Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta
Katedra informačních technologií

Diplomová práce

Bezpečnostní infrastruktura informačního systému v MSP

Autor: Bc. Jan Drmla

Vedoucí práce: Doc. Ing. Zdeněk Havlíček, CSc.

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Drmla Jan

Informatika

Název práce

Bezpečnostní infrastruktura informačního systému v MSP

Anglický název

The security IT infrastructure in SMEs

Cíle práce

Cílem diplomové práce je seznámit čtenáře s problematikou bezpečnosti IS a bezpečnostní politiky podniku . Praktická část práce je primárně zaměřena na navržení bezpečnostní infrastruktury v malém středním podniku a její simulace v příslušném softwaru, která bude použita jako podkladový materiál pro samotnou realizaci projektu.

Metodika

Vytvoření teoretické (rešeršní) části diplomové práce bude založeno na studiu a analýze odborných materiálů týkající se řešené problematiky informační bezpečnosti. Na základě získaných poznatků a skutečností v teoretické části práce bude vytvořena praktická ukázka návrhu bezpečnostní politiky a simulace chráněné počítačové sítě v reálném prostředí MSP. Na základě syntézy teoretických poznatků a výsledků praktické části pak budou formulovány závěry diplomové práce.

Harmonogram zpracování

6 / 2014 - Vyplnění zadání v Badisu
7 / 2014 - Studium odborné literatury
10 / 2014 - Tvorba teoretické a praktické části
2 / 2015 - Tvorba finálního dokumentu práce
3 / 2015 - Odevzdání práce

Rozsah textové části

60 - 80 stran

Klíčová slova

Bezpečnost IS, počítačová síť, zálohování, hardware, software, firewall, ACL, bezpečnostní politika, simulace sítě

Doporučené zdroje informací

KÁLLAY, Fedor a PENIAK, Peter. 2003. Počítačové sítě a jejich aplikace. 2.akt.vyd. Praha : Grada, 2003. str. 356. 80-247-0545-1.

SOSINSKY, Barrie. 2010. Mistrovství - Počítačové Sítě. 1.vyd. Brno : CPress, 2010. str. 840. ISBN: 978-80-251-3363-7.

NORTHCUTT, Stephan, a kol. Bezpečnost počítačových sítí. 1. vydání. Brno: Computer Press, 2005. 592 s. ISBN: 80-251-0697-7.

DOSTÁLEK, Libor, KABELOVÁ, Alena. Velký průvodce protokoly TCP/IP a systémem DNS. 5. vydání. Brno: Computer Press, 2008. 488s. EAN: 9788025122365.

SNYDER, Joel. UTM firewalls: READY FOR THE ENTERPRISE. Network World, 2007, č. 34, s. 35-36, 2 s.

PETERKA, Jiří. Jak fungují firewally [online]. Praha: Computerworld, 2003. Dostupné na WWW: <http://www.earchiv.cz/b03/b0800001.php3>.

Vedoucí práce

Havlíček Zdeněk, doc. Ing., CSc.

Termín odevzdání

březen 2015

Elektronicky schváleno dne 31.10.2014

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 11.11.2014

Ing. Martin Pelikán, Ph.D.

Děkan fakulty

Čestné prohlášení

Prohlašuji, že svou diplomovou práci na téma " Bezpečnostní infrastruktura informačního systému v MSP " jsem vypracoval samostatně pod vedením vedoucího diplomové práce s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 31. 3. 2015 _____

Jan Drmla

Poděkování

Rád bych touto cestou poděkoval panu Doc. Ing. Zdeňkovi Havlíčkovi, CSc. za věnovaný čas při konzultacích a cenné připomínky a odborné vedení mé diplomové práce. Poděkování také patří kolegovi Ing. Tomáši Tikalovi za odbornou pomoc z hlediska bezpečnostních řešení. A samozřejmě panu Ing. Pavlu Havlíčkovi, který mi poskytl zázemí svého podnikatelského prostředí, na jehož základě vznikla tato práce.

Bezpečnostní infrastruktura informačního systému v MSP

Souhrn

Obsah celé diplomové práce lze rozdělit do dvou hlavních částí, kdy se jedná o návrh bezpečnostní politiky pro vybraný MSP a druhá část zabývající se samotnou realizací bezpečnostní infrastruktury. Popsány jsou jednotlivé postupy tvorby bezpečnostní politiky vycházející z jednotlivých bezpečnostních ISO norem. Uplatnění této politiky lze zobecnit na firemní prostředí podobného rozsahu a zaměření. Praktická část diplomové práce je rozčleněna do jednotlivých dílčích projektů a postavena na reálném firemním prostředí. Kde byly aplikovány současné postupy podloženy odbornými materiály. Dílčí části této práce jsou zaměřeny na vybudování centrální místnosti, propojení vzdálených lokalit a vytvoření interního dokumentu bezpečnostní politiky.

The security IT infrastructure in SMEs

Summary

The content of Diploma thesis can be divided into two main parts a security policy for SMEs and implementation of security infrastructure. The thesis describes the various procedures of security policies based on ISO safety standards. Implementation of this policy can be generalized to the corporate environments similar size and specialization. The practical part of the thesis is divided into several subprojects based on a real business environment. Here have been applied the current procedures, which are supported by scientific sources. The subsectiont of this thesis is focused on building the central room, connecting the remote locality and create a document of an internal security policy.

Klíčová slova: bezpečnost IS, počítačová síť, zálohování, hardware, software, firewall, ACL, bezpečnostní politika, simulace sítě

Keywords: IS security, computer network, backup, hardware, software, firewall, ACL, security policy, network simulation

Obsah

1. Úvod

Bezpečnost přenášených a uchovávaných informací je dnes bezpochybně celosvětově nejdiskutovanější tématem. Nejen ve firemním prostředí, ale i v osobním světě jsou informace v podstatě nejcennějším vlastněným aktivem. Zároveň ale v mnoha případech jsou vystaveny vnějším i vnitřním rizikům v podobě hackerských útoků, nebo ztráty, popřípadě poškození vlastními zaměstnanci apod., Těmto rizikům, která nás ohrožují lze včas předcházet a adekvátně na ně reagovat.

„Pod nátlakem narůstajících okolních hrozeb si sami firmy velice dobře uvědomují skutečnost, že důležitá interní data musejí chránit před vnějším světem mnohem důsledněji, než tomu bylo doposud.“ Tento výrok pronesl uznávaný zahraniční odborník na bezpečnost Borek Boissy, který byl pozván na akademickou půdu ČZU, aby zde vedle cyklus přednášek o současné problematice ICT[1] a její bezpečnosti. Proto jsou firmy ochotny na zvýšení bezpečnosti dle doporučených ISO norem a standardů vyčlenit finanční prostředky a změnit i vlastní postoje k ochraně dat. V lepších případech dochází pouze k aktualizaci stávajících řešení. Jinde musí dojít k restrukturalizaci nebo úplnému zřízení nové infrastruktury a uzpůsobení k bezpečnému chování všech zúčastněných osob ve firemním prostředí. Pokud firma učiní kroky ke zřízení bezpečnostní politiky a zaručí se k jejímu striktnímu plnění, musí při porušení pravidel dodržet sankční limity i pro nejvýše postavené. Protože integrita vnitřní bezpečnosti je neméně důležitou stránkou pro uchránění firemních informací, před vynášením nebo špionáží z vlastních řad, s jakýmkoliv úmyslem.

V diplomové práci budou navrženy konkrétní kroky a doporučeny kontrolní mechanismy, jak zlepšit vnitřní i vnější bezpečnostní situaci v dané organizaci. Jelikož většina těchto kroků je používána jako standardizovaný postup, lze navrhovaná řešení zobecnit na podobné typy objektů. Popřípadě znásobit jednotlivé oblasti dle velikosti rekonstruovaného objektu v návaznosti na potřeby a požadavky konkrétní organizace.

[1] Information & Comunication Technologies

2. Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem předkládané diplomové práce je zanalyzovat informační systémy z bezpečnostního hlediska a navrhnout bezpečnostní infrastrukturu aplikovatelnou do vybraného podniku.

Tento hlavní cíl práce se sestává z mnoha důležitých dílčích cílů, mezi něž jsou zahrnuty především tyto následující, které kopírují obecně definovanou strukturu takto zaměřeného odborného textu.

- *Teoretické zkoumání bezpečnostních technik, postupů a opatření*, která jsou v současnosti diskutována a posléze v praxi aplikována pro zvýšení bezpečnosti informačního systému. Studiem a zkoumáním podkladů, bude možné zajistit provázanost teoretické s praktickou částí práce.
- *Analyzovat současný stav ve zvoleném podniku z bezpečnostního hlediska* a tím vytvořit základní charakteristiku krizových oblastí, pro které bude hledáno příslušné nápravné opatření, tak aby bylo docíleno požadovaného bezpečnostního stavu.
- *Navrhnout patřičná bezpečnostní opatření* pro zvýšení stability celého informačního systému vybraného podniku, založené především na vybudování centrálních IT služeb podniku.
- *Připravit dokument bezpečnostní politiky,* podle něhož bude podnik postupovat v budoucím jednání otázek bezpečnosti.
- *Formulovat obecné a specifické závěry dané problematiky* vyplývající z popisovaných kapitol diplomové práce a jejich možné aplikovatelné zobecnění do prostředí malých a středních organizací.

2.2 Metodika

Nejdříve budeme analyzovat teoretické přístupy při zajišťování bezpečnosti informačního systémů a poté charakterizovat dílčí bezpečnostní oblasti, v praxi využívané pro návrh a realizaci. Teoretické poznatky budou čerpány z odborné literatury, řádně zacitovány a v textu označeny. Za další zdroje lze považovat samostudium problematiky a také již nabyté praktické zkušenosti v oboru.

Praktická část, tvořící jádro práce, vychází z načerpaných teoretických podkladů a povede k aplikaci jednotlivých postupů tvorby bezpečnostní infrastruktury. V prvních fázích bude představena a interně analyzována společnost Dahl-tok s.r.o. na níž budou provedeny jednotlivá nápravná opatření pro zlepšení bezpečnosti systému. Počínaje vybudováním zabezpečené a klimatizované centrální místnosti, následováno propojením poboček do centrálního uzlu až po nastavení jednotlivých lokalit, jak z pohledu aplikačního prostředí, tak síťového rozhraní. Posledním krokem ke kompletizaci dílčích projektů bude vytvoření interního dokumentu bezpečnostní politiky v návaznosti na nově budovaný stav infrastruktury.

Závěrem budou synteticky zhodnoceny přínosy a nedostatky navrhovaných řešení, osvětleny některé realizační postupy a jejich současné rozpracování.

3. Teoretická východiska

Kapitola je především zaměřena na jednotlivé problematické celky zajišťující zvýšení bezpečnosti ve vybraném firemním prostředí. Zabezpečení ICT je vždy náročná a neustálá práce založena na kvalitních analýzách interního prostředí organizace, zkoumání, poučení se ze vzniklých incidentů, ale také musí odrážet vzájemné pochopení a komunikaci zainteresovaných stran s ohledem na optimalizaci celého systému pro 100% efektivnost všech zúčastněných. Příkladem lze nastínit situaci, kde bezpečnostní technik navrhne a zavede do organizace příliš přísná a do důsledku nepromyšlená pravidla, která uživatelům natolik znepříjemní práci, že to povede ke snížení efektivnosti jejich výkonů a v některých případech i k znemožnění přístupu k potřebným informacím.

V dnešním přetechnizovaném světě plném moderních technologií a aplikací, ke kterým se v naprosté většině přistupuje pomocí internetu, kde vyžadují naši kompletní identifikaci, je důležité si uvědomit hodnotu přenášených osobních informací a ostatních dat, které je zapotřebí patřičně zabezpečit dle stanovené priority.

Proto vznikl i tento návrhu firemní infrastruktury v určitém bezpečnostním měřítku popisovaný v diplomové práci. Vše souvisí se zabezpečením přístupu, ochranou a uchováním osobních údajů klientů a firemních informací v internetové síti, která je neustále vystavena bezpečnostním hrozbám v podobě hackerských útoků, virů, ale také v ohrožení vlastními uživateli.

3.1 ISO Normy a Bezpečnostní politika

Bezpečnostní dokument striktně definuje pravidla chování a zacházení s informacemi, dále práva a povinnosti jednotlivých zúčastněných subjektů, počínaje uživateli, ostrahou, vedením až po samotné majitele. K zavedení samotného bezpečnostního dokumentu je důležité rámcově dodržet doporučené postupy a k nim náležící předpisy a normy, z kterých například vychází, jak zacházet s osobními údaji, nebo jakou skupinu utajovaných informací podnik vlastní apod. Jedním z prvních a zároveň nejtěžších úkolů při zavádění takovéhoto dokumentu je přesvědčit nejvyšší management, aby tuto činnost podpořil a vyčlenil určité finanční i lidské zdroje.

3.1.1 Normy

V oblasti ICT je nevíce skloňována zkratka ISMS[2] a rodina norem ISO/IEC 2700x podle nichž jsou prováděny certifikace organizací a zároveň jsou považovány za jedny nejlepších směrů pro zavedení bezpečnostní politiky. *„Vlastní podstata ISMS spočívá v podpoře pro ustavení, zavedení, provozování, monitorování, udržování a zlepšování samotného bezpečnostního systému.“ (Chlup, 2008)* Snadno si lze hlavní procesy týkající se bezpečnosti zapamatovat díky stručnému obrázku č. 1 jinak také nazývanému PDCA.

Obrázek 1: Procesy ISMS
Zdroj: http://www.amiya.co.jp/solutions/isms_service/images/img_pdca.jpg

Organizace prokazující se touto certifikací je považována za kvalitního partnera. Dnes, kdy platí „Kybernetický zákon“ je certifikace pro organizace postižené zákonem z pohledu kritické infrastruktury státu, jednou z mála možností, jak prokazovat soulad s vydaným zákonem.

Například norma ISO 27001 nyní ve verzi 2013, vycházející z původního Britského standardu pro informační bezpečnost z roku 1995 vedeného pod názvem BS 17799-2. Aktuální verze normy, která je doporučujícím standardem, ale také se podle ní společnosti certifikují. V současnosti se certifikované organizace musí nechat re-certifikovat dle nové verze do září 2015, jinak o stávající certifikaci přijdou. Norma stanovuje pravidla pro řízení bezpečnosti informací dle struktury a požadavků na procesní i technickou bezpečnost. Kdežto norma ISO 27002 také v revizi 2013, obsahuje soubor praktických doporučení pro zavedení, udržování a zlepšování ISMS. Jak popisuje Tobolka, autor článku o změnách ISO, nové revize těchto norem přineslo *„redukci požadavků s tím, že požadavky již nejsou tak striktní a nesvazují ruce organizaci při plnění ducha požadavků normy.“* (Tobolka, 2014)

[2] Information Security Management System

Pro tvorbu bezpečnostní politiky je doporučeno být v souladu s následující legislativou: (AEC, 2008)

- zákon č. 101/2000 Sb. o ochraně osobních údajů
- zákon č. 127/2005 Sb. o elektronických komunikacích
- zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským (tzv. autorský zákon)
- zákon č. 227/2000 Sb., o elektronickém podpisu
- zákon č. 480/2004 Sb., o některých službách informační společnosti
- další legislativa (vyhlášky, standardy atd.) MV ČR[3], ÚOOÚ[4], NBÚ [5]apod.
- Problematika fyzické bezpečnosti je vztažena k zákonu č. 412/2005 Sb. a dále v souladu se zněním § 10 vyhlášky č. 528/2005 Sb. (NBÚ, 2011)
- Vyhláška č. 523/2005 Sb., - o bezpečnosti informačních a komunikačních systémů v pozdější novele vyhlášky č. 453/2011 Sb. (NBÚ, 2012)

Další sadou norem využívaných pro zavedení bezpečného IT systému je sada nazývaná ČSN ISO/IEC TR 13335 1-5. Jejíž stručný výčet je zde uveden a samotná názvosloví jsou pro využití v organizaci jasným vodítkem jaké kroky při zavádění zahrnout: (Chlup, 2008)

- **13335 1** – Pojetí a modely bezpečnosti IT, kdy například tato norma ustavuje základní pojmy při tvorbě bezpečnosti.
    - Aktivum – cokoliv co má pro organizaci nějakou hodnotu.
    - Dostupnost – zajištění, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby.
    - Důvěrnost – zajištění, že informace jsou přístupny nebo sděleny pouze těm, kteří jsou k tomu oprávněni.
    - Integrita – zajištění správnosti a úplnosti informací.
- **13335 2** – Řízení a plánování bezpečnosti IT
- **13335 3** – Techniky pro řízení bezpečnosti IT
- **13335 4** – Výběr ochranných opatření
- **13335 5** – Pokyny pro řízení síťové komunikace

[3] Mnisterstvo Vnitra ČR
[4] Úřad pro Ochranu Osobních Údajů
[5] Národní Bezpečnostní Úřad

3.1.2 Bezpečnostní politika

Jak uvádí Fabián v malých podnicích je ochrana firemních dat často přehlížena, i když je důležité se této problematice věnovat, stejně jako se jí věnují v korporátním prostředí. Protože při ztrátě interních dat mohou nastat velké problémy, *„podle serveru Small Business Computing až 80% podniků, které postihne vážný únik informací, do dvou let od incidentu čelí vážným finančním problémům, nebo dokonce bankrotu.“* (Fabián, 2012) Kdy hlavními chybami se stává omezený rozhled majitelů v otázkách bezpečnosti, obavy z finanční náročnosti a složitosti zavedení bezpečnostních opatření, nedůslednost při plnění minimálních bezpečnostních požadavků, jako je antivirové zabezpečení uživatelských PC nebo školení a informování právě vlastních zaměstnanců o aktuálních bezpečnostních hrozbách.

Ve svém článku Houser obecně popisuje aktuální situaci okolo bezpečnostní politiky. *„S tím, jak jsou podnikové procesy postupně automatizovány a veškeré obchodní informace převáděny do digitální formy, firmy stále více spoléhají na své informační systémy a sítě. O to více jsou také vystavovány bezpečnostním rizikům a hackerským útokům z nejrůznějších stran. Součástí každé podnikové informační strategie proto má být komplexní bezpečnostní politika, která povede k zajištění ochrany dat a ve finále také kontinuity podnikání.“* (Houser, 2013)

V malých a středních firmách je na místě vypracovávat dokument bezpečnostní politiky v součinnosti s externí odbornou firmou zabývající se bezpečností, protože ve většině případů organizace nedisponují tak kvalitním a informovaným bezpečnostním oddělením pro samostatné vypracování. Ovšem za předpokladu, že několik zasvěcených zaměstnanců, především z řad IT a managementu, musí při tvorbě spolupracovat a popřípadě vytvářet směr finální podoby interního dokumentu.

Z hlediska hackerských útoků je a bude každá organizace zranitelná, každá z nich se může na takové riziko připravit a v případě incidentu i čelit. Jak řekl ředitel FBI Robert Mueller na konferenci o počítačové bezpečnosti v San Franciscu. (Fabián, 2012) *„Jsem přesvědčen o tom, že existují pouze dva druhy společností – takové, do kterých se již hackeři nabourali, a ty, do nichž se teprve nabourají. Obávám se, že v blízké době budou existovat pouze společnosti, do jejichž systémů hackeři pronikli, a společnosti, do nichž proniknou znovu.“*

Proto by bezpečnostní politika měla tvořit jeden ze základních bezpečnostních pilířů, na kterém stojí systém řízení bezpečností informací a firemní systém jako takový. Z logického pohledu na věc je jednoznačné, že když nejsou oficiálně a striktně stanovena pravidla, role,

povinnosti a odpovědnost jednotlivých zaměstnanců v systému, snadno dojde k vybudování chaotického a neefektivního firemního prostředí.

Zavádění jednotného interního dokumentu je zpravidla v souladu s ISO normami 27001 a 27002 a nějakým způsobem se dotýká následujících kapitol: bezpečnostní politika, organizační bezpečnost, klasifikace a řízení aktiv, personální bezpečnost, fyzická bezpečnost, bezpečnost prostředí, zálohování dat, zabezpečení před viry, řízení komunikací a provozu, řízení přístupu, zajištění před krádeží, vývoj a údržba systémů, monitoring procesů, zvládání bezpečnostních incidentů, řízení kontinuity činnosti a zajištění shody a školení uživatelů. Při vytváření dokumentu je opět k dispozici doporučená a všeobecně standardizovaná struktura: (AEC, 2008)

- stanovení účelu bezpečnostní politiky
- definice požadované úrovně bezpečnosti
- definice zodpovědnosti za klasifikaci dat, zaměstnanců a přístupových práv (ve smyslu fyzickém i informačním)
- definice zodpovědnosti jednotlivých článků organizační struktury při řízení bezpečnosti ICT
- normy chování zaměstnanců (včetně právních a etických aspektů)
- havarijní plány a postupy při budování bezpečnosti ICT v obecné rovině
- definice úrovní zabezpečení a míry odolnosti v jednotlivých oblastech bezpečnosti (personální, organizační, technická atd.)
- podmínky a periodicita auditu

Výsledný dokument bude pro organizaci velkým přínosem a usnadněním v řízení informační oblasti, kam přinese jasně formulované principy. Ohledně zaměstnanců to přispěje k pravidelnému školení a ke stanovení jejich základních odpovědností a povinností při práci s informacemi v ICT. Pomůže, uvědomit si, jaké požadavky striktně požadovat a nastavit při spolupráci s externími subjekty formou doprovodných smluv SLA[6] a zároveň vůči partnerům vystupující firma působí seriózněji a obchodní partneři to patřičně ocení při vzájemné spolupráci. Protože když jedna organizace chrání svá data, znamená to pro ostatní, že i jejich poskytnutá data jsou v bezpečí. (AEC, 2008)

Závěrem je naprosto důležité zmínit neopomenutelný fakt, že po vytvoření dokumentu, práce na bezpečnosti firemního prostředí neskončila a respektive nikdy neskončí.

[6] Service Level Agreement

Jako se vyvíjí a mění firemní prostředí, musí se v průběhu času aktualizovat i interní bezpečnostní dokument, pro jehož aktualizace musí být striktně stanoveny intervaly revize. A v návaznosti na vzniklé incidenty musí být dokument revidován obratem po odstranění incidentu, tak aby v budoucnu k podobné situaci již nedošlo.

3.2 Zabezpečení firemní infrastruktury

Pro vytvoření komplexní bezpečné infrastruktury je zapotřebí věnovat pozornost několika klíčovým směrům. Nejdůležitější je samotné oddělní jednotlivých sítí a to vnitřní od vnější tedy internetu. Popřípadě zavedením DMZ[7] pro zabezpečení veřejně dostupných zdrojů firmy jako je např. e-mail a webové stránky. Poté jsou pohledy směřovány na samotnou fyzickou bezpečnost celého systému postupně přecházející k bezpečnosti vnější. Vnější bezpečnost infrastruktury potažmo interní sítě zajišťují jednotlivé implementované bezpečnostní prvky s korektní konfigurací na dané řešení. Především je uvažováno použití NAT[8], filtrování paketů, proxy, firewall a na něm spuštěné kontroly IDS a IPS[9]. Posledním krokem zvyšujícím zabezpečení jsou vnitřní mechanismy na bázi antivirových, antispamových a zálohovacích služeb.

3.2.1 Fyzická bezpečnost

Podle NBÚ[10] je fyzická bezpečnost druhem zajištění ochrany utajovaných informací tvořené systémem opatření, která zabrání nebo ztíží přístup neoprávněným osobám k těmto informacím. (NBÚ, 2011) Především se jedná o kontrolované vstupy pomocí EZS[11], protipožární opatření (EPS[12] a SHZ[13]) kamerový systém a další čidla ochrany v místnostech disponujících aktivními prvky infrastruktury. Bez tohoto prvku fyzické bezpečnosti ostatní níže uvedené mechanismy ztrácí na účinnosti. Protože stále platí skutečnost o napadení útočníky zevnitř systému. Všechny systémy zajišťující bezpečnost je důležité propojit do online stavu například pomocí GSM brány nebo vlastního managementu kontroly v podobě upozorňujících mailů, aby případná ohrožení mohla být eliminována již v zárodku incidentu.

[7] Demilitarizovaná zóna
[8] Network Address Translation
[9] Intrusion Detection System & Intrusion Prevention System
[10] Národní Bezpečnostní Úřad
[11] Elektronický Zabezpečovací Systém
[12] Elektronická Požární Signalizace
[13] Stabilní Hasicí Zařízení

Jak naznačuje ve svém článku Sikyta, kroky fyzické bezpečnosti v podniku směřují k automatizaci činnosti ostrahy a plného využití technologií a informací v nich obsažených pro zefektivnění běžných činností. To znamená, že nad veškerými kontrolními prvky je postaven jeden inteligentní systém, který mnohem lépe vyhodnotí dané situace z obrazu kamer a čidel. Tyto poznatky poté vyhodnotí a zařídí potřebné kroky – vyvolá poplach, informuje ostrahu daným kamerovým záznamem a zaznamená události do logu. Nebo také dokáže rozpoznat falešné poplachy. (Sikyta, 2011)

3.2.2 Vnější bezpečnost

Firewall dále jen FW – by dnes měl být hlavním bezpečnostním prvkem v každé organizaci bez ohledu na její velikost nebo obsah spravovaných informací. FW jako takový tvoří bezpečnostní zeď na hranicích interní sítě před propojením do vnější sítě zpravidla internetu, který je přístupný všem tedy i uživatelům se zločinnými úmysly. A před nimi je zapotřebí využít všech dostupných technologií pro vytvoření co možná nejbezpečnějšího prostředí pro firemní data. Dnešní robustní firewally dokáží interní síť ochránit na všech vrstvách ISO/OSI modelu, od linkové až po aplikační, díky využití technologie hloubkové inspekce paketů. (Strebe, a další, 2003) Základním účelem FW je zabránit neoprávněnému přístupu do nebo z privátní sítě na základě kontroly všech procházejících požadavků. Výsledkem je blokování těch požadavků, které nesplňují stanovená bezpečnostní kritéria většinou nastavována pomocí ACL[14] seznamů. (Beal, 2013) K zajištění veškerých kontrolních mechanismů jsou využívány základní tři metody a to filtrování paketů, překlad IP adres (NAT) a aplikační služby (Proxy). Pro uvedené metody není striktním pravidlem nutného využívání na FW, např. proxy služby lze provozovat na odděleném serveru. Zbyté metody a služby budou podrobněji popsány níže. FW dále poskytuje například šifrovanou autentizaci uživatelů a bezpečné propojení vzdálených lokalit.

Vzhledem k velkému nárůstu nově vyvíjených aplikací a zneužívání otevřeného portu http bylo zapotřebí FW také vyvíjet směrem k blokaci provozu na hlubší aplikační úrovni s vyšší mírou účinnosti. Tento směr a v něm vyvíjené prvky je nazýván jako Next Generation Firewalls – NGFWs. Na rozdíl od robustních UTM[15] řešení, kde neustále dochází k balancování na hraně mezi samotným výkonem a ochranou, nabízí NGFWs nové pojetí problematiky, ale stále s obrovským důrazem na celkovou bezpečnost a prováděním důkladné

[14] Access Control List
[15] Unified Threat Management

kontroly provozu bez zpoždění a blokování útoků. Zjednodušeně řečeno opouští od filtrování portů, IP adres, paketů a přechází na přímou kontrolu aplikačního obsahu, přidělovaného uživateli, jak popisuje Wegner ze společnosti Secure Edge Networks. (Wegner, 2013) Uvádí příklad, kdy NGFWs budou mít možnost integrovat adresářové služby a tím identifikovat uživatele a klasifikovat mu dané aplikace. Což povede k maximálnímu využití FW a ucelenému kontrolnímu přehledu, kdy vytvořené zásady na FW budou mnohem více konkrétní a to například takto: uživatel v síti s rolí „student“ bude moci navštívit stránky Facebooku, ale nebude moci zde nic psát během školních hodin. Autor článku „next-generation firewalls 101“ Ohlhorst popisuje fungování NGFWs následovně (Ohlhorst, 2013). Budou využívány různé techniky a předdefinované podpisy aplikací pro analýzy a kontrolu záhlaví k určení konkrétních aplikací. FW si ukládá knihovnu schválených žádostí a umožňuje jim tím přístup do sítě, dále sleduje chování nových aplikací, tím se učí, vytváří základní linii normálního chování a v případě vychýlení z linie upozorní správce. Celý tento systém identifikace aplikací vede k pomoci organizacím, aby získali kontrolu nad chaotickým webovým provozem.

Základními principy FW pro řízení ochrany jsou využívány paketové filtry, překlady adres, systémy detekce a prevence průniku do sítě.

Paketové filtry – první FW sloužily jako jednoduché filtry, ale filtrování paketů zůstalo hlavní doménou i současných FW prvků jež se člení do dvou hlavních typů. Jejichž primárním úkolem je kontrola informací v hlavičce paketu, na jejímž základě dojde k přeposlání nebo zablokování daného paketu.

- **Bezstavového filtrování** - nejvíce využívané směrovači
- **Filtrování pomocí kontroly stavu** – stateful inspection

Z hlavičky jsou pro kontrolu vyselektovány pouze užitečné informace, které podrobněji popisuje Perkins. (Strebe, a další, 2003)

- **Typ protokolu** – který se při filtrování paketů získává z údajů v poli Protokol IP. Podle těchto údajů lze rozlišit základní sady služeb – UPD[16], TCP[17], ICMP[18] a IGMP[19]. Příkladem je využívání jen a pouze webového serveru založeného na TCP se službou HTTP tz., že bychom mohli odfiltrovat veškeré

[16] User Datagram Protocol
[17] Transmission Control Protocol
[18] Internet Control Message Protocol
[19] Internet Group Management Protokol

služby založené na UDP. Bohužel filtrování pouze pomocí typu protokolu je hodně obecné a většinou je potřeba v aktivních prvcích nechat všechny protokoly otevřené.

- **Adresa IP** – tímto typem filtrování dokážeme omezit připojení na konkrétní hostitele identifikované pomocí IP adresy. Je zbytečné používat přístup zablokování konkrétních hostitelů – museli bychom znát adresy všech hackerů světa. Proto je využíván opačný a mnohem bezpečnější přístup, založený na metodě povolení vstupu pouze konkrétním adresám. Tato metoda je považována za nejbezpečnější formu, kterou bezstavové filtry mohou nabídnout. Tím, že se zablokuje přístup všem hostitelským adresám, vyjma povoleného seznamu nám zajistí, že k směrovači či FW dostanou pouze ta zařízení nebo sítě, které známe. Z důvodu zneužívání přímého směrování hackery k průniku do sítě, je významně doporučováno, aby paketové filtry byly vždy nastaveny, tak že pakety z přímého směrování automaticky zahazují.
- **Port TCP/IP** – nejčastěji využívaná metoda filtrování informací, vycházející z označení portů TCP / UDP, které je nepřesnějším nositelem informace o tom k čemu daný paket slouží. Platí zde stejný přístup ochrany jako u filtrování adres IP, tedy vše zakázat a povolit pouze vybraný seznam. Blokováním určitých portů získáme i výhodu proti hackerům, kteří si pro své útoky vybírají pouze konkrétní protokoly, které jim poskytují vysokou míru kontroly nad napadeným systémem. Jejich seznam a popis je uveden níže.
    - Telnet – poskytuje útočníkovi zpřístupnění příkazové řádky a tím pádem téměř úplnou kontrolu nad napadeným zařízením.
    - Relace NetBIOS – využívána na systémech Windows. Pokud útočníkovi poskytneme otevřený tento port, zároveň mu zpřístupníme možnost připojení k souborovým serverům z pozice jakoby lokálního klienta.
    - POP – zajišťující vzdálený přístup k poštovním mail boxům uživatelů v nezašifrované formě, což útočníkovi poskytuje možnost monitorování hesel uživatelů.
    - NFS – otevřením tohoto portu, ale v systémech Unix vzniká stejný problém jako v případě NetBIOS.

- Windows Terminal Services – vystavením tohoto portu do internetu bude znamenat ochranu terminálového serveru pouze uživatelským jménem a heslem, které jsou pro útočníka snadno prolomitelné.

Uvedeny jsou ještě dvě zastaralé metody využívané v Protokolu IP. A právě díky jejich zastaralosti jsou častým cílem útočníků, proto je důležité na ně při konfiguraci nezapomínat. Současné paketové filtry podporují funkci automatického zahození paketu, u kterého došlo k přímému směrování nebo fragmentaci.

- **Číslo fragmentu** – vychází z původního účelu metody, pro dělení velkých paketů, které směrovače nedovolovali předávat po síti v důsledku omezené velikosti rámců. Zásadním problémem je, že filtrování nejdůležitějších informací se nachází pouze v hlavičce prvního paketu tedy fragmentu 0 a v případě zahození tohoto fragmentu se stávají bezcenné i ostatní navazující fragmenty. A právě jednoduchým přenastavením zásobníku dokáží útočníci obejít filtr úplně, tím že vynechají nultý fragment.
- **Informace o přímém směrování** – název již napovídá, že se jedná o stanovení přesně dané trasy, kterou paket musí projít. Buď to je stanovena mezi dvěma klienty, nebo jsou určeni hostitelské body, přes které paket musí projít. Způsob, kterým využívají hackeři tuto metodu je prostý – hacker do hlavičky nastaví adresu svého zařízení, aby se mu paket vždy vrátil a tím získal další informace z napadené sítě.

Bohužel tyto bezstavové filtry nedokáží kontrolovat datovou část paketů a neuchovávají stavy spojení a bez použití dalších bezpečnostních prvků nezaručují vysokou míru zabezpečení. Proto tyto poznatky přispěly ke vzniku druhého typu paketového filtru s kontrolou stavu. Jehož fungování odráží předešlé nedostatky, tím že udržuje stav celé komunikace na síťové i relační vrstvě během zaslání jednotlivých paketů, které ze zásady nepřicházejí pohromadě za sebou nýbrž v dané relaci. Bezstavový filtr v těchto případech vždy zkontroloval pouze první hlavičku paketu, která bezpečnostními pravidly prošla, ale navazující pakety již mohly obsahovat infikované informace ve prospěch hackera. Po průchodu paketu obsahujícího informace o ukončení TCP relace, následně FW veškeré související položky odstraní ze stavové tabulky, tak aby nedocházelo k průchodům firewallu. Pro lepší kontrolu průchozích paketů se vytvářejí stavové bezpečnostní politiky určující základní pravidla chování stavového filtru.

Strebe ve své knize popisuje základní charakteristiky nejlepšího postupu pro použití filtrování paketů vzhledem k jejich nedostatkům. Především se jedná o použití kvalitního firewall řešení se všemi komponentami – proxy, filtrování paketů, NAT apod. Za druhé je důležité v prvotní konfiguraci deaktivovat úplně všechny porty a v neposlední řadě důsledně zabezpečit základní operační systém aktivních prvků. (Strebe, a další, 2003)

Network Address Translation – NAT (Wenstrom, 2003) je v interních sítích využíván k oddělení interních neveřejných adres z volného rozsahu od pevně stanovených vnějších veřejných adres, v České Republice toto spravuje organizace CZ.NIC. Výsledkem překladu je skrytí celé firemní sítě před vnějším světem například za jednu nebo několik veřejných IP adres, odvozeny od fyzického počtu propojených linek do internetu. Jednou z výhod NATu je šetření relativně vzácných veřejných adres pro použití v jednotlivých LAN sítích. Samotný mechanismus překladu funguje následovně: IP adresa příchozího paketu z internetu se ve FW přeloží podle nastavených pravidel překladu a paket se doručí do správného cíle. Obdobným způsobem dostávají i odchozí zprávy přidělenu veřejnou IP adresu, zatímco skutečné adresy vnitřní sítě zůstávají skryty. Alternativou směrování v sítích s využitím čísel portů namísto IP adres je Port Address Translation – PAT. Ve směrovačích Cisco je využívána následující terminologie při konfiguraci NATu, kterou sepsal Wenstrom:

- **Vnitřní lokální adresa** – IP adresa, přidělená hostitelskému systému ve vnitřní síti. Touto adresou obvykle není právoplatná veřejná IP, přidělená organizací NIC nebo poskytovatelem služeb.
- **Vnitřní globální adresa** – právoplatná IP adresa, přidělaná od CZ.NIC, která vůči vnějšímu světu reprezentuje jednu nebo více vnitřních lokálních adres.
- **Vnější lokální adresa** – IP adresa vnějšího hostitelského systému, platná pro vnitřní sít. Nemusí být nutně oficiální, je vybrána z adresního rozsahu směrovaného ve vnitřní síti.
- **Vnější globální adresa** – IP adresa, přidělená hostiteli ve vnější síti jeho vlastníkem. Tato adresa je vybrána z množiny globálně směrovatelných adres neboli síťového prostoru.

Při konfiguraci NATu a překladu mezi výše uvedenými typy adres lze provádět překládání statické, s vyrovnáváním zatížení, s redundancí v síti anebo využití i služeb dynamického překladu, který pro překlad a přidělení IP adresy využívá takzvaného poolu

vnitřních globálních adres. Například použití NATu s vyrovnáváním zatížení, prakticky uplatnit v situaci, kdy se překládá jedna IP adresa na více shodně nakonfigurovaných serverů. Strebe, ale také poukazuje na některé nedostatky NATu, jako například nemožnost použití určitých protokolů, které vyžadují otevření kanálu zpět ke klientovi, šifrování hlavičky TCP nebo použití původní adresy k zabezpečení. V praxi to například může při špatné konfiguraci znemožnit komunikaci formou konferenčních hovorů nebo omezení funkčnosti IPSec protokolu apod. (Strebe, a další, 2003)

Intrusion Detection System & Intrusion Prevention System - IDS & IPS (Bigelow, 2004) **-** systémy Detekce a Prevence proti průniku neboli služby běžící na FW prvku, zajišťují sledování sítě a činnosti na ní, za účelem včasného odchycení neoprávněné aktivity. V souvislosti s těmito službami je důležité mít v organizaci zavedené reakční plány na vzniklé incidenty proniknutí. Vývoj těchto systémů podpořila skutečnost, že na některé hackerské útoky byl samotný FW nedostačující a v případě šikovného útočníka i bezmocný. Pokud organizace disponuje širokým kontrolním týmem IT specialistů a nechce spouště služby IDS, může využít pouze přímého sledování protokolů vycházejícího z aktivních prvků nebo serverů. Rozdíl mezi aktivními FW prvky a systémem IDS je v tom, že se aktivně neúčastní přenosu dat v síti. IDS buď pouze pasivně monitoruje prostředky za účelem vypátrání zákeřných aktivit a upozornit na ně odpovídajícímu bezpečnostnímu správci formou výstrah a auditních stop nebo aktivně reagují a pokoušejí se útoky blokovat a spouštět různá protiopatření. *„Dnes jsou dostupné dva hlavní typy IDS – systémy založené na síti a systémy založené na hostiteli. Systém IDS založený na síti monitoruje sítě kvůli objevení zákeřných paketů, zatímco systémy založené na hostitelích monitorují jednotlivé hostitele, aby zjistily neoprávněné aktivity.“* (Bigelow, 2004) Důležité je vlastní nastavení varovných poplachů, které při správném a odladěném řešení vyloučí falešné poplachy. Po napadení a průniku do systému je dle poznatků „best practices,“ postižené místo opravit opětovným vybudováním od začátku nebo obnovit z původních nenapadených záloh.

Podle Strebeho lze detekční systémy rozčlenit na jiné dva typy – založené na inspekci a využití návnady. Detekčně inspekční systémy jsou zpravidla nejčastěji používané, hlavně se spoléhají na zde uvedené indikátory neoprávněného použití, kde sledují jejich různé kombinace, které zaprotokolují a vytvoří, tak auditní stopu.

- *„Síťový provoz, jako je skenování protokolu ICMP, skenování portů nebo připojení k neoprávněným portům.*

- *Výkyvy ve využití zdrojů, jako například procesoru, paměti nebo I/O síťových operací v neočekávanou dobu. Může to znamenat automatizovaný útok proti síti, manipulace se soubory, včetně vytvořených souborů, úpravy systémových souborů, změny uživatelských souborů nebo úpravy účtů uživatelů nebo oprávnění zabezpečení.“* (Strebe, a další, 2003)

Naproti tomu návnadové systémy neboli „Honeypots“ se snaží napodobit reálné chování cílového systému, který není správně zabezpečen. *„Neposkytují však útočníkovi vektor vniknutí, ale místo toho upozorní na své napadení. Protože návnadu nikdo v rámci organizace k běžné práci nepoužívá, jsou všechny pokusy o připojení k ní, pokusy o vniknutí“* (Strebe, a další, 2003)

Důležitou poznámku na konec teorie firewallů, sepsal ve své knize Bigelow. Po implementaci bezpečnostní topologie, kde bylo vytvořeno několik zásad zabezpečení – tedy zásad určující jak chránit interní informace, které jsou právě bránou FW implementovány. Na základě aplikovaných pravidel je důležité sledovat a protokolovat průběh provozu pro včasné odchycení potencionálního rizika, protože k samotnému incidentu dochází až po dlouhodobém skenování sítě samotnými útočníky. A v neposlední řadě zajistit kontrolu a otestování nastavených pravidel, zda jsou opravdu funkční. (Bigelow, 2004)

V jiné knize od Donahua, jsou použita tři velice účinná pravidla. Pro návrh bezpečnostních pravidel a konfiguraci FW je důležité udržet jednoduchost a srozumitelnost, proto „v jednoduchosti je krása.“ Dále využití zlatého pravidla bezpečnosti říkající „*Zakažte vše; povolte to, co potřebujete.*“ A nakonec distancovat se od všeho co není vaše, protože to již patří do vnější sítě. (Donahue, 2009)

Proxy server – další z řady bezpečnostně-kontrolních prvků síťového provozu na aplikační, zde popisovaného jako standardní proxy server bez nadstavbových komponent jako je například překlad IP adres. Tyto kontrolní mechanismy, v níže popisovaném návrhu, v plné míře zajišťuje firewall. Samotný funkční proces spočívá v tom, *„že naslouchají požadavkům o služby od interních klientů a pak je předávají na externí síť, jako kdyby byl klientem – původcem samotný server Proxy. Jakmile obdrží proxy od veřejného serveru odpověď, vrátí tuto odpověď původnímu internímu klientskému počítači, jako kdyby byl sám původním veřejným serverem.“* (Strebe, a další, 2003) Z původního účelu proxy zajišťujícího posílení výkonu přetrvalo pouze ono ukládání do vyrovnávací paměti. Dnes je tato vlastnost upravena a povýšena na reverzní typ proxy, která navíc dokáže rozkládat zatížení mezi ostatní

webové server. Využitím tohoto typu bude také zajištěna podpora šifrování SSL[20] při přenosu zabezpečených web stránek. Jedním z hlavních důvodů pro aplikování proxy do firemního prostředí je zvýšení bezpečnosti založené na následujících bodech, které ve své knize definoval Perkins. (Strebe, a další, 2003)

- Skrytí klientů ve vnitřní síti před veřejným internetem.
- Blokování nežádoucích URL adres a zamezení stahování určitého obsahu.
- Filtrování obsahu webových požadavků klientů a zamezí tím průniku virů.
- Vytváří jediný přístupový bod a umožňuje zaznamenat kdo, co, kdy navštívil.

Oproti tomu oponuje jiný autor některými omezeními, která u proxy vznikají. Zejména se jedná o pomalejší činnost vzhledem k důkladnému zkoumání přenášených paketů. A udržení stálé aktuálnosti serveru v návaznosti na vývoj nových protokolů a aplikací, kterým se proxy musí učit. (Thomas, 2005)

3.2.1 Vnitřní bezpečnost

Antivirová ochrana – neméně důležitým prvkem zvyšující ochranu celého systému je komplexní, centralizované a rezidentní řešení antivirové ochrany v podobě serverové konzole a na ni navázaných klientů. Serverové část zajišťuje plnou kontrolu nad online aktualizovanou virovou databází serveru, aktuálním stavem klientů a řízení pravidel rozdělení sítě do segmentů. Správně nastavené řešení zabrání proniknutí do systému naprosté většině škodlivého softwaru jako jsou trojské koně, viry, červy a další. V tomto směru bezpečnosti je zapotřebí volit takové produkty, které poskytují více stupňovou ochranu celé infrastruktuře počínaje hraničními prvky sítě přes jednotlivé servery až po nejnižší úroveň klientských PC. Dnešní antivirové společnosti poskytují svým zákazníkům aktualizace virové definice několikrát za hodinu, protože riziko napadení je obrovské a tvůrci virů nikdy nepřestávají s vývojem nového a neznámého škodlivého softwaru. Snaží se být vždy o krok před antivirovými giganty. Naopak některé společnosti si vypomáhají a vytváří obrovské týmy analytiků pro včasné odchycení virů a vytvoření aktualizované definice.

Antispamová ochrana – fungující na stejném principu jako výše uvedený antivir. Plní specifický úkol v podobě ochrany uživatele před nežádoucí příchozí elektronickou poštou. Tuto cestu využívají útočníci a záměrně ji směřují přímo na uživatele, kteří jsou v mnoha případech velice důvěřiví a poskytují důležité informace. Proto je zapotřebí prvek „uživatele“ co nejvíce extrahovat od těchto situací. Správně nastavené spamové filtry

[20] Secure Sockets Layer

to na 98% plní a zvyšují tím bezpečnost celého sytému. Opět je důležité spamové filtry a databáze, které korespondují s celosvětovými veřejnými seznamy nežádoucích odesílatelů, udržovat v nejaktuálnějším možném stavu. Z logické posloupnosti je zapotřebí tyto filtry umisťovat před samotné mail servery, tak aby nežádoucí pošta byla odchycena ještě dříve, než bude přesměrována na příslušný mail box uživatele.

Zálohování – při práci s velkým objemem dat často dochází ke ztrátám, proto je důležité do bezpečnosti systému zařadit zálohování a to nejen samotných dat, ale celých systému popřípadě virtuálních strojů pro případ havárie a následného obnovení. Podstata zálohování je podpořena i mezinárodními normami ISO, určující zacházení s informacemi a zajištění jejich atomických vlastností – důvěrnost, dostupnost a integrita. Prvním krokem k využívání zálohovacích mechanismů je zakomponování tohoto bodu do interního dokumentu s příslušnými přílohami jako zálohovací plán apod. Z něhož musí vycházet i pokyn pro protokolování prováděných záloh, který ve výsledku velice pomůže při případné obnově. Dle Bigelowa by protokol měl obsahovat následující body: datum, číslo sady, typ zálohy, co a z jakého umístění bylo zálohováno, kdo ji prováděl a kde jsou pásky uloženy. Poté je důležité zanalyzovat současně využívaná data a podle zjištěných kritérií vybrat vhodné zálohovací prvky a podpůrné softwary. (Bigelow, 2004)

V malém prostředí s několika zaměstnanci a malým objemem vytvořených dat se vyplatí využít služeb NAS[21] serveru s několika disky zapojených do RAID pole. Server disponuje softwarem pro správu a řízení uložiště, definování zálohovacího plánu a pravidelné provádění záloh v návaznosti na vybraný typ RAID pole např. RAID 1 – zrcadlení disků nebo RAID 5 využívající replikace dat mezi jednotlivými disky s odolností vůči výpadku jednoho disku.

Naopak ve velkých společnost s většími objemy dat je zapotřebí zajistit sofistikovanější způsob provádění záloh v rámci celého systému. Diskové kapacity v řádech desítek TB jsou umisťovány do diskových polic vytvářející snadno rozšiřitelná disková pole. Pro správu a distribuci kapacit musejí být využity robustní zálohovací systémy, které po vytvoření SAN[22] clusteru s napojením na zálohovací páskovou knihovnu vytvoří velice stabilní a účinný systém zálohy firemní dat. Zálohování na přepisovatelné pásky zajistí dlouhodobou archivaci důležitých informace s podmínkou uložení na bezpečném místě mimo zálohovací centrum. Tento způsob zálohy je nazýván jako D2D2T – Disk To Disk To Tape.

[21] Network Attached Storage
[22] Storage Area Network

Tento způsob dle Junka *„Využívá ty nejlepší vlastnosti disků a pásek, vytváří nákladově efektivní a komplexní řešení ochrany dat, řeší řadu nevýhod konvenčního způsobu zálohování, využívá v plné šíři rychlost zálohovacích mechanik a podstatně zkracuje zálohovací okno. Principem je prvotní záloha do diskového uložiště a následná další záloha na páskové zařízení. Data zálohovaná na disku mohou být velmi rychle obnovena, protože se nejedná o sekvenční zařízení, jak je tomu u pásek."* (Junek, 2013)

Samotný proces zálohování nazývaný také jako job má pevně stanovená pravidla a strukturu záloh. Jakým způsobem jsou zálohy prováděny, buď online formou bez výpadku nebo offline, kdy dojede k nedostupnosti služeb databází. V jakých intervalech a formátu (ne/komprimovaná data) dochází k archivaci na pásky nebo nastavení rotačního schématu dle retence jednotlivých typů záloh (roční, měsíční, týdenní) tedy za jak dlouho lze pásky přepsat. Tyto kritéria zpravidla odrážejí vlastnosti a typy záloh samotných, rozdělených do třech typů – Full, Incremental, Differential

*„**Plná záloha -** by byla ideálním typem pro všechna zálohování, protože je nejvíce komplexní a soběstačná. Nicméně takovéto zálohování zabere mnoho času, proto se příliš nevyužívá. Úplná záloha je často omezena na týdenní nebo měsíční periodu a je spuštěna převážně jen přes noc. Jedině plná záloha nám ale poskytuje možnost zcela a rychle obnovit všechny zálohované soubory, protože obsahuje kompletní data."* (Junek, 2013)

Inkrementální - neboli přírůstková je záloha, *„kde se na začátku vytvoří Plná záloha a to pouze jednou ihned na začátku zálohovacího procesu, poté další záloha už jen ukládá změny oproti ní (bude uložen pouze přírůstek takových dat, která se jakýmkoliv způsobem změnila oproti původní úplné záloze)."* (Junek, 2013) Velkou nevýhodou přírůstkové zálohy je obnovovací proces, kdy pro kompletní obnovu je zapotřebí poslední plná záloha a všechny přírůstkové. Proto je při tomto typu zálohy zapotřebí provádět po určitých intervalech znovu plné zálohy.

Diferenciální záloha – *„Obsahuje všechny soubory, které se změnily od poslední úplné zálohy. Výhodou diferenciální zálohy je, že se zkrátí čas obnovení v porovnání s plnou zálohou. Nicméně pokud bude diferenciální záloha prováděna velmi často, může její velikost být dokonce větší, než jak by tomu bylo u plné zálohy. Rozdíl mezi přírůstkovou a rozdílovou zálohou je takový, že zatím co přírůstková záloha ukládá pouze změny z hlavní zálohy a poté už jen změny z přírůstků, rozdílová záloha ukládá všechny soubory, které se změnily od poslední úplné zálohy. Pokud dojde k poškození některé z diferenciálních záloh, nemá to vliv na žádnou jinou diferenciální zálohu (zálohy na sobě nejsou závislé). Obnovení*

rozdílovou zálohou je rychlejší než obnovení přírůstkovou, protože jsou potřeba pouze dva soubory – poslední plná záloha a poslední rozdíl.“ (Junek, 2013)

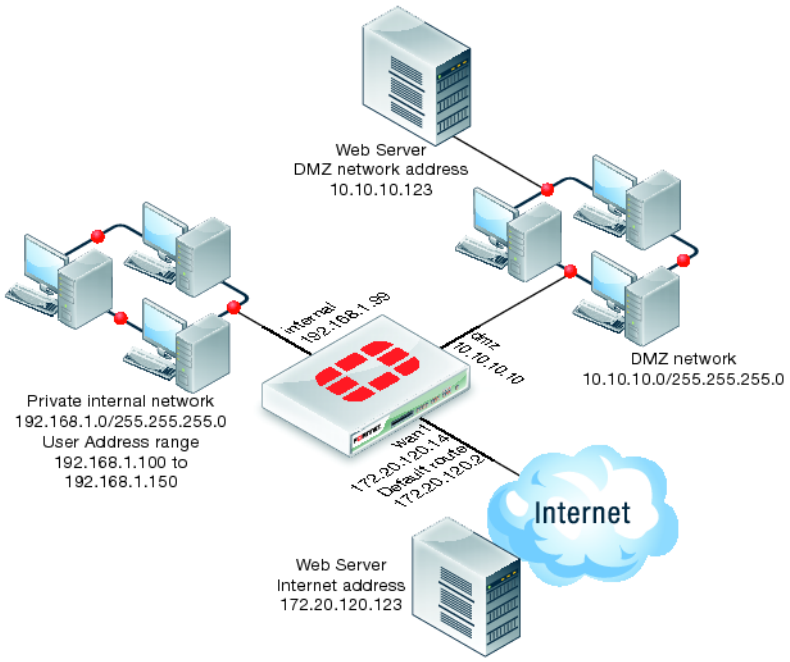
Protokol IEEE 802.1x – jedna z dalších bezpečnostních kontrol, neboli Framework navržený pro zajištění autentizace zařízení přistupujících do sítě LAN respektive WLAN a popřípadě zamezit přístupu do interní sítě neoprávněným zařízením. (Hon, 2012) Protokol zajišťující fyzickou bezpečnost pracující na linkové vrstvě ISO/OSI modelu s využitím ověřovacího protokolu EAP[23]. Základním principem protokolu je ověření nově připojeného zařízení do jakéhokoliv portu sítě, který je vždy před připojením v neautorizovaném stavu a pomocí po úspěšném ověření na ověřovacím serveru většinou RADIUS je změněn stav portu z down na up a zařízení je následně povolen přístup k určitým informacím. Protokol v případě zjištění snahy o neautorizovaný přístup učiní automatické odstřižení daného portu. Podle slov Boušky je na portu v neautorizovaném stavu povolena pouze komunikace pomocí protokolu EAPOL[24], STP[25], které postačují k zajištění ověření a udržování aktuálního stavu portů. (Bouška, 2007)

3.3 Demilitarizovaná zóna – DMZ

Pro zvýšení bezpečnosti celé infrastruktury a zpřístupnění firemní webové prezentace nebo poštovní komunikace směrem k vnějším sítím je zapotřebí tyto servery vyčlenit z vnitřního rozsahu sítě a vytvořit jim izolované a kontrolované prostředí. Pro tyto účely jsou v sítích vytvářeny demilitarizované zóny, vytvářené na firewallu s příslušným rozhraním. Je tedy zapotřebí pořídit firewall prvek disponující třemi zabezpečenými rozhraními – směrem do LAN, do WAN a do DMZ. V minulosti tyto kroky nebyly skoro vůbec řešeny, ostatně celkově problematika bezpečnosti začala nabírat na vážnosti až před několika lety, až postupem času se přešlo k řešení se dvěma firewally, které dnes plně nahradilo právě řešení s jedním firewall prvkem a třemi rozhraními.

[23] Extensible Authentication Protocol
[24] Extensible Authentication Protocol Over LAN
[25] Spanning Tree Protocol

Vytvořením DMZ je zajištěno nejen bezpečné zpřístupnění firemních veřejných serverů oddělených od interní sítě, ale také samotné zvýšení kontroly izolovaného prostředí pomocí auditu provozu nebo umístění detekčního systému. (Thomas, 2005) Základem je správná konfigurace jednotlivých rozhraní, směrování mezi nimi a nastavení přístupových pravidel protokolů pouze pro ty zařízení, které v zóně budou využívány. Pro ilustraci možného řešení je použito návrhu uznávané společnosti Fortinet v oblasti zabezpečení síťového provozu.



Obrázek 2: Znázornění DMZ
Zdroj: http://docs-legacy.fortinet.com/cb/html/FOS_Cookbook/Install_advanced/images/cb_install-dmz.017.1.1.png

3.4 Virtuální Privátní Sítě – VPN

Důvod, proč se začaly využívat služby VPN ve firemní komunikaci, vyústil z nemožnosti přímé a zabezpečené komunikace přes internet do vzdálených lokalit organizace. Řešení pomocí VPN přineslo velké snížení nákladů na provoz a komunikaci mezi lokalitami oproti dříve využívané technologii propojování a sdružování do WAN sítí. VPN můžeme provozovat pomocí firewallů, směrovačů nebo samotných serverů, kde je spuštěna softwarová verze služby. Technologie sama o sobě neposkytuje téměř žádné zabezpečení, a proto musí být téměř vždy začleněn do sítě s FW prvkem a dalšími bezpečnostními službami jako je zapouzdření IP, šifrovaná autentizace a šifrovaná datová část. Bez těchto charakteristik nelze považovat VPN spojení za důvěryhodné. Nyní tyto bezpečnostní prvky

krátce popíšeme, tak jak je uvádí Strebe. Při komunikaci přes veřejný internet, jsou nejčastěji pro VPN vytvářeny privátní zabezpečené tunely. Tímto způsobem zajistíme chráněnou komunikaci jednotlivých LAN sítí mezi sebou a zároveň nepřipustíme zachytávání komunikace zvenčí. (Strebe, a další, 2003)

- **Enkapsulace IP** – spočívá v zapouzdření jednoho paketu IP do druhého, který obsahuje jakýkoliv druh informace. Tento proces pomůže zkontaktovat požadovaného klienta v jiné nepřímo propojené LAN síti a vytvoří tím na síti dojem jedné velké sítě propojené směrovačem. Ve skutečnosti, ale tyto sítě odděluje mnoho bran a směrovačů.
- **Šifrovaná autentizace** – zajišťuje bezpečné ověření vzdáleně přistupujícího klienta a na základě stanovených pravidel používání klíčů a shody ověření lze klientovi povolit účast v šifrovaném tunelu. Dále je rozdělena na šifrování pomocí tajného klíče a šifrování na principu veřejného klíče.
- **Šifrovaná datová část** – jejímž hlavním úkolem je zašifrovat vložená dat obsahu jako celku, například s využitím SSL protokolu a zároveň při šifrování nedochází k utajení informací v hlavičce, takže lze z ní zjistit podrobnosti o síti.

Při zřizování VPN spojení lze využít jednu ze tří základních konfigurací reflektující počet klientů vstupujících do spojení, jak je uvádí Strebe. (Strebe, a další, 2003) Za prvé je možné nakonfigurovat síť s okruhy, kde má každý klient s každým dalším přímé bezpečnostní spojení. Za druhé využití konfigurace do hvězdy, které funguje na principu propojení každého účastníka jednou bezpečnostní relací do centrálního směrovače VPN, který disponuje bezpečnostním spojením s každým dalším VPN prvkem. Poslední variantou propojení pomocí VPN je kombinace dvou předcházejících konfigurací nazývanou také jako hybridní VPN. Perkins podotýká, že v praxi většinou vznikají, i nezáměrně hybridní spojení. I přesto zastává názor na využívání hvězdice z prostého důvodu: vzniká tím centrální správa a konfigurace všech klientů s podmínkou, příslušné přenosové kapacity.

3.4.1 Typy VPN

Typově jednotlivá VPN spojení rozčlenit dle typu založení, tedy založené na serverech, firewallech nebo směrovačích v podobě SW nebo HW konfigurace. Každá z variant poskytuje funkční řešení a záleží pouze na zřizovateli, která varianta je pro jeho řešení nejvhodnější. Například softwarová VPN založená na serveru poskytne ideální zázemí

pro malé firmy s využitím bezpečnostních protokolů. Oproti tomu VPN založená na směrovačích je nejlépe uplatnitelná v rozsáhlých sítích, jako jsou například univerzitní kampusy. Kde se vyskytuju několik propojených směrovačů zajišťujících interní směrování v jednotlivých segmentech sítě. A právě s využitím funkce zapouzdření, kterou jsme si popsali již dříve, snadno nakonfigurujeme bezpečné VPN spojení mezi jednotlivými segmenty sítě. Poslední variantou VPN spojení založeného na firewallu poskytne organizace zvýšenou formu zabezpečení v podobě silné autentifikace jednotlivých zařízení s detailním výpisem z logu spojení. A vzhledem k široké funkčnosti FW prvků, kterým by měla disponovat každá bezpečnostně smýšlející organizace, lze snadno nakonfigurovat zabezpečené přenosové tunely pro VPN spojení.

3.4.2 Způsoby využití VPN

Pro potřeby organizace lze definovat tři základní typy využití VPN technologie. Jak uvádí Shinder, první možností je umožnění vzdáleného přístupu svým zaměstnancům, kteří jsou mimo firemní prostory, například pracujícím z domova popřípadě na pracovní cestě. Pro tyto účely je důležité zajistit korektní konfiguraci klientského PC s podporou VPN klienta a šifrovacích protokolů používaných na straně serveru. Po použití příslušných protokolů například MPPE[26] dojde k ověření a navázání bezpečného spojení mezi organizací a klientem. V pracnosti asi nejjednodušší varianta spojení, ale o to větší musí být kladen důraz na reálné zabezpečení a šifrování komunikace. (Shinder, 2003)

Druhým type k vytvoření VPN spojení do organizace je takzvaný extranet, ke kterému mají povolen přístup jen definované skupiny – zaměstnanci, klienti nebo obchodní partneři. Již podle názvu lze rozpoznat využití, kdy z interní sítě je vyčleněna oblast pro sdílení určitých dokumentů pro dané skupiny. Pomocí klasického přístupu a autentifikace přes webové rozhraní můžeme operovat s firemními prostředky s využitím podpůrných standardů jako je HTML, XML nebo OBI.[27]

Poslední a velice často využívanou variantou je využití VPN k propojení vlastních pobočkových lokalit mezi sebou popřípadě propojení do centrální sítě. Základem pro nasazení této varianty je využití modelu směrovač – směrovač, kdy každý jeden má nastavené rozhraní, jak pro LAN, tak pro WAN. Musí být provedena konfigurace směrovacích tabulek a vlastního

[26] Microsoft Point-to-Point Encryption Protocol
[27] Open Buying on the Internet

směrování mezi routery s příslušnými adresami založené například na routovacím protokolu OSPF[28]

3.4.3 VPN protokoly

Tuto podkapitolu lze snadno rozdělit na dvě hlavní protokolové části, kde se protokoly dělí na „tunelové," které zajišťují samotné vybudování VPN tunelu a „šifrovací," které již podle názvu zajišťují bezpečnost přenášených dat mezi lokalitami. Níže v textu je popsán výběr několika typových protokolů z obou směrů, jak je uvádí Shinder. (Shinder, 2003)

- **Tunelové protokoly** – jejichž úkolem je zapouzdření dat z hlavičky originálního protokolu, především se jedná o tyto následující:
  - Point-to-Point Tunneling Protocol (PPTP) – patří mezi první tunelové protokoly, ale v dnešní době je již nahrazen jinými, níže uvedenými protokoly, protože byl v roce 2012 prolomen a není tedy možné jej považovat za bezpečný. Pro šifrování byl nepřímo nucen používat MPPE, který je popsán níže. Ve své podstatě měl problém s průchodem skrze firewally a byl ohrožován slabými hesly uživatelů.
  - Layer 2 Forwarding (L2F) – protokol od společnosti Cisco poskytuje hlavně autentizaci koncových bodů vytvořeného tunelu. Ve spojení PPTP od společnosti Microsoft vznikl další níže uvedený protokol, přebírající výhody obou.
  - Layer 2 Tunneling Protocol (L2TP) – mezi jeho hlavní výhody patří podpora pro vytvoření více oddělených tunelů mezi klienty, dokáže komprimovat hlavičky, již zmíněná autentizace tunelů a dokáže nepracovat na IP sítích, ale využívá virtuální obvody např. FrameRelay.
  - Internet Protocol Security (IPSec) – složen z dvou dílčích protokolů AH[29] a ESP[30], které při vzájemné kombinaci zajišťují plnou integritu přenášených dat. AH ručí za ověření dat a autentifikaci klienta po celou dobu přenosu a vzniká v okamžiku, kdy paket opouští koncový bod tunelu. Za to ESP ručí za šifrování pomocí 3DES[31] algoritmu a zapouzdření hlavičky.

[28] Open Shortest Path Protocol
[29] Authentication Header
[30] Encapsulating Security Payload
[31] Triple Digital Encryption Standard

- Secure Shell 2 (SSH2) – striktně založen protokol na silném šifrování a autentizaci primárně určen pro OS Linux a Unix. Při komunikaci vytváří takzvaný „Circuit-level Gateway," který pracuje na relační vrstvě OSI modelu. Tím takzvaně skrývá interní síť, jelikož poslaná data se tváří jako že byla odeslána přímo z výchozí brány.
- Crypto IP Encapsulating protocol (CIPE) – využívá jej kernel Linuxu, právě k vytvoření tunelu zabezpečeného na síťové vrstvě, některé zdroje uvádí, že je mnohem jednodušší a efektivnější než IPSec.

- **Šifrovací protokoly** – tvoří nezbytnou komponentu k vytvoření bezpečného spojení pomocí tunelu.
  - Microsoft Point-to-Point Encryption (MPPE) – šifrovací protokol vytvořený k využívání pro protokol PPTP, který umožňoval použít i 128-bitové šifrovací klíče.
  - IPSec šifrování – využívá převážně kryptografický algoritmus 3DES v kombinaci s klíči, což ve výsledku zajišťuje velmi kvalitní zabezpečení dat. *„Deffie-Hellmanův algoritmus umožňuje bezpečnou výměnu sdíleného klíče, aniž by byl klíč samotný odeslán skrze síťové připojení."* (Shinder, 2003)
  - VPNd šifrování – protokol postavený pro Linuxové platformy používající šifrovací algoritmus Blowfish. Vyznačuje se svou rychlostí a dostupností zdrojového kódu, který používá proměnnou délku klíčů od 32 do 448 bitů.
  - SSH šifrování – ustavuje bezpečnou komunikaci mezi vzdálenými klienty, šifrováním pomocí tajného klíče a tím pádem tento klíč musí znát obě strany.

3.4.4 Zabezpečení VPN

Jeden metodický postup, jak zabezpečit komunikaci ve virtuální privátní síti byl již zmíněn v úvodu této kapitoly a zde přidáme další tři prvky zajišťující ochranu. Vlastnosti bezpečnostních komponent popisuje ve své knize Shinder především takto:

- **Autentizaci –** neboli ověření identity klienta a jeho PC při vytváření VPN relace s užitím tunelu na druhé vrstvě s bezpečnostním IPSec šifrováním,

založeného na výměně certifikátů. Autentizace je také závislá na použití dané metody ověření jako například: EAP[32], TTLS[33], IKEv2[34], MD5[35]

- **Autorizaci –** spočívá pouze v nastavení omezení přístupových pravidel a práv pro definované uživatele, kterým bude přístup povolen a ostatním nikoliv.
- **Šifrování –** je nejdůležitější komponentou pro vytvoření VPN relace a následné komunikace, protože zajišťuje šifrování interních dat přenášených po veřejné síti, tak aby zranitelnost přenosu byla téměř nulová.

3.4.5 Doporučení při využívání VPN

Využitím nejlepších poznatků přímo z praxe, lze zamezit tvorbě bezpečnostních mezer, při dodržení následujících doporučení, která sepsal Perkins. (Strebe, a další, 2003)

- **Použití kvalitního FW** – zajistí možnost centralizovat všechny bezpečnostní funkce do jednoho zařízení a tím mnoho násobně zvýšit celkovou bezpečnost řešení. V opačném případě je zapotřebí otevřít spojení pro VPN SW a zároveň tím umožnit i vstup útočníka.
- **Zabezpečení OS** – pro zajištění bezpečného ověření přistupujících klientů, je zapotřebí aby měli nainstalovaný prověřený a aktuální systém bez virů s nastaveným systémovým firewallem.
- **Jednotný ISP**[36] - poskytuje vyšší rychlost i zabezpečení koncové uživatel připojené do VPN sítě propojené tunelem do internetu, protože poskytovatel udržuje komunikace v maximálním možném objemu pouze na své vlastní síti a tím pádem se vyhne zácpám na veřejně přístupných ústřednách.
- **Filtrace paketů od neznámých klientů** – tímto doporučením je naznačen postup filtrace paketů, založené na zamítnutí všech počítačů vyjma seznamu povolených přistupujících klientů.
- **Dodržení šifrování a zabezpečené autentizace** – je doporučováno využívat funkcionalitu veřejných klíčů, které jsou oproti jednoduché autentizaci sdíleného tajemství mnohem bezpečnější. A vyhnout se konfiguraci VPN

[32] Extensible Authentication Protocol
[33] Tunneled Transport Layer Security
[34] Internet Key Exchange
[35] Message-Digest 5
[36] Internet Service Provider

šifrované pomocí tajného klíče, k jehož vytvoření se využívá síťového jména a hesla, čehož snadno útočník využije a následně se dostane do sítě.

- **Využití komprimace** – je v zásadě důležité provést před samotným šifrováním dat, protože poté již komprimace neprobíhá korektně a celý proces snížení velikosti proudu datového balíku bude nepoužitelný pro přenos většího objemu dat po sítí.

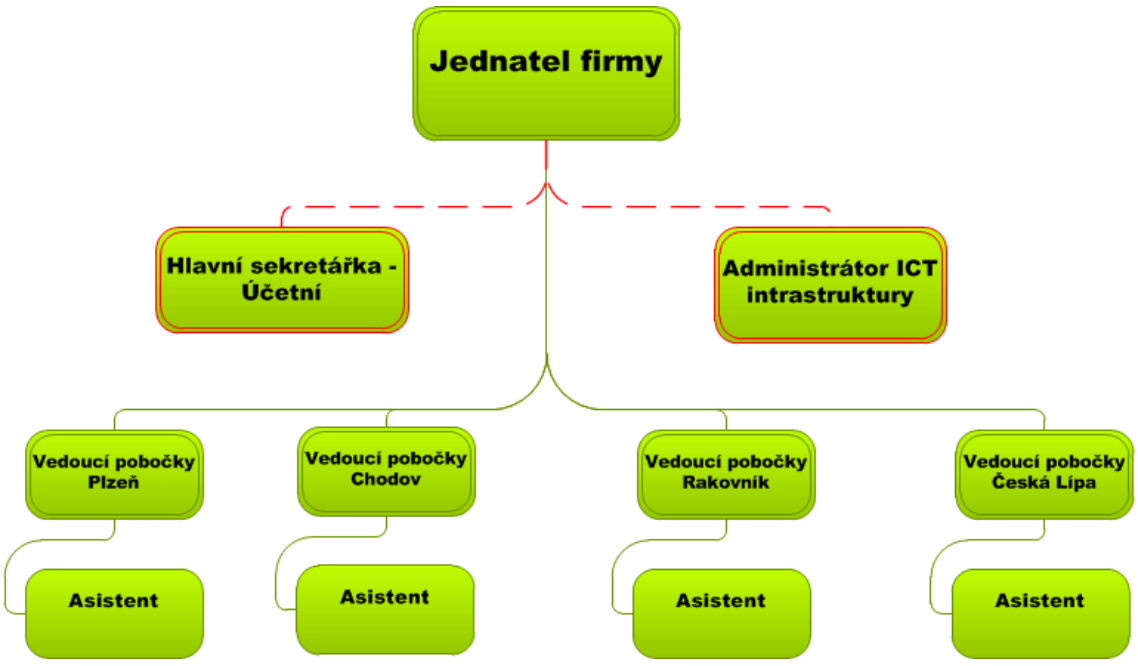
Pro závěrečné shrnutí nejlepšího využívání VPN poznamenal Perkins. *„Maximální pružností ve firewallech a softwaru pro vzdálený přístup dosáhnete, pokud zvolíte řešení VPN využívající IPSec + IKE, u nichž bylo otestováno, že spolu dobře spolupracují.“ (Strebe, a další, 2003)*

4. Praktická část

4.1 Představení společnosti

Pro diplomovou práci byla vybrána malá firma zabývající se velkoobchodní činností a přímým prodejem obuvi a kožených výrobků. Společnost byla založena již v roce 1994 pod obchodním názvem OBUV-DAHL-TOK s.r.o. s obchodním sídlem v Praze. V současné době zaměstnává 11 zaměstnanců. Většina z nich obstarává bezproblémový chod jednotlivých poboček, které se nacházejí v Plzni, České Lípě, Chodově a Rakovníku. Ke svému podnikání firma využívá také služeb internetu, kde se prezentuje a provozuje vlastní e-shop.

Pro další představení firmy jsem vytvořil organigram, kde se prolíná stav minulý se stavem aktuálním. Jak může vidět níže, aktuálně jsou v organizační struktuře zahrnuti i další dva zaměstnanci a to Účetní a Administrátor. Jejich pozice byly doposud zastávány externími pracovníky.



Obrázek 3: Aktuální organigram organizace
Zdroj: Vlastní tvorba v aplikaci MS Visio

V prostorách sídla v Lužné u Rakovníka byla doposud pouze kancelář a nedaleký sklad zboží čítající tisíce položek. Odtud jsou požadované kusy zboží distribuovány na pobočky popřípadě přímo zákazníkovi. Pro distribuci firma využívá služeb nasmlouvaných českých dopravců. Většinu skladových zásob si majitel nechává šít dle světových trendů světových značek z kvalitního materiálu od pracovníků z jihovýchodních zemí. V nemalé

míře firma zaměřuje své působení na zahraniční trhy a vytváří komunikaci se zahraničními partnery dodávající luxusní zboží do naší země.

4.2 Analýza a popis současného stavu společnosti

Upřesnění na začátek, již v této analytické části se budou objevovat zmínky o centrále potažmo serverové místnosti, která před zahájením diplomové práce ještě neexistovala. Z provedených průzkumů aktuálního stavu fungování firmy v oblasti IT vyplývají základní pilíře, které je zapotřebí zpevnit popřípadě od základu postavit. Ve své podstatě tyto pilíře navazují i na původní požadavky změn, které byly před začátkem projektu projednávány s jednatelem firmy. Veškeré aplikované analýzy odhalily obrovské množství nedostatků ze všech oblastí ICT až je neuvěřitelné, že doposud nedošlo k žádným závažným ztrátám na firemních datech apod.

Vzhledem k narůstajícím problémům stávajícího IT řešení firmy pomocí outsourcingových služeb dospěla firma k závěru vlastní správy a administrace technologického zázemí. Z toho vyplývá i skutečnost, že firma doposud neměla vlastní centrální prvek ani technickou místnost neboli serverovnu. Z pohledu IT se jedná o zcela decentralizované prostředí. Kde jednotlivé pobočky nemají přímý nebo aktuální kontakt s centrálou potažmo skladem. Každá pobočka disponuje tiskárnou a jedním PC, které je připojeno do internetu. Tiskárny jsou napřímo napojená na PC pomocí USB rozhraní bez další možnosti síťového připojení. Oba technické prostředky jsou více jak 4 roky staré bez pravidelné údržby a s propadlými záručními listy. Takže bude uvažováno nejen pořízení aktivních prvků, ale i obnovení stávající techniky na pobočkách.

4.2.1 Správa klientských stanic

Uživatelé mají na stanicích nastavena administrátorská práva, takže mohou cokoliv a kdykoliv nainstalovat bez vědomí a souhlasu nadřízeného. Dalším pochybením je skutečnost, že dva zaměstnanci pobočky přistupují k jednomu PC pod jedním uživatelským jménem a heslem. Tím pádem nelze snadno dohledat kdo, co a kdy udělal. Také je to zapříčiněno skutečností chybějících pravidel a centrálního dohledu nad uživateli a jejich stanicemi. Pokud uživatel například stanici zaviroval nebo se poškodila nějaká hardwarová komponenta, byla sjednána jednorázová oprava. Tito technici nebyli nijak nasmlouvaní a už vůbec neměli podepsané SLA. To ve výsledku znamenalo i několika denní výpadek služeb na dané pobočce. Ani při nákupech techniky nebyl brán zřetel na záruční a servisní

služby od výrobce což by při vadném hardwaru mohlo opravu mnohem více urychlit. V případě dlouhodobějšího odstavení stanice je k dispozici jedno náhradní PC, které se muselo převést z centrály na dané místo, aby se firma vyhnula výpadku pobočky. Tím pádem i ztráty zisku.

4.2.2 Připojení do internetu

Připojení jednotlivých poboček do internetu je zajištěno místními poskytovateli dle možností lokality bez zajištění symetrické linky. V tomto firemním prostředí ani nelze mluvit o jednotlivých LAN sítích, jelikož je využito pouze jedno přípojné místo pro přímé připojení PC do poskytovatelského routeru, který je předmětem smlouvy o poskytování služeb a dále do internetu. Zařízení jsou používána v tovární konfiguraci bez dalších bezpečnostních opatření.

Obchodní komplex Česká Lípa, jehož součástí je jedna z poboček firmy, poskytuje v rámci vnitřní sítě celého centra připojení k internetu od poskytovatele Ralskonet, který za cenu 440 Kč/měsíc garantuje rychlost připojení 24 Mbit/s a jednu pevnou IP adresu.

Na pobočce v Chodově je poskytovatelem firma Air Telecom, zajišťující přímé propojení do internetu přes pevnou IP adresu na vlastněném ADSL routeru s rychlostí 20 Mbit/s a paušální cenou 490 Kč.

Poslední dvě lokality jsou propojeny do internetu pomocí Wi-Fi rozhraní, ale na pobočkách je připojení řešeno pomocí datových UTP kabelů. V lokalitě Rakovník disponují připojením s rychlostí 20 Mbit/s jež zajišťuje poskytovatel CB Computers v.o.s. za cenu 498 Kč bez přidělení pevné IP adresy.

Plzeňská pobočka je zajištěna připojením od UPC s rychlostí 40 Mbit/s přidělenou pevnou IP adresou a připojena do poskytovatelského Wi-Fi routeru za cenu 449 Kč za měsíc.

4.2.3 Technické vybavení firmy a hostované servery

V majetku firmy je jedno výkonnější zařízení, umístěno v sídle firmy výhradně pro potřeby majitele, který řídí celý chod firemního prostředí. Jako jediné zařízení bylo v průběhu let aktualizováno do dnešní podoby. PC od společnosti Hewlett-Packard s procesorem Intel Core i5 4590S Haswell, pamětí 4 GB, grafickou kartou Intel HD 4600, 500 GB HDD a systémem Windows 8.1 Pro 64-bit.

Na pobočkách jsou využívány notebooky s průměrnou délkou stáří okolo 5 let značky Acer. Typově se jedná o 14 palcový Acer Aspire 4349 s procesorem Intel Celeron B800 a frekvencí 1,5 GHz, operační pamětí pouze 1 GB, integrovanou VGA Intel HD grafikou

a pevným diskem 320 GB. Bohužel na noteboocích je stále používán již nepodporovaný operační systém Windows XP Professional SP3.

Před spuštěním projektu docházelo ke spouštění nového e-shopu podporující moderní technologie pro tvorbu webu a zjistilo se, že nám poskytované serverové prostředky hostingových služeb jsou nedostačující. Jelikož dříve s tímto poskytovatelem nebyly nastaveny žádné smluvní podmínky pro servisní a reakční doby, bylo velkým problémem zajistit aktualizace prostředí serveru. Který disponoval jedním procesorem Intel Xeon L5630 s celkem 8 vlákny, operační pamětí 32 GB DDR3, dvěma SAS disky o kapacitě 146 GB a operačním systémem Linux CentOS 5.11 a neaktualizovaným aplikačním prostředím podporující nové webové technologie na straně serveru. Při sdílení serverových prostředků s mnoha dalšími zákazníky hostingu, to vyvolalo delší odezvy, než které byly dříve zaručovány.

4.2.4 Aplikační prostředí

Softwarové vybavení firmy také nepatřilo k nejaktuálnějším a postrádalo sofistikované aplikace podporující a usnadňující samotný prodej a podnikání. Téměř na všech firemních počítačích byly provozovány MS Office ve verzích 2003 nebo 2007 s nepřenositelnou licencí na jiné zařízení neboli OEM[37] licence pořízené zároveň s koupí notebooků. Vyplývající ze samotného licenčního ujednání MSLT[38] společnosti Microsoft. Ve výsledku to opět znamená další nákup kancelářského balíku a také nemožnost využít „bezplatný upgrade“ na novější verzi. Ještě horším zjištěním je využívání již nepodporovaného systému MS Windows XP SP3, alespoň chráněného antivirovým programem od společnosti AVG ve verzi business edition. V systému Windows je zapnutá standartní brána firewall, což lze považovat za malý bezpečnostní plus. Pro mailovou komunikaci je využíván volně dostupný mailový klient společnosti Seznam.cz s vytvořenou firemní schránkou, do které pod jedním uživatelským jménem a heslem přistupují všichni zaměstnanci.

4.2.5 Bezpečnost dat i celého systému firmy

Otázkou bezpečnosti firemních dat se dnes musí zabývat každý, kdo se pohybuje v komerčním prostředí. Bohužel analýzou bylo opět zjištěno, že došlo k obrovskému až fatálnímu pochybení. Samotná firma zálohu svých dat prakticky neprováděla a v každé lokalitě měla nekonzistentní údaje. Největší část dat samozřejmě schraňuje u sebe jednatel

[37] Original Equipment Manufacture
[38] Microsoft Software License Terms

firmy, který občas na doporučení externího IT technika provedl zálohu na externí disk. Řádově se jednalo o archivaci jednou za rok. Jediným pravidelně zálohovaným aktivem firmy byly webové stránky a k nim připadající databáze, jejichž zálohu zajišťoval poskytovatel hostingových služeb, k čemuž se zavázal při sepsání spolupráce. Přitom během každodenního provozu vzniká velké množství důležitých i citlivých dat nejen v rámci firmy, ale i údaje o zákaznících jako například:

- Reklamační protokoly
- Objednávkové listy
- Registrace zákazníků
- Dodavatelsko-odběratelské smlouvy apod.

Z pohledu dalších bezpečnostních rizik nebyla řešena ani problematika náhradní dodávky elektrické energie pomocí UPS[39] stanic nebo zabezpečení síťového provozu. Ani uschování externích disků s roční zálohou dat nebylo provedeno dle bezpečnostních pravidel a umístěno do bezpečnostní schránky.

4.2.6 Souhrnná analýza rizik spojených s provozem

Z výše uvedených analýz firemního prostředí, vykrystalizovalo několik rizikových oblastí, které by v rámci projektu měly být úplně odstraněny nebo alespoň minimalizovány na takovou úroveň, že by je při auditních šetření auditor neměl považovat za prvky ohrožující jak firemní prostředí, tak potencionálního zákazníka.

	Riziko	Možné Důsledeky	Míra vzniklého rizika	Pravděpodobnost výskytu
1	Výpadek el. Energie	Ztráta aktuální dat	Vysoká	80%
2	Nekontrolovaná aktivita uživatelů	Zahlcení nepotřebnými daty	Střední	100%
3	Decentralizované prostředí	Nemožnost přímé komunikace	Střední	100%
4	Nezabezpečená síť a připojení do internetu	Napadení IT útočníkem (Hacker)	Vysoká	70%
5	Zastaralá technika	Náhlý a dlouhodobý výpadek služeb	Střední	70%
6	Neaktualizované aplikační prostředí	Napadení HW virem	Vysoká	90%
7	Chyby uživatelů	Vymazání dat	Vysoká	50%
8	Chybějící zálohovací systém	Ztráta dat	Vysoká	90%

Tabulka 1: Výčet rizikových faktorů
Zdroj: Vlastní tvorba

4.3 Návrh řešení nové instalace prvků a centralizace služeb

Po provedení hloubkové analýzy vznikly jednotlivé závěry, které byly předloženy jednateli společnosti k prostudování. Následně byly projednávány jednotlivé varianty nových

[39] Unit Power System

řešení. Byla vysvětlena rizika stávajícího stavu a nastíněna nová řešení a postupy, jak docílit efektivnějšího a bezpečnějšího provozu firmy. Z pohledu distribuční firmy je zapotřebí zajistit aktuální zabezpečená data a bez výpadkový chod celé infrastruktury tedy dostupnost jednotlivých zdrojů kdykoliv.

Na vybavení centrální místnosti byla doporučena firmu Pollux s.r.o., kde se dodavatel zaručil za kvalitu a včasné dodání HW prostředků a vybavení celé serverovny. Firma disponuje mnoha kvalifikovanými a renomovanými subdodavateli s výbornými smluvními podmínkami na distribuované zboží. Na toto konto byla sjednána i smlouva. Již tato smlouva byla podepsána dle nastavených kritérií SLA, k jejichž plnění dodavatelská firma zavázala i subdodavatele. Bylo dohodnuto rozdělení hlavních projektů, jejich termínu realizace a vyčleněny finanční prostředky na realizaci celého projektu. Projekty jsou postupně popisovány jak v průběhu prací, tak v navrhovaných řešeních, ke kterým budování nové infrastruktury teprve dospěje. Rozdělení hlavních projektů je následující:

- **Vybudování centrální místnosti – serverovny**
- **Zřízení datového připojení a propojení poboček**
- **Rozvržení a nastavení bezpečnostní topologie**
- **Příprava vzdálených lokalit**
- **Návrh interního bezpečnostního dokumentu firmy**

Na pozadí těchto projektů je důležité připravit podklady pro rozvázání jednotlivých smluv s externími dodavateli či poskytovateli hostingu. A dále splnit jeden ze základních požadavků na nalezení odpovídající a zkušené osoby, která převezme odpovědnost za správu nové centralizované ICT infrastruktury. S novým administrátorem bude sepsána běžná pracovní smlouva na dobu neurčitou a dále připojená smlouva o přebrání veškeré zodpovědnosti za infrastrukturu, jež zavazuje administrátora k dodržování bezpečnostních pravidel sepsaných v dokumentu „Bezpečnostní politika firmy.“ V takto malém firemním prostředí bylo přistoupeno na to, že nový administrátor se rovnou posune na druhou nejvyšší pozici dle organizační struktury, aby právem mohl projednávat jednotlivá nastavení, kárná řízení a postupy přímo s jednatelem bez nutnosti dalších přidružených osob.

4.4 Vybudování centrální místnosti - serverovny

Prvotním projektem a zároveň nejdůležitějším bylo vybudovat serverovou místnost pro uložení síťových prvků, serverů, diskových polí, záložních zdrojů energie a doplňujících

bezpečnostních prvků pro nově budovanou ICT infrastrukturu firmy. Dle přání jednatele byla tato místnost zřízena v sídle firmy ve sklepních prostorách. Které samozřejmě musely projít zásadními stavebními úpravami. Při jednotlivých jednáních bylo zjištěno, že při povodních nehrozí zaplavení objektu, doposud k tomu nedošlo ani při velkých povodňových stavech v předešlých letech.

Předmětem této práce nebylo zajištění a provedení stavebních prací, proto jsou zde jen popsány kroky, které byly učiněny. V místnosti bez oken o rozloze 9 m^2 bylo zapotřebí zhotovit zdvojenou podlahu pro případ zaplavení místnosti spodní vodou a s příslušnou nosností minimálně 450 kg/m^2, protože se hmotnost samotného racku a UPS jednotky naplněné bateriemi pohybuje okolo 250 kg. Mezi podlažní prostor je také využit pro elektrické vedení svedeného do společné chráničky pod podmínkou, že veškerá zakončení a spojení jsou realizována mimo tento prostor. V místnosti využité kalcium-sulfátové podlahové desky jsou navrženy s požární odolností kolem 30 min dle normy ČSN EN 13501-1 a dále bylo zapotřebí ji vybavit protipožárními dveřmi. V hlavní rozvodné skříni provést instalaci slaboproudých a silnoproudých rozvodů. Do podružného rozvaděče bylo přivedeno napětí 3 x 400/230 V 50Hz s jištěným přívodem 16A/3F, které je dále rozvedeno do racku a zakončeno v distribučních lištách PDU plus zajištění podružného měření, přepěťové ochrany a proudové ochrany. Po těchto úpravách mohlo dojít k samotnému vybudování plnohodnotné serverovny. Jejíž součástí je racková skříň, zdroj záložní energie – UPS, klimatizační jednotka, zhášecí nádoby a zabezpečovací technika.

Dle doporučení byl zakoupen oboustranně perforovaný, uzamykatelný rack o typizované velikosti 36U (Š x V x H – 0,56 x 1,7 x 0,8) ve kterém jsou umístěny veškeré technické prostředky i s jednotkou UPS. Velikost skříně byla vybrána záměrně, abychom docílili dostatečné prostoru a cirkulace vzduchu i mezi jednotlivými prvky a tím se vyhnuli nežádoucímu zvyšování teploty. I když je v místnosti umístěna klimatizační jednotka, v případě kdy jsou prvky od sebe rozmístěny s minimální vzdáleností a při nepřetržitém běhu může docházet k přehřívání. Bezpečnostní prvky v místnosti jsou rozděleny do dvou okruhů: vnější a vnitřní. V každém z těchto okruhů jsou nainstalována příslušná čidla zaznamenávající aktuální stav o teplotě, požáru, neoprávněném vstupu nebo záplavové čidlo také jednotlivé prvky umístěné v racku obsahují alert agenty hlásící jakékoliv vychýlení ze standartních hodnot. Všechna tato upozornění jsou odesílána na dvě nejvyšší osoby ve firmě pomocí mailu nebo GSM brány na telefon dle stanovených pravidel v dokumentu bezpečnostní politiky.

Do vnitřního okruhu patří zhášecí systém, protože jsou přímo do racku nainstalovány zhášecí hadice a senzory od SHZ umístěného mimo rack, který při indikaci zvýšené hladiny kouřových látek sepne zhášecí mechanismus napojený na EPS[40], zároveň dojde k automatickému odstavení UPS zdroje a vypuštění hasiva do rackového prostoru. Systém obsahuje dvě opticko-kouřová čidla propojených do dvou smyčkové závislosti pro vyloučení planých poplachů. Je ošetřen i případ, kdy může dojít ke kontrolovanému vypnutí systému pomocí centrální ústředny, pokud kouř nebo zvýšená prašnost v místnosti je způsobena omylem. V závislosti na ochraně silnoproudých rozvodů je naistalován i lokální AHS FK1A2 pro elektrické rozvaděče. Obsahuje speciální teplo citnou hadičku, která v případě zvýšení teploty na 120 °C praskne a zaplaví prostor hasivem. Systém FK-Komplet obsahuje hasící látku HFC 236fa byl nainstalován firmou Klika-BP s.r.o. a jí bude pravidelně revidován v souladu s vyhláškou č. 221/2014 Sb. *Hasicí látky jsou z hlediska ochrany životního prostředí schválené příslušnými certifikačními orgány, kdy se jedná o nevodivé, nekorozní a nehořlavé hasivo s nulovou hodnotou ODP vlastní výroby.* (Klika-BP, 2015)

Osazení rackové skříně prvky, si lze prohlédnout na obrázku č. 5 v přílohách. Tato podkapitola popisuje samotné osazení podrobněji. Od spodu jsou usazeny nejtěžší části, jako jsou baterie k UPS a samotná jednotka UPS, která bude zajišťovat nepřerušované napájení celé místnosti. Pořízeno bylo zařízení od firmy Eaton 9130i s výkonem 2kVA / 1,8kW s jedním externím modulem baterií. Při předpokládaném zatížení, které by nemělo překročit hodnotu 3,8kW, bude zařízení UPS schopné při výpadku rozvodné sítě zabezpečit čas běhu kolem 63 minut při zatížení prvků na 75% a při sníženém zatížení 50% lze zabezpečit běh až na 95 minut. UPS je vybavena management rozhraním na platformě ETHERNET pro notifikaci o výpadcích a stavu UPS. Z jednotky jsou vyvedeny dvě zařízení PDU osazeny 16A zásuvkami každá po 8 vstupech typu C20 / C13 / C19 pro připojení ostatních prvků do zdroje energie. Zásuvky na PDU[41] jsou v konstrukčním provedení, které ve spojení se speciálními výstupními napájecími kabely ochrání jednotku proti náhodnému vytažení z PDU lišty. V grafickém znázornění jsou PDU umístěna v čelní části racku, ale reálně jsou nainstalovány do boků v zadní části racku pro lepší přístupnost. UPS jednotka je přímo propojena s hlavní rozvodní skříní na silnoproudý přívod, vyvedený z podlahových prostor do rackové skříně. Vzhledem k tomu, že nejsou na serverovnu a systém jako takový kladeny

[40] Elektronický požární systém
[41] Power distribution unit

požadavky o dostupnosti 24x7x365. Byl proto tento záložní zdroj navržen pouze pro potřeby bezpečného odstavení veškerého zařízení bez rizika ztráty dat při krátkodobém výpadku.

Důležitou částí je diskové pole Fujitsu Eternus DX60 S3 v provedení 2U, disponující dvěma řadiči a HBA[42] kartami potřebných k propojení s FC Switchem a dále 4 GB cache paměti a dynamickými vlastnostmi, jak pro výběr jednotlivých disků v podobě všech dnes známých typů, tak rozšiřitelnosti na větší kapacity přidáním dalších polic. Pole nabízí typické úrovně RAID[43] replikací pro vyšší zabezpečení dat v podobě (0,1,1+0,5,5+0,6) a také nové kontrolní prvky jako je cache protection nebo data block guard V řešeném návrhu bylo pole osazeno 10 disky typu SAS v 3,5“ provedení s rychlostí otáček 10 000 a kapacitou disků 900 GB. Pro co nejlepší využití pole a poskytnutí vysoké míry zabezpečení dat byla realizována SAN[44] síť dále připojena do clusterové provedení celého systému. Díky dvěma řadičům a nastavené replikaci mezi nimi lze pole logicky rozdělit na dvě části primary a backup. A v návaznosti na cluster tím zajistit nepřerušený chod souborových služeb v případě, kdy dojde k výpadku hlavní diskové části. A to automatickým překlopením na záložní část bez nutnosti zásahu administrátora. Redundantním optickým propojením pole a páskové knihovny pomocí FiberChannel zajišťující rychlost 8 Gbit/s a FC Switche vznikla SAN, která v napojení na cluster vytvořila stabilní systém pro souborové služby.

Nejdůležitějším prvkem a srdcem celé infrastruktury jsou dva výkonné servery Fujitsu Primergy RX1330 M1 v provedení 1U. V hardwarové konfiguraci se čtyř jádrovým a osmi vláknovým procesorem Intel Xeon E3-1271v3 jehož takt je 3,60 GHz na frekvenci 1 600 MHz, využívající cache paměť o velikosti 8 MB a RAM paměť o čtyřech slotech po 8 GB DDR3. Servery jsou vybaveny čtyřmi sloty pro připojení pevných disků na rozhraní SAS i SATA s možností vložení disku za běhu serveru: Hot-plug. Úložný prostor budou všechny serverové stanice čerpat z připojeného diskového pole. Pro každý server byl nakonfigurován příslušný diskový prostor dle předpokládaného využití a nastavena priorita přístupu. V budoucnu není problém při zvýšení využívaných kapacit doplnit další disky do pole a tím zajistit stabilitu výpočetního sytému. Tímto krokem se urychlí i proces zálohování systému. Komunikační rozhraní zajišťují dva síťové adaptéry založeny na PCIe 2.1 sběrnici o rychlosti 10 Gbit/s využívající k propojení osm SFP modulů.

[42] Host Bus Adapter
[43] Redundant Array of Independent Disks
[44] Storage Area Network

Výkonnost těchto dvou fyzických serverů bude využita pro vytvoření dalších šesti virtuálních serverů, přičemž všichni budou postaveni na operačním systému Windows 2012 R2. Virtualizace pomocí technologie Hyper-V umožní efektivní rozdělení serverových prostředků pro vytvoření kořenových serverů. Jako je například poštovní, proxy, databázový, antivir, tiskový a backup server.

Po instalaci serverových verzí systému Windows bylo zapotřebí nakonfigurovat a zapnout podpůrné služby serverů dle přepokládané funkce plnění, tak aby nebyly zapnuty zbytečné prvky a tím neubíraly HW prostředky ostatním serverům. V navrhovaném řešení bylo zapotřebí mimo jiné využívat například služeb Active Directory - AD, GroupPolicy a WSUS[45] pro správu, nastavení a update uživatelů účtů a politik. Serverové prostředky byly tedy rozděleny mezi tyto prvky infrastruktury:

Doménový řadič – virtuální stroj zajišťující chod domény Hurt.cz, správu uživatelských účtů a hesel v AD, centrální správa politik přes GroupPolicy Management Console, přidělování IP adres pomocí DHCP[46] a udržování aktuálnosti systému pomocí WSUS Console.

Exchange server – od společnosti Microsoft ve verzi 2013 je nainstalovaný na jeden z dalších virtuálních strojů zajišťující poštovní služby v plném rozsahu produktu. To znamená, že jsou aktivovány i služby OWA[47] a ActiveSync poskytující zabezpečený vzdálený a mobilní přístup do uživatelského mailboxu. Vzhledem přístupnosti služeb z vně firemního prostředí bude tento server umístěn do DMZ.

Backup server – jeden z nejdůležitějších serverů v daném řešení z prostého důvodu. Tento fyzický server disponuje softwarem řídící zálohovací a archivační služby celého systému s příslušnou ochranou dat. Jedná se o aplikační prostředí přímo od firmy Fujistu Eternus SF – Flexible Data Management dodané zároveň s diskovým polem, plně kompatibilní s páskovou knihovnou. Díky tomuto řešení bude zajištěna komplexní ochrana dat i virtualizovaných prvků s možnostmi obnovy, replikace a následné archivace na LTO6[48] pásky. Nainstalovaný software obsahuje management konzoli pro správu, řízení, analýzu a kontrolu dat, dále řídí jednotlivé zálohovací sektory s příslušnými skripty pro spuštění záloh.

[45] Windows Server Update Services
[46] Dynamic Host Configuration Protocol
[47] Outlook Web App / Access
[48] Linear Tape Open

Web server – sloužící pro běh e-shopu a prezentaci firmy na webu byl nainstalován na virtuální stroj a na otevřené platformě Apache. S podporou nejaktuálnějších verzí webových technologií a s propojením na databázový stroj. Server je nastaven do režimu keepalive, kdy s klientem udržuje jednu vytvořenou relaci po stanovenou dobu, místo relací po každém kliknutí a tím nezatěžuje výpočetní výkon serveru ani síťové linky. Tento server virtualizaci využívá i pro vytvoření druhé virtuální síťové karty a využití záložního apache serveru pro případ fyzického přetížení webového serveru. Tento stroj bude zařazen také do DMZ pro zabezpečení interní sítě proti přímým útokům z internetu.

Aplikační server – zajišťující distribuci využívaných aplikací v celém firemním prostředí, zejména se jedná o pokladní a docházkový systém Qpos, kancelářské balíky a další obdobné aplikace. Z využitých virtuálních prostředků je server schopen bez potíží obsloužit všechny požadavky uživatelů v jeden okamžik s minimální odezvou. S využitím síťového sdíleného disku jsou nainstalované aplikace mapovány přímo do uživatelských profilů. Vzhledem k rezervám výkonnostních prostředků je tento server dále využíván jako tiskový server, který spravuje tiskové fronty dokumentů, ovladače tiskáren, vzdálenou správu a nastavení jednotlivých zařízení.

Proxy server – provozovaný opět ve virtuálním prostředí založený na reverzním typu, kdy kontroluje síťový provoz z internetu. Také vytváří další pomyslnou ochrannou vrstvu proti útokům z internetu. V doméně hurt.cz je vydefinováno několik pravidel přístupu do internetu přes proxy. Proxy na adrese 10.168.1.15 nepovoluje uživatelům stahování z internetu, streamování, komunikátory a prohlížení nepovolených stránek, které doporučil a schválil zaměstnavatel. Nastavení pravidel vychází z požadavku o nadbytečném vytěžování firemní sítě uživatelskými požadavky do internetu.

Databázový server – pro potřebu vyššího výpočetního výkonu byl využit druhý fyzický server, který vytvořil srdce celého systému, jelikož zajišťuje několik databází pro různé důležité aplikace. Hlavním úkolem je zpracovávání požadavků z aplikačního, webového, antivirového a Exchange serveru. Tyto požadavky jsou zpracovávány na systému řízení báze dat od společnosti Microsoft ve verzi SQL Server 2008 R2 SP3. Záměrně bylo přistoupeno k nasazení starší verze oproti nové SQL 2014, kvůli odladění a stabilitě.

Antivirový server - mezi klíčové systémové služby IS, které ovlivňují bezpečnost a spolehlivost, patří bezesporu antivirová ochrana. Pro ochranu bylo využito podnikového řešení od společnosti Symantec, jehož virová databáze a správa celého systému je velice účinná, pomocí centrální management konzole Symantec Endpoint Porotection Manager – SEPM a Symantec klienta. Tento server vytváří za firewallem další ochrannou vrstvu serverového a uživatelského prostředí. Centrálně spravuje vzdálené lokality i jednotlivá PC ve firmě pomocí nastavených pravidel chování, doplňujících skriptů pro úpravu klientů a vynucených updatů virové databáze nebo klientského softwaru. V konzoli lze sledovat kompletní síťový záznam, aktuální stav o daném PC a přihlášeném uživateli nebo zakázat spuštění nežádoucího programu apod.

Další prvky patří do kategorie aktivních, zajišťující síťové propojení jednotlivých prvků ve skříni, hlavně propojení do internetu a dále do vzdálených poboček. U těchto prvků na páteřní síti v centrále je využito redundantního faktoru, kříženého propojení a funkce LACP[49], která v případě výpadku jednoho z nich automaticky přesměruje datový provoz na druhý, aby nedošlo k pádu celého systému.

Do datového rozvaděče byly umístěny zařízení značky Fortinet v podobě dvou management switchů a hlavního routeru sloužícího i jako firewall. Typově se jedná o označení FS-124B a FG-80CM, přičemž firewall disponují velice kvalitním bezpečnostním systémem FortiOS 5, kterým disponují i pobočkové routery s označením FG-60D. To nám umožnilo snadnou konfiguraci komunikačních protokolů a směrování mezi jednotlivými vzdálenými lokalitami. V rozvaděči je mimo jiné umístěn i externí border směrovač a převodník od společnosti GTS, který je plně ve správě společnosti a zajišťuje propojení do internetu. Do lokality je přivedeno symetrické připojení, každé z jiného směru pro zajištění konektivity v případě výpadku. Topologie propojení prvků je v provedení hvězda a jsou propojeny pomocí 1Gbit/s optických kabelů.

Management switch s rychlostí portů 10/100/1000 Mbit/s zajišťuje propojení veškerých ostatní prvků v datové skříni. V konfiguračním rozhraní bylo nastaveno několik důležitých služeb jako například jednotlivé VLAN a TRUNK spojení, STP, SNMP[50] pro monitorování sítě a vytvoření dvou párů agregovaného spojení pro zvýšení propustnosti při komunikaci aplikací s databázovým serverem.

[49] Link Aggregation Control Protocol
[50] Virtual LAN, Spanning Tree Protocol, Simple Network Management Protocol

Bezpečnostní prvek FG-80CM byl redundantně připojen symetrickou linkou k externímu routeru, díky dvěma WAN portům. Připojením dvou požadovaných venkovních serverů do portu DMZ byla vytvořena a nakonfigurována oddělená bezpečná zóna. Fyzicky jsou prvky zapojeny v jediném DMZ portu, ale logicky je v síti vytvořena zdvojená brána firewallu viz obrázek 5 v kapitole 4.6. Pro zabezpečení celé infrastruktury bylo vytvořeno několik určujících pravidel směrování a komunikace z/do interní sítě z/do internetu a vzdálených lokalit. Dále bylo nastaveno filtrování HTTP a SMTP[51] provozu na síti, zablokování nežádoucích prvků ohrožující integritu systému. Důležité nastavení samotného směrování v celé síti pomocí OSPF protokolu, nastavení NAT předkladu vnitřního rozsahu sítě na několik přidělených veřejných IP adres a provázání komunikace se vzdálenými pobočkami pomocí VPN spojení založeného na protokolu IPSec a zabezpečené SSL LDAP[52]autentifikace pro vzdálené uživatele řádně zařazené v Active Directory. Posledním velice důležitým nastavením bylo zapnutí a nastavení monitoringu a logování veškerých situací a incidentů, které na síti během provozu vznikají.

Posledním nezmíněným prvkem zvyšující bezpečnost ukládaných dat je zálohovací pásková knihovna Fujitsu Eternus LT20. Tento prvek zajišťuje dlouhodobé zálohování důležitých firemních dat na externí přepisovatelné nosiče, které budou uloženy mimo centrální místnost. Knihovna disponuje dvěma úložnými schránkami neboli magazíny na magnetické LTO 6 pásky s kapacitou 2,5 GB / 6,25 GB (nekomprimovaná / komprimovaná data). Každý úložný magazín, disponuje 4 sloty a je tedy možné knihovnu naplnit 8 páskami a docílit celkové úložné velikosti až 20TB bez komprese dat, ovšem s využití komprese můžeme tuto velikost až zdvojnásobit. Svými rozměry zabere v racku prostor pouze 1U. Díky možnosti propojení pomocí FiberChannel můžeme docílit datové propustnosti 576 GB/h surových dat nebo 1 440 GB/h dat komprimovaných a rychlosti zápis / čtení 160 MB/s / 400 MB/s. Tyto vlastnosti jsou plně využity ve spojení s diskovým polem a nad nimi vytvořeným cluster. Pro zajištění dynamického využití celého clusteru bylo zároveň pořízeno i SW řešení Fujistu Eternus SF – Flexible Data Management. Zajišťující kompletní správu diskového pole a řízení zálohování. Podrobněji se o nastavení zálohování a jejím plánu se zmíním v kapitole 4.8 při tvorbě interního dokumentu.

Bezpečnostní opatření neoprávněného vstupu do místnosti jsou zajištěna vnějším okruhem fyzické ochrany nově vybudované místnosti u vstupních dveří magnetickým čidlem,

[51] Hypertext Transfer Protocol & Simple Mail Transfer Protocol
[52] Secure Socket Layer & Lightweight Direcotry Access Protocol

akusticko-vizuální sirénou a EZS ovládaného pomocí klávesnice. Vzhledem k povaze provozu v místnosti serverovny budou zvoleny detektory s vyšším stupněm citlivosti. Jak bylo uvedeno, celý systém je napojen na modul pro komunikaci prostřednictvím GSM[53] brány a ETHERNET sítě tak, aby jednotlivé události, jež budou systémem logovány, mohly být automaticky ukládány v daných intervalech na disky firmy. Kontrola vstupu do místnosti je řešena prostřednictvím autorizačních údajů – PIN kódů. Stanovení intervalů ukládání logu, pravidel přístupu a chování v centrální místnosti je podrobněji zpracováno v kapitole 4.8.

Pro zajištění přísunu studeného vzduchu k aktivním prvkům a dodržování stálé teploty v místnosti na hodnotě 22 °C, byla zakoupena a naistalována podstropní klimatizační jednotka Sinclair ASGE-09A propojena pomocí měděného izolovaného dvoj potrubí chladiva s venkovní kondenzační jednotkou Sinclair ASGE-09A WK se zárukou a servisní službou na 3 roky. O chladícím výkonu 2,6 kW a příkonu 1000 W, které jsou pro naše potřeby naprosto dostačující, dle technické specifikace prvek je schopen vychladit prostor o objemu 40 m^3 a v tomto případě se jedná pouze o 27 m^3. Díky správnému umístění na stěnu za rackovou skříň, podpoříme nasávání teplého vzduchu přímo z racku a vyfukování chladného, do prostoru před rack. Ze stropního podhledu nad rackem byl pro lepší nasměrování proudícího vzduchu připevněn kovový půloblouk, který jej sráží přímo do čela racku. Nastavením jednotky bylo přispěno k dokonalenému proudění vzduchu v místnosti. Tím pádem se vytvořila studená a teplá ulička kolem racku samotného. Kdy je studená ulička vytvářena před rackem, prvky nasávají chladnější vzduch, kdežto za rackem vzniká teplo, které je přirozenou cirkulací nasáváno zpět do klimatizační jednotky.

4.5 Zřízení datového připojení a propojení poboček

Vzhledem k současným podmínkám decentralizovaného síťového prostředí a různých poskytovatelů připojení dle dané lokality, bylo zapotřebí tyto faktory sjednotit a vytvořit kompaktní firemní síť i s odlehlými pobočkami.

Bylo osloveno několik firem s požadavkem na připojení do internetu a propojení čtyř poboček do centrálního uzlu firmy. Uvažovaná varianta pro nabídky bylo vytvoření chráněného VPN připojení a poskytnutí dostatečné rychlosti sítě. Požadavky na technické parametry připojení byly následující. Od poskytovatele do centrálního uzlu přivést dedikovanou symetrickou linku o minimální přístupové rychlosti 4Mbit/s. Jedna z linek bude

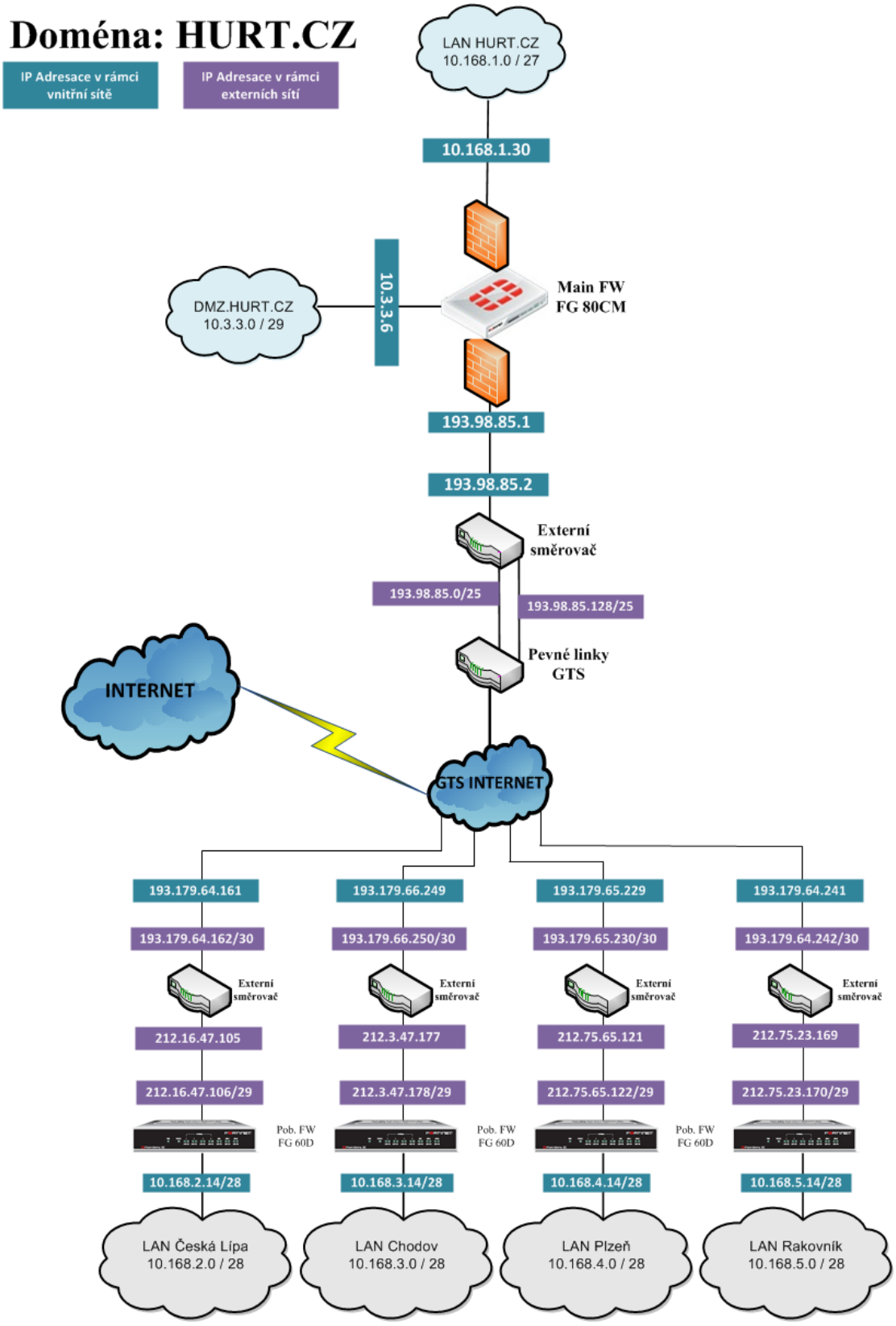
[53] Global Systém for Mobile

sloužit jako záložní pro případ výpadku hlavního vlákna a lze snížit požadavky na rychlost 1Mbit/s při omezeném provozu. Pro pobočkové lokality zajistit přístup s minimální hodnotou 2Mbit/s. A zároveň pro firmu zajistit 5 veřejných IP adres a zaregistrování doménového jména „hurt.cz.“

K propojení poboček a centrály do internetu byla přizvána firma GTS Czech s.r.o. nyní již „T-Mobile“, od které byla obdržena ucházející předběžná nabídku i vhodné řešení problému vzdálených poboček, kdy by pro toto řešení využilo své vlastní služby GTS IP VPN využívající progresivní technologii MPLS[54] zabezpečené protokolem IPSec zajišťující bezproblémové propojení do centrálního uzlu. Nakonec bude využito pouze služby k vytvoření přístupové dedikované linky o rychlosti 2Mbits pro vzdálené lokality a symetrické dedikované 4Mbits linky přivedené do centrály. Oba tyto uzly jsou ukončeny v IP síti poskytovatele GTS v konfiguraci rozhraní a konektoru 100BASE-Tx a RJ-45. Zároveň s poskytování služby bude zapotřebí pronajímat edge routery poskytovatele, která právě zajišťují komunikaci mezi sítí GTS a firemní sítí hurt.cz. Následné vlastní propojení pro navázání přímého spojení poboček s centrálou bude realizováno vlastními silami. A to hlavně kvůli vysoké, několika tisícové paušální ceně za provozování služeb ze strany poskytovatele. Společnost sama je velice kvalifikovaný partner a sám se zavazuje k plnění smluvně dohodnutých garancí v podobě SLA, které z pohledu bezpečnostní politiky jsou velice důležité. GTS Czech s.r.o. jsi vyhradila právo na tříměsíční průzkum jednotlivých lokalit, aby potvrdila bezproblémové propojení a garantovala požadované rychlosti bez nutnosti agregace linky. Technici firmy GTS v současné době již dokončují svá šetření a zároveň připravují vše k finálnímu propojení jednotlivých lokalit, protože v žádné z nich nebyla zjištěna žádná závažná překážka pro realizaci projektu. Po dokončení prací vznikne ve firemním prostředí ucelená komunikační infrastruktura pod správou jediného poskytovatele zajišťujícího správu přístupové a přenosové sítě a v případě výpadku jedné z linky zajištění okamžitého automatického překlopení na druhou trasu.

[54] Multiprotocol Label Switching – zajišťuje vysokoryslostní a velkokapacitní směrování v sítích

4.6 Rozvržení a nastavení bezpečnostní topologie



Obrázek 4: Grafické znázornění logického propojení infrastruktury
Zdroj: Vlastní tvorba v aplikaci MS Visio

V této kapitole je popsáno grafické řešení logického propojení v jednotlivých lokalitách a nastavení LAN sítí z pohledu bezpečnostní infrastruktury, jejichž dílčí grafické znázornění je k nahlédnutí v příloze. Grafické znázornění situace naznačuje použití dvou fyzických firewall prvků, ale ve skutečnosti je použit pouze jeden fyzický aktivní firewall prvek FortiGate–80CM zajišťující toto logické uspořádání. V celé interní síti pod doménou HURT.CZ, probíhá komunikace na třetí síťové vrstvě primárně pomocí TCP/IP protokolu, kde je použit privátní rozsah IP adres třídy A: 10.0.0.0 – 10.255.255.255. Adresace je nastavena od centrální sítě do nižších uzlů následovně, kde centrála je v síti 10.168.1.0 /27 a pobočkám je postupně přidělen rozsah sítě od 10.168.2.0 – 10.168.5.0 /28, což poskytuje 13 použitelných IP adres pro klienty. Ohledně DMZ, v které jsou umístěny servery pro komunikaci do internetu neohrožující vnitřní síť, této zóně byl z bezpečnostních důvodů přidělen jiný rozsah a to 10.3.3.0 /29. Vyšší maska sítě byla navržena záměrně, jelikož v daných LAN sítích používáme málo zařízení, není proto třeba plýtvat rozsahem. I když se jedná o adresaci firemní sítě nezasahující do veřejného prostoru IP adres. A také snížit riziko zneužití volných IP adres. Z bezpečnostního hlediska vnitřního napadení je v celé síti nasazen síťový prvek kontrolující aktuálně připojená zařízení do sítě pomocí protokolu IEEE802.1x v kontinuálním přidruženém nastavení se Spanning Tree Protokolem, zajišťujícím okamžité ukončení spojení v příslušného portu, kde bylo identifikováno neznámé zařízení. Vytvořením virtuálních interface – VLAN a dalších logických sub-interface, jejichž provoz je řízen protokolem LACP v režimu passive na straně firewallu a fyzickým propojením do hlavního switche pomocí 2 x 5Gbit/s interface bylo docíleno následujícího stavu. Principem celého řešení je, že veškerý provoz ze všech sítí s možnou přenosovou rychlostí až 10Gbit/s je posílán těmito VLAN přes centrální firewall, kde je podrobován bezpečnostním kontrolám.

Na základě rozhodnutí o vytvoření VPN propojení poboček byly nakonfigurovány jednotlivé aktivní prvky Fortinet vytvářející jednotné HW i SW prostředí. Na hlavním firewall prvku proběhla konfigurace jednotlivých VPN tunelů pro vzdálené lokality s přesně definovaným směrováním na cílové fyzické porty, tak aby byla zajištěna vzájemná nedostupnost jednotlivých VPN tunelů. Nastavení prvků v lokalitách je totožné liší se pouze v konfiguraci IP adres jako například v lokalitě Plzeň pro představu v tabulce č. 2 pod textem. Celá VPN topologie je založena na technologii MPLS. Komunikace mezi centrálou v Lužné a vzdálenými lokalitami je realizována přes šifrované VPN IPSec site-to-site spojení, topologicky „do hvězdy,“ se středem v Lužné.

Položka	Nastavení
Název prvku:	Forti - Plzeň
Vnitřní IP FG60D / maska:	10.168.4.14 /28
Vnější IP FG60D / maska:	212.75.65.122 /29
Vnitřní IP GTS routeru (gateway pro FG60D)	212.75.65.121
Vnější IP GTS routeru PtP / maska:	193.179.65.230 /30
Gateway pro GTS router PtP:	193.179.65.229

Tabulka 2: Ukázka směrování vzdálených lokalit
Zdroj: Vlastní tvorba

4.7 Příprava vzdálených lokalit

Tímto posledním dílčím projektem v rámci konfiguračních prací se blížíme ke konci jednoho z dílčích cílů praktické části diplomové práce. V rámci této kapitoly je zmíněna i konfigurace techniky pro dva stálé zaměstnance v centrále – na pozici administrátor a sekretářka. Oba typy jsou opět podpořeny 5 letou servisní zárukou. Pro sekretářku byla dodána shodná sestava jako pobočkovým zaměstnancům, ale pro potřeby větší mobility administrátora byl dodán 15,6“ notebook Lenovo T430 v konfiguraci: s procesor Intel Core i5-3380M 2,9GHz 3M Cache s integrovanou 1GB grafickou kartou NVIDIA Optimus, pamětí RAM 4GB DDR3, SATA harddisk o kapacitě 3200GB s 7200 otáčkami / s, veškeré výstupní porty (např. 2xUSB 3.0, RJ-45), WiFi a bezpečnostní čip. Jinak tato část patřila mezi nejjednodušší i proto byla ponechána až nakonec. Na pobočkách došlo pouze k připojení jednotlivých zařízení do sítě, jejich ruční konfiguraci. Zejména proběhlo zapojení malé UPS jednotky do pobočkové sítě a následná základní konfigurace využití energie, mailových výstrah apod. Připojení síťové tiskárny HP LaserJet 3015, IP telefonu a aktivních prvků FortiGate-60D, které byly předem nakonfigurovány. V základní konfiguraci bylo nastaveno směrování mezi externím routerem a propojením do internetu a do centrály, dále proběhlo nastavení VPN komunikace založené na IPSec protokolu a nastavení dílčích bezpečnostních pravidel na úrovni firewallu. Postupnými přípravami dospěla situace k instalaci nově dodaných PC sestav značky Lenovo. Sestavy disponují procesory Intel Core i5-3470 3,2GHz 6M Cache s integrovanou grafickou kartou, pamětí RAM 4GB DDR3, SATA harddisk o kapacitě 250GB s 7200 otáčkami / s, veškeré výstupní porty (např. 4xUSB 3.0, GIGA NIC), monitor Lenovo 22“ s rozlišením 1680x1050. Na celou sestavu je vystavena 5 letá záruka s možnou opravou nebo výměnou na místě zákazníka next business day od nahlášení problému. Instalace probíhala z připravených image s nastaveným systémem Windows 7 Professional, kancelářským balíkem Office 2013, antivirovou ochranou Symantec propojenou

s centrální serverovou správou antivirovou ochranou a plnohodnotný pokladní systém QPOS od stejnojmenné firmy QPOS systém s.r.o. Po samotné instalaci proběhlo pouze přejmenování PC dle dané lokality a přidání do firemní domény hurt.cz. Další dodatečné nastavení PC je automaticky přebráno z nastavení v GroupPolicy, jako je Proxy brána, uživatelské účty a s nimi spojená přístupová práva, vzdálený přístup pro administrátora, automatické aktualizace softwaru apod. Současně s dodávkou podkladního systému byl objednán i docházkový systém. Obě tyto aplikace jsou centrálně spravovány pomocí administrátorského modulu, díky němuž všechna důležitá data jako stavy pokladen, tržeb, skladu jsou ze všech provozů online dostupná z jednoho PC a lze je proto snadno aktualizovat. Provedené změny naskladnění nebo přecenění se v systému projeví ihned po uložení akce. Na druhé straně v docházkovém systému je zabudován i mzdový, který přehledně zaznamenává strávený čas zaměstnance na pracovišti a na konci měsíce automaticky vygeneruje výplatní pásky. Ke komunikaci pokladního a docházkového systému je využito vybudovaného VPN spojení mezi lokalitami. K dokonalému fungování a propojení těchto dvou systémů je důležité správně nakonfigurovat serverové platformy aplikací na našich prostředcích. A dále zaregistrovat příslušné zaměstnance i s otiskem prstů do databáze aplikace pro rychlejší přihlašování přes čtečku otisků. Nejprve byl systém otestován na jedné z poboček, kde se přibližně po měsíci testování nevyskytly žádné komunikační, uživatelské ani jiné problémy. Na základě toho byla vytvořena kompletní objednávka na pokladní a docházkový systém s administrátorským modulem s možností instalace jak na serverové, tak uživatelské stanice plus další drobné příslušenství k pokladně jako je například laserová čtečka kódů nebo termální tiskárna účtenek. I když firma nabízí celý balíček i s dotykovým HW v našem případě postačí pouze bezdotykový SW v návaznosti na vlastní techniku a nastavená pravidla v GroupPolicy apod. Náklady na pořízení tohoto vybavení je znázorněno v níže v kapitole 5 – zhodnocení, v tabulce č. 3.

4.8 Návrh interního bezpečnostního dokumentu firmy

Výše definované návrhy a praktické postupy vychází především z návrhu tohoto dokumentu, i když je uváděn až v poslední části vlastní práce. Obě části jsou spolu úzce provázány a navzájem se doplňují, a tedy nezáleží na jejich vlastním pořadí. Vytvořený návrh dokumentu Bezpečnostní politiky bude sloužit jako závazný dokument pro všechny zúčastněné osoby organizace i pro úzce spolupracující objekty. Vzhledem k doposud

nepoužívaným praktikám řízení bezpečnosti firmy závislé na interním dokumentu vycházející z doporučení organizace ISO a jejich „best practises.“ Bude po jeho schválení provedeno podrobné vstupní školení všech zúčastněných osob, které se v pravidelných intervalech bude opakovat, maximálně však v ročním horizontu.

Z dokumentu také vychází i povinnost aktualizace jeho samotného v daných intervalech nebo v návaznosti na změny ve firmě nebo vnějším okolí. Jako například v případě změn organizační struktury, legislativních změn nebo v důsledku nalezení bezpečnostní trhliny v Bezpečnostní Infrastruktuře - BI. Aktualizační intervaly byly rozděleny do dvou hlavních úseků kontroly a revize plus jeden mimořádný stav.

- Kdy byly stanoveny nepovinné čtvrtletní kontroly stavu BI a v návaznosti na případné pochybení, provedena příslušná opatření a revize dokumentu. Ve většině případů je tato čtvrtletní lhůta adekvátně dlouhá vůči nekritickým změnám.
- Povinná kontrolní revize dokumentu musí být prováděna jednou ročně, v návaznosti na uplynulé změny v BI a systému jako celku.
- Revizní výjimka je udělena na případy akutní změny v důsledku nalezení kritického bodu BI ohrožujícího stabilitu.

Dokument vychází z obecných doporučení pro tvorbu podobných předpisů a metodiky Národního Bezpečnostního Úřadu České Republiky (NBÚ, 2014). Primárně bude rozčleněn do subkapitol popisující jednotlivé části systému. Nejprve v úvodní části popíšeme typické povinnosti zúčastněných osob a poté vlastní obsah dokumentu.

V rozsahu malého firemního prostředí bude bezpečnostním správcem určen zároveň administrátor celého systému, proto obě činnosti jsou vzájemně provázány. S tím, že role bezpečnostního správce je v uvozovkách nadřazena správci IS. Osoba tímto pověřená automaticky podléhá vrchnímu schvalovacímu prvku neboli jednateli firmy Dahl-Tok s.r.o. Proto typické povinnosti těchto dvou subjektů zde budou sloučeny dohromady. Povinnosti jsou popsány rámcově a jejich podrobnější výčet je uveden až v samotném těle dokumentu. Mezi povinnosti správce budou patřit následující body:

- Vytvoření a udržování aktuálnosti seznamu oprávněných uživatelů přistupujících do systému, který vycházející z Active Directory. Schválení práv uživateli dle organizační struktury a popisu pracovního místa. Popřípadě odebrání nebo smazání účtu.

- Stanovuje osoby s vyšším statutem oprávnění pro přístup do centrální místnosti – severovny a spravuje agendu přístupů do vzdálených lokalit – osoby, klíče a hesla k objektům.
- Přiděluje uživatelům login dle níže specifikovaných pravidel.
- Zastává funkci interního kontrolního prvku, kde zkoumá auditní záznamy, logy a evidence z bezpečnostních systémů. Tyto záznamy je povinen uchovávat na bezpečném místě, pro případnou kontrolu či vzniku incidentu minimálně po dobu 3 let.
- Zkoumám, řeší a eviduje vzniklé bezpečnostní incidenty a následně je hlásí jednateli. V případě pochybení uživatele stanovuje sankce za vzniklý incident.
- Zajišťuje agendu k periodickému proškolení uživatelů, které je jím osobně vedeno a uchovává výstupní protokoly.
- Správa aktuálnosti interního dokumentu BI.
- Zajišťuje zálohování systémů a interních dat, které jsou následně uloženy na bezpečné místo mimo centrální místnost do žáruvzdorného trezoru.
- Dohlíží na externí subjekty při jakékoliv revizi či opravě v centrální místnosti nebo opravě HW firemním prvků, tak aby byla vyloučena případná modifikace.
- Zajišťuje po technické stránce chod celého IS a BI v plném možném rozsahu bez výpadkově v pracovní době tedy od 7:00 – 16:00. To zahrnuje konektivitu vzdálených lokalit, chod aplikačního a serverového prostředí.
- Provádí aktualizace aplikačního prostředí, které jsou zautomatizovány díky WSUS konzoli antivirové konzoli. Opravuje poškozené OS na uživatelských stanicích pomocí přednastavených image obrazů systému.
- Vytváří skripty a spouští bezpečnostní politiky dle dříve schválených ujednání vycházejících z bezpečnostní dokumentace.
- Spravuje uživatelské účty a jejich přístupy i pomocí biometrické čtečky, správce dále zajišťuje pravidelné zálohování systému dle stanoveného plánu zálohování, který je uveden níže.

Pro správné a konzistentní fungování celého systému je důležité také stanovit povinnosti formou směrnice pro zúčastněné uživatele a jasně jej o nich informovat.

Je zapotřebí tyto povinnosti zpracovat srozumitelně s vyjmutím obsahu a údajů, které uživatele nepotřebují znát, aby jich nezneužili proti informačnímu systému.

- Uživatel je povinen po příchodu na pracoviště odblokovat EZS, vizuálně zkontrolovat technické zázemí a následně se pomocí svých přihlašovacích údajů přihlásit do PC. K přístupu mu poslouží dva způsoby – klasický login skript na PC nebo biometrická čtečka otisků prstů, která má logu uložený obraz otisků. Pravidla zadávání apod. jsou stanovena v další kapitole.
- Uživateli je důrazně doporučeno, aby dbal nepsaných pravidel chování vůči používání technických zařízení a bez měkkého vypnutí jej neodpojoval od elektrické energie apod.
- Dále je povinen hlásit každé nestandartní chování systému i v případě vlastního zavinění.
- Při práci s daty využívá síťové disky, které jsou automaticky zálohovány a chráněny proti výpadku s možností obnovy ztracených dat.
- Používání vlastních externích úložných zařízení je možné pouze po kontrole a domluvě se správce systému, aby nedošlo k narušení firemního systému.
- Pro ukládání osobních dat je k dispozici uživateli místní disk v PC, u které není nastaveno zálohování a zaručena návratnost dat při defektu disku.
- Při krátkodobém odchodu od běžícího PC je povinen stanice uzamknout a v případě opuštění místnosti i zajistit její uzavření / uzamčení.

Jádro celého dokumentu bude obsahovat několik důležitých oblastí týkající se správného zabezpečení chodu firemní infrastruktury, které bude podmíněno dodržováním stanovených pravidel bez výjimek. Zohledněny budou především tyto podkapitoly: Počítačová bezpečnost, Komunikační bezpečnost, Personální bezpečnost, Požadavky na dostupnost – Zálohovací plán, Administrativní bezpečnost a Fyzické zabezpečení IS.

Na začátku je potřeba dodat, že v tomto souhrnném dokumentu by mělo být zaznamenána i skutečnost popisující HW a SW vybavení a údaji o LAN, jímž firma disponuje, ale vzhledem k obsáhlému rozepsání v dříve uvedených kapitolách se nebudeme opakovat. Již bylo řečeno, že tyto dílčí projekty jsou vzájemně provázány.

4.8.1 Počítačová bezpečnost

Základními prvky kapitoly je identifikace a autentifikace uživatele a záznamy o auditní stopě. Na základě záznamu v Active Directory, kde každému oprávněnému uživateli

je vytvořen účet. Z popisu pracovní pozice přidělena příslušná práva přístupu do systému, složek síťových disků a vytvořeno uživatelské jméno a prvotní heslo. Uživatelské jméno je složeno z příjmení a prvního písmene ze jména například „Novakj.“ Heslo uživatel musí během prvního dne nástupu do zaměstnání změnit dle příslušných parametrů: minimální délka hesla je stanovena na 8 znaků a nesmí obsahovat uživatelské jméno. Musí obsahovat povolené znaky v kombinaci minimálně 3 typů znaků z následujících 4 typů: malá, velká písmena, číslic nebo vybrané speciální znaky (* - + ? - ! ._), tak aby splňovalo vysokou složitost. Důvěrnost a integrita autentizační informace je během přenosu sítí zajištěna v rámci domény a nastavení transakčních pravidel.

- První důležitou zásadou je ochrana, tedy osobní heslo nikomu nesdělovat a chránit jej jako utajovanou informaci nejvyššího stupně.
- Druhou zásadou při krátkodobém opuštění pracovní stanice uživatel musí běžící PC uzamknout.
- Třetí zásada určuje platnost aktuálního hesla, která činí 3 měsíce. Před vypršením dojde k automatickému oznámení o změně a uživatel je povinen tak učinit s touto podmínkou, že heslo bude odlišné od posledních pěti předchozích, které jsou stále uchovávány v systému.
- Čtvrtou zásadou je omezený počet pokusů pro zadání hesla, jsou povoleny tři pokusy, poté dojde k uzamčení účtu na 15 minut. V případě, že uživatel heslo zapomněl, musí požádat administrátora o reset hesla. Nové bude zasláno SMS zprávou na uživatelský telefon.
- Pátou zásadou výše uvedená pravidla stejně platná i pro správce systému bez výjimek.
- Šestá zásada popisuje úroveň oprávnění pro běžné uživatele v tom smyslu, že jejich účet je typu User s omezenými právy vytvořeného formou profilu pomocí GroupPolicy. Proto, aby se zamezilo uživatelskému instalování neprověřeného SW.

Pomocí funkce ve Windows umožňující zaznamenávání událostí v doméně jsou ukládány především záznamy o úspěšnosti autentizace do systému, pokusy o prolomení přístupu do zakázané složky a časový interval přihlášení. V tomto bodě více než důležité, aby auditní stopa byla sledována supervizorem i u administrátora z důvodu plného přístupu do systému. Prvky v centrální místnosti disponují vlastními systémy záznamu událostí

a aktuálního stavu, při změně jsou automaticky generovány výstražné zprávy, které jsou zaslány na administrátora. Veškeré zaznamenané události jsou ukládány a uchovávány po dobu šesti měsíců v diskových oddílech nepřístupných pro běžné uživatele.

4.8.2 Komunikační bezpečnost

Vytvořený model WAN sítě s vnitřním neveřejným IP rozsahem a s jedním přístupovým bodem do internetu přes veřejnou adresu je složený z centrálního prvku a vzdálených lokalit umístěných v jedné doméně Hurt.cz zajišťuje ověřování jednotlivých lokalit proti autorizačnímu serveru na bázi ověření MD5. Propojení lokalit je zajištěno zabezpečením VLAN spojením pomocí vytvořeného IPSec tunelu a technologie MPLS. Z pohledu přístupnosti sítě je veškerý síťový provoz pomocí aktivních prvků sítě filtrován s využitím kontrolního protokolu SNMP na TCP[55] portu 161 a mnoha podpůrných funkcí OS na firewallu. Například IDS a IPS kontroly, monitoring, DPL, NAC[56], aplikační kontrola apod. Správce online zaznamenává neobvyklé pohyby, jak směrem do interní sítě, tak i ven do internetu a ihned reaguje na případné vychýlení z normy. S užitím zásady „co není povoleno, je zakázáno“ jsou pravidla přístupu nastavena pomocí ACL[57]. Například povolující uživatelskou webovou a poštovní komunikaci na portech 80, 443, 25, 220. Na druhé straně zakazující komunikaci na sociálních sítích přímo vytvořeným pravidlem se specifikovanou skupinou blokovaných adres.

4.8.3 Personální bezpečnost

Směrnice stanovující příslušné role uživatelů a jejich odpovědnost v systému.

Bezpečnostní správce zodpovídá za vedení aktuálního seznamu uživatelů. V případě ukončení smlouvy se zaměstnancem dojde v hierarchické posloupnosti oznámení a schvalování těchto změn přes jednatele firmy až k zajištění skutečnosti fyzického smazání uživatele ze systému odpovědnou osobou, tedy správcem. Proto, aby bylo dodrženo korektní chování v systému je nezbytnou součástí této směrnice bezpečnostní školení. Školení provádí sám osobně bezpečnostní správce v pravidelných intervalech nepřekračující délku mezidobí šesti měsíců. Nebo v případě nového zaměstnance toto školení provést nejpozději v den nástupu do zaměstnání. Výstupem školení je podepsaný dokument uživatelem o pochopení

[55] Transmission Control Protocol
[56] Denied Parties List & Network Access Control
[57] Access Control List

a dodržování bezpečnostních směrnic. V opačném případě hrozí uživateli stanovené sankce dle vzniklého incidentu.

4.8.4 Požadavky na dostupnost – Zálohovací plán

Směrnice udávající pravidla zálohování a ukládání pásek v rámci bezpečnostní politiky firmy. Zálohovací služby databázových a systémových prostředků firemní infrastruktury jsou zajištěny řešením firmy Fujistu Eternus SF – Flexible Data Management, jež zajišťuje správu řízení, monitoring, replikaci, zálohování a obnovu veškerých dat. Tato zálohovací služba je provozován na dedikovaném serveru disponujícím dostatečnými prostředky tak, aby zajistil odpovídající odezvy očekávané od tohoto typu služeb. Zálohy probíhají na principu Disk to disk to tape, kdy na primární diskové úložiště jsou na denní bázi zálohována data databázové vrstvy a uchovávána po dobu 14 dnů. Na týdenní, měsíční a roční bázi jsou data zálohována na páskovou knihovnu s tím, že pásky jsou umístěny v off-site lokalitě. Backup server zajišťuje přístup k zálohovací knihovně. Fyzický přenos dat na zálohovací médium probíhá prostřednictvím FC rozhraní. Přenos dat z jednotlivých aplikací na zálohovací server je řešen 2 způsoby:

- **pomocí standardních služeb OS** – přístup k souborům a adresářům,
- **pomocí speciálních SW agentů** – přístup k DB, poštovnímu serveru, atd.

Vlastní zálohovací proces probíhá prostřednictvím „jobů“ automaticky v nočních hodinách tak, aby během dne nedošlo ke zbytečnému zatížení datové sítě či výkonu jednotlivých serverů. Zálohy pobočkových serverů probíhají dvoustupňově, v prvním stupni jsou zálohy replikovány na vybrané datové oblasti na centrále. V druhém stupni jsou v rámci hlavního jobu přehrávány na pásky. Pro zajištění úplné kontinuity je vytvořeno několik skupin zálohovacích pásek: denní, týdenní, měsíční a roční. Pravidelné denní zálohy od pondělí do čtvrtka jsou zajišťovány Incremental neboli přírůstkovou zálohou od poslední změny, v pátek je provedena plná záloha a v sobotu a neděli je zálohování vypnuto.

Denní pásky: Zůstávají stále v knihovně. Jednotlivé pásky (3 ks) jsou pravidelně přepisovány v intervalu 14 dnů. Tyto pásky umožňují obnovit data 14 dní nazpět po jednotlivých dnech.

Týdenní pásky: pravidelně se mění každý čtvrtek mimo první čtvrtek v měsíci. Ve skupině LTO6 jsou 2ks pásek. Tyto pásky se vyměňují za nejstarší týdenní. Když se tyto pásky vyjmou z knihovny, vznikne sada, která se uloží do trezoru. Celkově jsou 4 sady pásek. Jedna sada je vždy v knihovně a zbylé tři jsou v trezoru.

Měsíční pásky: pravidelně se mění každý první čtvrtek v měsíci. Ve skupině LTO6 jsou 2ks pásek. Tyto pásky se vyměňují za nejstarší měsíční. Když se tyto pásky vyjmou z knihovny, vznikne sada, která se uloží do trezoru. Celkově je 13 sad pásek. Jedna sada je vždy v knihovně a zbylých 12 je v trezoru.

Roční pásky: vyměňují se každý první čtvrtek v měsíci únoru. Ve skupině LTO6 je jedna páska. Tato páska se vyměňuje za nejstarší roční. Když se tato páska vyjme z knihovny, vznikne sada, která se uloží do trezoru. Celkově jsou 2 sady pásek. Jedna sada je vždy v knihovně a druhá je v trezoru.

4.8.5 Administrativní bezpečnost

Určující osoby pro výkon a správu dokumentace IS a úložných zařízení. Tato činnost je přidělena správci systému z důvodu nejbližší přístupnosti a přehledu o spravovaném systému. Udržuje agendu oprav, údržeb, prováděních záloh, o kontrole auditních záznamů, krizových situacích a incidentech formou provozního deníku IS. V souvislosti s dokumentační agendou udržuje interní bezpečnostní dokument v aktuálním stavu, díky stanoveným pravidelným kontrolám. A to v minimálním čtvrtletním intervalu a jednou ročně pro kompletní revizi. Při likvidaci těchto zařízení zajišťuje dozorem, že dojde k dokonalé skartaci disku a tím odstranění citlivých dat. O tomto kroku poté uloží protokol o likvidaci s příslušnými parametry zlikvidovaného zařízení – S/N, velikost apod.

4.8.6 Fyzické zabezpečení IS

Směrnice, z níž vychází postup zabezpečení centrální místností, přístupu do ní, ukládání zálohovacích pásek. Pro záložní zařízení je vyhrazen oddělený úložný prostor, umístění mimo hlavní kancelář zabezpečen proti požáru a opatřen zakódovaným přístupem, který je znám pouze dvěma osobám – majitel a správce. Pro fyzickou ochranu centrální místnosti jsou použity standardní prvky ochrany splňující evropské normy EZS, EPS a kamerový systém sledující nepřetržitě dění okolo prvků. Místnost je opatřena protipožárními dveřmi s dvojitým bezpečnostním zámkem. Uvnitř je samotný datový rozvaděč také opatřen bezpečnostními zámky proti vniknutí. Do místnosti je povolen vstup opět pouze dvěma osobám – majitel a správce ovšem každý vlastním osobní přístupové heslo. Pro případ incidentu a zjištění ze záznamu, kdo se v daný moment v místnosti vyskytoval. Vzdálené lokality jsou také zabezpečeny EZS a disponují oddělenou, uzamykatelnou místností obsahující aktivní prvky sítě.

5. Zhodnocení návrhu

Hlavním přínosem této kapitoly je zohlednit přínos navrhovaného řešení v konfrontaci s potřebnými hrubými náklady pro zavedení jednotlivých dílčích částí. Není pochyb o zvýšení bezpečnosti celé infrastruktury, ale především bude tímto řešením zajištěna ochrana a zálohování interních dat, které patří k nejdůležitějším aktivům firmy.

V návaznosti na počátek praktické části a použitou tabulku č. 1 lze vyhodnotit návrh podle stanovených rizikových faktorů, u kterých byla snaha o postupnou nápravu, popřípadě úplné eliminování. Například byl zaveden sofistikovaný zálohovací systém, který ochrání data za téměř jakýchkoliv okolností. A tím firmě nezpůsobí finanční ztráty dalších desítek let. Centrální infrastruktura byla opatřena náhradním zdrojem elektrické energie pro případ krátkodobého výpadku. Došlo k vybudování zabezpečeného a šifrovaného komunikačního spojení pro interní komunikaci i se vzdálenými lokalitami, tak aby bylo co nejvíce eliminováno riziko vnějšího napadení IT útočníkem. Pro zvýšení vnitřní bezpečnosti byla zavedena pravidelná bezpečnostní školení pro zaměstnance, která vyplývají z vytvořeného interního bezpečnostního dokumentu, který dále stanovuje práva, povinnosti a zodpovědnost uživatelů za dodržování pravidel chování v systému.

Na případně vynaložené investice musí býti nahlíženo jako na rentabilní prostředky s budoucí návratností v podobě stability systému s mnohem vyšší efektivitou. V důsledku to může přinést vyšší příjem zisků firmy. V případě vzniku nějakého incidentu, bude firma ochráněna, díky navrhovanému řešení, které je na typické incidenty uzpůsobené a v reálném čase na ně dokáže reagovat a eliminovat je.

Vzhledem k původnímu, téměř nulovému stavu technickému zázemí firmy, jsou mezi součtové částky návrhu podstatně vyšší, než kdyby byla navrhována pouze obnova stávajícího prostředí. Proto i největší finanční prostředky bylo zapotřebí vynaložit na vybudování centrální místnosti v hodnotě okolo 800 000 Kč. Další dílčí cenové ohodnocení jednotlivých opatření jsou k náhledu níže v tabulce č. 3. U některých položek mohlo být sáhnuto po méně nákladných a výkonných prvcích, ale je důležité na návrh pohlížet jako na řešení budoucích stavu a případných problémů. Na které je již tato infrastruktura nyní připravena a v případě potřeby ji snadno rozšířit. A tím podpořit budoucí růstu firmy bez ohledu na finanční, bezpečnostní i kapacitní situaci.

Všechny ceny jsou uvedeny bez **DPH**

CENTRÁLNÍ MÍSTNOST	
Silnoproudé rozvody + stavební práce + materiál	196 758 Kč
Racková skříň - Digitus Server-Line 36U	21 521 Kč
Záložní jed. el. Ener. UPS centrála - Eaton UPS 9130i - XL2U - 2kVA	23 205 Kč
+ externí baterie	10 250 Kč
PDU 2x jednotková cena 1 278,-	2 556 Kč
Vnitřní jednotka klimatizace - Sinclair ASGE-09A	8 690 Kč
+ vnější Kkndenzační jednotka	14 370 Kč
Elektronický zabezpečovací systém - EZS	51 046 Kč
Automatický zhášecí systém - AZS	83 660 Kč
Pásková knihovna Fujitsu ET LT20	62 548 Kč
+ 8ks LTO 6 Ultrium - jednotková cena 4 952,-	39 616 Kč
Server - FJ P RX 1330 2x - jednotková cena 33 250,-	66 500 Kč
Diskové pole Fujitsu ET DX60	112 389 Kč
Centrální směrovač (Firewall) FortiGate - 80CM	20 072 Kč
Centrální switch FortiSwitch - 124B - 2x - jednotková cena 17 931,-	35 862 Kč
Instalační a konfigurační práce	68 650 Kč
Zřízení datového připojení + konfigurace- jednorázový poplatek	19 000 Kč
Paušální měsíční poplatek za datové připojení	2 329 Kč
Součet:	**836 693 Kč**

HLAVNÍ KANCELÁŘ	
Komplet PC sestava Lenovo ThinkCentre M92 + Monitor ThinkVision LT2252p 22"	18 075 Kč
Tiskárna HPLJ 3015	8 838 Kč
NB Lenovo Thinkpad T430	30 791 Kč
Součet:	**57 704 Kč**

VZDÁLENÉ LOKALITY	
Pobočková UPS jednotka - Eaton UPS 5S1000i - 4x - jednotková cena 4 307,-	17 228 Kč
Tiskárna HPLJ 3015 4x jednotková cena 8 838,-	35 352 Kč
Komplet PC sestava Lenovo ThinkCentre M92 - 4x - J.C. 18 075,- + Monitor ThinkVision LT2252p 22"	72 300 Kč
Pobočkový směrovač FortiGate - 60D - 4x - jednotková cena 12 048,-	48 192 Kč
Zřízení datového připojení + konfigurace - 4x jednorázový poplatek 19 000,-	76 000 Kč
Paušální měsíční poplatek za datové připojení - 4x - J.C. 1 428,-	5 712 Kč
Součet:	**173 072 Kč**

QPOS pokladní a docházkový systém	
QPOS SERVER - Pokladna	20 000 Kč
QPOS SERVER - Docházka	45 000 Kč
QPOS Software - modul Administrátor	7 500 Kč
Pokladna QPOS Software 4x - jednotková cena 2 500,-	10 000 Kč
Docházka QPOS Software User 4x - jednotková cena 2 500,-	10 000 Kč
Licence na Software na 1 rok užívání	2 400 Kč
SLA ze strany dodavatele 2.typ (tel. Support) měsíční paušál	1 000 Kč
Příslušenství k pokladně - 4x - jednotková cena 4 500,-	18 000 Kč
Příslušenství pro docházku - Biometrická USB čtečka - 4x - jednotková cena 2 800,-	11 200 Kč
Součet:	**125 100 Kč**

Celková sumu navrhovaného projektu:	**1 192 569 Kč**
Cena DPH 21%	250 439 Kč
Celková sumu navrhovaného projektu s DPH:	**1 443 008 Kč**

Tabulka 3: Celkový souhrn nákladů na pořízení a provoz
Zdroj: Vlastní tvorba

6. Závěr

Hlavní cíl, analýza informačních systémů z bezpečnostního hlediska a návrh bezpečnostní infrastruktury byl splněn na základě dílčích cílů předkládané diplomové práce, z kterých postupně vznikaly výsledné návrhy a závěry:

- *Teoretické zkoumání bezpečnostních technik, postupů a opatření*

Formulace úvodních teoretických podkladů jednotlivých bezpečnostních technologií a postupů byl plně využit pro vypracování praktické části diplomové práce. Obě hlavní kapitoly práce jsou úzce provázány a ve výsledku aplikovány do reálného firemního prostředí. Studiem a analýzou odborných materiálů zaměřených na standardy a normy bylo přispěno k vytvoření teoretického podkladu pro definování interního dokumentu bezpečnostní politiky.

- *Analyzovat současný stav ve zvoleném podniku z bezpečnostního hlediska*

Vlastní analýza vybraného podniku odhalila ukázkový příklad decentralizovaného a nezabezpečeného firemního prostředí velice náchylného k výpadku služeb a velkým množstvím rizikových faktorů jako například chybějící záloha interních dat. Na těchto základních analýzách byla stanovena jednotlivá bezpečnostní opatření, která byla demonstrována v další kapitole práce.

- *Navrhnout patřičná bezpečnostní opatření*

Dílčí návrhy bezpečnostních opatření využívají celou množinu vnitřních a vnějších bezpečnostních prvků nabitých z teoretických a praktických podkladů a využité pro samotné aplikování do reálného prostředí. Především došlo k centralizaci infrastruktury a přechod na samosprávu prvků zajišťující bezpečný chod celého systému umístěného v nově vybudované zabezpečené centrální místnosti. Další opatření podpořila vznik nového bezpečného a šifrovaného propojení vzdálených lokalit nebo vytvoření stabilního zálohovacího systému, kterým bylo zcela eliminováno i kritické místo v podobě ztráty interních dat.

- *Připravit dokument bezpečnostní politiky*

Zavedení připravovaného dokumentu v budoucnu poslouží pro kontrolované řízení bezpečnosti informačního systému jako celku. Návrh bezpečnostního dokumentu je založen na doporučených ISO standardech a ostatních normách. Dokument se dotýká všech nově navrhovaných opatření bezpečnostní infrastruktury a určuje pravidla a povinnosti osobám pracujícím v systému. Návrh byl z hlediska správnosti postupů a norem ověřena nezávislým

odborníkem zabývajícím se auditními bezpečnostními kontrolami. V důsledku toho byla doporučena každoroční revizní schůzka k provedení důležitých aktualizací dokumentu.

- *Formulovat obecné a specifické závěry dané problematiky*

Se závazným doporučením aktualizací a průběžných kontrol je samozřejmě svázána i celá bezpečnostní infrastruktura nevyjímaje ani povědomí o aktuální informační bezpečnosti svých zaměstnanců. Hlavně z důvodu dynamického rozvoje bezpečnostních technologií, které zejména reagují na propracovanost kybernetické kriminality, proto z pohledu firmy a ochrany jejich interních dat nelze podcenit žádnou část bezpečnostní infrastruktury. A vždy se zabývat každým incidentem i malého rozsahu, který ve firmě nastane a vyvodit z nich příslušná opatření.

Za specifikum takovýchto návrhů je považována finanční náročnost jednotlivých bezpečnostních opatření, která v oblasti IT nečiní malé náklady. Proto je vždy důležité myslet na případná rizika a ztráty plynoucí z nezabezpečeného systému. Náklady vložené do bezpečnostních opatření mohou narůstat do statisícových částek, jako je tomu v zde v diplomové práci, kde se vybudování centrální místnosti pohybuje okolo 800 000 Kč pro konkrétní řešení. Uvědomme se, že ztrátu dat nelze snadno vyčíslit nebo nahradit finančními prostředky, proto by měly být investice vložené do bezpečnosti chápány pouze pozitivně jako budoucí zisk.

7. Seznam použitých zdrojů:

AEC IT Security Bezpečnostní politika organizace [Online] // AEC.cz. - 7. Listopad 2008. - 25. Únor 2015. - http://www.aec.cz/cz/sluzby/bezpecnostni-politika-organizace.

Beal Vangie [Online] // Webopedia. - Quinstreet Enterprise, 2013. - 22. Leden 2015. - http://www.webopedia.com/TERM/F/firewall.html.

Bigelow Stephen J. Mistrovství v počítačových sítích [Kniha]. - Brno : Computer Press, 2004. - str. 992. - ISBN: 80-251-0178-9.

Bouška Petr Cisco IOS 11 - IEEE 802.1x [Online] // Samuraj-cz.com. - 10. říjen 2007. - 11. prosinec 2014. - http://www.samuraj-cz.com/clanek/cisco-ios-11-ieee-802-1x-autentizace-k-portu-ms-ias/.

Donahue Gary A. Kompletní průvodce síťového experta [Kniha]. - Brno : Computer press, 2009. - ISBN: 978-80-251-2247-1.

Fabián Jaroslav Small Business Solutions I [Online] // SystemOnLine.cz. - 2012. - 1. Březen 2015. - http://www.systemonline.cz/it-security/bezpecnostni-politika-v-malych-organizacich.htm.

Hon Petr [Online] // cisco.com. - Cisco System, Inc., 22. Květen 2012. - 11. Leden 2015. - http://www.cisco.com/web/CZ/expo2012/pdf/T-SECA3-Pripadova-studie-IBM.pdf.

Houser Robert Priority bezpečnostní politiky v malých a středních firmách [Online] // SystemOnLine.cz. - 2013. - 15. Leden 2015. - http://www.systemonline.cz/it-security/priority-bezpecnostni-politiky-v-malych-a-strednich-firmach.htm.

Chlup Marek Bezpečnost ICT a standardy ISO [Článek] // Computerworld. - Praha : IDG Czech, a.s., 2008. - Ročník 19.. - Číslo 2 : Sv. 1.-14.2.

Junek Pavel Zálohování a archivace dat v podnikovém prostředí [Online] // StorageCraft. - 4. září 2013. - 22. leden 2015. - http://www.zalohovani.net/zalohovani-a-archivace-dat-v-podnikovem-prostredi-5-dil-typy-zaloh-a-jejich-rotacni-schemata/.

Klika-BP a.s. Klika-BP, a.s Specialista na požární bezpečnost [Online]. - 2015. - 3. Únor 2015. - http://www.klika.cz/cs/katalog/plynova-shz-fk-komplet.html.

NBÚ Metodický pokyn bezpečnostní dokumentace ver. 3.0 [Online] // NárodníBezpečnostníÚřad.cz. - 15. Září 2014. - 23. leden 2015. - http://www.nbu.cz/cs/ochrana-utajovanych-informaci/bezpecnost-informacnich-systemu/certifikace-informacnich-systemu/metodicke-pokyny/.

NBÚ NBÚ - právní předpisy [Online] // NárodníBezpečnostníÚřad.cz. - 1. Leden 2012. - 3. Prosinec 2014. - http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/vyhlaska-c-5232005/.

NBÚ Ochrana utajovaných informací [Online] // NárodníBezpečnostníÚřad.cz. - 31. Prosinec 2011. - 25. Březen 2015. - http://www.nbu.cz/cs/ochrana-utajovanych-informaci/fyzicka-bezpecnost/informace/.

Ohlhorst Frank [Online] // NetworkComputing. - 1. Březen 2013. - 3. Březen 2015. - http://www.networkcomputing.com/careers-and-certifications/next-generation-firewalls-101/a/d-id/1234097?.

Shinder Debra Littlejohn Počítačové sítě [Kniha]. - Praha : SoftPress, 2003. - str. 752. - ISBN: 80-86497-55-0.

Sikyta Josef Správa IT a fyzická bezpečnost v podniku [Online] // Systemonline. - CCB spol s.r.o., 2011. - 21. Únor 2015. - http://www.systemonline.cz/sprava-it/sprava-it-a-fyzicka-bezpecnost-v-podniku-1.htm.

Strebe Matthew a Perkins Charles Firewally a proxy-servery [Kniha]. - Brno : Computer press, 2003. - ISBN: 80-7226-983-6.

Thomas M. Thomas Zabezpečení počítačových sítí [Kniha]. - Brno : ComputerPress, 2005. - str. 331. - ISBN: 80-251-0417-6.

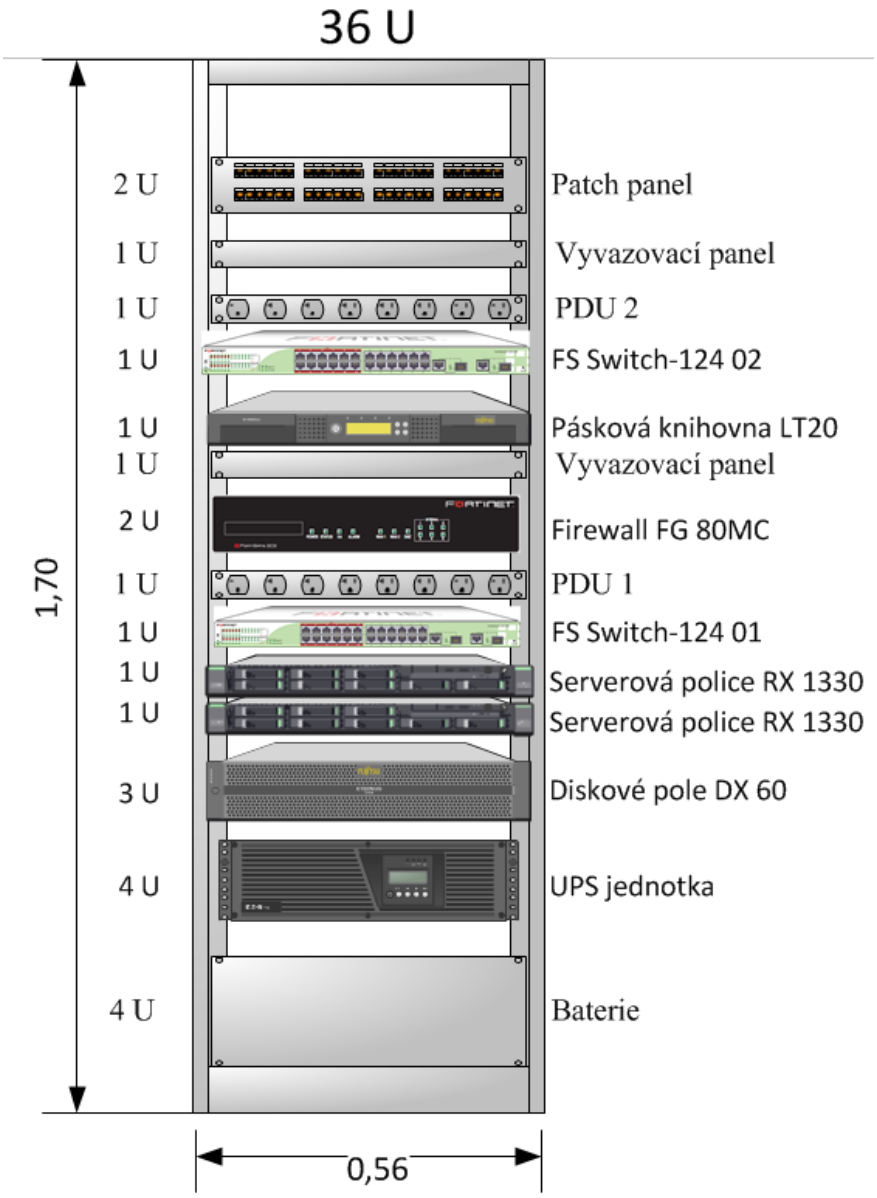
Tobolka Martin Změny a dopady nové normy ISO/IEC 27001:2013 [Článek] // IT Systems. - 2014. - Ročník 16.. - 7-8. - stránky str. 26-27.

Wegner Philip What is a next generation firewall [Online] // Secure edge networks. - 2013. - 12. Únor 2015. - http://www.securedgenetworks.com/security-blog/What-is-a-Next-Generation-Firewall.

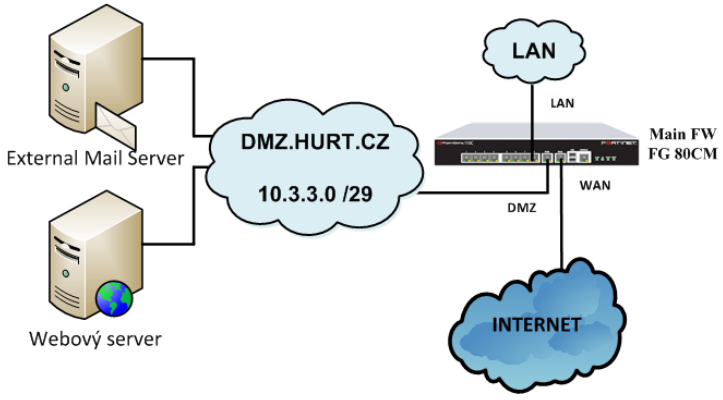
Wenstrom Michael Zabezpečení sítí Cisco [Kniha]. - Brno : Computer press, 2003. - str. 743. - ISBN: 80.7226-952-6.

8. Seznam obrázků a tabulek

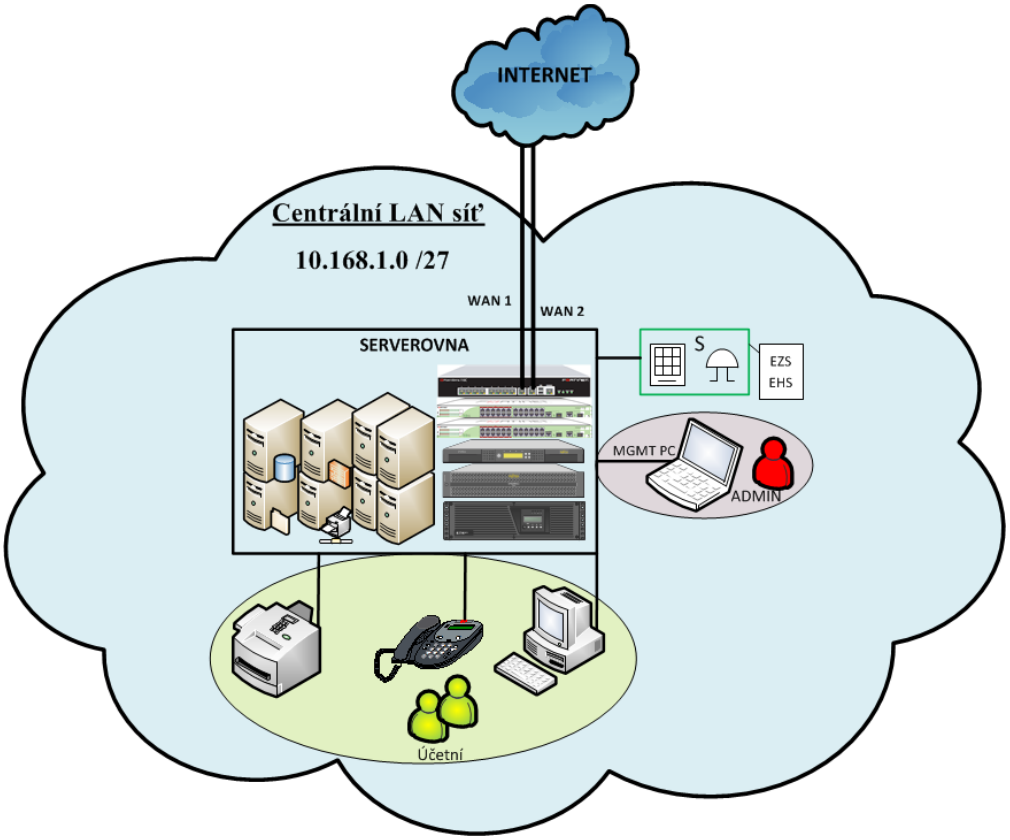
9. Přílohy



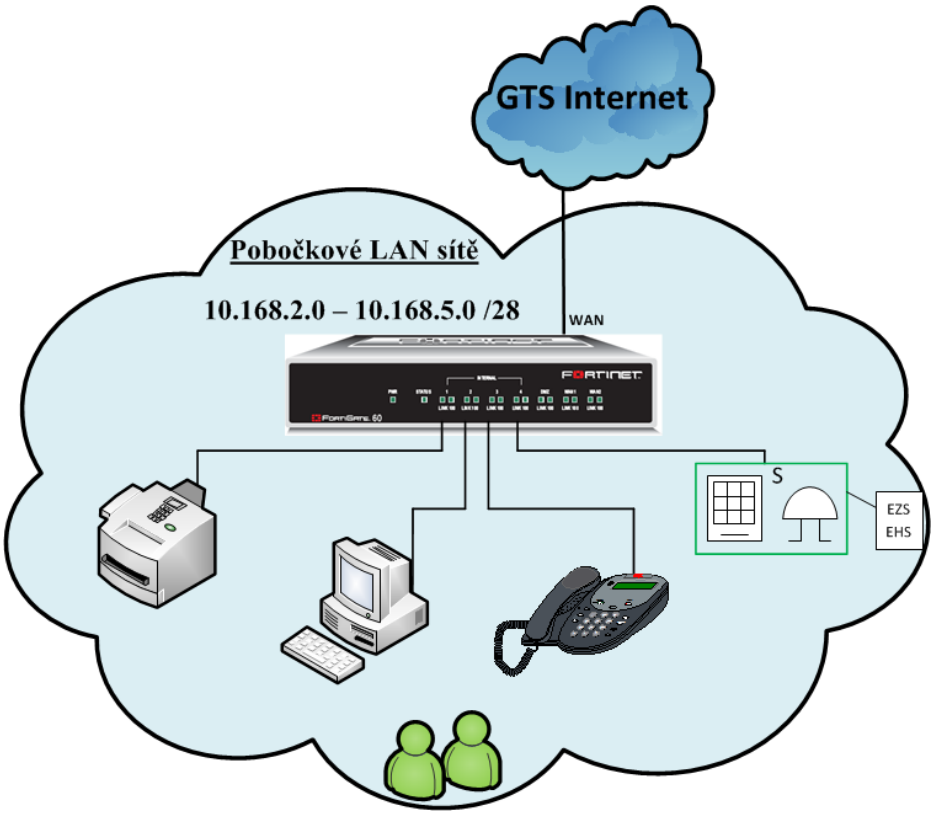
Obrázek 5: Grafické znázornění - osazení rackové skříně
Zdroj: Vlastní tvorba v aplikaci MS Visio



Obrázek 6: Grafické znázornění prvků v zóně DMZ
Zdroj: Vlastní tvorba v aplikaci MS Visio



Obrázek 7: Grafické znázornění centrální LAN sítě
Zdroj: Vlastní tvorba v aplikaci MS Visio



Obrázek 8: Grafické znázornění pobočkové LAN sítě
Zdroj: Vlastní tvorba v aplikaci MS Visio