organizaci považováno za bezpečnostní incident, by mělo vyplývat z bezpečnostní politiky organizace. Security manager musí mít nastavený a zdokumentovaný proces pro řešení bezpečnostních incidentů, dle kterého se postupuje při této situaci.

V procesu řízení rizik je důležité vnímat rizika, které hrozí vybraným aktivům. Tyto je třeba snížit na přijatelnou mez. V kapitole Analýza rizik se k této problematice dostaneme podrobněji.

3.1.4 ITIL

ITIL (Information Technology Infrastructure Library) je rozsáhlý, procesně orientovaný rámec přístupů k zajištění dodávky služeb. Slouží managementu jako rámec k vytvoření návrhu procesů. Poprvé byl definován v 80. letech pro účely britské vlády společností OGC. V této první podobě obsahoval 31 knih. Dále byl rozvíjen i dalšími podniky a organizacemi. V letech 2000-2004 byl ITIL setříděn do 7 knih. ITIL verze 3 se skládá již z 5 knih zaměřující se na životní cyklus služby.

- Strategie služeb (Service stratégy)
- Návrh služeb (Service design)
- Přechod služeb (Service transition)
- Provoz služeb (Service operation)

- Neustálé zlepšování služeb (Continual service Improvement)

Obrázek 10.ITIL[27]

ITIL v jednotlivých knihách popisuje procesy, které IT většinou musí vykonávat, aby vůbec mohlo fungovat a nějaké služby poskytovat. ITIL se snaží dívat na poskytované služby z pohledu zákazníka, který dané služby odebírá. Předpokládá se a výsledky mnohých studií to i potvrzují, že společnosti, které své procesy zavedly podle ITIL, dosahují vyšší efektivity a jejich zákazníci mají větší záruku, že služba, za kterou platí, bude splňovat parametry uvedené v SLA. Další výhoda zavedení procesů podle ITIL spočívá v tom, že společnosti v takovém případě používají stejnou terminologii a měly by se tak díky ní lépe dorozumět se svými partnery a zákazníky. Spousta nedorozumění totiž dost často vyplývá z toho, že mnohé společnosti jen používají rozdílné pojmy pro pojmenování stejných skutečností nebo naopak stejný termín pro různé skutečnosti. Myšlenka ITIL je celkem jednoduchá, proč navrhovat a vymýšlet celý proces znovu od začátku, když už ho spousta jiných firem má zavedený a průběžně ho i vylepšuje. Bohužel, některé společnosti ITIL nepochopily a moc dobrou reklamu mu neudělaly. Spousta manažerů tak k němu přistupuje s určitými předsudky. O nejhorších zkušenostech „worst practices“ se zaváděním ITIL koneckonců pojednává i kniha ABC of ICT. [27]

ITIL popisuje vazby mezi jednotlivými procesy a definuje, jaké by měly být vstupy, výstupy, role a metriky. Vzhledem k tomu, že nositeli každého procesu jsou lidé, musí být jasně určeno, kdo za co odpovídá. V ITIL se používá pojem role, ta je přiřazena člověku nebo týmu, který pak v rámci daného procesu vykonává jednu nebo více činností. Je zřejmé, že pokud má daná role vykonávat příslušnou činnost, musí mít nejen požadované schopnosti, ale potřebuje k tomu též nástroje tj. HW, SW a musí být vybavena i odpovídajícími pravomocemi a nést určitou odpovědnost. ITIL doporučuje pro každý proces vytvořit tzv. RACI tabulku, která v záhlaví bude obsahovat role a v řádcích jednotlivé činnosti, které se musí v rámci procesu vykonat. U každé činnosti by mělo být uvedeno, kdo ji vykonává (Responsible), kdo je odpovědný za výsledek (Accountable), s kým je nutno postup konzultovat (Consult) a koho je třeba informovat (Inform). Pro úplnost je třeba dodat, že ITIL používá ještě pojem funkce a myslí tím organizační jednotku nebo tým, který určitý proces nebo aktivity v rámci daného procesu vykonává. Ač je všech pět knih, které tvoří jádro ITIL poměrně rozsáhlých – každá čítá několik set stran, detailní popis procesů v nich přesto nenajdete, neboť ITIL popisuje jen hlavní aktivity v rámci daných procesů. [27]

3.2 Analýza rizik

Analýzu rizik provádíme pro definovanou činnost, většinou jí je kritická činnost, na které závisí prosperita celé organizace. Zjednodušeně řečeno, hlavním cílem této aktivity je stanovení rizika hrozícího danému systému. Pokud chceme býti přesnější, a to bezpochyby chceme, je třeba si uvědomit, že máme jistá aktiva a ty mají své zranitelnosti. Dále existují určité hrozby, které zneužívají právě těchto zranitelností jednotlivých aktiv. Nyní si definujme použité pojmy:

- Aktivum – Je vše co má pro organizaci nějakou hodnotu a z tohoto důvodu je nezbytnost jej zabezpečit
- Hrozba – Nebezpečí, které existuje a může zavinit narušení informační bezpečnosti
- Zranitelnost – jedná se o vlastnost aktiva, která pokud je zneužito hrozbou, tak může dojít k narušení dostupnosti, integrity a důvěrnosti informací
- Riziko – je stanoveno pravděpodobností s jakou hrozba zneužije zranitelnosti aktiva
- Opatření – zavádíme za účelem snížení zranitelnosti aktiva a tím i klesá pravděpodobnost její zneužití hrozbou

Na tomto místě je nezbytné upozornit na skutečnost, že dost často dochází ke ztotožnění pojmu riziko a hrozba. Je třeba si však uvědomit, že hrozba může být zdrojem pro jedno nebo více rizik a že hrozba sama o sobě riziko nepředstavuje. Hrozby pouze zneužívají zranitelnosti vedoucí k ohrožení, což je riziko, které lze snížit prostřednictvím opatření chránící aktiva před působením těchto hrozeb. Tuto skutečnost nejlépe ilustruje následující obrázek. [22]

Obrázek 11. Analýza rizik [22]

Než se do AR pustíme, musíme si rozmyslet jestli si vystačíme sami a budeme analýzu provádět vlastními prostředky, nebo si najmeme specializovanou firmu. Každá z variant má své výhody i nevýhody. Pokud analýzu budeme provádět pomocí vlastních zaměstnanců je potřeba si uvědomit následující úskalí:

- Neobjektivní pohled interních pracovníků
- Vlastní zaměstnanci pravděpodobně nebudou mít tolik zkušeností v této problematice, jako specializovaní pracovníci
- Z předešlého bodu vyvstává nutnost školit vlastní zaměstnance na danou problematiku
- Zaměstnanci nebudou mít tolik času na svou primární pracovní náplň, jelikož budou zaměstnáni náročným projektem

Toto řešení má však i své výhody:

- Ušetříme finance za placení specializované firmy
- Nikdo cizí (pracovníci z externí firmy) se nedostane do styku s důvěrnými informacemi organizace
- Zaměstnanci lépe znají vnitřní prostředí a procesy společnosti a interní kulturu

Jestliže analýzu rizik svěříme do rukou externí firmy, výhody a nevýhody se nám budou zrcadlit z předešlého přehledu. Tudíž za výhody považujeme:

- Vysoká odborná způsobilost externích pracovníků
- Mnohem širší zkušenosti z více projektů prováděných ve více společnostech
- Interní pracovníci nebudou zatíženi projektem v podobě nutnosti podílet se na vytváření tohoto procesu

Nevýhody, které mohou vyvstat, jsou následující:

- Externí pracovníci se dostávají do styku s interními informacemi
- Externí pracovníci nemají tak veliký přehled o systémech a procesech ve společnosti jako interní zaměstnanci
- V rozepři s předchozím bodem je fakt, že externí zaměstnanci mohou objevit problémy, jež interní zaměstnanci nevidí (profesní slepota)
- Musíme se připravit na finanční výdaje za svěření AR do rukou externí firmy

Další variantou, která se nabízí, je kombinace obou možností, kdy se na implementaci podílí vlastní zaměstnanci a spolupracují s externími experty. Zde však nemůžeme čekat finanční úspory, spíše naopak. Najmutí odborníci mají za úkol dohlédnout, aby nebyly vynechány žádné důležité body a vnést do problematiky nezaujatý pohled zvenčí. Výhodou bude, že naši pracovníci budou spolupracovat a přebírat know-how od zkušených specialistů a přitom je implementovat do nám dobře známého prostředí.

Pokud máme jasno, kdo bude AR provádět, je třeba se rozmyslet, jestli budeme provádět kvalitativní, či kvantitativní analýzu.

Kvalitativní analýza je méně náročná na zdroje a trvá kratší mnohem kratší dobu než kvantitativní analýza rizik. Především proto, že hodnotu aktiva není nutné vyjadřovat

v penězích stejně jako možnou škodu v případě realizace konkrétní hrozby. To však vede k horší kontrole nákladů ve fázi zvládání rizik, kdy vybíráme vhodná opatření.[23]

Kvantitativní analýza je náročnější na zdroje a její provedení trvá mnohem déle než kvalitativní analýza rizik. Je tomu tak proto, že hodnotu aktiva je nutné vyjádřit v penězích stejně jako možnou škodu v případě realizace konkrétní hrozby. Vyjádření škody ve finančních jednotkách však umožňuje jednodušší rozhodování ve fázi zvládání rizik, kdy vybíráme vhodná opatření.[23]

3.2.1 Analýza Aktiv

K provedení analýzy rizik je nezbytné začít identifikací a ohodnocením aktiv organizace. Aktivum je vše co má pro organizaci určitou hodnotu a tudíž je potřeba chránit. Každá společnost má jistě spoustu aktiv odlišných významů a tím pádem hodnot. S největší pravděpodobností se budeme zabývat pouze těmi významnými aktivy. Které to jsou? Tuhle otázku je nutné položit vrcholnému managementu, který musí definovat systémy, či poskytované služby, jež mají zásadní vliv na naši podnikatelskou činnost. Vynaložení prostředků na řízení rizik nevýznamných aktiv je plýtvání financemi i časem. Z tohoto důvodu nám vedení jistě zadá zabývat se aktivy majícími vliv na hlavní obchodní cíle organizace. Pokud je tento stanoven, můžeme se pustit nejprve do identifikace a poté do ohodnocení aktiv.

3.2.1.1 identifikace aktiv

Jelikož už nám bylo deklarováno, které významné činnosti se máme věnovat, můžeme přistoupit k definování aktiv. Těch bude jistě několik a s různou významností na prováděnou aktivitu. Některá aktiva mají při svém výpadku na žádoucí průběh aktivity vliv zásadní, jiná pouze okrajová. Při definování aktiv nesmíme zapomenout na fakt, že komponenty budou spadat do několika skupin, které s největší pravděpodobností budou HW, SW, síť, data, dokumentace, image firmy, zaměstnanci. Nejedná se tedy jen o fyzické zařízení, ale také sem spadají síťové trasy, aplikace, antivirové programy, obchodní smlouvy, výrobní dokumentace, ale také zaměstnanci. Správu zmíněných zařízení, dokumentů mají na starosti právě pracovníci. Využívají při tom právě svých schopností, které jsou také aktivem. Aktiva a jejich význam, bude samozřejmě odlišný v závislosti na oboru podnikání

Vždy je také třeba identifikovat vlastníka každého aktiva. Vlastníkem aktiva rozumíme přímo pověřenou osobu, plně odpovědnou za toto aktivum.[1] Jedná se o osobu odpovědnou za klasifikaci citlivosti a důležitosti daného aktiva, schvaluje systémové administrátory, určuje kontrolní mechanizmy pro užívání aplikací a dále seznamuje uživatele aktiv s kontrolními požadavky.

3.2.1.2 Ohodnocení aktiv

Dalším logickým krokem je stanovit stupnici a hodnotící kritéria, která budou použita k přiřazování ohodnocení určitého aktiva. Tato stupnice může být vyjádřena penězi nebo kvalitativními hodnotami. Je na uvážení organizace a výskytu konkrétních aktiv, kterou z variant zvolíte. Možné je také obě varianty kombinovat. Stupnice peněžní bude vyjadřovat v místní měně hodnotu určitého aktiva. Stupnice kvalitativní vyjadřuje hodnotu v termínech například od velmi nízká až po kritická. Typické termíny používané pro kvalitativní hodnocení jsou uvedeny v následující tabulce.

Stupeň	Zkratka	Úroveň	Pravděpodobnost
1	N	Nízká	Malé škody
2	S	Střední	Vážné škody
3	V	Vysoká	Velmi vážné škody
4	J	Jistá	Existenční škody

Tabulka 1. Stupnice hodnocení aktiv[25]

Vhodné je také barevné odlišení. Máme-li mít rozsáhlé tabulky s hodnocením aktiv, pomohou vhodně zvolené barvy k jednodušší orientaci. Výběr a rozsah termínů, které si organizace zvolí, závisí na bezpečnostních potřebách organizace, její velikosti apod. Má-li organizace zaveden systém řízení kvality (ISO 9001), může využít stávající model k ohodnocení aktiv.[1]

Hlavním principem při ohodnocení aktiv jsou náklady vzniklé v důsledku porušení důvěrnosti, integrity a dostupnosti. Tedy tyto tři kritéria poskytují podklady pro ohodnocení aktiv. Typická otázka tak může například znít: „ jaký dopad bude mít na

organizaci nedostupnost centrálního informačního systému?" Odpověď od „žádný dopad na organizaci, až po existenční potíže organizace". Toto hodnocení je třeba provádět s majitelem aktiv. Protože jeho hodnocení může být subjektivně zbarveno, je vhodné provést podobné interview s některým „superuživatelem" daného aktiva. Tato forma křížové kontroly je důležitým faktorem upřesnění hodnoty aktiva a je doporučováno provádět ji u všech aktiv, u nichž existuje předpoklad vysoké hodnoty pro organizaci.[1]

Celá řada aktiv může mít v průběhu hodnocení přiřazeno několik hodnot. Například informační systém může být hodnocen z hlediska pořizovacích investic, z hlediska důvěrnosti a dostupnosti, z hlediska práce nutné na implementaci apod. Každá z takto definovaných hodnot se bude zcela jistě lišit. Finálně přiřazená hodnota se může rovnat maximální hodnotě ze všech uvedených, může být průměrem nebo součtem. Ať si vyberete jakýkoliv model, musíte jej pak použít pro všechny aktiva, u nichž je využita kombinovaná hodnota. Nezapomeňte, že zde stanovené hodnoty slouží jako základ pro analýzu rizik a výpočet nákladů na jejich ochranu.[1]

Pro výpočet nám poslouží tzv. součtový algoritmus. Sčítáme dostupnost, integritu, důvěrnost aktiva a dělíme třemi. Použijeme-li výše zmíněnou stupnici a zvolíme si ukázkové hodnoty:

Aktivum: Switch (přepínač)

Dostupnost: 4

Integrita: 4

Důvěrnost: 4

Vztah: (4+4+4)/3=4

Hodnota 4 znamená, že ohrožení tohoto aktiva může způsobit vážné potíže či podstatné finanční ztráty.

skupina aktiv	Identifikované aktiva	dostupnost	integrita	důvěrnost	Hodnota aktiva
SW	Operační systém	4	4	4	**4**
	Databázový systém	4	4	4	**4**
HW	Router	4	3	4	**4**
	Switch	4	4	4	**4**
	PC	1	3	3	**2**
Informace	Data v databázovém serveru	4	4	4	**4**
síť	Přenosové médium	4	2	2	**3**
personál	Specializovaný pracovník	3	2	2	**2**
prostory	Datový sál	1	1	2	**1**

Tabulka 2. Hodnocení aktiv

Tento jednoduchý vztah nám poskytne nejrychlejší způsob, jak získat hodnotu aktiva. Zároveň také odpovídá na otázku, jaký dopad na organizaci bude mít zničení, případně poničení tohoto systému. Při hodnocení aktiva je vhodné věnovat zvýšené úsilí detailnímu popisu a „pátrání", kde všude dané aktivum může být umístěno[1]. V tento moment tedy známe aktiva a jejich hodnotu. Můžeme tedy přistoupit k identifikaci hrozeb a zjistit zda působí na námi definované aktiva.

3.2.2 Analýza Hrozeb

Hrozbu můžeme definovat jako nebezpečí hrozící našemu systému, přičemž využívá zranitelnosti jednotlivých aktiv a pravděpodobnost narušení dostupnosti, integrity a důvěrnosti informací je pro nás rizikem. Abychom mohli provést analýzu hrozeb, je třeba znát, pro jaké aktiva máme identifikovat hrozby. Tuhle první fázi nazýváme Identifikace hrozeb. V dalším kroku je třeba jednotlivé hrozby ohodnotit pro vyjmenované aktiva, neboli kvantifikovat. Druhou fází je tedy Kvantifikace hrozeb.

- Identifikace hrozeb
- Kvantifikace hrozeb

Výstupem z části Identifikace hrozeb je seznam všech hrozeb, jejich zdroje a na jaké aktiva působí. V části druhé očekáváme dokumentaci obsahující ohodnocené hrozby a jasný přehled, které naší organizaci nejvíce ohrožují.

3.2.2.1 Identifikace hrozeb

Hrozby se vyskytují v různých podobách, mají schopnost vyvolávat další hrozby, ovlivňovat více aktiv, a časem modifikovat své vlastnosti. Pokud máme například hrozbu úder bleskem, tak je nám schopna vyvolat další hrozbu a tou je požár. Aktiva jsou vystaveny hrozbě požáru. Při zásahu proti němu může nastat ohrožení aktiva vodou při hašení. Jedna hrozba je schopna působit i na několik aktiv najednou. Hrozby lze dělit dle několika hledisek. Jednou z možností může být třídění podle místa jejich působení z pohledu organizace na:

- Vnitřní
- Vnější

Pokud se budeme bavit o vnitřních hrozbách, máme na mysli ty, které vznikají uvnitř organizace. Tyto hrozby máme šanci jistou mírou ovlivnit, eliminovat je. Vnější hrozby nacházející se za hranicemi našeho podniku půjde ovlivnit jen stěží. Případný dopad na organizaci se však můžeme snažit snížit. Dělení dle časového působení:

- Trvalé
- Dočasné

Je však třeba mít na mysli, že hrozby jsou časově proměnné a jejich působení se může změnit.

Mnohem zajímavější rozdělení je podle zdroje vzniku hrozby:

- Přírodní vlivy
- Působení člověka
    - Úmyslné jednání
    - Neúmyslné jednání

Obrázek 12. Kybernetické hrozby [33]

Přírodní vlivy jako jsou například povodeň, zemětřesení, požár, hurikán atd. jsou hrozby, které nemůžeme ovlivnit, pouze jen pomocí metodik zmírnit jejich dopad na organizaci. Lidé nám mnohdy mohou způsobit mnohem větší škody než přírodní katastrofa, zejména pokud se jedná o úmyslné počínání za cílem vlastního obohacení, či záměrně existenčně poškodit náš systém. Tady nastává další otázka, odkud útočník pochází, zda z řad vlastních zaměstnanců, či se jedná o cizí osobu.

V následujícím přehledu vycházíme z normy ČSN ISO/IEC TR 13335, jež definuje hrozbu jako „potenciální příčinu nežádoucího incidentu, který může mít za následek poškození systému nebo organizace“.

V tabulce č. máme přehled obecných hrozeb. Seznam udává u každé hrozby odpovídající typ:

- D (Deliberate) – úmyslný
- A (Accidental) – náhodný
- E (Environmental) - přírodního charakteru

D je používáno pro všechny úmyslné akce, zaměřené na aktiva IT, A je používáno pro všechny lidské aktivity, které mohou náhodně poškodit aktiva IT, E je používáno pro všechny incidenty, které nejsou založeny na lidských aktivitách.

HROZBA	Typ
Zemětřesení	E
Povodně	DAE
Hurikán	E
Blesk	E
Průmyslová akce	DA
Bombový útok	DA
Použití zbraní	DA
Požár	DA
Úmyslná škoda	D
Selhání dodávky energie	A
Selhání dodávky vody	A
Selhání klimatizace	DA
Selhání hardwaru	A
Kolísání proudu (energie)	AE
Extrémní teplota a vlhkost	DAE
Elektromagnetická radiace	DAE
Elektrostatický náboj	E
Krádež	D
Neoprávněné použití paměťového média	D
Poškození paměťového média	E
Chyba provozních zaměstnanců	DA
Chyba údržby	DA
Selhání softwaru	DA
Použití softwaru neautorizovanými uživateli	DA
Použití softwaru neautorizovaným způsobem	DA
Předstírání identity uživatele	D
Nelegální používání softwaru	DA
Škodlivý software	DA
Přístup k síti neautorizovanými uživateli	D
Použití síťového vybavení neautorizovaným způsobem	D
Technické selhání síťových komponent	A
Chyba přenosu	A
Poškození vedení	DA
Přetížení provozu	DA
Odposlech	D
Infiltrace komunikací	D
Analýza provozu	D
Chybné směrování zpráv	A
Selhání komunikačních služeb (tj. síťových služeb)	DA
Chyby uživatele	DA
Nesprávné použití zdrojů	DA

Tabulka 3. Hrozby[25]

Pokud provádíme identifikaci hrozeb poprvé, je vhodnější použít přehled obecných hrozeb. Tuto tabulku poté budeme modifikovat dle vlastních potřeb. Jestliže usoudíme, že některé hrozby se nás netýkají, tak je odstraníme a nebudeme se jimi zabývat, naopak přidáme ty, které zde postrádáme. V momentě, kdy máme identifikovány všechny hrozby, nastává ohodnocení hrozeb.

3.2.2.2 Kvantifikace hrozeb

V této části budeme identifikované hrozby hodnotit. Budeme hodnotit pouze týkající se našich systémů. K této činnosti je nezbytné stanovit si metodiku hodnocení. Možností je využít automatizované softwarové nástroje, či si určit vlastní metodiku. Zjednodušeně řečeno je jedno jaké metody použijeme, důležité je aby odrážela skutečný stav, který analyzujeme. Stanovení stupnice a přiřazení číselné hodnoty ke každé hrozbě je jedna z využívaných metod. Každý preferuje jiné intervaly <1;100>, <1;5>. Důležité je stanovit si rozmezí, jež je pro nás nejvhodnější a splňuje naše potřeby. Obecně platí, čím více stupňů si definujeme, tím bude přiřazování hodnot složitější. Mnohem přehlednější a výstižnější je využití pětistupňového <1;5>, či dokonce čtyřstupňového <1;4> intervalu. Záleží pouze na nás, která varianta nám vyhovuje. Dle mého názoru je nejvíce výstižná čtyřstupňová stupnice, kterou prezentuje Miroslav Čermák ve své knize Řízení informačních rizik v praxi.

stupeň	zkratka	Úroveň	Pravděpodobnost	Od	Do
1	N	Nízká	Nepravděpodobná	0%	25%
2	S	Střední	Pravděpodobná	25%	50%
3	V	Vysoká	Vysoce pravděpodobná	50%	75%
4	J	Jistá	jistá	75%	100%

Tabulka 4. Stupnice hodnocení rizik[25]

V případě pětistupňového přehledu přibývá úroveň Žádná hrozba. To je ovšem naprosto zbytečné, jelikož takové hrozby nás nezajímají a nebudou figurovat mezi definovanými hrozbami. V následující tabulce č. 5 vidíme ukázku přehledu identifikovaných a ohodnocených hrozeb.

	Hrozba	Typ	Stupeň
1.	Povodeň	DAE	3
2.	Blesk	E	4
3.	Extrémní teplota a vlhkost	DAE	2
4.	Technické selhání síťových komponent	A	2
5.	Kolísání proudu	AE	2

Tabulka 5. Hodnocení hrozeb

Výše uvedené údaje se jsou čistě náhodné, nevztahují se na žádnou organizaci a slouží pouze pro modelovou situaci. Budeme s nimi pracovat i nadále při definování a kvantifikování zranitelností.

3.2.3 Analýza Zranitelnosti

V této fázi budeme hodnotit zranitelnost jednotlivých aktiv, nebo skupin. Každé aktivum má svou zranitelnost a my potřebujeme znát její rozsah. Míru zranitelnosti aktiva, či skupiny aktiv určujeme vůči konkrétní hrozbě. Jak, nebo podle čeho, budeme stanovovat míru zranitelnosti? Budeme hodnotit kvalitu současných opatření. Jako vstup lze použít několik eventualit. Vycházet lze například z provedených penetračních testů na systému, které odhalí zranitelné místa. Velmi užitečná je vedená dokumentace implementovaných opatření v průběhu provozu systému.

Sestavíme si matici, v níž budeme definovat zranitelnost pro dvojici Aktivum – Hrozba.

	aktiva	Operační systém	Databásový systém	Router	Switch	PC	Data v databázovém serveru	přenosové médium	specializovaný pracovník	Serverovna
	Hodnota aktiva	4	4	4	4	2	4	3	2	1
Hrozby	Hodnota hrozby	Zranitelnost								
Povodeň	4			4	1	1		1	1	1
Blesk	4			2	2	2		2	2	2
Selhání hardware	2			3	3	3				
Selhání software	2	3	3				4			
Viry	2	5	5				2			

Tabulka 6. Zranitelnost

V tabulce si můžeme všimnout, že hrozba nepůsobí na všechna aktiva. Vždy záleží, jaké skupiny aktiv si definujeme. Pokud budeme mít skupiny stanoveny tak podrobně, jako v tabulce č. 6, na aktivum působí pouze některé hrozby. Bereme-li v úvahu aktivum serverovna, tak na něj viry ani selhání SW/HW nebude mít vliv. Avšak povodeň, či blesk ano. Naopak na operační systém, ač se to zdá divné, nebude mít v našem případě vliv povodeň. Tato hrozba bude mít vliv na router, PC. Kdybychom definovali pouze skupinu aktiv serverovna, tak by sem jistě patřil HW, SW i data. V tomto případě by na tuto skupinu aktiv působily hrozby povodeň, selhání HW, selhání SW i viry.

3.2.4 Výsledné riziko

Výsledným rizikem definujeme pravděpodobnost, s jakou hrozba zneužije zranitelnosti aktiva. Výsledné riziko (R) je tedy závislé na zranitelnosti aktiva (Z) vůči hrozbě (H) a samotném aktivu (A). Matematicky lze tento vztah vyjádřit rovnicí:

$$R= A*H*Z$$

Budeme vycházet z tabulky, kde jsme stanovili zranitelnost. Podle uvedeného vztahu doplníme tabulku výsledných rizik.

	aktiva	Operační systém	Databásový systém	Router	Switch	PC	Data v databázovém serveru	přenosové médium	specializovaný pracovník	Serverovna
	Hodnota aktiva	4	4	4	4	2	4	3	2	1
Hrozby	Hodnota hrozby	Riziko								
Povodeň	4			64	16	8		12	8	4
Blesk	4			32	32	16		24	16	8
Selhání hardware	2			24	24	12				
Selhání software	2	24	24				32			
Viry	2	40	40				16			

Tabulka 7. Výsledné riziko

Když máme přehled výsledných rizik, je třeba stanovit hranice, kdy se jedná o zanedbatelné či kritické rizika. K tomuto rozdělení využijeme stejného modelu jako při hodnocení aktiv, hrozeb a zranitelností.

Stupeň	**Zkratka**	**Úroveň**	**Pravděpodobnost**	**Od**	**Do**
1	N	Nízké	Riziko je možné akceptovat a dále jen monitorovat	0	16
2	S	Střední	Riziko musí být zvládnuto dle plánu	16	32
3	V	Vysoké	Riziko musí být zvládnuto dle plánu s vysokou prioritou	32	48
4	K	Kritické	Riziko musí být ihned zvládáno s nejvyšší prioritou	48	64

Tabulka 8. Stanovení stupnice rizik[25]

Výstupem z této fáze je seznam rizik. V tomto dokumentu by měla být data sdělující, která aktiva jsou riziky nejvíce ohrožena, které hrozby tato rizika vytvářejí a jaké zranitelnosti využívají. Součástí by mohlo býti i ohodnocení námi definovanou stupnicí, která přispěje k větší přehlednosti, avšak mám pocit, že více či méně spíše pro nás.

Vrcholné vedení, pro které tyto procesy provádíme, zcela jistě našemu hodnocení porozumí, ale je ne vždy si efektivně představí důsledky. Z tohoto důvodu je velmi vhodné zavést finanční hodnocení rizik. To je přehled pro vrcholné manažery nejpřehlednější a nejkonkrétnější.

3.2.4.1 Hodnocení rizik

Provedeme-li výše zmíněným způsobem hodnocení rizik, ušetříme spoustu času nejen sobě, ale také vedení. Z naší pozice budeme obhajovat požadované finanční prostředky na provedení opatření ke snížení rizik. Budete se mnou určitě souhlasit, že mnohem účinnější pákou k uvolnění zdrojů, bude vyčíslená případná finanční ztráta, než jen riziko ohodnoceno stupněm 4.

Finanční ohodnocení rizika je nezbytné i k návrhu opatření. Budeme zcela jistě navrhovat pouze takové opatření, nebo spíše do takové finanční výše, která bude přiměřená výši pravděpodobných ztrát. Není naším záměrem vytvořit velkolepé, nákladné opatření, na systému, kde případná ztráta informací se nerovná ani jedné polovině nákladů na vytvoření těchto opatření. Musíme si uvědomit, že finanční prosperita je bezesporu významným faktorem a naše aktivity se podle toho musí řídit.

Jak takové hodnocení ale provést? Správné ohodnocení není tak jednoduché, jak se zprvu může zdát. Je nutné počítat s náklady spojenými s oblastmi:

- **Pořízení nového HW** – v případě, že dojde ke zničení zařízení (požár,voda)
- **Zprovoznění systému** – obnovení běhu systému (instalace, konfigurace HW, SW, aplikací)
- **Obnova informací** – obnova dat ze záložních systémů
- **Ušlý zisk** – Jedná se o zisk ušlý z důvodu nefunkčnosti systémů, služeb:
    - Finanční postihy za nedodržení smluvních podmínek (např. SLA)
    - Neuskutečnění nových projektů

- **Pošramocení dobré pověsti**
    - Ztráta důvěry klientů – zde se musíme ptát, zda dojde ke ztrátě důvěry klientů, akcionářů a veřejnosti a kolik klientů pravděpodobně odejde a jak velký zisk nám generuje jeden klient a vůbec jaký bude mít ztráta důvěry dopad na tempo růstu.[24]
    - Pokles ceny akcií v důsledku ztráty důvěry akcionářů lze těžko odhadnout. Nicméně je možné ji ale přibližně stanovit podle společností, u kterých k poklesu cen akcií ze stejného důvodu došlo. [24]
    - Náklady na marketing a PR za účelem přesvědčení klientů, akcionářů a veřejnosti, že situace, ke které došlo, byla výjimečná a nebude se již opakovat a tím získat zpět jejich důvěru a postavení na trhu. [24]

Tento přehled však není šablonou, s níž se nesmí hýbat. Jedná se pouze o výčet obvyklých oblastí v této problematice. Ne pokaždé využijeme všechny vyjmenované body. Tento výčet je nutné modifikovat dle daného rizika. Samozřejmě se najdou i oblasti, u kterých bude nutné započítat mezi náklady i aktivity, jež zde nejsou uvedeny.

3.2.5 Opatření

Opatření zavádíme na základě výsledků analýzy rizik. Naším cílem je vhodným opatřením snížit míru rizika na přijatelnou mez. Z toho vyplývá skutečnost, že snižujeme zranitelnost určitého aktiva vůči hrozbě. Riziko se nám nepodaří nikdy docela eliminovat, přesto našim úkolem je stlačit jej na co nejmenší míru. Avšak jaká je ta přijatelná mez, kde se nachází? Odpověď na tuto otázku nalezneme v následujících řádcích.

Jak bylo řečeno na začátku odstavce, opatření je nutné provádět v návaznosti na analýzu rizik. Z tohoto procesu využijeme výstupy, dle kterých se budeme při implementaci opatření řídit. Jelikož máme definovány kritické služby, aktiva nezbytné k fungování těchto služeb, zranitelnosti těchto aktiv a hrozby, tak z výsledků AR zjistíme, u kterých systémů je nutné implementovat nápravné opatření. K dispozici je jistě několik eventualit, které máme možnost vybrat. Otázku, kterou volbu zvolit, pravděpodobně rozhodne cena daného řešení. Faktor je to jistě významný, avšak je třeba si uvědomit, že je třeba brát v potaz rovněž efektivitu řešení vůči našim skutečným požadavkům na celý systém. Je důležité zvolit přiměřené opatření. Přehnané i podceněné nápravné aktivity nebudou tím

pravým ořechovým. Obě varianty znamenají finanční ztrátu organizace. Uveďme si malý příklad.

Jestliže naším primárním obchodním cílem bude například zajištění chodu IS, máme se zákazníkem nasmlouvány SLA, je třeba zajistit pokud možno nepřetržitou konektivitu, do těchto systémů. Konektivita je zajištěna přes síťový prvek, který když selže, dojde k přerušení provozu našich služeb a než je tento problém vyřešen, dochází k nemalým finančním ztrátám. Jestliže porušíme i nasmlouvané SLA, bude to pro nás znamenat další finanční postih. Hrozbou našemu systému je tedy selháni HW. Zranitelnost této služby snížíme přidáním dalšího síťového prvku. Vytvoříme buď další redundantní cestu, nebo nový prvek dáme do clusteru se současným prvkem. Riziko je tedy sníženo na přijatelnou mez. Náklady na pořízení nového HW stály např. 100 000,- Kč. Škody, které by způsobil výpadek nezálohovaného HW, mohou činit řádově statisíce, tudíž výrazně převyšují náklady na nový síťový prvek. Takovéto opatření je samozřejmě v pořádku. Jistě nevhodným by bylo opatření, pakliže by se jednalo např. o uživatelský switch, který by při výpadku zavinil nedostupnost internetu a vnitřních sítí společnosti pro koncové uživatele společnosti, kteří nepotřebují stálý přístup ke své pracovní náplni. V tomto případě by způsobené škody byly téměř nulové, tudíž tak nákladné opatření jako v předešlém případě není nutné.

3.3 Bezpečnostní dokumentace

Správné řízení jakéhokoliv procesu se neobejde bez kvalitní dokumentace. Ne jinak tomu je samozřejmě i při řízení bezpečnosti informací. Dokumentace může být vedená jak v elektronické, tak i v papírové podobě. Dnes se více využívá první varianta. Mnohem důležitější fakt je, že musí být uložena ve stanoveném úložišti, jež je chráněno nastavenými přístupovými právy pro danou skupinu uživatelů. Řízení informací se dotýká tedy i sebe samé.

Dokumenty, se kterými budeme jistě pracovat, jsou bezpečnostní politika, bezpečnostní směrnice, seznam rizik, dokumentace jednotlivých procesů, návrhů na vylepšení, implementace a monitorovací záznamy. Je nezbytné kvalifikovat jednotlivé dokumenty dle jejich významu a podle toho s nimi nakládat. Bezpečnostní politika bude jistě ohodnocena jako informace veřejná. Zpřístupněná může být na internetových stránkách, kde do ní mohou nahlédnout potenciální zákazníci, ale i ostatní široká veřejnost. Bezpečnostní standardy už veřejně přístupné být nemohou. Pokud by se tomu tak stalo, znamenalo by to

bezpečnostní incident. Jedná se převážně o interní směrnice pro zaměstnance, jak se chovat v otázce informační bezpečnosti, co je v rámci bezpečnosti organizace povoleno a co je naopak zakázáno. Také zde mohou být uvedeny postupy pro různé varianty situací. Jedná se o data, které by mohly být zneužity třetí stranou k napadení dostupnosti, důvěrnosti a integrity informací. Bezpečnostní standardy, postupy můžeme klasifikovat jako interní informace. Veřejnosti jsou tyto data nedostupná, ale interní zaměstnanci k nim mají přístup. Seznam řízení rizik můžeme ohodnotit jako data citlivá. Jsou vyhrazeny pouze určeným zaměstnancům.

Každý dokument by měl mít svého vlastníka, jenž je určen v hlavičce dokumentu. Dokumenty musí být vytvářeny dle stanoveného vzoru a obsahovat stanovené informace. Mohou jimi být název dokumentu, již zmíněný vlastník dokumentu, datum poslední aktualizace, očíslované stránky.

3.3.1 Bezpečnostní politika

Základním dokumentem, který zastřešuje přístup organizace k bezpečnosti ICT je bezpečnostní politika. Tímto dokumentem dává firma jasně najevo svou vůli zabývat se řízením bezpečnosti. Bezpečnostní politika je pomyslnou špičkou pyramidy řízení bezpečnosti ve firmě, která definuje jednotlivé oblasti a procesy, kterými se společnost v této otázce zabývá. Tento dokument je nezbytné pečlivě vypracovat, aby nemusel být při sebemenších změnách ve společnosti přepracováván. To ovšem neznamená, že dokumentace bude mít neměnnou podobu. Samozřejmostí je, že listina musí odrážet aktuální postoj organizace v otázce bezpečnosti. Důležité však je, aby dokument byl pevný a jasně dával najevo postoj organizace a nebyl měněn při jakékoliv příležitosti. Na veřejnost, zákazníky by příliš častá modifikace dokumentu a změny v přístupu k bezpečnosti mohly působit nevěrohodně a neprofesionálně.

Bezpečnostní politika by nám měla odpovídat na otázku, co chceme chránit, jak to chceme chránit a proč to chceme chránit.

Bezpečnostní politika ICT musí vycházet z celkové bezpečnostní politiky organizace. Výsledný dokument musí být schválen vedením společnosti a teprve až po té může být uveden v platnost. Z tohoto dokumentu vycházejí další bezpečnostní směrnice, postupy, které se zabývají jednotlivými oblastmi a jasně stanovují pravidla pro přístup a manipulaci s informacemi ve firmě. Takovými dokumenty mohou být postupy pro koncové uživatele

stanic, pravidla pro přístup do vnitřní sítě, pravidla pro udělování práv přístupu do systému atd.

3.4 Implementace bezpečnostní politiky

Na úvod celého projektu je důležité vytvořit časový harmonogram. V tomto dokumentu je třeba časově rozvrhnout jednotlivé aktivity a především stanovit jejich termín splnění. Musí být pověřená osoba, nejlépe projektový manažer, který dohlíží na dodržení těchto termínů. Výstupem jsou poté jednotlivé procesy, bezpečnostní politiky, směrnice, pracovní postupy atd. Všechny výstupy by měly dokumentovány v elektronické, nebo papírové podobě.

K uvedení v platnost informační bezpečnosti musíme mít všechny procesy připravené. Jakmile dojde k schválení těchto procesů, je třeba začít tyto aktivity plnit. Je potřeba, aby organizace vydala nařízení, že bezpečnostní politika a směrnice vchází v platnost od určitého data. Od stanoveného dne jsou zaměstnanci povinni se těmito dokumenty řídit. Bezpečnostní manager musí dohlížet na plnění bezpečnostní politiky, bezpečnostních směrnic a řídit se stanovenými procesy.

II. PRAKTICKÁ ČÁST

4 ÚVODNÍ USTANOVENÍ

Tato diplomová práce byla zpracovávána pro společnost, jejímž primárním obchodním cílem je poskytování ICT služeb. Jedná se o mladou organizaci, která vstoupila na trh s vysokými ambicemi a již nyní poskytuje své služby významnému podnikatelskému subjektu. Přesto se dá říci, že stojí na počátku svého působení. S tímto je spojeno budování a shromažďování velkého množství aktiv, díky kterým se společnost může stát úspěšnou na svém poli působnosti. Vrcholný management své úsilí již od počátku nasměřoval na vybudování silného zázemí. Zaměřil se především na pořízení prvotřídního zařízení, nezbytného pro provozování tohoto druhu služeb. Dále se jednalo o shromáždění odborníků v této oblasti a v neposlední řadě vybudování kvalitního obchodního týmu.

Další oblastí, kterou je nezbytné se zabývat, je kvalita poskytovaných služeb. Nastavení potřebné kvality služeb a její dodržení je významným faktorem v konkurenčním souboji. Zákazníkovi však nestačí konstatování dané společnosti o úrovni a kvalitně vlastních služeb. Potřebuje objektivní pohled, který v dnešní době splňuje nejen reference zákazníků a partnerů, ale především certifikace. Vedení organizace si uvědomuje význam tohoto faktoru, a proto se rozhodlo podstoupit certifikaci. Vybrána byla norma prokazující kvalitu poskytovaných služeb v oblasti ICT, jímž je ISO/IEC 20000.

Praktická část je zaměřena na oblast security management. Tato sekce se zabývá řízením bezpečnosti informací v organizaci. V následujících kapitolách blíže objasním, čím bylo nutné se zabývat v přípravě a implementaci security managementu. Záměrně píši, blíže objasním, jelikož ne všechny informace je možné v diplomové práci uvést z důvodu klasifikace jejich významnosti. V oblasti bezpečnosti se spousta těchto informací klasifikuje jako důvěrná či citlivá.

5 PŘÍPRAVA A IMPLEMENTACE INFORMAČNÍ BEZPEČNOSTI

Celému procesu příprav a implementace informační bezpečnosti předcházela podrobná analýza, která byla prováděna externí firmou. Výsledky analýzy zodpověděly na otázky, které oblasti jsou v souladu s danou certifikací a které činnosti a procesy je třeba zlepšit, či zcela nově zavést tak, aby splňovaly potřebné podmínky. Informační bezpečností se v minulosti zabývala jednotlivá oddělení, avšak každé pouze na své úrovni a jejich činnosti nebyly vždy vzájemně propojeny. ISO 20000 tento problém řeší zavedením role Security manager. Ten má za úkol nastavit procesy, působícími napříč jednotlivými odděleními. Bezpečnostní manager je zodpovědný za vytvoření bezpečnostní politiky, bezpečnostních směrnic a postupů.

V rámci ISO 20000 jsem se soustředil především na tyto dva hlavní procesy:

- Řízení bezpečnostních incidentů
- Řízení rizik

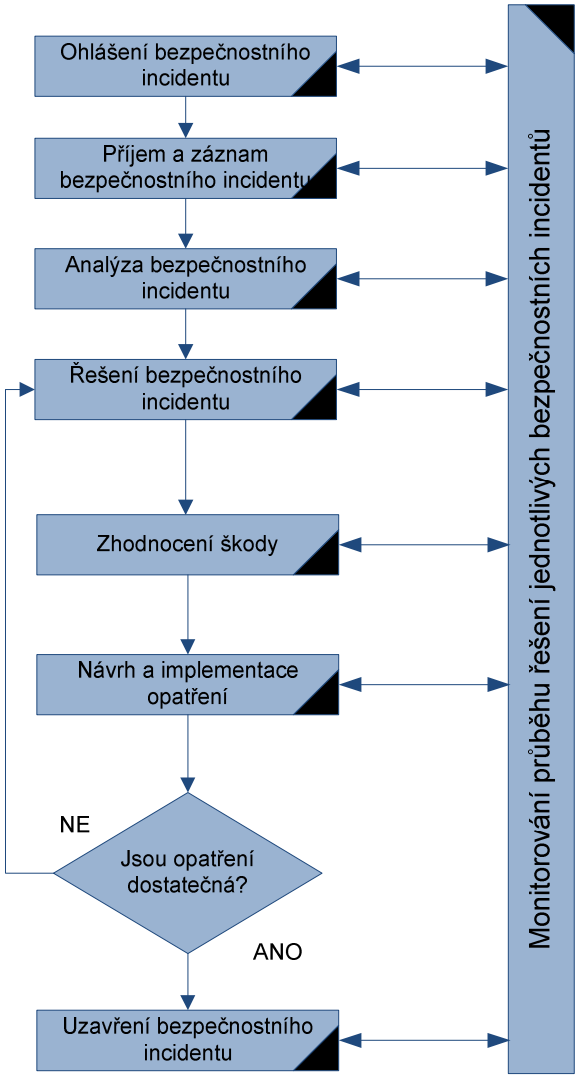
Veškeré procesy, je bylo nutné nastavit tak, aby vyhovovaly organizaci a lidem, kteří se jimi zabývají, či se jimi řídí. Účelem není nastavit velkolepé a složité procesy, které by pak nebylo možné plnit. Naopak je třeba nastavit splnitelné a účelné procesy, které jsou prokazatelně plněny.

5.1 Proces řízení bezpečnostních incidentů

Cílem tohoto procesu je zajistit, aby v organizaci byly řízeny bezpečnostní incidenty, které mají vliv na bezpečnost informací při poskytovaní servisních služeb zákazníkovi.

- Vstupy procesu: Hlášení bezpečnostního incidentu
- Výstupy procesu: Záznam o bezpečnostním incidentu

Pro proces řízení bezpečnostních incidentů jsem navrhl model uvedený na obrázku č. 12. Jednotlivé aktivity jsou popsány pod uvedeným schématem.



Obrázek 13. Řízení bezpečnostních incidentů

1. **Ohlášení bezpečnostního incidentu**

Bezpečnostním incidentem se rozumí událost, která přímo nebo nepřímo může vést k narušení bezpečnosti informací z těchto pohledů:

- Dostupnost - například není dostupný server s důležitými daty zákazníka
- Integrita – například došlo k poškození dat na serveru a je ohrožena kompletnost dat zákazníka
- Důvěrnost – například byl ukraden/ztracen NB, na němž byly uloženy citlivé informace (smlouvy, databáze,…)

Výskyt bezpečnostního incidentu je povinen hlásit každý zaměstnanec organizace a to neprodleně telefonicky, případně emailem na pracoviště Call Centra.

Výstup:

- Výstupem této činnosti je telefonické nebo emailové oznámení výskytu bezpečnostního incidentu

2. Příjem a záznam bezpečnostního incidentu

Bezpečnostní incident je zaznamenán a je určena osoba, která je zodpovědná za řešení bezpečnostního incidentu. Dále jsou informování vedoucí všech oddělení ICT, na které by bezpečnostní incident mohl mít vliv a případně vedoucí projektu za stranu zákazníka, jestliže se bezpečnostní incident týká i zákazníka.

Výstup:

- Záznam bezpečnostního incidentu v Service Desk Manageru

3. Analýza bezpečnostního incidentu

Bezpečnostní incident je prvotně analyzován. Zaměstnanec popíše kdy, za jakých činností narazil na BI, řešitel BI provede prvotní analýzu příčin a ohledání případných odchylek od požadovaného stavu systému, které mohli způsobit BI, zaznamená tyto stopy.

Výstup:

- Záznam pro detailnější analýzu a návrh opatření

4. Řešení bezpečnostního incidentu

Osoba zodpovědná za řešení bezpečnostního incidentu přímo incident vyřeší nebo použije náhradní řešení (jestliže existuje). Jestliže je použito náhradní řešení, je nutné incident „regulérně“ vyřešit. Do záznamu o bezpečnostním incidentu zaznamená potřebné údaje.

Osoba zodpovědná za řešení bezpečnostního incidentu, je oprávněna v případě, kdy nemůže bezpečnostní incident vyřešit (např. nemá potřebné zdroje, pravomoci, není ji poskytnuta součinnost), řešení bezpečnostního incidentu eskalovat. Bezpečnostní incident se eskaluje Security managerovi, jestliže to není možné, pak řediteli Synot ICT Services.

Výstup:

- Záznam o řešení bezpečnostního incidentu

5. **Zhodnocení škody**

   Security Manager provede zhodnocení škod, které byly způsobeny bezpečnostním incidentem. Metrikou jsou finanční náklady na vyřešení bezpečnostních incidentů a především škodu jakou bezpečnostní incident způsobil organizaci

   Výstup:

   - Záznam o způsobených škodách

6. **Návrh opatření a implementace**

   Security Manager určí, zda je nutné pro uzavření bezpečnostního incidentu zpracovat nové nebo upravit současné preventivní nebo nápravné opatření. Pokud ano, řešitel bezpečnostního incidentu navrhne opatření vedoucí k zamezení opakování tohoto BI a navrhne postup implementace nových opatření. Člen vedení společnosti a Security manager rozhodne, zda je návrh opatření vzhledem ke způsobeným škodám adekvátní a rozhodne o implementaci opatření.

   Výstup:

   - Návrh opatření a postup implementace

7. **Uzavření bezpečnostního incidentu**

   Za přezkoumání a uzavření bezpečnostního incidentu je zodpovědný Security manager společně s dalšími osobami z vedení společnosti, kterých se incident týká.

   Výstup:

   - Uzavřený bezpečnostní incident

8. **Monitorování průběhu řešení jednotlivých bezpečnostních incidentů**

   Řešení bezpečnostních incidentů je průběžně monitorováno. Může docházet například k přiřazení jiných priorit, eskalacím apod.

   Výstup:

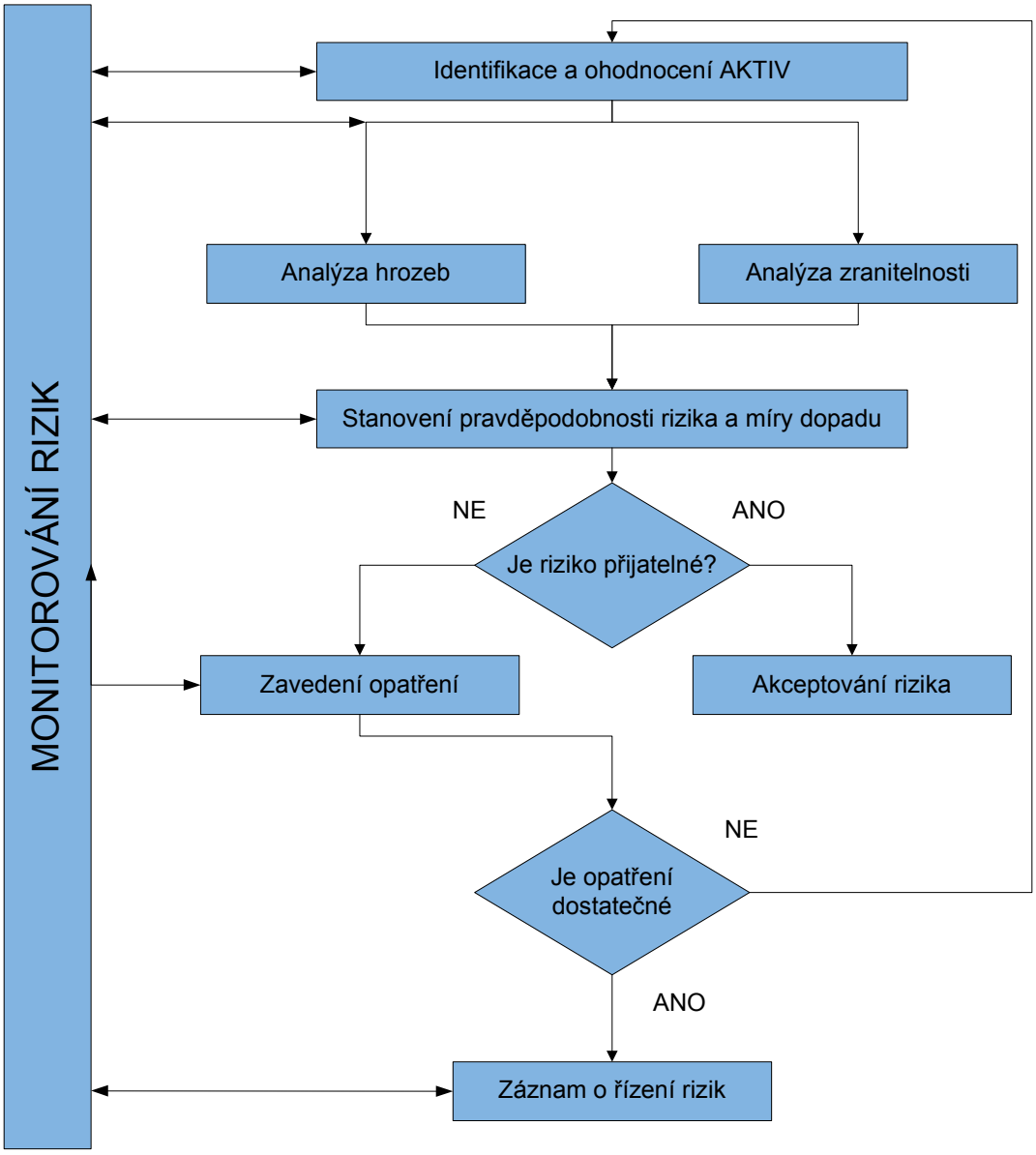
   - Korektní opatření

5.2 Proces řízení rizik

Cílem je zajistit, aby v organizaci byla řízena rizika, která mají vliv na bezpečnost informací při poskytovaní servisních služeb zákazníkovi.

- Vstupy procesu: Aktiva, rizika
- Výstupy procesu: Záznam o řízení rizik

Pro proces řízení rizik jsem navrhl model znázorněný na obr. č. 13.



Obrázek 14. Řízení rizik

1. **Identifikace a ohodnocení aktiv**

   Odpovědná osoba, pravděpodobně člen vedení organizace, definuje kritická aktiva a provede jejich ohodnocení. Ostatní aktiva definuje člen vedení společnosti a taktéž je ohodnotí.

   Výstup:

   - Záznam aktiv a jejich ohodnocení

2. **Analýza hrozeb**

   Ze seznamu obecných hrozeb vybereme hrozby týkající se našich aktiv, popřípadě definujeme hrozby specifické. Vypracujeme matici, která bude zachycovat faktory důležité k hodnocení jednotlivých hrozeb.

   Výstup:

   - Seznam hrozeb a pravděpodobnost výskytů

3. **Analýza zranitelnosti**

   V tomto kroku definujeme zranitelnosti na úrovni fyzické, komunikační, organizační a logické. Každé zranitelnosti přiřadíme stupeň zranitelnosti.

   Výstup:

   - Seznam zranitelných míst a určení stupně zranitelnosti

4. **Stanovení pravděpodobnosti rizika a míry dopadu**

   Na základě AR a AZ stanovíme pravděpodobnost výskytu rizika a míru dopadu.

   Výstup:

   - Seznam rizik, pravděpodobnosti výskytu a míra dopadu

5. **Akceptování rizika**

   Sem budou zahrnuty rizika přijatelné a zbytkové, na které nebudou uvolněny prostředky pro jejich zmírnění či odstranění.

   Výstup:

   - Seznam přijatých rizik

6. Zavedení opatření

Zavedení opatření vedoucí ke snížení míry rizika. Vypracování havarijních plánů, plánů obnovy.

Výstup:

- Havarijní plány, Plán obnovy

7. Záznam o řízení rizik

Zaznamenávání změn prováděných v oblasti řízení rizik.

Výstup:

- Záznam řízení rizik

5.3 Bezpečnostní dokumentace

ISO 20000 klade důraz na vedení dokumentace politik a jednotlivých procesů. Ne jinak tomu je v managementu bezpečnosti informací. V rámci této oblasti bylo nezbytné vytvořit a uvést v platnost bezpečnostní politiku a bezpečnostní směrnice.

5.3.1 Bezpečnostní politika

Bezpečnostní politika je hlavním dokumentem, který zastřešuje veškeré procesy a směrnice v oblasti managementu bezpečnosti informací. Tento hlavní dokument byl vypracován v návaznosti na provedení podrobné analýzy v oblasti bezpečnosti IT a analýzy rizik. Jak již bylo zmíněno, analýza bezpečnosti IT byla prováděna externí firmou. Analýza rizik byla prováděna bezpečnostním managerem a pracovníky jednotlivých oddělení. Jelikož dokument Výsledky analýzy rizik je klasifikován jako důvěrná informace, seznámeni s ní mohou být jen vybraní zaměstnanci společnosti.

Dokument Bezpečnostní politika je klasifikována jako informace veřejná a z toho vyplývá, že je veřejně přístupná. Celý dokument je uveden v příloze Diplomové práce.

5.3.2 Bezpečnostní směrnice

Bezpečnostní směrnice byly vypracovány za účelem stanovení jasných pravidel, kterými se zaměstnanci společnosti musí řídit. Navazují na bezpečnostní politiku a jasně definují,

kterými oblastmi bezpečnosti je nezbytné se zabývat. Stanovují bezpečnostní procesy a povinnosti, které se musí plnit. Na rozdíl od bezpečnostní politiky se jedná o dokument klasifikovaný jako interní informace, tudíž není možné ji zveřejnit široké veřejnosti.

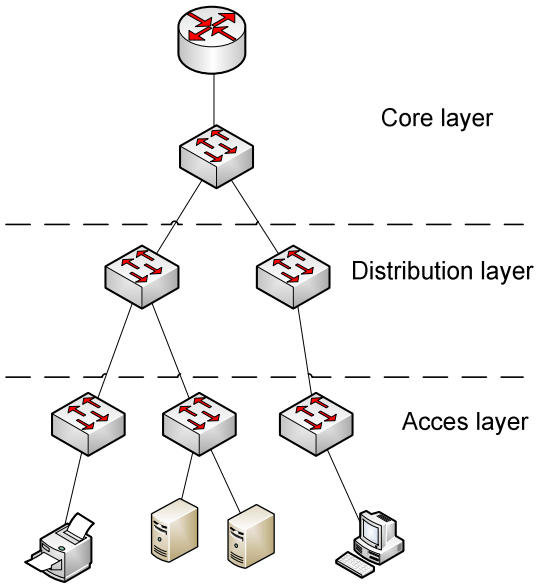
5.4 Komunikační bezpečnost

Síťová infrastruktura je velmi důležitou součástí při poskytování ICT služeb. Pro zajištění dostupnosti služeb a dodržení nastavených smluv se zákazníkem je nezbytné mít síť na úrovni tomu odpovídající, ještě lépe tyto potřeby přesahující.

5.4.1 Hierarchický síťový model

Síť byla vybudována na principu hierarchického síťového modelu zobrazeného na obr. níže. Hierarchický síťový model je rozdělen do tří vrstev, přičemž každá splňuje svůj účel a je třeba dbát na dodržení potřebných parametrů.

- Páteřní vrstva (Core layer)
    - Kritická vrstva – připojení konektivity
    - Nezbytná redundance
    - Vysoká přenosová rychlost
- Distribuční vrstva (Distribution layer)
    - Nezbytná redundance
    - Agregační vrstva mezi páteřní a přístupovou vrstvou
- Přístupová vrstva (Access layer)
    - Přístupové místo do sítě
    - Připojení koncových zařízení (PC, telefony, servery, AP, atd)
    - Nutná aplikace bezpečnostních pravidel
    - Monitorování připojených zařízení, zda některé není neoprávněně připojeno do sítě

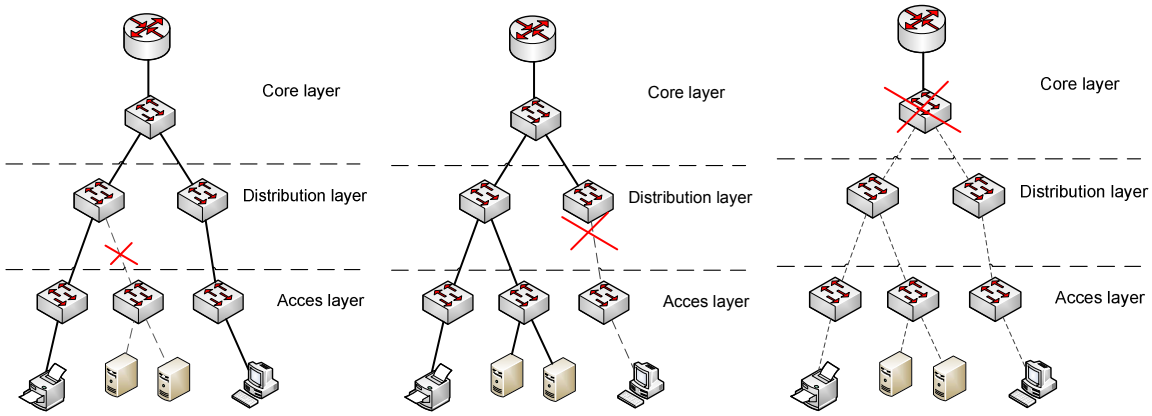


Obrázek 15. Hierarchický síťový model

5.4.2 Redundance

Vysoká dostupnost byla jedním z hlavních požadavků na novou síťovou infrastrukturu. Z tohoto důvodu bylo nutné celou infrastrukturu navrhnout tak, aby v případě selhání prvku či trasy nedošlo k výpadku poskytovaných služeb. Pokud ve schématu, zobrazenému na obr. č. 14, dojde k výpadku některého ze zařízení, či tras, nastane výpadek v datové komunikaci. Jedná se o velmi závažnou hrozbu.

Selže-li prvek, či trasa na daném místě, celá větev umístěná od tohoto bodu směrem k přístupové vrstvě je bez konektivity. Budeme-li se bavit o prvku, či trase umístěné v distribuční, nebo přístupové vrstvě, bude nedostupná „pouze“ část sítě. Za předpokladu, že jsou zde umístěny servery, tak budou nedostupné. Bude-li se jednat o část sítě, kde jsou umístěni uživatelé, nebudou mít dostupnost do internetu a ani do žádných interních systémů umístěných za tímto bodem. Přestane-li fungovat komunikace na úrovni páteřní vrstvy, celá síť bude nefunkční.



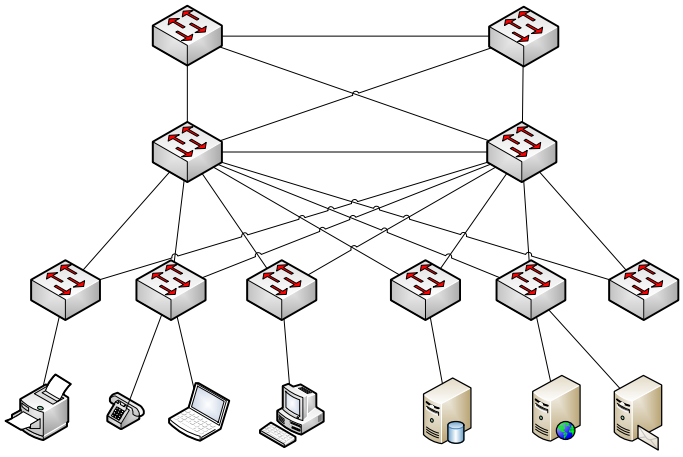
Obrázek 16. Výpadek v síti

Dostupné trasy jsou znázorněny plnou černou čarou, nedostupné trasy jsou znázorněny přerušovanou čarou. Místo výpadku je označeno červeným křížkem.

Rizikem v tomto případě je nedostupnost služeb. Snížit ho musíme vhodným opatřením vůči těmto hrozbám:

- Výpadek trasy
- Selhání HW

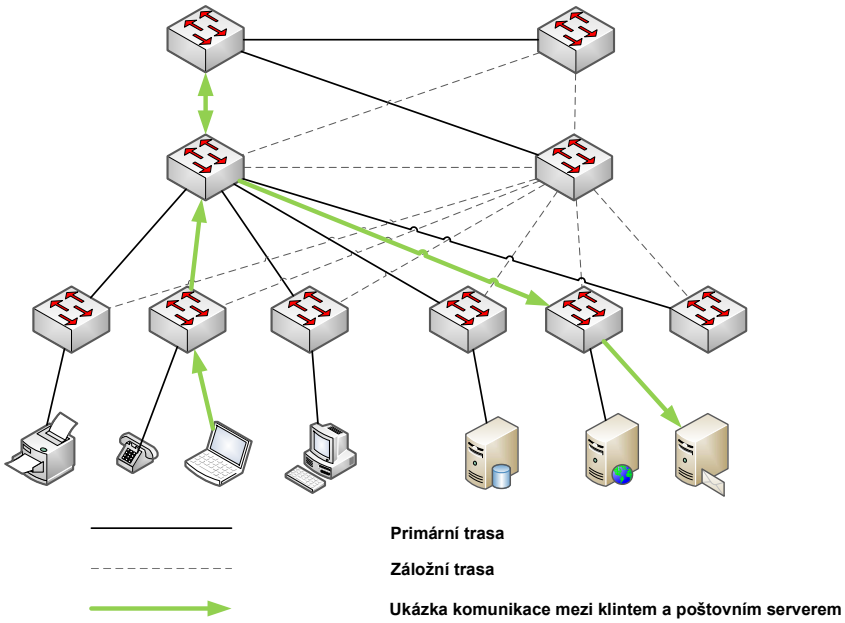
Opatřením v našem případě je umístění redundantních prvků a vybudování záložních komunikačních tras.



Obrázek 17. Redundance

Takovým zapojením však vytváříme v síti smyčky, které jsou nežádoucí, jelikož způsobují broadcastové bouře. Abychom dosáhli požadovaného stavu, musíme správně

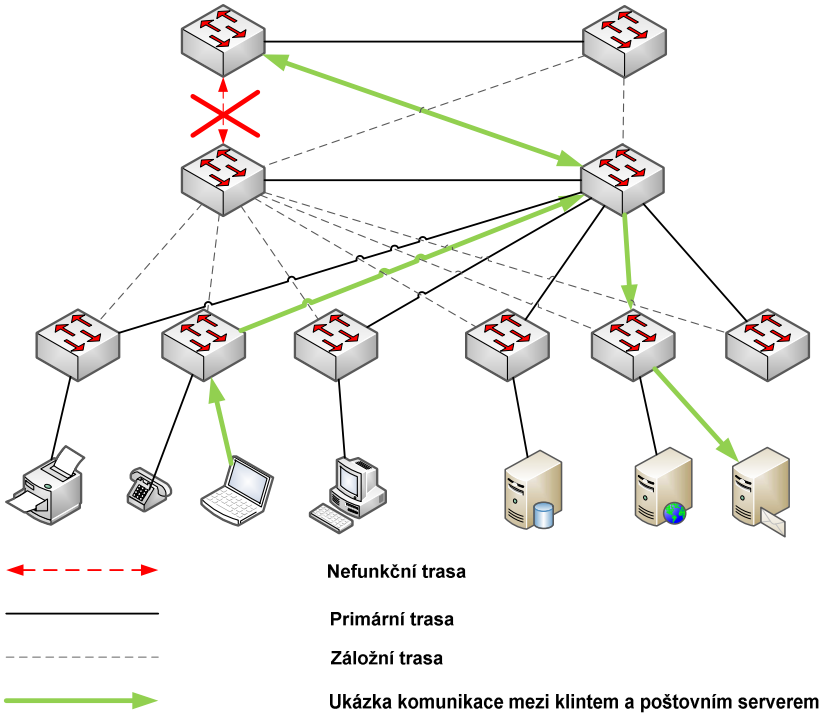
nakonfigurovat jednotlivé switche. Zařízení Cisco k zabránění vzniku smyček v síti, používá Spanning Tree Protokol (STP). V síti definujeme tzv. root switch. K tomuto prvku se vypočítá nejlepší cesta ze všech aktivních prvků pomocí STA (spanning tree algorithm). K datové komunikaci jsou využívány pouze tyto trasy. Ostatní cesty jsou nedostupné, jelikož STP příslušné fyzické porty na zařízení uvede do stavu blokace. Popsaná situace je graficky znázorněna na obr. č. 17.



Obrázek 18. STP-Primární trasa

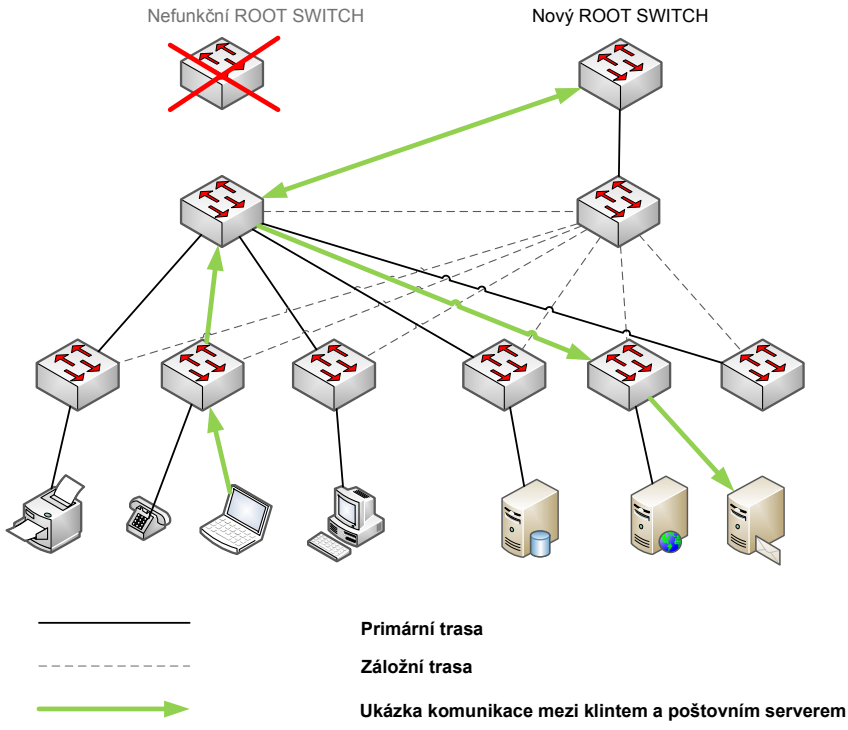
Primární cesta vypočtená STP je znázorněna plnou černou čarou. Přerušované trasy znázorňují trasy, které jsou ve stavu blokace. Zeleně znázorněná trasa, je ukázka komunikace mezi klientem a Poštovním Serverem.

Vypadne-li trasa, nebo zařízení, STP opět vypočítá pomocí STA nejvýhodnější cestu do root switche.



Obrázek 19. Selhání trasy

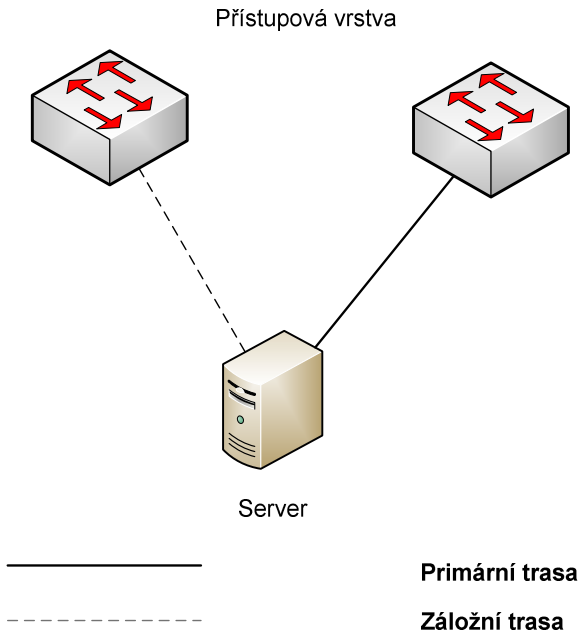
Pokud selže root switch, STP určí podle priorit jiný prvek root switchem a k tomu opět vypočítá nejlepší trasu ze všech zařízení.



Obrázek 20. Selhání HW

Poskytované služby běží na serveru. Jak vidíme na obrázku č. 19, servery jsou připojeny pouze jednou trasou z jednoho acces switche. Pro minimalizaci rizika je nezbytné ještě zajistit dostupnost i v případě selhání HW, nebo trasy na úrovni přístupové vrstvy.

Předpokladem tohoto řešení je, že server má dvě síťové karty. Každá síťová karta je připojena do jiného acces switche.



Obrázek 21. Redundance na přístupové vrstvě

ZÁVĚR

Cílem diplomové práce bylo zpracovat obecný přehled problematiky řízení bezpečnosti informací. Na úvod bylo zhodnoceno, zda je řízení bezpečnosti v organizacích věnována adekvátní pozornost. Zjistili jsme, že problematika bezpečnosti informací se v oblasti ICT zařadila mezi nejvíce probíraná témata současnosti. Na téma bezpečnost v ICT jsou zaměřeny spousty konferencí. Bezpečnost je probírána z různých úhlů pohledů, přičemž jsou představovány jednotlivé možnosti opatření vůči konkrétním hrozbám. Objasnili jsme pojem informace a dozvěděli se, jakým životním cyklem prochází. Každá fáze vyžaduje specifický přístup k zajištění ochrany dat. Zjistili jsme, že celkový proces bezpečnosti informací se skládá z fyzické bezpečnosti, organizační bezpečnosti, komunikační bezpečnosti, personální bezpečnosti a logické bezpečnosti. Každým z těchto způsobů, zajišťující bezpečnost dat, je nezbytné se adekvátně zabývat. Musíme si uvědomit, že celý systém je tak bezpečný, jak je bezpečný jeho nejslabší článek.

Zavedení procesu řízení informační bezpečnosti je projekt, který nám zabere řádově několik měsíců. Pokud se vedení společnosti rozhodne zavést proces řízení informační bezpečnosti, je vhodné vybrat některý z vyzkoušených standardů. Tyto standardy nám pomohou rychleji a lépe nastavit procesy, které bychom sami těžce vytvářeli. Nejprve je nutné provést důkladnou analýzu bezpečnosti v organizaci. Z výsledků se dozvíme, na jaké úrovni je ochrana dat v příslušné organizaci. Zjistíme, na které oblasti se musíme zaměřit více a na které méně. Dále je potřeba definovat obchodní cíle, aktiva a provést analýzu rizik. V návaznosti na provedení analýzy rizik stanovíme bezpečnostní politiku a vytvoříme bezpečnostní směrnice.

Cílem praktické části byla problematika implementace informační bezpečnosti v organizaci poskytující ICT služby. Společnost se rozhodla zavést normu ISO/IEC 20000, přičemž jednou z oblastí této normy je právě management bezpečnosti informací. V rámci této oblasti bylo nutné nastavit procesy řízení rizik a bezpečnostní incidenty. Analýzu rizik následovalo vytvoření bezpečnostní politiky. Bezpečnostní směrnice byly vypracovány v návaznosti na bezpečnostní politiku.

Bezpečnostní rizika se budou objevovat stále více a útoky směřující na naše informace budou mnohem sofistikovanější. Je tedy nutné procesy týkající se bezpečnosti informací udržovat stále aktualizované a pokud možno je ještě zdokonalovat.

Předpokládám, že společnosti, které se touto problematikou nebudou zabývat, budou mít vážné existenční problémy. Ty mohou být způsobené jednak odlivem zákazníků, kteří dají přednost konkurenci, jež zaručuje bezpečné zacházení s daty. Jiné organizace mohou zcela zaniknout, což může být právě důsledek špatného nakládání s informacemi.

ZÁVĚR V ANGLIČTINĚ

The aim of this diploma thesis was to produce the general outline of the informatition security management. At the beginning it was evaluated if there si enough attention paid to the safety management in companies. We found out that the information security issues in the field of ICT belong among the most discussed topics. A lot of conferences are held in this topic. This topic is discussed in several different ways and individual possibilities are introduced. We cleared up the term „information“ and found out what is it´s life cycle. Each phase requires specific approach to the data protection. We found out that the whole process of the information security consists of the physical security, organisational security, communication security, personal security and logical security. All of these must be dealt with. We have to realize that the whole system is as safe as it is it´s weakest part.

The implementation of the information security management process is the project which will take several months. If the management of the company decides to implement this, it is suitable to choose one of the tested norms. These norms will help us to set the processes faster. At first it is neccessary to do the close analysis of the security in the company. From the results we will see the level of data protection. We will find out on which area we need to focus. It is also neccessary to define the aims of the business, find out the risks. Following the analysis of risks we will specify the security policy and create safety guidelines.

The aim of the practical part was the issue of information security implementation in the company providing ICT services. The company decided to implement ISO/IEC 20000. In this area it was neccessary to set the processes of the risks management and safety incidents. The analysis of the risks was followed by the creation of the safety policy. Then the safety guidelines were created.

Safety risks will appear more and more and the attacks on our information will be more and more sophisticated. So it is neccessary to update and improve the information security processes.

I assume that the companies which are not interested in this issue will face serious existencial troubles. These might be caused by the lower number of customers who will prefer the competitors which guarantee the safety of data. Other companies might come to an end which might be the result of the bad manipulation with data.

This diploma thesis deals with the issue of information security in companies providing ICT services. Individual possibilities of the information security will be solved. At the end of this work I will focus on implementation of the information security in the company providing ICT services.

SEZNAM POUŽITÉ LITERATURY

[3] *Bezpečnost v kostce* [online]. 2010 [cit. 2011-03-04]. Dostupné z WWW: <www.chrantesidata.cz>.

[2] PUŽMANOVÁ, Rita. *Moderní komunikační sítě od A do Z : Technologie pro datovou,hlasovou i multimediální komunikaci*. 2. aktualizované vydání. Brno : Computer Press, a.s., 2006. 430 s. ISBN 80-251-1278-0.

[3] STREBE, Matthew ; PERKINS, Charles. *Firewally a proxy-servery : Praktický průvodce*. Vydání první. Brno : Computer Press, a.s., 2003. 450 s. ISBN 80-7226-983-6.

[4] HORÁK, Jaroslav. *Bezpečnost malých počítačových sítí : praktické rady a návody*. První vydání. Praha : Grada Publishing, a.s., 2003. 200 s. ISBN 80-247-0663-6.

[5] NORTCUTT, Stephen, et al. *Bezpečnost sítí : Velká kniha*. Vydání první. Brno : CP Books, 2005. 589 s. ISBN 80-251-0697-7.

[6] LOCKHART, Andrew. *Bezpečnost sítí na maximum*. Vydání první. Brno : CP Books, 2005. 276 s. ISBN 80-251-0805-8.

[7] KABELOVÁ, Alena, et al. *Velký průvodce protokoly TCP/IP a systémem DNS : 3. aktualizované a rozšířené vydání*. První dotisk 3. aktualizovaného vydání. Brno : CP Books, 2005. 542 s. ISBN 80-7226-675-6.

[8] ŠEBESTOVÁ, Marie; VÁŇA, Vladimír; SEDLÁČEK, Miroslav . *Management služeb IT : Komentované vydání souboru ISO/IEC/DIS 20000:2004*. [s.l.] : ČNI, 2004. 65 s. ISBN 807283186-0.

[9] HUCABY, David; MCQUERRY, Steve. *Konfigurace směrovačů Cisco : Autorizovaný výukový průvodce*. Vydání první. Brno : Computer Press, a.s., 2004. 632 s. ISBN 80-722-6951-8.

[40] *Bezpečnost v kostce* [online]. 2010 [cit. 2011-03-04]. Dostupné z WWW: <www.chrantesidata.cz>.

[51] *SystemOnLine* [online]. 2010 [cit. 2011-03-09]. Dostupné z WWW: <http://www.systemonline.cz/it-security/bezpecnost-informaci-se-netyka-jen-it-firem-1.htm>.

[62] *SystemOnLine* [online]. 2010 [cit. 2011-03-09]. Dostupné z WWW: <http://www.systemonline.cz/it-security/zabezpeceni-malych-a-strednich-spolecnosti.htm>.

[73] *Autocont* [online]. 2010 [cit. 2011-02-27]. Dostupné z WWW: <http://www.autocont.cz/sluzby-ebs-infrastruktura-bezpecnostict.cml>.

[84] Systém řízení bezpečnosti informací. *Wiki* [online]. 5.11.2010, 1, [cit. 2011-03-09]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Syst%C3%A9m_%C5%99%C3%ADzen%C3%AD_bezpe%C4%8Dnosti_informac%C3%AD>.

[95] DOUČEK, Petr. *Česká společnost pro systémovou integraci* [online]. 2005 [cit. 2011-03-09]. Česká společnost pro systémovou integraci. Dostupné z WWW: <http://www.cssi.cz/cssi/bezpecnostni-incidenty-ict-jejich-reseni>.

[106] *ZnámOdpověď.cz* [online]. 15.1.2011 [cit. 2011-03-09]. Co je Bezpečnost informačního systému?. Dostupné z WWW: <http://www.znamodpoved.cz/co-je-bezpecnost-informacniho-systemu/>.

[117] ČERMÁK, Miroslav. *Clever and smart* [online]. 2010 [cit. 2011-03-17]. Informační bezpečnost: životní cyklus informace. Dostupné z WWW: <http://www.cleverandsmart.cz/informacni-bezpecnost-zivotni-cyklus-informace/>.

[128] ČERMÁK, Miroslav . *Clever and smart* [online]. 2010 [cit. 2011-03-17]. CIA: Důvěrnost. Dostupné z WWW: <http://www.cleverandsmart.cz/duvernost/>.

[139] ČERMÁK, Miroslav . *Clever and smart* [online]. 2010 [cit. 2011-03-17]. CIA: Dostupnost. Dostupné z WWW: <http://www.cleverandsmart.cz/dostupnost/>.

[20] *CORPORATE ICT* [online]. 2010 [cit. 2011-03-23]. Opomíjená, leč kritická: personální bezpečnost. Dostupné z WWW: <http://www.corporateict.cz/11/01/1-bezpecnost-vs-naklady/opomijena-lec-kriticka-personalni-bezpecnost.html>.

[21] HABRMAN, Robert. *OWEBU.cz* [online]. 2007 [cit. 2011-03-23]. Síťové protokoly (I. část) - Model OSI. Dostupné z WWW: <http://owebu.bloger.cz/PC-site/Sitove-protokoly-I-cast-Model-OSI>.

[22] ČERMÁK, Miroslav . *Clever and smart* [online]. 2010 [cit. 2011-04-13]. CIA: Analýza-rizik-jemný-úvod-do-analýzy-rizik. Dostupné z WWW: < http://www.cleverandsmart.cz/analyza-rizik-jemny-uvod-do-analyzy-rizik/>.

[23] ČERMÁK, Miroslav. *Clever and Smart* [online]. 2009 [cit. 2011-04-13]. Analýza rizik: kvantitativní vs. kvalitativní. Dostupné z WWW: <http://www.cleverandsmart.cz/analyza-rizik-kvantitativni-vs-kvalitativni/>.

[24] ČERMÁK, Miroslav. *Clever and smart* [online]. 2010 [cit. 2011-04-15]. Analýza rizik: Jak stanovit hodnotu dopadu?. Dostupné z WWW: <http://www.cleverandsmart.cz/analyza-rizik-jak-stanovit-hodnotu-dopadu/>.

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

[26] *BPM téma* [online]. 2007 [cit. 2011-04-15]. Případová studie analýzy rizik informační bezpečnosti. Dostupné z WWW: <http://bpm-tema.blogspot.com/2007_11_01_archive.html>.

[27] ČERMÁK, Miroslav. *Clever and Smart* [online]. 2010 [cit. 2011-04-15]. ITIL tajemství zbavený. Dostupné z WWW: <http://www.cleverandsmart.cz/itil-tajemstvi-zbaveny/>.

[28] Iso27000 [online]. 2010 [cit. 2011-04-17]. ISO/IEC 27001:2005 . Dostupné z WWW: <http://www.iso27000.cz/rac/homepage.nsf/CZ/27001>.

[29] *GamePark* [online]. 2010 [cit. 2011-04-28]. Sociální inženýrství. Dostupné z WWW: <http://www.gamepark.cz/nejlepsi_socialni_inzenyr_v_dejinach_kevin_mitnick_360890.htm>.

[30] ČERMÁK, Miroslav. *Clever and Smart* [online]. 2010 [cit. 2011-05-16]. Integrita. Dostupné z WWW: <http://www.cleverandsmart.cz/integrita/>.

[31] *Chrante si data* [online]. 2010 [cit. 2011-05-16]. ISMS nebo ITIL?. Dostupné z WWW: <http://www.chrantesidata.cz/cs/art/1155-dil-8/>.

[32] *Akela.mendelu* [online]. 2009 [cit. 2011-05-22]. Bezpečnost IS/IT. Dostupné z WWW: <https://akela.mendelu.cz/~lidak/bis/11prot.htm#1>.

[33] *Presstv* [online]. 1.4.2011 [cit. 2011-05-22]. Pentagon networks threatened by cyber attack . Dostupné z WWW: <http://www.presstv.ir/usdetail/172613.html>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AP	Acces point (přístupový bod k bezdrátové síti)
AR	Analýza rizik
CD	Compact Disk (kompaktní disk)
DVD	Digital Versatile Disc (Digitální víceúčelový disk)
FW	Firewall
HDD	Hard Disc Drive (Pevný disk)
HW	Hardware (Technické vybavení počítače)
ICT	Informační a komunikační technologie
IL	Information Lifecycle (Životní cyklus informace)
IS	Informační systém
ISO	Mezinárodní organizace pro standardizaci
ITIL	Knihovna infrastruktury informačních technologií
LAN	Lokální počítačová síť
MAN	Metropolitní síť
PDCA	Plánuj, Dělej, Kontroluj, Jednej
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SLA	Smlouva o úrovni/kvalitě poskytovaných služeb
STA	Spanning Tree Algorithm
STP	Spanning Tree Protocol
SW	Software (Programové vybavení)
WAN	Wide Area Network (Rozsáhlá počítačová síť)

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Bezpečnostní politika

PŘÍLOHA P I: BEZPEČNOSTNÍ POLITIKA

Bezpečnostní politika

Obsah

1) Všeobecné prohlášení k bezpečnostní politice

Synot ICT Services a.s. si uvědomuje významnou hodnotu a důležitost informací, které jsou ve společnosti zpracovávány, uchovávány a sdíleny. Proto je z pohledu Synot ICT Services a.s. (dále jen Synot) nezbytné řídit proces bezpečnost informací. Informace je nutné zabezpečit proti zneužití, zcizení, narušení dostupnosti, integrity a důvěrnosti.

Informace jsou významnými aktivy Synot ICT Services a.s. Všichni zaměstnanci a smluvní pracovníci firmy Synot (dále jen zaměstnanci) jsou odpovědní za ochranu informací. K jejímu zajištění vytvoříme patřičné bezpečnostní mechanismy k ochraně před úmyslným či neúmyslným zničením, ztrátou, zcizením a vyzrazením. Přístupové práva k jednotlivým aktivům budou zabezpečeny a přiděleny konkrétnímu zaměstnanci stejně jako odpovědnost za daná aktiva.

Zdroje a zařízení informačních systémů Synot budou využívány pouze pro určené pracovní účely. Každý zaměstnanec je odpovědný za dodržování zásad, uvedených v tomto dokumentu, vztahujících se k jeho působnosti.

Synot si je vědom povinností plynoucích z procesu řízení bezpečnosti informací, významem procesu pro svou činnost, stejně jako nezbytnosti soustavného zdokonalování, vyvíjení a aktualizace procesu vedoucí ke stavu splňující požadavky legislativní, potřeby zákazníků, partnerů.

2) Administrativa a plnění bezpečnostní politiky

Plnění bezpečnostní politiky společnosti Synot je vyžadováno vedením organizace, která stanovuje povinnost zaměstnanců jednat v souladu tohoto dokumentu a rozšiřujících dokumentů, kterými jsou bezpečnostní směrnice, postupy.

Bezpečnostní směrnice, postupy je třeba podrobně rozpracovat v rozšiřujících dokumentech dostupných zaměstnancům společnosti.

3) Odpovědnost vedení a zaměstnanců

Ochrana všech informačních aktiv, jako počítačový hardware, aplikační a systémový software, data, dokumentace a zaměstnanci je klíčovou zodpovědností vedoucích pracovníků.

Vedoucí na všech úrovních jsou přímo odpovědní za to, že zajistí, aby si všichni zaměstnanci a smluvní pracovníci uvědomili své povinnosti ve vztahu k ochraně dat.

Vedoucí pracovníci jsou rovněž odpovědní za plnění bezpečnostních standardů a postupů. Všechny osoby, zaměstnanci a externí smluvní pracovníci se seznámí s bezpečnostní politikou, standardy a postupy a vědomě budou podporovat jejich naplnění.

Každý zaměstnanec potvrdí písemně, nezávisle na jeho pozici, že se seznámil a pochopil bezpečnostní politiku a standardy a postupy z ní vycházející.

4) Porušení bezpečnostní politiky a případné postihy

Porušením bezpečnostní politiky jsou události, nebo činnosti, které jsou v rozporu s touto strategií a odvozenými bezpečnostními standardy a postupy.

Všichni zaměstnanci jsou odpovědní za seznámení se s bezpečnostní politikou, souvisejícími směrnicemi a postupy, které se vztahují k jejich činnosti a za oznámení jakýchkoliv porušení bezpečnostní politiky.

5) Oznámení porušení bezpečnostní politiky

Synot si uvědomuje nezbytnost dodržování bezpečnostní politiky a stanovuje povinnost všem zaměstnancům ohlásit, dle způsobu určenému ve směrnicích, zjištěné počínání, které je v rozporu s bezpečnostní politikou, směrnicemi a postupy.

6) Postihy za porušení bezpečnostní politiky

Následkem porušení bezpečnostní politiky bude nápravné opatření vedení Synot. Postihy budou zohledňovat významnost přestupku, na základě prošetření.