Návrh zabezpečení informačního systému podniku střední velikosti ve více lokacích

Bc. Michal Rubeš

Diplomová práce
2016

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2015/2016

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Michal Rubeš**
Osobní číslo:	**A13389**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Návrh zabezpečení informačního systému podniku střední velikosti s pobočkami ve více lokacích**
Téma anglicky:	**Draft Security Information System Medium-sized Companies with Offices in Multiple Locations**

Zásady pro vypracování:

1. **Formou literární rešerše popište současný stav předmětné problematiky a úroveň jeho řešení v informačních zdrojích.**
2. **Vytvořte modelovou strukturu podniku a jeho informačního systému.**
3. **Analyzujte současný stav zabezpečení informačního systému podniku.**
4. **Na základě výsledků analýzy navrhněte vhodný způsob zabezpečení informačního systému podniku.**
5. **Proveďte vyhodnocení celého projektu.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **JAŠEK, R. Ochrana znalostí a dat v podnikových informačních systémech. Zlín : Univerzita Tomáše Bati ve Zlíně, 2002. 115 s. ISBN 80-7318-095-2.**
2. **JAŠEK, R. Informační a datová bezpečnost. Univerzita Tomáše Bati ve Zlíně. 2006. 140s. ISBN 80-7318-456-7.**
3. **MALANÍK D., VÝZNAM FYZICKÉHO ZABEZPEČENÍ IT SYSTÉMŮ. Security Revue září 2010. ISSN 1336-9717.**
4. **DOUCEK, Petr, NOVÁK, Luděk, SVATÁ, Vlasta. Řízení bezpečnosti informací. 2. rozšíř. vyd. Praha : PROFESSIONAL PUBLISHING, 2011. 266 s. ISBN 978-80-7431-050-8.**
5. **SOSINSKY, Barrie. Mistrovství - počítačové sítě. [editor] Libor Pácl. [překl.] Josef Pojsl a Pavel Vaida. Brno : Computer Press, a.s., 2010. ISBN 978-80-251-3363-7.**

Vedoucí diplomové práce:	**doc. Ing. Jiří Gajdošík, CSc.** Ústav bezpečnostního inženýrství
Datum zadání diplomové práce:	**5. února 2016**
Termín odevzdání diplomové práce:	**16. května 2016**

Ve Zlíně dne 5. února 2016

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

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Jméno, příjmení: Michal Rubeš

Název bakalářské/diplomové práce: Návrh zabezpečení informačního systému podniku střední velikosti ve více lokacích

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 připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, 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/bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne 13.5.2016

.....
podpis diplomanta

ABSTRAKT

Účelem této diplomové práce je zabezpečení informačního systému podniku střední velikosti s více pobočkami. Práce se skládá ze dvou hlavních částí. V první části jsou představeny současné trendy používané v zabezpečení informačních systémů. Část druhá se již zabývá bezpečnostní analýzou současného stavu informačního systému daného podniku a návrhem vhodných řešení pro zvýšení bezpečnosti informačního systému.

Klíčová slova: bezpečnost, IS, IPS, firewall, zálohování, switch, diskové pole

ABSTRACT

The purpose of this diploma thesis is the proposal for the security of mid-size company located in more locations. This thesis is composed of two parts. In the first part are introduced contemporary trends in security of information systems. The second part deals with security analysis of current state of information system of company and proposal of suitable steps for the increase of security of the information system.

Keywords: IS, IPS, firewall, backup, switch, RAID

Na tomto místě bych rád poděkoval vedoucímu své diplomové práce panu doc. Ing. Jiřímu Gajdošíkovi, Csc. za jeho obětavou pomoc, věnovaný čas a odborné vedení mé diplomové práce.

Také bych chtěl vyjádřit díky své přítelkyni a rodině za trpělivost a podporu.

Motto:

„Informační bezpečnost je imunitní systém v těle podnikání.“

Kevin Pietersma, Information Security Architect, University of Toronto

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Zabezpečení informačních systémů je i v dnešní době v některých podnicích značně zanedbáváno. Management těchto podniků často nevidí žádné rozumné důvody pro investování do vylepšení či zabezpečení jejich firemní infrastruktury. Tento pohled se ovšem vždy změní po zažití krizové situace, při které podnik čelí ztrátě dat, výpadku výroby z důvodu nedostupnosti informačního systému nebo prozrazení výrobního tajemství. Náklady vynaložené na odstranění vzniklých škod potom často mnohonásobně převýší původní náklady vyčíslené na zabezpečení podniku před krizovou situací.

První část této práce je zaměřena teoreticky. V první polovině je čtenář seznámen s postupy, které mu pomohou identifikovat současný stav informačního systému, analyzovat jej a navrhnout vhodná řešení či opatření pro zvýšení jeho bezpečnosti. K tomu mu následně pomůže druhá polovina teoretické časti, která čtenáři představí současné trendy používané ve fyzické, datové i personální bezpečnosti.

Druhá část je praktická a je zaměřena na řešení zadaného problému. Postupně je analyzován současný stav informačního systému podniku střední velikosti s pobočkami v různých lokacích, identifikovány bezpečnostní problémy, navržena vhodná řešení, jenž pomohou minimalizovat či plně odstranit následky identifikovaných problémů. V závěru je nastíněn i další možný rozvoj bezpečnosti informačního systému.

I. TEORETICKÁ ČÁST

1 INFORMAČNÍ SYSTÉM

Informační systém (IS) je soubor lidí, hardwarového a softwarového vybavení, záznamových médií, dat a metod, které zajišťují práci s informacemi. Prací s informacemi rozumíme jejich sběr, zpracování a uchovávání za účelem prezentace těchto dat uživatelům IS.

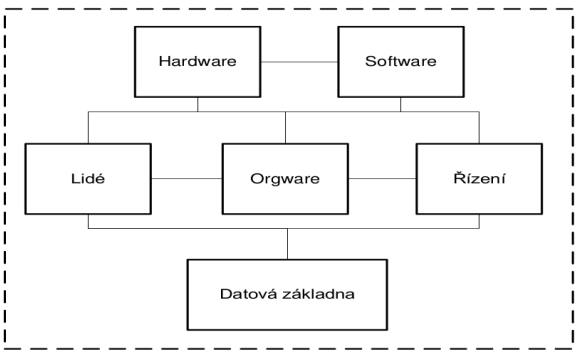
Šíře a implementace informačních systémů ve společnosti je různorodá. Od zápisníku starší paní, přes chytrý telefon podnikatele až po sofistikovaný informační systém nadnárodní společnosti.

V této práci mají jednotlivé prvky IS následující podobu:

- hardwarové vybavení – servery, pracovní stanice, počítačová síť, atd.,
- softwarové vybavení – operační systémy, aplikace, atd.,
- záznamová média – pásky, DVD, atd.,
- data – soubory, databáze, atd.,
- lidé – administrátoři, uživatelé, atd.

Výše uvedený popis je ale značně zjednodušený. Pokud někdo bude informační systém zkoumat do větší hloubky, jistě zjistí, že informační systém lze definovat jako určitou skupinu prvků, jejich vzájemných vazeb a chování.

U informačních technologií jsou zajisté hlavními částmi IS hardware a software. Tyto součásti by ale určitě nemohly dokonale spolupracovat bez dalších neméně důležitých prvků IS. Firmy mají svá interní pravidla a definované odpovědnosti - co se má kam vkládat, ukládat či zaznamenávat. Tato část IS se nazývá orgware. Neopomenutelnou součástí správně fungujícího IS jsou i zaměstnanci firmy, kteří systém používají a management firmy, jenž se stará o rozvoj systému a určuje úroveň jeho řízení. [21]



Obrázek 1 – Informační systém [21]

2 BEZPEČNOST

Pod pojmem „bezpečnost“ si každý člověk ve společnosti vybaví něco jiného. Je to ovlivněnou prostředím, ve kterém se dennodenně vyskytuje. Ale i tyto různé představy budou mít něco společného. Spojovat je bude myšlenka na ochranu, ochranu něčeho, co pro daného člověka má určitý význam. Může se jednat o ochranu zdraví, života, majetku, ale i informací a znalostí.

Zaručení bezpečnosti těchto subjektů v konečném důsledku může být i značně propojeno. Prozrazení informace o úkrytu skrývané osoby může znamenat značné ohrožení jejího života. Proto i bezpečnost informačních systému má svůj význam.

2.1 Obecné pojmy informační bezpečnosti

Pokud se začneme zabývat informační bezpečností, narazíme na pojmy, které nemusí být úplně jasné či hned zřejmé, proto si v následující časti uvedeme ty nejhlavnější a krátce si je vysvětlíme. [20]

- **Autentizace** – akce, při které musí osoba či zařízení předložit svou identitu k ověření. Více o autentizaci v kapitole 5.9.
- **Autorizace** – proces ověření, zda osoba či zařízení smějí na základě přidělených oprávnění či práv provést danou činnost. Více o autorizaci v kapitole 5.9.
- **Autenticita** – znak, který poskytuje ověřující informaci o tom, že identita a původ osoby či zdroje je opravdu takový, jaký prohlašují. Lze ji stáhnout na objekty, jako jsou uživatelé, informace, procesy či systémy.
- **Citlivá data** – data důležitá pro firmu. Jejich zneužití, zničení či ztráta může mít negativní dopad na chod firmy.
- **Dostupnost** – vlastnost zdroje dat, který musí být dostupný po celou nutnou dobu pro všechny autentizované a autorizované subjekty v systému.
- **Důvěrnost** (Důvěryhodnost) – data jsou poskytována pouze autentizovaným a autorizovaným osobám či zařízením.
- **Hrozba** – možné ohrožení informačních aktiv firmy.
- **Informační aktiva** – jinými slovy se jedná o aktiva – data, která mají pro firmu hodnotu a význam (data vytvořena při práci lidí ve firmě).

- **Integrita** – aby si data udržela správnost, je nutné, aby operace s nimi byly prováděny pouze ověřenými osobami nebo zařízeními (musí být autentizované a autorizované).
- **Nepopiratelnost** – nemožnost popřít autorství autentických dat. V praxi řešeno například elektronickým podpisem.
- **Riziko** – možnost naplnění hrozby. Každá potenciální hrozba má jinou míru rizika jejího naplnění.

2.2 Informační bezpečnost

Hodnota informace je v dnešní době nepopiratelná. Ten kdo ví něco, co ostatní ne, ví něco přesněji nebo rychleji než ostatní, je ve výhodě. Dříve stačilo takové informace zaznamenané na papíře uschovat do zabezpečeného trezoru. V kombinaci s vhodně zvolenou fyzickou ostrahou pak byla tato informace velice dobře chráněna proti možným hrozbám.

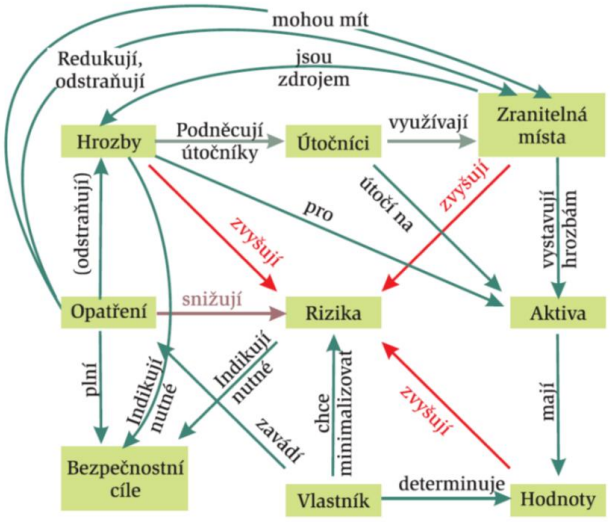
V dnešní době je situace ale značně odlišná. S digitalizací informací a jejich přemístěním z papíru na disky počítačů se situace nijak dramaticky v ochraně nezměnila. Stále stačilo počítač umístit do dobře chráněného trezoru. Vše ale změnil nástup internetu a zapojení většiny počítačů do něj. Takový počítač již nelze považovat za dostatečně zabezpečený. K jeho ochraně a ochraně informací na něm uložených je nyní potřeba vyvinout mnohem větší úsilí a použít mnohem více znalostí.

I přes tento vývoj a změny v postupech ochrany informací lze bezpečný informační systém definovat pro každou dobu. Bezpečný informační systém je systém, který dokáže chránit informaci během jejího vzniku, zpracování, ukládání, přenosu a likvidace prostřednictvím logických, technických, fyzických a organizačních opatření, která informaci chrání proti ztrátě důvěrnosti, integrity a dostupnosti.

Důležité je si také uvědomit, že IS nelze nikdy zabezpečit stoprocentně a vždy bude existovat míra přijatelného rizika, která se bude lišit na základě charakteristiky prostředí, ve kterém je daný IS implementován (státní organizace, výzkum, malé až střední firmy, atd.). [1]

2.3 Obecný model bezpečnosti IT

Bezpečnost informačních technologií je nikdy nekončící proces, jehož hlavním cílem je neustále se zlepšovat, reagovat a řešit nově vzniklá rizika. Následující obrázek nám znázorňuje obecný model bezpečnosti, jeho hlavní prvky a vztahy mezi nimi.



Obrázek 2 – Obecný model bezpečnosti informačních technologií [22]

2.4 Analýza bezpečnosti informačního systému

Cílem bezpečnostní analýzy (BA) rizik je prověření aktuálního stavu bezpečnosti námi zkoumaného IS. BA by měla zejména odhalit slabá místa v systému a poskytnout co nejvhodnější řešení k odstranění těchto slabých míst. Výstupem analýzy je podrobná dokumentace o situaci IS firmy.

Při provádění BA IS nesmíme zapomenout, že cílem zkoumání není IS samotný, ale i lidé a procesy, jenž do styku s IS přijdou. Proto při správně prováděné analýze IS je kladen důraz i na sociální oblast, neboli lidský faktor, který se při opomenutí této oblasti může stát slabým místem systému. Toho pak mohou zneužít i lidé, kteří vůbec nedisponují potřebnými znalostmi nebo nejsou zaměstnanci daného podniku (uklízečky, ostraha objektu, atd.).

Implementace BA může zabránit úniku kritických dat, zachránit poškození dobrého jména firmy, stabilizovat organizaci, dokonce při zvolení BA, která splňuje podmínky certifikátů řady ISO (např. ISO 13335[1]) i značně přispět ke zvýšení důvěryhodnosti firmy. [2]

Bezpečnostní analýza rizik se může například skládat z těchto obecných kroků:

- **Stanovení hranice bezpečnostní analýzy rizik** – na začátku analýzy je potřeba určit, která data do analýzy patřit budou a která naopak ne. Tímto krokem je určen výsledný rozsah analýzy. Tato hranice je většinou stanovena vedením podniku.
- **Identifikace aktiv** – vytvoření seznamu aktiv, která byla identifikována uvnitř stanovené hranice pro bezpečnostní analýzu rizik.
- **Stanovení hodnoty a seskupování aktiv** – hodnota aktiv může být stanovena podle různých kritérií. Obecně tato kritéria můžeme rozdělit na nákladové a výkonnostní charakteristiky aktiv. Při výběru se vždy použijí ty, které pro podnik mají vyšší hodnotu. Příkladem kritérií mohou být například know-how, pořizovací cena, zisky z aktiv, ochranná známka a další. Do hodnoty aktiv je také potřeba započítat hodnotu aktiv pro firmu v případě jejich ztráty, zničení, prozrazení, atd. Jelikož podnik může vlastnit velké množství aktiv, je vhodné daná aktiva členit do skupin podle typů a na základě toho stanovit jejich hodnotu pro danou skupinu.
- **Identifikace hrozeb** – v tomto kroku je zapotřebí identifikovat hrozby, jenž hrozí určeným aktivům. Každá identifikovaná hrozba musí vždy ohrožovat nejméně jedno aktivum. Hrozby jsou vybírány z různých zdrojů jako například z oborových zkušeností, předešlých analýz atd.
- **Analýza hrozeb a zranitelností** – pro každou určenou hrozbu z předchozího kroku je potřeba určit její ohodnocení vůči všem skupinám aktiv. Je nezbytné, aby pro aktiva, kde lze danou hrozbu uplatnit byla uvedena úroveň hrozby vůči aktivu a také míra zranitelnosti aktiva vůči hrozbě. Vlivy, jako jsou motivace, přístup či nebezpečnost se použijí pro stanovení úrovně hrozby. Kritičnost a citlivost budou použity naopak pro určení míry zranitelnosti.
- **Pravděpodobnost jevu** – hodnocení kritičnosti hrozby je potřeba také doplnit o hodnotu, jenž určuje s jakou pravděpodobností se daná hrozba může vyskytnout.

[1] Více o ISO normách - http://www.iso.org/iso/catalogue_detail.htm?csnumber=39066

Tuto hodnotu je pak nezbytné zahrnout do celkového výpočtu a návrhu adekvátních protiopatření. Pravděpodobnost pak může být označená jako náhodný jev, může být určen interval pravděpodobnosti nebo naopak může být hrozba úplně vyloučena ze seznamu uvažovaných hrozeb.

- **Měření (hodnocení) rizika** – výše rizika je odvozena z hodnoty aktiv, úrovně hrozby a zranitelnosti aktiv. Jak již bylo zmíněno dříve, tato ohodnocení mohou mít různé hodnoty podle úhlu pohledu. Proto je stanovení míry rizika dosti obtížný úkol.

  Příklad stupnice hodnocení rizika:

  - **Bezvýznamné, zanedbatelné riziko** – nehrozí žádný dopad na chod firmy či její aktiva.
  - **Akceptovatelné, méně významné riziko** – dopad je pro firmu zanedbatelný. Je potřeba rozhodnout, jestli finanční náklady spojené s eliminací rizika nepřevýší cenu jeho dopadu.
  - **Nízké riziko** – firmě hrozí při projevení rizika potíže (například s výrobou) a finanční ztráty.
  - **Nežádoucí riziko** – firmě hrozí při projevení rizika vážné potíže a velké finanční ztráty.
  - **Nepřijatelné riziko** – firmě hrozí existenční potíže (například nemožnost vyrábět, neplnit závazky). [23]

2.4.1 Metody analýzy rizik

Metody analýzy rizik se rozdělují na dvě základní skupiny – kvantitativní nebo kvalitativní. Toto dělení je provedeno na základě vyjádření hodnot, se kterými se v analýze rizik pracuje. V praxi se používá jedna nebo druhá metoda, či jejich kombinace.

1. **Kvalitativní metody** – vyjadřují riziko v určitém rozsahu (např. bodování <1,10>), nebo určité pravděpodobnosti (např. <0,1>) nebo slovně (např. <malé, střední, velké). Jsou rychlejší a jednodušší, ale i více subjektivní. Obvykle přináší problémy při posuzování finančních nákladů na eliminaci hrozby, kde částka vyčíslená pro tuto eliminaci se těžko porovnává s hodnocením hrozby jako je např. „velká až kritická“.

   Jednou z nejpoužívanějších kvalitativních metod je metoda účelových interview (zvaná také Delphi), která je založena na řízeném kontaktu experty hodnotící

skupiny a vybranými jedinci zastupujícími daný objekt. Metoda je postavena na řízeném pokládání otázek, které mají dvě části. Pevnou, předem připravenou, a variabilní, která se mění dle průběhu pohovoru. Pohovory jsou vedeny vždy odděleně s každým reprezentantem objektu, aby se vyloučilo jejich ovlivňování. V rámci této metody se používají různé subvarianty jako např. metoda scénářů, metoda matic atd.

2. **Kvantitativní metody** – riziko je vypočítáno na základě matematického výpočtu založeném na frekvenci výskytu hrozby a jejího dopadu. Dopad je často vyjádřen finančními jednotkami např. miliony Kč, riziko v roční předpokládané ztrátě. Na rozdíl od kvalitativních metod jsou metody kvantitativní více exaktní. Jejich provedení vyžaduje daleko větší časovou náročnost.

   Mezi nejznámější kvantitativní metodu patří metodika CRAMM (CCTA Risk Analysis and Management Methodology). Využívá se hlavně v případech kdy je vyžadováno, aby analýza rizik byla provedena v souladu s normou ČSN ISO/IEC 13335 a mezinárodním standardem ISO/IEC 17799. Analýza za použití CRAMM řeší ohodnocení systémových aktiv, jejich seskupení do logických skupin a stanovení hrozeb pro tyto skupiny, určení zranitelnosti systému a stanovení požadavků na bezpečnosti jednotlivých skupin, díky čemuž pak mohou být navržena adekvátní bezpečnostní opatření. Důležité je také zmínit, že CRAMM se zabývá vždy jen modelem systému místo systému samotného. Celá tato metodika je silně závislá na výsledcích strukturovaných interview s odborníky zadavatele. [24]

2.5 Bezpečnostní postupy a opatření

Na základě provedené analýzy rizik musíme určit, která rizika jsme schopni akceptovat a adekvátním způsobem minimalizovat či plně odstranit jejich dopad s použitím havarijních plánů a plánů obnovy.

Havarijní plán IS se uplatní v případě, že IS čelí krizové situaci. Příkladem může být například selhání prostředí (výpadek proudu, nefunkčnost klimatizace, porucha diskového pole, atd.), přírodní katastrofa (záplava, vichřice, atd.) nebo například i napadení systému virem či hackerem. Havarijní plán při řešení krizové situace jednoznačně přiřazuje role a odpovědnosti zodpovědným osobám, popisuje postupy, tak, aby minimalizoval prvotní i druhotné následky havárie.

Plán obnovy se zabývá zajištěním minimalizace úsilí a zdrojů při obnovení provozu do původního stavu. Tímto snižuje dopad havárie na chod podniku.

Funkčnost obou plánů by před uvedením do produkce měla být otestována a nadále pravidelně ověřována. Příkladem z praxe, kdy vhodně zvolená obrana nepomohla díky netestování, může být nenastartování naftových agregátů po výpadku proudu, protože dlouhou dobu stály a nafta ucpala filtr.

2.6 Bezpečnostní politika informačního systému

Bezpečnostní politika informačního systému (BPIS) je dokument, jenž obsahuje následující tři oblasti:

- definice hlavního cíle při ochraně informací,
- stanovení způsobu, jakým bude bezpečnost řešena,
- rozdělení pravomoci a zodpovědnosti.

Jedná se tedy o soubor norem, požadavků a pravidel, které formulují přístup daného podniku k zajištění integrity, dostupnosti informací a důvěrnosti. Jakožto dokument je zásadní pro deklaraci bezpečnostní politiky podniku, a proto je třeba, aby jeho schválení provedl management firmy.

Jelikož tento dokument definuje všechny budoucí aktivity společnosti v oblasti informační bezpečnosti je na něj kladen požadavek úplnosti politiky. Úplnost politiky však ještě nedefinuje žádnou úroveň detailu nově vytvořené politiky. Existují BPIS s délkou pár stran, kde BPIS obsahuje pouze základní definice pojmů, odpovědností a pravomocí. Existují ale také BPIS, které svojí délkou přesahují 100 stran. V nich už jsou problémy řešené do úrovně detailů, obvykle řešených - ve standardech.

Pokud je zpracována a schválena BPIS (byly definovány konkrétní a měřitelné cíle v bezpečnosti organizace) a existuje analýza rizik (vím, co chráním a proč), může být vytvořen bezpečnostní projekt. Tento projekt stanovuje konkrétní bezpečnostní opatření k omezení pravděpodobnosti uplatnění hrozeb, plán jejich implementace a zdroje, které si tato opatření vyžádají. [3]

3 HROZBY PRO INFORMAČNÍ SYSTÉM

V této kapitole budou představeny hrozby, které nejčastěji ovlivňují chod informačních systémů.

3.1 Škodlivý software

Ve spojitosti se škodlivým softwarem se většině uživatelů počítače vybaví virus. Virus jako takový je program, jenž dokáže šířit sám sebe bez vědomí uživatele v počítači. Při tomto šíření vkládá sám sebe do dalších spustitelných souborů či dokumentů. Následky působení viru mohou vyústit až ve ztrátu či poškození dat.

V dnešní době se již virus jako takový často nevyskytuje. Spíše narazíme na jeden z následujících druhů škodlivého softwaru:

- **Trojský kůň** – Jedná se o program, jenž obsahuje skrytou část funkcí, se kterou uživatel nesouhlasí. Příkladem může být spořič obrazovky, který ale také při svém spuštění otevře všechny komunikační porty počítače pro snadnější přístup hackerů.
- **Adware** – Hlavním cílem adwaru je šíření reklamy. Podle úrovně jeho agresivity se na napadeném počítači mohou objevovat různé reklamní poutače, vyskakovací okna nebo se stále mění domovská stránka prohlížečů.
- **Backdoor** – Program v počítači otvírá tzv. zadní vrátka, která mají útočníkovi usnadnit přístup do počítače. Často si nechávají zadní vrátka otevřená administrátoři systému sami, aniž by si uvědomili, že tím snižují bezpečnost svého systému.
- **Červ/Worm** – Samovolně se sítí šířící škodlivý kód. Jeho šíření je většinou velice rychlé. Příkladem může být nevyžádaná pošta. Po otevření nevyžádané pošty a napadení počítače červem, začne červ okamžitě odesílat spam z nově napadeného počítače.
- **Spyware** – Cílem Spywaru je odesílání získaných informací o uživatelích napadeného počítače. Odesílaná data mohou být například navštívené internetové stránky, v horších případech ale i hesla do internetového bankovnictví a podobně. [7]

3.2 Útoky z venčí

V souvislosti s útoky na počítačové systémy si jistě každý vybaví pojem hacker. Hackeři jsou počítačoví specialisté, kteří dokonale znají fungování počítače a jeho softwarového vybavení. Vše si dokáží upravit podle svých potřeb. Pojem hacker ale nemá moc co doči-

nění s pronikáním do cizích počítačů. Správné označení pro narušitele útočícího zvenčí na počítače je cracker.

Nejčastějšími útoky těchto kybernetických útočníků jsou:

- **Útok hrubou silou (Brutal Force Attack)** – Jedná se o útok s využitím velkého výpočetního výkonu, kdy se útočník snaží uhádnout heslo zkoušením všech možných kombinací. Patří sem i slovníkový útok.
- **Sociální inženýrství (Social Engineering)** – Při využití sociálního inženýrství se útočník vydává za někoho/něco jiného. Snaží se s využitím vykonstruované situace zjistit přihlašovací data nebo informace, jenž mu pomohou k přihlášení.
- **Útoky na hardware** – Útočník zde uplatňuje svoje technické znalosti. Díky nim například s použitím keyloggeru může odchytávat znaky, které uživatel stiskl na klávesnici, odposlouchávat datový tok na síti a mnohé další.
- **Útoky na software** – Jedná se o nejpoužívanější útoky poslední doby. Zneužívají se při nich nedokonalosti aplikací. Jedním z nejznámějších a jednoduše proveditelných útoků v této kategorii je DoS útok, neboli odepření služby. Jeho cílem je zahltit danou aplikaci tak, že nebude stíhat odpovídat na nové požadavky. Příkladem může být mailbombing[2]. [12]

3.3 Útoky z vnitřku

Nejčastějšími útočníky z vnitřku systému bývají sami zaměstnanci. Jejich „útok“ na systém může být způsoben omylem, ať již smazáním důležitých dat nebo například neúmyslným poškozením svého počítače. Útoky zaměstnanců ale mohou být i úmyslné s daleko rozsáhlejšími následky. Zaměstnanec může být podplacen, aby vynesl z podniku důvěrné informace nebo zhrzený zaměstnanec, jenž například dostal výpověď, může chtít úmyslně poškodit informační systém ze msty. Vnitřním útočníkem mohou být ale i zaměstnanci jiných firem, kteří mají oprávnění vstupovat do areálu a nebo tam dočasně pracují na nějaké zakázce.

Často si na vlastní systém útočí i IT administrátoři sami. Z jejich lenosti či neznalosti podcení bezpečnostní nastavení systému nebo si nechají „zadní vrátka“ pro svůj pří-

[2] Mailbombing je útok při němž je zasíláno velké množství emailů na jednu adresu. Cílem je zahltit kapacitu schránky nebo přetížit mailový server.

stup. Tím ale značně sníží bezpečnost celého systému a tím i ulehčí práci útočníkům zvenčí.

3.4 Přírodní katastrofy

Mezi přírodní katastrofy se řadí zemětřesení, sněhová kalamita, povodeň, požár půdy, sesuv půdy, ale třeba i tsunami, výbuch sopky, atd. I když je člověk schopen na základě geografické polohy některé z přírodních katastrof vyloučit či eliminovat jejich dopad, největší jejich hrozbou je nepředvídatelnost jejich výskytu. Proto jako nejúčinnější obrana proti přírodním katastrofám se jeví prevence již od počátku návrhu IS. To znamená neprojektovat budovy v oblastech působnosti těchto jevů, instalace vhodných hlásičů, které včas upozorní na hrozící nebezpečí, atd.

4 FYZICKÁ BEZPEČNOST

Fyzická bezpečnost bývá často podceňována. Pozornost bývá soustředěna na zabezpečení přístupu do systému heslem, ochranu proti virům a podobně. Přitom bezpečnost informačního systému je soubor všech opatření a jeho nejslabší prvek určuje míru zabezpečení celého tohoto systému.

Fyzická bezpečnost řeší zabezpečení prostor podniku tak, aby v něm nedocházelo k neautorizovaným přístupům, manipulaci s vybavením a následně jeho neoprávněným užíváním či dokonce poškození. Potřebnou ochranu proti těmto hrozbám nám poskytnou vhodně zvolené prvky fyzické bezpečnosti.

4.1 Fyzický přístup

Fyzický přístup do kritických prostor podniku by měl být regulován stejně jako například pravidla firewallu. Tedy na začátku zakázat přístup všem. V momentě, kdy se ukáže, že někdo z určitého důvodu přístup potřebuje, mu jej přidělit a definovat jeho úroveň.

Zapomínat by se v žádném případě nemělo ani na odbornost osob, které vstupují do kritických prostor. Je nezbytné je řádně proškolit nebo zajistit, aby je při vstupu do těchto prostor doprovázela osoba odborně poučená o pravidlech v daných prostorech stanovených.

Do prostor s omezeným přístupem patří:

- prostory s uloženými síťovými prvky (routery, switche, patch panely),
- serverové místnosti,
- úložiště dat (kartotéky, místnost s diskovým polem),
- rozvodny elektrické energie,
- kanceláře IT administrátorů.

Cílem těchto opatření je předcházení mimořádným událostem způsobených neodbornou manipulací s prvky IS, jejich poškození či zcizení.

Do fyzické bezpečnosti můžeme zařadit i fyzickou bezpečnost počítačové sítě, kdy volně dostupné ethernetové zásuvky, či nezabezpečená Wi-Fi síť může být zneužita pro neoprávněný přístup do chráněné sítě.

Je také vhodné se zaměřit také na dislokaci a redundanci všech kritických prvků IS.

Vyřešeno by dále mělo být nakládaní s vyřazenými či poškozenými paměťovými médii. Před opuštěním kritických prostor by měla být zajištěna jejich kompletní nečitelnost. Ta se dá zajistit několika způsoby. Jedním z jednoduchých a velice účinných nástrojů, které se dají použít i přímo v serverové místnosti, je zařízení pro manuální destrukci elektronických zařízení. [6]

Obrázek 3 - Zařízení pro manuální destrukci disků a drobné elektroniky [19]

5 DATOVÁ BEZPEČNOST

Základní funkcí datové bezpečnosti je zaručení důvěryhodnosti, dostupnosti a integrity dat v IS. Jinak řečeno, hlavním cílem datové bezpečnosti je co nejvyšší dostupnost nepozměněných informací oprávněným osobám. K zajištění těchto podmínek se využívají následující technologie.

5.1 Fyzické a virtuální sítě

Z bezpečnostního pohledu přístupu k počítačové síti je vždy lepší, aby uživatelská zařízení měla přístup pouze k zařízením, jejichž služby jsou nezbytně nutné pro jejich bezproblémové fungování. Omezení tohoto přístupu lze provést dvěma způsoby.

Prvním způsobem je zapojení síťových prvků do oddělených síťových směrovačů a přepínačů. Toto segmentování je označováno jako fyzické. V dnešní době se již spíše nepoužívá pro jeho složitou obslužnost a škálovatelnost.

Druhým, více používaným řešením, je segmentace logická (virtuální). Existuje více způsobů jak jí docílit. Prvním způsobem je použití přemostění na úrovni přepínačů, kdy se definují tzv. skupiny přemostění. Tedy skupiny portů jenž na přepínači vytvoří logické sítě a zařízení je schopné komunikovat pouze se zařízeními ve stejné logické skupině. Nevýhodou tohoto způsobu je možnost konfigurace logických sítí pouze v rámci jednoho přepínače. Tato nevýhoda byla odstraněna s příchodem virtuálních sítí (VLAN), které umožňují při použití vhodných směrovačů či L3 přepínačů posílat pakety i mezi virtuálními sítěmi. Toto přeposílání je možné díky implementaci standardu IEEE 802.1Q, který ke klasickému ethernetovému paketu přidá čtyř bajtovou informaci, která je pak schopná identifikovat cílový přepínač. Díky této funkci se také mohou uživatelé v sítích pohybovat mezi přepínači, aniž by ztratili připojení.

Implementací segmentace sítí můžeme značně omezit vytížení sítě, protože data pro komunikaci místo celé sítě budou využívat jen svůj vlastní segment a navíc elegantně zvýšit i bezpečnost celé sítě (zařízení z účtárny se nebude schopné připojit na zařízení na osobním oddělení). [4]

5.2 Vysoce dostupný cluster

Vysoce dostupný cluster (High-availability cluster) je skupina serverů, routerů nebo jiných zařízení, která je propojena pomocí speciálního softwaru. Tento software má za úkol sle-

dovat dostupnost zařízení ve skupině a v případě nedostupnosti některého z nich následně přenést aplikaci na něm běžící na jiné zařízení ze skupiny. Proces je nazýván failover. Tímto procesem se minimalizuje čas, kdy je daná aplikace nedostupná. Po návratu nedostupného zařízení zpět do provozu má specializovaný HA software za úkol přenést aplikaci zpět na původní server. Tento proces je znám také jako failback.

Nejčastěji je vysoká dostupnost použita u kritických databází, souborových serverů nebo síťových zařízení. [8]

5.3 Firewall

Firewall je specializované zařízení umístěné mezi důvěryhodnými (interní síť podniku) a nedůvěryhodnými (Internet) sítěmi. Jeho hlavní funkcí je kontrolovat veškerá data, která se mezi těmito sítěmi pohybují a v případě, že určitý datový tok neodpovídá nastaveným pravidlům jej musí přerušit/zakázat.

Firewally můžeme rozlišit podle stylu, jakým fungují a jsou definována jejich pravidla. Rozlišujeme je na paketové filtry, aplikační brány a stavové paketové filtry.

U paketových filtrů jsou pravidla tvořena pomocí dvojic, které vždy definují zdrojovou adresu, port a cílovou adresu, port. Výhody této konfigurace spočívají v rychlosti, filtrování dat, transparentnosti pro uživatele a v ceně zařízení. Nevýhodou je pak přímé spojení mezi důvěryhodnými a nedůvěryhodnými sítěmi a špatná udržovatelnost, kdy pro některé protokoly je potřeba otevřít velký rozsah portů.

Aplikační brány (proxy servery) oproti paketovým filtrům zcela oddělí důvěryhodné sítě od nedůvěryhodných. Pro komunikaci mezi těmito sítěmi je potřeba dvou spojení. Iniciátor spojení kontaktuje aplikační bránu se svým požadavkem, ta jej vyhodnotí. V případě schválení sama aplikační brána kontaktuje cílový server a v ustanoveném spojení pak nadále funguje jako prostředník předávající nezměněná data. Kontrola dat se provádí na sedmé vrstvě síťového OSI modelu, proto aplikační brána. Mezi výhody zde patří značná úroveň zabezpečení, která je ovšem vykoupena vysokou náročností na použití hardware.

Stavové paketové filtry vylepšují funkcionalitu paketových filtrů. Kontrolu provádějí naprosto stejně, ale pro každé spojení si uloží i jeho stav (povoleno/zakázáno). Navíc není pro spojení nutné uvádět jeho směr. Druhý směr je firewallem doplněn automaticky podle rozhodnutí pro směr předchozí. Velkou výhodou je také možnost nastavení pravidla pro všechny porty známého protokolu (FTP, SSH, ad.). Posledním vylepšením stavových

paketových filtrů byla implementace kontroly protokolů a systému pro detekci útoků (IDS). Firewall je tak schopný rozeznat, jestli se někdo nesnaží po portu určeném pro komunikaci WWW serveru přenášet například data P2P aplikace (ICQ, Skype, ad.). Výhody tohoto typu firewallů jsou vysoká úroveň zabezpečení při relativně vysoké rychlosti kontroly a snadné konfiguraci pravidel. Nevýhodou je rozsah kódu, které musí tyto firewally implementovat. Značně se tak zvyšuje možnost výskytu chyby, která může být zneužita útočníkem. [4]

5.4 Vícenásobné diskové pole nezávislých disků

Vícenásobné diskové pole nezávislých disků (RAID) je metoda používaná pro zabezpečení dat v případě výpadku pevného disku. Zabezpečení je provedeno specifickým ukládáním dat na více nezávislých disků, kdy data zůstávají dostupná i při výpadku některého z nich. Úroveň zabezpečení je dána typem použitého RAID, kdy se od sebe jednotlivé typy liší počtem disků, jenž mohou selhat před úplnou ztrátou dat. Mezi nejpoužívanější typy RAID konfigurace dnes patří RAID 1, RAID 5, RAID 6 a RAID 10.

RAID 1 je nazýván také zrcadlení. Jedná se o nejjednodušší ochranu dat, která je přitom ale značně efektivní. V této konfiguraci jsou data současně zapisována, zrcadlena, na dva disky zároveň. V případě výpadku jednoho z disků jsou data okamžitě dostupná z disku druhého. RAID 1 tedy chrání diskové pole před výpadkem jednoho z disků. Výhodou zde může být i zrychlení při čtení dat, kdy data mohou být čtena z obou disků naráz. Nevýhodou je poloviční kapacita dostupného místa, protože data se na diskovém poli nachází dvakrát.

Oproti RAID 1 RAID 5 potřebuje pro svou implementaci minimálně tři disky. Paritní informace zabírají místo jednoho disku, jsou ale střídavě rozděleny přes všechny disky v RAID 5 konfiguraci. Předchází se tak nadměrnému vytížení jednoho z disků. Díky rozdělení dat přes všechny disky je opět výhodou tohoto RAID rychlejší čtení. Nutnost složitějšího výpočtu paritní informace pak naopak snižuje rychlost zápisu. RAID 5 chrání diskové pole opět proti výpadku jednoho z disků.

RAID 6 funguje v podstatě úplně stejně jako RAID 5. Rozšiřuje jej ale o přidání jednoho paritního disku, čímž rozšiřuje počet možných vypadnutých disků na dva. Pro implementaci RAID 6 jsou nutné minimálně čtyři disky. Rychlost čtení je srovnatelná

s RAID 5, zápis je díky nutnosti výpočtu dvou paritních informací ještě pomalejší, než u RAID 5.

Kombinací RAID0[3] a RAID1 dostáváme RAID10. Jeho velkou výhodou je rozložení zátěže při zápisu i čtení dat a v případě nutnosti obnovy dat i jejich rychlá obnova. Nevýhodou je využití pouze poloviního dostupného prostoru.

Je nutné si uvědomit, že žádná z RAID konfigurací nenahrazuje zálohování dat. RAID chrání systém pouze proti hardwarové poruše disků, nikoli proti ztrátě, pozměnění či poškození dat. [4]

5.5 Zdroj nepřerušovaného napájení

Zdroj nepřerušovaného napájení (UPS) chrání servery, pracovní stanice a další zařízení proti nečekanému výpadku napájení. Neočekávané přerušení elektrické energie může způsobit nesprávnou funkci serveru. Jeho nastavení může být pak porušeno, v extrémním případě může dojít i ke ztrátě dat. UPS je zařízení, jenž se zapojuje mezi zásuvku a zdroj napájení zařízení. Jeho hlavní funkcí je v případě výpadku proudu přepnout napájení z klasické sítě na baterie v něm obsažené a umožnit tak bezpečné vypnutí všech zařízení na něm připojených. [4]

5.6 Detekce síťového narušení / Systém prevence průniku

Systém detekce narušení (IDS) je technika, která dokáže odhalovat neoprávněné, nesprávné, nebo nezvyklé aktivity v počítačové síti. Nejčastěji jsou tyto systémy implementované jako sensory, které neustále monitorují veškerý provoz na síti a porovnávají ho s databází dosud známých sítových útoků (network based IDS). Další možností je implementování IDS přímo na sledovaném hostovy (host based IDS), kde systém detekuje přímo napadení. Systém se nezaměřuje jen na dosud známé vzorce útoků, ale i na jejich přípravu. Dokáže totiž detekovat i kontrolní úkony, které útočník provádí před zahájením útoku samotného („pre-attack probes“). V případě detekce napadení systému se IDS dokáže některým útokům sám bránit, informovat o něm správce sítě či jiné definované osoby a v reálném čase

[3] RAID 0 není považován za plnohodnotný RAID. Nechrání totiž diskové pole před výpadkem žádného disku. Pouze zlepšuje rychlost čtení a zápisu.

upravit i konfiguraci firewallu tak, aby útok ukončil, případně co nejvíce zkomplikoval. [25]

Systém prevence průniku (IPS) je v podstatě rozšířením IDS. Jeho výhodou je možnost monitorování i aktivit operačního systému. Hlavním cílem IPS je identifikovat škodlivé činnosti, zaznamenat jejich průběh a následně je zablokovat. [14]

Oba výše zmíněné mechanismy bývají velmi často již implementovány jako součást funkcí firewallu. [14]

5.7 Data loss prevention

Data loss prevention DLP je strategie pro zajištění toho, aby koncoví uživatelé nesdíleli citlivé dokumenty nebo informace mimo podnikovou síť. Tento termín je ale také spojován se softwarem, který umožňuje kontrolu a nastavení omezení pro nakládání s daty. V rámci systému si můžeme nadefinovat pravidla pro kritická data (např. tento soubor je tajný) a k nim definovat i různá omezení (např. pouze tito uživatelé mohou soubor tisknout, tento uživatel jej může předat dál, atd.). Při pokusu o jejich porušení pak DLP zamezí jeho provedení a vše nahlásí správci systému či předdefinovaným osobám. [9]

5.8 Virtuální privátní síť

Virtuální privátní síť (VPN) je šifrované spojení mezi dvěma důvěryhodnými sítěmi, které musí při komunikaci mezi sebou přenášet data přes síť nedůvěryhodnou, většinou Internet.

VPN je často považována za nástroj zvyšující bezpečnost sítí. Je nutné si ale uvědomit, že VPN vytváří pouze bezpečné spojení mezi dvěma sítěmi a úroveň zabezpečení daných sítí se s jeho použitím nijak nemění. [5]

Připojení funguje tak, že klient za pomoci speciálních protokolů, které jsou založené na protokolu TCP/IP a označovány jako protokoly tunelových propojení virtuálně volá virtuální port na serveru VPN. Propojení mezi dvěma body je vytvořeno díky emulaci (neboli zapouzdření) dat do hlavičky TCP/IP paketů. Tato hlavička pak obsahuje směrovací informace, které umožní paketu průchod přes sdílené nebo veřejné sítě až ke svému cílovému bodu. Privátní spojení je vždy šifrováno. To znamená, že i kdyby někdo odchytával pakety na síti, bez znalosti šifrovacích klíčů, si je stejně nebude moc přečíst. Propojení, kde jsou privátní data zapouzdřena a šifrována je nazýváno VPN. [26]

Výše popsané vlastnosti splňují VPN vytvořené za využití protokolů PPTP, L2TP, L2TPsec a SSTP[4]. [26]

5.9 Autentizace a autorizace

Autentizace slouží k jednoznačnému určení uživatele, který přistupuje k systému. Cílem je jednoznačně identifikovat osobu, jež do systému přistupuje s existujícím uživatelem v něm. Ve správně nastaveném systému by pak odpovědné osoby měli být schopny ověřit, kdy se daný uživatel přihlásit a odhlásil, případně, co vše v systému dělal. [11]

Autentizační metody jsou založené na něčem co daný uživatel zná, nebo má nebo je. Typickým příkladem toho „co uživatel zná“ je PIN kód, heslo či například správné pořadí bodů na obrazovce. Zástupci kategorie druhé, „co uživatel má“, jsou fyzické objekty, jako je platební karta nebo token. V poslední kategorii jsou to přímo fyzické charakteristiky samotného jedince, které umožní jeho ověření – otisk prstu, dlaně a podobné. Obecně nazývané jako biometriky.

Mezi výhody „něčeho co uživatel zná“ je, že se nejedná o objekt, který musí uživatel mít neustále u sebe. Jeho znalost je abstraktní veličina, kterou lze snadno přenášet, zadávat do počítače. Hlavní nevýhodou je její snadné zjištění, někdy dokonce i bez vědomí uživatele. Lidská paměť ani není stavěna na zapamatování si náhodných dlouhých složitých hesel, což také negativně ovlivňuje celou bezpečnost této autentizační metody.

Naopak „něco, co uživatel má“ je fyzický objekt – token. Mezi hlavní výhody patří, že token je jen obtížně kopírovatelný, snadno zjistíme, že jsme jej ztratili a na rozdíl od lidského mozku je token schopný zpracovávat dlouhé řetězce náhodných znaků s velkou entropií (míra informace). Nevýhody spočívají ve vzájemné nekompatibilitě různých typů tokenů a jejich složité konstrukci. Pro jejich čtení je většinou potřeba vlastnit speciální čtecí zařízení. V případě, že uživatel token zapomene, nemůže být ověřena jeho identita. To samé nastane při poruše tokenu.

V poslední kategorii uživatel nemusí nic znát, ani vlastnit. „Něco co uživatel je“ jsou informace zjistitelné z fyziologických vlastností těla uživatele – biometriky. Příkla-

[4] Více o způsobu využití protokolů tunelového propojení můžete najít na https://technet.microsoft.com/cs-cz/library/cc771298(v=ws.10).aspx

dem může být například dynamika jeho podpisu. Nespornou výhodou těchto autentizačních metod je, že biometriky nelze zapomenout či ztratit. Největší nevýhodou je obtížnost měřit dané biometriky (pro určité typy biometrik). A právě přesnost těchto měření často značně snižuje bezpečnost biometrických systémů.

V současné praxi se k eliminaci nevýhod pro výše zmíněné autentizační metody používají při ověření uživatelů kombinace těchto metod. Nejrozšířenějším případem z dnešní doby může být mobilní telefon, kdy při jeho aktivaci je potřeba vložit SIM kartu (token) a zadat PIN kód (heslo). Použití dvou autentizačních metod najednou se nazývá dvoufaktorová autentizace. Pokud bychom přidali i metodu třetí (biometriky) bude se jednat o autentizaci třífaktorovou.

Po úspěšné autentizaci uživatele je nutné provést jeho autorizaci. Tedy proces, kdy jsou ověřována oprávnění, která jsou uživateli přidělena (přístup do systému, provádění modifikací, vytváření nových uživatelů, ad.). [11]

5.10 Antivir a antispam

Antivir je specializovaný software, jenž chrání počítač před nákazou viry a jiným škodlivým softwarem. Jeho hlavní součástí je virová databáze. Vůči ní antivir porovnává data při odhalování nákazy. V dnešní době vznikají virové mutace tak rychle, že se může stát, že výrobce antiviru vydá aktualizaci virové databáze i několikrát týdně. Proto pro správnou funkci antiviru je potřeba mít i správně nastavené aktualizace tohoto softwaru. [10]

Antispam je inteligentní software, jenž se snaží rozeznávat spam a přesouvat jej do určené složky v elektronických poštovních schránkách. Spam je nevyžádaná pošta, která je většinou rozesílána pomocí robotů. Často bývá ke spamu přidán i skrytý škodlivý kód. Antispam stejně jako antivir pro svoji funkci využívá rozsáhlou databázi s informacemi o spamu. Proto i zde jsou nutné pravidelné informace. [13]

5.11 Zálohování a archivace

Zálohováni je proces, při němž je vytvářena kopie zdrojových dat (záloha). Tato kopie by měla být uložena na jiném místě než se nacházejí produkční data. Systém a struktura zálohování by měly být nastaveny tak, aby v případě potřeby byla data obnovena co možná nejblíže jejich stavu před havárií. Důraz je kladen také na rychlost obnovy. Aby byly spl-

něny tyto podmínky, zálohy se v současné době nejčastěji ukládají na diskové pole, která jsou mnohem rychlejší než páskové mechaniky.

Cílem archivace je zachování již nepotřebných dat, kdy je kladen důraz na jejich dlouholetou dostupnost. Rychlost obnovy zde již není tak důležitá. Data proto mohou být uložena například na datové pásky, které jsou značně levnější než disky.

5.12 Aktualizace

Aktualizace neboli záplata je novější verze již používaného softwarového vybavení. Jejím cílem je zvýšit bezpečnost, opravit nalezené chyby nebo poskytnout novou funkcionalitu. Z pohledu bezpečnosti je implementace aktualizací jednou z nutností, jak udržet systém bezpečný. Při aplikaci aktualizací je potřeba si dát pozor na jejich kompatibilitu s již používaným softwarem.

5.13 Šifrování dat

Převádění dat z podoby otevřeného textu do podoby, kdy jsou data čitelná pouze na základě určité speciální znalosti se nazývá šifrování dat. A jako takové tvoří významný prvek v bezpečnosti informačních systémů. Hlavním důvodem pro použití šifrování je ochránit důvěrné a osobní informace před nepovolanými osobami. Šifrování je také vhodné jako metoda pro omezení přístupu administrátorů systému k citlivým informacím. [25]

Opakem pro šifrování je dešifrování. Tedy proces, při kterém se šifrovaná data dekódují zpět do originální podoby.

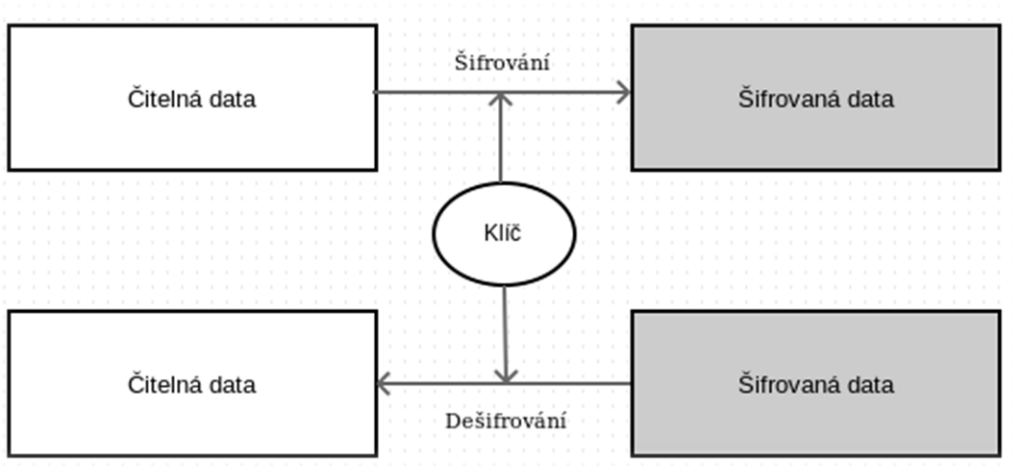
Oba výše popsané postupy pro svou správnou funkci potřebují nějakou tajnou informaci. Obvykle je to klíč a použitá metoda. Klíč si můžeme představit jako klasické heslo, které používáme dennodenně pro přístup např. k internetovému bankovnictví. V dnešní době jsou už i velmi rozšířené klíče biometrické (otisk prstu či dlaně, dynamika podpisu a mnohé další). [25]

V současné době se pro šifrování dat používají dva typy kryptografických algoritmů – symetrické a asymetrické šifry.

1. **Symetrické šifry** – pro šifrování a dešifrování používají jeden a ten samý klíč. Algoritmy založené na symetrickém šifrování jsou velmi rychlé díky jejich malé výpočetní náročnosti. Podle způsobu práce s daty je dělíme na proudové a blokové. Proudové šifry kódují bit po bitu, zatímco blokové zakódují najednou celý blok dat.

Často se symetrické šifry používají pro kódování velkého množství dat. Příkladem mohou být databázové soubory. [25]

Mezi zástupce symetrických šifer patří algoritmy jako DES, 3DES, IDEA, AES, Blowfish a CAST. Asi nejznámější je z nich AES, který se díky své oblibě již implementuje i přímo jako součást HW. [25]



Obrázek 4 - Symetrické šifrování [Zdroj: Vlastní]

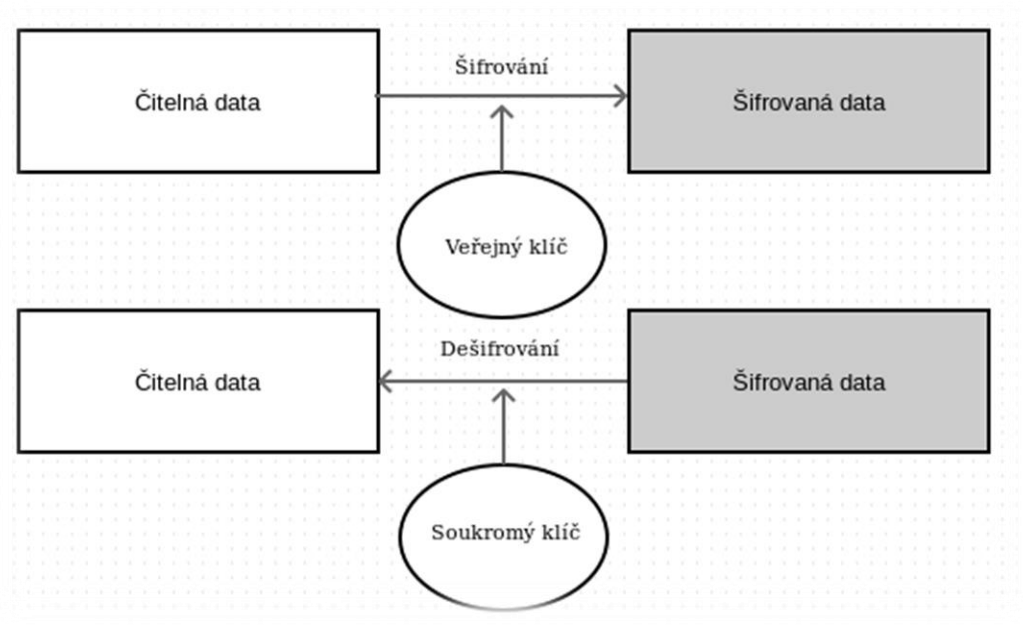
2. **Asymetrické šifry** – hlavním rozdílem oproti symetrickým šifrám je nahrazení šifrovacího klíče tzv. šifrovacím párem. Šifrovací pár se skládá ze dvou klíčů. První je označován jako „veřejný klíč“ druhý jako „soukromý klíč“. Klíče jsou mezi sebou neodvoditelné, takže znalostí jednoho nejsme schopni si odvodit ten druhý. Veřejným klíčem se data šifrují, soukromým pak dešifrují. Aby byla zaručena vysoká bezpečnost asymetrického šifrování je nezbytné, aby soukromý klíč vlastnila pouze jedna osoba a řádně si jej střežila. [25]

   Nejznámějšími zástupci asymetrických šifer jsou algoritmus RSA. Asymetrické šifry se používají hlavně pro šifrování malých datových souborů jako jsou např. certifikáty, šifrovací klíče symetrických šifer a další. [25]

   Pro zaručení bezpečnosti při asymetrickém šifrování je důležité dodržet následující pravidla: [25]

   - Použít dostatečně dlouhé klíče. Doporučené jsou klíče s minimální délkou 128b, lépe však rovnou použít 256b.

- Konstruovat algoritmy, které umožňují s využitím matematických principů útoky pouze s použitím hrubé síly.



Obrázek 5 - Asymetrické šifrování [Zdroj: Vlastní]

6 PERSONÁLNÍ BEZPEČNOST

Životní cyklus pracovníka rozděluje bezpečnostní opatření v oblasti lidských zdrojů na tři hlavní etapy.

Opatření jež jsou činěna před vznikem pracovního poměru, mají za úkol ověřit, že informace poskytnuté osobou, která se uchází o pracovní poměr v podniku jsou pravdivé. Dále je vhodné prověřit si pracovní historii a reference o této osobě. Vše ovšem v rámci zákonných možností. Poslední fází přijímání nového pracovníka by mělo být stanovení přesných podmínek a zodpovědností, jenž se vztahují k pozici, na kterou je nový zaměstnanec přijímán.

Přijetí nového zaměstnance je druhá bezpečnostní fáze. V ní je potřeba dbát na to, aby vedoucí pracovníci vhodně seznamovali své podřízené s bezpečnostními pravidly a motivovali své podřízené k jejich dodržování. Bezpečnostní povědomí zaměstnanců by mělo být rozšiřováno také výběrem vhodných školení, seminářů, tréninků a jiných vzdělávacích aktivit. Nutné je určit také pravidla disciplinárních řízení, která zaměstnancům hrozí při porušování pravidel. Při drobném porušení může stačit domluva, při vážnějším pokuta, změna pozice či až ukončení pracovního poměru.

Ukončením pracovního poměru (dobrovolného či nedobrovolného) začíná poslední, třetí, fáze opatření. V ní je potřeba mít jasně určený proces, který jasně definuje kroky a role osob v tomto procesu tak, aby například personální oddělení nevydalo zaměstnanci všechny nutné dokumenty, než zaměstnanec vrátí všechny zapůjčené pracovní pomůcky (laptop, nářadí, ad.). Zaměstnanec by měl být také seznámen se závazky, které platí i po ukončení poměru (mlčenlivost). Zajistit by se mělo také odstranění všech firemních materiálů ze soukromých zařízení zaměstnance. Tento krok však bývá často problematický, a proto je lepší řešení, kdy je zakázáno používání soukromých zařízení pro firemní potřeby. Posledním, avšak možná nejdůležitějším krokem je odstranění všech přístupových oprávnění zaměstnance ze systému, tak, aby již neměl přístup do žádných firemních prostor. [3]

II. PRAKTICKÁ ČÁST

7 ANALÝZA SOUČASNÉHO STAVU

Analýza současného stavu zabezpečení informačního systému bude provedena ve firmě zabývající se výrobou plastových výlisků pro automobilový průmysl. Jméno firmy nebude z bezpečnostních důvodů uvedeno.

Firma byla založena v roce 1995. Na konci roku 2014 díky dobrým hospodářským výsledkům a rostoucí poptávce po jejich službách odkoupila menší konkurenční firmu z blízkého okolí, aby byla schopná rostoucí poptávku uspokojit.

V současné době firma zaměstnává okolo 300 pracovníků. Struktura firmy je rozdělená do následujících oddělení:

- kancelář ředitele,
- obchodní oddělení,
- ekonomické oddělení,
- péče o základní prostředky,
- autodoprava,
- lisovna plastů,
- kovovýroba a montáž,
- nástrojárna, konstrukce a technologie.

Z geografického hlediska je firma rozdělena do dvou lokací. Řekněme na „hlavní“ a „vedlejší“. V hlavní lokaci najdeme administrativní budovu společně s výrobní halou, která v sobě hostí i kanceláře vedoucích pracovníků výrobních oddělení. Ve 20 km vzdálené lokaci se nachází druhá výrobní hala. Tato hala byla připojena nedávno v rámci rozšiřování výroby, jak již bylo zmíněno výše. Také v ní můžeme najít nejen výrobní stroje, ale i kanceláře vedoucích pracovníků.

7.1 Datové toky ve firmě

V první řadě si datové toky rozebereme z pohledu jednotlivých oddělení.

Hlavní komunikační kanál mezi odděleními tvoří elektronická pošta. Pokud je potřeba přenést mezi odděleními soubory větší, než dovoluje e-mail, používá se sdílený disk. Další specifické toky jsou rozebrány podrobněji níže.

Kancelář ředitele požaduje dostávat každé ráno podrobné zprávy o chodu firmy v podobě elektronické pošty. Tyto reporty jsou následovně rozebírány na denních poradách s vedoucími jednotlivých oddělení.

Obchodní oddělení se stará o zajištění objednávek materiálu nutného k provozu firmy (materiál k lisování, pracovní pomůcky, kancelářské pomůcky, atd.). Správa objednávek a jejich sledování je řešena Access databází OBCHOD, která byla vytvořena na míru podniku. Dále se obchodní oddělení zaměřuje jak na získávání nových zákazníku, tak i na vyřizování požadavků zákazníků současných. K tomuto účelu slouží databáze SQL, která je propojená s internetových obchodem a běží na webovém serveru.

Ekonomické oddělení používá stejnou Access databázi jako obchodní oddělení. Dále se také stará o personalistiku ve firmě. Všechny úkoly spojené s personalistikou ve firmě jsou řešeny pomocí systému OKbase.

Péče o základní prostředky, neboli hlavní úřad mechanika, má na starosti veškerou agendu spojenou s opravami budov, strojů a komunikací uvnitř areálu firmy. K tomuto účelu používá vlastní Access databázi SPRÁVA navrženou pro jejich potřeby.

Autodopravu ve firmě spravují pomocí softwaru AUTODOPRAVA. Autodoprava také přistupuje k některým výrobním SQL systémům uvedeným níže.

Lisovna plastů, kovovýroba, montáž, nástrojárna, konstrukce a technologie využívají mimo sdílených disků pro ukládání konstrukčních dat také výrobní databáze MES (sledování a vyhodnocování výroby), Helios (Enterprise Resource Planning (ERP) systém) a WMS (skladovací systém). Technické výkresy, dokumentace, nákresy a provozní dokumenty jsou ukládány na sdílené disky.

Nyní se podíváme na datové toky z pohledu lokací.

Jelikož ve vedlejší lokaci se nacházejí zejména výrobní stroje, největší datový tok představuje přístup k výrobním SQL systémům Helios, MES a WMS. Důležitý je ale také přístup ke správě objednávek a e-mailové komunikaci.

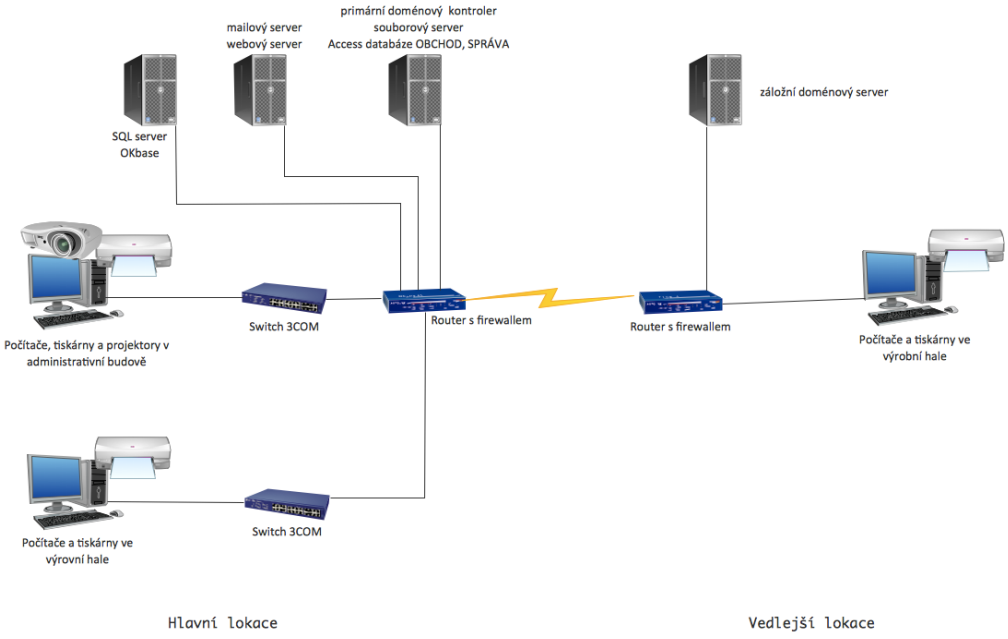
7.2 Analýza informačního systému

Informační systém firmy byl budován posledních 10 let. Zatímco pracovní stanice zaměstnanců prošly obnovou v poslední době a většina z nich běží na systému Windows 7 Professional, serverová část zůstala více méně nezměněna. Síťové prvky prošly výměnou přibližně před 7 lety.

Síť se skládá ze dvou routerů s firewallem MIKROTIK Cloud Router Switch CRS125, 24x Gbit LAN, Gbit SFP port (Tyto routery byly instalovány nedávno z důvodu

propojení obou lokací mezi sebou.) a dvěma síťovými přepínači (switchy) 3COM 4500 50-port (48x 10/100 + 2x SFP 1000). Tyto síťové prvky propojují 4 fyzické servery.

Topologie sítě je zobrazena na následujícím obrázku.



Obrázek 6 - Současný stav sítě [Zdroj: Vlastní]

První server je použitý jako primární doménový řadič s Windows Server 2003, souborový server a běží na něm také Access databáze verze 2003. Jedná se o IBM x346 2U, 1x(2) XEON 3.0GHz EM64T, 4GB RAM, 2x 146GB SCSI. Disky jsou konfigurovány v RAID 1. Záloha se provádí na externí USB disk, který je připojený na jeden z USB portů. Záloha nemá pravidelné časování a je prováděna IT administrátorem jednou týdně. V případě obsazenosti externího disku je z něj vymazána nejstarší záloha.

Druhý server hostuje mailový a webový server. Hardwarově se jedná o totožný server, jako primární doménový řadič. Záloha probíhá stejným způsobem na jiný externí disk.

SQL server a personální databáze OKbase běží na třetím serveru. Opět se jedná o IBM X server IBM x346 2U, 1x(2) XEON 3.0GHz EM64T, 4GB RAM s odlišným počtem disků (4x 146GB SCSI). Disky jsou konfigurovány opět v RAID 1. Záloha probíhá denně na externí LTO2 pásku. Páska by měla být každý den vyměněna za jinou s rotací 14 dní.

Záložní doménový řadič je jako jediný server uložen ve vedlejší lokaci. Jeho konfigurace je shodná s primárním doménovým řadičem. Běží na něm pouze Windows Server 2003. Není nijak zálohován.

Po výčtu serverů je zapotřebí také zmínit uživatelskou stanici, na které je nainstalovaná aplikace Autodoprava. Intel Celeron G1620 Ivy Bridge, RAM 4GB DDR3, Intel HD Graphics, HDD 500GB 7200 otáček byla využita z důvodu nekompatibility aplikace s operačními systémy serverů. Záloha je prováděna uživatelem stanice denně pomocí funkce aplikace na externí disk.

7.3 Identifikace aktiv firmy a jejich ohodnocení

Na základě provedených analýz datových toků a informačního systému jsme schopni určit aktiva firmy a jejich ohodnocení.

Pro hodnocení zjištěných aktiv bylo navrženo následující hodnocení, které bylo následně i na identifikovaná aktiva aplikováno.

Váha aktiva	Váha vyjádřena slovně	Hodnocení dopadu
1	Bezvýznamná	Žádný či bezvýznamný dopad
2, 3	Nízká	Malý dopad
4	Střední	Citelné potíže
5	Vysoká	Existenční problémy

Tabulka 1 - Klasifikace hodnocení aktiv [Zdroj: Vlastní]

Identifikovaná aktiva firmy jsou následující:

- servery,
- síťové prvky,
- mailová databáze,
- databáze webového serveru,
- Access databáze OBCHOD,
- Personální systém OKbase,
- Access databáze SPRÁVA,
- aplikace AUTODOPRAVA,
- výrobní SQL aplikace MES, Helios a WMS,
- obsah sdílených disků,
- datové spojení mezi lokacemi „hlavní“ a „vedlejší“.

V následující tabulce jsou identifikovaná aktiva ohodnocena. K ohodnocení váhy byla použita následující kritéria:

a. Dostupnost – pokud jsou aktiva potřebná jsou dostupná.
b. Důvěryhodnost – aktiva jsou dostupná pouze oprávněných osobám.
c. Integrita – aktivum bylo dostupné v nepozměněné podobě.
d. Váha aktiva – určuje výslednou hodnotu aktiva pro firmu.

Aktivum	**Dostup-nost**	**Důvěryhod-nost**	**Integrita**	**Váha ak-tiva**
Servery	5	5	5	5
Síťové prvky	5	4	3	4
Mailová databáze	3	4	5	4
Access databáze OBCHOD	4	3	5	4
Personální systém Okbase	4	5	5	5
Access databáze SPRÁVA	3	4	4	3
Aplikace AUTODOPRAVA	4	4	4	4
SQL aplikace MES, Helios a WMS	5	5	5	5
Obsah sdílených disků	3	4	5	4
Spojení mezi lokacemi	4	3	3	3

Tabulka 2 - Určení hodnoty/váhy aktiv pro firmu [Zdroj: Vlastní]

Tabulka číslo 3 popisuje do jaké míry nám dokáže dané aktivum ovlivnit chod firmy na základě jeho ohodnocení.

Váha aktiva	Popis hodnoty dopadu na firmu
Bezvýznamná	Dopad je bezvýznamný - zanedbatelný. Odstranění následků probíhá bez problémů. Časový horizont pro odstranění následků je krátký. Následky dopadu se neprojevují na chodu firmy.
Nízká	Dopad na firmu je akceptovatelný. Odstranění následků probíhá stále v krátkém časovém horizontu, avšak s menšími problémy. Projevuje se na vnitřních firemních jednotkách. Z venčí organizace nepozorovatelný.
Střední	Dopad na firmu je značný - nežádoucí riziko. Odstranění následků probíhá v citlivými problémy v neurčitém čase. Finančně nákladný. Projevuje se jak na vnitřní organizaci firmy, tak z venčí.
Vysoká	Dopad na firmu je katastrofální. Odstranění následků v reálném čase značně komplikované až nemožné. Nemožnost plnit závazky. Existenční potíže.

Tabulka 3 - Dopad aktiv na firmu podle hodnocení [Zdroj: Vlastní]

7.4 BEZPEČNOSTNÍ ANALÝZA

V následující kapitole si představíme identifikovaná bezpečnostní rizika.

7.4.1 Fyzická bezpečnost

Fyzická bezpečnost informačního systému této firmy není řešena šťastně. Všechny budovy jsou sice mimo záplavovou oblast, tím ale bohužel výčet kladů končí.

Nejprve si rozebereme problémy v hlavní lokaci.

Serverová místnost, dostupná přes kancelář IT administrátora, není nijak zabezpečena proti vstupu cizích osob. Klíč od kanceláře je sice dostupný pouze omezenému počtu zaměstnanců na recepci firmy, ale v případě, že IT administrátor opustí svoji kancelář během pracovní doby a nezamkne ji, stává se serverovna snadno přístupnou.

Problémem je také lokace zálohovacích zařízení ve stejné místnosti jako servery, což například v případě požáru může představovat vážný problém spojený se ztrátou veškerých dat.

Bezpečnostní hrozba spočívá také v nedostatečném počtu UPS jednotek. V současné konfiguraci jsou oba zdroje každého ze serverů napojené do jedné UPS jednotky, která v případě poruchy odpojí oba připojené zdroje.

Strukturovaná kabeláž sítě není zabezpečena proti přepětí, což v případě počítačů může mít fatální následky na elektroniku v nich.

Další bezpečnostní riziko bylo identifikováno v nezabezpečených stolních počítačích proti manipulaci s HW komponentami. Kdokoli s přístupem k PC si jej může otevřít a například ukrást pevný disk, či jinou HW součástku. Tento nedostatek značně zvyšuje potencionální úspěch vnitřního útočníka.

BIOS/UEFI počítačů není chráněn heslem proti neoprávněným změnám nastavení. Toto nastavení dovoluje například změnit bootovací pořadí zařízení a tak i nastartovat počítač z jiného disku.

Ve vedlejší lokaci trpí informační systém stejnými nedostatky. Zde je ale potřeba zdůraznit ještě větší chybu, a to v umístění serveru. Tento server je instalován společně

s routerem v jedné z kanceláři vedoucího pracovníka. Tato kancelář je volně přístupná celý den. Není klimatizovaná.

V poslední řadě je také potřeba zmínit stáří zařízení informačního systému. Jejich technologie je již značně zastaralá a nedosahuje schopností současného HW vybavení. Příkladem může být technologie TPM (Trusted Platform Module[5]). Samozřejmostí je také zvyšující se pravděpodobnost selhání součástky v zařízení s rostoucí dobou použití.

7.4.2 Datová bezpečnost

Největším problémem datové bezpečnosti je zabezpečení dat proti selhání disků, ztráty dat, jejich modifikaci či úmyslnému poškození.

RAID 1 (zrcadlení) sice chrání systém proti výpadku jednoho disku v systému, ale již nezabraňuje zkopírování chyby v datech nebo například úmyslnému poškození dat interním pracovníkem.

V případě úmyslného poškození dat by na řadu měla přijít jejich obnova ze zálohy. Obnova dat by měla být co nejrychlejší, a také by měla vrátit systém do stavu co nejbližšímu tomu původnímu před havárií systému. Bohužel systém a typ zálohování informací v této firmě nesplňuje ani jeden předpoklad zotavení po krizové situaci. Zálohování chybí pravidelnost, strukturovanost a automatizace. IS momentálně nedisponuje ani dostatečně velkou kapacitou pro uchovávání záloh.

Dalším neduhem informačního systému je chybějící redundance serverů. V případě výpadku jednoho ze serverů se doba obnovy systému bude prodlužovat o dobu potřebnou na pořízení nového hardwaru.

Ve vnitřní síti neexistuje členění na podsítě (virtuální sítě). Následkem tohoto nastavení je to, že kdokoli připojený v síti má možnost přístupu ke všem dalším zařízením v síti, tedy i například ke správě administračních rozhraní kritických prvků infrastruktury. Jelikož v síti jsou používány i sdílené disky, jsou i ty přístupné všem uživatelům sítě bez ohledu na oddělení. Naštěstí jsou tyto disky chráněny alespoň přístupovým heslem.

---

[5] Více o technologii TPM - http://windows.microsoft.com/cs-cz/windows-vista/what-is-the-trusted-platform-module-security-hardware

Aktualizace počítačů nejsou řízeny centrálně. Počítače mají aplikované odlišné verze aktualizací, což může způsobit problémy s rozdílnou kompatibilitou aplikací. U antivirových programů neřízené aktualizace mají za následek větší pravděpodobnost nákazy.

Nastavení operačního systému umožňuje připojit k počítačům externí média (pevné disky, flash paměti, paměťové karty, atd.), což v kombinaci s absencí systému DLP (data loss prevention) umožňuje v podstatě volné šíření firemních dat bez varování.

Zapojení serverů přímo do routerů také nepatří mezi šťastná řešení.

7.4.3 Personální bezpečnost

Personální bezpečnost je ve firmě nastavena správně. Personalista absolvoval kurzy psychologie pro personalisty. Pracovní historie uchazečů o místo je ověřována u minulých zaměstnavatelů. V případě ucházení se o pozici, kde je předpoklad práce s počítačem, je zaměstnanec testován na počítačovou gramotnost.

Pro současné zaměstnance byl nastaven systém odměn za výkonnost. Snaha je i pravidelné zvyšování platů zaměstnanců.

Bohužel ani výše zmíněné opatření nedokáže zabránit zaměstnanci v úmyslném poškození dat nebo jejich vynesení ven z firmy.

7.5 Identifikace a ohodnocení hrozeb

Nyní jsou již určena aktiva a je vypočítána jejich váha. Byla provedena i bezpečnostní analýza na fyzické i datové úrovni. V tuto chvíli je nutné specifikovat možné hrozby a určit pro každou z nich pravděpodobnost, s jakou může daná hrozba nastat.

Pro správné určení pravděpodobností je potřeba si nejdříve určit klasifikační schéma pro výskyt hrozeb. To je následující:

Hodnota	Pravděpodobnost
1	Nepravděpodobná
2	Malá
3	Střední
4	Vysoká
5	Kritická

Tabulka 4 - Klasifikační schéma pro výskyt hrozeb [Zdroj: Vlastní]

V následující tabulce jsou uvedeny konkrétní hrozby společně s ohodnocením pravděpodobnosti jejich výskytu:

Hrozba	Pravděpodobnost
Neoprávněný přístup	3
Nemožnost obnovy dat	4
Porucha HW	5
Krádež HW	2
Selhání komunikace	3
Napadení sítě	3
Krádež dat	4
Živelná pohroma	2
Úmyslný útok	4

Tabulka 5 - Tabulka hrozeb a jejich ohodnocení [Zdroj: Vlastní]

7.6 Výpočet míry rizik

Pro výpočet míry rizika využijeme maticovou metodu analýzy rizik. Tato metoda spočívá ve čtyřech krocích.

1. Krokem číslo jedna je vytvoření matice zranitelnosti spojením tabulek hodnocení aktiv a hodnocení hrozeb.
2. Ve druhém kroku jsou posouzené jednotlivé zranitelnosti a hodnocení je doplněno do tabulky.
3. V kroku třetím, vypočteme míru rizika pomocí vzorce R = T x A x V, kde R – míra rizika, T – pravděpodobnost vzniku hrozby, A – hodnota aktiva a V – zranitelnost aktiva.
4. V posledním, čtvrtém, kroku stanovíme hranice rizika (nízká, střední, vysoká).

V Zranitel-nost	Popis aktiva	Servery	Síťové prvky	Mailová db.	Access db. OB-CHOD	Person. ap. Okbase	Access db. SPRÁVA	Ap. AUTODO-PRAVA	SQL ap. MES, Helios a WMS	Obsah sdílených disků	Spojení mezi lokacemi
	Hodnota aktiva	5	4	4	4	5	3	4	5	4	3
Popis hrozby	Pravděpodobnost										
Neoprávněný přístup	3	4	3	3	3	4	3	3	4	3	3
Ztráta dat	5	5	5	5	5	5	5	5	5	5	5
Porucha HW	5	5	5	5	5	5	5	5	5	5	5
Krádež HW	2	4	3	3	3	4	2	3	4	3	2
Selhání ko-munikace	3	4	3	3	3	4	3	3	4	3	3
Napadení sítě	3	4	3	3	3	4	3	3	4	3	3
Krádež dat	4	5	5	5	5	5	4	5	5	5	4
Živelná po-hroma	2	4	3	3	3	4	2	3	4	3	2
Úmyslný útok	4	5	5	5	5	5	4	5	5	5	4

Tabulka 6 – Matice zranitelnosti [Zdroj: Vlastní]

R Riziko	Popis aktiva	Servery	Síťové prvky	Mailová db.	Access db. OBCHOD	Person. ap. Okbase	Access db. SPRÁVA	Ap. AUTODOPRAVA	SQL ap. MES, Helios a WMS	Obsah sdílených disků	Spojení mezi lokacemi
	Hodnota aktiva	5	4	4	4	5	3	4	5	4	3
Popis hrozby	Pravděpodobnost										
Neoprávněný přístup	3	60	48	36	36	60	36	36	60	48	27
Ztráta dat	5	125	100	100	100	125	75	100	125	100	75
Porucha HW	5	125	100	100	100	125	75	100	125	100	75
Krádež HW	2	40	24	24	24	40	12	24	40	24	12
Selhání komunikace	3	60	36	36	36	60	27	36	60	36	27
Napadení sítě	3	60	36	36	36	60	27	36	60	36	27
Krádež dat	4	100	80	80	80	100	48	80	100	80	48
Živelná pohroma	2	40	24	24	24	40	12	24	40	24	12
Úmyslný útok	4	100	80	80	80	100	48	80	100	80	48

Tabulka 7 – Matice rizik [Zdroj: Vlastní]

Míra rizika	Slovní ohodnocení	Doba pro řešení
0 - 25	Bezvýznamné riziko	Nemusí se řešit
26 - 50	Akceptovatelné riziko	3 - 5 let
51 - 75	Nízké riziko	1 - 3 roky
76-100	Nežádoucí riziko	Do 1 roku
100 a více	Nepřijatelné riziko	Ihned

Tabulka 8 – Klasifikační schéma pro vyhodnocení matice rizik [Zdroj: Vlastní]

7.6.1 Zhodnocení míry rizik

Z výše provedené analýzy rizik vyplývá, že největší riziko pro firmu plyne ze ztráty dat nebo poruchy hardwaru. Míra rizika pro obě hrozby vyšla stejně. Z dalších hrozeb nejvíce ohrožující chod firmy byly identifikovány krádež dat a úmyslný útok na aktiva firmy. Nemělo by se ale zapomenout ani na hrozby neoprávněného přístupu k aktivum, selhání komunikace či napadení sítě.

V rámci další kapitoly budou představeny možnosti pro řešení rizik či zmírnění jejich dopadu na firmu.

NÁVRH VHODNÉHO ŘEŠENÍ

V provedené analýze byly identifikovány nedostatky v současném zabezpečení informačního systému. Některé z nich byly vyhodnoceny jako závažné, jiné méně. Hlavním cílem této části práce bude navrhnout vhodná řešení pro jejich odstranění nebo alespoň zmírnění.

Výběr veškerých prvků uvedených níže probíhal ve volně dostupných internetových e-shopech. Uvedená data a informace o nich jsou aktuální ke dni 4.5.2015.

7.7 Fyzická bezpečnost

7.7.1 Fyzické zabezpečení serveroven

Analýza fyzické bezpečnosti označila zabezpečení přístupu osob do serveroven jako nedostatečné.

V hlavní lokaci by k minimální nápravě stavu stačilo opatřit vstup do serverovny zamykatelnými dveřmi. Už toto základní opatření zamezí přístupu do místnosti nechtěným osobám. Toto zabezpečení je ale spíše minimální a pořád ještě nedokonalé. V ideálním případě budou současné dveře nahrazeny dveřmi bezpečnostními, které mají zvýšenou odolnost proti násilnému vniknutí, požáru a dokáží i tlumit hluk. Při výměně dveří nesmíme zapomenout ani na výměnu zárubní ze stávajících na bezpečností. Nutností u těchto dveří by měl být certifikát, zařazující dveře do stupně zabezpečení podle normy ENV1627.

Jako doplňující opatření pro ztížení přístupu nechtěné osoby k technickému vybavení serverovny je také doporučeno použít zamykatelnou rackovou skříň. Její pořízení může být dobře obhájeno faktem, že díky ní se zamezí přímému přístupu k výpočetní technice osobám, které například do serverovny mají přístup k provádění kontroly stavu místnosti, ale již nejsou oprávněny manipulovat s hardwarem. Tato skříň může také zamezit nechtěnému vytažení kabelů ze serveru při manipulaci s ostatními předměty v serverové místnosti (oproti otevřené rackové skříni).

Obrázek 7 - Zamykatelná racková skříň [18]

Nyní se zaměříme na stejný problém v lokaci vedlejší. Díky současnému umístění serverů v kanceláři vedoucího pracovníka nám nastává více problémů s řešením.

Jedním z řešení je osazení kanceláře výše popsaným zamykatelným rackem, který by situaci značně vylepšil. Bohužel by nám ale neřešil problém druhý, který spočívá v chybějícím chlazení této kanceláře. Umístění klimatizace do této místnosti není možné z hygienických důvodů. Bylo by také značně neefektivní s přihlédnutím k časté fluktuaci zaměstnanců v této místnosti.

Dalším řešením je možnost přestěhování hardwarového vybavení do samostatné místnosti, která bude odpovídat požadavkům na serverovnu s respektováním výše popsaných řešení pro lokaci hlavní.

V případě, že taková místnost ve výrobní hale neexistuje, v úvahu přichází i výstavba takové místnosti s využitím vnitřních protipožárních příček a instalováním klimatizace.

Ve případě, kdy jsou obě serverovny dobře zabezpečeny proti vstupu nechtěných osob je potřeba také určit okruh lidí, kteří mohou do serveroven vstupovat, jejich pravomoci a také okolnosti, za kterých je jim přístup umožněn. Všechny tyto osoby musí být patřičně proškoleny jak se v serverovně chovat a jak řešit krizové situace (hašení požáru, vypnutí serveru v případě nouze, výměna nefunkčního disku v poli).

7.7.2 Fyzické zabezpečení počítačů

Označení nezamčených počítačových skříní a nezaheslovaného BIOSu proti změnám se mohou zdát jako malichernost. Tyto dvě maličkosti ale dokáží značně zjednodušit přístup útočníka k datům uloženým v počítači. Představme si následující scénář: Útočník chce

ukrást konstrukční data z kolegova počítače. Počítač je ale zabezpečen proti připojení externích paměťových zařízení. Po síti není dané soubory také možno poslat. Jelikož ale stanice nemá zamčenou skříň a BIOS není chráněn proti změnám v nastavení, útočník může použít následující postupy. 1) Otevře skříň, připojí druhý pevný disk a data zkopíruje na něj. 2)Odnese si celý pevný disk. 3) Připojí USB klíčenku s jiným systémem, nabootuje z ní a poté zkopíruje data z disku na USB klíčenku.

Přitom aplikování hesla pro změny v BIOS/UEFI je akce, která nevyžaduje žádné dodatečné náklady. Je potřeba pouze u každého počítače vstoupit do BIOS/UEFI a provést nastavení.

Zamčení počítačových skříní proti otevření u některých z nich není také otázkou dodatečných nákladů. Zámek je již součástí skříně. U zbytku počítačů lze vyměnit skříně, oslovit externí firmu pro dodání zámků do existujících skříní nebo se situace dá elegantně vyřešit svépomocí. Více viz. obrázek níže.

Obrázek 8 - Zámek počítačové skříně [17]

V případech, kdy je například obtížné ohlídat, co si zaměstnanci odnáší z firmy, protože ve firmě je hojný výskyt pracovníků jiných společností, nebo prostě jen chceme elegatně zvýšit fyzickou bezpečnost hardwarového vybavení firmy, je možné použít i zámky, které brání fyzickémů přemístění vybavení. Většina současných počítačů, monitorů, tiskáren atd. je již vybavena slotem pro připojení tohoto zámku.

Obrázek 9 - Zámek hardwaru [16]

7.7.3 Ostatní nedostatky fyzické bezpečnosti

Pro ochranu strukturované kabeláže proti přepětí je doporučeno použít zařízení APC ProtectNet PNET1GB, které filtruje napětí na všech vodičích, ale stále umožňuje propuštění POE napájení.

Zbylé identifikované problémy není možné odstranit bez změny návrhu současného stavu informačního systému, a proto jejich řešení bude navrženo v další části této práce.

7.8 Datová bezpečnost

Největším problémem firemního informačního systému je nedostatečně vybavený a zastaralý hardware. Příkladem může být proces jakým jsou zálohována data, kde jednoznačně chybí nějaké datové pole či pásková knihovna, jež by umožnila komplexní zálohování systémů s delší retencí.

Operačnímu systému Windows Server 2003 skončila podpora ze strany Microsoftu 14. července 2015. Po tomto datu už Microsoft nebude vydávat tzv. bezpečnostní záplaty a systém se stane značně rizikovým.

Doporučeným řešením je přechod na nový operační systém Windows Server 2012 R2. Současné servery by svým výkonem měly ovšem problém daný systém hostovat. Jelikož jsou fyzické, nedovolují ani použít maximální počet licencí, jež je umožněno použít při využití serverů virtuálních.

Z výše zmíněných důvodů se další část práce zaměří na návrh nového systému, jenž splní bezpečnostní požadavky na něj a bude podporovat současné IT trendy.

7.8.1 Počítačová síť

Předpokladem správně fungujícího informačního systému je vhodně dimenzovaná a nastavená počítačová síť.

V konfiguraci té současné bylo označeno několik neduhů, které její bezpečnost a rychlost počítačové sítě omezují. Nečlenění na podsítě a zapojení serverů, tiskáren atd. přímo do routeru jsou příklady konfigurací, které negativně ovlivňují chod celé sítě a budou odstraněny při návrhu nové sítě.

Při pohledu na současné prvky počítačové sítě vidíme, že switche 3COM 4500 50-port umožňují připojení stanic do sítě pouze 100MB, což při dnešním trendu centralizace počítačových zdrojů může značně ovlivnit výkonost této sítě. Řešením je nahrazení těchto switchů switchy novými, které budou podporovat komunikaci s rychlostí 1GB.

Jako vhodné zařízení doporučuji použít switche Cisco SG500-52 jenž nabízí dostatečný výkon pro podnik střední velikosti, 52 portů Gigabit Ethernet a jsou stohovatelné, což nám značně usnadní jeho správu ve větším počtu.

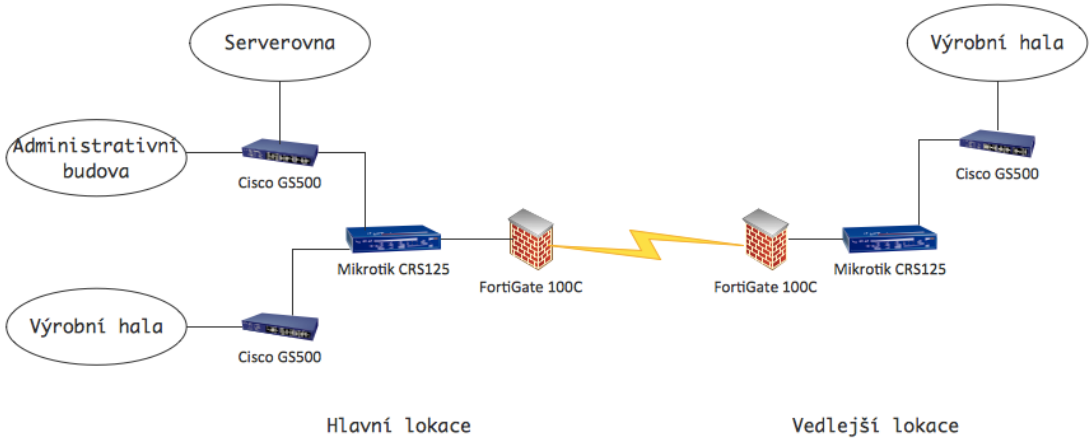
Aktuálně použité routery MIKROTIK Cloud Router Switch CRS125 mají dostatečný výkon i potřebnou portovou rychlost pro naše řešení. Jedinou jejich nevýhodou je absence některých pokročilých bezpečnostních funkcí jako jsou IPS či DLP. Tyto funkce a mnohé další se dají ale do systému implementovat předřazením zabezpečovacího zařízení před router. Mezi výrobce těchto bezpečnostních zařízení patří firmy Sophos, Fortigate a Cisco. Pro naši implementaci doporučuji použít zařízení FortiGate-110C od výrobce ForiGate. Mezi jeho hlavní funkce patří firewall, VPN, detekce průniku do systému (IPS), prevence proti úniku informací (DLP), aktivní ověřování uživatelů vůči Active Directory (FSAE), záloha nebo vyvážení zátěže primárního a sekundárního připojení do internetu, vysoká dostupnost spojením 2 a více FortiGate zařízení a mnohé další.

Jelikož všechna síťová zařízení podporují IEEE 802.1Q je vhodné rozdělit vnitřní síť na menší samostatné virtuální sítě. Toto nastavení nám v první řadě pomůže zvýšit bezpečnost sítě rozdělením do segmentů, což se například projeví tím, že administrativní rozhraní síťových prvků a servery nebudou primárně viditelné z ostatních virtuálních sítí (segmentů). Navrhované rozdělení:

- VLAN10 – infrastruktura – servery, síťové prvky
- VLAN20 – počítačové stanice, tiskárny, servery a projektory
- VLAN30 – speciální VLAN určená pro hosty ve firmě

- VLAN40 – VPN síť

Konečné schéma zapojení síťových prvků je zobrazeno na obrázku níže.



Obrázek 10 - Konečné schéma zapojení síťových prvků [Zdroj: Vlastní]

Z obrázku také vyplývá, že pro propojení hlavní a vedlejší lokace bude potřeba nastavit virtuální privátní síť (VPN), díky níž bude komunikace mezi lokacemi šifrovaná. Tato VPN se bude moci použít i pro přístup zaměstnanců přistupujících z firemních laptopů do sítě z venku.

Přístup do firemní sítě by měl být zajištěn i při možném výpadku připojení primárního poskytovatele Internetu. Proto je zde nutné myslet na nadbytečnost (redundanci) internetového připojení. Ta bude zaručena již výše zmíněnou funkcí zařízení FortiGate - záloha nebo load balancing primárního a sekundárního připojení do internetu, v kombinaci s vhodně vybranými poskytovateli internetu.

7.8.2 Serverové vybavení

Jak již bylo zmíněno výše, současnému operačnímu systému Windows Server 2003 byla ukončena podpora ze strany výrobce 14. července 2015. Současné servery nemají dostatečný výpočetní výkon, ani plnou kompatibilitu použitého hardwaru s Windows Server 2012. Další jejich nevýhodou je, že nepodporují plně virtualizaci. V našem případě by se jednalo o virtualizaci hardwarovou. Hlavním přínosem virtualizace serverů bude vyšší využití hardwarového výkonu serverů, které nám umožní při stejném počtu fyzických serverů nasazení více serverů virtuálních a tudíž i využití více služeb. Zjednodušení zálohování serverů a jejich případné obnovy ze zálohy, kde již nejsme závislí na specifické hardwaro-

vé konfiguraci poškozeného serveru. V případě potřeby nám virtualizace i umožní dynamicky zvýšit výkon (v případě volných zdrojů na serveru).

Jako náhradu současných serverů navrhuji použít servery HP ProLiant DL360G9 s šestijádrovým procesorem Intel Xeon E5-2620v3 (2.4 GHz, 15MB cahche), 32GB RAM (možnost rozšířit až na 512GB), 4 x 300 GB SAS 15 000 RPM, 4 x Gigabit Ethernet, Raid Smart Array B140i.

Takto výkonné servery poskytnou dostatek výkonu pro hostování minimálně dvou virtuálních serverů současně. Vyšší počet ethernet konektorů umožní rychlé propojení s datovým polem pomocí iSCSI protokolu a jejich interní RAID řadič nám umožní konfigurovat lokální disky do RAID 1, jenž ochrání běžící systém před výpadkem v případě ztráty jednoho z disků.

7.8.3 Hypervisor

Trh se současnými virtualizačními nástroji se za poslední roky značně vyrovnal a VMware jakožto průkopník virtualizace má dnes již silnou konkurenci ve firmách Citrix, Microsoft a RedHat. Mnoho z nich své produkty nabízí se základní funkcionalitou zcela zdarma.

Mezi nejlepší určitě patří řešení od VMware – vSphere Hypervisor a od Microsoftu – Hyper-V. Nabízené funkce jsou víceméně podobné. Ve výsledku ale dávám přednost a doporučuji pro nový informační systém použít Hyper-V, který již v základu podporuje zálohování celých virtuálních serverů (pro platformu Windows). Řešení od VMware tuto funkcionalitu nabízí také, ale nutné je bohužel dokoupit licenci. Cena této licence vychází v některých případech dráže, než pořízení specializovaného zálohovacího nástroje, a proto mi toto řešení přijde značně neekonomické.

7.8.4 Operační systém a zdroje

Použité aplikace v informačním systému nám znatelně omezují možnosti výběru operačního systému. Mnoho z jich je kompatibilních pouze s platformou Windows. O použití jiného systému by se dalo uvažovat pouze u web a mail serveru. Komplikace spojené s migrací dat těchto serverů v kombinaci s nutným dodatečným školením IT administrátora však tuto výměnu zavrhují.

Jako jediné rozumné řešení zde proto budeme uvažovat pouze o Windows Server 2012 R2. Nyní je ale potřeba vybrat jeho vhodnou edici, tak aby poskytovala licence pro dostatečné množství virtuálních serverů.

Abychom byli schopni vybrat správnou edici, musíme si nyní připravit schéma rozmístění virtuálních serverů přes servery fyzické a přidělení jejich zdrojů. Tato informace s celkovým počtem uživatelů v systému a s požadovanými funkcemi nám pomůže určit potřebnou edici operačního systému Windows Server 2012 R2.

Box 1

VM1 – AD (2cpu, 8GB RAM)

VM2 – WBS (2cpu, 8GB RAM)

Box 2

VM1 – file server, WSUS, DHCP (2cpu, 8GB RAM)

VM2 – Access, aplikace (OKbase, Autodoprava) (2cpu, 8GB RAM)

Box 3

VM1 – SQL server (4cpu, 24GB RAM)

Box 4

VM1 – AD (2cpu, 8GB RAM)

VM2 – WBS (2cpu, 8GB RAM)

V úvahu nakonec připadají pouze dvě z edic. Standard a Datacentr. Po technické stránce jsou verze totožné, zásadní rozdíl je ale v počtu licencí na virtuální servery. Zatímco edice Standard umožňuje současně mít 2 servery, edice Datacentr žádné takové omezení nemá. Novinkou od verze 2012 je také potřeba zakoupení licence za základě počtu procesorů, jenž obsahují fyzické servery, kde je plánováno využívat virtualizaci.

Na základě všech informací zde uvedených vychází jako nejekonomičtější řešení, které ovšem neubírá nic na nabízené funkcionalitě pořízení pěti edic Windows Server 2012 R2 Standard. Pátá edice nebude ihned použita. Bude připravena pro případnou instalaci při havárii jednoho ze serverů pro rozšíření počtu licencí na již běžícím fyzickém serveru.

7.8.5 Diskové pole

V aktuální konfiguraci systému diskové pole není obsaženo. Nepotřebnost diskového pole pravděpodobně souvisí se špatně nastaveným procesem zálohování. Je zde ale potřeba si uvědomit, že diskové pole samotné nenahrazuje zálohování dat. Diskové pole díky své funkcionalitě zálohování dat značně ulehčuje. Jak svou kapacitou, tak i případně funkcemi, které dnešní diskové pole jsou schopna nabídnou v kombinaci s vlastním operačním systémem na nich běžících.

Jedním z návrhů, místo hledaní již hotového řešení, je možnost si postavit takové pole vlastní. Výhodou by byla nižší pořizovací cena, nevýhodou by však byla vyšší provozní cena (spotřeba energie), záruka na každou komponentu zvlášť a chybějící podpora výrobce pro datové pole jako celek. Z těchto důvodů doporučuji výběr již hotového řešení před stavbou řešení vlastního.

Při výběru diskového pole si musíme stanovit parametry, které by toto pole mělo poskytovat. Tyto parametry jsou:

- Podpora RAIDu 5,6,10,
- Podpora SSD disku jako cache paměti pro rozšíření propustnosti,
- Redundance připojení, možnost agregace připojení,
- Rychlá možnost rozšíření diskové kapacity,
- Podpora Active Directory,
- Podpora virtualizace pro Windows Server 2012 R2,
- Šifrování dat,
- Podpora snapshotů, clonování dat,
- Možnost konfigurace pro vysokou dostupnost (HA),
- Podpora ODX pro Windows Server 2012 R2,
- Podpora iSCSI.

Na základě stanovených kritérií a zkušeností z praxe nakonec navrhuji použít zařízení od firmy Synology RS3614xs. RS3614xs splnilo všechny stanovené podmínky pro výběr diskového pole a mezi jeho velké přednosti patří špičkový management systém DiskStation Manager (DSM), který i méně zkušenému uživateli značně usnadní orientaci ve správě diskového pole.

Pro nově navrhované řešení doporučuji použít následující konfigurace.

V lokaci hlavní navrhuji pořídit Synology RS3614xs společně s expanzní jednotkou. Tato konfigurace poskytne celkem 24 diskových pozic, které by měly být využity následovně. Prvních 12 pozic nakonfigurovat do RAIDu 10, kde bude 5 disků použito pro data, 5 pro výpočet parity, 1 jako náhradní (spare) disk a jeden bude použit pro SSD disk, který bude fungovat jako cache paměť, což vylepší výkonost pole. Těchto 12 pozic bude osazeno 1TB disky s 10 000 otáčkami (RPM), jež poskytnou celkem 5TB místa použitelného pro produkční data (SQL databáze, sdílené disky, atd.). Zbylých 12 pozic expanzní jednotky bude nakonfigurováno v RAIDu 6, kde bude 8 disků použito pro data, 2 pro výpočet parity a 2 budou náhradní (spare) disky. Pozice budou osazeny 2TB disky s 7 200 otáček (RPM), což nám ve výsledku poskytne 16TB volného místa, jež bude použito pro uložení záloh produkčních dat a dat z profilů uživatelů.

Do vedlejší lokace stačí pořídit pouze diskové pole Synology RS3614xs. V této lokaci není potřeba poskytnout produkční výkon, jelikož v ní není žádný SQL server a pro sdílené disky stačí výkon nižší. Toto pole může být konfigurováno do RAIDu 6 stejně, jako expanzní box v lokaci vedlejší. Jeho hlavním účelem bude ukládání záloh uživatelů z lokace vedlejší, poskytnutí sdílených disků a replikace důležitých dat z lokace hlavní.

Při objednávání disků je potřeba si dát pozor, aby jednotlivé disky byly z více výrobních sérií. Tímto opatřením se jednoduše eliminuje pravděpodobnost výpadku více disků ve stejný čas kvůli výrobní vadě.

7.8.6 Zálohování dat

V této části práce se zaměříme na nastavení zálohování dat pro nově navržený systém. Toto řešení je možné implementovat díky změnám provedeným v konfiguraci sítě, virtualizaci serverů a centralizovanému ukládání dat.

Aby bylo možné centrálně řídit zálohování virtuálních serverů, uživatelských profilů a dat je nezbytně nutné připojit všechny uživatelské stanice do domény. Celý proces zálohování uživatelských počítačů bude totiž řízen pomocí pravidel distribuovaných přes doménu. Další neméně nutnou součástí tohoto řešení je instalace minimálně jednoho virtuálního serveru s rolí Windows Server Backup (WSB). Tento server bude mít na starosti kompletní řízení zálohování případně i obnovy dat. V této implementaci budou data zálohována na diskové pole ve svých lokacích. Z tohoto důvodu máme WSB servery 2, v každé lokaci jeden. Každý si tak bude řídit zálohování dat ve své části.

WSB server si také bude sám spravovat místo na zálohovací části pole. Vždy když nebude mít dostatek místa pro vytvoření nové zálohy, vymaže nejstarší zálohu. Zde nám pomůže se zachováním co nejvíce záloh deduplikace dat, která je dostupná ve Windows od verze Windows Server 2012.

I když kapacita diskového pole by měla být schopná uchovat zálohy minimálně na půl roku, nikdo tento čas negarantuje, protože v případě velkých změn v datech serverů a sdílených disků může být kapacita pole vyčerpána po pár týdnech. Jelikož se ale na discích nacházejí i data vývojářů, retenční doba by měla být pro tato data minimálně rok. Lépe ještě déle.

Řešením by bylo zálohovat například jednou týdně data také na pásku. Zde ale narážíme na problém. Windows Server od verze 2008 nepodporuje zálohování na pásky. Stá-

le ale disponuje ovladači pro ně. Proto jediným východiskem pro zálohování dat na pásky je použití softwaru třetí strany, jenž tento způsob podporuje. Příkladem takového softwaru je Veeam Backup Free Edition. Tento nástroj podporuje všechny základní funkce pro zálohování virtuálních serverů. Navíc nabízí i některé pokročilé funkce, jednou z nich je například šifrování dat.

V ideálním případě by zálohování dat na pásky probíhalo s pomocí páskového robota, jenž by sám vyměňoval pásky před zálohováním. Jeho pořízení je ale stále značně nákladné a při frekvenci zálohování dat na pásku jednou týdně je tato akce stále v silách lokální IT podpory. K zálohování může být použita současná pásková mechanika.

Pro ukládání pásek doporučuji pořídit ohnivzdorný trezor.

7.8.7 Centralizované aktualizace

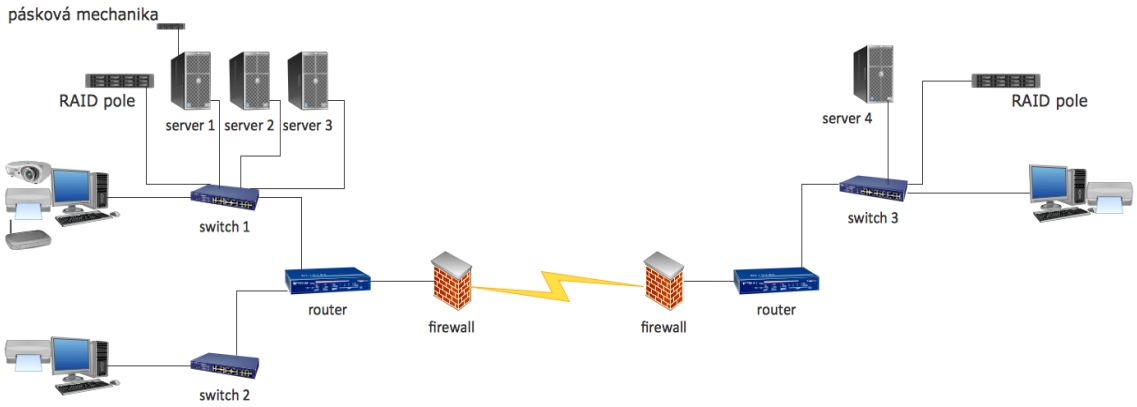
Díky připojení všech počítačů do domény se dá vyřešit centralizované řízení aktualizací velice jednoduše. Potřeba je pouze na jednu z instalací Windows Server 2012 R2 Standard přidat roli Windows Server Update Service. Tato role se pak postará o řízení aktualizací pro všechny počítače připojené v doméně.

Díky faktu, že všechny potřebné balíčky jsou stahované z internetu pouze na server, kde je přiřazena WSUS role, šetří se tak i přenos dat zvenčí sítě.

Další nespornou výhodou je možnost nastavení automatického hlášení o stavu aktualizací pro jednotlivé stanice.

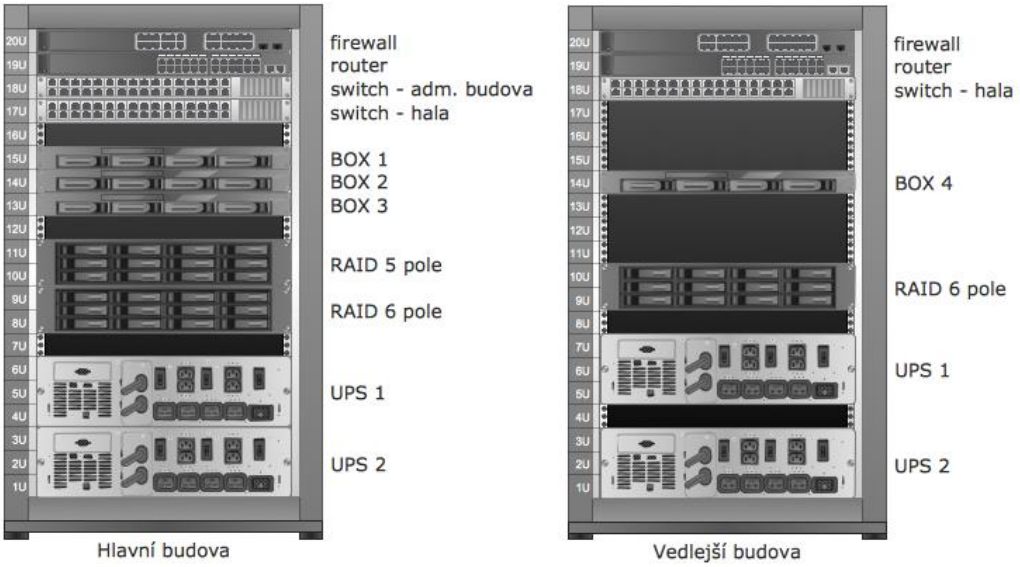
7.8.8 Vizualizace systému po úpravách

Na obrázku níže je zobrazeno zapojení počítačové sítě po úpravách provedených v navrhovaném řešení.



Obrázek 11 - Navrhovaný stav sítě po úpravách [Zdroj: Vlastní]

Následující vizualizace zobrazuje správné uspořádání zařízení umístěných v rackových skříních.



Obrázek 12 - Rozmístění zařízení v rackových skříních [Zdroj: Vlastní]

8 ZHODNOCENÍ A MOŽNÝ ROZVOJ

Navrhované řešení značně mění konfiguraci celého informačního systému. Jeho proměna do finální podoby spotřebuje značné množství časových i finančních prostředků. Podíváme-li se ale na současný stav z pohledu bezpečnosti, je tato proměna nutná.

Po transformaci systému do nové podoby je očekáváno kladné přijetí zejména ze strany IT administrátorů, kterým plná implementace domény značně usnadní dennodenní práci. Management firmy jej plně ocení až v situacích, kdy se ukáží jeho schopnosti (zabránění úniku dat, obnova dat po havárii). Pro běžné uživatele nový systém přinese zjednodušenou správu dat v kombinaci s mnohými omezeními, která ovšem přispějí k bezpečnosti systému (nutnost přihlašování se při přístupu na internet, zákaz používání externích médií, zvýšený monitoring provozu na síti).

V budoucnu by bylo dobré do systému přidat také centrální monitoring, jenž bude schopný podat informaci o současném využití sítě, serverů a diskového pole. Tento monitoring by byl také schopný zasílat emaily a SMS na předem definované akce (výpadek disku, požár, atd.).

V současně navrhované implementaci systému také stále zůstávají data záloh ve stejné místnosti jako produkční data. Řešením by bylo pořízení nového diskového pole, které by se umístilo do jiné místnosti, než je současné, a nakonfigurovalo by se pro vysokou dostupnost s existujícím. Toto řešení by také dokázalo zachránit produkci před výpadkem v případě havárie aktivního diskového pole.

ZÁVĚR

Cílem této práce bylo navrhnout zabezpečení informačního systému podniku střední velikosti s více pobočkami. Snažil jsem se uplatnil své znalosti z problematiky bezpečnosti a informačních systémů, které jsem získal studiem na vysoké škole.

Informační systém podniku, ve kterém jsem řešil praktickou část své diplomové práce, neprošel v posledních letech žádnými velkými renovacemi. Proto jeho konfigurace a struktura byla pro dnešní dobu nevhodná až zastaralá. Vedení firmy si tuto situaci uvědomilo a chtělo zjistit, jaký je reálný stav jeho systému v porovnání s dnešními trendy.

V teoretické části této práce byly představeny možné hrozby, které v dnešní době nejčastěji hrozí IS, společně s ochrannými prostředky, které dokáží tyto hrozby minimalizovat či plně vyloučit.

V praktické časti byl nejdříve představen informační systém podniku. Následně byla provedena bezpečnostní analýza tohoto IS, která odhalila slabá místa v jeho konfiguraci. K eliminaci či odstranění těchto slabých míst byla navržena vhodná opatření. Nastíněn byl i možný rozvoj těchto opatření do budoucna v případě, že vedení firmy bude s funkcionalitou a chodem nového IS spokojeno.

Na závěr této práce je vhodné připomenout, že nelze nikdy navrhnout stoprocentně bezpečný systém, proto je péče o bezpečnost informačních systémů nikdy nekončícím procesem.

SEZNAM POUŽITÉ LITERATURY

[1] JAŠEK, Roman. *Ochrana znalostí a dat v podnikových informačních systémech*. Vyd. 1. Zlín: Univerzita Tomáše Bati, Fakulta managementu a ekonomiky, 2002, 115 s. ISBN 80-7318-095-2.

[2] JAŠEK, Roman. *Informační a datová bezpečnost*. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006, 140 s. ISBN 80-7318-456-7.

[3] DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011, 286 s. ISBN 978-80-7431-050-8.

[4] BIGELOW, Stephen J. *Mistrovství v počítačových sítích: správa, konfigurace, diagnostika a řešení problémů*. Vyd. 1. Brno: Computer Press, 2004, 990 s. ISBN 80-251-0178-9.

[5] SOSINSKY, Barrie A. *Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]*. Vyd. 1. Brno: Computer Press, 2010, 840 s. ISBN 978-80-251-3363-7.

[6] MALANÍK, David. *Význam fyzického zabezpečení IT systémů.* Security Revue září 2010. ISSN 1336-9717.

[7] *Co je to počítačový vir a škodlivý software* [online]. [cit. 2015-05-12]. Dostupné z: http://napoveda.seznam.cz/cz/co-je-to-pocitacovy-vir-a-skodlivy-software.html

[8] Data Center High Availability Clusters. *CISCO* [online]. [cit. 2015-05-12]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Data_Center/HA_Clusters/HA_Clusters/HAOver_1.html

[9] DATA LOSS PREVENTION. *Ami* [online]. [cit. 2015-05-12]. Dostupné z: http://www.ami.cz/reseni-a-sluzby/bezpecnost-dat/data-loss-prevention-1

[10] Antivirový program. *Antivirové centrum* [online]. [cit. 2015-05-12]. Dostupné z: http://www.antivirovecentrum.cz/antiviry.aspx

[11] Autentizace a autorizace. *Web4company* [online]. [cit. 2015-05-12]. Dostupné z: http://www.web4company.cz/bezpecnost-autentizace-autorizace/

[12] Typy útoků používané hackery. *OWEBU.cz* [online]. [cit. 2015-05-12]. Dostupné z: http://owebu.bloger.cz/Bezpecnost/Typy-utoku-pouzivane-hackery

[13] AntiSpam. *Antivirové centrum* [online]. [cit. 2015-05-12]. Dostupné z: http://www.antivirovecentrum.cz/antispam.aspx

[14] INTRUSION DETECTION SYSTEM - IDS TECHNOLOGY AND DEPLOYMENT. *Antivirové centrum* [online]. [cit. 2015-05-12]. Dostupné z: https://www.paloaltonetworks.com/resources/learning-center/what-is-an-intrusion-detection-system-ids.html

[16] [online]. [cit. 2015-05-12]. Dostupné z: http://www.fujitsu.com/cz/Images/WCM20381_tcm58-13523.png

[17] [online]. [cit. 2015-05-12]. Dostupné z: http://www.securityrevue.com/wp-content/uploads/2010/09/image-3.jpg

[18] [online]. [cit. 2015-05-12]. Dostupné z: http://www.bechtle.cz/shop/BD_CZ-cs/APC%20NetShelter%20SV%2042U%2C%2080cm%2C%20rack_812497

[19] [online]. [cit. 2015-05-13]. Dostupné z: http://prodevice.eu/wp-content/uploads/2014/03/2.jpg

[20] TULLOCH, M. *Microsoft Encyclopedia of Security.* Washington (USA): Microsoft Press, 2003. 480 s. ISBN 0-7356-1877-1.

[21] KOCH, M., et al. *Management informačních system.* 3. vyd. Brno: Akademické nakladatelství CERM, s.r.o., 2010. 171s. ISBN 97880-214-4157-6.

[22] STAUDEK, J. *Úvod do problematiky bezpečnosti IT.* 3. [online]. FI MU Brno, verze podzim 2007. [cit. 2016-04-20]. URL: http://www.fi.muni.cz/usr/staudek/vyuka.

[23] *Analýza rizik* [online]. Brno, 2013 [cit. 2016-05-03]. Dostupné z: http://www.vutbr.cz/www_base/priloha.php?dpid=74652.

[24] RAIS, Karel a Radek DOSKOČIL. *Risk management: studijní text pro kombinovanou formu studia*. Brno: Akademické nakladatelství CERM, 2007. ISBN 978-80-214-3510-0.

[25] JAŠEK, Roman a David MALANÍK. *Bezpečnost informačních systémů.* 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013. ISBN 978-80-7454-312-8.

[26] Co je VPN? *Microsoft TechNet* [online]. [cit. 2016-05-08]. Dostupné z: https://technet.microsoft.com/cs-cz/library/cc731954(v=ws.10).aspx

[27] *J. Krhovják, V. Matyáš. Autentizace a identifikace uživatelů.* Zpravodaj ÚVT MU. ISSN 1212-0901, 2007, roč. XVIII, č. 1, s. 1-5.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AD	Active Directory
BA	Bezpečnostní analýza
BIOS	Basic Input-Output System
BPIS	Bezpečnostní analýza informačního systému
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Prevention
DVD	Digital Versatile Disc
HA	High Availability
HTTPS	Hypertext Transfer Protocol Secure¨
HW	Hardware
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IMAP	Internet Message Access Protocol
IPS	Intrusion Prevention System
IS	Informační systém
iSCSI	Internet Small Computer System Interface
IT	Informační technologie
ODX	Offloaded Data Transgers
PGP	Pretty Good Privacy
POE	Power over Ethernet
RAID	Redundant Array of Independent Disks
SCSI	Small Computer System Interface
SQL	Structured Query Language
SSD	Solid-State Drive

UEFI	Unified Extensible Firmware Interface
UPS	Uninterruptible Power Supply
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WBS	Windows Backup Server
WSUS	Windows Service Update Server

SEZNAM TABULEK

SEZNAM OBRÁZKŮ