Bezpečnostná politika podniku pre informačno komunikačné technológie

Security policy in the enterprise for information communication technologies

Andrej Čavojský

Bakalářská práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

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

Jméno a příjmení:	**Andrej ČAVOJSKÝ**
Osobní číslo:	**A08188**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Bezpečnostní politika podniku pro informačně komunikační technologie**

Zásady pro vypracování:

1. **Zhodnoťe ukládání informací z hlediska bezpečnosti.**
2. **Určete rozsah přístupu uživatele.**
3. **Uveďte způsob přihlášení se do systému.**
4. **Popište zabezpečení serverů.**
5. **Popište přístup na internet z hlediska možných rizik.**
6. **Definujte tzv. elektronický podpis jako zabezpečovací prvek.**
7. **Popište možnosti ochrany před útoky z vnějšku.**
8. **Zhodnoťte dodržování mezinárodních standardů ISO.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. 81 s. ISBN 978-80-7318-889-4.**
2. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007. 123 s. ISBN 978-80-7318-631-9.**
3. **LAUCKÝ, Vladimír. Řízení technologických procesů v průmyslu komerční bezpečnosti. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006. 101 s. ISBN 80-7318-432-X.**
4. **KAMENÍK, Jiří; BRABEC, František. Komerční bezpečnost: soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur. Vyd. 1. Praha: ASPI, 2007. 338 s. ISBN 978-80-7357-309-6.**
5. **BRABEC, František. Ochrana bezpečnosti podniku. Vyd. 1. Praha: Eurounion, 1996. 203 s. ISBN 80-85858-29-0.**
6. **JAŠEK, Roman. Informační a datová bezpečnost. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta managementu a ekonomiky, 2006. 140 s. ISBN 80-7318-456-7.**

Vedoucí bakalářské práce: **JUDr. Vladimír Laucký**
Ústav bezpečnostního inženýrství

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

Termín odevzdání bakalářské práce: **23. května 2011**

Ve Zlíně dne 25. února 2011

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Úlohou mojej bakalárskej práce je vytvorenie korektnej bezpečnostnej politiky IKS pre spoločnosť Universal Media Corporation /Slovakia/ s.r.o.. V bakalárskej práci sa čitateľ oboznámi s aktívami spoločnosti, definíciami dôležitých pojmov, ktoré sú charakteristické pre IKS. V ďalšej časti práce sa oboznámi s organizačnou štruktúrou spoločnosti. Následne sú popísané riziká spojené s prevádzkou IKS a navrhnuté postupy s opatreniami pre zamedzenie nežiaducej situácie.

Kľúčové slová: bezpečnostná politika, aktíva, osobné údaje, dáta, archivácia.

ABSTRACT

The Assignment of my bachelor´s work is making correct secure politics IKS for Universal Media Corporation /Slovakia/s.r.o. company. Reader will acquaint with assets of company in my bachelor ´s work, definition of important concepts, which are characteristic for IKS. He will acquaint with organizational structure of company in next part. There is a description of risks joined with operation IKS and proposed methods with measures for prevent to undesirable situation.

Keywords: security policy, assets, personal data, data archiving

Chcel by som poďakovať pánovi JUDr. Vladimíru Lauckému za odborné vedenie pri písaní tejto bakalárskej práce a zároveň IT oddeleniu v spoločnosti Universal Media Corporation /Slovakia/ s.r.o., za poskytnutie potrebných informácii, cenných námetov a rád.

Prohlašuji, že

- beru na vědomí, že odevzdáním 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 bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk 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 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 – 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 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 bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem 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 bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně 2.5.2011 …….……

podpis diplomanta

OBSAH

ÚVOD

Položme si otázku: akú cenu má informácia? Odpoveď je veľmi ťažká a zložitá. K odpovedi sa dopracujeme až vtedy, keď potrebná informácia chýba, mešká, je nepresná, stratí sa, alebo sa dostane do neoprávnených rúk. Hodnotu informácie určujú náklady na vytvorenie, náklady na aktualizáciu, náklady na prístup, uloženie, ochranu a pod. V jednotlivých oblastiach hospodárstva sa nároky - tým aj náklady - na ochranu informácií lineárne zvyšujú s aktivitou konkurenčného prostredia na jej získanie. Moderné metódy získavania informácií, vzhľadom na ich ilegálny charakter, zaručujú skoro úplnú beztrestnosť pre páchateľov. Aj v prípade, že sa páchateľ odhalí, renomované firmy sa snažia tento fakt zatajiť, aby si zachovali dobré meno spoločnosti a väčšinou si to riešia "doma". V každom prípade platí pravidlo, že v prosperujúcich spoločnostiach, súbežne s opatreniami na ochranu elektronických informácií sa treba sústrediť aj na ochranu proti neoprávnenému sledovaniu. Každý vedúci pracovník spoločnosti si musí uvedomiť cenu dôvernej a chránenej informácie a musí vykonať príslušné opatrenia na elimináciu možností ilegálneho sledovania a odposluchu.

I. TEORETICKÁ ČASŤ

1 ANALÝZA

1.1 Bezpečnostná politika

Definícia: „Bezpečnostná politika obsahuje súhrn bezpečnostných požiadaviek pre riešenie informačnej bezpečnosti na úrovni fyzickej, personálnej, administratívnej, počítačovej a komunikačnej bezpečnosti. Bezpečnostná politika musí byť ako dokument schválený vedením spoločnosti ako záväzná vnútropodniková smernica. Bezpečnostná politika je chápaná ako základný písomný dokument organizácie, obsahujúci predstavu vedenia o riešení bezpečnosti a základné požiadavky na jednotlivé bezpečnostné oblasti celého IS. Bezpečnostná politika ponúka odpovedať na niekoľko základných otázok:

- *Čo chceme chrániť,*
- *Prečo to chceme chrániť,*
- *Ako to chceme chrániť,*
- *Čo budeme robiť, keď dôjde k zlyhaniu systému.“*[1]

1.2 Popis spoločnosti

Spoločnosť Universal Media Corporation /Slovakia/ s.r.o. sa radí k mladším expandujúcim spoločnostiam na trhu so spotrebnou elektronikou. Hlavné zameranie spoločnosti je výroba LCD a LED TV. 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.

1.3 Bezpečnostný prieskum

Súčasný stav: V súčasnej dobe funguje bezpečnostná politika na úrovni dodržiavania legálnosti softvéru vo forme kontroly osobných počítačov 1x ročne a ochrane osobných údajov zamestnancov.

Spoločnosť má v súčasnej dobe minimálnu úroveň ochrany v oblastiach:

- používanie súkromných prenosných zariadení,
- zasielanie informácii pomocou emailu,
- spoločný pracovný účet pre viacerých užívateľov,
- tlač a kopírovanie dokumentov,
- inštalácia nepovoleného softwaru,
- využívanie internetu.

Ciele: Cieľom spoločnosti je dosiahnutie čo najvyššieho stupňa zabezpečenia, kontroly zamestnancov počas pracovnej doby, zvýšenie povedomia o možných rizikách a hrozbách u zamestnancov.

1.4 Vývoj informačnej kriminality na území SR.

Podľa štatistiky kriminality v Slovenskej republike, ktorú vedie Polícia SR vyplýva:

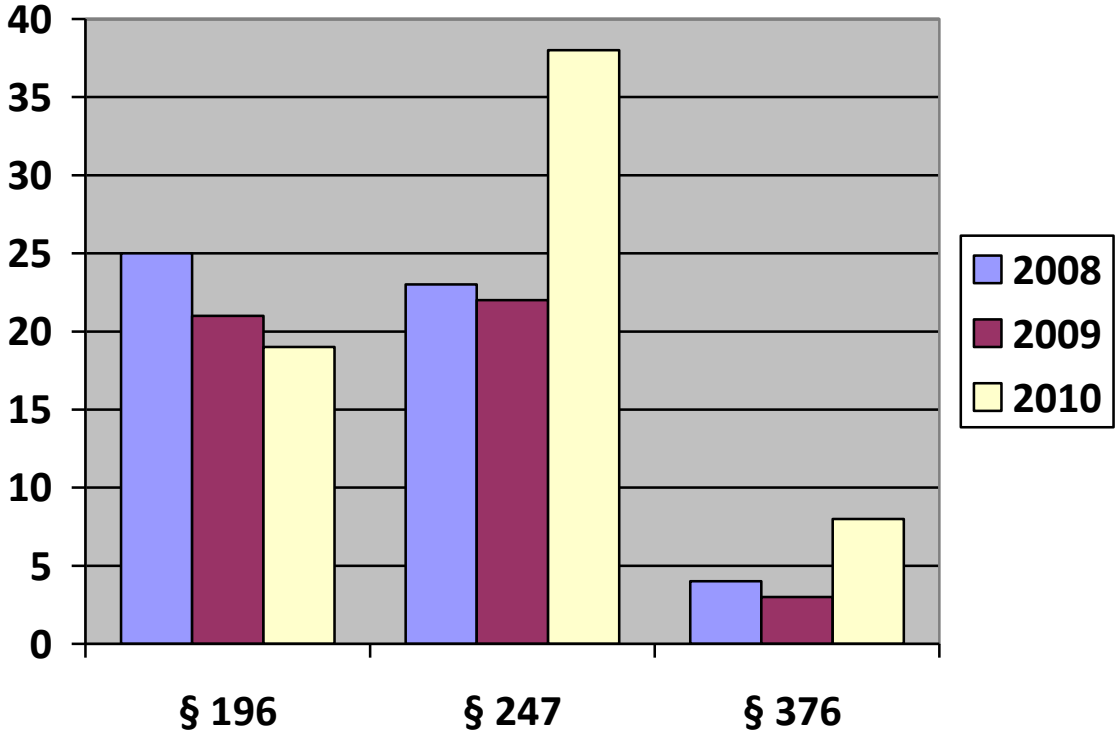
1. Klesajú trestné činy zamerané na odchytávanie dát v sieťach.
2. Vzrástli trestné činy v oblasti krádeži dát, priamo zo spoločnosti.
3. Mierne vzrástli trestné činy oblasti vyzradenia citlivých informácii.

Štatistika bola zostavená z trestného zákonníka SR (zákon 300/2005 z. z.), z paragrafov, ktoré sa týkajú počítačovej kriminality.

§ 196 Porušovanie tajomstva prepravovaných správ

§ 247 Poškodenie a zneužitie záznamu na nosiči informácií

§ 376 Poškodzovanie cudzích práv



Obrázok 1: Vývoj informačnej kriminality na uzemí SR

2 KLASIFIKÁCIA AKTÍV A AKTÍVA

Definícia: „Všetko, čo má pre organizáciu hodnotu. Aktíva organizácie spravidla zahrňujú:

- *fyzické aktíva (napr. počítačový hardware, komunikačné prostriedky, výrobné prostriedky, budovy a pod.),*
- *informácie / dáta,*
- *software,*
- *schopnosť vytvárať určité produkty alebo poskytovať služby,*
- *ľudia,*
- *nehmotné hodnoty (napr. abstraktná hodnota firmy, image, apod.).“*[2]

2.1 Klasifikácia dát

2.1.1 Verejné dáta

Popis: Do tejto kategórie zaraďujeme informácie určené pre verejnosť, ktoré sú voľne šíriteľné a zverejnené. Tieto informácie slúžia na propagáciu spoločnosti, predaj tovarov a služieb. Informácie tejto kategórie chránime len proti pozmeňovaniu obsahu.

Hodnota: Strata a krádež týchto údajov je zanedbateľná. Nemajú žiadny vplyv na chod spoločnosti.

2.1.2 Interné dáta

Popis: Prístup k týmto informáciám majú všetci zamestnanci spoločnosti. Zaraďujeme sem informácie týkajúce sa dodávateľov a zákazníkov, činnosti zamestnancov, ktoré nie sú predmetom obchodného tajomstva a nie sú osobnými údajmi. Tieto informácie sú zakázané poskytovať tretým stranám, z dôvodu zneužitia.

Hodnota: Strata a krádež môže narušiť chod spoločnosti.

2.1.3 Citlivé dáta

Popis: Do tejto skupiny sa radia informácie o účtoch zákazníkov ako aj vlastných, technické výkresy, informácie o zákazníkoch a dodávateľoch, časti obchodných zmlúv a dohôd. Prístup k týmto informáciám má stredný a vyšší manažment, zamestnanci s povolením a externí partneri, ktorí musia byť zmluvne zaviazaní ochranou týchto údajov. Sú to informácie, ktoré by mohli ohroziť dobré meno spoločnosti, postavenie na trhu a spôsobiť ekonomickú ujmu. Prístup k týmto informáciám je chránený prístupovými právami užívateľov, ktoré sú definované na FTP serveri.

Hodnota: Strata alebo krádež môže vážne narušiť chod spoločnosti, ohroziť postavenie na trhu a poškodiť dobré meno spoločnosti.

2.1.4 Mimoriadne citlivé dáta

Popis: Informácie zaradené do tejto kategórie sa týkajú hlavne obchodných zmlúv a dohôd, výrobného procesu, know-how, marketingového štýlu. K mimoriadne citlivým informáciám majú prístup iba najvyšší manažéri, zamestnanci s povolením a externí partneri, ktorí musia byť zmluvne zaviazaní ochranou týchto údajov. Tieto informácie

môžu vážne ohroziť postavenie na trhu, spôsobiť veľkú ekonomickú ujmu, alebo ohroziť meno spoločnosti. Informácie tohto druhu sú najprísnejšie chránené informácie v spoločnosti. Informácie sú ukladané oddelene od ostatných informácii, sú chránené prístupovými právami a sú uchovávané šifrovanej podobe. Prístupy k týmto súborom sú monitorované a zaznamenávané, pre neskoršie potreby odhalenia páchateľa.

Hodnota: Strata alebo krádež vážne môže narušiť činnosť spoločnosti, ohrozenie existencie spoločnosti, straty zákazníkov , zisku, prebranie technológie, zničenie dobrého mena a postavenia na trhu.

2.1.5 Dáta chránené zákonom

Popis: Týmito informáciami sú osobné údaje zamestnancov ako napr.: rodné číslo, číslo účtu, číslo občianskeho preukazu... Tieto údaje je zamestnávateľ povinný chrániť pred zneužitím. Táto povinnosť mu vypláva zo zákona č. 428/2002 Z. z. o ochrane osobných údajov v znení zákona č. 602/2003 Z. z., zákona č. 576/2004 Z. z. a zákona č. 90/2005 Z.z. Slovenskej republiky.[1] S osobnými údajmi môžu pracovať len osoby na to poverené.

Hodnota: Stratou alebo krádežou osobných údajov zamestnancov spoločnosti hrozí žaloba a pokuta zo strany štátu a vzniknutá situácia môže poškodiť dobré meno spoločnosti.

2.2 Aktíva

2.2.1 Ekonomické dáta

Popis: Zaraďujeme sem výdaje a príjmy spoločnosti, ceny za tovar a služby poskytované spoločnosťou, ekonomické plány do budúcnosti, informácie o stavoch účtov.

Riziko: Zneužitie tretími stranami, poskytnutím výhodnejších cien tovarov a služieb tomu istému zákazníkovi, zverejnenie informácii o finančnom stave spoločnosti.

Následok: Oslabenie spoločnosti na trhu, strata zákazníka, strata zisku, poškodenie mena spoločnosti.

---

[1] Pozn.: Pre Českú republiku Zákon č. 101/2000 Sb.z. Českej republiky. Zákony v platnosti dňa 10.2.2011

Zabezpečenie: Dáta sú ukladané samostatne na hardisk a zároveň sú zálohované na záložný hardisk, ktorý sa nachádza v zabezpečenej zóne. Prístup k dátam chrániť prístupovým menom a heslom.

Klasifikácia: Citlivé dáta

2.2.2 Osobné údaje zamestnancov

Popis: „Osobnými údajmi sú údaje týkajúce sa určenej alebo určiteľnej fyzickej osoby, pričom takou osobou je osoba, ktorú možno určiť priamo alebo nepriamo, najmä na základe všeobecne použiteľného identifikátora alebo na základe jednej či viacerých charakteristík alebo znakov, ktoré tvoria jej fyzickú, fyziologickú, psychickú, mentálnu, ekonomickú, kultúrnu alebo sociálnu identitu“[3] – meno, priezvisko, rodné číslo, pracovné zaradenie, plat.

*Riziko: Z*neužitie osobných údajov za účelom obohatenia predajom tretím stranám, prevzatie identity.

Následok: Úrad na ochranu osobných údajov môže uložiť pokutu spoločnosti, dotknutý zamestnanec môže žalovať spoločnosť a žiadať odškodné, poškodenie dobrého mena spoločnosti.

Zabezpečenie: Dáta sú zálohované na záložný hardisk, ktorý sa nachádza v zabezpečenej zóne. Prístup k dátam je chránený prístupovým menom a heslom.

Klasifikácia: Dáta chránené zákonom.

2.2.3 Osobné údaje klientov

Popis: Sú to údaje, ktoré jednoznačne identifikujú klienta, právnickú osobu alebo fyzickú osobu – meno, priezvisko, IČ, číslo účtu, faktúry, telefónne číslo.

*Riziko: Z*neužitie osobných údajov za účelom obohatenia, predajom tretým stranám, páchanie trestnej činnosti.

Následok: Úrad na ochranu osobných údajov môže uložiť pokutu spoločnosti. Dotknutý zamestnanec môže žalovať spoločnosť a žiadať odškodné. Hrozí poškodenie dobrého mena spoločnosti.

Zabezpečenie: Dáta sú zálohované na záložný hardisk, ktorý sa nachádza v zabezpečenej zóne. Prístup k dátam je chránený prístupovým menom a heslom.

Klasifikácia: Citlivé dáta.

2.2.4 Ochranné známky

Popis: „Označenie, ktoré môže tvoriť ochrannú známku, je akékoľvek označenie, ktoré možno graficky znázorniť a ktoré tvoria najmä slová vrátane osobných mien, písmená, číslice, kresby, tvar tovaru alebo jeho obal, prípadne ich vzájomné kombinácie, ak takéto označenie je spôsobilé rozlíšiť tovary alebo služby jednej osoby od tovarov alebo služieb inej osoby.“[4] U spoločnosti UMC-Slovakia s.r.o. sú to značky, pod ktorými predáva svoje výrobky.

Riziko: Tieto údaje sú verejne prístupné.

Následok: Žiadny.

Zabezpečenie: Užívatelia majú zakázané upravovať tieto dokumenty a sú k dispozícii len na čítanie.

Klasifikácia: Dáta chránené zákonom.

2.2.5 Hardware

Popis: Sú to všetky fyzické časti IKS, ktoré sú nutné k funkčnosti informačného systému a bezproblémovému chodu. Zaraďujeme sem osobné počítače s príslušenstvom, tlačiarne, kopírovacie zariadenia, servery, smerovače, sieťová kabeláž, mobilné zariadenia.

Riziko: Nedostupnosť systému pri výpadku elektrickej energie, poškodenie opotrebovaním, krádež časti systému, poškodenie elektromagnetickým výbojom.

Následok: Strata dôležitých dát, narušenie fungovania spoločnosti, hrozba porušenia obchodných zmlúv a zákona, strata zisku.

Zabezpečenie: Rozvádzače a servery sú umiestnené v chladenej a zabezpečenej miestnosti, do ktorej má prístup len poverená osoba. Táto miestnosť je monitorovaná 24 hodín denne a 365 dní v roku, pomocou kamerového systému a elektronického požiarneho systému. Súčasti systému, ktoré sa časom opotrebovávajú sú periodicky kontrolované a zamieňané

za nové. Prístup k tlačiarňam je bez kontroly, ale všetka tlač je zaznamenávaná a kontrolovaná.

Klasifikácia: Citlivé dáta.

2.2.6 Software

Popis: Je to všetok software zakúpený spoločnosťou, ktorý je potrebný pre prácu zamestnancov spoločnosti a k zabezpečeniu IKS.

Riziko: Krádež softwaru, zneužitie tretími stranami

Následok: Hrozba narušenia siete, strata a krádež dát, narušenie funkčnosti IKS.

Zabezpečenie: Inštalácie zakúpeného softwaru môže vykonávať iba osoba na to poverená, odobratie práva na inštaláciu softwaru všetkým ostatným užívateľom a zákaz kopírovania na vlastné média.

Klasifikácia: Citlivé dáta.

2.2.7 Databáza s heslami pre prístup do IKS

Popis: Je to špeciálna databáza, v ktorej sú uchovávané zašifrované prístupové heslá zamestnancov spoločnosti.

Riziko: Vážne narušenie bezpečnosti systému, zneužitie rôznych typov dát, falšovanie dokumentov, prebratie identity spoločnosti treťou stranou.

Následok: Trestnoprávna zodpovednosť, strana finančného zisku, porušenie zmlúv, ochromenie IKS, strata dát nevyčísliteľnej hodnoty.

Zabezpečenie: Celá databáza je uložená samostatne od systému, vykonáva sa pravidelná kontrola zabezpečenia, aktualizácie ochranného softwaru. Databáza je zálohovaná na médium a uložená do trezora. Záloha je pravidelne aktualizovaná. Za všetky tieto úkony zodpovedá osoba na to poverená.

Klasifikácia: Mimoriadne citlivé dáta.

2.2.8 Obsah poštových schránok

Popis: Sú to informácie nachádzajúce sa mimo štandardného úložného priestoru. Slúžia na komunikáciu medzi zamestnancami, predávajú si nimi rôzne podklady a informácie potrebné pre svoju prácu.

Riziko: Zaslanie alebo zachytenie správy s citlivou informáciou tretími stranami, pozmenenie alebo zmazanie informácie.

Následok: Poškodenie dobrého mena spoločnosti, strata zisku, narušenie komunikácie.

Zabezpečenie: Dáta sú hotline zálohované na ďalší hardisk, priebežne sa vykonáva hlavná záloha údajov. Komunikácia prebieha pomocou šifrovania a prístup do systému je chránený menom a heslom. Dáta mimoriadne citlivého charakteru musia byť uložené na určené miesto na serveri a vymazané z pošty.

Klasifikácia: Mimoriadne citlivé dáta.

2.2.9 Dáta uložené na užívateľských kontách

Popis: Sú to dáta potrebné pre prácu zamestnancov. Tieto dáta sú rôzneho charakteru, ako napr.: reklamné informácie, zmluvy, licencie, ekonomické dáta.

Riziko: Hrozba zmazania, pozmenenia informácií, krádež priamo z osobného počítača.

Následok: V prípade citlivých a mimoriadne citlivých dát, hrozí strata zisku, ohrozenie obchodných vzťahov, ochromenie systému a pozmeňovanie údajov.

Zabezpečenie: Prístup je chránený menom a heslom, pred každým prerušením práce sa musí uzamknúť prístupový účet. Po ukončení práce s údajmi, musí ich užívateľ uložiť na určené miesto a vymazať zo svojho hardisku.

Klasifikácia: Mimoriadne citlivé dáta.

2.2.10 Know-how

Popis: Jedná sa o informácie ťažko vyčísliteľnej hodnoty, ktoré opisujú proces výroby, návrhu, konštrukcie výrobkov spoločnosti.

Riziko: Ohrozenie postavenia na trhu, narušenie ekonomických plánov, ohrozenie existencie spoločnosti.

Následok: Strata výhody na trhu, strata zisku, strata obchodných partnerov.

Zabezpečenie: K týmto dátam má prístup len určitý okruh zamestnancov, dáta sú pravidelne zálohované a uchovávané v šifrovanej podobe, chránené s prístupovým heslom.

Klasifikácia: Mimoriadne citlivé dáta.

2.2.11 Zmluvy a obchodné dohovory

Popis: Jedná sa o zmluvy a dohovory uzatvorené s dodávateľom alebo zákazníkom. Tieto zmluvy a dohovory sú utajované podľa dohody oboch strán.

Riziko: Zmarenie zákazky a spolupráce s dodávateľom alebo zákazníkom.

Následok: Strata zisku, poškodenie mena na trhu.

Zabezpečenie: So zmluvami môžu pracovať len zamestnanci na to určení. Dáta sú chránené prístupovým menom a heslom.

Klasifikácia: Mimoriadne citlivé dáta.

3 KATEGÓRIE PÁCHATEĽOV

Definícia: „Osoba, ktorá sa dopúšťa trestného činu, označeného zákonom ako trestný čin, ale i niektoré osoby, ktoré orgány činné v trestnom konaní trestne nestíhajú (napr. kvôli veku, stavu vedomia, duševnej poruche ap.). V Trestnom zákone sa rozlišuje:

- ***organizátor** – kto zosnoval alebo riadil spáchanie trestného činu,*
- ***návodca** – kto naviedol iného na spáchanie trestného činu,*
- ***pomocník** – kto poskytol inému pomoc na spáchanie trestného činu, najmä zadovážením prostriedkov, odstránením prekážok, radou, utvrdzovaním v predsavzatí, sľubom prispieť po trestnom čine.*

Z hľadiska ochrany osôb a majetku sa tiež rozlišuje:

- ***vonkajší páchateľ**, ktorý pôsobí zvonka chráneného objektu,*
- ***vnútorný páchateľ**, napr. vlastný zamestnanec.“*[5]

3.1 Rozdelenie podľa vedomostí

3.1.1 Amatér

Popis: Je to užívateľ, ktorý má základné znalosti o počítačových sieťach a zariadeniach. Nevie využiť získané informácie a programy určené na využitie týchto informácii.

Riziko: Nehrozí žiadne, riziko.

Opatrenie: Pravidelná zmena prístupových hesiel.

3.1.2 Mierne pokročilý útočník

Popis: Útočník má základné vzdelanie pre oblasť IKS, ale nevie efektívne využiť získané informácie a efektívne narábať s programami určenými pre narušenie integrity IKS.

Riziko: Hrozí riziko narušenia IKS a ukradnutiu dát.

Opatrenie: Pravidelná aktualizácia firewallu, pravidelná zmena prístupových hesiel, zaznamenávanie prístupov k citlivým dátam.

3.1.3 Pokročilý útočník

Popis: Má prehľad v oblasti IT. Venuje sa správe podobnej alebo rovnakej štruktúre IKS. Vie si zistiť potrebne informácie a ma odhad v správaní sa systému. Vie používať software pre narušenie bezpečnosti systému.

Riziko: Narušenie zabezpečenia systému, funkčnosti IKS, krádež citlivých údajov zo systému.

Opatrenie: Pravidelná zmena prístupových hesiel, pravidelná aktualizácia firewallu, zaznamenávanie prístupov do systému, používanie šifrovanej komunikácie a bezpečnostné certifikáty, pravidelná kontrola udalosti v IKS.

3.1.4 Profesionálny útočník

Popis: Je vzdelaný v oblasti IT. Pozná podrobne štruktúry IKS a jeho najslabšie miesta. Vie využiť všetky získané informácie a prostriedky pre narušenie systému.

Riziko: Úplné ochromenie funkčnosti IKS, krádež a strata všetkých údajov, poškodenie mena a postavenia spoločnosti na trhu.

Opatrenie: Pravidelná aktualizácia firewallu, zavedenie proxy servera pre kontrolu komunikácie, pravidelná zmena hesiel a dodržiavanie štruktúry hesla. Používanie šifrovanej komunikácie, certifikáty a elektronický podpis.

3.2 Rozdelenie podľa zámeru útočníka

3.2.1 So zámerom narušiť zabezpečenia siete

Popis: Jeho cieľom nie je zničiť a vážne poškodiť spoločnosť. Jeho cieľom je dosiahnutie narušenia systému a následne zistený problém oznámi administrátorovi systému.

Riziko: Vytvorenie nervozity na pracovisku, spomalenie činnosti zamestnancov a spomalenie chodu systému.

Opatrenie: Štandardná ochrana pred útočníkmi.

3.2.2 So zámerom ukradnúť dáta

Popis: Hlavným cieľom je získanie citlivých dát zo systému. Väčšinou sú za útokmi bývalí nespokojní zamestnanci alebo profesionáli, ktorí potom tieto informácie predávajú tretím stranám.

Riziko: Strata dobrého mena, žaloby, ohrozenie existencie spoločnosti.

Opatrenie: Ochrana pred útočníkmi na vysokej úrovni a vykonávanie pravidelných záloh dát a aktualizácii.

3.2.3 So zámerom poškodenia alebo znefunkčnenia systému

Popis: Prioritou útočníka je znefunkčnenie celého systému alebo aspoň jeho čiastočné poškodenie. K týmto činom sú motivovaní hlavne bývalí zamestnanci spoločnosti alebo profesionáli, ktorí to robia za účelom zisku.

Riziko: Ochromenie spoločnosti, strata zisku, sankcie a žaloby za nesplnenie podmienok a dohôd.

Opatrenie: Zavedenie záložných systémov, ktoré sú oddelené od používaného systému, pravidelné zálohy.

3.2.4 So zámerom ovládnutia systému

Popis: Systém potrebuje skryto ovládať, aby mohol vykonávať ďalšiu trestnú činnosť. Pri páchaní ďalšej trestnej činnosti sa tvári, ako ovládnutý server danej spoločnosti.

Riziko: Žaloby od poškodených strán, ťažké dokazovanie neviny.

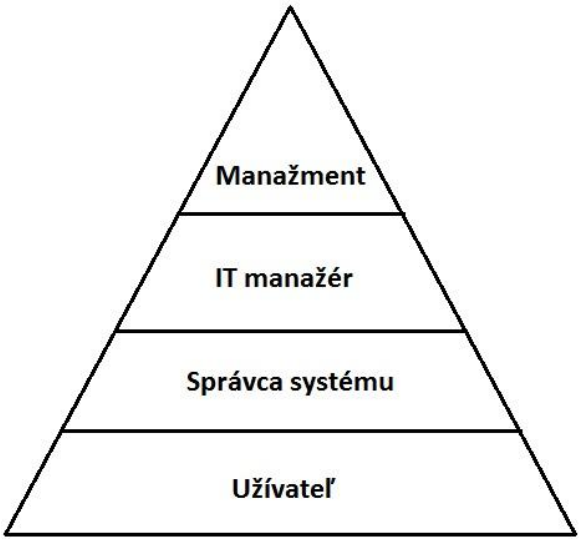
Opatrenie: Kontrola neobvyklých procesov a javov, zabezpečenie na veľmi vysokej úrovni, zaznamenávanie všetkých prístupov z internetu do systému.

II. PRAKTICKÁ ČASŤ

4 ORGANIZAČNÁ ŠTRUKTÚRA IT BEZPEČNOSTI

4.1 Rozdelenie povinností

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



Obrázok 2: Štruktúra právomocí pre IKS

4.1.1 Manažment

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

4.1.2 IT manažér

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

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

4.1.3 Správca systému

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

Spôsob: 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.

4.1.4 Užívateľ

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

Spôsob: 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.

4.2 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."[6]

4.2.1 Interný audit

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

Spôsob: 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.

4.2.2 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: 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.

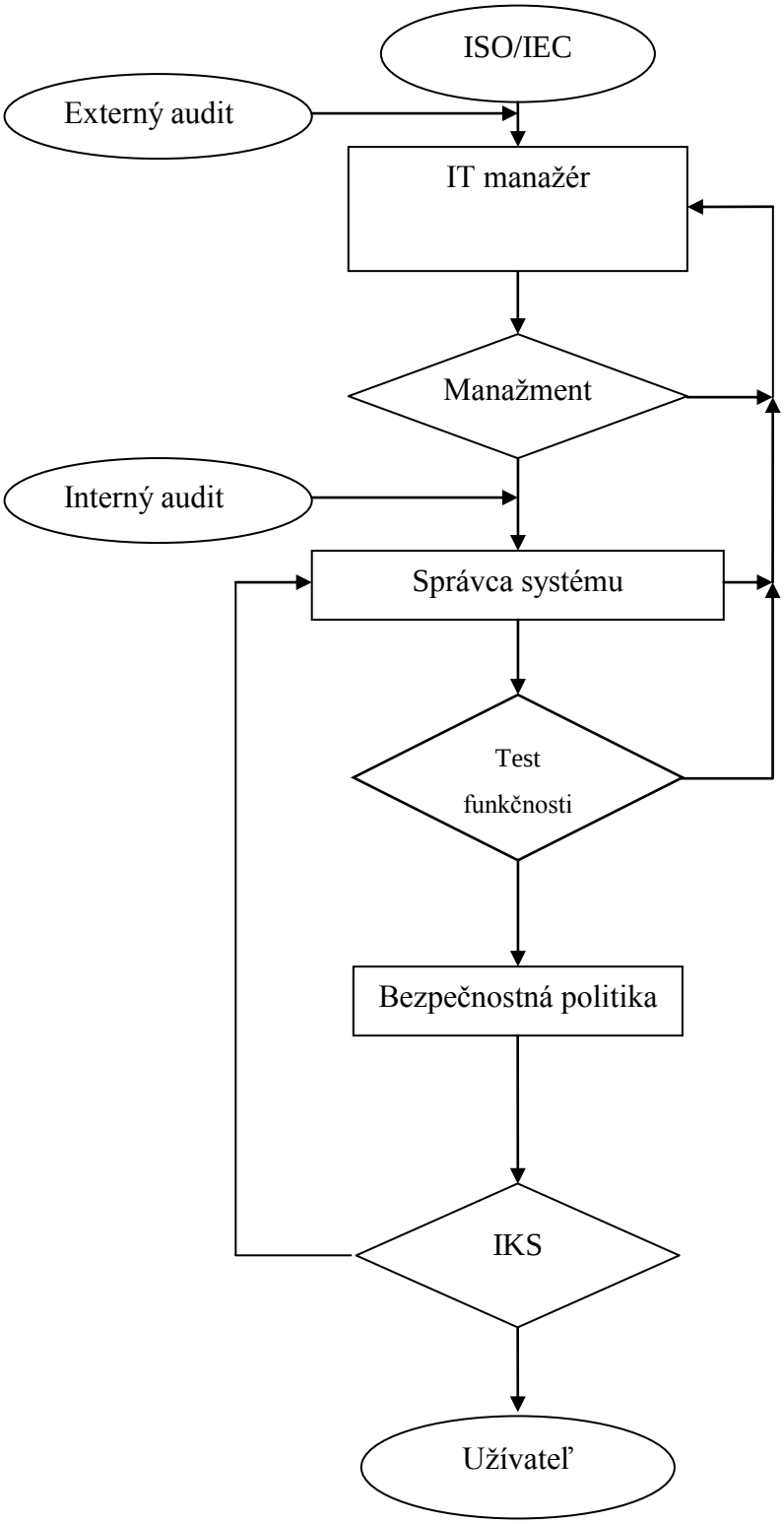
4.3 Proces fungovania IT bezpečnosti

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. Ich úloha je vysvetlená v podkapitole 4.2.



Obrázok 3: Organizačná štruktúra

5 KOMUNIKÁCIA A KONFIGURÁCIA SYSTÉMU

5.1 Sieť

5.1.1 Konfigurácia siete

Riziko: Útočník sa môže pokúsiť o prebranie identity počítača pripojeného do siete a následne sa pokúšať odpočúvať sieťovú komunikáciu.

Následok: Narušenie integrity systému, hrozba krádeže citlivých údajov.

Opatrenie: Každý PC sa identifikuje vlastnou MAC adresou a ku každej MAC adrese je pridelená privátna IP adresa. Na sieťovom routri je zadefinovaná prístupová tabuľka, podľa ktorej sa kontroluje zhoda pridelených IP adries k MAC adresám.

Prínosy: Jednoduchá kontrolovateľnosť zariadení.

5.1.2 Izolácia siete od internetu

Riziko: Napadnutie sieťových prvkov a serverov, čím si môže umožniť prístup do siete.

Následok: Ochromenie systému, činnosti zamestnancov, ktorí pre svoju činnosť potrebujú pripojenie k internetu a strata informácií.

Opatrenie: Výstup a vstup zo siete bude chránený Proxy serverom, firewalom a všetka komunikácia bude zaznamenávaná.

Prínos: Jednoduchá kontrolovateľnosť prístupov do siete a sledovanie komunikácie a vystopovanie potenciálneho útočníka.

5.1.3 Názov sietí, serverov a pracovných staníc

Riziko: Jednoduchšie identifikovanie cieľov pre útočníka a problém včasnej obrany.

Následok: Ochromenie celého systému a strata informácii.

Opatrenie: Použiť nesystematické pomenovanie alebo číslovanie. Súbor, v ktorom budú zaznamenané pridelené názvy ku konkrétnym počítačom, bude považovaný ako mimoriadne citlivý dokument.

Prínos: Skomplikovanie ovládnutia systému útočníkom.

5.2 Kontrola systému a administrácia

5.2.1 Nový správca systému a IT manažér

Riziko: Zmazanie citlivých dát, poškodenie a narušenie činnosti systému.

Následok: Strata dôležitých dát a spomalenie pracovného procesu.

Opatrenie: Každý nový administrátor musí spĺňať požiadavky na danú pozíciu a jeho vedomosti budú overené testom. Po prijatí do zamestnania, musí prejsť minimálne mesačným zaškolením, aby sa oboznámil so systémom. Zaškolenie skončí, keď zvládne interný test z kontroly systému. Po kladnom vyhodnotení testu, preberá plnú zodpovednosť za svoju prácu.

Prínos: Zminimalizovanie rizika narušenia činnosti spoločnosti.

5.2.2 Pomocné administrátorské programy

Riziko: Pri narušení bezpečnosti systému, útočníkovi sa poskytuje jednoduchšie a rýchlejšie ovládnutie systému.

Následok: Narušenie činnosti IKS a možná strata dát.

Opatrenie: Potrebné je zvýšiť zabezpečenie systému, alebo špeciálna ochrana pre tieto programy. Obmedziť prístupové práva len pre administrátora a vstup do týchto programov umožniť len po zadaní autorizačného mena a hesla.

Prínos: Administrátor má uľahčenú prácu v systéme, efektívnejšie a rýchlejšie ovláda a kontroluje systém.

5.2.3 Anomálie v systéme

Riziko: Je to prejav napadnutia alebo poškodenia systému, spomalenie systému, systém sa nepredvídateľne správa.

Následok: Možná strata dát a poškodenie systému.

Opatrenie: Podrobné monitorovanie systému. Zaznamenávanie aj banálnych anomálii a ich následná analýza s návrhom nápravných opatrení.

Prínos: Ochrana pred podobnými situáciami v budúcnosti.

5.2.4 Plánovanie operácii v systéme

Riziko: Pri nesprávnom naplánovaní operácii v systéme, môže to viesť k zahlteniu alebo vytuhnutiu serverov.

Následok: Spomalenie alebo zastavenie činnosti užívateľov systému.

Opatrenie: Počas štandardnej pracovnej doby nevykonávať operácie, ktoré by vo veľkej miere obmedzili užívateľov alebo spomalili ich činnosť. Po skončení štandardnej pracovnej doby sa na systéme začnú vykonávať zálohovacie, skenovacie, aktualizačné procesy a údržbové zásahy do systému.

Prínos: Efektívne využitie výkonu serverov.

5.2.5 Neplánované zmeny v systéme

Riziko: Záplata systému, ktorá nebola otestovaná, nemusí byť kompatibilná s použitým SW.

Následok: Môže to narušiť bezpečnosť systému, strata dôležitých dát a obmedzenie práce zamestnancov.

Opatrenie: Snažiť sa minimalizovať zásahy do systému počas hlavnej pracovnej doby. Vyskúšať záplatu na virtuálnom serveri, ktorý by mal odhaliť možné riziko. Pred zásahom do systému, musí správca siete upozorniť užívateľov systému, aby mohli bezpečne ukončiť svoju prácu. Pred zavedením záplaty sa musí spraviť záloha systému a dát.

Prínos: Odhalenie problému s monitorovaním systému.

5.2.6 Výpadok elektrického napätia

Riziko: Poškodenie systému, strata neuložených dát.

Následok: Strata finančných prostriedkov pri poškodení systému, pozastavenie výrobného procesu, zastavenie komunikácie všetkej administratívnej činnosti.

Opatrenie: Zavedenie záložného zdroja (UPS), aby pri výpadku elektrickej energie bolo možné bezpečne uložiť dáta a korektne ukončiť procesy v systéme. Pri spustení chodu UPS bude rozoslaná informačná správa, aby užívatelia ukončili svoju prácu v systéme. UPS musí byť pravidelne kontrolované a uložené na bezpečnom mieste, aby ho nemohol útočník odpojiť.

Prínos: Ochrana proti poškodeniu systému aj proti výkyvom elektrického napätia v sieti.

5.2.7 Synchronizácia času v systéme

Riziko: Nesynchrónne nastavenie času na zariadeniach, môže vyvolať rôzne anomálie a poruchy v systéme.

Následok: Spomalenie systému, problémy pri rozdielovom zálohovaní dát.

Opatrenie: Čas je synchronizovaný pomocou časového servera, ktorý sa aktualizuje podľa svetového času 1x denne. Následne podľa tohto servera sú 2x denne synchronizované ostatné zariadenia .

Prínos: Rovnakým nadstavením času sa predchádza rôznym anomáliám, poruchám systému a odstraňujú sa problémy pri komunikácii.

5.2.8 Šifrovacie kľúče

Riziko: Pri nedbalom zaobchádzaní s médiami, kde sú uložené šifrovacie kľúče, môže dôjsť pri odchytávaní komunikácie k získaniu citlivých dát tretími osobami.

Následok: Získanie citlivých informácii treťou stranou.

Opatrenie: Šifrovacie kľúče, musia byt uložené samostatne od všetkých dát. Tieto dáta budú uložené v zašifrovanej podobe a prístup k nim bude mat iba hlavný správca siete. Pri nástupe alebo zmene nového hlavného správcu budú kľúče zmenené. Pri ich odcudzení je nutné zmeniť všetky šifrovacie a dešifrovacie kľúče.

Prínos: Zvýšenie bezpečnosti komunikácie a dát.

5.3 Archivácia dát a obnova systému

5.3.1 Obnovenie systému

Riziko: Systém sa po reštarte nemusí navrátiť do štandardnej podoby a chodu.

Následok: Zastavenie výrobného a administratívneho procesu spoločnosti, strata nezálohovaných dát.

Opatrenie: Systém je pravidelne reštartovaný pre zlepšenie jeho výkonu a implementácie softvérových záplat. Reštart systému musí byť mimo hlavnej pracovnej doby, pod

dohľadom administrátora. Reštart v inej dobe nie je povolený. Ak nastane problém, prechádza sa na záložný systém.

Prínos: Systém bude rýchlejšie pracovať, zrušia sa zle ukončené procesy. Spoločnosť bude pripravená, keď vypadne hlavný systém a ju to nezasiahne v plnom rozsahu.

5.3.2 Archivovanie dát

Riziko: Umožnenie prístupu k dátam pomocou nesprávneho uloženia dát s nesprávnymi právami.

Následok: Strata citlivých dát, ohrozenie spoločnosti.

Opatrenie: Úložné disky sú uchovávané v bezpečných a ohňovzdorných skriniach, ktoré sú uložené v zabezpečenej a monitorovanej miestnosti. Na tieto disky je povolené ukladať archívne dáta a zálohy systému. Tieto disky musia mať dostatočnú kapacitu, aby sa na ne dalo ukladať 2 roky, bez nutnosti vymazania dát. Po určení manažmentom, ktoré dáta sú pre firmu nepotrebné, budú následne po uplynutí doby archivácie vymazané administrátorom. Tieto disky musia byť pred skončením životnosti zamenené za nové a dáta prekopírované. Staré disky musia byť sformátované alebo fyzicky zničené.

Prínos: Možnosť dohľadania starších súborov, alebo rýchla obnova systému.

5.3.3 Zálohovanie dát z prenosných zariadení

Riziko: Pri poškodení alebo odcudzení zariadenia je strata dát trvalá.

Následok: Strata dôležitých dát, strata finančných prostriedkov

Opatrenie: Dáta budú automaticky zálohované, keď sa zariadenie pripojí k sieti a užívateľ je sám povinný si dáta zálohovať na média v šifrovanej podobe. Toto zariadenie nesmie využívať na inakšie účely ako pracovné, nesmie si tam samovoľne inštalovať neschválený SW a zapožičiavať zariadenie.

Prínos: Zachovanie časti dát, ktoré boli zálohované na záložné zariadenia pri poškodení alebo odcudzení zariadenia.

5.3.4 Kontrola archivovaných dát

Riziko: Zle uložené dáta na záložných diskoch.

Následok: Nepoužiteľné dáta pre obnovenie systému a nenávratná strata archivovaných dát.

Opatrenie: Pravidelne budú testované archívy na diskoch. Tento test sa bude vykonávať náhodne 1x denne na náhodne vybraných archívoch. Raz mesačne budú otestované všetky archivované dáta a zálohy.

Prínos: Istota, že archivované dáta nebudú poškodené.

5.3.5 Zabezpečenie archivovaných dát

Riziko: Útočník sa môže dostať k uloženým archivovaným dátam.

Následok: Strata citlivých dát.

Opatrenie: Prístup k archivovaným dátam má iba administrátor systému. Pre všetkých iných užívateľov je prístup zablokovaný. Dáta sú uchovávané v šifrovanej podobe. Prístup k dešifrovaciemu kľúču má iba správca siete.

Prínos: Zvýšenie zabezpečenia archivovaných dát.

5.4 Email

5.4.1 Prihlasovanie a komunikácia s emailovým serverom

Riziko: Odchytávanie komunikácie pri nezabezpečenom spojení. Útočník môže získať prihlasovacie údaje k emailovému účtu a následné získanie citlivých dát.

Následok: Strata citlivých údajov, získanie informácii o zámeroch spoločnosti.

Opatrenie: Komunikácia medzi užívateľom a serverom musí prebiehať pomocou šifrovanej komunikácie. Emailový server musí mať certifikát pre overenie autenticity servera.

Prínos: Zvýšenie bezpečnosti pri komunikácii.

5.4.2 Prijímanie emailov

Riziko: Hrozba označenia dôležitých emailov ako spam, alebo vymazanie antivírusom.

Následok: Strata citlivých dát a ohrozenie komunikácie so zákazníkom.

Opatrenie: Pri prijatí emailu systémom, je adresa odosielateľa preverená, či sa nenachádza v zozname spam adries. Ak sa nachádza, tak bude automaticky vymazaný.

Ak sa nenachádza, tak sa preveruje email antivírusom a antispamom. Pokiaľ je označený ako infikovaný, antivírus sa ho pokúsi vyliečiť. Pokiaľ sa mu to nepodarí bude ohlásený správcovi siete a ten určí, či bude vymazaný alebo nie.

Následne je uložený do priečinka adresáta a tam čaká pokiaľ si ho adresát nevyzdvihne po dobu 90 dní. Po vyzdvihnutí adresát skontroluje, či to nie je nevyžiadaná pošta. Ak áno, následne email zaradí do spamu.

Prínos: Spam sa nedostane k užívateľom a systém sa postupne učí rozpoznávať nevyžiadanú poštu.

5.4.3 Zasielanie emailov

Riziko: Užívateľ s cieľom poškodiť spoločnosť, môže zaslať email s citlivými údajmi tretej strane.

Následok: Strata zisku, ohrozenie dobrého mena spoločnosti, zneužitie citlivých údajov.

Opatrenie: Neobmedzené posielanie emailov s ľubovoľným obsahom, okrem osobných údajov, bude povolené iba v rámci spoločnosti.

Zasielanie emailov mimo spoločnosť, bude sprístupnené iba užívateľom, ktorým to povolí manažment a to iba na určité emailové kontá. Tieto emailové kontá budú zapísané v zozname povolených emailov. Ak nejaký email bude chýbať, požiada užívateľ správcu siete, aby ho pridal do zoznamu povolených emailov. Všetky emaily budú zaznamenávané, z dôvodu spätnej kontroly zamestnancov.

Prínos: Zabezpečené zasielanie dát .

5.4.4 Elektronický podpis

*Definícia: „Elektronický podpis tiež zaručuje **nepopierateľnosť** dokumentu – znemožňuje podpisujúcemu tvrdiť, že podpis nie je jeho a že nie je ten, kto dokument podpísal a odoslal.*

Zákon o elektronickom podpise definuje elektronický podpis ako „informáciu pripojenú alebo inak logicky spojenú s elektronickým dokumentom“, ktorá musí spĺňať zákonné požiadavky. Elektronický podpis obsahuje údaj, ktorý identifikuje podpisovateľa.“[8]

Princíp: „Na vyhotovenie elektronického podpisu je nevyhnutný tzv. ***súkromný kľúč*** *(tajná informácia, ktorá slúži na jeho vyhotovenie; bez tejto informácie elektronický podpis nemožno vyhotoviť). K súkromnému kľúču patrí* ***verejný kľúč****, t.j. tajná informácia, ktorá slúži prijímateľovi dokumentu na jeho overenie a bez ktorej by nebolo možné správu prečítať. Znamená to, že obsah podpísaného dokumentu je zašifrovaný a správa je čitateľná iba po dešifrovaní danej správy tajným kľúčom, ktorý má k dispozícii iba ten, komu správa bola určená. Ak by sa podpísaný dokument dostal do rúk nepovolanej osoby, uvidí iba nezmyselnú kombináciu núl a jednotiek.“*[7]

5.4.4.1 Používanie digitálneho podpisu

Riziko: Ukradnutie digitálneho podpisu.

Následok: Útočník môže zasielať falošné emaily v mene spoločnosti, strata finančných prostriedkov.

Opatrenie: Podpis sa používa iba pri zasielaní dôležitých emailov mimo firemnú sieť. Manažment určuje, kto bude mať oprávnenie využívať digitálny podpis. Každý kto dostal poverenie od manažmentu používať elektronický podpis, preberie na osobnú zodpovednosť certifikovaný USB kľúč, na ktorom je podpis uložený. Pri zistený odcudzenia podpisu, je zamestnanec, ktorý ho používal, povinný nahlásiť túto skutočnosť IT manažérovi, aby mohol zablokovať ukradnutý podpis a zakúpiť nový elektronický podpis.

Prínos: Väčšia istota správnosti a pravosti emailu.

5.5 Internet

5.5.1 Používanie Internetu pri práci

Riziko: Zadanie citlivých údajov spoločnosti do podvrhnutých aplikácii a stránok.

Následok: Útočník získa jednoduchým spôsobom citlivé údaje spoločnosti.

Opatrenie: Prístup k Internetu je umožnený iba zamestnancom, ktorý ho nevyhnutne potrebujú k svojej práci. Po prijatí do zamestnania, bude zamestnanec poučený o právnych

aspektoch a postihoch hroziacich zamestnancom, po porušení bezpečnostnej politiky spoločnosti. Preškoľovanie zamestnancov sa vykonáva 1x za rok a vykonáva ho IT manažér alebo zamestnanec na to určený IT manažérom. Všetka komunikácia je zaznamenávaná a následne vyhodnocovaná.

Prínos: Rýchle získanie potrebných informácii.

5.5.2 Sťahovanie súborov a SW z Internetu

Riziko: Inštalácia nebezpečného vírusu do systému, nainštalovanie a následne používanie nelicencovaného SW.

Následok: Narušenie bezpečnosti siete a vytvorenie chyby v zabezpečení siete, poškodenie zariadenia, pokuta za používanie nelicencovaného SW.

Opatrenie: Podľa vnútorných smerníc spoločnosti je zakázané sťahovať akýkoľvek SW bez overenia správcom siete. Keď užívateľ potrebuje špeciálny SW k svojej práci, požiada o zabezpečenie SW správcu siete. Po nedodržaní smerníc, budú vyvodené finančné postihy a finančná škoda spôsobená spoločnosti.

Prínos: Ľahké získanie dokumentov.

5.5.3 Ukladanie dokumentov na verejné FTP servery

Riziko: Zverejnenie citlivých údajov spoločnosti.

Následok: Strata zisku, poškodenie dobrého mena spoločnosti, strata zákazníkov a dodávateľov.

Opatrenie: Podľa vnútorných smerníc spoločnosti je zakázané ukladať dáta spoločnosti na verejne dostupné FTP servery. Všetky adresy verejných FTP serverov budú zapísané do zoznamu blokovaných stránok, takzvaného „black listu“. Aj keď sa užívateľ bude pokúšať dostať na tieto stránky, proxy server spoločnosti zablokuje prístup na takýto druh serveru.

Prínos: Jednoduché zdieľanie súborov.

5.5.4 Filtrovanie prístupu na internet

Riziko: Zablokovanie povolených stránok, infiltrovanie škodlivého SW.

Následok: Spomalenie procesu získavania informácii, narušenie bezpečnosti systému

Opatrenie: Na proxy serveri je vytvorený zoznam blokovaných stránok, takzvaný „Black list“. Na tomto zozname sa nachádzajú stránky, ktoré sú označované ako nebezpečné. Manažment môže tento list doplniť podľa svojich požiadaviek. Na tomto zozname sa nachádzajú adresy sociálnych sieti, video stránok a verejných FTP serverov.

Prínos: Efektívnejšie využívanie internetu.

5.6 Telefóny

5.6.1 IP telefóny

Riziko: Zneužívanie telefónov pre súkromné účely.

Následok: Finančná strata, únik informácii

Opatrenie: Telefonovanie v rámci spoločnosti je bez kontroly a ochrany. Telefonovanie do verejných sieti je chránené heslom a telefonát je zaznamenávaný. Povoľovacie heslo je sprístupnené užívateľovi telefónu.

Prínos: Priama a rýchla komunikácia.

5.6.2 GSM telefóny

Riziko: Zneužívanie telefónov pre súkromné účely.

Následok: Finančná strata, únik citlivých informácii.

Opatrenie: GSM telefóny sú pridelené len zamestnancom, ktorí musia byť dostupní nonstop. Hovory z GSM telefónov sú povolené iba na firemné telefónne čísla. Prijímanie telefonátov je neobmedzene. Každý prijatý telefonát je zaznamenávaný.

Prínos: Neustále dostupný zamestnanec

5.7 Prístupové práva do systému

5.7.1 Zaobchádzanie s heslami

Riziko: Neoprávnený prístup k citlivým dátam.

Následok: Únik citlivých dát spoločnosti, ktoré môžu viesť k oslabeniu pozície na trhu.

Opatrenie: Každý zamestnanec je povinný uchovávať svoje heslo v tajnosti, nesmie si ho zapísať. Pri zadávaní hesla do systému si musí dávať pozor, aby ho nikto neodsledoval. Heslo nesmie poskytnúť nikomu, ani správcovi systému.

Prínos: Zníženie rizika zneužitia hesla.

5.7.2 Zložitosť hesla pre užívateľov

Riziko: Ľahké odsledovanie a prelomenie hesla.

Následok: Zneužitie prístupového oprávnenia

Opatrenie: Užívateľ bude pri prvom prihlásení do systému, vyzvaný na zmenu hesla. Toto heslo musí byť zložené minimálne z 8 znakov. Týchto 8 znakov nesmie obsahovať meno a priezvisko užívateľa a jeho prihlasovacie meno. Heslo musí byť zložené z písmen a minimálne dvoch číslic.

Prínos: Zníženie rizika prelomenia a odsledovania hesla.

5.7.3 Zložitosť správcovských hesiel

Riziko: Jednoduché a rýchle prelomenie prístupového hesla.

Následok: Ovládanie systému a prístup k nezabezpečeným dátam.

Opatrenie: Administrátor si musí zvoliť takzvane „silné heslo“. Toto heslo sa skladá z rôznych symbolov, veľkostí písmen a číslic. Heslo musí byť kombinácia uvedených znakov a minimálna dĺžka hesla je 10 znakov. Toto heslo si nesmie nikde poznamenať a prezradiť ho žiadnej osobe.

Prínos: Zníženie rizika prelomenia hesla.

5.7.4 Zložitosť najvyššieho hesla pre vstup do systému

Riziko: Jednoduché a rýchle prelomenie prístupového hesla.

Následok: Absolútne ovládnutie systému.

Opatrenie: Toto heslo slúži pre zadanie administrátorských účtov a konfiguráciu serveru bez ohľadu na právomoci. Heslo musí byť kombinácia rôznych symbolov, písmen a číslic v nezmyselnom poradí o dĺžke 20 znakov. Po zadaní tohto hesla bude zapísané a uložené v zapečatenej obálke v ohňovzdornom trezore. Prístup do systému pod týmto špeciálnym

účtom sa smie len v špeciálnych prípadoch, keď sú oprávnenia administrátorov nepostačujúce. Pri práci v systéme pod týmto účtom musia byt prítomní IT manažér a dvaja správcovia siete.

Prínos: Zníženie rizika absolútneho ovládnutia systému.

5.8 Hardware

5.8.1 Nákup hardwaru

Riziko: Podcenenie funkčnosti a kvality zariadenia.

Následok: Vyššie finančné náklady za hardware.

Opatrenie: Zariadenie sa kupuje podľa účelnosti a potreby. U často sa poruchových zariadení sa kupujú náhradné diely alebo časti do zásoby, aby bola možná okamžitá výmena, pokiaľ nie je nutný špecializovaný servis. Pri nákupe sa kladie dôraz na kvalitu, bezpečnosť a efektivitu zariadenia. Potrebné zariadenia sa vyberajú podľa výsledkov testov, ktoré vykonali uznávané spoločnosti. Zariadenia musia byť svojou kapacitou a výkonom predimenzované o 10% z potrebnej kapacity, z dôvodu zvyšovania sa nároku na zariadenia.

Prínos: Dlhšia životnosť zariadení.

5.8.2 Evidencia prenosných zariadení

Riziko: Nesprávny záznam prideleného zariadenia k užívateľovi, strata zariadenia.

Následok: Finančná strata, problém pri zistení zodpovedného zamestnanca.

Opatrenie: Eviduje sa meno zamestnanca, číslo zamestnanca, sériové číslo zariadenia, model zariadenia a popis zariadenia. Ak sa jedná o mobilný telefón, eviduje sa aj pridelené telefónne číslo. Tieto údaje sa vedú v elektronickej a tlačenej podobe a sú zaradené do kategórie interné dáta.

Prínos: Rýchle a prehľadné zistenie užívateľa zariadenia.

5.8.3 Vyradenie zariadení

Riziko: Zariadenia môžu uchovávať citlivé dáta.

Následok: Strata a prezradenie citlivých dát spoločnosti.

Opatrenie: Na úložných zariadeniach, ktoré boli vyradené z dôvodu obnovy systému, musia byť vymazané systémové nastavenia a firemné dáta. Musí sa pri tom použiť metóda, aby sa tieto dáta nedali opätovne získať späť. Pokiaľ sa vymenia, poškodené zariadenia musia byť ekologicky a bezpečne znehodnotené. Znehodnotenie zariadenia musí prebiehať pod dozorom zamestnanca na túto prácu určeného.

Prínos: Odpredajom zariadenia sa navráti malá časť investovaných financií.

5.8.4 Používanie prenosných zariadení

Riziko: Zneužívanie zariadenia na súkromné účely.

Následok: Časté poškodenie zariadenia, opotrebovanie zariadenia.

Opatrenie: Užívateľ sa musí k zariadeniu správať šetrne. Pri nešetrnom zaobchádzaní, bude voči užívateľovi vyvodený finančný postih za spôsobenú škodu na zariadení. Do zariadenia nesmie inštalovať alebo kopírovať dáta, ktoré nie sú určené pre prácu. Pri poruche alebo poškodení je nutné túto skutočnosť okamžite nahlásiť správcovi siete. Užívateľ sa nesmie pokúsiť samovoľne opravovať toto zariadenie a nesmie ho používať pokiaľ chyba nebude odstránená.

Prínos: Zamestnanec je zodpovedný za zariadenie a nesie zodpovednosť za poškodenie.

5.8.5 Uloženie a uskladnenie hardwaru

Riziko: Ukradnutie alebo úmyselné poškodenie zariadení.

Následok: Strata a vyzradenie citlivých dát spoločnosti.

Opatrenie: Zariadenia s archivovanými dátami sú uložené v bezpečnostnom trezore, odolnom voči ohňu. Trezor by mal byť špecializovaný pre uchovávanie magnetických zariadení a inštalovaný na stráženom a bezpečnom mieste, oddelene od používaných dát.

Zariadenia s aktuálne používanými dátami sú uložené v zabezpečenej, monitorovanej miestnosti so samohasiacim systémom.

Prínos: Ľahká obnova dát a konfigurácie systému pri zničení systému.

5.8.6 Poistenie

Riziko: Uzavretie nevýhodného poistenia

Následok: Strata finančných prostriedkov neočakávaným poškodením zariadenia a neuznanie vyplatenia poistky.

Opatrenie: Spoločnosť musí mať uzatvorené poistenie na rôzne druhy hrozieb. Spoločnosť musí spĺňať všetky podmienky pre vyplatenie poistky. Poistná suma musí byť uzatvorená na minimálnu hodnotu nainštalovaného IS.

Prínos: Ochrana spoločnosti pred finančnými stratami spôsobenými nepredvídateľnou situáciou.

5.9 Dáta v tlačenej podobe

5.9.1 Tlačiarne

Riziko: Prenos elektronických dát do tlačenej nezistiteľnej podoby.

Následok: Získanie citlivých dát spoločnosti.

Opatrenie: Všetka tlač je monitorovaná a zaznamenávaná. Zo spoločnosti je zakázané vynášať dáta v tlačenej podobe, o ktorých nebolo informované vedenie. Po práci s citlivými dátami v tlačenej podobe musia byť papiere skartované, alebo uložené na zabezpečené miesto.

Prínos: Zabránenie fyzickému prístupu tretích osôb k dátam.

5.10 Software

5.10.1 Zakúpený SW

Riziko: Krádež SW a zneužitie zakúpenej licencie.

Následok: Žaloba spoločnosti od výrobcu SW.

Opatrenie: Zakúpený SW musí spĺňať potrebné licenčné podmienky. Vykonáva sa pravidelná kontrola užívateľských PC, či nie je nainštalovaný nelicencovaný SW. Kontroluje sa licencia SW a meno užívateľa. Všetky inštalačné súbory programov sú prístupné iba pre správcov siete. Inštalačné súbory a média sú zabezpečené proti krádeži, zneužitiu a poškodeniu v bezpečnostnej skrini.

Prínos: Rýchla a jednoduchá práca v systéme.

6 OCHRANA PRED ÚTOKMI A VÍRUSMI

6.1 Úmyselné vonkajšie útoky

Riziko: Ťažko zistiteľný útočník a ťažko zistiteľné škody.

Následok: Strata dát a narušenie bezpečnosti systému.

Opatrenie: Pri zistení narušenia systému sa zablokuje pripojenie k internetu. Tento útok sa nahlási orgánom činným v trestnom konaní. Po analýze škôd spôsobených útočníkom, sa musia všetky nedostatky odstrániť a vytvoriť nápravné opatrenia pre zabránenie opakovanému útoku.

Prínos: Snaha o minimalizáciu rizika útoku.

6.2 Úmyselné vnútorné útoky

Riziko: Útočník pozná systém a má k nemu uľahčený prístup.

Následok: Ukradnutie citlivých dát.

Opatrenie: Sieť je monitorovaná nástrojmi na to určenými. Monitorujú sa neúspešné pokusy o prihlásenie sa do systému a k chráneným dátam. Každý zamestnanec sa zaviazal pri nástupe do zamestnania správať sa podľa bezpečnostnej politiky. Pri zistení porušenia bezpečnostnej politiky, budú voči tomuto zamestnancovi vyvodené dôsledky. Po zistení narušenia sa vykoná analýza problému a vytvorenie nápravného opatrenia zamestnancami IT oddelenia.

Prínos: Snaha o minimalizáciu rizika útoku.

6.3 Vírusy

Riziko: Narušenie bezpečnosti systému.

Následok: Narušenie zabezpečenia systému.

Opatrenie: Na každej pracovnej stanici a na serveroch je nainštalovaný antivírusový program, ktorý je pravidelne aktualizovaný a monitorovaný. Antivírusový program monitoruje počas činnosti zariadenia všetku komunikáciu a zisťuje, či neobsahuje škodlivé

kódy. Pokiaľ škodlivé kódy zistí, pokúsi sa ich odstrániť zo súborov alebo ich odizoluje od systému. Umiestni ich do karantény a následne ich správca siete zanalyzuje.

Prínos: Zníženie rizika poškodenia zabezpečenia systému.

7 ZABEZPEČENIE PRÍSTUPU K SERVEROVNI

Riziko: Vniknutie cudzej osoby za účelom poškodenia zariadení.

Následok: Zastavenie fungovania spoločnosti, finančná strata.

Opatrenie: Objekt a prístup do objektu je strážený 24 hodín denne súkromnou bezpečnostnou službou. Serverovňa a archív sú chránené ohňovzdornými bezpečnostnými dverami. Prístup do serverovne a archívu má iba správca systému, ktorý pri ukončení pracovnej doby odovzdá kľúče od týchto miestností zamestnancovi SBS. Zamestnanec SBS je povinný spraviť protokol o prevzatí kľúčov a kľúče vložiť do kľúčového trezora. Tieto miestnosti sú 24 hodín denne monitorované kamerovým, bezpečnostným a protipožiarnym systémom.

Prínos: Zamedzenie finančným stratám.

8 ZMLUVNÉ ZAVIAZANIE DODRŽIAVANIA BEZPEČNOSTNEJ POLITIKY PRE IKS

Riziko: Ohrozenie spoločnosti, nervozita zamestnancov.

Následok: Ochromenie systému, zmena zamestnancov.

Opatrenie: Každý zamestnanec má v rámci pracovnej zmluvy zakotvený odsek o dodržiavaní interných predpisov spoločnosti, ako aj pracovnej disciplíny, bezpečnostných predpisov a zákaz podávania informácii tretím stranám. Podpisom sa zaväzuje, že porozumel a bol poučený o vnútornom poriadku a predpisoch. Je povinný ich dodržiavať a rešpektovať. Pokiaľ závažne poruší predpis, bude personálne riešený.

Prínos: Zodpovednosť za svoje konanie.

9 OBNOVENIE POVEDOMIA O BEZPEČNOSTNEJ POLITIKE

Riziko: Neabsolvovanie školenia.

Následok: Ohrozenie spoločnosti.

Opatrenie: Tieto školenia vedie IT manažér alebo zamestnanec na to určený. Každý zamestnanec je povinný sa školení zúčastňovať. Pokiaľ sa ho nemôže zúčastniť musí dať odôvodnenie personálnemu oddeleniu. Personálne oddelenie je povinné posúdiť a zorganizovať náhradný termín školenia. Na záver školenia musia zamestnanci vyplniť dotazník, ktorý sa týka bezpečnostnej politiky.

Prínos: Obnovenie povedomia o zachovávaní bezpečnosti systému.

10 PORUCHA A ZRÚTENIE SYSTÉMU

Riziko: Výpadok elektrického napätia a útok na IKS

Následok: Poškodenie systému a strata dát.

Opatrenie: Spoločnosť má vypracovaný krízový plán, pre postupy v krízových situáciách, ako výpadok energie, útok na systém a nepredvídateľné situácie. Pri výpadku energie je presne definované odstavenie systému za pomoci UPS zariadení. Za nepredvídateľné situácie sa považuje požiar, záplavy, zemetrasenie a ďalšie prírodné katastrofy. Z tohto dôvodu musia byť záložné dáta uložené čo najbezpečnejšie a na najodolnejšom mieste. Po strate IKS sa môže vykonať jednoduchá a rýchla obnova.

Prínos: Pripravenosť spoločnosti na nečakané udalosti.

ZÁVER

Po zavedení bezpečnostnej politiky pre IKS sa zlepšilo zabezpečenie systému a povedomie o politike spoločnosti na postačujúcu úroveň. Bohužiaľ, stopercentná ochrana proti útočníkom neexistuje. Ak nechceme svoj systém "odstrihnúť od Internetu" , musíme sa uspokojiť s "reálnejšími" metódami ochrany. Tieto metódy si kladú za cieľ, čo najviac minimalizovať riziko útoku na systém, jeho rýchlu detekciu v prípade, že bol úspešný a najmä - rýchle a bezpečné zotavenie sa z jeho následkov.

Samotná práca je len časť reálnej bezpečnostnej politiky, ktorá bola zavedená v spoločnosti.

.

ZÁVER V ANGLIČTINE

After the introduction of security policy for IKS to improve system security and awareness of company policy on a sufficient level. Unfortunately, a wholly owned no protection against attackers. If you do not want to cut system from the Internet, we must be content with "realistic" methods of protection. These methods aim to, as much as possible to minimize the risk of attack on the system, it´s rapid detection in the event that was successful and in particular - quickly and safty recover from it´s effects.

The work itself is only part of the actual security policy, which was introduced in the company.

ZOZNAM POUŽITEJ LITERATÚRY

1. *Tomáš LOVEČEK.* Bezpečnostná it politika ako jeden zo základných dokumentov organizácie. *Security Revue : Information Security* [online]. 19.4.2006, [cit. 2011-04-02]. Dostupný z WWW: http://www.securityrevue.com/article/2006/04/bezpecnostna-it-politika-ako-jeden-zo-zakladnych-dokumentov-organizacie/

2. MIKOLAJ, Ján, et al. *Security revue* [online]. 2005 [cit. 2011-03-25]. Terminológia bezpečnostného manažmentu výkladový slovník. Dostupné z WWW: <http://www.securityrevue.com/tbm/part1_a.html#aktivum>.

3. Slovenská republika. Zbierka zákonov. In *Zbierka zákonov Slovenskej republiky*. 2005, 167, s. 4403. [cit. 2011-03-25]. Dostupný z WWW: <http://www.zbierka.sk/zz/predpisy/default.aspx?PredpisID=16630&FileName=02-z428&Rocnik=2002 >.

4. Slovenská republika. Zbierka zákonov. In *Zbierka zákonov Slovenskej republiky*. 2009, 177, s. 3866. [cit. 2011-03-25]. Dostupný z WWW: <http://www.zbierka.sk/zz/predpisy/default.aspx?PredpisID=209337&FileName=zz2009-00506-0209337&Rocnik=2009 >.

5. MIKOLAJ, Ján, et al. *Security revue* [online]. 2005 [cit. 2011-03-25]. Terminológia bezpečnostného manažmentu výkladový slovník. Dostupné z WWW: <http://www.securityrevue.com/tbm/part1_p.html#pachatel>.

6. MIKOLAJ, Ján, et al. *Security revue* [online]. 2005 [cit. 2011-03-25]. Terminológia bezpečnostného manažmentu výkladový slovník. Dostupné z WWW: <http://www.securityrevue.com/tbm/part1_a.html#audit>.

7. *Ústredný portál verejnej správy* [online]. 2007 [cit. 2011-03-19]. Čo je elektronický podpis a časová pečiatka?. Dostupné z WWW: <http://portal.gov.sk/Portal/sk/Default.aspx?CatID=17&eventid=1677>.

8. LAUCKÝ, Vladimír. i komerční bezpečnosti I. Vyd. 3. Zlín : Univerzita Tomáše Bati ve Zlíně, 2010. 81 s. ISBN 978-80-7318-889-4.

9. LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II. Vyd. 2. Zlín : Univerzita Tomáše Bati ve Zlíně, 2007. 123 s. ISBN 978-80-7318-631-9.

10. LAUCKÝ, Vladimír. Řízení technologických procesů v průmyslu komerční bezpečnosti. Vyd. 2. Zlín : Univerzita Tomáše Bati ve Zlíně, 2006. 101 s. ISBN 80-7318-432-X.

11. KAMENÍK, Jiří; BRABEC, František. Komerční bezpečnost : soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur. Vyd. 1. Praha : ASPI, 2007. 338 s. ISBN 978-80-7357-309-6.

12. BRABEC, František. Ochrana bezpečnosti podniku. Vyd. 1. Praha : Eurounion, 1996. 203 s. ISBN 80-85858-29-0.

13. JAŠEK, Roman. Informační a datová bezpečnost. Zlín : Univerzita Tomáše Bati ve Zlíně, Fakulta managementu a ekonomiky, 2006. 140 s. ISBN 80-7318-456-7.

14. KOSTRECOVÁ, Eva : INFORMAČNÁ BEZPEČNOSŤ 4., Slovenska technická univerzita v Bratislave, Fakulta elektrotechniky a informatiky, Dostupne na internete: <http://download.matus.in/security/Informacna%20bezpecnost%20%20predmet%20na%20FEI/2008.04.ppt > (4.2.2011)

15. *LOVEČEK, Tomáš, http://www.securityrevue.com/article/2006/04/bezpecnostna-it-politika-ako-jeden-zo-zakladnych-dokumentov-organizacie/*

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

IKT Informačno -- komunikačné technológie

IKS Informačno – komunikačný systém

FTP Súborový server

SR Slovenskej republiky

Z. z. Zbierky zákonov

IT Informačné technológie

IP Internet Protocol

MAC Media Access Control address (MAC address)

PC Personal computer

SW Software

UPS Uninterruptible Power Supply (záložný zdroj)

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

ZOZNAM OBRÁZKOV

PRÍLOHA

Grafické zobrazenie výsledkov testov o povedomí bezpečnostnej politiky.