

Návrh implementace bezpečnostní politiky v informačním a komunikačním systému vybrané firmy

Bc. Vladimíra Mandincová



Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

akademický rok: 2014/2015

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	Bc. Vladimíra Mandincová
Osobní číslo:	A13379
Studijní program:	N3902 Inženýrská informatika
Studijní obor:	Bezpečnostní technologie, systémy a management
Forma studia:	kombinovaná
Téma práce:	Návrh implementace bezpečnostní politiky v informačním a komunikačním systému vybrané firmy
Téma anglicky:	A Proposed Design for the Implementation of a Security Policy in an Information and Communication System in a Selected Company

Zásady pro vypracování:

1. Formou literární rešerše popište současný stav předmětné problematiky a úroveň jeho řešení v informačních zdrojích.
2. Vytvořte model informačního a komunikačního systému pro firemní prostředí a popište zásady tvorby bezpečnostní politiky z hlediska komplexního způsobu zabezpečení – systémové, fyzické, personální, atd.
3. Analyzujte bezpečnostní rizika pro vnější a vnitřní prostředí a na základě této analýzy navrhnete implementaci bezpečnostní politiky.
4. Provedte zobecnění/ doporučení pro postup při zvládání rizik – implementaci bezpečnostní politiky v objektech obdobného typu.

Rozsah diplomové práce: 69 strán

Rozsah příloh: 2 přílohy - 6 strán

Forma zpracování diplomové práce: tištěná/elektronická

Seznam odborné literatury:

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

Vedoucí diplomové práce:

doc. Ing. Jiří Gajdošík, CSc.

Ústav bezpečnostního inženýrství

Datum zadání diplomové práce:

12. ledna 2015

Termín odevzdání diplomové práce:

15. května 2015

Ve Zlíně dne 6. února 2015



doc. Mgr. Milan Adamek, Ph.D.
děkan



doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

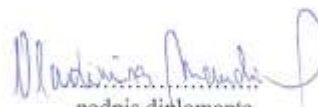
- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská 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 příjmem – tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považuji se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

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

Ve Zlíně

11.5.2015


podpis diplomanta

ABSTRAKT

Cieľom tejto diplomovej práce je poukázať na dôležitosť implementácie bezpečnostnej politiky v bezpečnostných systémoch v podnikoch. V teoretickej časti budem pojednávať o postavení a štruktúre bezpečnostnej politiky vo vzťahu k organizácii. V praktickej časti sa venujem samotnému návrhu implementovania bezpečnostnej politiky informačno-komunikačného systému a analýze jednotlivých častí.

Kľúčová slova: Informačné systémy, bezpečnosť, bezpečnostná politika,

ABSTRACT

The goal of this thesis is show the importance of the implementation of security policy in the security systems in enterprises. In the theoretical section, I will discuss the status and structure of the security policy of an organization. The practical part is focused on the very design of the implemented security policy area of information and communication system and analysis of its parts.

Keywords: Information systems, Security, Security Policy,

Chcem sa poďakovať všetkým, ktorí svojimi radami a pripomienkami veľmi prispeli k spracovaniu tejto diplomovej práce. Za odbornú konzultáciu a poskytnuté informácie ďakujem vedúcemu mojej diplomovej práce p. Doc. Ing. Jiřímu Gajdošíkovi CSc .

Ďakujem aj firme, v ktorej pracujem, hlavne pracovníkom z IT oddelenia, že mi umožnila nahliadnuť na funkčnosť informačného systému spoločnosti a do procesov, ktoré boli v práci použité.

Prehlasujem, že odovzdaná verzia diplomovej práce a verzia elektronická nahratá do IS/STAG sú totožné.

„Či už ide o Google alebo Apple alebo voľný softvér, máme úžasnú konkurenciu a to nás drží na nohách.“

Bill Gates

OBSAH

ÚVOD.....	8
I TEORETICKÁ ČÁST.....	9
1 INFORMAČNÉ TECHNOLOGIE.....	10
1.1 VYMEDZENIE POJMOV	11
2 BEZPEČNOSTNÁ POLITIKA	14
2.1 BEZPEČNOSŤ AKO POJEM	14
2.2 BEZPEČNOSTNÁ POLITIKA IT ORGANIZÁCIE	15
3 ISMS –INFORMATION SECURITY MANAGEMENT SYSTÉM	18
3.1 ŽIVOTNÝ CYKLUS ISMS.....	19
4 PRÁVNÝ RÁMEC SPOJENÝ S BEZPEČNOSTNOU POLITIKOU.....	22
4.1 ZÁKONY A VŠEOBECNE ZÁVÄZNÉ PRÁVNE PREDPISY PRI ZAVÁDZANÍ BEZPEČNOSTNEJ POLITIKY V ORGANIZÁCII.	22
4.2 PLÁN IMPLEMENTÁCIE NOVÝCH ALEBO DOPLŇUJÚCICH OCHRANNÝCH OPATRENÍ	23
4.2.1 Bezpečnostné normy	23
4.2.2 Bezpečnostné smernice	24
4.3 HAVARIJNÝ PLÁN A PLÁN OBNOVY IS	24
4.4 NOVELIZÁCIA NORIEM V ČESKEJ REPUBLIKE	25
II PRAKTICKÁ ČÁST	26
5 ZÁKLADNÁ CHARAKTERISTIKA SPOLOČNOSTI	27
5.1 ANALÝZA UMIESTNENIA ROZLOHY SPOLOČNOSTI.....	27
6 ANALÝZA SPOLOČNOSTI POMOCOU SWOT ANALÝZY	29
7 ZÁKLADNÁ CHARAKTERISTIKA BUDOVY.....	30
7.1 POŽIARNA ORGANIZÁCIA A SIGNALIZÁCIA BUDOVY.....	30
8 ANALÝZA ORGANIZAČNEJ ŠTRUKTÚRY SPOLOČNOSTI.....	32
8.1 PROCESNÉ RIADENIE SPOLOČNOSTI	33
8.2 ANALÝZA INTERNÉHO AUDITU SPOLOČNOSTI.....	35
8.3 ZHODNOTENIA A NÁVRH NÁPRAVNÝCH A PREVENTÍVNYCH OPATRENÍ.....	37
ZDROJ NO/PO.....	38
8.4 NÁVRH ZLEPŠOVACÍCH PROCESOV	39
9 ANALÝZA ŠTRUKTÚRY SPOLOČNOSTI Z HĽADISKA IT	40
9.1 ANALÝZA SW	40
9.1.1 Analýza procesov v jednotlivých produktových sadách.	41
9.1.2 Zhodnotenie softvéru Movex	42
9.2 PRÍSTUPY UŽÍVATEĽOV	42
9.2.1 LAN infraštruktúra	43
9.2.2 Kabeláž.....	43
9.3 MONITOROVANIE SIETE	44
9.3.1 Analýza monitorovania siete.....	44
9.3.2 Vyhodnotenie monitorovania siete	44

9.4	POUŽÍVANIE VÝPOČTOVEJ TECHNIKY	45
9.4.1	Analýza hardvérového vybavenia spoločnosti	45
9.4.2	Zhodnotenie hardvérového vybavenia	46
9.5	HESLÁ	46
9.5.1	Zhodnotenie používania hesiel	46
9.6	ZABEZPEČENIE ÚDAJOV	46
9.6.1	Zhodnotenie zabezpečenia údajov	47
9.6.2	Prístup k firemným údajom a k údajom zákazníkov	47
9.6.3	Bezpečnostné opatrenia voči neoprávnenému prístupu	47
9.7	POUŽÍVANIE INTERNETU	47
9.7.1	Prístup na internet	48
9.7.2	Zhodnotenie prístupu na internet	48
9.7.3	Bezpečnostné opatrenia pripojenia k internetu	48
9.8	POUŽÍVANIE ELEKTRONICKEJ POŠTY	48
9.8.1	Zhodnotenie využívania elektronickej pošty	49
9.9	POUŽÍVANIE ZÁZNAMU NA PRENOSNÉ MÉDIÁ	49
9.10	ANTIVÍROVÝ SOFTVÉR	49
9.10.1	Zhodnotenie softvéru	49
9.11	INTRANETOVÁ SIEŤ	50
9.11.1	Zhodnotenie intranetu v spoločnosti	50
9.11.2	Bezpečnostné opatrenia používania intranetu	50
10	NÁVRH IMPLEMENTÁCIE BEZPEČNOSTNEJ POLITIKY V PRÍPADE VZNIKU HAVÁRIE	52
10.1	TÍM NA REKONŠTRUKCIU INFRAŠTRUKTÚRY INFORMAČNÝCH TECHNOLOGIÍ	52
10.2	POSTUP PRI ODSTRANOVANÍ HAVÁRIE	53
10.3	STUPNE HAVÁRIÍ	53
10.4	KOMUNIKAČNÝ PLÁN	54
10.5	STUPEŇ OHROZENIA	55
10.6	ÚROVNE KRITÉRIÍ	56
10.7	SERVEROVŇA	57
10.7.1	Návrh testu LAN konektivity	58
10.7.2	Zhodnotenie ochrany serverovne	59
10.7.3	Návrh ochrany serverovne pred požiarom	59
11	IMPLEMENTÁCIA BEZPEČNOSTNEJ POLITIKY MIMO REŽIM HAVÁRIE	61
11.1	ZHODNOTENIE POSTUPOV PRI IMPLEMENTÁCII BEZPEČNOSTNEJ POLITIKY	61
	ZÁVER	63
	ZOZNAM POUŽITEJ LITERATÚRY	65
	ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK	66
	ZOZNAM OBRÁZKOV	67
	ZOZNAM TABULIEK	68
	ZOZNAM PRÍLOH	69

ÚVOD

Prirodzenou vlastnosťou ľudí je vnímanie bezpečnosti alebo nebezpečenstva na základe signálov, ktoré sa vyskytujú v jeho okolí. Zabezpečenie istoty života človeka v bezpečnej krajine s priaznivými podmienkami v súkromnej sfére, ale aj v zamestnaní chápeme ako nadôležitejšiu povinnosť. Svoju bezpečnosť chápajú aj podnikateľské subjekty v rôznych rovinách. Najčastejšie ju vnímajú z pozície ochrany svojho hmotného majetku, pričom podceňujú dôležitosť ostatných aktív. Pod pojmom bezpečnostná politika musíme brať do úvahy všetky opatrenia a činnosti, ktorými subjekt bezpečnosti zabezpečuje svoju ochranu tak, aby obmedzil a zabránil vzniku pôsobenia bezpečnostných ohrození, ktoré negatívne ovplyvňujú záujmy spoločnosti.

Cieľom tejto práce je objasniť miesto a úlohy bezpečnostnej politiky v podniku a navrhnúť jej možnú aplikáciu v podniku.

V prvej kapitole som sa venovala charakteristike základných pojmov ako je bezpečnosť, politika, bezpečnostná politika. Ďalšia kapitola je venovaná bezpečnostnej politike v podniku, kde som sa zaoberala právnymi aspektami, obsahom bezpečnostnej politiky. Ďalej som sa venovala metodike spracovania bezpečnostnej politiky, štruktúre a právomoci bezpečnostného manažmentu. V poslednej kapitole som sa zaoberala návrhom bezpečnostnej politiky podniku v prípade vzniku havárie vzhľadom k informačným technológiám, dosiahnutím bezpečnostného povedomia zamestnancov a spôsobom implementácie bezpečnostnej politiky.

I. TEORETICKÁ ČÁST

1 INFORMAČNÉ TECHNOLOGIE

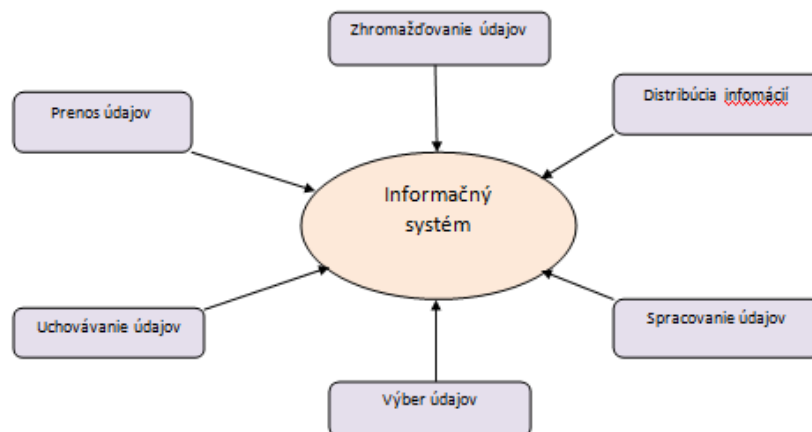
Úlohou informačných technológií je spracovávať stále viac a viac informácií s veľkou hodnotou. Pod pojmom spracovanie sa rozumie uchovávanie, prenos, spracovanie, zhromažďovanie a výber údajov, distribúcia informácií (Obr.č. : 1). Informácie majú často nezanedbateľnú hodnotu. Sú to strategické plány firiem, zdravotné záznamy, daňové priznania, bankové účty, rôzne elektronické platobné nástroje atď. V prípade, že sa informácie týkajú charakteristík dokumentov (názov, autori, heslá kníh...), hovoríme o dokumentačných systémoch. Používajú sa napr. v knižniciach. Ďalším prípadom sú riadiace informačné systémy, ktoré uchovávajú všetky veličiny a údaje, ktoré sú významné pre optimálne riadenie podnikania.

Dôvodov ochrany informácií je veľa :

- Prístup k informáciám mali iba oprávnené osoby
- Spracovávanie iba nesfalšovaných informácií
- Nezverejnenie nekontrolovaným spôsobom informácií
- Dostupnosť informácií iba vtedy, keď to je potrebné
- Zistenie , kto informáciu vytvoril, zmenil, odstránil.

Informačný systém je tvorený určitým aplikačným programom. Každý počítač zvyčajne má nainštalovaných viacej týchto programov. Aplikácia je zameraná na určitý druh činnosti a spracovanie informácie:

- Spracovanie textu (Word, Acrobat Reader, NotePad, ...)
- Grafické informácie (maľovanie, Photoshop, Adobe Illustrator, CorelDraw...)
- Multimediálne informácie (Windows Media player, Quick time video, ...)



Obr.č. : 1 Skladba informačného systému

Informácia je tovar, ktorý je možno ukradnúť. Nie je zaujímavé prepadať na uliciach, pri vysokých hodnotách sa krádeže medzibankového transferu dejú denne, priamo z účtov klientov. Preto je dôležité vedieť údaje chrániť. Existujú právne, morálne pravidlá, zákonné úpravy na ochranu údajov (bankový zákon, daňový zákon, zákon o zdravotnom poistení, o ochrane osobných údajov, o ochrane utajovaných skutočností...) [2]

1.1 Vymedzenie pojmov

Informatika

Definíciu informatiky ako moderné ponímanie podľa Američan society for Information Science:

„Informatika je veda, ktorá sa zaoberá vznikom, vyhľadávaním, zhromažďovaním, prenosom, organizáciou, ukladaním, rozširovaním, spracovaním a využívaním informácií s osobitným zreteľom na používanie výpočtovej techniky v týchto oblastiach.“

Informácia

- Akýkoľvek údaj, poznatok, čo nejakým spôsobom vnímame.
- Zahrňuje v sebe správu, ktorá je pre prijímateľa dôležitá. Je to správa vyjadrujúca istý stav, slúži nejakému cieľu alebo vyvoláva nejakú akciu.

- Správa sa stáva informáciou z dôvodu ľudskej interpretácie alebo , že je spracovaná algoritmom, alebo že je uložená v súboroch.

Informácia má dve základné charakteristiky:

- možno ju merať - jej množstvo (kvantitu)

má svojho adresáta - pre ktorého môže, ale nemusí mať význam. Z tohto hľadiska ju delíme na: užitočné a neužitočné. [2]

Formy informácie môžeme deliť na:

- **Analógové** – vytvárané, prenášané, spracovávané a uchovávané inak ako za pomoci výpočtovej techniky
- **Digitálne** - vytvárané, prenášané, spracovávané a uchovávané v elektronickej forme.
- **Digitalizácia** - Digitalizácia je proces, pri ktorom sa analógové informácie (alebo údaje) prevádzajú na digitálne. To znamená, že každému údaju sa priradí určitý počet bitov čiže jedinečná kombinácia jednotiek a núl. Toto priradenie musí byť také, aby sa údaj z digitálnej podoby dal jednoznačne pretransformovať späť do analógového tvaru

Komunikácia - komunikovať (z lat. communicatus) znamená dorozumieť sa, odovzdať a prijať, vzájomne si vymieňať informácie, preniesť a šíriť, sprístupniť a spájať sa. Aby sme mohli komunikovať a posúvať informácie ďalej , musíme ich najprv zbierať. [2]

Existujú rôzne formy komunikácie:

- Ústna komunikácia , pošta, telefón, telegraf, mobil, rádio, noviny, televízia, fax, e-mail, internet.

Komunikovať cez internet sa dá dvoma spôsobmi:

- **Neinteraktívna komunikácia** sa uskutočňuje medzi ľuďmi vtedy, keď nemôžu okamžite jeden na druhého reagovať. To znamená, že vypovedané alebo vyslané informácie jednou osobou sa dostanú k adresátovi až po istom čase (napr. listová komunikácia, telefónne odkazovače, e-mail...).
- **Interaktívna komunikácia** (s možnosťou okamžitej reakcie). Pri tomto spôsobe komunikácie je odosielateľ pripojený na Internet v tom istom čase ako prijímateľ a

môžu medzi sebou bezprostredne komunikovať (napr. textovo, hlasom, príp. sa môžu navzájom aj vidieť). Interaktívnu komunikáciu umožňujú špeciálne programy – textové telefóny (prenos textu), alebo videokonferenčné programy (prenos zvuku a obrazu, napr. Talk, Skype, ICQ, ...).

Údaj - je každá správa bez ohľadu na to, či má pre nás nejaký informačný obsah alebo nie. Sú to správy, ktoré vyjadrujú určité fakty o procesoch, alebo prvkoch reálneho sveta. Údajom môžeme označiť písmená, čísla, slová, znaky, prípadne ich kombinácie. Všetky tieto údaje nesú určitý informačný obsah. V prípade ,ak nám daný údaj nepovie nič nového, hovoríme, že jeho informačný obsah je nulový. [2]

Dáta - sú všetky informácie alebo ich časti v digitálnej forme, ktoré sa dajú spracovať. Dátami sú informácie, ktoré sú nositeľmi významu pre ľudí. Informácia je teda produkt, výstup spracovania správ.

Symbol - je určitý rozlíšiteľný prvok správy (údaj). Pokiaľ má symbol určité grafické znázornenie hovoríme mu **znak**.

Ak chceme správu preniesť alebo zaznamenať musí mať správa nejakého fyzikálneho nositeľa. Jedna a tá istá správa môže byť vyjadrená rôzne, pomocou rôznych abecied.

Abeceda- je to množina prvkov, slúžiaca k zobrazeniu správy. Abeceda nie je viazaná na žiadnu fyzikálnu podstatu je to abstrakcia.

Hardvér - technické vybavenie počítača, čiže všetky jeho pevné časti vzájomne poprepájané a spolu tvoria jeden celok, ktorým je počítač.

Softvér - programové vybavenie počítača. Informačné technológie zahŕňajú všetky prostriedky (najmä hardware, software a know-how) slúžiace k využívaniu, získavaniu, spracovaniu, prenosu, prezentácii a uchovaniu dát a informácií. [2]

Dôležité úlohy informačného systému:

- manažérske (EIS - Executive IS), (MIS - Management IS),
- taktické (DSS - Decision Support System),
- kancelárske (OIS - Office IS),

V súčasnosti chápeme informačné systémy ako automatizované, je to integrovaný celok hardwaru, softwaru a dát, kde významnú úlohu hrá personál (peopleware), ktorý s informačným systémom pracuje.

2 BEZPEČNOSTNÁ POLITIKA

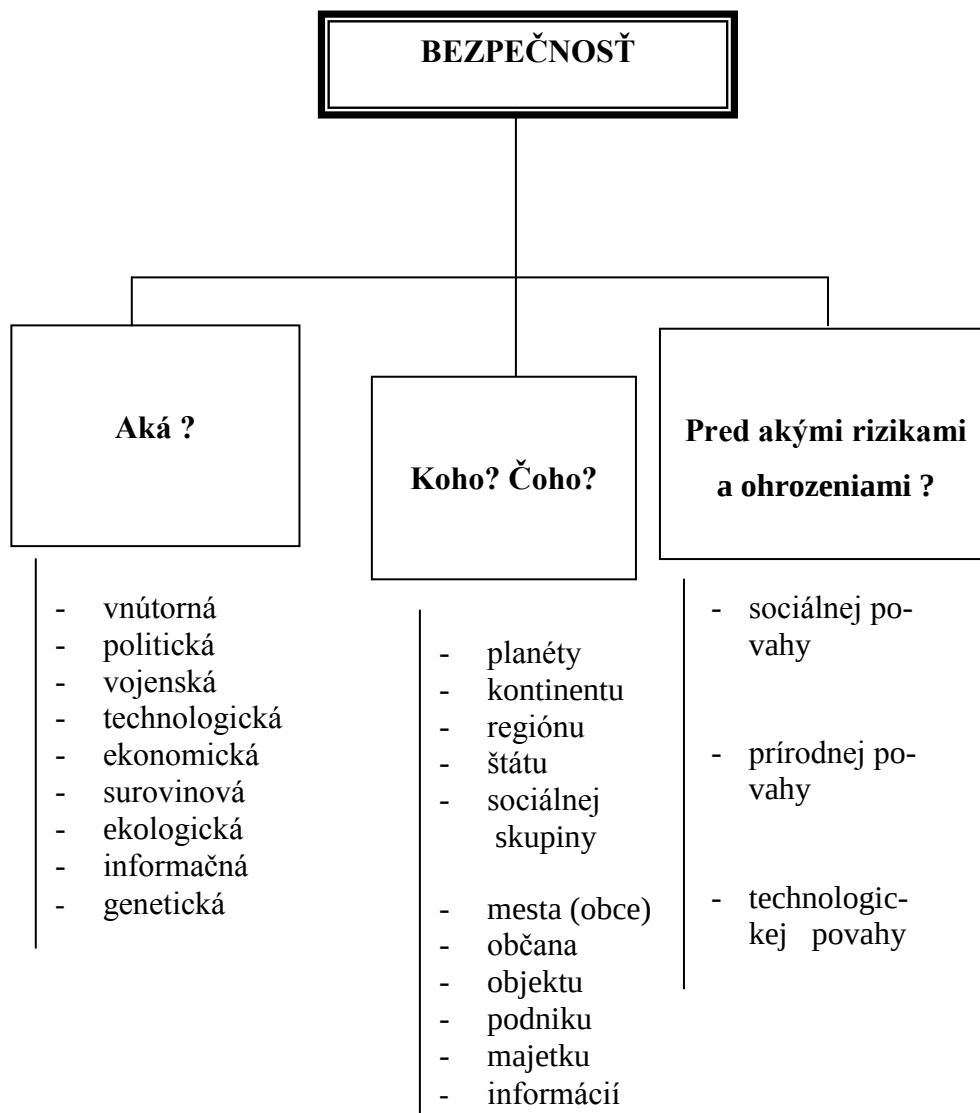
Definovanie pojmu bezpečnosť je veľmi zložitá, pretože má široký obsah. Viacerí autori ho vysvetľujú v závislosti od oblasti ich pôsobenia. Bezpečnosť je chápaná ako jedna z najsilnejších ľudských potrieb. V modernej dobe znamená bezpečnosť oveľa viac, ako vojenskú silu na odradenie vonkajších a vnútorných ohrození. V súčasnom svete je ťažšie stanoviť hranice medzi vnútornou a vonkajšou bezpečnosťou. Odstránenie bariér, či už politických, alebo administratívnych medzi niektorými štátmi umožnili voľný pohyb nielen osobám, ale aj peniazom a rôznym tovarom. Definíciu pojmu bezpečnosť nachádzame v slovníkoch, odborných článkoch, či zákonoch. Pojem bezpečnosť rôzne vysvetľujú vojači, politici, sociológovia a právnici. [3]

2.1 Bezpečnosť ako pojem

Bezpečnosť – „(lat. securitas, angl. security, nem. Sicherheit - bezstarostnosť, bezpečnosť, istota, ale aj duševný pokoj, ochrana, zabezpečenie, určitosť, nespornosť) - znamená stav, v ktorom je zachovaná vnútorná bezpečnosť a poriadok, demokratické základy štátu, jeho suverenita a integrita a je chránené životné prostredie“ [8].

V kontexte „súkromnej bezpečnosti“, resp. „súkromných bezpečnostných služieb“ je najvšeobecnejšia definícia bezpečnosti vyjadrená takto: „Bezpečnosť je ochrana života a zdravia osôb, ochrana majetku všetkého druhu pred stratami, ktoré by mohli vzniknúť v dôsledku nehody, krádeže, podvodu...“ [9]

Bezpečnosť má vnútorný a vonkajší rozmer. Vnútorná bezpečnosť je založená na interpretácii vlastného stavu subjektu. Vonkajšia bezpečnosť je založená na pôsobení rôznych ochranných prvkov spoločenského života. Je nevyhnutné ju však vnímať, posudzovať i navonok prezentovať spoločne ako komplexný mnohorozmerný jav, súvisiaci s ochranou života, slobody a majetku občanov (Hofreiter, 2002). V bežnej i odbornej praxi sa výraz bezpečnosť používa s rôznymi prívlastkami, napr. vonkajšia a vnútorná bezpečnosť, vojenská bezpečnosť, ekonomická bezpečnosť, informačná bezpečnosť. (Obr.č. : 2).



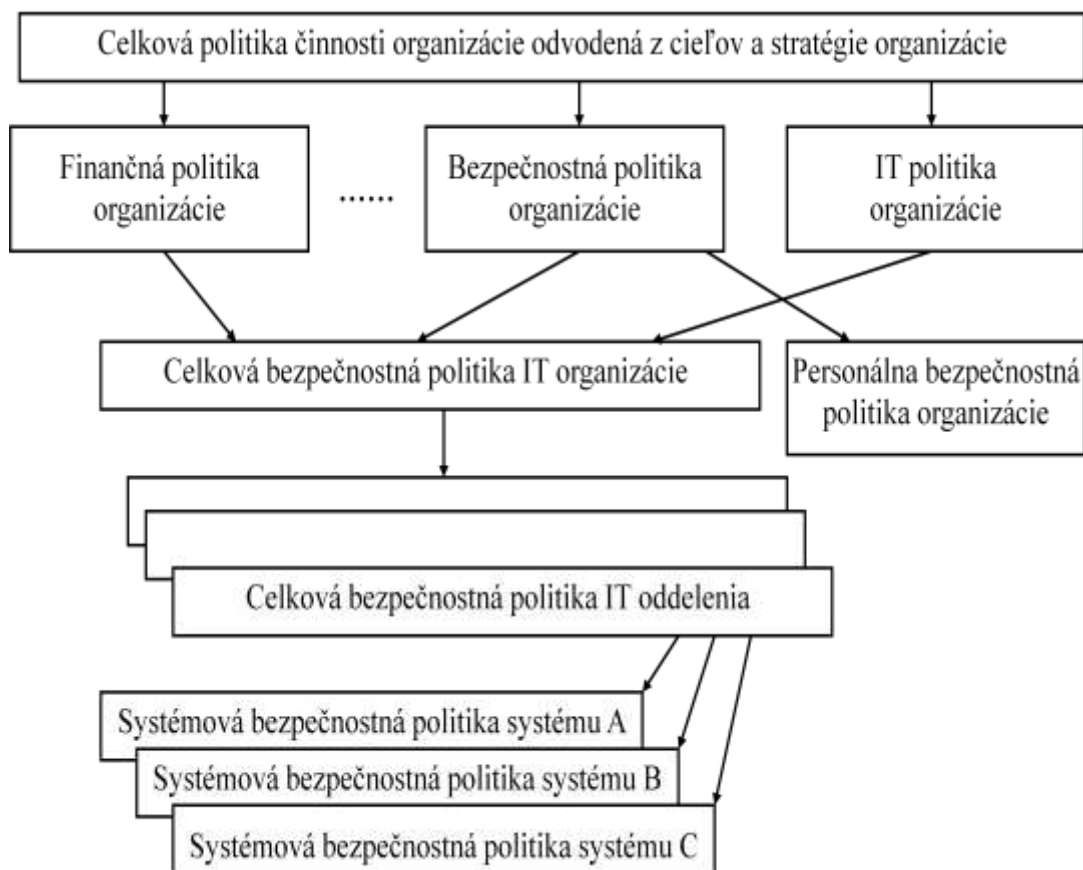
Obr.č. : 2 Možný obsah a štruktúra pojmu bezpečnosť [8]

2.2 Bezpečnostná politika IT organizácie

Bezpečnostná politika IT organizácie je odvodená od z cieľov a stratégie organizácie. Definuje spôsob zabezpečenia organizácie jako celku, od fyzickej ochrany, cez ochranu súkromia až po ochranu ľudských práv. (Obr.č. : 3) Zahrňuje :

- Výber bezpečnostných zásad a predpisov
- Definuje bezpečné používanie informačných systémov v rámci organizácie
- Detailné normy, pravidlá, praktiky , predpisy definujúce spôsob správy, ochrany, distribúcie citlivých informácií a iných IT zdrojov v rámci organizácie.

- Špecifikáciu bezpečnostných opatrení a spôsob ich implementácie
- Určenie spôsobu použitia celkovej bezpečnostnej politiky IS.



Obr.č. : 3 Schéma bezpečnostnej politiky organizácie . [9]

Informačná bezpečnosť

Bezpečnosť informácií predstavuje ochranu informácií a informačných systémov pred zneužitím, neoprávneným prístupom, zmenou alebo zničením. Proces dosiahnutia a udržiavania dôvernosti, integrity, dostupnosti a účtovateľnosti, authenticity, spoľahlivosti informácií na primeranej úrovni pomôžu zabezpečiť, technologické a manažérske štandarty- normy, tak aby boli údaje správne chránené, bezpečné a k dispozícii. [9]

Bezpečnosť IT systémov

Zabezpečenie výpočtového systému spočíva v udržaní troch základných vlastností :

Dôvernosť(Confidentiality)

- K aktívam prístupujú iba oprávnené osoby
- Typy prístupov môžu byť –čítanie, tlačenie, iba informácia o existencii objektu

- Utajenosť , privátnosť údajov

Integrita (Integrity)

- Aktíva môžu byť modifikované iba predpísaným spôsobom

Dostupnosť (Availability)

- Aktíva sú dostupné iba oprávneným entitám.
- Oprávnenej entite nesmie byť bránené v prístupe k aktívam, ku ktorým má oprávnenie prístup.

Ďalšími bezpečnostnými vlastnosťami sú autentickosť, nepopierateľnosť , účtovateľnosť.

Generické hrozby výpočtových systémov

Pod pojmom hrozba si treba predstaviť potenciálnu možnosť využitia zraniteľného miesta, spôsobenie škody na aktívach IS alebo ich strate. Hrozby môžeme kategorizovať do dvoch skupín:

Objektívne hrozby

- Prírodné – požiar , povodeň
- Fyzické – výpadok napájania, poruchy

Subjektívne hrozby

- Úmyselné
 - vonkaší útočník (špióny, teroristi, kriminálne živly)
 - vnútorný útočník (prepustený ,nahnevaný ,chamtivý , vydieraný zamestnanec)
- Neúmyselné
 - neškolený používateľ/administrator
 - chyba , omyl

Aby sme predchádzali vzniku hrozby v systéme, je nutné pomocou analýzy vyhľadať zraniteľné miesta. Nedokonalou implementáciou bezpečnostného mechanizmu riadenia prístupu hrozí strata dôvernosti, integrity, má celkovo nepriaznivý dopad na organizáciu.

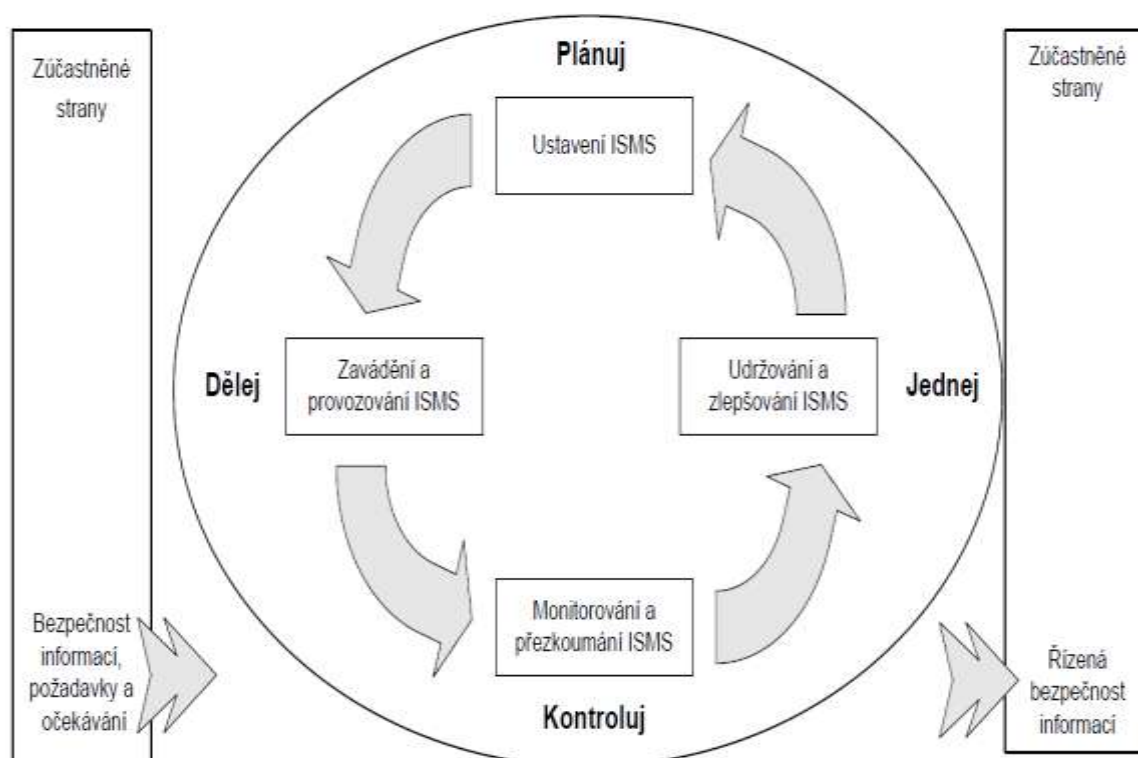
[8]

3 ISMS –INFORMATION SECURITY MANAGEMENT SYSTÉM

ISMS je efektivní systém řízení a správy informačních aktiv, cílem je eliminovat jejich možnou stratu nebo poškození tím, že :

- SÚ identifikované aktiva ,které sa majú chrániť
- SÚ zvolené a riadené možné riziká bezpečnosti informácií
- SÚ zavedené opatrenia s požadovanou úrovnou záuk a tie sú následne kontrolované.

ISMS sa môže zaviesť pre organizačnú zložku spoločnosti, informačný systém alebo jeho časť ,popřípadě může zahrňat celú organizáciu.Zavedenie systému řízení bezpečnosti informácií (ISMS) je strategickým rozhodnutím vedení společnosti. Tento systém využívají organizace bez ohledu na jejich velikost, pro které jsou informace a informační technologie klíčovou součástí podnikatelských procesů, nebo které zpracovávají citlivá data svých klientů a mají potřebu zajistit jejich bezpečnost.



Obr.č. : 4 ISMS Procesný přístup[11]

Procesný prístup

Procesný prístup je postavený na myšlienke ,že akákoľvek činnosť, ktorá vyžaduje zdroje a je riadená tak, aby premenila vstupy na výstupy, je považovaná za proces. V ISMS je tento prístup používaný bežne a nazýva sa Demingov cyklický model PDCA. Znamená – Plan - plánuj, Do- rob, Check- kontroluj , Act- konaj .(Obr.č. : 4)

3.1 Životný cyklus ISMS

Plan – fáza pre analyzovanie danej situácie v organizácii. Definuje sa oblasť pôsobenia a politiky ISMS tak, že :

- Stanovia sa zásady a ciele bezpečnosti informácií v danej oblasti
- Zhodnotia sa záväzky, ktoré plynú zo zmlúv a zo zákonov
- Nastavia sa kritériá, podľa ktorých budú hodnotené riziká
- Politika ISMS musí byť schválená vedením organizácie
- Definuje sa systematický prístup k hodnoteniu rizík a vytvoria sa podmienky pre akceptovanie rizík .

Identifikujú sa riziká

- Určíme aktíva v rámci ISMS a ich vlastníkov,
- definujeme hrozby, ktoré aktívam hrozia a aké zraniteľnosti môžu byť pomocou hrozieb využité.

Identifikujú sa a zhodnotia rôzne varianty pre zvládanie rizík

- Spravíme rozhodnutia, či budú riziká odstránené vhodným opatrením, akceptované alebo bude prenesená zodpovednosť na tretiu stranu (poisťovne, dodávatelia) .

Pripravlia sa Prehlásenia o aplikácii

- Je to vytvorenie dokumentu, ktorý obsahuje súhrn všetkých opatrení, ktoré boli pre ISMS vybraté, alebo zamietnuté aj s odôvodnením tohoto rozhodnutia,
- následne vedenie organizácie musí odsúhlasiť navrhované zbytkové riziká a opatrenia, verifikovať a uviesť do prevádzky ISMS.[11]

Do – prebieha implementácia plánov, ktoré boli vytvorené vo fáze Plan. V tejto fáze úlohou organizácie je :

- Stanovenie formálneho plánu na zvládanie rizík
- Implementácia tohto plánu a opatrení tak, aby boli dosiahnuté stanovené ciele opatrení.
- Určenie spôsobu, ako merať opatrenia, aby boli výsledky porovnateľné.
- Zaistiť programy školenia a informovania zamestnancov
- Riadiť prevádzku ISMS
- Aplikovať postupy a opatrenia pre rýchlu detekciu a reakciu na bezpečnostné incidenty.

Check – monitorovanie a preskúmavanie ISMS

V tejto časti je úlohou organizácie :

- Neustále monitorovanie procesu, testovanie a audit ISMS v bežnej prevádzke vrátane,
- dokumentovania dôkazných materiálov, kontroly plnenia bezpečnostnej politiky, merania účinnosti zavedených opatrení,
- preskúmavanie hodnotenia rizík, zbytkového a akceptovaného rizika pri zmene ISMS,
- pravidelné vykonávanie interných auditov,
- skúmanie dôkazných materiálov,
- aktualizácia bezpečnostných plánov podľa výsledkov monitorovania a preskúmavania,
- záznam všetkých činností a udalostí, ktoré mohli by mať dopad na chod ISMS [11]

Act – prijatie opatrení na odstránenie chýb a následne treba dbať o neustále zlepšovanie ISMS.

V tejto fáze je úlohou organizácie :

- Zaviesť zlepšenie ISMS a zaručiť, že týmito zlepšovacími procesmi budú dosiahnuté stanovené ciele,
- aplikovať nápravné a preventívne činnosti pre správny chod ISMS.

Výhody ISMS

Systém riadenia bezpečnosti informácií je vhodné zaviesť pre zníženie zbytočne vynaložených nákladov organizácie na opakujúci sa nesystematické zaobchádzanie s rizikami.

ISMS nám poskytuje zaručené postupy ako zaobchádzať s informáciami, ktoré sa využívajú po celom svete k minimalizácii rizík, ktoré hrozia informačným aktívam.

Zároveň je ale použiteľná pre všetky typy organizácií, nakoľko poskytuje ucelené postupy pre celý životný cyklus systému, od naplánovania, cez preskúmanie až po vylepšenie. [11]

4 PRÁVNÝ RÁMEC SPOJENÝ S BEZPEČNOSTNOU POLITIKOU

Pri aplikovaní bezpečnostnej politiky by mali byť nastavené procesy tak, aby ich cieľom bolo zníženie pravdepodobnosti výskytu hrozby. Z právneho hľadiska sa jedná o súhrn definovaných smerníc, podľa ktorých, by sa mali zamestnanci, ale aj osoby nachádzajúce sa v určitom vzťahu s organizáciou správať a nadobudnutím určitého právneho stavu sa zaviazat' k napĺňovaniu uvedených pravidiel.

4.1 Zákony a všeobecne záväzné právne predpisy pri zavádzaní bezpečnostnej politiky v organizácii.

Pri riešení bezpečnostnej politiky z komplexného pohľadu, by malo viesť k poznaniu jednotlivých právnych úprav danej oblasti, ktorej sa venuje podnikateľský subjekt. V prípade, že sa jedná o podnik z viacerými odvetviami podnikateľských aktivít, je potreba na daný subjekt pozerat' z pohľadu systému, ktorý je tvorený zo subsystémov spĺňajúce uvedené právne predpisy a zároveň musia spĺňať predpisy týkajúce sa ich pôsobenia z hľadiska vzájomných väzieb. [8]

V tomto prípade do pozornosti prichádzajú zákony :

- Zákon č.428/2002 Z.z. o ochrane osobných údajov
- Zákon č. 90/2005 Z.z. Zákon ktorým sa mení a dopĺňa zákon č. 428/2002 Z.z. o ochrane osobných údajov v znení neskorších predpisov
- Zákon 363/2005 Z.z. Úplné znenie zákona č. 428/2002 Z.z. o ochrane osobných údajov
- Listina Základných ľudských práv a slobôd vydaná v Zbierke zákonov č.23/1991 Zb.
- Ústava SR (Ústavný zákon), čl. 19 ods. 2 a 3
- Dohovor RE č. 108 o ochrane jednotlivcov pri automatizovanom spracúvaní osobných údajov spolu s dodatkami, bol ratifikovaný SR 24. augusta 2000
- Dodatokový protokol k Dohovoru 108

4.2 Plán implementácie nových alebo doplňujúcich ochranných opatrení

Plán implementácie nových alebo doplňujúcich ochranných opatrení definuje pravidlá a opatrenia, ktoré sa musia prijať aby mohli byť v praxi implementované navrhované ochranné opatrenia čo najúčinnnejšie. Plán implementácie obsahuje najmä:

- priority jednotlivých navrhovaných ochranných opatrení,
- časový rozvrh implementácie vo vzťahu k prioritám,
- potrebný finančný rozpočet,
- zodpovednosť jednotlivých pracovníkov,
- spôsob vytvorenia povedomia o bezpečnosti medzi užívateľmi a postupy pre bezpečnostné školenia,
- časový rozvrh pre postupy odsúhlasenia tam, kde je to potrebné.

4.2.1 Bezpečnostné normy

„Norma“ je technická špecifikácia schválená uznávaným normalizačným orgánom pre opakované alebo stále používanie, ktorej používanie však nie je povinné. Bezpečnostné normy určujú pravidlá používania technických prostriedkov, prístupové a správčovské práva, organizačnú štruktúru, rozdelenie zodpovedností a právomocí a celkový proces ochrany aktív IS. [6] [10]

Zoznam dôležitých noriem pre informačné technológie:

- STN ISO/IEC 17799 Informačné technológie. Kódex praxe manažérstva informačnej bezpečnosti,
- STN ISO/IEC TR 13335-1 Informačné technológie. Návod na manažérstvo bezpečnosti IT. Časť 1: Koncepcie a modely bezpečnosti IT,
- STN ISO/IEC TR 13335-2 Informačné technológie. Návod na manažérstvo bezpečnosti IT. Časť 2: Riadenie a plánovanie bezpečnosti IT,
- STN ISO/IEC TR 13335-3 Informačné technológie. Návod na manažérstvo bezpečnosti IT. Časť 3: Techniky pre manažment bezpečnosti IT,
- STN ISO/IEC TR 13335-4 Informačné technológie. Návod na manažérstvo bezpečnosti IT. Časť 4: Výber bezpečnostných opatrení.

- STN ISO/TR 13569 – Bankovníctvo a príbuzné finančné služby. Pokyny pre informačnú bezpečnosť.
- ISO/IEC 27 001 Informačné technológie. Manažérsky systém informačnej bezpečnosti.
- (STN ISO/IEC TR 13 335 Informačné technológie. Návod na manažérstvo bezpečnosti IT.)
- STN ISO/IEC 15 408 Informačné technológie. Bezpečnostné techniky. Kritériá na hodnotenie bezpečnosti IT.
- ISO/IEC DIS 21 827 Informačné technológie. Bezpečnostné inžinierstvo systémov. Model vyspelosti schopností. [7]

4.2.2 Bezpečnostné smernice

- popis technických, organizačných a personálnych opatrení vymedzených v bezpečnostnom projekte a ich využitie v konkrétnych podmienkach, rozsah oprávnení a popis povolených činností jednotlivých oprávnených osôb, spôsob ich identifikácie a autentizácie pri prístupe k informačnému systému,
- rozsah zodpovednosti oprávnených osôb a osoby zodpovednej za dohľad nad ochranou osobných údajov,
- spôsob, formu a periodicitu výkonu kontrolných činností zameraných na dodržiavanie bezpečnosti informačného systému,
- postupy pri haváriách, poruchách a iných mimoriadnych situáciách vrátane preventívnych opatrení na zníženie vzniku mimoriadnych situácií a možností efektívnej obnovy stavu pred haváriou.

4.3 Havarijný plán a plán obnovy IS

Havarijný plán nám definuje, čo robiť po odhalení útoku (bezpečnostného incidentu) a ako postupovať. Súčasťou havarijného plánu je najmä :

- miesta skladovania a počty náhradných dielov,
- miesta skladovania a spôsob organizácie záloh dát,
- obsah pohotovostného skladu technických a softvérových náhrad,

- metodiku udržiavania aktuálnosti dát, softvéru a hardvéru,
- metodiku aktualizácie a testovania hardvéru.
- zadenfinovanie spôsobu vyhlásenia a zrušenie havarijného stavu,
- návody ako postupovať v poskytovaní služieb po zistení útoku (plán činnosti po útoku – Contingency Plan).

Vyhlásenie a zrušenie havarijného stavu – nám vysvetľuje, čo je to havarijný stav, kto a za akých podmienok ho vyhlasuje a akým spôsobom. Taktiež nám definuje, kedy havarijný stav sa končí a kto ho má právo zrušiť.[8]

4.4 Novelizácia noriem v Českej republike

V Českej republike nastal ten istý proces ako v Slovenskej republike. Na základe novelizácie noriem a boli akceptované normy rady 27000.

1. ČSN ISO/IEC 27000 Systémy řízení bezpečnosti informací - Přehled a slovník
2. ČSN ISO/IEC 27001 Systémy managementu bezpečnosti informací – Požadavky
3. ČSN ISO/IEC 27003 Směrnice pro implementaci systému řízení bezpečnosti informací
4. ČSN ISO/IEC 27004 Řízení bezpečnosti informací – Měření
5. ČSN ISO/IEC 27005 Řízení rizik bezpečnosti informací
6. ČSN ISO/IEC 27006 Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací

Tak ako Slovenská republika, je vidieť, že i Česká republika prevzala normy z medzinárodných normalizačných organizácií. Česká republika má prijatých podstatne viac noriem rady z uvedenej rady 27000. Slovensko má zjednotené 3 normy .

II. PRAKTICKÁ ČÁST

5 ZÁKLADNÁ CHARAKTERISTIKA SPOLOČNOSTI

Spoločnosť sa radí medzi svetových lídrov v technologickej inovácii a vývoji aplikácií spájania plastov. Používa jedinečnú kombináciu technologických inovácií a vývoja aplikácií v oblastiach dizajnu, vývoja, výroby a marketingu spájania plastov, využitím ultrazvukových procesov.

Spoločnosť je globálne orientovaná, vo svete má viac ako 70 predajných a servisných kancelárií. Technologické a výrobné zariadenia sú rozmiestnené na viacerých kontinentoch, v štátoch : USA, Mexiku, Nemecku, na Slovensku, v Číne, Hong Kongu, Japonsku a Kórei.

Súčasťou rozsahu produktov sú systémy pre ultrazvukové spájanie, lineárne a orbitálne vibračné zvarovanie, zvarovanie taviacim telesom, infračervené a laserové zvarovanie. Sú navrhnuté podľa potrieb pracovišť, od strojov na vstupnej úrovni až po plne automatizované výrobné systémy. Konkrétne plánujeme a navrhujeme, vyvíjame, konštruujeme, inštalujeme, automatizujeme a dopravujeme vždy s dôrazom na váš prínos. To preto, že všetky naše technológie sledujú jediný cieľ: zvýšiť a udržať vašu konkurencieschopnosť.

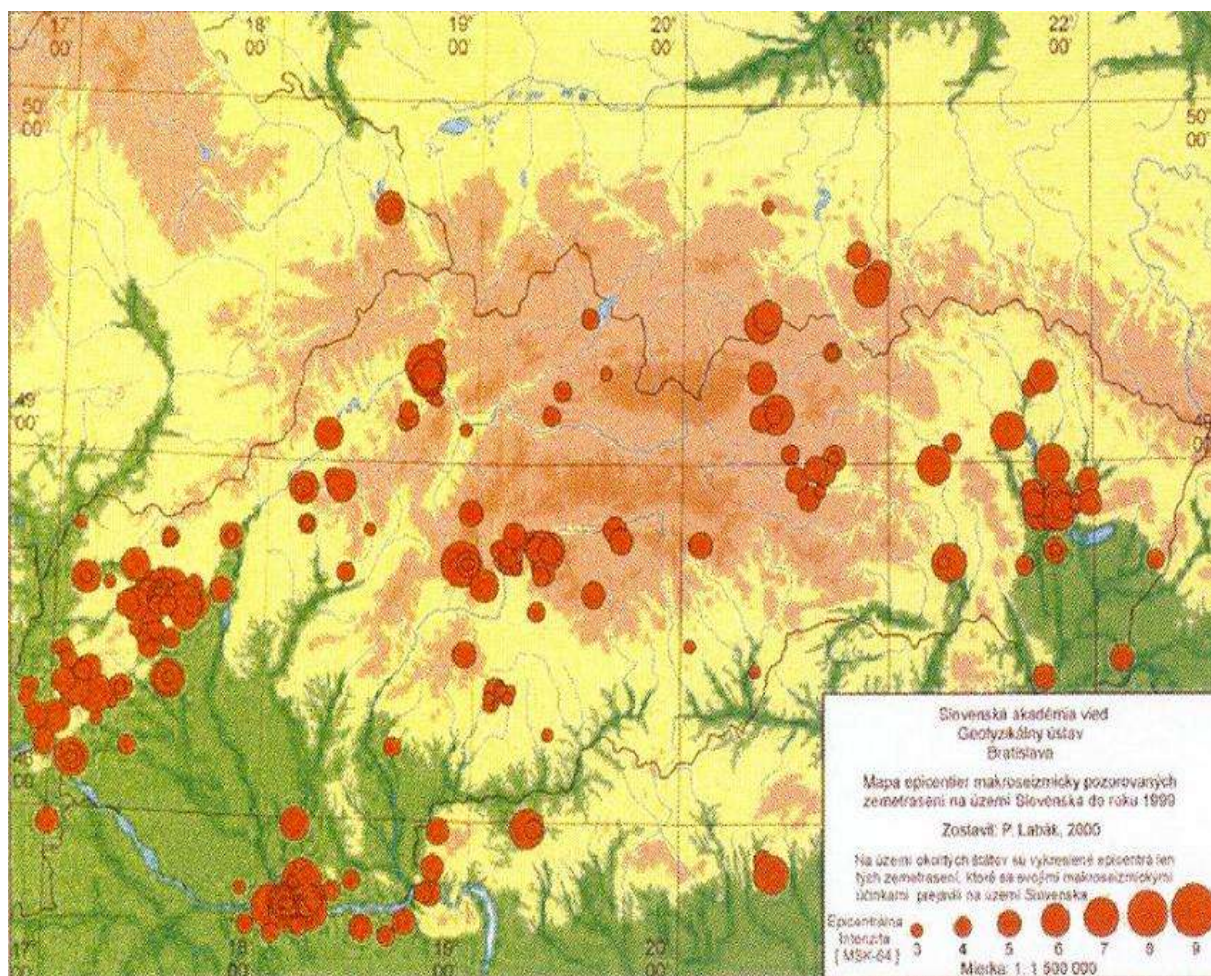
5.1 Analýza umiestnenia rozlohy spoločnosti

Nové Mesto nad Váhom je súčasťou Trenčianskeho regiónu, ktorý je jedným z ôsmich administratívnych regiónov Slovenskej republiky. Trenčiansky región leží na západe Slovenska pri rieke Váh.

Hydrogeologické pomery sú dané geologickou stavbou územia. Kolektorom podzemnej vody sú štrkopiesčité sedimenty so súvislou nádržou podzemných vôd s voľnou hladinou v hĺbke priemerne okolo 5.5m pod terénom. Vodný tok rieky Váh prevažne infiltruje podzemné vody údolnej nivy. Podzemné vody sú v priamej závislosti na vodách vodného toku.

Trenčín neleží, ako vidieť na obrázku, v seizmicky aktívnej oblasti a ani blízka rieka Váh nie je ohrozením pre prípadné zaplavenie serverovne. (Obr.č. : 5)

Jadrová elektrárň leží približne 60 km od spoločnosti, tiež nie je potenciálnym ohrozením.



Obr.č. : 5 Geofyzikálna mapa Slovenskej republiky

6 ANALÝZA SPOLOČNOSTI POMOCOU SWOT ANALÝZY

Spoločnosť sa opiera sa o dlhoročnú tradíciu vývozu využitím znalosti slovenského trhu a potrieb slovenských partnerov. Existencia ponuky výrobkov s optimálnym pomerom ceny ku kvalite. Schopnosť kombinovať vývoz s vyššími formami spolupráce, vrátane výrobnéj a technologickej kooperácie a zakladanie spoločných podnikov; schopnosť predávať a využívať skúseností z reštrukturalizácie slovenského priemyslu a skúsenosti so získavaním zahraničných investorov; dobrá pozícia vo vybraných regiónoch.

Silné stránky

- Firma má záujem na rozvoji vzájomných hospodárskych vzťahov a tomu odpovedajúca tvorba, využíva a zdokonaľuje súbor finančných a nefinančných nástrojov na podporu vývozu.

Slabé stránky

- pretrvávajúce predsudky pri spracovávaní trhu, v niektorých prípadoch spojené s negatívnymi skúsenosťami,
- príliš veľká orientácia výroby na automobilový trh a v prípade hospodárskej krízy problém s odberateľmi.

Príležitosti spoločnosti

- dynamický rast ekonomiky a zlepšený stav verejných financií,
- podpora procesu štrukturálnych reforiem najvyššími miestami,
- modernizácia zastaranej výrobnéj základne a zavádzanie nových technológií v celej rade priemyslových odvetví,
- rozvoj dopravnej infraštruktúry v oblasti pôsobenia firmy,
- rast reálnych príjmov (v priemere o 4,5 % ročne),
- zlepšená platobná a investičná schopnosť removených zákazníkov,
- začínajúci trend zameriavací sa na štíhlu výrobu.

Hrozby

V súvislosti s uvedenými faktormi a na základe ich analýzy je stratégia založená na potrebe rozvíjaní predpokladov pre využitie príležitostí zúčastniť sa na svetových trhoch. Neistoty sú spojené so schopnosťou udržať dlhodobé vysoké tempo rastu, jeho obchodní partneri a prispôbujú tomu svoj prístup. Prešľapovanie a ďalšie váhanie môže znamenať, že v budúcnosti budú rásť konkurencieschopné firmy .

7 ZÁKLADNÁ CHARAKTERISTIKA BUDOVY

Celý komplex zaberá plochu 14 800 m², z toho asi tri štvrtiny predstavuje výroba.

Budova je konštrukčne riešená ako montovaný oceľový skelet s dvojpodlažnými administratívno –sociálnymi prístavkami. Obvodový plášť je sendvičový, rovnako tak strešný plášť. Požiarne deliace konštrukcie a konštrukcie zabezpečujúce stabilitu stavby sú druhu D1. Budova bola pred užívaním posúdená podľa STN 73 0804 a nadväzujúcej normatívy. Je zaradená do I.stupňa požiarnej bezpečnosti.Stavebná konštrukcia je v požiarnebezpečnostnom riešení uvádzaná s požiarnou odolnosťou 15 minút.

Priestor sa delí na :

Výrobný úsek - samostatný požiarly úsek ,je oddelená požiarlymi uzávermi-dvere, okná, požiarne klapky a prestupy.

Úsek administratívy – táto časť je vybavená požiarlymi uzávermi,čízbe bezpečnostnými dverami, elektropožiarlyou signalizáciou ,prepojenou na hlásič na vrátnici.

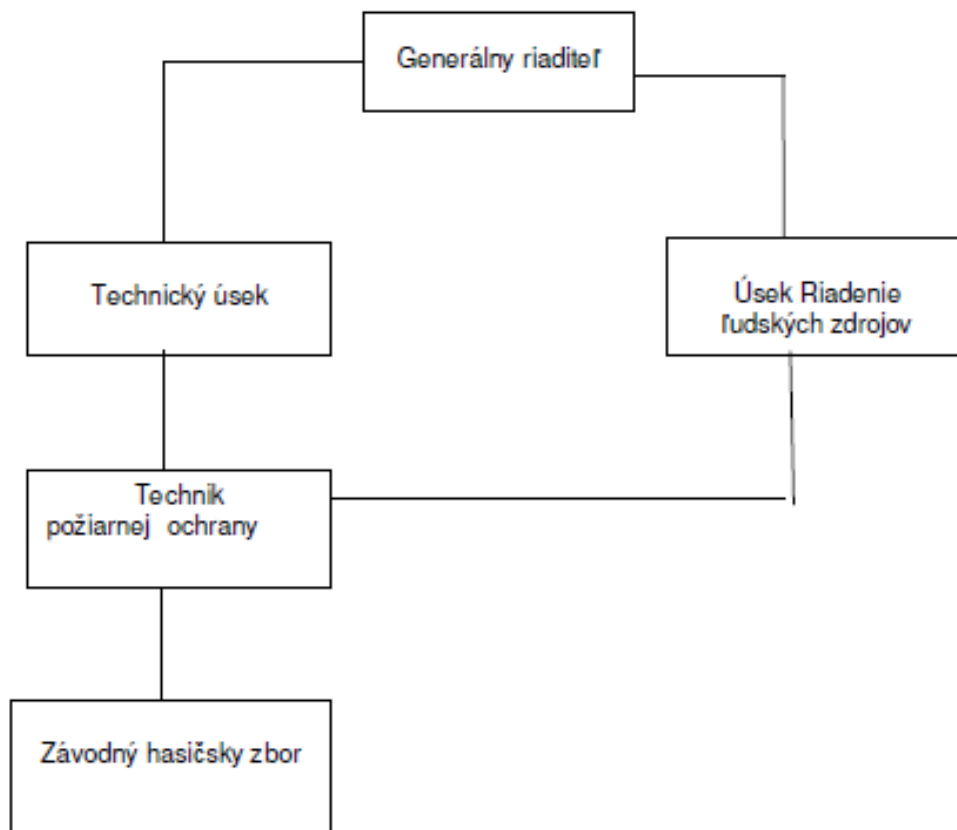
7.1 Požiarly organizácia a signalizácia budovy.

Spoločnosť má vypracovaný požiarly a evakuačný plán, ktorý je v súlade s § 28 Vyhľ.MV SR č.121/2002 Zz.,ktorou sa vykonávajú niektoré ustanovenia Zákona SNR č.314/2001 o ochrane pred požiarlymi v znení neskorších zmien .

Účelom je organizácia evakuácie osôb ,cenného a nebezpečného majetku z objektu zasiahnutého alebo ohrozeného požiarlym .

Za riadenie evakuácie zodpovedá osoba dopredu určená spoločnosťou -je to vždy príslušný vedúci pracoviska,oddelenia na jednotlivých priestoroch objektu.V neprítomnosti uvedeného vedúceho ,požadované činnosti evakuácie zabezpečujú ich priami podriadení danej pracovnej smeny.

Organizačné usporiadanie zodpovedností spoločnosti ochrany pred požiarmi môžeme vidieť na (Obr.č. : 6)



Obr.č. : 6 Organizačná schéma zodpovedností.

Evakuácia sa vyhlasuje pokrikom a spustením poplašných sirén (aktivovať tlačidlový hlásič EPS).

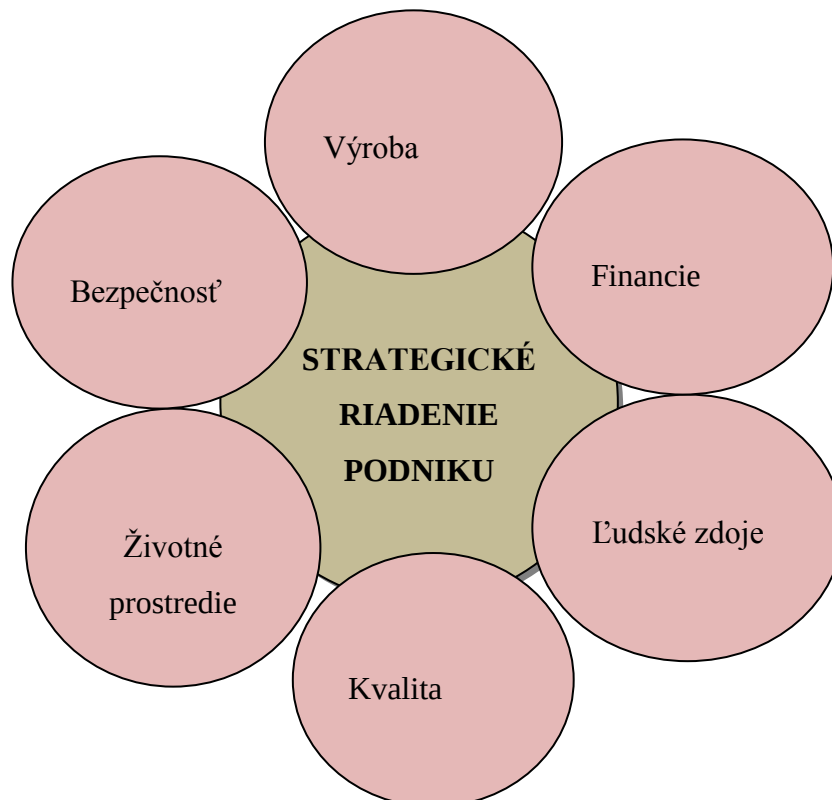
Budova má síce požiarnu signalizáciu, ale nemá vybudovaný automatický systém hasenia. Najbližší hydrant a hasiaci prístroj sa nachádza na chodbe približne 5 m od serverovne.

8 ANALÝZA ORGANIZAČNEJ ŠTRUKTÚRY SPOLOČNOSTI

Preskúmanie výrobitel'nosti produktov realizuje tím zložený z Automotív Manažéra, Manažéra výroby (CMS aj ATG), Materiálového manažéra, Manažéra kvality, pričom Automotív Manažér a Manažér výroby preveruje výrobitel'nosť z hľadiska dostupnosti technológií, infraštruktúry a kapacít (včítane kooperácií), Materiálový manažér z hľadiska možnosti zabezpečenia potrebných materiálových zdrojov a Manažér kvality z hľadiska dostupnosti potrebnej monitorovacej a meracej techniky. (Obr.č. : 7)

Ak je výrobitel'nosť posúdená ako možná, pristupuje sa k zmene príslušnej výrobnéj technickej dokumentácie (podľa smernice Riadenie technickej dokumentácie) prípadne k ostatným relevantným zmenám.

Ak je potrebné k zabezpečeniu výrobitel'nosti investovať do infraštruktúry, postupuje sa podľa smernice Zabezpečenie materiálových zdrojov.



Obr.č. : 7 Strategické riadenie podniku

Správne nastavený informačný tok zohráva v riadení firmy jednu z kľúčových úloh. Zabezpečuje totiž výmenu informácií potrebných pre efektívnu realizáciu všetkých procesov a činností.

V rámci spoločnosti sa využívajú viaceré nástroje internej komunikácie. Sú to predovšetkým:

- Porady
- Firemné nástenky
- Intranet
- Stretnutia so zamestnancami
- Prieskum spokojnosti zamestnancov
- Priama, operatívna komunikácia

8.1 Procesné riadenie spoločnosti

Pre efektívne riadenie spoločnosti, zaistenie spokojnosti zákazníka je dôležité funkčné procesné riadenie a správna nadväznosť jednotlivých procesov. (Obr.č. : 8) Uvedená spoločnosť má procesy v troch kategóriách :

- Riadiace procesy,
- hlavné procesy,
- podporné procesy.

Základnou povinnosťou každého zamestnanca je pracovať a konať tak, aby firma a značka bola na trhu úspešná. U zákazníka je nutné vybudovať dôveru v schopnosť firmy a značky dodávať požadovanú kvalitu a sústavne ju udržiavať.

Spoločnosť zostavuje rozpočtový plán na obdobie jedného roka (finančný rok začína 1. 10. a končí 30. 9.) Na príprave plánu sa podieľajú manažéri jednotlivých úsekov. Gestorom tvorby plánu je finančný manažér (FM), ktorý od jednotlivých manažérov vyžaduje zadať podklady k plánu (požiadavky na investície, požiadavky na ľudské zdroje, objemy predaja, predpokladaný objem režijných nákladov...).

Podklady z jednotlivých úsekov spracúva FM a jeho tím. Finálna verzia rozpočtového plánu musí byť spracovaná v termíne, ktorý požaduje materská firma. Definitívnu verziu plánu posudzuje riaditeľ divízie (RD) a FM. Po schválení rozpočtového plánu, FM informuje jednotlivých manažéroch o schválených, resp. zamietnutých investíciách.

Riadiace procesy :

1. Interná komunikácia

2. Preskúmanie vedením

3. Riadenie finančných zdrojov

4. Aplikácia výsledkov vývoja

5. Interné audity

6. Riadenie dokumentácie

7. Nápravné a preventívne opatrenia

8. Riadenie technickej dokumentácie

9. Legislatívna podpora

10. Riadenie záznamov

11. Riadenie návrhu konštr. zmeny

Hlavné procesy :

1. Vypracovanie ponuky

2. Vypracovanie ponuky intracompany

3. Vypracovanie ponuky servis

4. Príjem, preskúmanie objednávky, potvrdenie

5. Projekcia ,konštrukcia produktu

6. Zabezpečenie materiálu

7. Výroba, montáž

8. SW oživenie testovanie

9. Balenie a expedícia

10. Servis

Podporné procesy:

1. Strateg. nákup výber dodávateľov ,

2. Riadenie prístrojov na monitorovanie a testovanie

3. Kontrola kvality

4. Riadenie ľudských zdrojov

5. Budovy a ich údržba

6. Infraštruktúra ,údržba strojov a zariadení

7. HW, SW, Inf. systém a ich údržba

8. Reklamačné konanie

9. Riadenie nezhodného produktu

Požiadavka
zákazníkaSpokojný
zákazník

Obr.č. : 8 Procesná mapa spoločnosti

8.2 Analýza interného auditu spoločnosti

Spoločnosť vykonáva v plánovaných intervaloch interné audity (IA), ktorými preveruje efektívnosť vybudovaného systému manažérstva kvality, ako aj jeho zhodu s požiadavkami normy ISO 9001:2000.

Interné audity vykonávajú vyškolení interní audítori, ktorých na výkon IA poveruje manažér kvality (MK).

Výber audítorov je vykonávaný tak, aby bola zaistená nestrannosť a objektívnosť auditu – audítori nesmú auditovať svoju vlastnú prácu.

IA začína úvodným jednaním, ktorého účelom je:

- predstaviť členov previerkovej skupiny
- oboznámiť preverovaných s náplňou interného auditu
- poskytnúť stručný prehľad metód a postupov, ktoré budú pri realizácii použité
- odhaliť prekážky znemožňujúce realizáciu interného auditu (neúčast' zodpovedných preverovaných pracovníkov, nedostupnosť materiálov požadovaných v IA)

Po úvodnom jednaní sa pristúpi k zhromažďovaniu dôkazov. Dôkazy sú zhromažďované pomocou pohovorov, skúmaním dokumentov a zisťovaním činnosti a podmienok v daných oblastiach záujmu.

Informácie zhromažďované pri pohovoroch majú byť overené z nezávislých zdrojov a pokiaľ je to možné podložené dôkazom (záznam, meranie, a pod.).

Všetky významné náznaky nezhôd, týkajúcich sa preverovanej problematiky, sa prešetrujú, vrátane tých, ktoré nie sú uvedené v Kontrolnom liste pre IA.

Zistenia a dôkazy sa zaznamenávajú do Kontrolného listu pre IA.

Hodnotenie zistení vykonajú audítori priradením príslušného počtu bodov pre každú otázku. Bodovacia škála je od 0 do 10 bodov.

- ➔ 10 bodov je udelených v prípade úplnej zhody.
- ➔ 5 bodov je udelených v prípade zistenia menej závažnej nezhody (ktorá priamo neohrozuje funkčnosť a efektívnosť SMK, je prevažne dokumentačného charakteru)

- ➔ 0 bodov je udelených v prípade zistenia závažnej nezhody (ktorá ovplyvňuje funkčnosť a efektívnosť SMK, môže ohroziť spokojnosť zákazníkov, prípadne spôsobiť mimoriadne náklady.

Hodnotenie sa zapisuje do Kontrolného listu pre IA.

V rámci hodnotiacej fázy vypracúva vedúci audítor a audítor Protokol z interného auditu.

Ak sa pri internom audite vyskytnú návrhy na zlepšenie preverovaných oblastí, tieto sa uvedú do Protokolu z interného auditu. Protokol z IA obdržia zodpovední pracovníci z preverovaných organizačných jednotiek (uvedení v programe IA) a MK. Ďalšie zhotovenie a rozdeľovanie kópií protokolu o audite je neprípustné vzhľadom na dôvernosť a charakter oznamovaných informácií.

Vedúci audítor odovzdá Protokol z IA preverovaným a MK do 5 pracovných dní od vykonania IA. Protokol musí byť podpísaný vedúcim previerkovej skupiny, ako aj zodpovednými pracovníkmi preverovaných oddelení, čo slúži ako dôkaz uznania zistených nezhôd. V prípade ak má preverovaný akékoľvek pripomienky k zneniu výsledkov auditu, tieto uvedie do príslušnej časti protokolu a pripojí svoj podpis.

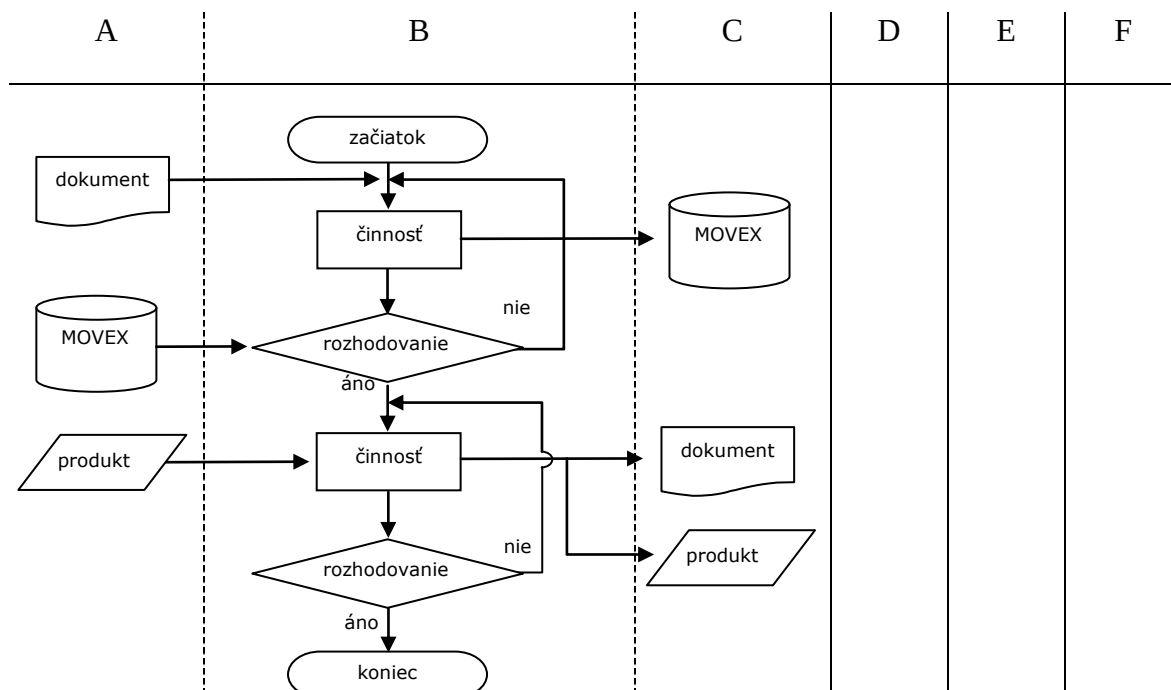
Smernica pre proces

Smernica pre proces slúži na zdokumentovanie procesov SMK, ktoré sú zadefinované v platnej Procesnej mape. Pozostáva z dvoch častí - Definície procesu a postupu procesu.

V prvej časti (Definícia procesu) sú uvedené nasledovné informácie:

- Vlastník procesu
- Operátor(i) procesu
- Predchádzajúci proces(y)
- Vstupy
- Výstupy
- Nasledujúci proces
- Prípadne externe zabezpečované činnosti a ich riadenie
- Zdroje pre proces
- Regulatívy procesu
- Parametre procesu
- Monitorovanie, meranie, analýzy

V druhej časti (Postup procesu) je prednostne formou vývojového diagramu, prípadne textovo / verbálne, popísaný postup procesu. Vývojový diagram je členený nasledovne:



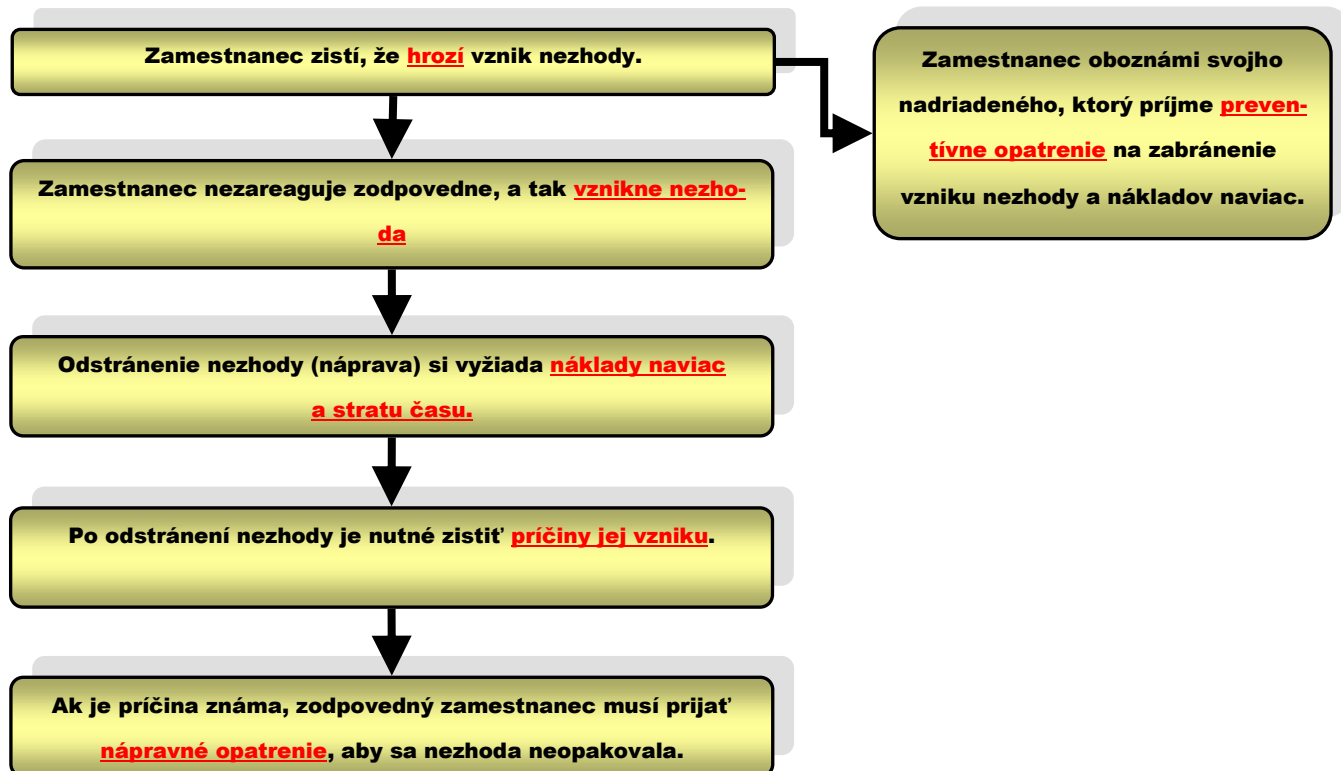
- A - vstupy do procesu
- B - popis procesu, činnosti.
- C - výstupy procesu, záznamy
- D - zodpovedná osoba (kto?)
- E - podpora (kto?)
- F - informácia (komu?)

Smernicu pre proces (SpP) vypracováva vlastník procesu, preskúmava zamestnanec poverený Manažérom Kvality (MK), schvaľuje ho riaditeľ spoločnosti (RS), ktorý tiež definuje kedy smernica vstupuje do platnosti.

8.3 Zhodnotenia a návrh nápravných a preventívnych opatrení

Nezhody a zistenia vyplývajúce z realizovaných auditov sú podnetom k prijímaniu nápravných, resp. preventívnych opatrení. V tomto prípade sa postupuje podľa SpP Nápravné a preventívne opatrenia, zlepšovanie. (Obr.č. : 9)

Na základe prijatých nápravných a preventívnych opatrení môže MK stanoviť termín ďalšieho IA na preverenie ich efektívnosti



Obr.č. : 9 Postup pri odstraňovaní nehody

Príčiny každej potenciálnej alebo existujúcej nehody, chyby, alebo inej nežiadúcej situácie musia byť riešené a odstraňované (Riadenie nezhodného produktu). Najčastejšie zdroje prijímania NO/PO sú uvedené v nasledovnej tabuľke (Tabuľka 1)

Zdroj NO/PO	Dôkazový materiál	Riešiteľ NO/PO
Interný audit	Protokol z interného auditu	Vedúci zodpovedný za úsek, kde bol identifikovaný podnet.
Reklamácia	Reklamačný protokol	MK
Nápravné opatrenie, neefektívne	Nápravné / preventívne opatrenie	MK v spolupráci s vedúcim, zodpovedným za úsek, kde bolo pôvodné opatrenie prijaté
Nezhoda	Záznam o nehode	MK v spolupráci s vedúcim zodpovedným za úsek, kde bola zistená nezhoda
Neplnenie cieľov politiky kvality	Správa o fungovaní a účinnosti SMK	MK v spolupráci s vedúcim zodpovedným za úsek, kde bol listený podnet.

Tabuľka 1:Nápravné a preventívne opatrenia

8.4 Návrh zlepšovacích procesov

Každý pracovník divízie má možnosť kedykoľvek podať návrh na zlepšenie. Podmienkou podania návrhu je vyplnenie formulára Návrh na zlepšenie. Čisté formuláre sú k dispozícii na určenom mieste. Riadne vyplnený formulár je nutné vhodiť do pripravenej uzamykateľnej schránky.

Asistentka riaditeľa v týždenných intervaloch kontroluje obsah schránky a prípadné návrhy predkladá na porade vedenia. Počas porady vedenia sú všetky návrhy na zlepšenie preskúmané z hľadiska ich efektívnosti, realizovateľnosti, možného prínosu a pod.

Asistentka riaditeľa je povinná bezodkladne informovať každého navrhovateľa o prijatí/neprijatí jeho návrhu.

Pri komplikovanejších prípadoch vedenie menuje pracovníka, ktorý zodpovedá za zostavenie riešiteľského tímu (spravidla by mal byť zložený z pracovníkov konštrukcie, výroby, montáže, kontroly kvality...), ktorý najprv posudzuje takýto návrh a prípadne následne aj koordinuje realizáciu a informuje o priebehu všetkých zainteresovaných.

Celý priebeh zaznamenáva asistentka riaditeľa prípadne menovaný pracovník do príslušných častí formulára.

Asistentka riaditeľa vedie elektronickú databázu, kde zaznamenáva všetky vznesené návrhy a vyjadrenia k nim. Databáza tiež obsahuje informácie o realizácii a prínosoch schválených návrhov.

Riaditeľ, prípadne menovaný pracovník, sa dohodne s riadiacim pracovníkom dotknutého úseku na spôsobe realizácie zlepšovateľského návrhu, rovnako priebežne dohliadajú na implementáciu zlepšovateľského návrhu.

Každý realizovaný zlepšovací návrh je s primeraným odstupom času na porade vedenia vyhodnotený z hľadiska reálnych prínosov.

9 ANALÝZA ŠTRUKTÚRY SPOLOČNOSTI Z HĽADISKA IT

Spoločnosť využíva k riadeniu firemných údajov systém Movex. Prepojenie je globálne, čiže medzi všetkými sekciami po celom svete. Cesta každej požiadavky po stlačení Enter : 680 + 680 km . (Obr.č. : 10)



Obr.č. : 10 Prenosová trasa údajov pre Movex

9.1 Analýza SW

Movex - softvér slúžiaci pre správu distribúcie, vhodný pre stredné a veľké spoločnosti.

Tento softvér sa nazýva aj M3, umožňuje:

- Zjednodušenie prevádzky, zviditeľnenie spoločnosti,
- prístup k informáciám kedykoľvek a kdekoľvek s cieľom zlepšiť proces rozhodovania a rýchlosť odozvy,
- ľahko sa prispôbiť k novým výrobným postupom, meniacim sa požiadavkám zákazníkov, rozvíjajúcim sa obchodným stratégiám,
- podpora predaja uviesť nové výrobky na trh rýchlejšie a so ziskom,
- optimalizácia zásob a výrobných prostriedkov za účelom zvýšenia efektivity,
- zlepšenie kvality,
- zvýšenie spokojnosti zákazníkov.

9.1.1 Analýza procesov v jednotlivých produktových sádach.

Celý softvér sa skladá zo štyroch integrovaných produktových sád, ktoré dohromady spravujú všetky hlavné a podporné procesy vo firme. Aktualizácia zmien údajov v softvéri tak aby prebehli vo všetkých procesoch, prebieha automatickým upgradom-preplánovaním v noci o 23-tej hodine, každých 24 hodín.

Tieto štyri integrované produktové sady umožňujú rozšíriť ich hodnotu a chrániť investície tým, že zjednodušuje oddeľuje technologické vrstvy od M3 obchodných aplikácií.

Predaj a servis zákazníkov

- Spravovanie údajov o zákazníkoch v súvislosti s predajom výrobkov,
- konfigurácie produktov vrátane ich servisných požiadaviek,
- vypracovanie analyz pre určenie najpredávanejších produktov na základe cenovej ponuky ,alebo nakonfigurovania zariadenia,
- optimalizácia úrovne zákazníckych služieb.

Manažment dodávateľského reťazca

- Nástroje pre strategické plánovanie dodávok, operatívne plánovanie riadenia objednávok,
- riadenie a plánovanie dodávateľského reťazca,
- optimalizácia úrovne dodávateľských služieb, s cieľom maximalizovať efektívnosť a ziskovosť,
- funkcie plánovania globálneho dopytu.

Manažment výroby

- Definovanie všetkých aspektov vyrábaných produktov,
- centrálné riadenie výroby produktov,
- konfigurácia vyrábaných produktov,
- tvorenie kalkulácií výroby, plánovanie,
- tvorenie výrobných postupov,
- optimalizácia výrobných procesov,
- simulácia priebežného času výroby a dostupnosti komponentov.

Finančný manažment

- Spracovávanie všetkých požiadaviek účtovníctva,
- rozpočtovanie, konsolidácia, párovanie s objednávkami,

- vypracovávajú finančných analýz za jednotlivé obdobia,
- spravovanie obchodných jednotiek v rámci viacerých krajín,
- využitie nástrojov softvéru, ktorý slúži na zachytenie, analyzovanie finančných informácií súvisiacich s činnosťou organizácie a to ako externe, tak interne.

9.1.2 Zhodnotenie softvéru Movex

Využívaním daného softvéru spoločnosť má možnosť zjednodušovať operácie a lepšie ich rozlišovať. Výrazne posilňuje riadenie operačných aktív, optimalizuje zákaznícke služby a maximalizuje ziskovosť. Má pod kontrolou informácie o finančných tokoch.

Výhody systému Movex:

- príležitosť veľmi rýchlej implementácie zásluhou nespočetného rozsahu funkcií a najmodernejších konfiguračných možností
- záruka úspešných zámerov podnikov za pomoci vysoko kvalitných aplikácií, starostlivo vypracovaných metodík a dôveryhodných poradcov,
- možnosť zvýšenia výkonnosti výrobných podnikov, za pomoci dôsledne uplatňovanej koncepcii podnikových procesov.

Nevýhody:

- veľké množstvo prvotného zápisu do zošita, až druhotný zápis sa deje do Movexu
- možnosť nastavenia Movex systému je ohraničený
- možnosť predraženia Movex systému
- užívateľovi môže sa zdať systém príliš neohybný a ťažko adaptovateľný.

V časti základné činnosti používané v Movexe sa všetok presun zaznamenáva do zošita presunov a až potom sa zapisujú do Movexu. Stačí ak sa pozabudne len na jeden jediný presun a už nám nesedí skutočný stav so stavom uvádzaným v Movexe.

9.2 Prístupy užívateľov

Jednotliví zamestnanci majú prístupové práva do IS Movex podľa svojej kompetencie. O potrebnom rozsahu prístupových práv rozhoduje vždy priamy nadriadený daného zamestnanca.

Pri nástupe nového zamestnanca oddelenie IT podľa požiadaviek priameho nadriadeného zabezpečí prístupové práva a taktiež vykonáva vstupné zaškolenie zamestnanca ohľadne práce v IS Movex. O špecifických aplikáciách IS Movex zaškolí zamestnanca priamy nad-

riadený alebo ním poverený zamestnanec. Trikrát nesprávne zadané heslo spôsobí zablokovanie ďalšieho prístupu daného používateľa do servera.

Prístupy užívateľov sú :

- Lokálny (v dosahu firemnej siete LAN) prístup k údajom
- Vzdialený (mimo dosahu firemnej siete LAN) prístup k údajom

9.2.1 LAN infraštruktúra

Local area network (LAN) - lokálna sieť je počítačová sieť, spájajúca počítače a ďalšie zariadenia, pokrývajúca menšiu geografickú oblasť (do niekoľko 1000m), ako napríklad domácnosť, kancelárie, alebo skupinu budov. Súčasné LAN bývajú najčastejšie založené na prepínaných ethernetových sieťach, alebo na technológii Wi-Fi.

Na obrázku (Príloha č.:1) je znázornená topológia siete v budove čiastočne aj s okolím v rámci areálu spoločnosti. Racky sú umiestnené jednak v serverovni (RD1) jednak na viacerých miestach vo výrobe a administratíve (RD3.1, RD3-1, RD3-2, RD4, RD5, RD6) a sú osadené príslušnými aktívnymi prvkami CISCO podľa schémy.

9.2.2 Kabeláž

Kabeláž je FTP kategórie 5E.(Obr.č. : 11) FTP kategória znamená štvorpárový 100Ω UTP, s jednoduchou fóliou (F- foliované) pre minimalizáciu elektromagnetického rušenia a vyžarovania. Tienený TP často označujeme aj ako FTP (Foiled Twisted Pair). FTP je myslené ako tienená verzia káblov kategórií 3, 4 a 5. Sú použiteľné pri všetkých Ethernet aplikáciách a sú ekvivalentom jednotlivých kategórií UTP káblov. Kategória 5e je určená pre vysokorýchlostný prenos.



Obr.č. : 11 Krútená dvojlinka FTP

Ukončenie kábla je aplikované konektorom RJ-45(Obr.č. : 12) , alebo zásuvkou rovnakého typu , krimpľuje sa pomocou krimplovacích kleští .



Obr.č. : 12 Tienený konektor RJ-45

Zásuvky majú nožový systém kvoli rýchlej inštalácii. Na inštaláciu je použité špeciálne zatlačacie náradie. Zásuvky a zástrčky sú vyrobené v tých istých kategóriách jako káble. [3]

9.3 Monitorovanie siete

9.3.1 Analýza monitorovania siete

Spoločnosť využíva na monitorovanie siete nasledovné programy : netstat, logcheck a ippl. Tieto programy bežia neustále na serveri určenom na kontrolovanie a správu siete.

Netstat slúži na priame monitorovanie portov a spojení, ktoré odchádzajú alebo prichádzajú do siete. Určuje, ktorý port je využívaný procesom alebo programom. Tento program je spúšťaný podľa vôle správcu siete.

Logcheck slúži na filtrovanie logov servera a upozorňuje na nebezpečné udalosti. Pri každom zapnutí analyzuje určené logy administrátorom, odfiltráva nepodstatné riadky a upozorňuje na nebezpečné udalosti. Citlivosť balastných filtrov je nastavená na úroveň „servera“.

IPPL slúži na logovanie pokusov o prístupy na porty servera pomocou protokolov TCP, UDP a ICMP. Tento program zaznamenáva aj pokusy o pripojenie, ktoré neprešli pravidlami nastavenými na firewally.

9.3.2 Vyhodnotenie monitorovania siete

Tieto sieťové monitorovacie programy sú dostačujúce na monitorovanie internej LAN siete spoločnosti a činnosti sieťových zariadení. Sú v dostatočnej miere schopné analyzovať, skúmať a upozorňovať na neočakávané aktivity na sieti. Poskytujú v potrebnej miere pres-

né a prehľadné dáta pre správcu siete, po vyladení a nastavení filtrov. Problém vzniká pri pravidelnosti kontroly výsledkov zo strany správcu siete. Správca kontroluje výsledky analýz podľa vlastného uváženia. Pokiaľ zanedbá pravidelnú kontrolu, môže prehliadnúť únik dát, monitorovanie komunikácii potenciálnym útočníkom alebo páchatelom.

9.4 Používanie výpočtovej techniky

Zamestnanci, ktorí majú pridelené PC, sú povinní pri práci s nimi dodržiavať určité zásady. Počítač a iné obdobné technické prostriedky sa môžu používať len na účely určené pracovným zaradením jednotlivého pracovníka. Pracovník je povinný používať určenú identitu – svoje konto.

Pracovník nesmie vyvíjať aktivity smerujúce proti plynulej prevádzke počítačov a firemnej počítačovej siete. Nesmie realizovať akékoľvek technické zásahy do siete alebo do žiadneho firemného počítača bez povolenia oddelenia IT.

9.4.1 Analýza hardvérového vybavenia spoločnosti

V prípade každého hardvéru nasadeného v prevádzke po rokoch dochádza k opotrebeniu, a tým k zvýšenej chybovosti, ktorá sa nedá nahradiť správne fungujúcim softvérom. Je potrebné venovať zvýšenú pozornosť hlavne pamäťovým médiám (disky, sieťové disky...), na ktorých sa nachádzajú informácie (databázy údajov, dokumenty...).

Hardvérové vybavenie spoločnosti:

● Pracovné stanice (PC)	160 x
● Notebook – firemné DELL	22 x
● Multifunkčné zariadenia BW Xerox WC 5230 -	4x
● Multifunkčné zariadenia BW Xerox WC 5740 -	2x
● Color multifunkčné zariadenie Xerox WC 7120 -	1x
● Digitálna veľkoformátová kopírka-Ploter Xerox A0 -	1x
● Scanner (HP)	5x

9.4.2 Zhodnotenie hardvérového vybavenia

Je potrebné dodržiavať pravidelnú kontrolu hardvérových častí systému (server, pracovné stanice, sieť, ostatné prvky). Správne dimenzovať hardvér z hľadiska zaťaženia operačnými systémami a ostatnými programami. Zátťaž môže narastať s narastaním počtu údajov. Dôležité je vybavenie hlavného počítača (resp. servera) správne dimenzovaným záložným zdrojom (UPS).

9.5 Heslá

Počítač musí byť zabezpečený najmenej jedným heslom – sieťovým heslom počítača. Sieťové heslo sa musí skladať z najmenej 8 znakov. Musí obsahovať najmenej tri typy znakov z nasledujúcich štyroch: malý znak abecedy, veľký znak abecedy, číslica a zvláštny znak (napr. znaky !, #, &, @ a pod.). Musí byť vytvorené tak, aby sťažilo nepovolaným možnosť jeho rozlúštenia (nesmie sa opakovať už použité heslo).

Nepoužíva sa žiadne meno manžela, dieťaťa, dátum narodenia a podobne. Počítače so zvýšenou ochranou prístupu musia byť zabezpečené heslom v BIOSe. Tento typ ochrany určuje priamy nadriadený. Svoje heslá pracovníci neprezrádzajú za žiadnych okolností druhým osobám.

9.5.1 Zhodnotenie používania hesiel

Spoločnosť vyžaduje od používateľov softvéru MOVEX ešte jedno heslo na prihlásenie na aplikačný server. Pri údajoch, ktoré si vyžadujú zvláštnu ochranu sa používa ochrana heslom aj pre jednotlivý dokument. Každý pracovník je zodpovedný za škodu spôsobenú v dôsledku prezradenia informácií ochrany prístupu k firemným údajom.

9.6 Zabezpečenie údajov

Pracovník je zodpovedný za zachovanie údajov, s ktorými pracuje. Údaje na prenosných počítačoch (notebookoch a pod.) sú chránené softvérovým šifrovaním. Zašifrovanie údajov každého prenosného počítača vykoná pracovník IT predtým, ako sa príslušný počítač začne používať. Na šifrovanie používa IT oddelenie aktuálnu verziu softvéru Pointsec pre enkryptovanie diskov od firmy Check Point Software.

Pracovníci sú povinní ukladať všetky pracovné dáta na sieťovom disku. Zálohovanie údajov uložených na sieťových diskoch zabezpečuje oddelenie IT denne. Obnovenie údajov na požiadanie vykonajú pracovníci IT oddelenia z ostatnej kópie týchto údajov.

Zálohové médiá sa ukladajú v trezore na oddelení IT. Týždňová kópia sa skladuje v prenajatom bankovom sejfe mimo objektu. Prístup k nemu majú finančný manažér a poverený pracovník oddelenia IT.

9.6.1 Zhodnotenie zabezpečenia údajov

Prínosom využitia kvalitného softvéru je redukcia bezpečnostných rizík, ktoré sú spojené so stratou alebo odcudzením počítačou alebo notebookov. Rýchla implementácia nám umožňuje dosiahnuť zosúladenie s legislatívnymi požiadavkami pri zachovaní zdrojov. Udržiava vysokú produktivitu koncových užívateľov a kontrolu IT. V prípade odcudzenia notebookov sa cudzia osoba k údajom na disku nedostane.

9.6.2 Prístup k firemným údajom a k údajom zákazníkov

So všetkými údajmi, ktoré sa týkajú spoločnosti alebo jeho zákazníkov sa zaobchádza ako s dôvernými informáciami. Ich odovzdanie tretiemu subjektu je zakázané. Prístupy do WiFi sietí musia byť schválené a sú obmedzené iba pre určitých užívateľov.

9.6.3 Bezpečnostné opatrenia voči neoprávnenému prístupu

Potenciálne nebezpečenstvo firme hrozí pri pridelení IP adres pomocou DHCP servera. Najjednoduchším spôsobom ako dané riziko odstrániť alebo minimalizovať, je vypnúť DHCP server a nastaviť IP adresy napevno. Je to síce náročnejšie riešenie na čas, no prináša i možnosť presne identifikovať zariadenia, ktoré sú. Pri infiltrovaní sa do siete cez AP, tak sa nedostane k citlivým údajom, pretože sieťové zariadenia neumožnia komunikovať mimo určený server pre správu.

9.7 Používanie internetu

Inštalácia akéhokoľvek softvéru je podľa firemných pravidiel vyhradená pre oddelenie IT. Ak pracovník potrebuje taký program, ktorý nie je na jeho počítači nainštalovaný a potrebuje ho k práci, požiada o túto službu pracovníkov IT oddelenia. Taktiež, ak pracovník potrebuje zmenu už nainštalovaných programov, požiada o pomoc pracovníkov IT

oddelenia. Každý firemný počítač podlieha previerke v zmysle zistenia dodržovania licenčných podmienok a príslušných interných predpisov spoločnosti .

9.7.1 Prístup na internet

Pracovníci majú možnosť používať v rámci siete Emerson pripojenie na sieť Internet. Tento prístup bude nainštalovaný len vtedy, ak ho pracovník potrebuje k svojej práci. Prístup k internetu sa nesmie používať na osobné účely. Zakázané sú prístupy na pornografické a iné stránky, ktoré sa netýkajú pracovnej náplne zamestnanca. Rovnako nie je dovolené sťahovať z internetu akékoľvek údaje, alebo softvér pre súkromné použitie (napr. filmy, hudbu v MP3 a iných formátoch a pod.) a nie je dovolené ukladať ich na firemných médiách. Všetky prístupy na internetové stránky sú monitorované a kontrolované na oddelení IT. K týmto údajom majú prístup priamy a vyšší nadriadení na požiadanie. Záznamy sú považované za dôverné a je tak s nimi potrebné zaobchádzať.

9.7.2 Zhodnotenie prístupu na internet

Pripojenia majú dosť veľkú kapacitu, aj pri výpadku jedného z nich dokáže spoločnosť komunikovať so svetom. Nakoľko spoločnosť vyžaduje pripojenie 24 hodín denne, výpadok internetu na dobu jedného dňa sťaží jej fungovanie. Dôležitým bodom zmluvy chrániacich spoločnosť je poskytnúť náhradné pripojenia, cez mobilnú sieť, pokiaľ nebude poskytovateľ schopný odstrániť poruchu.

9.7.3 Bezpečnostné opatrenia pripojenia k internetu

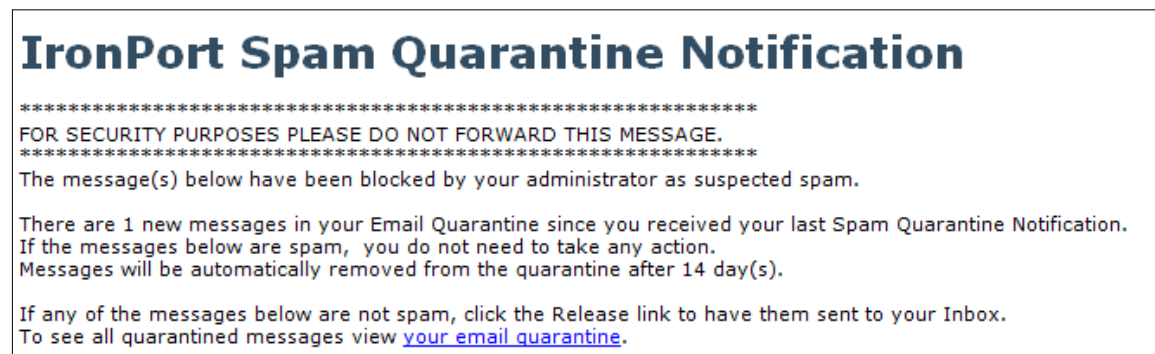
Na základe analýzy nie je potrebné prijímať bezpečnostné opatrenia, nakoľko je pripojenie dostatočne zmluvne ošetrené. Spoločnosť je riadne chránená zmluvou s dodávateľom poskytovania služby tak, aby sa vyhla prípadným vzniknutým problémom s výpadkom pripojenia.

9.8 Používanie elektronickej pošty

Ak počítač pracovníka slúži na pripojenie k systému elektronickej pošty, má možnosť vymieňať si údaje a správy elektronicou formou. Táto možnosť sa nemá zneužívať pre osobné účely. Vo všeobecnosti je zakázané posilať nedovolený softvér alebo údaje pornografického rázu v akejkoľvek forme. Vhodné je zvážiť aj posielanie údajov väčšieho rozsahu. Správy od neznáameho odosielateľa sa doporučujú bez otvorenia mazať, resp. v prípade podozrenia prizvať pracovníka IT oddelenia.

9.8.1 Zhodnotenie využívania elektronickej pošty

Spoločnosť má veľmi dobre zabezpečené odchyťovanie podozrivých mailov, ktoré automaticky, no i tak je dôležité sa mať na pozore. Obr.č. : 13)



Obr.č. : 13 Zachytenie podozrivého mailu

9.9 Používanie záznamu na prenosné médiá

Zariadenia takéhoto druhu je zakázané používať na osobné účely. Rovnako je zakázané vytvárať na firemných zariadeniach ilegálne kópie na médiách akéhokoľvek druhu.

9.10 Antivírusový softvér

Na počítačoch je nainštalovaný antivírusový softvér od firmy Symantec. Tento softvér slúži na ochranu údajov a programov každého jednotlivého počítača. Zabezpečuje a kontroluje emailové správy, chatové správy a všetky súbory automatickým odstraňovaním vírusov, červov a trójskych koňov. Funkcie novej verzie detekujú aj niektoré nevírusové hrozby ako napríklad spyware. Program obsahuje funkciu skenovanie komprimovaných súborov, pred otvorením. Norton AntiVirus umožňuje automatické sťahovanie aktualizácií vírusovej databázy pomocou vlastnej služby LiveUpdate. Blokovanie červov a skriptov dokáže zabrániť infekcii systému aj takým vírusom, na ktoré ešte neboli vytvorené detekčné údaje.

O aktualizáciu databázy vírusov sa pravidelne stará oddelenie IT. Nedostatky v ochrane proti počítačovým vírusom pracovníci oznamujú na IT oddelenie.

9.10.1 Zhodnotenie softvéru

Softvérový gigant, ktorého produkty Norton Commander alebo Norton Utilities pozná snáď každý pokročilejší užívateľ. Medzi obrovskou škálou produktov nájdeme aj Norton Antivirus. Súčasná verzia ponúka najkomplexnejšie riešenia ako pre jednotlivcov tak i

spoločnosti. Počas svojej existencie pohltil IBM Antivirus .Medzi zápory patrí predovšetkým jeho vyššie systémové nároky na PC.

9.11 Intranetová sieť

Intranet je počítačová sieť, využívajúca technológie TCP/IP, HTTP založená na Klient/Server architektúre. Určená iba pre malé skupiny používateľov, napríklad pre pracovníkov nejakého podniku. Je to v podstate interný Internet. V súčasnosti sa stáva nevyhnutnosťou každej organizácie. Úlohou intranetu je dokonalá organizácia pracovných procesov a zasielanie medzi jednotlivými zamestnancami. Intranet zvyšuje spoločnosti produktivitu práce.

9.11.1 Zhodnotenie intranetu v spoločnosti

Technickú stránku intranetu spravuje oddelenie IT. Za obsahové aktualizácie jednotlivých sekcií sú stanovené nasledovné zodpovednosti:

Sekcia Movex (zodpovedá oddelenie IT)

Sekcia SMK – manažment kvality (zodpovedá manažér kvality)

Sekcia ENVIRO – (zodpovedá manažér kvality)

Fotodokumentácia k jednotlivým zákazkám (zodpovedá manažér kvality)

Ekonomika (zodpovedá finančný manažér)

Telefónny zoznam (zodpovedá manažér ľudských zdrojov)

Dochádzka (zodpovedá spoločnosť .)

Banka informácií (zodpovedá oddelenie IT)

Legislatíva (zodpovedá manažér ľudských zdrojov)

9.11.2 Bezpečnostné opatrenia používania intranetu

Zložitosť systému bráni správne ho využívať. Zamestnanci túto skutočnosť používania intranetu často vnímajú ako preťaženie množstvom informácií, ktoré potrebujú k svojej práci. Pravidelné preškolenie používania, eliminovanie posielania zbytočných správ a korektné členenie mailov ,prispeje k správne použitiu tohoto komunikačného nástroja .

IT oddelenie, ako prevenciu dodržiavania interných pravidiel užívania počítačov (najmä nelegálny a nepovolený software), vykonáva kontrolu počítačov. Všetky porušenia pravidiel sú riešené v súlade s platným pracovným poriadkom.

10 NÁVRH IMPLEMENTÁCIE BEZPEČNOSTNEJ POLITIKY V PRÍPADE VZNIKU HAVÁRIE

Tento plán podáva návrh riešenia havarijnej situácie v oblasti IT vybranej spoločnosti .Serverovňa zastrešuje nasledujúce IT funkcie:

- LAN infraštruktúru
- Servery pre ukladanie údajov
- Databázové servery
- Zálohovanie údajov
- Centrálna UPS

Prvým krokom nasledujúcim po havárii by malo byť presné zistenie príčin havárie a určiť stupeň poškodenia jednotlivých zariadení a či je možné pokračovať v prevádzke zariadení s minimálnym výpadkom

V prípade kolapsu počítačovej siete v danej spoločnosti, prípadne niektorého zo serverov a ak sa porucha nedá odstrániť bezodkladne, je nutné informovať „Tím na rekonštrukciu infraštruktúry informačných technológií“:

10.1 Tím na rekonštrukciu infraštruktúry informačných technológií

1. riaditeľ spoločnosti
2. finančný manažér
3. manažér pre Automotív
4. EU manažér spoločnosti
5. IT administrátor
6. IT administrátor

Tento tím je zodpovedný za koordináciu a vykonanie prác potrebných na obnovenie pôvodného stavu, prípadne zabezpečenie riešenia náhradnej prevádzky informačných technológií po dobu nevyhnutne nutnú.

10.2 Postup pri odstraňovaní havárie

Ako prvý krok, ktorý treba bezodkladne spraviť a je úlohou povereného tímu :

- zistiť presnú príčinu havárie a určiť stupeň poškodenia jednotlivých zariadení,
- zistiť možnosť pokračovania v prevádzke zariadení s minimálnym výpadkom.

V závislosti na príčinách a dosahu havárie je nutné:

- obnoviť LAN infraštruktúru
- zabezpečiť nové technické zariadenia
- reinstalovať OS a aplikačný SW
- obnoviť databázu z archivných kópií

Inicializáciu plánu musia schváliť dvaja z nižšie uvedených pracovníkov

- riaditeľ spoločnosti
- IT manažér
- IT administrátor

10.3 Stupne havárií

Podľa dopadu a príčiny rozdelíme definované tri stupne havárie.(Tabuľka 2)

Stupeň	Časový prestoj	Príčina	Dopad
Žltý	Menaj ako 24 hod	Porucha servera	Nízky
Oranžový	24 – 72 hod	Výpadok energie	Stredný
Červený	Viac ako 72 hod	Zemetrasenie, hurikán, teroristický útok, vojna a pod.	Vysoký

Tabuľka 2 :Stupne havárií

Každý stupeň havárie musí mať vlastný komunikačný plán , musí obsahovať aj popis poškodených systémov a procesov a odhad času obnovy.(Tabuľka 3)

10.4 Komunikačný plán

Komunikačný plán slúži ako pohotovostný plán, určuje nám krok za krokom, ako postupovať v prípade vzniknutého problému. Taktiež nám do budúcnosti poskytne podklad pre analýzu preskúmania nastavenia bezpečnostnej politiky. Komunikačný plán projektu je miestom, kde je popísané:

- typ zdieľaných informácií – názov a účel komunikačného plánu,
- periodicita jednotlivých položiek,
- časové limity pre distribúciu a odozvy,
- zodpovednosť za tvorbu a distribúciu jednotlivých položiek,
- zodpovednosť za prijatie informácie a vyjadrenie k nej,
- forma predania informácie ostatným členom projektového tímu a prípadne mimo projekt.

Stupeň	Kto musí byť informovaný	Spôsob komunikácie	Kedy	Periódica
Žltý	IT manažér Zamestnanci	Telefón E-mail	Max 1 hod po zistení	2 hod
Oranžový	IT manažér Vedenie spoločnosti	Telefón Telefón	Max 2 hod po zistení	1 hod
Červený	IT manažér Vedenie spoločnosti	Telefón Telefón	Max 4 hod po zistení	1 hod

Tabuľka 3: Komunikačné procedury

Podľa potrieb komunikačného plánu a podnikových štandardov treba navrhnúť formuláre a šablóny pre špecifické a štruktúrované dokumenty, ktoré môžu projektovú komunikáciu významne zjednodušiť.

Ďalšími charakteristikami komunikačného plánu sú:

- časové limity určujúce, s akým predstihom pred jednaním alebo schválením musí byť dokument distribuovaný,

- detailná distribúcia zodpovednosti voči položke komunikačného plánu, napr. kto dokument vytvorí a kto sa k nemu postupne musí vyjadriť,
- archivačné predpisy, popisy miest uloženia a zaistenia dostupnosti archívu pre členov projektového tímu,
- predpisy pre zaistenie bezpečnosti a dôvernosti dokumentácie.

10.5 Stupeň ohrozenia

Pre vytvorenie stupňov ohrozenia je treba určiť hodnotenie štruktúry serverov, z ktorej vyplýva postupnosť obnovy systémov a služieb v prípade havárie. (Tabuľka 4)

Stupeň	Server / Servery	OS	Určenie
Úroveň 2	Servery pre údaje	WINDOWS 2003 a 2008 Server	Ukladanie konštrukčných a iných údajov
Úroveň 2	Licenčné servery	Windows 2003 Server	Server pre podporu konštrukč. procesov
Úroveň 2	Teamcenter	WINDOWS 2003	Centralizovaná databáza pre konštrukcie

Tabuľka 4 :Zoznam serverov

Servery pre údaje – obsahom sú údaje z jednotlivých oddelení :konštrukcia , nákup , účtovníctvo.

Licenčné servery – slúžia na podporu procesov pre oddelenie vývoja a konštrukcie

Teamcenter - je veľmi rozsiahly modulárny súbor aplikácií pre riadenie údajov o produkte. Je riadený centrálné , v rámci všetkých sekcií spoločnosti. Obsahom je podrobná spolupráca všetkých oddelení na každej procesnej zmene výrobných postupov , či zmene výkresovej dokumentácie komponentov ako nakupovaných ,tak vyrábaných.

10.6 Úrovne kritérií

Pri určovaní jednotlivých úrovní, sa musí brať do úvahy ,dôležitosť služby voči dĺžke výpadku elektrickej energie. (Tabuľka 5)

Do bezpečnostnej schránky majú prístup:

- Riaditeľ spoločnosti
- Určený pracovník IT oddelenia

Kópia dokladu o prístupe k bezpečnostnej schránke je archivovaná na IT oddelení spoločnosti .

Stupeň	Popis	Tolerovný výpadok
Úroveň 1	KRITICKÁ Táto služba je nevyhnutne potrebná a musí byť ako prvá obnovená	Max 24 hod
Úroveň 2	DÔLEŽITÁ Táto služba je dôležitá a musí byť odstránená následne	Max 72 hod
Úroveň 3	MENEJ DÔLEŽITÁ Táto služba je užitočná avšak nie je natoľko dôležitá	Max 120 hod

Tabuľka 5: Úrovne kritérií

Záloha údajov je vykonávaná každý pracovný deň na pásky označené poradovým číslom dňa, rotuje sa 5 pások. Okrem toho sa používajú tzv. mesačné pásky, na ktoré sa zachovávajú údaje raz za mesiac. Pásky s datami sú uložené v ohňovzdornom trezore YETI v určenej miestnosti . Raz týždenne je jedna páska uložená pracovníkom IT oddelenia v bezpečnostnej schránke v banke.

10.7 Serverovňa

Serverovňa je označenie pre špeciálny priestor pre umiestnenie počítačovej techniky serverového typu, ktorá je určená k nepretržitej prevádzke. Ide o miesto, ktoré má serverom a ďalším technologickým zariadeniam zaistiť bezproblémovú a stabilnú prevádzku, bez vplyvu okolia. Súčasťou serverovne je 9 serverov typu DELL PowerEdge R710.

Serverovňa je prepojená na switche Cisco Catalyst typu 2960, ktoré sú rozmiestnené po firme: výroba, oddelenie kontroly, sklad č.1, sklad č.2, oddelenie manažmentu, servis montáž.

Chladiaci systém

Serverovňa je vybavená dvoma klimatizačnými jednotkami INVENTOR, ktoré pracujú nepretržite celý rok. Teplota je v súčasnosti nastavená na 23°C.

Záložné zdroje

Serverovňa je zálohovaná záložným zdrojom Liebert NX 30 kVA (Obr.č. : 14). Tento typ zdroja je stredne veľký, trojfázový neprerušiteľný zdroj napájania (UPS), systém, ktorý poskytuje komplexné, centralizované dátové centrum s ochranou napájania. Je navrhnutý tak, aby spĺňal energetické potreby, bol dostupný širokej škále aplikácií.

Všetky servery aj zariadenia infraštruktúry siete LAN sú v prípade výpadku vonkajšieho prívodu elektriny napájané určitú dobu z tohto záložného zdroja.



Obr.č. : 14 Záložný zdroj Liebert NX 30 kVA

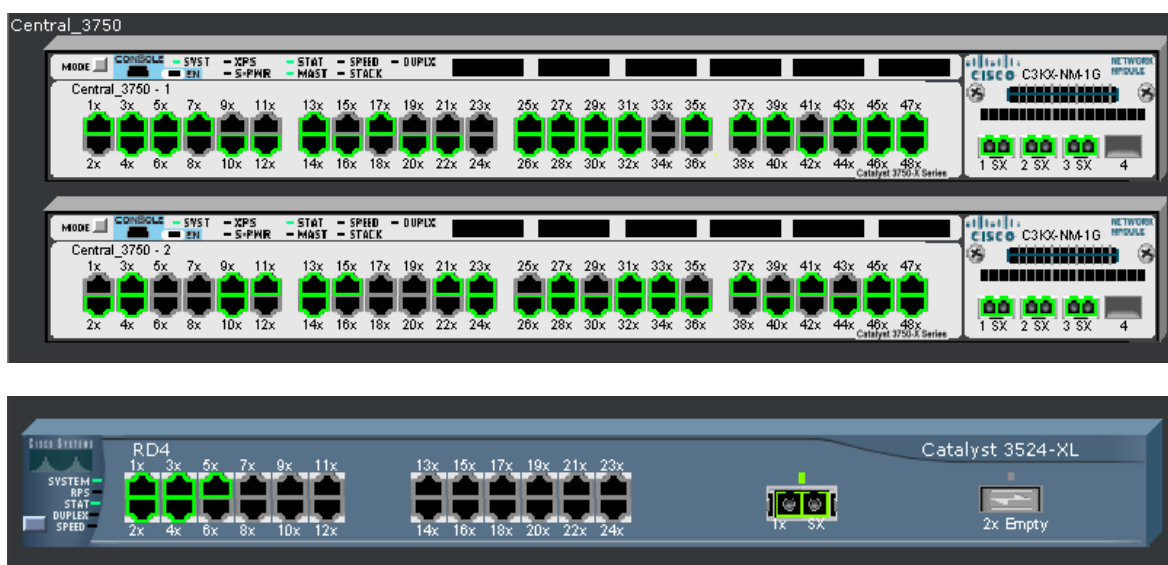
Prístup do serverovne

Do serverovne majú prístup dvaja pracovníci oddelenia IT –a finančný manažér. Ďalší rezervný kľúč je na recepcii. Prístup pomocou chipovej karty zriaďuje príslušný pracovník na správe budovy na základe povolenia vedúceho pracovníka žiadateľa.

10.7.1 Návh testu LAN konektivity

Ako návh testovania infraštruktúry v prípade, ak jeden zo switchov nebude pracovať.

T.1.1 – Výpadok jedného switchu



Obr.č. : 15 Schéma portov switchov

Postup testovania :

1. Vypnutie jedného aktívneho prvku
2. Prenesenie kritických portov do druhého aktívneho prvku
3. Test konektivity z kritických portov
4. Zapnutie vypnutého aktívneho prvku
5. Zapojenie kritických portov do východiskového stavu

Ako z popisu LAN infraštruktúry vidieť, v serverovni sú dva aktívne prvky.

V prípade výpadku jedného z nich sa prepoja kritické porty do funkčného zariadenia, pričom za kritické sú označené nasledujúce porty: 1.3, 1.4 , 1.6, 1.7, 1.8, 2.26, 2.27.

(Obr.č. : 15)

Tieto testovacie procedúry sú zamerané na výpadok jednotlivých častí systému, nesimulujú kompletný výpadok systémov.

10.7.2 Zhodnotenie ochrany serverovne

Serverovňa nie je z hľadiska ochrany pred požiarmi dostatočne chránená. Detekcia vzniku požiaru je jedna vec, ale dôležitou podstatnou úlohou je zabránenie šíreniu požiaru a hlavne jeho úplné zhasenie. Pre takéto úkony je nutné mať systém hasenia, ktorý je prepojený so systémom elektrickej požiarnej signalizácie, pomocou ústredne priamo ,alebo pomocou ovládacích prvkov .

Materiálna a finančná škoda, ktorá vznikne pri zhorení technologických procesov, škoda, ktorá vznikne pri odstávke zariadení je nevyčísliteľná.

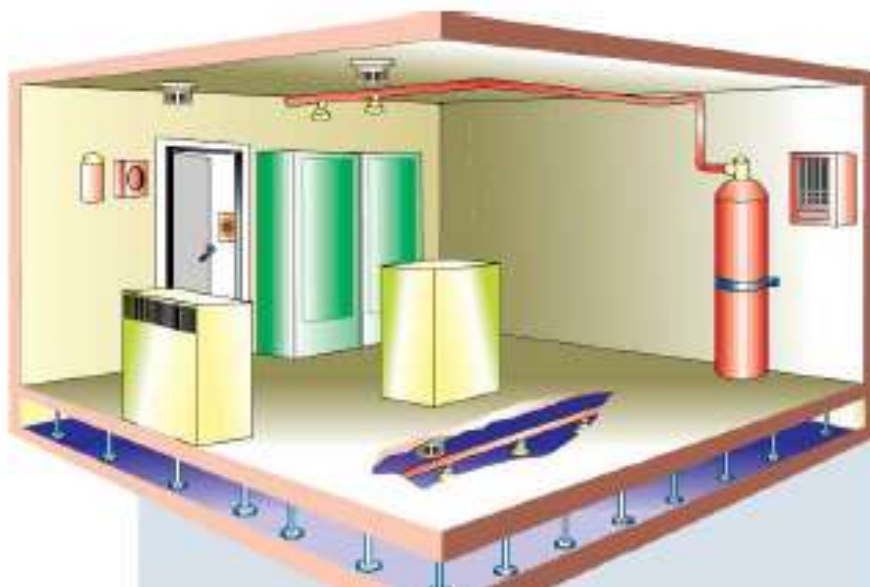
10.7.3 Návrh ochrany serverovne pred požiarmi

Princíp hasenia uzavretých priestoroch je nasledovný :Do daného priestoru, v tomto prípade serverovne, sa nainštalujú dva hlásiče, ktoré sú napojené na EPS, alebo k riadiacej jednotke. Tieto hlásiče sú vzájomnej závislosti. Keď sa aktivuje jeden hlásič, ústredňa spustí takzvaný predpoplach , v tomto momente zatiaľ nepríde k haseniu ,kompetentná osoba má čas aj priestor na kontrolu objektu. Hasenie sa aplikuje až v prípade, keď sa aktivujú oba hlásiče. Takýto systém by bolo vhodné doplniť o akustickú a optickú signalizáciu, ktorá nás informuje o predpoplachu ,ako aj o samotnom hasení.(Obr.č. : 16)

Na samotné hasenie v priestoroch ako serverovňa je odporúčaný zdraviu neškodný plyn FM 200 , ktorého chemická značka je CF₃-CHF-CF₃. [12] Jeho výhody :

- Doba spúšťania do 10 sekúnd
- Efektívna ochrana cenných či citlivých objektov
- Nehrozí nebezpečenstvo tepelného poškodenia potrubného systému
- Vhodný na použitie v obývaných priestoroch
- Nízke množstvo použitej hasiacej látky
- Nízka priestorová náročnosť na skladovanie
- Nízka hrozba kritického navýšenia tlaku
- Ľahké nahradenie už fungujúcich systémov

- Najvhodnejší na ochranu miestností počítačmi, telekomunikačnými zariadeniami, či inou výpočtovou technikou



Obr.č. : 16 Princíp hasenia

Princíp hasenia FM-200 je založený na absorpcii teploty plameňa a je teda najmä fyzikálnej povahy. FM-200 má hodnotu faktoru ODP 0, čo znamená, že vôbec nenarúša ozónovú vrstvu. Pozoruhodne krátka dĺžka atmosférického života je založená na relatívne krátkom procese prírodného rozkladu. Nevzťahuje sa naň Montreálsky protokol a teda jeho využitie nie je regulačne obmedzené. FM-200 je teda spoľahlivou, dlhodobou alternatívou bežným hasiacim produktom. [12]

11 IMPLEMENTÁCIA BEZPEČNOSTNEJ POLITIKY MIMO REŽIM HAVÁRIE

Po vytvorení bezpečnostnej politiky je dôležité, aby boli s dokumentom zoznámení všetci zamestnanci. Nie je nutné, aby sa zoznamovali s celým obsahom, ale iba s tými časťami, ktoré bezprostredne súvisia s výkonom ich pracovnej funkcie. V prípade rozsiahlejšej politiky je vhodné pripraviť tabuľku pracovnej role oblasti bezpečnostnej politiky, kde sa znamená, či je daná oblasť pre danú pracovnú funkciu potrebná.

Je taktiež dôležité, akou formou sú zamestnanci informovaní o bezpečnostnej politike. Nie je nič horšie, ako nudné a ubíjajúce školenie. Ak chceme dosiahnuť očakávaný efekt, je vhodné spolupracovať s profesionálmi.

11.1 Zhodnotenie postupov pri implementácii bezpečnostnej politiky

Aby bezpečnostná politika v spoločnosti fungovala je vhodné, aby sa vyvarovala problému a chybám hneď na začiatku.

● Veľké množstvo kompromisov

Ide o častý jav, kedy po procese schvaľovania z pôvodnej verzie zostane iba časť. Problematické pasáže nie je vhodné vypustiť, alebo prepísať. Taktiež právomoci a zodpovednosti nezdreďukovať na minimum. Politika by sa tak stala úplne sterilná a spoločnosť vlastne neumožní riešiť to, čo je skutočný problém.

● Nereálna bezpečnostná politika

Ide o veľmi prísnu politiku, kedy spoločnosti skoro vôbec nevyhovuje. Tu treba zadefinovať prechodné obdobie a postupný proces implementácie. V opačnom prípade môže nastať jav, že zamestnanci budú politiku ignorovať. Takáto neúcta potom zhorší situáciu v celej spoločnosti.

● Neadekvátny rozsah politiky

Ak sa manažmentu predloží rozsiahla politika, fakticky nemá možnosť zoznámiť sa dostatočne podrobne s celým dokumentom a pochopiť význam jednotlivých ustanovení. Obvykle spôsobí spomalenie, alebo zastavenie procesu schvaľovania politiky. Svoje výhody a nevýhody má ako krátko, tak rozsiahla politika. (Tabuľka 6)

	KRÁTKÁ POLITIKA	ROZSIAHLA POLITIKA
VÝHODY	• Relatívne jednoduchá a rýchla príprava dokumentov • Jednoduchší a rýchlejší proces • politiku nie je treba príliš často aktualizovať, je pomerne nemenná • bez problémov sa s politikou môžu zoznámiť všetci zamestnanci	• predstavuje veľmi komplexný kódex upravujúci oblasť informačnej bezpečnosti • definícia hlavných princípov a pravidiel je na jednom mieste • vzhľadom k detailom je eliminovaná možnosť prípadnej desinterpentácie alebo nepochopeniu • bezpečnostné štandardy upravujú veľmi detailne a špecificky oblasti informačnej bezpečnosti
NEVÝHODY	• hlavný objem prác je presunúť do fázy rozpracovania politiky do formy bezpečnostných štandardov • vzhľadom k rozsahu a obecnosti definovaných princípov politika mnoho nerieši • pre zamestnanca je problémom si pod obecnými termínmi predstaviť ich konkrétne plnenie	• pri akejkoľvek väčšej zmene v spoločnosti je treba politiku analyzovať, môže dôjsť k častým zmenám • práca na detailnej politike môže trvať neúmerne dlho a existuje značné nebezpečenstvo jej nevyváženosti • proces schvaľovania býva dlhý, komplikovaný s potrebou prijať radu kompromisov • zamestnanci sa nemôžu jednoducho zoznámiť s celou politikou a je potreba pre jednotlivé skupiny vytvoriť súhrny, ktoré so sebou prinášajú ďalšie náklady.

Tabuľka 6 : Rozdiely medzi krátkou a rozsiahlou politikou

● Podcenenie propagácie politiky.

V praxi je možné se stretnúť s prípadmi, kedy je existencia bezpečnostnej politiky pre väčšinu zamestnancov skrytá. Obvykle sa nejedná o úmysel, ale podcenenie či nezvládnutie komunikácie smerom dovnútra organizácie. Sebelepší dokument potom nepomôže ničomu, pokiaľ sa s jeho obsahom nezoznámia zamestnanci a pokiaľ sa podľa neho nebudú riadiť.

Zavedenie bezpečnostnej politiky predstavuje beh na dlhú trať a nikdy nekončiaci príbeh. Tento proces je v každej firme veľmi individuálny- ostatne ako riešenie celej problematiky bezpečnostnej politiky, pretože i keď sa to zdá veľmi podobné, nie sú dva úplne zhodné systémy, a už vôbec nie dve zhodné prostredia s rovnako zmýšľajúcimi manažérmi.

ZÁVER

Informačná bezpečnosť, bezpečnosť informácií, prosperita firmy, konkurencieschopnosť podniku, To sú všetko slovné spojenia, ktoré sa viažu k ochrane informácií s cieľom zabezpečiť ich primerané utajenie. Cieľom je zaistenie, aby niekto iný nezískal také možnosti, ktoré by mu umožnili získať zo spoločnosti informácie a ohrozili ju pri podnikaní. Ide o to, aby nedošlo k úniku informácií, prípadne aby nedošlo k fyzickému odstaveniu informačného systému.

K tomu je treba zaviesť vo firmách riešenie informačnej bezpečnosti s príslušným odborným personálnym obsadením v podobe informačného manažmentu a bezpečnostného informačného manažmentu. Prístup k tejto problematike je v každej organizácii špecifický. Sú však isté základné pravidlá a postupy ktoré by mali byť pre zaistenie informačnej bezpečnosti naplnené a to je cieľom aj tejto práce.

Informačná bezpečnosť má radu rovín, ktoré by sa dali charakterizovať ako koncepčné, riadiace, technologické, psychologické, právne a určite i nejaké ďalšie. Dnešní riadiaci pracovníci sú potom postavení pred úlohy, ktoré s informačnou bezpečnosťou súvisia a v rade svojich rozhodnutí sú nútení ich priamo do svojich úvah zahŕňať. K tomuto dochádza i keď im táto oblasť profesne neprináleží. Zo svojich pozíc a v rámci im dostupných nástrojov potom sami ovplyvňujú riešenia a riadenie informačnej bezpečnosti.

Vo svojej práci som sa zamerala na implementáciu bezpečnostnej politiky pre informačno-komunikačný systém. Poukázala som na nedostatky systému spoločnosti, ohľadom ochrany systému v spojitosti v prípade vzniku havárie. Následne som navrhla bezpečnostné riešenia na odstránenie uvedených nedostatkov systému, ktoré spĺňajú požiadavky bezpečnostnej politiky. Pre riešenia boli navrhnuté postupy, ktoré spĺňajú primeranú úroveň zabezpečenia s ohľadom na vlastníctvo spoločnosti a súčasný bezpečnostný stav. Tieto prostriedky spĺňajú environmentálne a hygienické normy.

Načrtla som fungovanie jednotlivých informačných prvkov a ich komunikácie s ohľadom na prvky zabezpečujúce objekt. Samotná spoločnosť aktívne hľadá riešenia nedostatkov a využíva možnosti inovovať informačný systém. V dnešnej dobe je veľmi dôležité držať

krok s vývinom technológií, nakoľko sa zvyšuje tlak na ochranu informačno - komunikačných systémov, pre udržanie bezproblémového chodu spoločnosti.

V práci nie sú použité fotografie z reálneho prostredia, ani uvedená presná spoločnosť, ktorej sa daná aplikácia návrhu týka z dôvodu dodržiavania bezpečnostnej politiky spoločnosti.

ZOZNAM POUŽITEJ LITERATÚRY

- [1] NAGY, P.2004. Bezpečnosť informačných systémov <http://fel.utc.sk/~nagy/>
- [2] DOSEĎEL, Tomáš. Počítačová bezpečnosť a ochrana dát, Brno: Computer Press,2004, ISBN 80-251-0106-1.
- [3] JAŠEK, Roman: Informační a datová bezpečnost. Univerzita Tomáše Bati ve Zlíně. 2006. 140s. ISBN 80-7318-456-7.
- [4] HANÁČEK, P.STAUDEK, J. 2000. Bezpečnost informačních systémů, Metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií, Úřad pro státní informační systém 2000
- [5] STN ISO/IEC TR 13335-1 Informačné technológie. Návod na manažérstvo bezpečnosti IT. Časť 1: Koncepcie a modely bezpečnosti IT
- [6] STN ISO/IEC TR 13335-3 Informačné technológie. Návod na manažérstvo bezpečnosti IT. Časť 3: Techniky pre manažment bezpečnosti IT
- [7] Zákon č. 363/2005 Z.z. Úplné znenie zákona č. 428/2002 Z.z. o ochrane osobných údajov. Dostupná z <http://www.zbierka.sk>
- [8] REITŠPÍS, Jozef. a kol.: Manažérstvo bezpečnostných rizík. 2004,
- [9] www.securityrevue.com.
- [10] Zbierka zákonov Slovenskej republiky. Dostupná z <http://www.zbierka.sk>
- [11] ONDRÁK,Viktor. SEDLÁK,Petr MAZÁLEK, Vladimír: Problematika ISMS v manažerské informatice , 2014
- [12] www.pyrokontrolslovakia.sk

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

ISMS	Systém riadenia bezpečnosti
IS	Informačné systémy
IT	Informačné technológie
LAN	Local area network
STN	Slovenská technická norma
SMK	Systém manažmentu kvality
ENVIRO	Enviromentálny
MK	Manažér kvality
FM	Finančný manažer
SpP	Smernica pre proces
RS	Riaditeľ spoločnosti

ZOZNAM OBRÁZKOV

Obr.č. : 1 Skladba informačného systému	11
Obr.č. : 2 Možný obsah a štruktúra pojmu bezpečnosť [8].....	15
Obr.č. : 3 Schéma bezpečnostnej politiky organizácie . [9]	16
Obr.č. : 4 ISMS Procesný prístup[11].....	18
Obr.č. : 5 Geofyzikálna mapa Slovenskej republiky	28
Obr.č. : 6 Organizačná schéma zodpovedností.	31
Obr.č. : 7 Strategické riadenie podniku	32
Obr.č. : 8 Procesná mapa spoločnosti	34
Obr.č. : 9 Postup pri odstraňovaní nehody.....	38
Obr.č. : 10 Prenosová trasa údajov pre Movex.....	40
Obr.č. : 11 Krútená dvojlinka FTP	43
Obr.č. : 12 Tienený konektor RJ-45	44
Obr.č. : 13 Zachytenie podozrivého mailu	49
Obr.č. : 14 Záložný zdroj Liebert NX 30 kVA.....	57
Obr.č. : 15 Schéma portov switchov.....	58
Obr.č. : 16 Princíp hasenia.....	60

ZOZNAM TABULIEK

Tabuľka 1:Nápravné a preventívne opatrenia.....	38
Tabuľka 2 :Stupne havárií	53
Tabuľka 3: Komunikačné procedury	54
Tabuľka 4 :Zoznam serverov	55
Tabuľka 5: Úrovne kritérií.....	56
Tabuľka 6 : Rozdiely medzi krátkou a rozsiahlou politikou	62

ZOZNAM PRÍLOH

Príloha č.: 1 : Schéma napojenia serverovne.....	70
Príloha č.: 2 : Špecifikácia serverov 5 strán.....	71