Návrh implementace bezpečnostní politiky v informačním a komunikačním systému

Design implementation security policy in the information and communication system

Bc. Andrej Čavojský

Diplomová práca
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

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

Jméno a příjmení:	**Bc. Andrej ČAVOJSKÝ**
Osobní číslo:	**A11344**
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**

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 navrhněte implementaci bezpečnostní politiky.**
4. **Proveďte zobecnění/ doporučení pro postup při zvládání rizik – implementaci bezpečnostní politiky v objektech obdobného typu.**
5. **Naznačte vývojové trendy v implementaci zásad bezpečnosti informačních a komunikačních systémů.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **JAŠEK, Roman: Ochrana znalostí a dat v podnikových informačních systémech. Zlín : Univerzita Tomáše Bati ve Zlíně, 2002. 115 s. ISBN 80-7318-095-2.**
2. **JAŠEK, Roman: Informační a datová bezpečnost. Univerzita Tomáše Bati ve Zlíně. 2006. 140s. ISBN 80-7318-456-7.**
3. **MALANÍK, David: Význam fyzického zabezpečení IT systémů. Security Revue září 2010. ISSN 1336-9717.**
4. **Ludvík Miroslav: Teorie bezpečnosti poč. sítí. Computer Media. 98str. ISBN: 80-86686-35-3.**
5. **Thomas, Thomas M. : Zabezpečení počítačových sítí bez předchozích znalostí. Vyd. 1. Brno : CP Books, 2005. 338 s. ISBN 80-251-0417-6.**
6. **Doseděl, Tomáš: Počítačová bezpečnost a ochrana dat. Vyd. 1. Brno : Computer Press, 2004. ix, 190 s. ISBN 80-251-0106-1.**

Vedoucí diplomové práce: **doc. Ing. Jiří Gajdošík, CSc.**
Ústav bezpečnostního inženýrství

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

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

Ve Zlíně dne 8. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
Ředitel ústavu

ABSTRAKT

V diplomovej práci sa zaoberám priamou implementáciou bezpečnostnej politiky do bezpečnostného systému. Spomenutú bezpečnostnú politiku som navrhol v rámci bakalárskej práce. Prvým krokom bude rozdelenie informačno-komunikačného systému a následne analýza jednotlivých blokov. Po analýze blokov budem navrhovať už priamo technické a SW riešenia podľa bezpečnostnej politiky.

Kľúčové slová:

Hardware; Software; Počítačová sieť; Bezpečnostná politika.

ABSTRACT

At the master work I deals with the direct implementation of security policy to the security system. I proposed mentioned security policy at the bachelor work. The first step will be dividing of information and communication system, and then analysis of individual blocks. After analyzing the blocks I will suggest technical and SW solutions according to security policy.

Keywords:

Hardware, Software, Computer Network, Security Policy.

Chcel by som poďakovať pánovi Doc. Ing. Jiřimu Gajdošíkovi CSc., za odbornú pomoc a konzultácie pri písaní tejto diplomovej práce, za poskytnutie potrebných informácii, cenných námetov a rád.

Motto:

Systém je tak bezpečný, ako je jeho najzraniteľnejší článok.

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

Implementácia bezpečnostnej politiky je neodmysliteľným ďalším krokom pre správne zavedenie alebo funkčnosť informačno-komunikačného systému. Implementácia bezpečnostnej politiky musí mať plnú podporu vedenia spoločnosti a mať dostatočný prídel financií pre jej implementáciu. V súčasnej dobe je nutné mať prijaté bezpečnostné opatrenia pre systémy vzhľadom na rýchle tempo meniacich sa technológii a nárast kybernetickej kriminality.

Je dôležité, aby sa situácia v tejto oblasti začala meniť. Všetky spoločnosti by si mali uvedomiť riziká plynúce z používania informačných technológii a aké dôsledky môže mať zanedbanie prípravy bezpečnostnej politiky a podcenenie samotnej implementácie. V prípade bezpečnostného incidentu sa spoločnosti dostávajú do ťažkej situácie. Z nej sa jednoduchšie budú dostávať tie spoločnosti, ktoré budú mať kvalitný núdzový plán. Pre spoločnosti s vybudovanou bezpečnostnou politikou platí: „I najspoľahlivejší bezpečnostný systém je iba teoretickou obranou proti útokom, pokiaľ nie je vyskúšaný v praxi. Samozrejme nemá zmysel čakať na skutočný útok, ideálne je riadená skúška robustnosti a spoľahlivosti bezpečnostných opatrení, ktorými firma chráni citlivé dáta“, ako tvrdia správcovia siete v spoločnosti Freedivision.

I. TEORETICKÁ ČASŤ

1 BEZPEČNOSTNÁ POLITIKA

1.1 Vymedzenie pojmov

Na začiatok tejto práce, ktorá je venovaná implementácii bezpečnostnej politiky, je vhodné ozrejmiť si základné pojmy, ktoré sa využívajú v práci a stretávame sa s nimi všeobecne i v spojitosti s problematikou bezpečnostnej politiky.

Dáta

Dáta sú údaje vo forme, ktorá sa dá spracovať pomocou informačných technológií, pričom údaj je formalizovaná charakteristika známeho, neznámeho deja alebo javu.

Dáta sú fakty získané výpočtom, pozorovaním, čítaním, meraním ... Chápeme ich ako :

1. Vyjadrenie myšlienok a skutočností v predpísanej podobe, aby ich bolo možné spracovávať a prenášať.
2. Sledovateľné a objektívne vyjadrenie skutočností alebo znalostí na médiu tak, aby ich bolo možné odovzdávať.
3. Vyjadrenie faktov a poznatkov vo forme, ktorá je vhodná pre ďalšie spracovanie.

Informácia

Pojem informácia patrí k veľmi všeobecným kategóriám súčasnej vedy, pričom k dispozícii sú rôzne skupiny definícií a podľa vedeckého odboru sa aplikujú jednotlivé prístupy ku skúmaniu informácií.

„ Informácia je poznatok tykajúci sa akýchkoľvek objektov, napr. faktov, udalostí, vecí, procesov alebo myšlienok vrátane pojmov, ktoré majú v danom kontexte zmysel. “[1]

Informácia nie je akýmkoľvek zdelením, ale ide iba o zdelenie, ktoré prináša niečo nové, doteraz nepoznané. Informácie sa v organizácii využívajú na ovplyvňovanie technologických, manažérskych, informačných a iných procesov, pričom ich obsahom sú predovšetkým vzťahy ľudí k manažérskej aktivite, konkrétne medziľudské vzťahy, ich vzájomné pôsobenie, potreby ľudí, ich záujmy a ciele. Využiteľná informácia je tovar, ktorý má určitú cenu a táto cena sa odvíja od mnohých faktorov. V tejto súvislosti je potrebné posúdiť hodnotu informácie.

Pre efektívne fungovanie spoločnosti sa vyžaduje, aby informácie, ktoré má pracovník firmy k dispozícii boli komplexné, presné, úplné, spoľahlivé, logicky usporiadané a užitočné.

Informačný systém

Pojem systém môžeme definovať v širšom a užšom význame. V širšom význame rozumieme informačným systémom - systém na zabezpečovanie informácií potrebných na riadenie, konkrétne informácií súvisiacich so spracovaním, prenosom, uchovávaním, zhromažďovaním, výberom a distribúciou údajov pre potreby riadiaceho subjektu. V užšom význame ide o označenie systému programov pre prácu s údajmi, ktorého primárnou úlohou je spracovanie údajov prameniacich z činnosti spoločnosti, pričom však nerieši problémy spojené s ďalšou úpravou údajov.

Informačný systém zahŕňa komplex prvkov nachádzajúcich sa vo vzájomnej interakcii. Môžeme ho vyjadriť pomocou vzorca S = (Q, a) kde systém (S), dynamický s účelovým správaním, je konečnou množinou prvkov (Q) a množina väzieb medzi nimi (a). Systém vyjadruje určitú abstrakciu reálneho sveta, ktorú môžeme definovať pri rešpektovaní vlastností prvkov danej množiny a väzieb medzi nimi. Informačný systém je súbor ľudí, technických prostriedkov a metód zabezpečujúcich viacero činností.

Všeobecne možno informačný systém chápať ako podporný systém riadenia. Pokiaľ chcem tento systém riadenia zdokonaľovať, musíme ho dobre poznať, stanoviť si naše ciele a koordinovať ho spôsobom, aby tieto naše ciele podporoval. Dobre skonštruovaný informačný systém je vynikajúcou pomôckou manažéra. Nesmie sa však stať nadradeným elementom, ktorý je nadriadený všetkým užívateľom. Naopak, informačný systém má slúžiť, pretože o ňom platí, že je „dobrý sluha, ale zlý pán“.

Informačná bezpečnosť

Zjednodušene povedané ide o ochranu informačno-komunikačných technológií a všetkého s nimi súvisiaceho. V zmysle informatizácie môžeme informačnú bezpečnosť definovať ako: *"Schopnosť siete alebo informačného systému ako celku odolať s určitou úrovňou spoľahlivosti náhodným udalostiam, alebo nezákonnému, alebo zákernému konaniu, ktoré ohrozuje dostupnosť, pravosť, integritu a dôvernosť uchovávaných alebo prenášaných údajov a súvisiacich služieb poskytovaných alebo prístupných prostredníctvom týchto sietí a systémov."* [2]

Je to komplex opatrení zahrňujúci proces navrhovania, schvaľovania a implementácií implementáciou softwarových, hardwarových, technických, personálnych ochranných opatrení spojených s minimalizáciou možných strát, predchádzaniu vzniku škôd, zničeniu alebo zneužitiu informačných systémov.

Narušenie bezpečnosti môže byť spôsobené mnohými faktormi – napr. poškodenie vzhľadu webovej stránky, napadnutie počítača, resp. systému škodlivým softvérom, zlyhanie zamestnanca, ktorý neúmyselne prezradí svoje heslo, zlyhanie bývalého zamestnanca, ktorý sabotuje zákaznícku databázu alebo práca priemyselného špióna, ktorý zistí interné údaje spoločnosti. Najčastejšími faktormi narušenia bezpečnosti sú krádeže, zneužitia a neoprávnené manipulácie s informáciami.

IT management

IT management zameriava svoju pozornosť na efektívne poskytovanie služieb a produktov IT a na účinné riadenie rozvoja a prevádzky IT. Jeho cieľom je efektívne a účinne realizovať stanovené ciele, k čomu využíva taktické a operatívne riadenie.

IT governance

IT governance znamená zodpovednosť najvyššieho vedenia, ktoré svojimi úlohami a vnútornými procesmi zaisťuje, že IT prispieva k realizácii dlhodobých cieľov spoločnosti a prehlbuje stratégiu spoločnosti. V podstate je snahou definovať strategické ciele IT v súlade s potrebami a záujmami celej organizácie.

Dôvernosť aktíva

Informačné aktíva sú všetky aktíva obsahujúce informácie potrebné na realizovanie podnikateľských aktivít alebo sú prostriedkom na využívanie iných aktív. Dôveryhodnosť aktíva je jedným z jej najpodstatnejších znakov, pretože zachovávanie aktív je vlastne dôvodom vzniku informačnej bezpečnosti. Tento znak má zabezpečiť, aby boli informácie prístupné výhradne tým osobám, ktoré majú oprávnenie k ich prístupu.

Dostupnosť aktíva

Dostupnosť aktíva je ďalším z jej atribútov. Jeho cieľom je zaistiť, aby oprávnení užívatelia mali, keď to budú potrebovať, prístup k informáciám a pridruženému majetku.

Integrita aktíva

Úlohou tohto atribútu aktíva je zabezpečiť presnosť a úplnosť informácií a spôsobov ich spracovania.

Bezpečnostná udalosť

Ide o definovanie stavu informačného systému, služby alebo počítačovej siete, ktorý môže viesť k narušeniu pravidiel bezpečnostnej politiky alebo k zlyhaniu niektorého opatrenia. Rovnako môže ísť o predtým neznámu alebo nepredvídanú situáciu, ktorá má potenciál zasiahnuť do bezpečnosti.

Bezpečnostný incident

Jedná sa o jednu alebo niekoľko nežiaducich alebo neočakávaných vyvolaných bezpečnostných udalostí prostredníctvom ktorých môže byť s vysokou mierou pravdepodobnosti narušená podpora hlavných úloh spoločnosti alebo ktoré môžu zapríčiniť narušenie bezpečnosti informačného systému.

Identifikácia

Identifikácia je prostriedkom pomocou ktorého rozpoznávame systém. Spravidla sa pri jeho realizácii využívajú na pomoc prostriedky výpočtovej techniky užívateľských mien. Mená sú jedinečné v rámci určitej skupiny, ktorej rozsah je daný systémovou politikou.

Autentizácia

Autentizácia je proces overovania identity subjektu. Ide o overovania pravosti, čo sa viaže k základu slova autentický – pôvodný, pravý, hodnoverný. Autentizáciu zaraďujeme k bezpečnostným opatreniam, zabezpečuje ochranu pred falšovaním identity, kedy sa subjekt vydáva za niekoho, kým nie je. Autentizáciu rozlišujeme na autentizáciu entity (osoby, programu, zariadenia) a autentizáciu správy.

Autorizácia

Autorizácia je procesom zisťovania oprávnenosti. Význam slova autorizovať je povoliť, schváliť, zmocniť, oprávniť. Ide o prípad, keď určitá entita (užívateľ, program, zariadenie) chce pristupovať k určitým zdrojom (napr. serveru, súboru, tlačiarni). Aby sa

tak mohlo stať a určitá entita pristúpila k zdrojom, musí byť autorizovaná, t.j. oprávnená, musí mať prístupové práva. Predpokladom autorizácie entity je tak úspešná autorizácia.

Hrozby

Aktíva sú predmetom mnohých typov hrozieb. Hrozbu definujeme ako potencionálnu schopnosť spôsobiť nežiaducu situáciu, ktorá môže viesť k poškodeniu systému alebo spoločnosti a jej aktív. Táto škoda môže byť dôsledkom priameho alebo nepriameho útoku na aktíva. Hrozba využíva zraniteľnosť aktív k tomu, aby spôsobila ich poškodenie.

Zraniteľnosť miesta

Zraniteľným miestom nazývame slabinu, ktorú môže hrozba využiť k spôsobeniu škody alebo straty. Zraniteľnosť sama o sebe nemusí byť príčinou škody, ale ide o podmienku, ktorá umožní hrozbe, aby ovplyvnila aktíva. Zraniteľnosť môže vzniknúť z rôznych zdrojov, jednotlivé zdroje ako aj samotná zraniteľnosť by mali byť monitorované, pretože môže dochádzať k dynamickej zmene prostredia. Vďaka tomu môžu byť identifikované zraniteľnosti, ktoré sa stali terčom starých alebo nových hrozieb.

1.2 Úvod do problematiky

„Informačný systém organizácie predstavuje súbor činností, ktoré zabezpečujú zhromažďovanie, prenos, uchovávanie, spracovávanie, distribúciu a prezentáciu informácií v organizácii na potreby rozhodovania tak, aby riadiaci pracovníci mohli efektívne vykonávať svoje riadiace funkcie.“ [3]

Firmy a ich informačno-komunikačné systémy sú v súčasnej dobe neustále vystavované hrozbám, ktoré môžu narušiť plynulý chod firmy alebo spôsobiť finančné problémy. Hrozby môžeme rozdeliť do troch kategórii:

1, Fyzický útok

2, Útok z „vonku“ (z internetu)

3, Útok z „vnútra“ (vlastný zamestnanec)

1.3 Návrh nových a doplňujúcich protiopatrení

Na základe bezpečnostného zámeru a analýzy kvalitatívneho zabezpečenia sú navrhované bezpečnostné opatrenia, ktoré sú v zhode s bezpečnostnými štandardami, vyhlásenými Výnosom Štatistického úradu Slovenskej republiky č. 372/1998-830, v znení Výnosu č. 1490/1999-833, a štandardami, ktoré obsahujú bezpečnostné normy ISO 17799/2000 a ISO/IEC TR 13335. V súčasnej dobe sú tieto normy zjednotené do normy STN ISO/IEC 27001 ; STN ISO/IEC 27002; STN ISO/IEC 27005.

Za účelom dosiahnutia ochrany spoločnosti a bezpečnosti dát a informácií je nevyhnutné zabezpečiť bezpečnostné požiadavky. To možno dosiahnuť prostredníctvom procesu riadenia informačnej bezpečnosti, ktorý je založený na vyššie spomenutých normách. Tento proces pozostáva z niekoľkých čiastkových procesov:

- definovanie cieľov informačnej bezpečnosti, analýza rizík,
- návrh systémovej bezpečnostnej politiky,
- plán bezpečnosti IT na nasledujúce obdobie,
- havarijný plán, plán obnovy prevádzky,
- audit a testovanie bezpečnosti IT,
- projekty riešiace bezpečnostné problémy.

1.4 Porovnanie noriem Slovenskej republiky a Českej republiky

Na Slovensku platia medzinárodné normy prebrané od International Organization for Standardization a International Electrotechnical Commission rady 27000. Je to zlúčenie noriem ISO 17799/2000 a ISO/IEC TR 13335/2004. Tieto normy sú rozpracované do 3 podskupín:

1. STN ISO/IEC 27001 Systémy manažérstva informačnej bezpečnosti.
2. STN ISO/IEC 27002 Pravidlá dobrej praxe manažérstva informačnej bezpečnosti
3. STN ISO/IEC 27005 Bezpečnostné metódy. Riadenie rizík informačnej bezpečnosti

V Českej republike prebehol podobný proces ako v Slovenskej republike. Prebehla novelizácia noriem a boli prijaté 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

Ako je zrejmé zo zoznamov, obidva štáty prevzali normy od medzinárodných normalizačných organizácii. Česká republika má prijatých viacej noriem rady 27000. V skutočnosti, obidva štáty majú prijaté rovnaké normy len, na rozdiel od Českej republiky ich má Slovensko zjednotené do 3 noriem.

1.5 Plán implementácie nových a doplňujúcich 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 najúčinnejšie. 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.

2 ISMS - INFORMATION SECURITY MANAGEMENT SYSTEM

2.1 Čo je ISMS

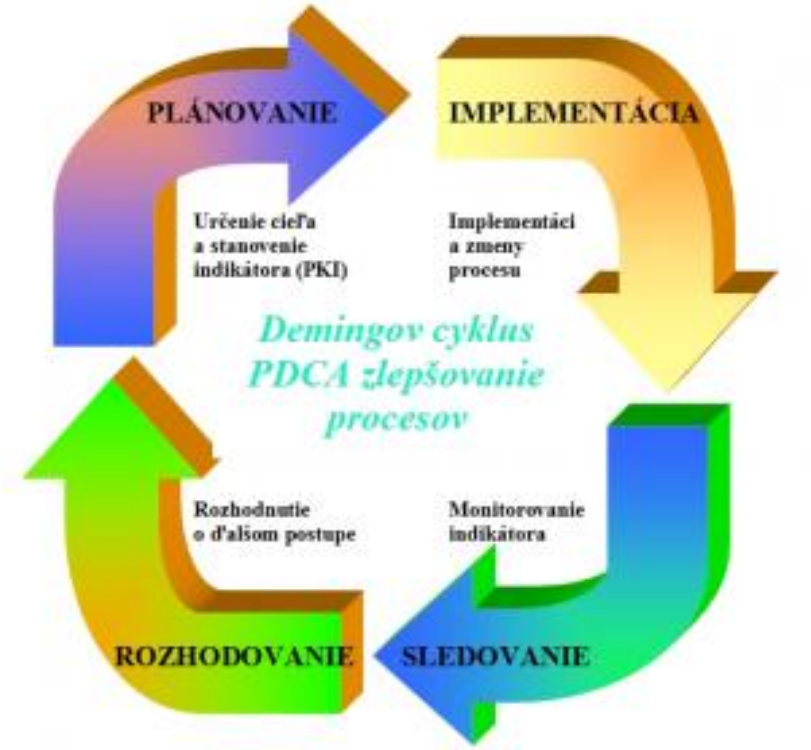
Základ bezpečnostnej politiky tvorí ISMS (Information Security Management System, v preklade Manažment bezpečnosti informačného systému). Je to politika, súbor pravidiel a riadenie systému zameraného na zabezpečenie informačného systému. Pomocou ISMS stanovujeme potrebné stupne ochrany, vytvárame plány bezpečnosti založené na zhodnotení vlastných rizík organizácie. ISMS obsahuje odpovede, postupy, čo sa má spraviť v prípade výskytu nežiadanej situácie alebo čo robiť, aby takáto situácia nenastala.

Hlavným významom ISMS je, aby organizácie navrhli spôsoby ako rovnomerne posilňovať dôveryhodnosť, integritu a dostupnosť informačných aktív, ktoré sú prioritne chránené spoločnosťou. Spoločnosti zvyšujú svoju informačnú bezpečnosť najúčinnejšie prostredníctvom vyhodnotenia efektívnosti riadenia implementovaného v ISMS s prihliadnutím na možné riziká. V tejto súvislosti aby ISMS ostalo efektívne a účinne po čo najdlhší čas, je nevyhnutné aby bolo v súlade so všetkými procesmi stanovenými manažmentom. ISMS sa musí vedieť prispôsobiť zmenám vo vnútorných aktivitách organizácie, ale súčasne i vonkajšiemu vplyvu. K tomuto slúži priebehov metóda známa ako PDCA.

2.2 PDCA

PDCA je štvorkrokový postup používaný ako jeden najtypickejších nástrojov na zdokonaľovanie procesov. Anglický názov tvoria štyri slová plan, do check a act (v preklade plánovanie, implementácia, overenie, údržba), ktoré súčasne pomenovávajú jeho fázy. Tento proces spočíva na princípe iterácie, to znamená, že po zadaní hypotézy sa vykoná cyklus, a ten následne prinesie ďalšie poznatky pre novú hypotézu. Opakovanie PDCA cyklov nám zabezpečí minimalizovanie bezpečnostných hrozieb. Zo zdrojov manažmentu vychádzajú procesy, na ktoré je táto priebehová metóda viazaná a ktorými sú riadené všetky aktivity. Účelom týchto procesov je transformovať vstupy na výstupy. Významom PDCA je rozlíšiť v spoločnosti jednotlivé procesy, využiť ich vzájomnú

interakciu, s následným cieľom aplikácie a využitia totožných procesov ako systémového celku. Využívanie metódy PDCA prináša spoločnostiam viaceré výhody. Sú nimi znalosť efektívnej obsluhy ISMS v dôsledku vzájomného pôsobenia procesov a ich ovládacích prvkov. Správna aplikácia PDCA modelu do informačno-bezpečnostných procesov dokáže zabezpečiť ochranu informačného systému a prostredníctvom toho uspokojiť nároky a očakávania užívateľov na bezpečnosť. Dôsledkom takejto správnej aplikácie PDCA je súčasne získanie výsledkov, z výstupov zo spracovaných procesov, ktoré môžu byť neskôr využité ako vstupy pre ďalšie požiadavky užívateľov. Primárny význam využitia modelu PDCA spočíva vo vylepšení procesov smerujúcich k produkcii využiteľných výstupov.



Obrázok 1: PDCA model

2.3 Fázy PDCA

2.3.1 Plan (plánuj, resp. vytvorenie ISMS)

V tejto fáze sa vytvárajú ISMS zásady, ciele, procesy, procedúry dôležité pre zachytenie rizík a rozvoj informačnej bezpečnosti v podobe v akej si to politika a ciele spoločnosti žiadajú. Fáza plan začína získavaním informácií a vytýčením problému, ktorý je smerodatný pre pripravenie plánu, teda analýzou. Obsahom analýzy by mali byť činnosti potrebné pre úspešné uskutočnenie odstránenie problému. PDCA nevymedzuje presný spôsob ako treba údaje analyzovať, preto analýza prebieha prostredníctvom samostatného procesu. Rozoznávame analýzu:

- korelačnú
- príčinno-následnú (cause-and-effect)
- nákladovej efektívnosti
- komparatívnu
- zohľadňujúcu externé odporúčania

Zrealizovanie zmeny vyžaduje zistenie a následné porozumenie príčinám konkrétneho problému a súčasne rozpoznať spôsob akým sa tieto problémy prejavujú. Teda vyhovieť požiadavkám zákazníka a odstrániť ich nesúlad s realitou. Pri riešení problému je nevyhnutné vytýčiť si niekoľko skutočností ako:

- ktorý proces sa má zlepšiť,
- do akej miery je zlepšenie potrebné,
- opísať zmenu, ktorá sa navrhuje,
- kedy bude zmena realizovaná
- akým spôsobom bude meraný efekt zmeny,
- čo táto zmena ovplyvní (dokumenty, metódy a pod.).

2.3.2 Do (rob, resp. implementácia a obsluha ISMS)

Táto fáza sa sústreďuje na implementáciu a obsluhu ISMS zásad, riadenia procesov a procedúr. Spočíva teda v implementácii zmeny v súvislosti s ktorou je nevyhnutné identifikovať ľudí, ktorý budú zmenou dotknutý a sprostredkovať im informáciu

o zavádzaní zmeny. Informovanie o zmene by malo obsahovať aj dôvod, prečo sa takáto zmena uskutočňuje. Prejavený efekt bude súvisieť aj s podnetmi a zisteniami subjektov informovaných o zmene. V nasledujúcej fáze budú získané dáta využité v ďalšom postupe. Zmeny je nutné monitorovať a tak sa ubezpečiť, že zmena neprinesie negatívne pôsobenie v systéme, prípadne toto eliminovať negatívne pôsobenie zmeny v systéme ak by nastalo.

2.3.3 Check resp. study (kontroluj, študuj, resp. monitorovanie a zhodnotenie ISMS)

Ide o fázu hodnotenia, v ktorej sa meria účinok procesov v súvislosti s ISMS zásadami, cieľmi, praktickými skúsenosťami a následne sa zapisujú výsledky pre posudok manažmentu spoločnosti. To znamená že sa sledujú dosiahnuté výsledky a tieto sa porovnávajú s plánom, ktorý predchádzal uskutočneniu zmeny. Dáta z predošlej fázy sa analyzujú. Analýza si vyžaduje položenie niekoľkých otázok:

- priniesol proces zlepšenie?
- do akej miery priniesol proces zlepšenie?
- podarilo sa naplniť naplánované ciele?
- spôsobilo zavedenie zmien skomplikovanie procesu?

2.3.4 Act (konaj, resp. udržiavanie a zdokonaľovanie ISMS)

Fáza slúžiaca na zrealizovanie nápravných a preventívnych krokov v spojitosti s výsledkami vnútornej kontroly ISMS a posudkami manažmentu, prípadne inými relevantnými informáciami. Cieľom je dosiahnuť pribežné a trvácne zlepšenie ISMS. V prípade, že sa výsledok kontroly líši od očakávaní a problém nie je vyriešený, je nevyhnutné nájsť príčinu problému. Nový plán tak bude zameraný na odstránenie príčin. Ak sa problém podarí úspešne odstrániť (dosiahnuť vytýčené ciele), je potrebné zmeny zaviesť do procesov alebo systému (štandardizovať ich). Treba sa presvedčiť, že všetky zmeny sa riadne uplatňujú a využívajú sa pri bežných každodenných činnostiach.

II. PRAKTICKÁ ČASŤ

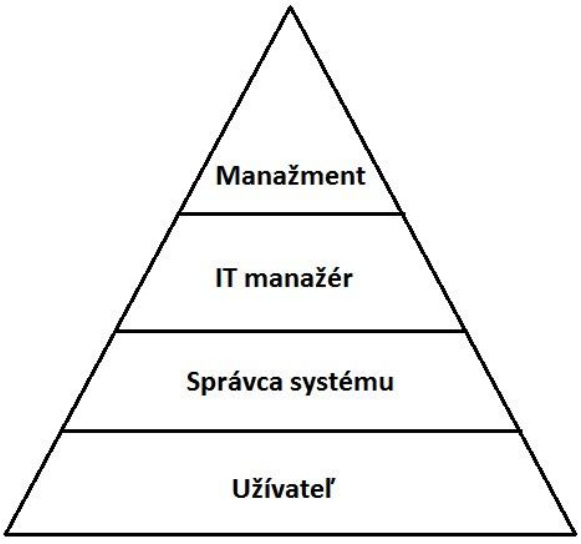
3 ORGANIZAČNÁ ŠTRUKTÚRA IT BEZPEČNOSTI

„Spoločnosť XYZ sa radí k mladším expandujúcim spoločnostiam na trhu so spotrebnou elektronikou. Hlavné zameranie spoločnosti je výroba zobrazovacích zariadení.. V súčasnosti exportuje produkty do celej Európy. Je významnou konkurenciou spoločnostiam Samsung, LG, Sony ...

Spoločnosť zamestnáva približne 400 výrobných zamestnancov a 100 administratívnych zamestnancov. Má vlastné výrobné priestory, v ktorých prebieha samotný proces výroby, proces návrhu, zhotovenia vzorových produktov a všetka administratívna činnosť spoločnosti. Z toho vyplýva, že disponuje veľkým množstvom osobných údajov o zamestnancoch, zákazníkoch, know-how, spôsob výroby, marketingový štýl, informácie o účtoch zákazníkov ako aj vlastných.

3.1 Rozdelenie povinností

Pre správnu funkčnosť bezpečnostnej politiky v spoločnosti je potrebné správne prerozdelenie povinnosti a právomoci. Na obrázku 1 je znázornená pyramída dôležitosti právomocí v spoločnosti.



Obrázok 2: Štruktúra právomocí pre IKS

3.1.1 Manažment

Úloha funkcie: Najvyššia riadiaca a kontrolná autorita spoločnosti, ktorá schvaľuje projekty a rozhoduje o uvoľňovaní finančných prostriedkov a ľudských zdrojov. Vyhodnocuje výsledky bezpečnostných auditov v spoločnosti.

Spôsob výkonu funkcie: Všetky rozhodnutia vykonáva na základe vyhodnotenia auditov a predloženia argumentov s prognózami o výsledkoch projektov.

3.1.2 IT manažér

Úloha funkcie: Zodpovedná osoba za implementovanie a dodržiavanie bezpečnostnej politiky pre IKT. Vytvára bezpečnostné projekty pre IKT, hlavný koordinátor interných auditov a riadi oddelenie IT.

Spôsob výkonu funkcie: Postupuje podľa medzinárodnej normy ISO 27001, ktorá je aktualizáciou normy BS 7799/ISO 17799 a podľa svojich doteraz získaných vedomostí.

3.1.3 Správca systému

Úloha funkcie: Je zodpovedný za správnu realizáciu bezpečnostných projektov, dohliada na dodržovanie bezpečnostnej politiky a predkladá návrhy IT manažérovi pre zlepšenie bezpečnosti systémov.

Spôsob výkonu funkcie: Kontroluje a uchováva všetky záznamy z monitorovacích systémov, vyhodnocuje všetky incidenty v IKS a všetky pokusy o preniknutie do IKS. IT manažérovi pravidelne predkladá správy a štatistiky z pokusov o porušenie integrity IKS. Jeho ďalšou úlohou je pravidelná aktualizácia systému a zabezpečenie bezproblémovej činnosti hardwaru.

3.1.4 Užívateľ

Úloha funkcie: Je to zamestnanec spoločnosti, ktorý pri svojej činnosti potrebuje IKS. V systéme pracuje v rozsahu pridelených práv pridelených administrátorom systému.

Spôsob výkonu funkcie: Každý užívateľ sa pre prácu v systéme musí prihlásiť menom a heslom, ktoré mu bolo pridelené pri nástupe do práce. Môže používať iba aplikácie, ktoré

mu boli povolené administrátorom. Užívateľ musí dodržiavať bezpečnostnú politiku, s ktorou bol oboznámený pri nástupe do práce.

3.2 Audit

Definícia: Audit je systematický proces objektívneho získavania a vyhodnocovania dôkazov, týkajúcich sa informácií o činnostiach a udalostiach, s cieľom zistiť mieru súladu medzi týmito informáciami a stanovenými kritériami a oznámiť výsledky zainteresovaným stranám. Audit je spôsob, ktorým je jedna osoba ubezpečená druhou o kvalite, podmienkach alebo stave predmetnej veci, ktorú druhá osoba skúmala.

3.2.1 Interný audit

Úloha: Priebežná kontrola stavu IKS, vyhodnotenie nápravných opatrení bezpečnostných incidentov, overenie povedomia o bezpečnostnej politike.

Spôsob výkonu: Audit sa vykonáva náhodne, ale musí sa vykonať minimálne 3x ročne. Náhodne sú vybraní zamestnanci, ktorí sú preverení bezpečnostným testom. Bezpečnostný test je zložený z otázok vyplývajúcich z bezpečnostnej politiky a je zostavený IT manažérom. Systém je preverený penetračným testom a výsledky sú vyhodnotené.

3.2.2 Externý audit

Úloha: Tento audit sa vykonáva pri certifikácii, či sú dodržané normy a predpisy podľa svetových štandardov. Externý audit sa vykonáva aj pri overení dodržiavania bezpečnostnej politiky a integrity systému.

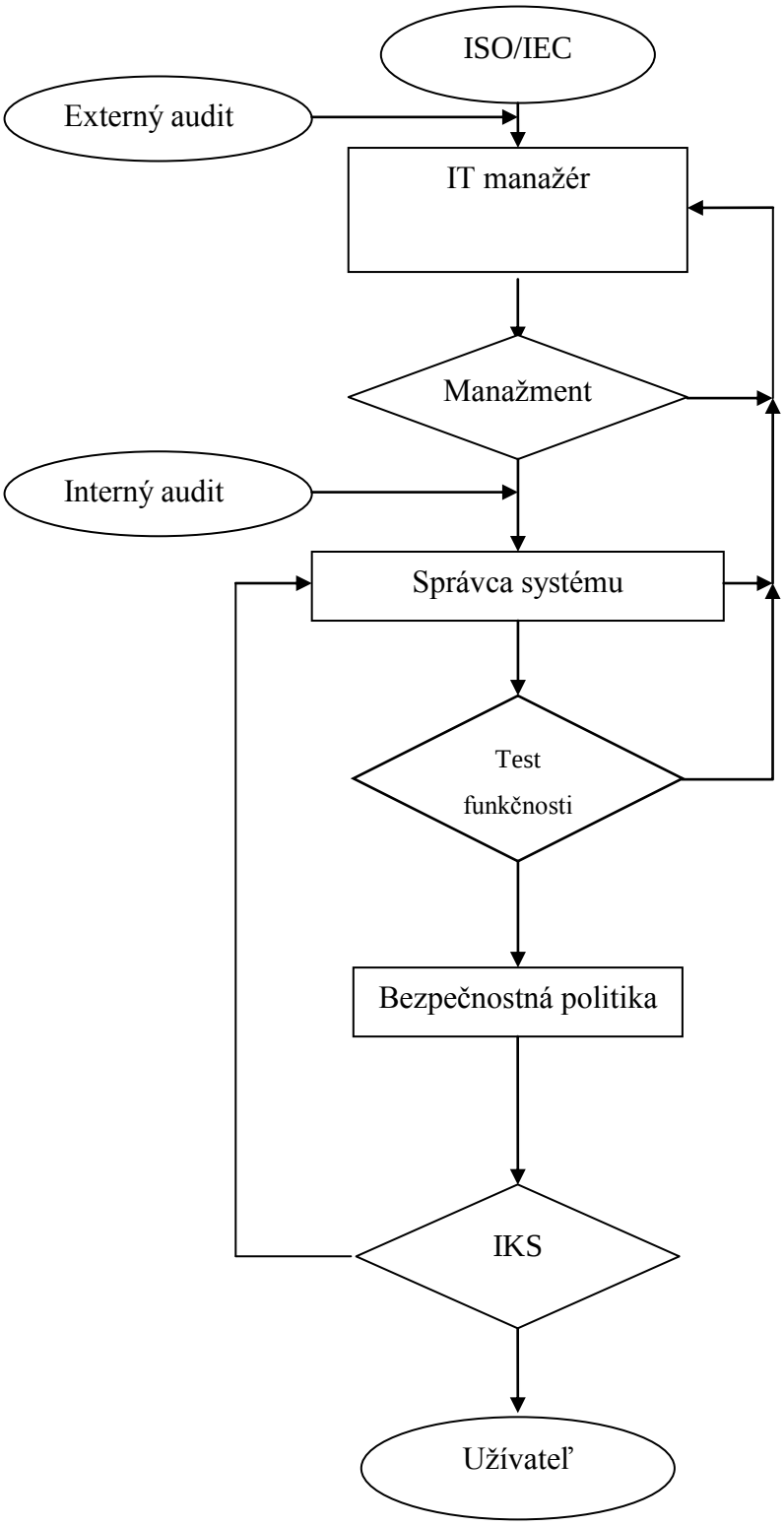
Spôsob výkonu: Tento audit vykonáva certifikovaná spoločnosť alebo certifikačná autorita. Tento audit sa musí vykonávať každé dva roky. Pre zvýšenie bezpečnosti by bolo ideálne, vykonávať tento audit každý rok.

3.3 Proces fungovania IT bezpečnosti

Na začiatku celého procesu je medzinárodne uznávaná norma ISO 27000 a ISO 20000. Podľa tejto normy sa riadi IT manažér a upravuje postupy. Po vytvorení projektu, ho predloží manažmentu z dôvodu uvoľnenia potrebných finančných prostriedkov. Ak manažment neodsúhlasí projekt, tak IT manažérovi predložia výhrady a následne IT manažér prepracuje projekt.

Po odsúhlasení projektu správca siete pod dozorom IT manažéra zakúpia potrebný SW a vybavenie v primeranom množstve, pre otestovanie. Pokiaľ testovanie nesplnilo potrebné očakávania, IT manažér prepracuje projekt a priloží dôvody, prečo pôvodný projekt neuspel pri testoch.

Pri úspešnom otestovaní nových systémov sa zavedie do bezpečnostnej politiky a následne sa implementuje do IKS. Následne tento systém je aplikovaný na užívateľov. Systém zostáva naďalej priebežne monitorovaný správcom siete a špeciálnym SW. Správca siete pravidelne predkladá správy IT manažérovi, ktorý ich vyhodnotí a podľa potreby vytvára nápravné opatrenia, ktoré zopakujú celý proces. Do procesu vstupuje externý alebo interný audit.“ [4]



Obrázok 3: Organizačná štruktúra

4 LAN

Bežná počítačová sieť predstavuje z fyzického hľadiska štruktúrovanú kabeláž, ktorá prepája počítače, prepínače, smerovače, tlačiarne a ďalšie zariadenia, ktoré využívajú ku komunikácii LAN. Je to prostriedok , pomocou ktorého zariadenia môžu komunikovať medzi sebou. Na sieťovú komunikáciu spoliehajú všetky zariadenia moderného komunikačného prostredia. Vďaka rýchlemu rozvoju LAN sietí dnes môžeme posielať dáta vrátane videa a zvuku na veľké vzdialenosti vysokými rýchlosťami.

4.1 Zadelenie siete

Počítačová sieť v spoločnosti je typu LAN. Rozsah siete je v rámci jednej budovy bez prepojenia ďalších LAN sietí z internetu. Logická topológia siete je stromového typu. Stromová topológia je prirodzeným rozšírením topológie typu hviezda. Vlastnosti stromovej topológie sú podobné ako u sietí typu hviezda:

- odolnosť siete voči výpadkom jednotlivých staníc a liniek
- citlivosť na výpadky uzlov
- ľahká rozšíriteľnosť
- dvojbodové spoje

Najdôležitejšou úlohou počítačovej siete v spoločnosti je zdieľanie údajov. Ide o to, že potrebné dátové súbory môže spracovávať viac používateľov súčasne. Je to umožnené tým, že dátové súbory sú uložené na serveroch siete a pripojení používatelia majú k nim prístup.

4.2 Fyzická kabeláž

4.2.1 Analýza kabeláže

V spoločnosti je použitá technológia 100BASE-T, ktorá je štandardizovaná podľa protokolu IEEE 802.3U. Chrbticu celej počítačovej siete tvorí prepojenie hlavných rekov, ktoré sa nachádzajú na rôznych miestach budovy. Tieto zariadenia sú navzájom prepojené pomocou optických káblov založených na 100BASE-FX. Optické káble sú vedené cez servisné priestory v ochrany trubkách z PVC materiálu .

Z rekov následne vedú UTP káble, ktoré ich spájajú s pracovnými stanicami a lokálnymi routrami. UTP káble sú vedené v uzavretých káblových lištách, na ktorých sa nachádzajú koncové zásuvky typu RJ45 cat 5e. Zásuvky sú rozostúpené v káblových lištách s odstupom 2m.

Z definovanej štruktúry je zrejmé, že sa používa hviezdicová typológia. Správy prechádzajúce cez túto typológiu súčasne prechádzajú cez centrálny počítač, ktorý riadi tok všetkých dát. Hviezdicová typológia disponuje tou výhodou, že je u nej jednoduché pridávať nové stanice, k čomu je potrebný len kábel od centrálneho počítača k sieťovému rozhraniu novej stanice.

Samostatnú kategóriu kabeláţnej štruktúry budovy tvoria UTP káble určené pre pripojenie IP kamier CCTV. Tieto káble sú vedené spoločne s UTP káblami pre pracovné stanice a lokálne routre bez akejkoľvek separácie.

4.2.2 Hodnotenie analýzy kabeláže

Kabeláž budovy pozostáva z viacerých typov káblov. Z nich každý plní svoju špecifickú funkciu. Nedostatkami kabeláţnej štruktúry však je jej rozmiestnenie a usporiadanie.

Skutočnosť, že UTP káble pre pripojenie IP kamier CCTV nie sú samostatne oddelené od ostatných typov káblov spôsobuje neprehľadnosť a problematickejšiu opravu pri poruche samotného prenosového média. Najväčšou hrozbou je indukcia napätia medzi jednotlivými UTP káblami, čo nám môže spôsobovať poškodenie packetov (el. impulzov) prechádzajúcimi cez kabeláž a následne vypadnutie obrazu na kontrolnom mieste. To môže spôsobiť vyhlásenie falošného poplachu a absencie digitálneho záznamu v recordery.

Ďalšou z potenciálnych rizík sú neobsadené zásuvky, ktoré môžu poslúžiť ako interné prípojné miesto do LAN pre neoprávneného užívateľa, zariadenie, s ktorým môže potenciálny útočník odchytávať packety, pokiaľ mu bude pridelená IP adresa alebo si nadstaví vhodnú statickú IP adresu.

4.2.3 Bezpečnostné opatrenie pre kabeláž

Vzhľadom na aktuálnu kabeláţnu štruktúru budovy vidíme, že by bolo vhodné uskutočniť zmeny vo vedení UTP káblov pre CCTV. Konkrétnym opatrením, ktoré by

prinieslo zlepšenie v tejto oblasti, je separátne oddeliť tieto káble od ostaných sieťových káblov. Vhodným riešením by bolo umiestniť UTP káble do ochranných tienených trubiek, ktoré zabránia alebo minimalizujú indukciu na vodičoch pri elektromagnetických impulzoch.

Ďalším vhodným opatrením je odpojenie smerovania na nevyužívané konektory. Každý UTP kábel je označený s príslušným kódom aby sa dal dodatočne identifikovať, kde je ukončený. Podľa identifikačného kódu a konektoru na routry, administrator siete vie odpojiť alebo pripojiť zásuvku (konektor).

4.3 Bezdrôtové pripojenie

4.3.1 Analýza bezdrôtového pripojenia

Zariadenia bezdrôtového pripojenia sa v spoločnosti nachádzajú v skladových priestoroch. Pre ich využitie v týchto priestoroch nie je praktické a efektívne, aby boli pripojené do LAN pomocou UTP káblu. Zariadenia sa pripájajú do siete pomocou „WI-FI“ ktoré pracuje na protokoloch IEEE 802.11b, 802.11a a 802.11g. Bezdrôtové spojenie je chránené pomocou protokolu WPA2 Personal (WPA2-PSK) a šifrované štandardom AES (CCMP).

Ďalším miestom, kde sa využíva bezdrôtové pripojenie sú kancelárske a konferenčné priestory. V nich je umožnené návštevám sa pripojiť k internetu alebo ku vlastným sieťam. Toto prístupové miesto (AP) je pripojené k najbližšiemu dostupnému reku.

4.3.2 Zhodnotenie bezdrôtového pripojenia

Wi-fi sieť je v dostatočnej miere zabezpečená proti amatérskym útočníkom, ktorý nie sú schopní narušiť bezdrôtové pripojenie spoločnosti, bez potrebných znalostí a vybavenia, z dôvodu slabého až minimálneho šírenia signálu z priestorov, kde sa využíva bezdrôtové pripojenie.

Počas celej doby vysielania AP, je vysielaný SSID (sieťové meno) prostredníctvom paketov nazývaných beacons (signály, majáky), ktoré sú vysielané každých 100 ms. Na

všetkých skladových a kancelárskych AP je nadstavené rovnaké SSID, ktoré umožňuje voľný pohyb po celej budove bez nutnosti odpojenia zariadenia. Z toho vyplýva, že všetky zariadenia majú rovnaké nadstavené prístupové parametre, čo poskytuje väčšie možnosti získania prístupových dát zo zariadení.

4.3.3 Bezpečnostné opatrenia pre bezdrôtové pripojenie

Pre zníženie pravdepodobnosti pripájania sa ďalších zariadení do siete, je ideálne schovať alebo vypnúť posielanie SSID prístupového zariadenia.

Ďalšou možnosťou ako minimalizovať pripájanie nežiadúcich zariadení je filtrovať zariadenie na základe MAC adries, kde AP pripojí iba zariadenia, ktoré má povolené v prístupovej databáze a všetky ostatné odmietne. Neoddeliteľnou súčasťou je aj pevné zadanie IP adries, nakoľko na tieto AP sa pripájajú definované zariadenia.

Čo sa týka prístupového AP pre návštevy, je vhodné aby aj tento AP bol zaheslovaný, ale s nesmie mať definované MAC adresy a statické IP adresy, aby sa mohli návštevy pripájať bez nutnosti zásahu konfigurácie AP. Hlavnou podmienkou je, aby tento AP bol priamo pripojený na Wlan a nebol pripojený do LAN siete podniku.

4.4 Pripojenie k internetu

4.4.1 Analýza pripojenia k internetu

Pripojenie k internetu zabezpečujú dve pripojenia DSL linkami o rýchlosti 10/10 Mb/s. Toto pripojenie poskytuje celoštátny poskytovateľ pripojení k internetu. V rámci poskytovania pripojenia sa dodávateľ služby zaručil, že odstráni poruchy pripojenia do 2 hodín od nahlásenia. Každé pripojenie je zakončené modemom, ktorý je pripojený k routru.

4.4.2 Zhodnotenie pripojenia k internetu

Pripojenia sú dostatočne veľkej kapacity, aj pri výpadku jedného z nich dokáže spoločnosť komunikovať so svetom. Pri výpadku oboch pripojení, je spoločnosť zmluvne chránená tak, že porucha bude odstránená zo strany poskytovateľa do dvoch hodín.

Nakoľko spoločnosť nepotrebuje byť pripojená 24 hodín denne, výpadok internetu na dobu jedného dna nijako neohrozí jej fungovanie. Ďalším z bodov zmluvy chrániacich spoločnosť je poskytnutie náhradného pripojenia, cez mobilnú sieť, pokiaľ nebude poskytovateľ schopný odstrániť poruchu.

4.4.3 Bezpečnostné opatrenia pre pripojenie k internetu

Na základe analýzy nie je potrebné prijímať bezpečnostné opatrenia, nakoľko je pripojenie dostatočne zmluvne ošetrené. Pokiaľ spoločnosť bude potrebovať neustále pripojenie k internetu, bude vhodné zaviesť pripojenie od ďalšieho poskytovateľa, ktorý má vybudovanú vlastnú celoštátnu sieť.

4.5 IP

4.5.1 Analýza IP

V spoločnosti sa nachádza približne 200 sieťových koncových zariadení ako PC, tlačiarne, mobilné skenovacie stanice a ďalšie sieťové zariadenia. Zariadenie ako PC a tlačiarne majú pridelené statické IP adresy. Ostatné zariadenia majú prideľované dynamicky IP adresy pomocou DHCP servera.

Vnútorná štruktúra IP adries je založená na privátnych adresách typu 192.168.0.0/16 až 192.168.255.254 /24. Tieto IP adresy sú rozdelené na 4 hlavné podsiete:

1. Office
2. Výroba
3. Sklad
4. CCTV

V podsieťach výroba a CCTV sú IP adresy pridelené staticky. V office a sklad sú statické IP pridelené len PC a statickým tlačiarňam. NB, skenery a mobilné tlačiarne sa pripájajú do siete pomocou WI-FI, ktorá prideľuje IP pomocou DHCP.

4.5.2 Zhodnotenie IP

Potenciálne nebezpečenstvo predstavuje prideľovanie IP adries pomocou DHCP servera. Útočník môže svoje zariadenia maskovať ako zariadenia spoločnosti a tým oklamať DHCP server. Problém pre páchateľa vzniká len pri získaní prístupu do počítačovej siete a na dobu keď falšované zariadenie nebude aktívne alebo prihlásené do siete.

4.5.3 Bezpečnostné opatrenia pre IP

Najjednoduchším spôsobom ako minimalizovať riziko pri prideľovaní IP adries je vypnutie DHCP servera a nadstavenie IP adries napevno. Toto riešenie je časovo náročnejšie na konfiguráciu AP a samotných zariadení. Veľkou výhodou, je presná identifikovateľnosť zariadení a predstava ako sa má zariadenie správať v sieti. Pri infiltrovaní sa do siete cez AP, tak sa nedostane k citlivým údajom nakoľko sieťové zariadenia mu neumožnia komunikovať mimo určený server pre správu skladových zásob.

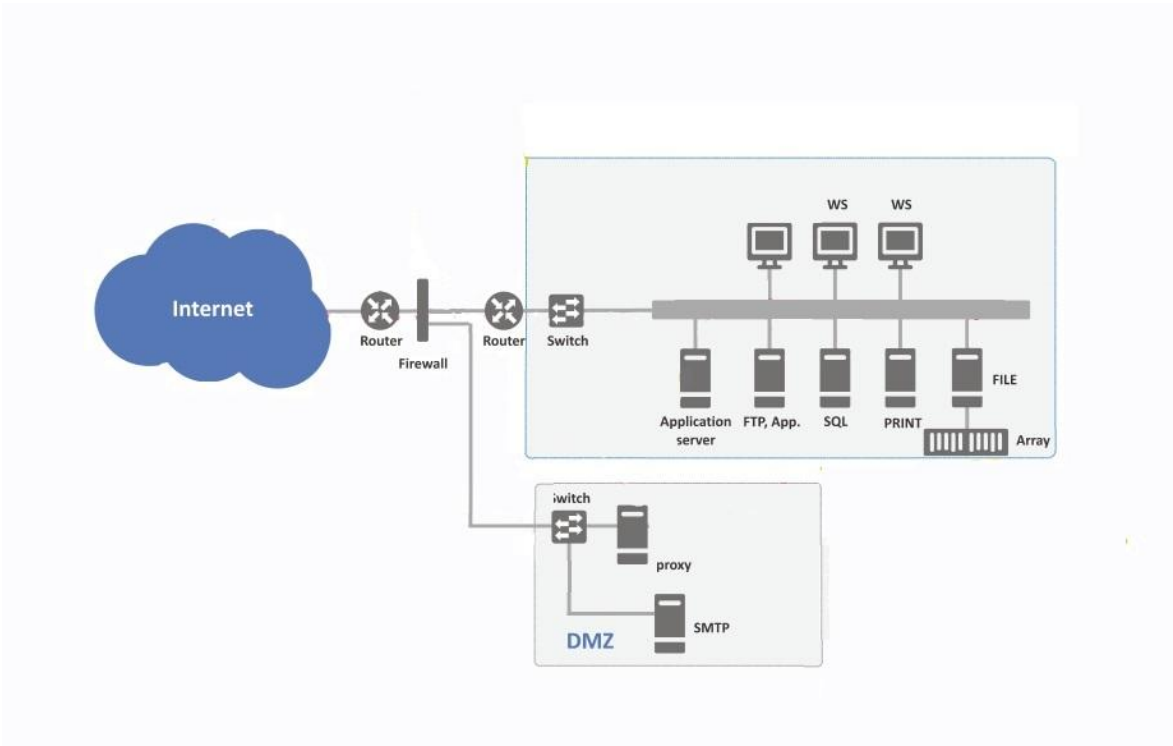
4.6 Firewall

4.6.1 Analýza firewall

Spoločnosť vlastní sieťové routre od spoločnosti Mikrotik, ktoré slúžia ako hlavný firewall oddeľujúci DMZ od internetu a intranetu. V DMZ zóne sa nachádza SMTP server s webovým serverom. Router 1 slúži ako vonkajší firewall, ktorý zabraňuje prienikom do DMZ.

Okrem týchto služieb zabezpečuje aj internetové pripojenie k internetu pre návštevy pomocou AP.

Router 2 oddeľuje DMZ a intranet. Všetky ostatné servery sa nachádzajú za týmto firewallom pripojené v intranete. Zabraňuje posielanie a prístupu k týmto serverom z internetu. Zabezpečuje DNS a vytvára kmeňový router, ktorý spája všetky vlákna siete.



Obrázok 4: Štruktúra siete

4.6.2 Zhodnotenie firewall

Intranet je v dostatočnej miere oddelený od internetu. Všetky vnútorné dôležité dokumenty sú schované za dvomi smerovačmi, kde defaultne je zakázané na routri 2 komunikácia FTP servera s inými IP adresami ako sú definované v intranete. Routre su naprogramované spôsobom „čo nie je povolené je zakázané.“ Potenciálne riziko vzniká krádežou elektronickej pošty, ktorej server je schovaný za 1. Firewallom.

4.6.3 Bezpečnostné opatrenia pre firewall

Vhodné bezpečnostné opatrenie je presunutie proxi servera na server, na ktorom nebeží samotný firewall, a to za účelom zníženia rizika na zmenu konfigurácie filtra. K takto zmenenému, inde umiestnenému serveru nemá potenciálny útočník priamy prístup. Musí prekonať firewall, a prelstiť sledovacie a skenovacie programy, ktoré kontrolujú celú LAN sieť.

4.7 Monitorovanie siete

4.7.1 Analýza monitorovania siete

V spoločnosti sa používajú k monitorovaniu siete nasledovné programy : netstat, logcheck a ippl. Tieto programy bežia neustále na unixovom serveri, ktorý je určený na kontrolu a správu siete.

Netstat je určený k priamemu monitorovaniu portov a spojení odchádzajúcich alebo prichádzajúcich do siete. Definuje, 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, odfiltrováva nepodstatné riadky a upozorňuje na nebezpečné udalosti. Citlivosť balastných filtrov je nadstavená 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 nadstavenými na firewally.

4.7.2 Zhodnotenie 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 presné a prehľadné dáta pre správcu siete, po vyladení a nadstavení filtrov. Problém vzniká pri pravidelnosti kontroly výsledkov zo strany správcu siete. Správca kontroluje výsledky analýz podľa vlastného uváženia. Pokiaľ zanedbá pravidelnú kontrolu, môže prehliadnuť únik dát, monitorovanie komunikácii potenciálnym útočníkom alebo páchateľom.

4.7.3 Bezpečnostné opatrenia pre monitorovania siete

Základný problém je nepravidelná kontrola výsledkov skenovacích a monitorovacích sieťových programov. Prvou a poslednou povinnosťou sieťového správcu v pracovný deň je kontrola chodu a vyhodnotenie výsledkov z týchto programov a následné zaslanie hodnotiacej správy hlavnému správcovi siete. Táto povinnosť musí byť zapracovaná do pracovnej zmluvy sieťového správcu, aby bol upovedomený o svojej povinnosti. Pri zistení narušenia zabezpečenia siete, podnikne príslušné kroky, ktoré sú definované v bezpečnostnej politike.

Ďalším bodom je dvojitá kontrola výsledkov. Túto povinnosť má hlavný správca siete, ktorého povinnosťou je 2x týždenne kontrolovať výsledky z programov a vyhodnocovať správy, ktoré mu zasiela správca siete.

Počas neprítomnosti správcu siete jeho povinnosti preberá hlavný správca a naopak. Nie je prípustné, aby obaja správcovia boli súčasne neprítomní na pracovisku.

Bezpečnostné opatrenie bude riešené interne, v rámci spoločnosti, zakomponovaním povinností do pracovnej zmluvy.

5 ZABEZPEČENIE PRÍSTUPU K SERVEROVNI

Prvým krokom správneho zabezpečenia dát a systému je primerané zabezpečenie perimetru a plášťa budovy. Pravdepodobnosť tohto typu útoku je nízka, ale je reálna. Páchateľ samotnou krádežou zariadenia môže spôsobiť rovnaké škody spoločnosti, ktoré sa dajú prirovnať hackerskému útoku. Môže spôsobiť nenávratnú stratu dát a je tu aj hrozba zneužitia osobných údajov zamestnancov spoločnosti.

5.1 Pozícia budovy spoločnosti a zabezpečenie serverovne

5.1.1 Analýza perimetru budovy

Budova sa nachádza na otvorenom priestranstve v priemyselnej zóne mesta. Okolo budovy sa nachádza otvorené priestranstvo o šírke 20m, ktoré je ohraničené poplastovaným štvorhranným pletivom do výšky 2m (veľkosť oka 50 mm a priemerom drôtu 2,8mm) a zakončené tromi radmi ostnatého drôtu. Tento priestor je monitorovaný kamerovým systémom a v noci nasvietený LED svietidlami. Výstupy (monitory) z kamerového systému sú pomocou LAN siete umiestnené na vrátnici, ktoré kontroluje stála SBS služba.

5.1.2 Analýza plášťu budovy

Budova je postavená z galvanizovanej ocele s dvojitou stenou vyplnenou sklenenou vlnou uchytenú na železobetónových nosníkov. Tento typ stien je štandardizovaný pre priemyselné stavby. Okná, nákladové rampy a dvere sú zabezpečené s elektromagnetickými kontaktmi pre kontrolu uzavretia. Plášť budovy, ale aj perimeter, je každú hodinu kontrolovaný SBS pracovníkom.

5.1.3 Hodnotiaca analýza pre perimeter a plášť budovy

Zabezpečenie perimetru budovy je v súčasnej dobe na dostatočnej úrovni. Ohrozenie narušenia je minimálne, nakoľko firma nie je vlastníkom zariadení, ktoré by mali väčšiu hodnotu na trhu a nelákajú páchateľa k fyzickej krádeži. Ďalším dôležitým

aspektom je, že okolo perimetru budovy nie je žiadny pohyb, nakoľko okolo sa nachádza iba orná pôda.

5.1.4 Bezpečnostné opatrenia pre perimeter a plášť budovy

Aby bolo možné kontrolovať pracovníkov SBS či dodržiavajú pravidelné obchádzky, treba zaviesť obchádzkový systém. Tento systém je určený pre kontrolu dodržiavania obchôdzok zamestnancov SBS. Podľa výpisu zo systému sa dá určiť čas kontroly daného miesta, kto kontroloval a ako rýchlo prešiel kontrolné body. Dôležitým aspektom prechodu kontrolných bodov je rýchlosť kontroly objektu. Čím rýchlejšie zamestnanec SBS prešiel jednotlivé body, tým nepozornejšie a nekvalitnejšie splnil svoje povinnosti.

Navrhovaním systémom je KosGuard od spoločnosti AVARIS. Je cenovo dostupný a nenáročný na svoju činnosť. Potrebné je zakúpiť :

1. elektronický snímač
2. adaptér k PC
3. vyhodnocovací SW
4. identifikačné čipy pre každého SBS
5. kontrolné body umiestnené na potrebných miestach

Základná cena systému bez identifikačných čipov je cca 540€, ceny čipov sa pohybujú cca 4€ za kus vrátané DPH.

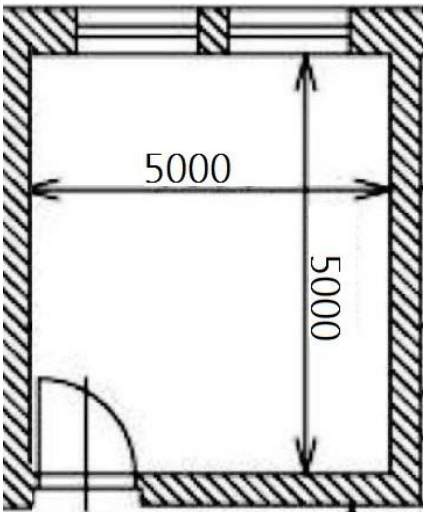
Obrázok 5: Elektronický snímač KOS 1000

Obrázok 6: Identifikačný čip iButton typ DS1990A-F5

5.2 Serverovňa

5.2.1 Analýza miestnosti serverovne

Miestnosť sa nachádza na prízemí budovy s priamym výhľadom na stanovisko SBS. Postavená je z murovaného jadra s rozmermi 5x5m.



Obrázok 7: Pôdorys serverovne

Dvere do serverovne sú protipožiarne a protidymové. Dokážu odolávať šíreniu tepla 45min pri teplote 800°C. K serverovni sú dva kľúče. Jeden kľúč ma administrátor siete a druhý sa nachádza v kľúčovom trezore.

5.2.2 Zhodnotenie serverovne

Serverovňa nieje dostatočne zabezpečená pre prípadne vlámanie sa zamestnanca, ktorý by chcel účelne spôsobiť škodu spoločnosti. V prípade vylomenia dverí nieje možné identifikovať páchateľa a pripadne ohlásenie vlámania.

5.2.3 Bezpečnostné opatrenie pre serverovňu

Nakoľko v serverovni sa nenachádza žiadne bezpečnostné zariadenie a ani prístupové zariadenie, ideálnym riešením pre zabezpečenie oboch druhov zariadení je CCTV kamera. Vhodná pre toto riešenie je IP kamera od spoločnosti TP-Link - TL-SC3171. Táto kamera má nočné prisvietenie do 10m a automatickú detekciu pohybu, jej cena sa pohybuje okolo 100€.

Obrázok 8: TLC-SC3171 s IR prisvietením

5.3 Požiarna ochrana serverovne

5.3.1 Analýza požiarneho systému

V súčasnej dobe sa v serverovni nenachádza žiadny automatický hasiaci systém. Jediný hasiaci systém je vzduchotesne uzavretá miestnosť, ktorá nemá žiadny prívod vzduchu. Pri vzniku požiaru sa sám aj uhasí pri vyhorení kyslíka vo vzduchu. Aj napriek tomuto opatreniu môže prísť k značnému poškodeniu technického zariadenia. Prídavné požiarne opatrenie je nehorľavá podlaha, snehový hasiaci prístroj pred vstupom do serverovne a dymový hlásič.

5.3.2 Hodnotenie analýzy požiarneho systému

Z opisu požiarneho systému v budove je zrejmé, že systém trpí značnými nedostatkami. Nestačí reagovať na všetky alternatívne nebezpečenstvá, ktoré môže požiar priniesť. Technické zariadenie môže v dôsledku týchto nedostatkov utrpieť značné škody. Na ich opravu by spoločnosť musela vynaložiť finančné prostriedky vo vysokej hodnote, čo je pre ňu značne nežiaduce.

5.3.3 Bezpečnostné opatrenie pre požiarny systém

Optimálnym riešením pre bezpečnosť požiarneho systému je zavedenie plynového hasiaceho systému. Tento systém slúži ako prevencia pred vznikom požiaru a aj pri vzniku požiaru s minimálnym poškodením zariadení. Navrhovaným riešením je samočinný skriňový hasiaci prístroj FM-200 Unit A-model od spoločnosti YAMATO, ktorého cena je 500$. Obsahuje Vlastnú riadiacu a detekčnú jednotku a schopnosť hasiaceho priestoru je 100m^3.

Obrázok 9: Hasiaci systém FM-200 UNIT

„ FM-200 je hasiaci plyn s chemickým vzorcom CF3-CHF-CF3. Hasiaci účinok FM-200 spočíva v absorpcii tepla z plameňov. Je teda z veľkej časti podmienený fyzikálne a z

menšej časti chemicky. Hasiaca schopnosť plynu FM-200 bola podrobená testom v národných i medzinárodných ústavoch, na ich základe bola táto látka schválená ako hasiaci prostriedok.“[5]

5.4 Elektrické zabezpečenie serverovne

5.4.1 Analýza elektrického zabezpečenia serverovne

Spoločnosť vlastní 2 záložné zdroje o výkone 8000 W (10000 VA) určené pre servery s oloveno gélovými batériami. Každý zo zdrojov zálohuje vždy len jeden server z dvojice. Záložný zdroj dokáže udržať server v plnohodnotnom chode 10 minút a následne 10 minút poskytuje na uloženie dát a vypnutie serveru. Záložné zdroje zálohujú aj sieťový HW v reckoch mimo serverovnu. Nakoľko tieto zariadenia majú malý výkon približne 20W (jedno zariadenie), tak záložný zdroj poskytuje dostatočne potrebnú dobu pre uloženie dokumentov na sieťové disky.

5.4.2 Zhodnotenie elektrického zabezpečenia serverovne

Súčasný stav je vyhovujúci potrebám spoločnosti. Nakoľko sa záložné zdroje nepoužívajú pre všetky PC, nie je požadovaná dlhá výdrž UPS. Záložné zdroje postačujú pre bezpečné uloženie dát pre užívateľov pracujúcich na notebookoch a vypnutie serverov. Životnosť batérie je určená na 5 rokov.

5.4.3 Bezpečnostné opatrenie pre elektrické zabezpečenie serverovne

Navrhovaným bezpečnostným opatrením je výmena záložných zdrojov každé 3 roky, dôvodom je ešte optimálna cena. Tým sa vykompenzujú finančné náklady na kúpu nového zariadenia. Táto podmienka musí byť zavedená do bezpečnostnej politiky spoločnosti a byť záväzná.

6 DÁTOVÉ A RIADIACE SYSTÉMY

6.1 Technická špecifikácia serverov

6.1.1 Analýza technickej špecifikácie serverov

V spoločnosti sa nachádza 12 serverov, ktoré sa vyznačujú zhodnou hardwarovou špecifikáciou, pričom využité sú servery HP DL380G5 so štvorjadrovými procesormi Intel Xeon X5450 na pracovnej frekvencii 3,0GHz, 16GB pamäte RAM. Servery disponujú duálnym gigabitovým multi-funkčným sieťovým adaptérom s technológiou TOE, ktorá znižuje odozvy v sieti. Servery obsahujú aj viacero výdobytkov, napríklad 8 zásuvek SFF, ku ktorým je možno pripojiť disky SATA za chodu počítača alebo integrovanú správa Lights-Out 2 (iLO 2), ktorá umožňuje zrealizovať tzv. hardwarovo založenú vzdialenú správu, kedy je možné na diaľku zapnúť server a konfigurovať BIOS. Všetky uvedené servery v spoločnosti obsahujú pevné SAS disky o rôznych počtoch a veľkostiach.

6.1.2 Zhodnotenie technickej špecifikácie serverov

Všetkých 12 serverov je rozdelených do dvojíc, ktoré sú prepojené clustrom typu zabezpečenia dostupnosti. Prostredníctvom tejto metódy sa znižuje riziko ohrozenia výpadku servera. Cluster so zabezpečením dostupnosti (Failover ‚High-availabilíty) – zapojenie kedy každé zariadenie môže poskytovať služby a v prípade, že nastane výpadok niektorého zariadenia, je toto nahradené iným zariadením. Akonáhle je pôvodné zariadenie opätovnom zfunkčnené, preberie si služby naspäť.

Servery dosahujú výkonnosť, ktorá niekoľkonásobne prekračuje minimálne požiadavky na funkčnosť OS Windows server 2008 Enterprise nainštalované na serveroch. Pri najvyššej vyťaženosti serverov je procesor zaťažení max. na 85% a RAM zaplnená na 75%. Ak sa pevné disky na serveroch zaplnia, je možné ich dokúpiť a zapojiť do voľných zásuviek.

6.1.3 Bezpečnostné opatrenia pre technickej špecifikácie serverov

Je potrebné zaistiť ochranu nezávislosti jednotlivých serverov. Za týmto účelom je vhodné zapojiť vždy jeden z dvojice serverov na samostatnú fázu elektrickej rozvodne. Tak je možné docieliť, že pri prepätí na jednej fáze a zlyhaní príslušnej ochrany nepríde k poškodeniu oboch serverov.

6.2 Operačný systém

Väčšina serverov disponuje najnovšou verziou serverového operačného systému Windows server 2008 Enterprise od firmy Microsoft, ktorý vychádza z rovnakého kódu ako Windows Vista s jadrom Windows NT 6.0 kernel, s ktorou má podobnú funkcionalitu a architektúru.

Konfigurácia serveru je riešená tak, že systém má prideľované úlohy a služby, ktoré má server vykonávať. Po novej inštalácii serveru nemá server pridelenú žiadnu z možných úloh a tieto úlohy je potrebné aktivovať. Výhodné je aktivovať iba úlohy a služby, ktoré pre server požadujeme z dôvodu maximálneho výkonu. Základné úlohy pre ktoré možno server konfigurovať sú Doménový radič/Active Directory doména, DNS server, DHCP server, aplikačný server, súborový server, tlačový, terminálové služby, webový server, Update server WSUS.

6.2.1 Analýza serveru 1-2

6.2.1.1 Doménový radič

Doménový radič (Domain Controller) tvorí jedna dvojica serverov na ktorých je umiestnená celá časť Active Directory. V prípade popisovaného systému sú vytvorené dva virtuálne stroje zapojené v clustom s vysokou dostupnosťou (failover), kedy v prípade výpadku jedného stroja je druhý stroj schopný prevziať úlohu nefunkčného stroja, vďaka čomu je zaistená väčšia spoľahlivosť celého systému. Spoločne so službou Active Directory sú na doménových radičoch prevádzkované dôležité služby DNS, DHCP a WSUS.

6.2.1.2 DNS

Okrem Active Directory je na doménovom radiči prevádzkovaná tiež úloha DNS (Domain name stystem). Táto úloha je založená na hierarchickom priraďovaní doménových názvov IP adresám priradených doménovým serverom a naopak. DNS je zásadná úloha pre funkciu Active Directory, nakoľko každá doména vytvorená v AD má vlastný doménový názov, napr. firma.sk.

6.2.1.3 DHCP

DHCP je úloha zaisťujúca prideľovanie IP adries, masiek siete, brány, adries serverov DNS a ďalších parametrov jednotlivým klientským počítačom, ktoré sa prihlasujú do siete. V prípade statického prideľovania je ku každej MAC (Media Access Control – jedinečné označenie sieťového prvku) adrese pridelená jedna definovaná IP adresa. V prípade dynamického prideľovania je zadaný rozsah adries, kedy voľné adresy sú náhodne prideľované prihlasujúcim sa klientom. Kvôli jednoduchšej administrácii sa v spoločnosti využíva dynamické prideľovanie IP adries, kedy už jedna pridelená IP adresa je uložená v zozname. Ak stanica požiada o novú IP adresa, je pridelená adresa rovnaká, čím sa dosahujú minimálne zmeny IP adries na jednotlivých staniciach.

6.2.1.4 WSUS (Windows Server Update Services)

WSUS je služba nahrádzajúca aktualizácie prijímané operačnými systémami Microsoft Windows zaistené službou Windows Update. Internetové pripojenie značne zaťažuje prijímanie veľkého množstva automatických aktualizácií z internetu jednotlivými stanicami a administrátori nemajú kontrolu nad jednotlivými aktualizáciami. Z uvedeného dôvodu je vhodnejšou alternatívou využitie služby WSUS, ktorá tieto problémy odstraňuje. Je založená na princípe jedno stiahnutie aktualizácií na server, odkiaľ je rozoslaná na jednotlivé stanice. Administrátor sa môže rozhodnúť, ktoré aktualizácie budú alebo nebudú inštalované na dané stanice a všetko prebieha už výhradne v rámci vnútornej siete. Ďalšou výhodou služby WSUS je možnosť spolupráce s Active Directory, kedy napríklad pri použití skupinových politík možno zamedziť staniciam odmietnuť inštaláciu aktualizácií.

6.2.1.5 Print server (správa tlače)

Print server (správa tlače) poskytuje aktuálne informácie o stave tlačiarní a tlačových serverov v sieti. Tento nástroj možno použiť k simultánnej inštalácii pripojenia tlačiarní k skupine klientských počítačov a vzdialenému sledovaniu tlačových frontov. Rovnako umožňuje pomocou filtrov nájsť tlačiarne v chybovom stave. Print server možno nakonfigurovať aj tak, aby odosielal emailové upozornenia alebo spúšťal skripty v prípade, že tlačiareň alebo tlačový server vyžaduje pozornosť. U tlačiarní poskytujúcich webové rozhranie pre správu môže print server zobraziť ďalšie údaje, napríklad množstvo papieru a toneru. Ďalšou úlohou, ktorú vykonáva print server je záznam tlačených dokumentov. Tento záznam je evidovaný po dobu jedného roka a obsahuje informácie:

- Kto tlačil
- Čo tlačil
- Kedy tlačil
- Kde tlačil

6.2.2 Zhodnotenie serveru 1-2

Doménový radič, DNS a DHCP sú pevne stanovené identifikačné parametre, ktoré sa nemenia a sú zaznamenané v systémových záznamoch. WSUS má zakázané šírenie nových aktualizácií, pokiaľ ich správca siete neschváli a otestuje. Print server dostatočne uchováva dáta o tlačených dokumentoch, podľa ktorých sa dá dohliadať na užívateľov, ktorí tlačili daný dokument.

6.2.3 Bezpečnostné opatrenia pre server 1-2

Predmetné úlohy spĺňajú požiadavky BP.

6.2.4 Analýza serveru 3-4

6.2.4.1 Databázový server

Ide o jeden z najdôležitejších serverov pre firemné informačné systémy. Databázový server je určený pre správu a poskytovanie databáz a databázových služieb. V dôsledku nevyhnutnosti rýchlej práce s obrovským množstvom dát, je potrebné vybaviť tento server najmä dostatočnou veľkosťou pamäte RAM, aspoň 2x8GB. Server obsahuje niekoľko databáz využívajúcich rôzne aplikácie, kde najdôležitejšie aplikácie sú SAP, Axelos a Kodys. Tieto aplikácie majú na serveri nainštalované servere, ku ktorým sa pripájajú ostatné zariadenia. Hlavným databázovým systém je Microsoft SQL server 2005.

6.2.5 Zhodnotenie serveru 3-4

Tieto programy neobsahujú citlivé dáta okrem SAP-u. SAP má dopredu definovanú štruktúru prístupov k jednotlivým častiam systému. K samotným databázam serveru nemá prístup žiadny užívateľ okrem administrátora systémov.

6.2.6 Bezpečnostné opatrenia pre server 3-4

Nie je potrebné aplikovať žiadne bezpečnostné opatrenia, nakoľko postačuje len dodržanie definovaných potrieb užívateľov.

6.2.7 Analýza serveru 5-6

6.2.7.1 Monitorovanie

Linuxový server pre prevádzkovanie open source systému (systém je popísaný v kapitole 4.6.). Tento systém je navrhnutý na automatické sledovanie počítačovej siete a v nej prevádzkovaných služieb. Umožňuje monitorovať služby systému Linux, aj služby systému Windows. Napríklad možno sledovať dostupnosť zariadenia pomocou služby ping, ktorou sa kontroluje sieťová dostupnosť serverov v iných pobočkách alebo dostupnosť internetu

zasielaním pingov, napríklad webový server google. Sledovať je možné aj funkčnosť jednotlivých hardwarových komponentov dôležitých zariadení, ktorými sú predovšetkým servery a aktívne sieťové prvky, ďalej vyťaženie procesorov, ich teploty, otáčky ventilátorov, využitie pamäte RAM alebo zaplnenie pevných diskov. U všetkých sledovaných okolností je možné nastavovať limity a hodnoty, pri ktorých systém automaticky zašle upozornenie prostredníctvom emailovej správy. Je dôležité venovať týmto nastavenia náležitú pozornosť, pretože zlé nastavenia môžu viesť k zaslaniu veľkého množstva správ, v ktorých sa ľahko prehliadnu dôležité informácie.

6.2.7.2 Proxy server

Proxi server je v spoločnosti riešení pomocou služby Squid prevádzkovanej na linuxom systéme. Ide o server, ktorý slúži ako dočasná pamäť k uloženiu navštívených webových stránok. Ak sa vyskytne opakovaná požiadavka na zobrazenie stránky, ktorá je už uložená na serveru, je klientovi poskytnutá stránka priamo z Proxy serveru a nie z webu, vďaka čomu sa zníži objem prenášaných dát z internetu. Nevýhoda tohto systému je, že môže byť týmto spôsobom klientovi poskytnuté neaktuálne stránky. Programátor má možnosť ovplyvniť dobu uchovania dát na Proxy serveri napríklad zápisom meta tágu v načítanej HTML stránke. Proxy server umožňuje tiež blokovať prístupy do internetu, sťahovanie súborov alebo návštevu adries s nevhodným či erotickým obsahom, a to cez funkciu, ktorú zabezpečuje služba SquidGuard. Službu Suiqguard možno prepojiť so službou squid. Okrem toho je možné Proxy server využiť pre skrytie IP adries vnútornej siete alebo pre umožnenie prístupu klientom iba za pomoci užívateľského mena a hesla, čím sa určia klienti, ktoré majú mať prístup a ktorí nie.

6.2.8 Zhodnotenie serveru 5-6

Proxi server a monitorovacie programy poskytujú dostatočné chránenie a monitorovanie komunikácie siete. Na proxi serveri sú nadstavené filtre podľa BP. Monitorovacie programy zabezpečujú monitorovanie celej siete a celej škály komunikačných programov, ktoré komunikujú s domácimi servermi na internete.

6.2.9 Bezpečnostné opatrenia pre server 5-6

Proxi sever je nutné nadstaviť podľa požiadaviek BP, v súlade s ktorými je nutnosť blokovania sociálnych sietí, úložiskových serverov a ďalších nežiaducich stránok. Ďalej je to blokovanie nežiaducej prichádzajúcej komunikácie z internetu, ktorá môže ohroziť systém.

6.2.10 Analýza serveru 7-8

6.2.10.1 Exchange server 2007

Úloha Exchange serveru 2007 spočíva sprostredkovaní príjmu a odosielaní emailových správ, správ kalendára a kontaktov alebo napríklad v zdieľaní verejných zložiek. Mobilní užívatelia a užívatelia pracujúci mimo firmu majú možnosť využiť napríklad prístup k emailu cez webové rozhranie (OWA – Outlook web Access) a prístup prostredníctvom mobilných zariadení. Podobne ako u Windows serveru je po inštalácií nevyhnutné priradiť a doinštalovať serveru úlohy, ktoré má vykonávať. Nie je nutné mať nainštalované všetky komponenty a docieliť tak vyššieho výkonu systému a tiež vyššej bezpečnosti, čo je výhodou tohto systému.

Úlohy vykonávané Exchange serverom 2007 sú:

- Hub Transport Server Role (HUB)
- Client Access Server Role (CAS)
- Outlook Web Access
- Exchange ActiveSync
- Mailbox Server Role (MBX)

6.2.11 Zhodnotenie severu 7-8

Server sa nachádza v DMZ, čím je dostupný aj zo strany internetu. Z tohto dôvodu si vyžaduje zvýšenú pozornosť a prísnejšie bezpečnostné opatrenia. Dôležitý je v tomto prípade monitoring pripojenia, ktorý musí byť nepretržitý. Pripojenie k serveru prebieha

pomocou https protokolu, ktorý poskytuje dostatočnú ochranu pre komunikáciu medzi užívateľom a serverom.

6.2.12 Bezpečnostné opatrenia pre sever 7-8

Navrhovaným riešením je nadstavenie počtu nesprávnych pokusov a následné zablokovanie daného pripojenia. Ďalšou ochranou je dĺžka pripojenia, ktorá by mala byť nadstavená na určitú dobu.

6.2.13 Analýza severu 9-10

6.2.13.1 Dátové úložisko

Dátové úložisko v spoločnosti zabezpečuje systém SAN. Ide o zdieľanie dát na úrovni blokov a nie na úrovni súborov. Úložisko využíva surové dáta a neberie do úvahy filesystém, ktorý je nad dátami vybudovaný. Server virtuálny disk pripojený z úložiska vníma ako nenaformátovaný pevný disk, chová sa a používa sa rovnako ako keby bol pripojený priamo. Server si až nad týmto vybuduje súborový systém. Komunikácia medzi serverom a úložiskom vyzerá ako „prečítaj blok X“ a „zapíš blok X“. V podstate platí, že medzi serverom a pevným diskom, ktorý by bol normálne pripojený priamo, je iba vložená sieť. Hardwar sa skladá z 2 diskových polí od spoločnosti DELL, ktoré sú riadené metódou RAID1. Tieto polia sú plne osadené dvadsiatimi SATA hardiskami o kapacite 500GB od spoločnosti WD. Polovička úložného priestoru slúži ako zálohovací priestor pre dáta. Ďalšia časť úložného priestoru je obsiahnutá v samotných serveroch, ktoré sú osadené SAS diskami. Uvedené zariadenia sú prepojené pomocou iSCSI – SCSI protokol cez IP, pričom nie je nutné zaobstarávať prepojovacie prvky, ale sa využije aktuálna IP sieť a bežné ethernetové switche.

6.2.13.2 Zalohovanie

Proces zálohovania prebieha v niekoľkých fázach, počas ktorých sa zálohujú tri rôzne typy zálohovaných dát, ktoré sú zálohované pomocou rôznych zálohovacích

systémov. Prvý typ zálohovaných dát súvisí s databázou serverov Exchange a SQL server, druhý typ zálohuje dáta systémových diskov serverov a tretí typ zálohovania súborového systému obsahuje všetky dáta Active Directory a dáta úživateľov.

Databázy sa zálohujú 3x denne a o zálohovanie sa stará program SnapManager, inštalovaný na hlavnom serveri. Zálohovanie kompletného súborového systému zabezpečuje program Backupexec, ktorý vytvára plnú zálohu raz týždenne. Posledný typ zálohovaných dát, a to systémové disky serverov, sa zálohujú raz týždenne.

Takéto riešenie zálohovania uľahčuje obnovu stratených dát, kedy obnova dát užívateľov a dát z databáz sú pomerne časté, avšak obnova systémových diskov je pomerne výnimočná. Citlivé dáta sa ukladajú samostatne na externý úložný priestor, ktorý je pripojený pomocou systému NAS. Ukladanie dát sa realizuje v šifrovanej podobe pomocou programu Truecrypt a úložisko tvoria 4 hardisky o kapacite 500GB.

6.2.14 Zhodnotenie severu 9-10

Dátové úložisko je v dostatočnej miere samostatne zabezpečené pred stratou dát. Dôvodom tohto rozhodnutia je ukladanie súborov dvojmo pomocou RAID1. Zálohovanie slúži ako druhotné zabezpečenie pred stratou dát. Zálohovanie citlivých dát je dostatočne chránené. Tieto dáta sú ukladané šifrovanej podobe separátne na hardisk. Problém vzniká v súvislosti s miestom ukladania. Dáta sú ukladané na samotný externý hardisk, kde vzniká hrozba krádeže. Ďalšou slabinou je nízka odolnosť proti požiaru. Nakoľko môže prísť k vznieteniu samotného zariadenia alebo v okolí zariadenia, nemusí protipožiarny systém včas zareagovať.

6.2.15 Bezpečnostné opatrenia pre sever 9-10

Navrhované bezpečnostné riešenie sa týka externého úložného priestoru pre citlivé dáta. Externý úložný priestor by sa mal zameniť za externý priestor odolný voči prírodným živlom ako je voda, oheň, prach. Navrhovaným riešením je ioSafe N2. pri jeho využití je telo úložiska vo vypnutom stave schopné zniesť teplotu cez 800°C a to po dobu pol hodiny. V prípade zaplavenia severovne je úložisko vodotesné ešte dlhšie, do hĺbky troch metrov

vydrží vodotesné po dobu tri dni. Kapacita zariadenia je do 8TB (2x4TB). Cena tohto zariadenia sa pohybuje okolo 600$.

6.2.16 Analýza serveru 11-12

Tieto servery slúžia ako náhradné servery pre prípad výpadku niektorých aktívnych serverov a zároveň slúžia ako skúšobné servery pre správcov siete. Na týchto simulačných serveroch sú skúšané aktualizácie, programy a konfigurácie. Týmto procesom sa predchádza zlyhaniu celého funkčného systému a vzniku bezpečnostných chyb v systému.

6.2.17 Zhodnotenie severu 11-12

Tieto servery sú aktívne využívané. Nie je nutné kupovať samostatný server pre správcov siete, aby mali na čom skúšať a simulovať nové konfigurácie. Podmienkou je, aby náhradné severy boli dostupné pre prípad nahradenia funkčného serveru.

6.2.18 Bezpečnostné opatrenia pre server 11-12

Musia byť vyhradené finančné prostriedky pre nákup nového serveru pre prípad pokazenia jedného z náhradných serverov.

7 UŽÍVATELIA

7.1 Štruktúra užívateľov

7.1.1 Analýza štruktúry užívateľov

V spoločnosti sú vytvorené 4 skupiny užívateľov:

1. Administrátorská (pre správu siete)
2. Hospodársky pracovníci (oddelenie mzdové a finančné)
3. Technický pracovníci (oddelenie inžinieringu, nákupu, kvality, skladového hospodárstva, ...)
4. Užívatelia (zamestnanci na nižšej úrovni riadenia)

Administrátorskú skupinu predstavujú účty správcov siete, ktorí spravujú routre, servery a ostatné zariadenia. Pracujú s právami superužívateľa, aby minimalizovali hrozbu rozladenia, narušenia a poškodenia behu systému. Pod administrátorské účty sa pripájajú len v nevyhnutných situáciách, keď treba urobiť zásahy do systému, ako úprava konfiguračných súborov a databáz.

Hospodárski pracovníci majú už bežné účty s ktorými majú práva zapisovať na svoj pridelený sieťový disk a čítať dáta na sieťovom disku technických pracovníkov. Pre vykonávanie niektorých svojich činností potrebujú prístup k dátam od oddelenia nákupu.

Technickí pracovníci majú rovnako pridelený vlastný sieťový disk, na ktorom sa nachádzajú ich dáta. S týmito účtami nemajú prístup k sieťovému disku hospodárskych pracovníkov a teda nemôžu čítať dáta na.

Užívatelia, do tejto kategórie patria riadiaci pracovníci (zmenoví pracovníci, predáci a kontrolní pracovníci). Pre interné potreby výkazov dát z výroby, majú pracovníci taktiež zriadené svoje sieťové úložné miesto. K týmto dátam majú prístup všetci zamestnanci v spoločnosti s oprávnením na čítanie. Užívatelia majú zriadení priečinok na sieťovom disku technických pracovníkov. Z tohto priečinku majú možnosť čerpať podklady na výkon svojej pracovnej náplne.

7.1.2 Zhodnotenie štruktúry užívateľov

Súčasné rozdelenie užívateľských skupín je v dostatočnej miere zabezpečujúce bezpečnosť citlivých dát, nakoľko majú obmedzené prístupy k jednotlivým sieťovým diskom, na ktorých sú tieto dáta uložené. Z toho vyplýva, že zamestnancom sú prístupné len nutné množstvá dát potrebné k práci. S dátami im prístupnými narábajú bez kontroly. Najväčšie riziko tu vytvára prvá skupina – administrátori siete a druhá skupina – hospodárski pracovníci, pretože majú prístup ku všetkým dátam. Naopak najmenšie riziká predstavujú skupiny užívatelia a technickí pracovníci, z dôvodu, že nemajú prístup k citlivým dátam.

7.1.3 Bezpečnostné opatrenie pre štruktúru užívateľov

Takéto rozvrstvenie rôznych možností prístupu k citlivým dátam medzi jednotlivými zamestnancami je pre fungovanie spoločnosti efektívne. Skupiny užívateľov majú dostatok dát k dispozícii na výkon svojej pracovnej pozície, pričom rozsah prístupu k dátam závisí od druhu pracovnej pozície, a súčasne je spoločnosť v rámci bezpečnosti svojich citlivých dát dostatočne chránená.

7.2 Účty užívateľov

7.2.1 Analýza účtov užívateľov

V spoločnosti sa vyskytujú dva typy účtov : jednotlivé a skupinové.

Jednotlivé účty majú povytvárané všetci technicko-hospodársky pracovníci spolu s riadiacimi pracovníkmi v sklade a vo výrobe. Tieto účty sú zaradené do kategórií podľa štruktúry, ktorá bola spomenutá v predchádzajúcej kapitole. Účty sú priraďované na meno zamestnanca, ktorý je zodpovedný za činnosť v počítačovej sieti pod svojim účtom a je viazaný o mlčanlivosti svojich pridelených heslách do systémov. Tieto heslá si je povinný raz mesačne zmeniť.

Skupinové účty nemá pridelené na zodpovednosť žiaden pracovník. Sú to účty, ktoré využívajú kontrolní a koordinační zamestnanci na získavanie informácií potrebných

k svojej činnosti. Zamestnanci s týmito účtami nemajú žiadne oprávnenie na kopírovania, zápis a úpravu súborov, slúžia výlučne len na čítanie a prezeranie povolených súborov. Prístup do účtu je chránený heslom, ktoré je oznámené zamestnancom, ktorý potrebujú prístup k tomuto účtu. Na účtoch je zablokovaná akákoľvek možnosť inštalácie HW a SW.

7.2.2 Zhodnotenie účtov užívateľov

Jednotlivé účty sú v dostatočnej miere zabezpečené proti zneužitiu neautorizovanými užívateľmi. Je tam povedomie o nutnosti sa starať o ochranu vlastného účtu, za ktorý sú zodpovední ich užívatelia.

Skupinové účty tvoria potenciálne riziko zneužitia, nakoľko je heslo všeobecné známe, ale aj tu je povinnosťou zamestnancov udržiavať heslo v tajnosti a nešíriť ho pomedzi ďalších neautorizovaných zamestnancov. Každý zamestnanec je povinný sa odhlásiť alebo uzamknúť svoj účet pred opustením pracovného miesta.

7.2.3 Bezpečnostné opatrenie pre účty užívateľov

Žiaduce je zaviesť automatické uzamykanie účtov, po určitej dobe neaktivity. Vhodný časový interval je 5 minút Táto doba je postačujúca na potrebné listovanie v papierových dokumentoch s dátami.

Ďalším vhodným opatrením je zaviesť prihlasovacie terminály pre zamestnancov, ktorí pracujú s citlivými údajmi ako osobné a finančné údaje. Ekonomickým riešením sú buď čítačky prstov alebo Smartcard klávesnice. USB Smartcard klávesnice sa však dá obísť vyzradením prístupového pinu a zapožičaním identifikačnej karty. Bezpečnejším riešením je čítačka prstov, ktorá vyžaduje fyzickú prítomnosť zamestnanca na rozdiel od USB Smartcard klávesníc. Zakúpenie čítačok na prsty by bolo vhodné v počte 10ks v hodnote 20 € od spoločnosti Microsoft.

7.3 Emailový účet

7.3.1 Analýza emailového účtu

Každý užívateľ, ktorý vlastní sám účet má zriadený aj emailový účet na firemnom servere. Tento účet slúži na doplnkovú komunikáciu medzi jednotlivými užívateľmi, ktorí sú rozmiestnení po budove spoločnosti. K práci s poštou užívatelia používajú program Microsoft Outlook. Tento program obsahuje potrebné nástroje k pohodlnej správe emailového účtu. Komunikácia medzi emailovým serverom a užívateľom prebieha pomocou šifrovaného spojenia SSL 3.0 / TLS 1.0. Každý účet má dátovo obmedzenú veľkosť schránky. Systém pred zaplnením schránky automatický upozorní užívateľa, aby si ju prečistil alebo uložil dáta na svoj lokálny disk v PC. Emailový klient automaticky overuje každé 2 minúty aktuálnosť emailovej schránky na nové emaily, ktoré sú určené užívateľovi.

7.3.2 Zhodnotenie emailového účtu

Ako už vyplýva z analýzy je zrejmé, že už komunikácia v rámci vnútornej siete je chránená šifrovaním pri prenose správy alebo požiadavky, medzi klientom – serverom a naopak. Táto komunikácia prebieha každé 3 minúty, čo pri súčasnom počte užívateľov postačuje, prebieha bez problémov a má malú odozvu. Riziko zneužitia dát tu vytvára možnosť odosielania emailov na cudzie emailové servery, kde si ich môže preberať páchateľ. Aj napriek tomu, že tieto emaily sú zaznamenávané, je ťažko zistiteľné, kto bol odosielateľom danej správy, pri veľkom počte odoslaných emailov a odosielajúcich.

7.3.3 Bezpečnostné opatrenie pre emailový účet

Riešením je úplné obmedzenie posielania emailov do internetu a nadefinovanie, povolených účtov, na ktoré sa môžu posielať emaily. Tieto vonkajšie externé kontá sú rozdelené na dôveryhodné a cudzie. Dôveryhodným patria pobočky spoločnosti s vlastnými servermi, cudzie sú to emailové servery zákazníkov a dodávateľov. Z tohto dôvodu vyžadujú zvýšenú pozornosť a nutnosť záznamu komunikácie pre spätné dohladanie.

S týmito zákazníkmi a dodávateľmi komunikuje len obmedzený počet osôb v spoločnosti, ktorí sú aj sprostredkovatelia komunikácie medzi ostatnými oddeleniami spoločnosti s nimi. Tu pripadá zodpovednosť a istá kontrola aj na prostredníka, ktorý má možnosť zasiahnuť a obmedziť komunikáciu. Týmto vzniká istá forma autodetekcie ochrany dát.

7.4 Možnosti užívateľských účtov

7.4.1 Analýza možností užívateľských účtov

Každý užívateľ má poskytnutý od spoločnosti PC alebo notebook, na ktorom vykonáva svoju prácu. Toto zariadenie je pripojené do siete pomocou doménového radiča. Tieto účty sú konfigurované a spravované z jedného miesta – zo servera. Každý účet má možnosť pracovať na hardisku prideleného zariadenia. K dispozícii má aj príslušný sieťový disk podľa oddelenia, do ktorého je zaradený. Využívať môže aj DVD mechaniku v zariadení, ktoré je plne funkčné bez obmedzení. Ďalej má k dispozícii aj USB porty, ktoré sú bez akejkoľvek kontroly o pripojení prenosných pamäťových zariadení. Užívatelia majú povolenie inštalovať certifikovaný SW do zariadení, na ktorých pracujú, ktoré si priniesli alebo stiahli z internetu, bez predchádzajúceho povolenia od administrátora siete.

7.4.2 Zhodnotenie možností užívateľských účtov

Nadstavenie účtov je príliš benevolentné a spolieha sa na čestnosť zamestnanca. Ako je uvedené v analýze, zamestnanec si môže rôznymi prenosnými médiami preniesť dáta, ktoré si mohol stiahnuť z firemnej siete, v rámci svojho oddelenia. Používanie zariadení bez akéhokoľvek monitoringu a obmedzenia je neprípustné. Ďalším rizikom je neobmedzený prístup na internet, kde môže využiť virtuálne FTP servery.

Hlavným kritickým bodom je inštalácia certifikovaného SW. Potenciálny útočník môže podhodiť SW, ktorý ma upravený kód, a tým nevedome užívateľ nainštaluje aj nežiaduci SW. Nežiaducu aktivitu nežiaducich programov by mali zachytiť ochranné prvky zariadenia a počítačovej siete.

7.4.3 Bezpečnostné opatrenie možností užívateľských účtov

Využívanie prenosných zariadení sa dá obmedziť pomocou ESET Endpoint Protection Standard. Táto verzia obsahuje pokročilejšie nadstavenie používania prenosných zariadení oproti pôvodnému ESET NOD32 Antivirus 4. Nakoľko niektorí zamestnanci potrebujú používať k svojej činnosti prenosné zariadenia, dá sa v ňom nadstaviť Identifikačné číslo prenosného zariadenia. Na konci pracovnej doby je povinný toto zariadenie odovzdať nadriadenému zamestnancovi.

Problém so sťahovaním SW a ukladaním dát na Internetové FTP servery, rieši úplný zákaz prístupu na Internet. Pokiaľ zamestnanec nebude mať odkiaľ stiahnuť SW a možnosť dostať sa na internetový FTP server, tak nie je nutné zavádzať ďalšie špeciálne opatrenia v rámci užívateľskej stanice a siete. Zamestnanec, ktorý potrebuje k svojej činnosti prístup na internet, bude monitorovaný pomocou proxi serveru a bude mať filtrovaný prístup k stránkam. Bude mať zablokované prístupy na sociálne siete a FTP servery.

8 TESTY SYSTÉMU

Spoločnosť môže byť potencionálnym útočníkom vďaka najrôznorodejším útokom z internetu alebo útočníkom používajúcim rozličné ľahko dostupné programy, tzv. hackovacie techniky. Tieto hrozby často nastávajú z dôvodu nedostatočného zabezpečenia informačných systémov a komunikačnej infraštruktúry proti neoprávneným prístupom nielen pri napadnutí zvonku, ale aj vo vnútri organizácie. Jednou zo základných možností ako dôkladne, včas a bezpečne preveriť zabezpečenie informačnej štruktúry spoločnosti sú penetračné testy (ethical hacking). Ak sú včas odhalené slabiny informačnej štruktúry a prijaté účinné opatrenia na ich odstránenie možno tak predísť značným stratám, ktoré by úspešné napadnutie mohli spôsobiť.

Penetračné testy cielene napádajú počítačové siete a zisťujú ich slabé miesta, čím umožňujú spoločnosti preveriť odolnosť a zabezpečenie jej infraštruktúry proti pokusom o nežiaduce prieniky. Efektívne je ich vykonávať opakovane, pretože sa stále objavujú nové bezpečnostné riziká a zároveň sa tak dá zistiť úspešnosť odstránenia slabín z minulých šetrení. Testy sú schopné odhaliť ako by informačný bezpečnostný systém spoločnosti obstál pri reálnom pokuse o neoprávnený prienik do siete spoločnosti.

Testy využívajú kombináciu nástrojov a testovacích poznatkov prostredníctvom ktorých možno získať množstvo poznatkov o skutočnom stave bezpečnosti. Rozlišujeme penetračné testovanie externé, ktoré nám má odhaliť mieru do akej je schopný útočník z vonka, z internetového prostredia schopný ochromiť chod organizácie a penetračné testovanie interné, ktoré sa naopak zameriava na odhalenie útočníkov z vnútra, zo zamestnancov organizácie majúcich úmysel poškodiť spoločnosť alebo zneužiť niektoré informácie spoločnosti.

Penetračné testovanie má niekoľko zásad svojho procesu. Sú to:

- jednoznačne stanovený cieľ,
- časový limit pre uskutočnenie testovania,
- súhlas vedenia organizácie,
- eliminácia dopadov na funkčnosť IS,
- získanie rozsahu IP adries, ktoré majú byť predmetom penetračného testovania.

Fázy penetračného testovania delíme na:

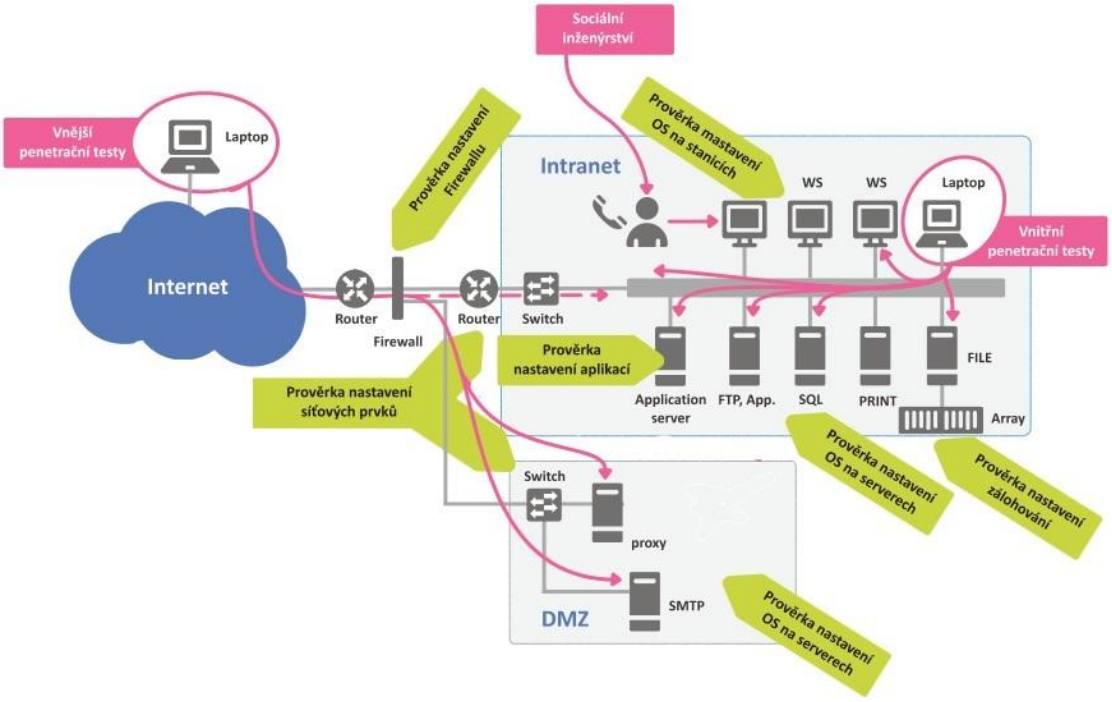
1. Zber informácií – cieľom je zistiť odolnosť IS spoločnosti. Prebieha identifikácia napr.: voľne prístupných účtov (ftp), aktívnych komponentov internetového pripojenia (ping scan), aktívnych služieb dostupných na týchto komponentoch (port scan), užívateľských účtov a ich využívania (finger, smtp,), používaných komunikačných protokoloch, potenciálnych únikov informácií z cieľovej siete, smerovania elektronickej pošty, zistenia podporovaných/používaných autentifikačných metód.

2. Prienik – uskutočnenie testov na známe, ale aj menej známe chyby napr. v OS, aplikáciách, firewalloch,: chyby konfigurácie FW, skúšanie defaultných a obvyklých hesiel, pretečenie vyrovnávacej pamäte – chyba v ošetrení vstupných dát (je možné "prepašovať" do systému škodlivý príkaz), využitie chýb konfigurácie WWW servera (napr. zneužitie CGI skriptov, etc.), obchádzanie autentifikačných mechanizmov, hádanie hesiel a kľúčov.

3. Odporúčania – na základe výsledkov testov je spracovaná a predložená záverečná správa zahrňujúca výsledky testu a spôsoby odstránenia zistených slabín.

Externý penetračný test sa vždy realizuje v presne stanovenom časovom intervale a jeho zistenia odzrkadľujú stav v danom časovom intervale. Jeho rozsah sa dohodne na začiatku testovania a do úvahy sa pri vymedzení rozsahu berie i podrobnejšia analýza aktuálneho stavu a počet verejne dostupných IP adries. Interný penetračný test sa vykonáva podobne ako externý s tou výnimkou, že sa vytvorí prístup do siete organizácie s prístupovými právami bežného používateľa IS.

Výsledkom penetračného testovania je odborné zistenie slabín bezpečnostného systému spoločnosti, konkrétne zneužiteľných dier, nedostatkov práce IT správcov spoločnosti, stav siete spoločnosti všeobecne a následne z vyhodnotených zistení stanovenie postupu na odstránenie bezpečnostných nedostatkov spolu s formuláciou odporúčaní na ich riešenie podľa stupňa závažnosti týchto nedostatkov. Súčasne sa takto výsledkami penetračného testovania môže zabezpečiť i zvýšenie konkurencieschopnosti spoločnosti.



Obrázok 10: Ciele testovania

9 FINANČNÁ SUMARIZÁCIA

Výrobca	Model	Cena za 1ks.	Požadované ks	Cena celkovo v €	Poznámka
AVARIS	KOS 1000	395€	1	395	
AVARIS	ADAPTER K PC	72€	1	72	
AVARIS	WSOK Standard	84€	1	84	
iButton	DS1990A-F5	4€	20	40	
TP-Link -	TL-SC3171	100€	1	100	
YAMATO	FM-200 Unit A-model	500$	1	386	1 USD = 0,77 EUR
Microsoft	FINGERPRINT READER	20$	10	16	1 USD = 0,77 EUR
ioSafe	N2	600$	1	462	1 USD = 0,77 EUR
	SUMARIZÁCIA			1555€	

Tabuľka 1: Cenová sumarizácia[1]

V tabuľke je zaznamenaná sumarizácia zariadení, ktoré treba zakúpiť pre implementáciu bezpečnostnej politiky. Zariadenia boli vyberané podľa technických parametrov tak, aby spĺňali požiadavky v celom rozsahu. Tieto náklady je možné znížiť , výberovým procesom. Predpoklad zníženia nákladov je o 20% ceny tovaru. Ostatné zásahy pri implementácii BP sú vykonávané na systémoch, ktoré vykonávajú správcovia siete. Je to priame nadstavenie konfigurácií riadenia a kontroly systémov.

[1] Prevod $ na € bol uskutočnený konverzným kurzom 1 USD = 0,77 EUR platným 27.5.2013

ZÁVER

V práci som sa zameral na implementáciu bezpečnostnej politiky pre informačno-komunikačný systém. Poukázal som na nedostatky informačno-komunikačného systému spoločnosti v spojitosti s bezpečnostnou politikou spoločnosti. Následné som navrhol bezpečnostné riešenia na odstránenie uvedených nedostatkov systému, ktoré spĺňajú požiadavky bezpečnostnej politiky. Pre riešenia boli použité technické zariadenia, ktoré spĺňajú primeranú úroveň zabezpečenia s ohľadom na vlastníctvo spoločnosti a súčasný bezpečnostný stav. Tieto technické prostriedky spĺňajú environmentálne a hygienické normy. Časový horizont možnej priamej implementácie do systému je približne 1 týždeň pri okamžitej dostupnosti zariadení.

Existencia spomenutých nedostatkov informačno-komunikačného systému spoločnosti dokazuje aká dôležitá je implementácia inštitútu bezpečnostnej politiky do informačno-komunikačného systému spoločnosti pre bezproblémový chod spoločnosti.

V práci nie sú použité fotografie z reálneho prostredia a ani presné špecifikácie systémov z dôvodu dodržiavania bezpečnostnej politiky spoločnosti.

ZÁVER V ANGLICKOM JAZYKU

At work I focused on the implementation of security policy for information and communication system. I pointed to deficiencies of information and communication system of the company in conjunction with the company's security policy. Then I proposed security solutions to remedy the deficiencies of system which are in concern with the requirements of security policy.

At work, for solutions, were used technical devices that satisfy appropriate level of security with regard to the ownership of the company and the current security situation. These technical resources satisfy environmental and health standards. The time horizon of the possible direct implementation of the system is probably 1 week at the immediate availability of equipment.

The existence of the mentioned shortcomings of information and communication system of the company shows how important is the implementation of the institute security policy in information and communication system of company for its smooth running.

In this work are no used the photographs from the real environment and no exact specification of systems because of observe security policy of company.

ZOZNAM POUŽITEJ LITERATÚRY

1. *JAŠEK, Roman: Ochrana znalostí a dat v podnikových informačních systémech. Zlín : Univerzita Tomáše Bati ve Zlíně, 2002. 115 s. ISBN 80-7318-095-2.*
2. *JAŠEK, Roman: Informační a datová bezpečnost. Univerzita Tomáše Bati ve Zlíně. 2006. 140s. ISBN 80-7318-456-7.*
3. *MALANÍK, David: Význam fyzického zabezpečení IT systémů. Security Revue září 2010. ISSN 1336-9717.*
4. *LUDVÍK, Miroslav: Teorie bezpečnosti poč. sítí. Computer Media. 98str. ISBN: 80-86686-35-3.*
5. *THOMAS, Thomas M. : Zabezpečení počítačových sítí bez předchozích znalostí. Vyd. 1. Brno : CP Books, 2005. 338 s. ISBN 80-251-0417-6.*
6. *DOSEDĚL, Tomáš: Počítačová bezpečnost a ochrana dat. Vyd. 1. Brno : Computer Press, 2004. ix, 190 s. ISBN 80-251-0106-1.*
7. Slovenská republika. Zbierka zákonov. In *Zbierka zákonov Slovenskej republiky*. Dostupná z http://www.zbierka.sk
8. *STANEK, William R.: Microsoft Windows Server 2008* , Computer Press, 2008. 704str. ISBN: 97-880-25119-36-5

ZOZNAM CITÁTOV

[1] ING. VACULÍK. Návrh optimálneho riešenia ochrany informačného systému. [online]. [cit. 2013-05-28]. Dostupné z: http://nf110.uniza.sk/dizp/bis23.htm

[2] BÍRO, Peter. Informačná bezpečnosť: Čo to je informačná bezpečnosť. [online]. [cit. 2013-05-28]. Dostupné z: http://www.informatizacia.sk/informacna-bezpecnost/

[3] KOKLES, Mojmír a Anita ROMANOVÁ. *Informatika*. Btatislava: Sprint dva, 2008. ISBN 97-880-89393-01-5.

[4] ČAVOJSKÝ, Andrej. *Bezpečnostná politika podniku pre informačno komunikačné technológie*. Zlín, 2011. Dostupné z:

http://dspace.k.utb.cz/bitstream/handle/10563/16525/%C4%8Davojsk%C3%BD_2011_bp.pdf?sequence=1. Bakalárska práca. Univerzita Tomáše Bati ve Zlíně.

[5] PYROKONTROL SLOVAKIA, s.r.o. *Kiddle KD – 200* [online]. [cit. 2013-05-28]. Dostupné z:

http://www.pyrokontrolslovakia.sk/wp-content/uploads/2010/10/KBE_KDE_200_sk.pdf

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

SW - Software

HW - Hardware

IT - Informačné technológie

STN - Slovenská technická norma

ISO - International Organization for Standardization

IEC - International Electrotechnical Commission

ČSN - Česká technická norma

ISMS - Information security management system

PDCA - plan–do–check–act

IKS - Informačno -- komunikačné technológie

IKT - Informačno – komunikačný systém

BS – British Standards Institution

LG – Life´s Good

LAN – Local area network

IEEE - Institute of Electrical and Electronics Engineers

PVC - Polyvinylchlorid

UTP - Unshielded Twisted Pair

CCTV - Closed-circuit television

WPA - Works Progress Administration

AES - Advanced Encryption Standard

AP - Access point

SSID - Service Set Identifier

MAC - Access Control address (MAC address)

DSL - Digital Subscriber Line

IP - Internet Protocol

PC - Personal computer

NB - Notebook

DHCP - Dynamic Host Configuration Protoco

DMZ - Demilitarized zone

SMTP - Simple Mail Transfer Protocol

DNS - Domain name system

FTP - File Transfer Protocol (FTP, doslova protokol prenosu súborov)

IPPL - International Primate Protection League

ICMP - Internet Control Message Protocol

UDP - User datagram protocol

TCP - Transmission Control Protocol

LED - Light-Emitting Diode

SBS – Súkromná bezpečnostná služba

DPH – Daň pridanej hodnoty

€ - Evro

$ - Dolar

°C – Stupne Celzia

m - meter

CF3-CHF-CF3 - fluorine and hydrogen

W - Watt

VA – Volt Ampér

UPS - Uninterruptible Power Supply (záložný zdroj)

RAM - Random-access memory

SATA - Serial ATA

TOE - TCP offload engine

SFF - Small form factor

GHz - Gigahertz

GB - Gigabajt

BIOS - Basic Input-Output System

SAS - Serial Attached SCSI

OS – Operačný systém

WSUS - Windows Server Update Services

BP – Bezpečnostnej politiky

SQL - Structured Query Language

WD – Western Digital

SCSI - Small Computer System Interface

ISCSI - Internet Small Computer System Interface

NAS - Network-attached storage

TB - Terabyte

USB - Universal Serial Bus

SSL - Secure Sockets Layer

TLS - Transport Layer Security

DVD - Digital Versatile Disc

IS – Informačný systém

WWW - World Wide Web

CGI - Common Gateway Interface

ZOZNAM OBRÁZKOV

ZOZNAM TABULEK