Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Počítačová bezpečnost a ochrana dat v malých organizacích

Bc. Jaroslav Čech

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Jaroslav Čech

Informatika

Název práce

Počítačová bezpečnost a ochrana dat v malých organizacích

Název anglicky

Computer security and data protection in small organizations

Cíle práce

Primárním cílem této práce je poskytnout přehled o současných trendech v oblasti počítačové bezpečnosti a ochraně dat, vhodně tuto problematiku aplikovat v existujícím firemním prostředí a navrhnout cenovou kalkulaci pro danou firmu.
Dílčí cíle:
- charakterizovat typické síťové útoky, možnosti zabezpečení přenosu a šifrování dat;
- představit moderní trendy v této oblasti, které se používají zejména v menším firemním prostředí;
- zpracovat aktuální stav zabezpečení, analyzovat možnosti fyzické ochrany dat a jejich šifrování v existujícím firemním prostředí;
- vypracovat návrh pro zabezpečení firemního prostředí;
- připravit cenovou kalkulaci;
- formulovat doporučení při zajišťování počítačové bezpečnosti a ochrany dat;
- vyhodnotit závěry vyplývající ze zpracované diplomové práce;

Metodika

V teoretické části práce budou nejprve charakterizovány základní pojmy, představeny typické síťové útoky, možnosti zabezpečení přenosu, šifrování dat a nejčastější chyby z této oblasti.

Následující kapitola bude představovat moderní trendy a nové technologie, budou analyzovány jejich výhody a nevýhody.

Po dokončení teoretické části bude proveden průzkum v existujícím firemním prostředí. Bude analyzován současný stav zabezpečení, fyzická ochrana dat a aktuálně používané technologie. Na základě tohoto průzkumu bude vypracován návrh pro kompletní zabezpečení firemního prostředí.

Výsledkem praktické části bude zpracování cenové kalkulace na zabezpečení firemního prostředí a diskuse s majiteli firmy o navrženém řešení, jak z technického, tak z ekonomického hlediska.

V závěru práce bude doporučen postup při zajišťování počítačové bezpečnosti a ochrany dat, budou shrnuty a diskutovány poznatky a výsledky diplomové práce.

Doporučený rozsah práce

50 – 60 stran

Klíčová slova

Počítačová bezpečnost, ochrana dat, zabezpečení, autentizace, autorizace, šifrování dat, zálohování dat

---

Doporučené zdroje informací

DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Vyd. 1. Brno: Computer Press, 2004. ISBN 80-251-0106-1

HILL, David G. Data protection: governance, risk management, and compliance. Boca Raton, FL: Taylor & Francis, c2009. ISBN 1439806926.

HORÁK, Jaroslav. Bezpečnost malých počítačových sítí: (praktické rady a návody). 1. vyd. Praha: Grada, 2003. Podrobný průvodce začínajícího uživatele. ISBN 80-247-0663-6

HUNT, Craig. TCP/IP network administration. Beijing: O'Reilly & Associates, 2002. ISBN 0-596-00297-1

PETERKA, Jiří. Přednášky. eArchiv.cz: archiv článků a přednášek Jiřího Peterky. [online]. 2015 [cit. 2016-04-08]. Dostupné z:http://www.earchiv.cz/i_prednasky.php3

Předběžný termín obhajoby

2016/17 LS – PEF

Vedoucí práce

Ing. Jiří Vaněk, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 23. 5. 2016

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 2. 8. 2016

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 31. 03. 2017

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Počítačová bezpečnost a ochrana dat v malých organizacích" jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů 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 30.3.2017 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Jiřímu Vaňkovi, Ph.D. za cenné rady, připomínky a vedení diplomové práce. Dále bych chtěl poděkovat své rodině za neustálou podporu během celého studia.

Počítačová bezpečnost a ochrana dat v malých organizacích

Souhrn

Tato diplomová práce je zaměřena na problematiku počítačové bezpečnosti a ochrany dat v malých organizacích. V teoretické části práce jsou charakterizovány vybrané bezpečnostní oblasti. Nejprve jsou představeny základní pojmy pro tvorbu počítačových sítí a služeb. Následně jsou definovány bezpečnostní hrozby a možnosti prevence před nimi. Praktická část práce se zaměřuje na analýzu bezpečnosti a ochrany dat v reálném firemním prostředí. Součástí analýzy je zhodnocení oblastí, ve kterých by mohl vzniknout bezpečnostní problém. Vyhodnocen je zejména využívaný hardware, jeho konfigurace a stav. Na základě této analýzy jsou aplikovány změny v dané společnosti, které jsou vyžadovány pro vylepšení zabezpečení. Součástí změn je konfigurace stávajících zařízení a doporučení nákupu nového hardware. Výsledkem práce je celkové zlepšení počítačové bezpečnosti a ochrany dat daného podniku.

Klíčová slova: Počítačová bezpečnost, ochrana dat, zabezpečení, autentizace, autorizace, šifrování dat, zálohování dat

Computer security and data protection in small organizations

Summary

This thesis is focused on computer security and data protection in small organizations. In the theoretical part are characterized selected security areas. The basic concepts for the creation of computer networks and services are introduced. Consequently there are defined security threats and prevention possibilities before them. The practical part is focused on the analysis security and data protection in real business environment. The evaluation of the areas is part of analysis where could be created a safety threat. On the basis of this analysis are applied changes in the company, which are required to improve safety. The part of the changes are the configuration of existing equipment and recommendations of purchase new hardware. The result is an overall improvement in computer security and data protection of the company.

Keywords: Computer security, data protection, security, authentication, authorization, data encryption, data backup

Obsah

1. Úvod 11

2. Cíl práce a metodika 12

2.1. Cíl práce 12

2.2. Metodika 12

3. Teoretická východiska 14

3.1. Základní pojmy 14

3.1.1 Local area network 14

3.1.2 Transmission Control Protocol/Internet Protocol 14

3.1.3 Dynamic Host Configuration Protocol 17

3.1.4 Hypertext Transfer Protocol 18

3.2. Síťové útoky 18

3.2.1 Man in the middle 19

3.2.2 Distributed Denial of service 21

3.3. Ochrana organizace 24

3.3.1 Bezpečnostní politika 24

3.3.2 Firewall 26

3.3.3 Antivirový program 27

3.3.4 Intrusion detection system 28

3.4. Zabezpečená spojení 28

3.4.1 Virtual Private Network 29

3.4.2 Wi-Fi Protected Access 2 30

3.4.3 Hypertext Transfer Protocol Secure 30

3.5. Šifrování dat 30

3.5.1 Šifrování souboru 30

3.5.2 Šifrování emailu 31

3.5.3 Šifrování disku 33

3.6. Nejčastější chyby 34

4. Vlastní práce 36

4.1. Charakteristika společnosti 36

4.1.1 Organizační struktura 36

4.2. Definice zadání 37

4.3. Počítačová síť 38

4.3.1 Bezdrátová síť 40

4.3.2 Vzdálený přístup 40

4.4. Přehled stavu ICT 41
4.4.1 Aktivní prvky 41
4.4.2 Koncové stanice 42
4.4.3 Servery 43
4.5. Zaměstnanci 43
4.6. Fyzická bezpečnost 44
4.6.1 Budova 44
4.6.2 Serverovna 44
4.7. Ostatní oblasti 44
4.7.1 Zálohování dat 44
4.7.2 Politika hesel 45
4.7.3 Šifrování 45
4.8. Návrh a provedené změny 45
4.8.1 Výměna routeru 45
4.8.2 Nasazení domény 50
4.8.3 Konfigurace serveru 52
4.8.4 Zaměstnanci 54
4.8.5 Výměna PC s Windows XP 54
4.8.6 Stanice 56

5. Výsledky a diskuse 57

6. Závěr 59

7. Seznam použitých zdrojů 60

8. Přílohy 66

Příloha 1 : Seznam použitých zkratek 67

Seznam obrázků

Obrázek 1: Architektura TCP/IP 15
Obrázek 2: Princip DHCP 17
Obrázek 3: Útok man in the middle 19
Obrázek 4: Útok ARP spoofing 20
Obrázek 5: Útok SYN flooding 23
Obrázek 6: Spojení přes VPN 29
Obrázek 7: Schéma použití asymetrické kryptografie pro šifrování zpráv 32
Obrázek 8: Schéma použití asymetrické kryptografie pro elektronický podpis 33

Obrázek 9: Schéma zapojení počítačové sítě LAMPS, a.s. 39
Obrázek 10: Přehled IP adresace 46
Obrázek 11: Nastavení NAT maškarády 46
Obrázek 12: Nastavení výchozích bran 49
Obrázek 13: Nastavení kontroly gateway pomocí ping 49
Obrázek 14: Zakázání facebooku 49
Obrázek 15: Vytvoření GPO Mapování disku 50
Obrázek 16: Nastavení Mapování disku 51
Obrázek 17: Přiřazení GPO k dané doméně 51
Obrázek 18: Přihlašovací obrazovka ESET Remote Administrator 52
Obrázek 19: Přidání nové politiky 53
Obrázek 20: Přidání nové politiky 53

Seznam grafů

Graf 1: Motivace k síťovým útokům 19
Graf 2: Používáné útoky DoS 22

Seznam tabulek

Tabulka 1: Konfigurace Wi-Fi 40
Tabulka 2: Varianta 1 – Nové PC 55
Tabulka 3: Varianta 2 – Nové PC 55
Tabulka 4: Cenová kalkulace č. 1 57
Tabulka 5: Cenová kalkulace č. 2 57
Tabulka 6: Přehled změn nad současným hardware 58

1. Úvod

Diplomová práce navazuje na bakalářskou práci Analýza a demonstrace vybraných síťových útoků z roku 2015 a rozšiřuje problematiku o počítačovou bezpečnost a ochranu dat. [1]

Všechny organizace existují za určitým cílem, nejčastěji se snahou vygenerovat zisk. Tato snaha vyžaduje materiální, lidské a finanční zdroje. Pro organizace je nutné si veškeré zdroje chránit před ztrátou, zcizením nebo poškozením.

Jednou z mnoha oblastí, kterou musejí organizace zabezpečit je bezpečnost informačních technologií, používaných v dané organizaci. Oblast je to velmi široká a nové hrozby vznikají denně. Z tohoto hlediska je vyžadováno, aby každá organizace zavedla bezpečností politiku, od správného nastavení zařízení v podnikové síti až po školení zaměstnanců.

Nevhodné zabezpečení by mohlo poškodit společnost z ekonomického hlediska. Je vhodné si nechat vždy vypracovat komplexní návrh bezpečnosti od zkušeného odborníka, neboť síla bezpečnosti je stejně velká jako její nejslabší článek.

Diplomová práce se zabývá analýzou bezpečnosti v existující společnosti LAMPS, a.s., vypracováním návrhu na zlepšení bezpečnosti v oblastech, ve kterých bude zjištěna nedostatečná úroveň zabezpečení. Po vypracování návrhu je vedení společnosti nabídnuto několik variant na celkové zlepšení bezpečnosti IT. V závěru práce jsou shrnuty veškeré poznatky z analýzy a návrhu nové bezpečností politiky.

2. Cíl práce a metodika

2.1. Cíl práce

Hlavním cílem diplomové práce je poskytnutí přehledu o současných trendech v oblasti počítačové bezpečnosti a ochrany dat, vhodně tuto problematiku aplikovat v existujícím firemním prostředí a navrhnout cenovou kalkulaci pro danou společnost.
Dílčími cíli jsou:

- charakterizovat typické síťové útoky, možnosti zabezpečení přenosu a šifrování dat
- představit moderní trendy v této oblasti, které se používají zejména v menším firemním prostředí
- zpracovat aktuální stav zabezpečení, analyzovat možnosti fyzické ochrany dat a jejich šifrování v existujícím firemním prostředí
- vypracovat návrh pro zabezpečení firemního prostředí
- aplikovat změny schválené vedením společnosti při analyzování
- připravit cenovou kalkulaci
- formulovat doporučení při zajišťování počítačové bezpečnosti a ochrany dat
- vyhodnotit závěry vyplývající ze zpracované diplomové práce

2.2. Metodika

V teoretické části práce budou nejprve charakterizovány základní pojmy, představeny typické síťové útoky, možnosti zabezpečení přenosu, šifrování dat a nejčastější chyby správců počítačových sítí a uživatelů z této oblasti.

Po dokončení rešerše bude proveden průzkum v existujícím firemním prostředí. Bude analyzován současný stav zabezpečení, fyzická ochrana dat a aktuálně používané technologie. V rámci této analýzy bude analyzován současný stav počítačové sítě, zálohování dat, koncových stanic a další oblasti, které souvisejí s počítačovou bezpečností. Na základě tohoto průzkumu bude vypracován návrh pro komplexní zabezpečení firemního prostředí. Součástí návrhu budou úpravy v souladu s aktuálními trendy a doporučovanými postupy v oblasti počítačové bezpečnosti a ochrany dat.

Výsledkem práce bude zpracování cenové kalkulace na zabezpečení firemního prostředí, provedení některých návrhů ihned po analyzování a diskuse s majiteli firmy o navrženém řešení, jak z technického, tak z ekonomického hlediska.

3. Teoretická východiska

3.1. Základní pojmy

Následující kapitola se věnuje základním pojmům, které tvoří teoretický základ diplomové práce. Jsou zde vysvětleny základní používané protokoly TCP/IP, pojem lokální počítačová síť a charakterizovány nejpoužívanější protokoly. Následující pojmy jsou základem pro tvorbu sítí a služeb běžících v síti

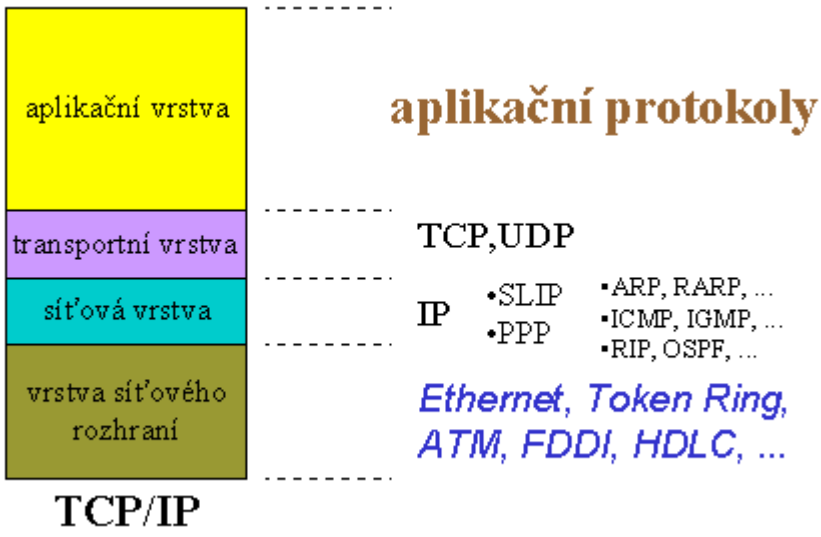
3.1.1 Local area network

Local area network (LAN) je označení pro počítačovou síť, rozléhající se na relativně malé geografické oblasti. Používá se pro propojení prvků v rámci místnosti, budovy, skupin budov, v rámci domácnosti nebo podnikové sítě. Nejčastějším způsobem zapojení je pomocí technologií Ethernet a Wi-Fi. K propojení cílových uzlů se v této síti používají aktivní a pasivní prvky, nejčastěji switche a routery. Jednotlivé prvky jsou propojeny kroucenou dvojlinkou, koaxiálním kabelem, optickým vláknem nebo bezdrátově. V těchto sítích jsou dosahovány vysoké přenosové rychlosti, v řádech Gb/s. [2]

3.1.2 Transmission Control Protocol/Internet Protocol

Transmission Control Protocol/Internet Protocol (TCP/IP) je síťová architektura obsahující čtyři vrstvy programového vybavení. Počátky tohoto standardu se datují do konce 60. let, k projektu účelové agentury Advanced Research Projects Agency (ARPA) ministerstva obrany USA, která si nechala tyto nové protokoly vyvinout pro svou počítačovou síť ARPANET. První specifikace tohoto protokolu byla prezentována v září roku 1974 na počítačové konferenci na Univerzitě v Sussexu [3]. Koncem 70. let získaly tyto nové protokoly svou dnešní podobu a postupně začaly být používány v síti ARPANET, která se později stala zárodkem a páteří konglomerátu sítí, dnes nazvané Internet.

Architektura je členěna do čtyř vrstev, znázorňující hierarchii činností. Výměna informací mezi jednotlivými vrstvami je přesně definována pravidly. Každá vrstva poskytuje své služby vrstvě vyšší a využívá služeb nižších vrstev. [2]



Obrázek 1: Architektura TCP/IP [4]

Členění architektury TCP/IP do čtyř vrstev [5]:

- **Vrstva síťového rozhraní (network interface)** je nejnižší vrstvou tohoto modelu, starající se o vše, co je spojeno s ovládáním konkrétní přenosové cesty, vysíláním a příjmem datových paketů. V této vrstvě jsou definovány metody přístupu na médium. TCP/IP tuto vrstvu blíže nespecifikuje, neboť zde velmi záleží na konkrétní přenosové technologii.

- **Síťová vrstva (internet layer)** zajišťuje přenos jednotlivých paketů od odesilatele ke svému příjemci, přes případné směrovače. Hlavním požadavkem kladeným na tuto vrstvu je rychlost přenosu dat, v důsledku čehož vrstva nezajišťuje spolehlivost přenosu dat. Spolehlivost si musí samostatně zajištovat vyšší vrstvy nebo samotné aplikace. Síťová vrstva je opatřena IP protokolem.

- **Transportní vrstva (transport layer)** je třetí vrstvou architektury TCP/IP a je často označována jako TCP vrstva, neboť její realizace je nejčastěji pomocí protokolu TCP. Účelem této vrstvy je zajištění přenosu mezi koncovými účastníky, kterými jsou v tomto případě přímo aplikační programy. Podle potřeby může transportní vrstva zajišťovat spolehlivost přenosu a také změnit charakter přenosu z nespojovaného na spojovaný. Dalším používaným protokolem na této vrstvě je například protokol UDP, který nezajišťuje spolehlivost přenosu.

- **Aplikační vrstva (application layer)** je čtvrtou a nejvyšší vrstvou modelu TCP/IP, jejími entitami jsou jednotlivé aplikační programy, které komunikují s transportní vrstvou. Oproti modelu ISO/OSI [6] sdružuje dohromady aplikační, prezentační a relační vrstvu.

Základní protokoly TCP/IP:

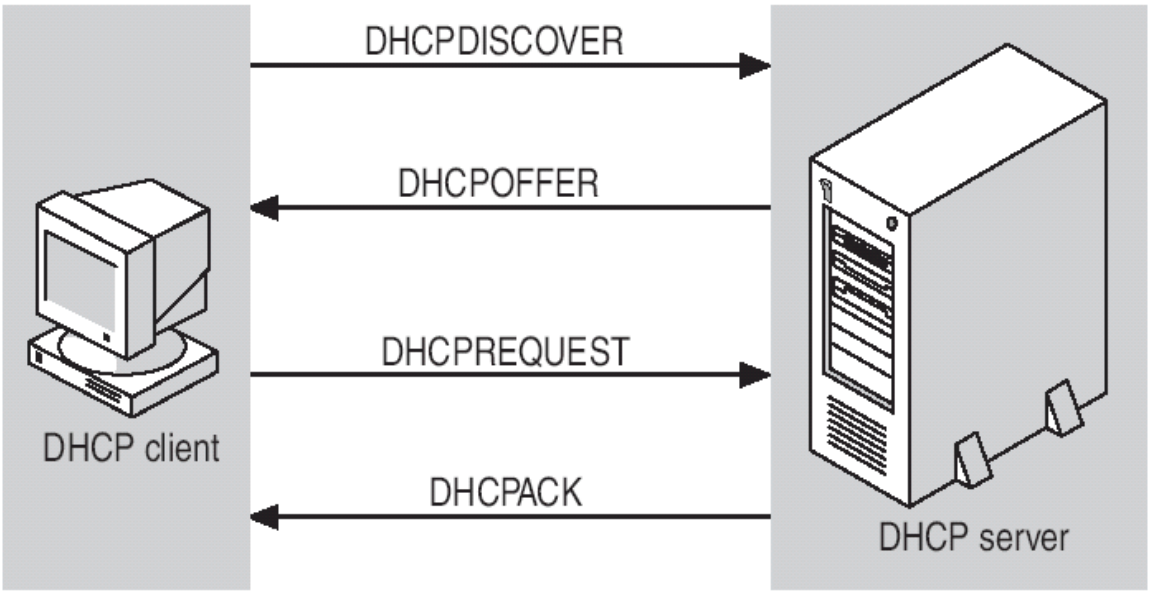
- **Address Resolution Protocol (ARP)** je standardizovaný protokol, který slouží k vyhledání MAC adresy k zadané IP adrese, je definován v RFC 826 [7]. Tento protokol zjišťuje MAC adresu pomocí broadcastového dotazu, na který mu odpoví pouze cílová stanice, která má nastavenou hledanou IP adresu. Tento protokol pracuje na síťové vrstvě modelu TCP/IP.

- **Internet Control Message Protocol (ICMP)** je protokol, definovaný v RFC 792 [8], který je nezbytnou součástí IP protokolu. Všechny uzly, které mají implementovaný IP protokol musí podporovat i ICMP. Nejvíce používaným způsobem je zasílání zpráv, definovaných v RFC 1122 [9], o chybách IP datagramů při přenosu. ICMP protokol se dále využívá pro routovací a diagnostické účely.

- **Internet Protocol (IP)** slouží pro komunikaci v počítačových sítí a v síti Internet, jedná se o hlavní komunikační protokol. Pracuje na síťové vrstvě modelu TCP/IP. První verzí tohoto IP protokolu byla verze IPv4, který je dnes dominantní na síti Internet. Jejím nástupcem je protokol IPv6, který se postupně rozšiřuje. [2]

3.1.3 Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) je protokol, používaný v modelu TCP/IP. Standard DHCP vznikl v roce 1993 v RFC 1531 [10] jako nástupce protokolu BOOTP, se kterým není zpětně kompatibilní. Používá se pro automatickou konfiguraci klientů v rámci sítě. Zjednodušuje a umožňuje centralizovanou správu počítačové sítě. DHCP poskytuje klientům typicky platnou IP adresu, výchozí bránu, adresu DNS serveru, masku sítě, dalšími parametry, které může poskytovat jsou například servery pro NTP a WINS.



Obrázek 2: Princip DHCP [11]

Princip činnosti DHCP:

Komunikace probíhá pomocí protokolu UDP na portech 68 na straně klienta a portu 67 na straně serveru. Klient po připojení do sítě vyšle DHCPDISCOVER paket broadcastem. Na tento paket odpoví server DHCP paketem DHCPOFFER obsahující nabízenou IP adresu. Klient po obdržení paketu a vybrání IP adresy odpoví serveru zpět paketem DHCPREQUEST. Server následně potvrdí přiřazení paketem DHCPPACK, po jehož obdržení již může klient zadanou IP adresu používat. Po vypršení lhůty platnosti

si klient musí obnovit svou IP adresu, případně ji přestat používat, pokud nedostane platné potvrzení. [12]

Server poskytuje IP adresu dynamicky z předem definovaného intervalu nebo staticky, ze seznamu, který je nakonfigurován na serveru. Tento seznam je vázán na zadanou MAC adresu žadatele. Klient se zadanou MAC adresou následně obdrží zadané parametry.

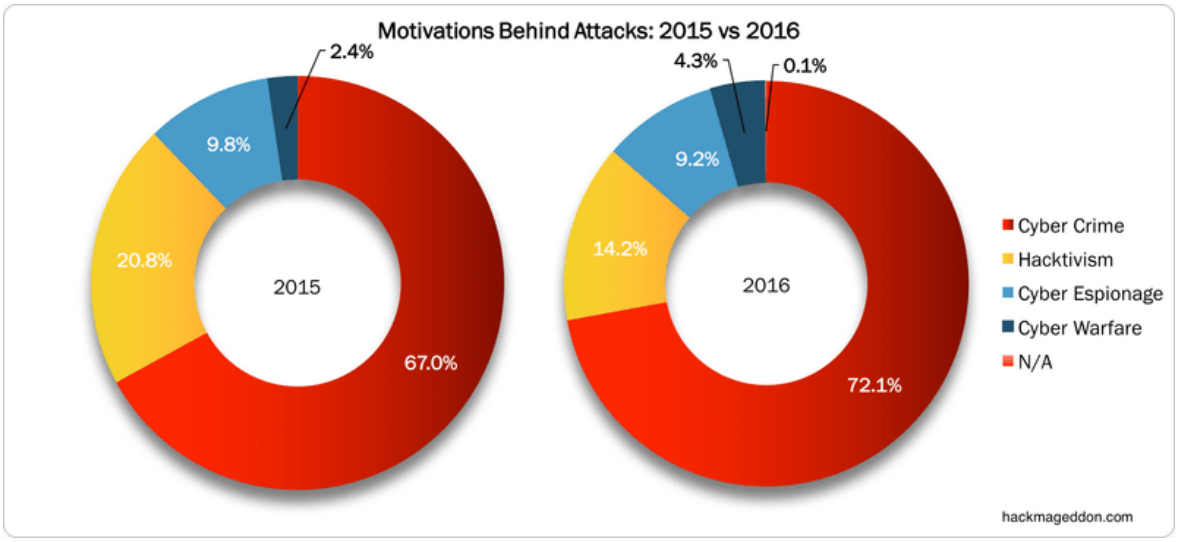
3.1.4 Hypertext Transfer Protocol

Hypertext Transfer Protocol (HTTP) je internetový protokol určený pro výměnu dokumentů ve formátu HTML, jehož poslední verze 1.1 je definována v RFC 2616[12]. Používá se obvykle na portu 80. Jedná se o nejpoužívanější protokol, který se zasloužil o rozmach Internetu.

Protokol funguje na jednoduchém principu dotaz-odpověď. Jestliže uživatel zašle po obdržení odpovědi další dotaz na stejný server, bude se jednat o nezávislý dotaz a odpověď, jelikož nelze rozpoznat, zda dotaz souvisí s předchozí komunikací či nikoli. Kvůli této vlastnosti je tento protokol nazýván bezstavový [13]. Komunikace v rámci tohoto protokolu probíhá nezabezpečeně, pro zabezpečený přenos je potřeba využít protokol HTTPS.

3.2. Síťové útoky

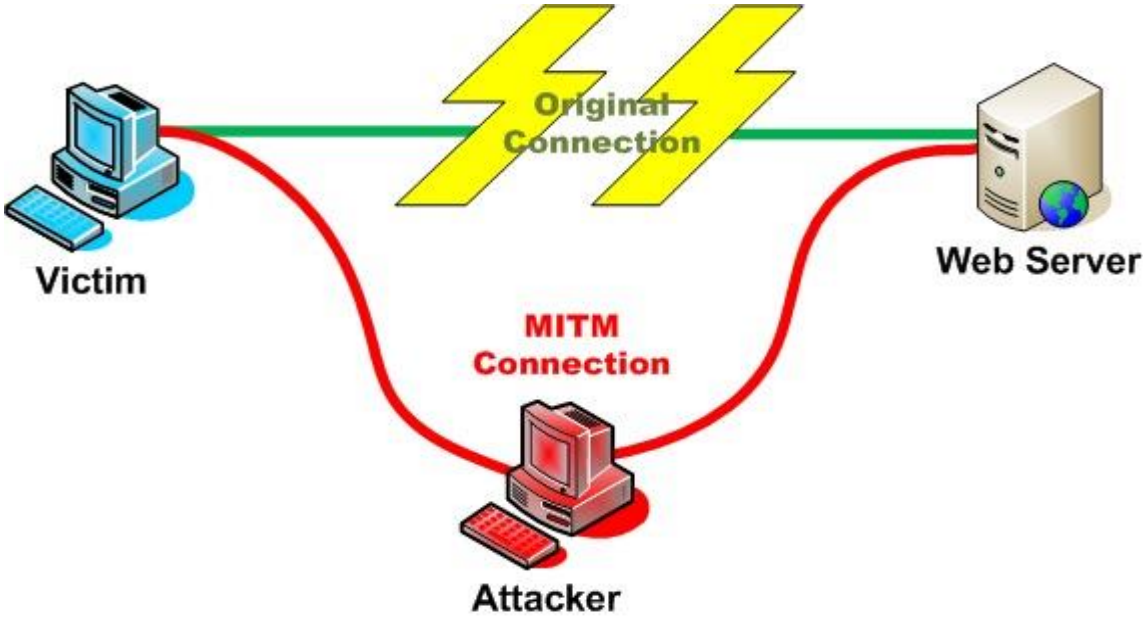
Ve druhé kapitole teoretické části jsou charakterizovány základní síťové útoky. Tyto útoky jsou rozděleny do dvou kategorií z hlediska způsobu útoku, man in the middle a denial of service. Z hlediska bezpečnosti bude v následujících částech věnována pozornost základním síťovým útokům v kapitolách 3.2.1 a 3.2.2, více do hloubky této problematiky je zaměřena bakalářská práce autora [1]. Bezpečnostní hrozba v této oblasti neustále roste, neboť počet síťových útoků stoupá každým rokem, na grafu č. 1 je znázorněna motivace útočníků pro takové útoky.



Graf 1: Motivace k síťovým útokům [14]

3.2.1 Man in the middle

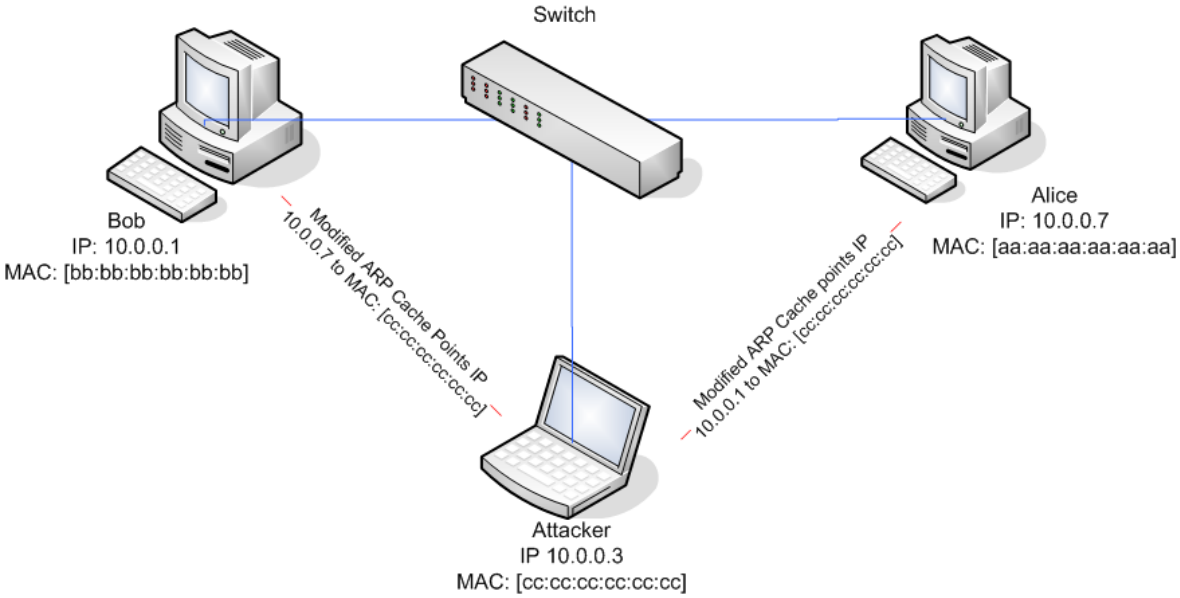
Cílem tohoto útoku je aktivní snaha útočníka stát se aktivním prostředníkem mezi komunikujícími stranami a odposlouchávat komunikaci mezi nimi. Útočník se vydává zpravidla za obě komunikující strany a snaží se získat přístup k informacím, které si snaží obě strany poslat. Útočník může komunikaci odposlouchávat a přeposílat k původním adresátům, případně zprávu modifikovat. [15]



Obrázek 3: Útok man in the middle [16]

Arp spoofing

Arp spoofing je síťový útok typu man in the middle, tento druh útoku se snaží přesvědčit oběť, že daná IP adresa odpovídá jiné MAC adrese, zpravidla útočníkově. Toho se útočník snaží docílí rozesíláním paketu tzv. ARP reply, obsahující útočníkovu MAC adresu a cílovou IP adresu, všem zařízením v síti. Informace obsažené v tomto paketu si cílové stanice zapíši do ARP cache a následná komunikace určená pro původní adresu bude směrována na adresu útočníka. [17]



Obrázek 4: Útok ARP spoofing [18]

Příklad útoku ARP spoofing

Počítač Boba chce komunikovat s počítačem Alice, bohužel s ním nemůže komunikovat, jelikož nemá uloženou jeho MAC adresu. Zašle tedy do sítě broadcastově ARP request a čeká na odpověď. Jelikož protokol ARP nemá implementovány žádné obranné mechanismy, stačí útočníkovi zachytit tuto žádost a zaslat modifikovanou odpověď zpět Bobovi. Následně Bob zasílá komunikaci určenou pro Alici přes počítač útočníka. [19]

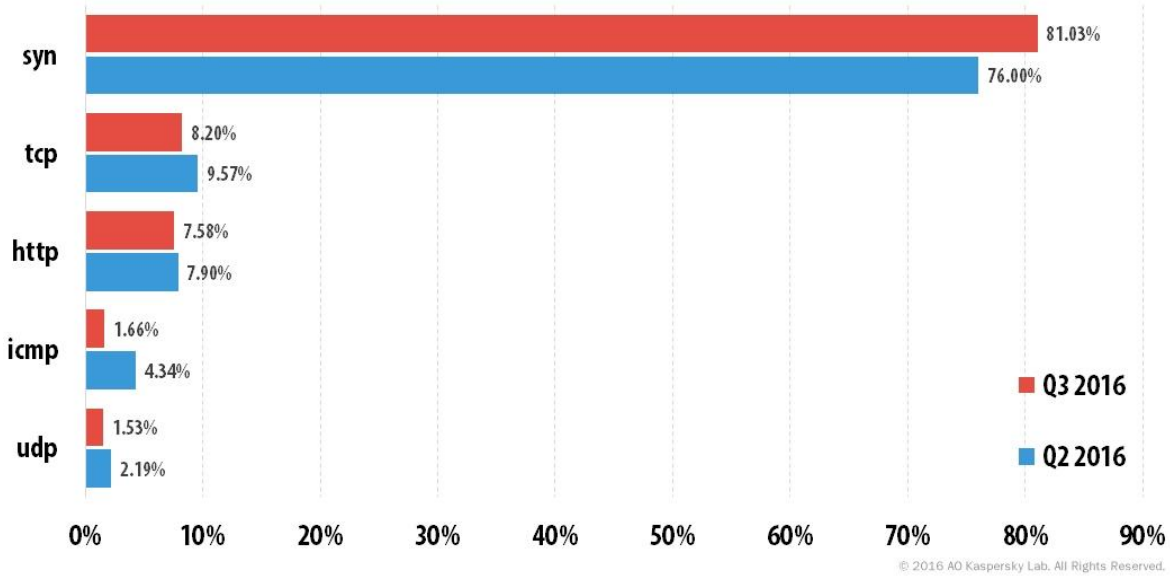
Možnosti obrany proti ARP spoofing

- **Statické ARP záznamy** je metoda obrany spočívající ve vytvoření ARP cache staticky na každém počítači. Jelikož uživatel nejčastěji pracuje se sítí Internet, kam také odesílá nejčastěji svá data, je vhodné si přidat do ARP cache statickou položku výchozí brány. Pro úplné zabezpečení je nutné definovat záznamy pro všechna zařízení v síti, čehož lze dosáhnout dávkovým souborem, který nejprve vymaže veškeré záznamy z ARP cache a následně ji naplní námi definovanými hodnotami. Tento dávkový soubor je vhodné umístit na server, aby ho klientské počítače mohly vždy spustit po startu. Pokud se následně do sítě zapojí nové zařízení, bude fungovat správně, pouze nebude ochráněno. [20]

- **Dynamic ARP Inspection** je bezpečnostní funkce, která zabraňuje přeposílání neplatných ARP dotazů a odpovědí na jiné porty switche. Vylepšenou variantou je funkce IP Source Guard [21], která blokuje veškerý provoz s neoprávněnou IP adresou odesílatele, s výjimkou DHCP. Ke správné funkčnosti je potřeba zabránit vytváření neoprávněných DHCP serverů na síti, čehož docílíme DHCP snoopingem, tedy možností stanovit, za kterými porty se může nacházet DHCP server. Pokusí-li se někdo připojit mimo daný port dojde k zabránění komunikace na úrovni switche. [21]

3.2.2 Distributed Denial of service

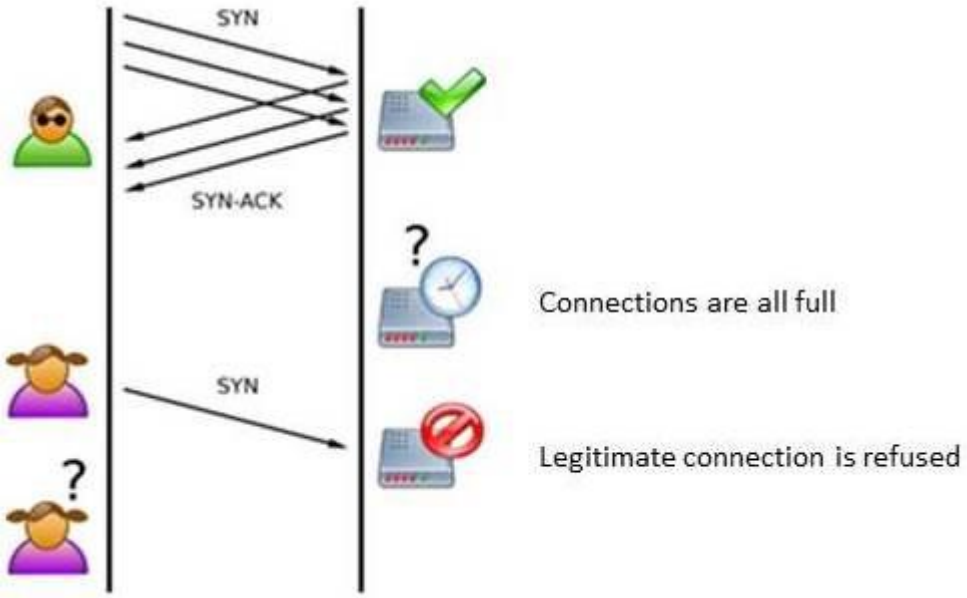
Distributed Denial of service (DDoS) je síťový útok s cílem úmyslného přetížení nějaké služby pomocí více zdrojů. V útoku jde převážně o narušení komunikace mezi klientem a serverem, v takovém rozsahu, že cílová služba bude nepoužitelná. V rámci jednoho útoku na službu je vhodné kombinovat více typů útoků, aby se server nedokázal efektivně bránit. Útočník využívá pro útok také počítače, dříve napadnuté malwarem, těmto počítačům zasílá instrukce, na jaký server a v jakou dobu mají zaútočit. V důsledku čehož mohou být útočících zařízení desetitisíce. [22] Na grafu č. 2 je jsou znázorněny nejčastější metody útoku DDoS.



Graf 2: Používáné útoky DoS [23]

SYN flood

SYN flood je útok typu DDoS, jehož cílem je způsobit nefunkčnost určité služby, zpravidla webové služby. Vhodně navržený SYN flood dokáže velmi rychle přetížit webový server. Podstatou útoku je využití vlastnosti TCP protokolu, three-way handshake. TCP je nejběžnějším spojením mezi uživatelem a serverem. Přes TCP se například navštěvují webové stránky nebo stahují emaily. Na začátku komunikace probíhá navázání spojení mezi účastníky komunikace. Uživatel nejprve vyšle na server synchronizační paket SYN, což je žádost o navázání komunikace. Server mu zašle zpět SYN-ACK paket, což představuje potvrzení synchronizace. Uživatel dokončí navázání spojení poslední paketem ACK. [24]



Obrázek 5: Útok SYN flooding [25]

Příklad útoku SYN flood

Pokud je znám princip navazování komunikace pomocí TCP, je provedení útoku již snadné. [1] Stačí serveru zasílat dostatečné množství SYN paketů, na které server musí zasílat odpovědi a čekat na dokončení spojení. Útočník bude ignorovat odpovědi ze serveru, čímž způsobí, že server bude muset udržovat velké množství polootevřených spojení, na které bude potřebovat systémové prostředky. Po vyčerpání systémových prostředků server již nebude schopen reagovat na nové žádosti o spojení a stane se nedostupným. Jelikož útočník v tomto útoku nepotřebuje obdržet odpověď ze serveru, je pro něho vhodné maskovat svou činnost průběžnou změnou IP adresy.

Možnosti obrany proti SYN flood

- **SYN cookies** je aktivní metoda ochrany, která využívá vlastnosti, že určení hodnoty initial sequence number, která se využívá u three-way handshake, je na straně serveru [1]. Server nejprve vypočítá odpověď ze zdrojové adresy, portu a dalších hodnot, následně odešle odpověď SYN+ACK a polootevřené spojení uzavře. Jestliže obdrží následně ACK paket obsahují initial sequence number, které

odpovídá tomu, které mohl vygenerovat otevře spojení, jako kdyby existovalo polootevřené spojení. Výhodou této metody je relativní jednoduchost, nevýhodou teoretická možnost uhodnutí výpočtu. Kvalitní hashovací funkce spotřebovává výpočetní čas, proto se metoda používá, pokud jsou buffery pro polootevřené spojení již zaplněny. [26]

- **Filtrování paketů** je možnost inteligentního filtrování paketů spočívající v udržování seznamu všech SYN paketů za určitý časový úsek. Pokud by došlo k překročení počtu přicházejících paketů na jeden soket, porovnala by se charakteristika takových paketů a následně by se podezřelé spojení uzavřelo. Nevýhodou tohoto algoritmu je, že detekce by musela být velice chytrá a rychlá. [26]

3.3. Ochrana organizace

Následující kapitola charakterizuje základní obranné mechanismy, které může společnost používat pro svou ochranu před vnějšími, ale i vnitřními útoky. Je zde charakterizována bezpečnostní politika, kterou by si měla stanovit každá společnost. Poté jsou vysvětleny pojmy, se kterými se lze setkat během tvorby bezpečností politiky.

3.3.1 Bezpečnostní politika

Bezpečností politika je komplexní soubor pravidel, která vedou k zajištění ochrany dat, ochraně před bezpečnostními riziky a hackerskými útoky z nejrůznějších stran. Žádný podnik či organizace nemůže pokrýt všechny oblasti bezpečnosti, z důvodu finančního nebo personálního. Je třeba vždy najít optimální řešení a zabezpečit zejména klíčové oblasti v dané firmě.

Bezpečností politika obsahuje celou řadu oblastí [27]:

- **Fyzická bezpečnost** neboli místo, kde dochází k fyzickému skladování dat. Nutná identifikace, zda je toto místo vhodné z hlediska fyzického přístupu, zda je zajištěno z hlediska požáru či jiné přírodní pohromy.

- **Zálohování a archivace dat** je prevencí před ztrátou a změnou dat. Zálohování je určeno k uchovávání operativních dat, která mohou být rychle obnovena v případě incidentu. Archivace je důležitá z hlediska uchování historických záznamů, často stanovené zákonem.

- **Zabezpečení před viry a malwarem** je základním opatřením, které zabraňuje průniku virů, mělo by být nainstalováno na poštovním serveru, internetové bráně a koncovém zařízení. Ochrana by měla být založena na kombinaci různých antivirových jádrech, tak aby bylo zachycení virů co nejefektivnější.

- **Patch management** je proces několika kroků, vedoucí k pravidelným aktualizacím softwarového vybavení. Nutná je pravidelná aktualizace veškerého software od Windows Update po aplikace třetích stran.

- **Externí přístup k datům** znamená definování pravidel pro přístup do podnikové sítě, zejména z domácí kanceláře a na cestách.

- **Periodické kontroly a audit** jsou klíčovou oblastí pravidelné kontroly nastavené bezpečností politiky. Tuto kontrolu je možné provádět manuálně nebo pomocí specializovaného software pro skenování zařízení v síti, který provede kontrolu plně automaticky. Doporučený je také pravidelný audit nezávislou kontrolou.

3.3.2 Firewall

Firewall je softwarový nebo hardwarový nástroj, který odděluje provoz mezi dvěma sítěmi a slouží jako bezpečností brána. Jedná se o první linii síťové bezpečnosti. Firewall monitoruje veškerou příchozí a odchozí komunikaci, rozhoduje, zda dané spojení na základě předem definovaných bezpečnostních pravidel povolit či zakázat. Pravidla zahrnují identifikaci zdroje a cíle dat, zdrojový a cílový port, modernější firewally využívají informace o stavu spojení, znalost kontrolovaných protokolů a případně prvky IDS. Vytváří bariéru mezi zabezpečenou a kontrolovanou vnitřní sítí a důvěryhodnými a nedůvěryhodnými vnějšími sítěmi, například Internetem.

Základní rozdělení firewallů:

- **Paketový filtr** je nejstarší a nejjednodušší formou firewallu, která spočívá v kontrole, zda ze zdrojové adresy a portu může být paket doručen na cílovou adresu a port v předem definovaných pravidlech. Paket je poté buď propuštěn nebo zamítnut. Výhodou tohoto řešení je vysoká rychlost zpracování, proto se dnes používají zejména na místech, kde není potřebná přesnost nebo důkladná analýza procházejících dat, ale spíše rychlý přenos velkého množství dat. Nevýhodou je nízká úroveň kontroly procházejících spojení, která u složitější protokolů není dostatečná. [28]

- **Aplikační brána** funguje na úrovni aplikační vrstvy, rozhoduje se tedy podle údajů příslušných k aplikační vrstvě. Nejčastěji se využívá řešení aplikační brány na principu proxy brány. Komunikace následně probíhá přes proxy bránu, klienti z vnitřní sítě nemají přístup k vnější síti a obráceně. Klient musí předat požadavek bráně, která ho následně pod svou identitou přepošle serveru mimo síť. Cílový server v tomto případě nevidí IP adresu skutečného odesílatele. Data, která dostane brána od serveru, následně předá klientovi. [29] Výhodou tohoto řešení je vysoké zabezpečení známých protokolů, skrytí identity uživatele a možnosti funkce cache na proxy bráně. Nevýhodou je vysoká náročnost na hardware a nižší rychlost.

- **Stavový paketový filtr** je firewall, který provádí kontrolu podobně jako jednoduchý paketový filtr, navíc si však ukládá informace o povolených spojeních, která mohou být použita při rozhodování, zda procházející paket patří do již povoleného spojení a může být propuštěn nebo musí projít znovu rozhodovacím procesem. [30] Největší výhodou stavového paketového filtru je vysoká rychlost. Toho je dosaženo, neboť již nemusí být zpracovány pakety již povolených spojení. Dále lze v pravidlech uvádět směr spojení a firewall je schopen automaticky rozhodnout o povolení portu a spojení pro známé protokoly. Dynamicky tak otevírá porty na základě známých spojení. Nevýhodou je nižší bezpečnost než u aplikačních bran.

- **Stavový paketový filtr s kontrolou a IDS** poskytuje nejvyspělejší metodu ochrany, která kromě informace o stavu spojení a dynamického otevírání portů je schopna progresivního skenování paketu na podobné bázi jako antivirové heuristické analýzy, kdy firewall podle známých vzorců dokáže kontrolovat příchozí i odchozí komunikaci a v případě, že nalezne vzorec evidovaný jako škodlivý, tak jej zablokuje. Dokáže zakázat například http spojení, v němž nalezne informace, které indikují, že se nejedná o požadavek na webový server. [31] Výhodou tohoto systému je vysoká bezpečnost kontroly při zachování dobré konfigurovatelnosti. Dále vysoká rychlost kontroly. Nevýhodou je, že tento firewall obsahuje vysoké množství funkcionalit, čímž se zvyšuje pravděpodobnost, že v některé části se bude vyskytovat chyba, která by mohla být zneužita k nefunkčnosti a snadnému obejití firewallu.

3.3.3 Antivirový program

Antivirový program je počítačový software, který sleduje nejpodstatnější vstupní a výstupní místa, kterými by viry mohly do počítačového sytému proniknout. Slouží k identifikaci a odstranění počítačových virů a jiného škodlivého software. V dnešní době se používají antivirové systémy, které prohledávají soubory na discích a porovnávají obsah

se známými definicemi virů, dále monitorují aktivitu počítačových programů a detekují podezřelé aktivity, které by mohly značit infekci. [32]

3.3.4 Intrusion detection system

Intrusion detection systém (IDS) je obranný systém, který monitoruje síťový provoz a snaží se odhalit podezřelé aktivity. IDS nástroje mají za cíl detekci počítačových útoků, veškeré příchozí a odchozí síťové aktivity. Systém se nezabývá pouze finálními pokusy o prolomení bezpečnosti, ale také detekcí akcí, které jim předcházejí. IDS systém je podobný poplašnému systému v domě, po detekci neobvyklé aktivity zapíše záznam do logu, informuje správce sítě a případně tuto aktivitu zastaví. IDS se dělí podle umístění na dvě kategorie hostitelsky orientované (HIDS) a síťové (NIDS). [33]

Síťové systémy monitorují provoz na sítí a hledají podezřelé aktivity, které by mohly být útokem nebo neoprávněnou aktivitou. Velký NIDS server je zpravidla umístěn na hranicích sítě, tak aby monitoroval veškerý provoz. Menší systémy lze nastavit tak, aby sledovaly provoz na daném serveru, přepínači nebo routeru. NIDS může také skenovat logovací soubory a vyhledávat podezřelé aktivity. [34]

Hostitelské systémy jsou nainstalovány lokálně na počítačích připojených do sítě. To činí lokální IDS přizpůsobivějšími, neboť mohou zohlednit zdroje a informace, které od zařízení požadujeme. Jsou založeny na softwarovém agentovi, který běží na pozadí a sleduje veškerou aktivitu počítače.

3.4. Zabezpečená spojení

Následující kapitola se zabývá charakteristikou možností zabezpečeného přenosu v rámci bezdrátové sítě ve společnosti, připojením do počítačové sítě organizace z míst mimo tuto síť a následně je vysvětlena možnost zabezpečeného webového serveru.

3.4.1 Virtual Private Network

Virtual Private Network (VPN) je virtuální privátní síť neboli bezpečné spojení vytvořené mezi koncovým zařízením, zpravidla osobním počítačem a serverem, který je uvnitř počítačové sítě organizace. VPN slouží tedy ke vzdálenému přístupu z internetu do počítačové sítě organizace. Díky síti VPN má uživatel všechny možnosti, jako by se fyzicky nacházel v organizaci. Toto spojení je plně zabezpečené proti narušení a odposlechům. Připojení se proto využívá k zabezpečenému přístupu do podnikové sítě pracovníkům, kteří pracují na cestách nebo z domova. Doporučeným protokolem pro VPN spojení je v dnešní době open source řešení OpenVPN [35], které je rychlé a bezpečné, nevýhodou je komplikovanější nastavení a instalace software třetích stran.

Obrázek 6: Spojení přes VPN [36]

Typy VPN podle typu spojení [37**]:**

- **Site-to-Site VPN** slouží ke spojení dvou nebo více sítí dohromady, většinou spojuje centrálu a pobočky. V těchto sítích se používají speciální síťová zařízení, která slouží jako VPN gateway a naváží mezi sebou VPN spojení, následně uživatelské stanice již nepotřebují VPN klienta.

- **Remote Access VPN** připojuje klienty do lokální sítě, klienti musí mít nainstalován speciální software neboli VPN klienta, na straně privátní sítě se nachází opět specializované síťové zařízení.

3.4.2 Wi-Fi Protected Access 2

Wi-Fi Protected Access 2 (WPA2) je označení pro zabezpečení bezdrátové sítě, vylepšující standard IEEE 802.11. Tento standard vylepšuje autentizační a šifrovací algoritmus. WPA2 bylo schváleno v roce 2004 a nahradilo původní zabezpečení WEP a WPA, které měly mnoho bezpečnostních slabin. Tyto verze používaly pro zabezpečení proudovou šifru RC4, WPA2 přidává nový algoritmus CCMP založený na proudové šifře AES, který poskytuje utajení, integritu a autentizaci a je považován za zcela bezpečný. WPA2 je dnes povinný standard pro všechna zařízení certifikovaná jako Wi-Fi od roku 2006. [38]

3.4.3 Hypertext Transfer Protocol Secure

Hypertext Transfer Protocol Secure (HTTPS) je nadstavbou síťového protokolu http, která umožňuje zabezpečené spojení mezi klientem a serverem před odposloucháváním, podvržením dat a umožňuje ověření identity. Přenášená data jsou šifrována pomocí SSL nebo TLS a standardní port na straně serveru je 443. Ve webových prohlížečích je zabezpečení spojení indikováno v adresním řádku. Nevýhodou přesunu webu na HTTPS je cena za certifikát a vlastní IP adresu. Pro navštěvované stránky je nevýhodou změna URL, ke které dojde, což by mohlo vést ke ztrátě návštěvnosti z vyhledávání. [39]

3.5. Šifrování dat

Následující část práce vysvětluje možnosti šifrování citlivých dat, tedy souborů, emailů a celých disků. Šifrování je proces, který převede čitelná data pomocí kryptografie na data šifrovaná, která jsou čitelná pouze pomocí dešifrovacího klíče. Pro šifrování dat je nezbytné použití hesla, na síle tohoto hesla závisí bezpečnost dat. Silné heslo by mělo obsahovat malá, velká písmena, číslice a případně speciální znaky o minimální délce 10 znaků.

3.5.1 Šifrování souboru

Šifrování souborů je softwarové šifrování a dešifrování jednotlivých souborů a složek. V operačním systému Windows se používá k šifrování technologie Encrypted

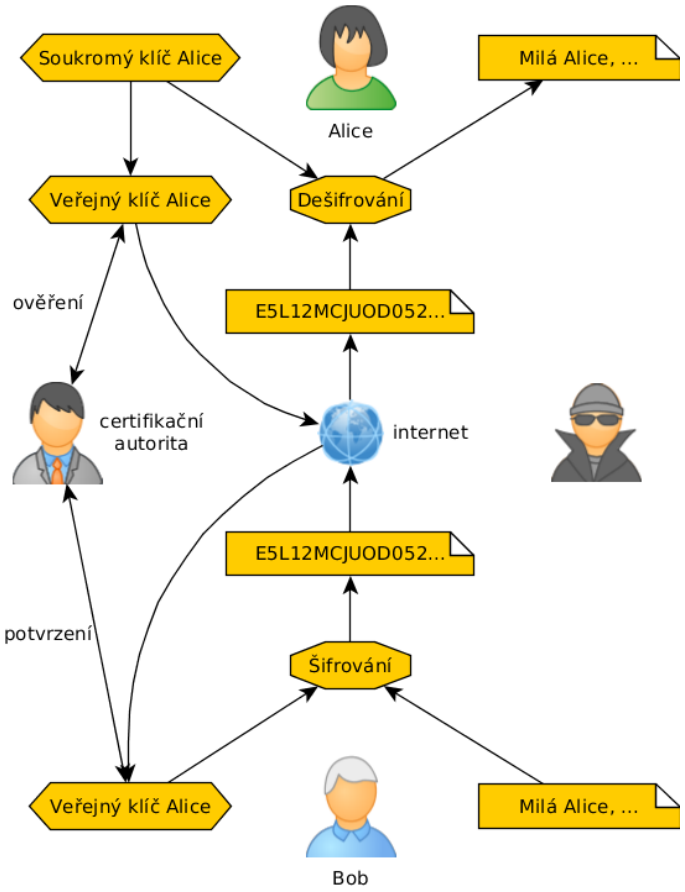
File System (EFS). EFS je služba systému souborů NTFS a nelze ji využít na discích se souborovým formátem FAT ani FAT32. Služba je dostupná od verze Windows 7 Professional. Tato technologie nedokáže šifrovat systémové soubory. K šifrování se používá hybridní kryptografie neboli používá se jak symetrická, tak i asymetrická kryptografie, čím je dosaženo dobrých vlastností při šifrování i dešifrování. Data jsou nejprve šifrována symetricky pomocí FEK, následně je tento unikátní klíč uživatele zašifrován asymetricky. Data jsou skutečně šifrována a útočník se k nim nedostane, pokud nevlastní certifikát, to platí také pro majitele souboru, musí si tedy vždy certifikát zálohovat. Pokud by certifikát ztratil, ke svým datům se již nedostane. V systému lze stanovit agenta obnovení, který by vlastnil zotavovací klíč, kterým je možné zašifrovaná data dešifrovat. [40]

3.5.2 Šifrování emailu

Princip šifrování emailů vychází z asymetrické kryptografie. Šifrování emailu umožňuje zašifrovat email pomocí veřejného klíče a zajistit, že nikdo kromě adresáta vlastnícího soukromý klíče nebude schopen zprávu přečíst.

Příklad šifrování emailu

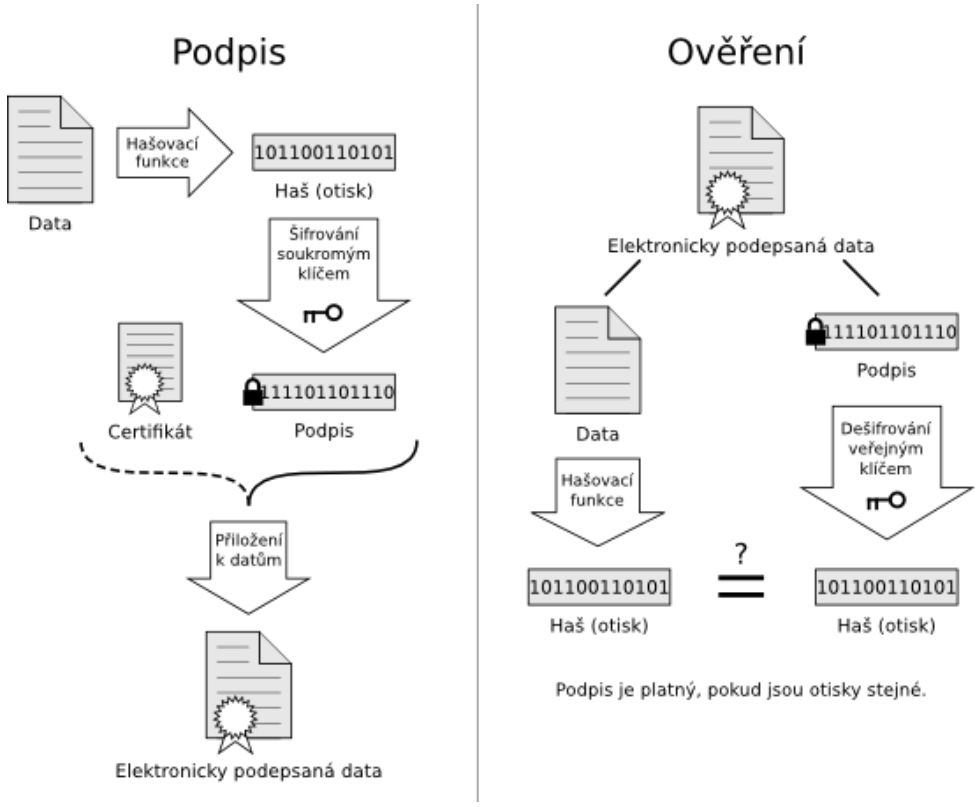
Bob se snaží odeslat důvěrnou zprávu Alici. K zašifrování obsahu použiji veřejný klíč Alice, který je volně dostupný, tento výsledek odešle Alici. Ta použije svůj soukromý klíč k dešifrování obsahu. Pokud chce odpovědět, musí novou zprávu zašifrovat pomocí veřejného klíče Boba. Ověřování pravosti veřejných klíčů je pomocí certifikační autority. Jedná se o důvěryhodnou instituci, které svým podpisem ověřují pravost veřejného klíče. Toto šifrování je dostupné v běžně používaných emailových klientech. [41]



Obrázek 7: Schéma použití asymetrické kryptografie pro šifrování zpráv [42]

Elektronický podpis

Elektronický podpis pracuje také na principu asymetrické kryptografie a slouží k ověření, že přijatá zpráva je v přesně stejné podobě, ve které byla odeslána. Zajišťuje tedy identitu odesílatele a integritu zprávy. Odesílatel svým soukromým klíčem zašifruje otisk zprávy. Příjemce následně ověří zprávu veřejným klíčem. Jelikož bez přístupu k soukromému klíčí nelze podpis vytvořit, máme jistotu, že daný dokument skutečně vytvořil vlastník a nedošlo k modifikaci během přenosu. Ověření klíčů zde probíhá opět pomocí certifikační autority. [43]



Obrázek 8: Schéma použití asymetrické kryptografie pro elektronický podpis [44]

3.5.3 Šifrování disku

Šifrování disku nabízí maximální úroveň zabezpečení, jelikož dokáže zašifrovat všechny soubory na disku včetně oddílu Master Boot Record (MBR). Proces šifrování probíhá průběžně a dochází tak k poklesu výkonu počítače. K šifrování disku lze použít technologii BitLocker [45], která je součástí operačního systému Windows od verze Vista. Program BitLocker funguje nejlépe v prostředí, kde se o počítače a data stará oddělení IT a kde uživatelé ani netuší co je to šifrování. Uživatel má přístup ke svým datům, pouze pokud se přihlásí ve stejném prostředí Windows pod svým uživatelským jménem. Šifrovací programy třetích stran jsou přímočařejší, vyžadují heslo pro šifrování před spuštěním operační systému. Vzhledem k tomu, že se takové heslo používá při každém spuštění počítače, je nepravděpodobné, že by se ztratilo.

3.6. Nejčastější chyby

Následující kapitola definuje nejčastější chyby, kterých se dopouštějí uživatelé a správci počítačové sítě. Kterákoli chyba může vést ke ztrátě dat, odcizení dat, případně přístupu útočníka do podnikové sítě.

- **Nesprávná volba přístupových hesel** – navzdory neustálé mediální kampani a doporučení odborníků se situace ohledně hesel nelepší, uživatelé stále používají slabá a lehce uhodnutelná hesla. Heslo by mělo být rozumně složité a unikátní, pro každé přístupové místo bychom měli mít jiné heslo, což je mnohdy také ignorováno ze strany uživatelů. Heslo by se mělo volit snadno zapamatovatelné, ale neuhodnutelné pomocí tzv. slovníkového útoku. [46]

- **Nepoužívání antivirových a bezpečnostních programů** – absence pravidelně aktualizovaného antivirového a bezpečnostních programů je dalším častým problémem firem. Zejména u malých podniků, pokud podnik disponuje těmito programy, je zpravidla neaktualizují pravidelně, případně nemají nastavenou vhodnou konfiguraci.

- **Nezálohování –** uživatele lze rozdělit do dvou skupin, na uživatele, kteří již přišli o svá data a na ty kteří o svá data zatím nepřišli. Zálohování nás ochrání před ztrátou dat při poruše hardwaru či nechtěném smazání. Data lze zálohovat manuálně, případně automaticky.

- **Nedostatečné školení zaměstnanců –** bezpečnostní problémy vznikají nejčastěji po chybách uživatelů. Ve společnosti by se měla provádět pravidelná školení s cílem seznámit zaměstnance se základními bezpečnostními prvky, které se využívající ve společnosti. Zaměstnanci by měli být varování, aby ignorovali veškeré emaily, webové stránky a soubory od neznámých odesílatelů, jedná se o nejčastější způsob infiltrace podnikové sítě počítačovým virem či jiným škodlivým software.

- **Neaktuální software –** veškerý software používaný v podnikové síti by měl být pravidelně aktualizován. Uživatelé si zpravidla vystačí s jednou verzí programu, kterou aktualizují pouze při aktualizaci funkcí daného programu. Bezpečností záplaty uživatele zpravidla nenutí software aktualizovat, čehož využívají útočníci, neboť takto používaný software může být starý i několik let.

- **Špatná bezpečnostní politika –** bezpečnost v organizace je tak silná, jako její nejslabší článek. Při tvorbě bezpečnostní politiky je třeba dbát na bezpečnost jako celek, nikoli zabezpečovat pouze jednotlivá místa.

- **Nezabezpečený přístup do firemní sítě** – pro přístup do podnikové sítě z míst mimo tuto síť by měla být komunikace vždy zabezpečena. V opačném případě by mohl útočník odposlechnout komunikaci zasílanou skrz nezabezpečený kanál a získat přístup k datům, která mohou být klíčová pro danou společnost.

4. Vlastní práce

4.1. Charakteristika společnosti

Pro vytvoření bezpečnostní analýzy byla vybrána společnost LAMPS, a.s. Ve firmě se v současné době nenachází správce sítě, požadované údaje poskytovalo vedení společnosti, které nebylo schopno poskytnout veškeré nutné údaje, chybějící údaje bylo nutné nalézt samostatně. Společnost LAMPS, a.s. byla založena roku 2002 v Praze a navazovala na předchozí podnikatelské aktivity majitelů od roku 1992 [47]. V současné době je společnost ryze českou, finančně zcela stabilní a úspěšnou firmou. Společnost působí již od počátku pouze na českém trhu v oblasti velkoobchodní prodeje hraček, kde se společnosti daří navyšovat prodeje a zisky každým rok. Firma se zabývá dovozem hraček z Evropy a dálného východu, převážně z Číny a jejich následným prodejem zejména na českém trhu. V sortimentu společnosti lze nalézt také hračky od největších výrobců v oblasti hraček například Mattel, Hasbro nebo Zapf, kterým společnost zajišťuje distribuci v České republice. V současné době nemá firma žádné pobočky nebo prodejny. Sídlo společnosti, které bylo dokončeno před 3 lety dle požadavků společnosti, se nachází v Praze v Horních Počernicích. V diplomové práci budu analyzovat stav zabezpečení v tomto sídle společnosti v Praze.

4.1.1 Organizační struktura

Ve firmě LAMPS, a.s. v současné době pracuje 14 lidí, které lze rozdělit do 5 skupin, které vzájemné spolupracují, každé oddělení má jiné potřeby a znalosti z oblasti informačních technologií.

Rozdělení organizační struktury podniku:

- **Majitel –** společnost má v současné době jednoho majitele, kterému se zodpovídají ostatní oddělení. Majitel je jediná osoba, která zná většinu používaných technologií, protože se podílel na jejich nákupu a nastavení.

- **Obchodní oddělení –** do toho oddělení patří 4 lidé, kteří se starají o prodej a nákup zboží. Připravují i podklady pro externí účetní. Všichni tito uživatelé zvládají pokročilou práci s počítačem. Pro svoji práci využívají zejména emailovou komunikaci, kancelářský balík Office a skladový a účetní program MRP.

- **Sklad –** ve skladu pracuje 6 lidí, jejichž hlavní náplní práce je příprava objednávek a naskladňování zboží. Při své práci využívající zejména program MRP.

- **Reklamační oddělení –** v této skupině se nachází pouze 1 člověk, vyřizují reklamace. Pro svoji práci používá email a MRP.

- **Oddělení pro vztah se zákazníky –** vztah se zákazníky mají na starost 2 zaměstnanci, využívající programy ke komunikaci se zákazníky.

4.2. Definice zadání

Ze strany zadavatele, podniku zabývajícího se prodejem hraček byly určeny následující úkoly, které má analýza v daném podniku vyřešit, ke každému úkolu byly stanoveny cíle, kterých bylo třeba dosáhnout. S vedením podniku bylo dohodnuto, že jednotlivé oblasti budou vyhodnocovány průběžně a nasazení nových zařízení nebo změna konfigurace současného hardware může být prováděna ihned, po schválení vedením.

Zadané cíle a požadované výstupy:

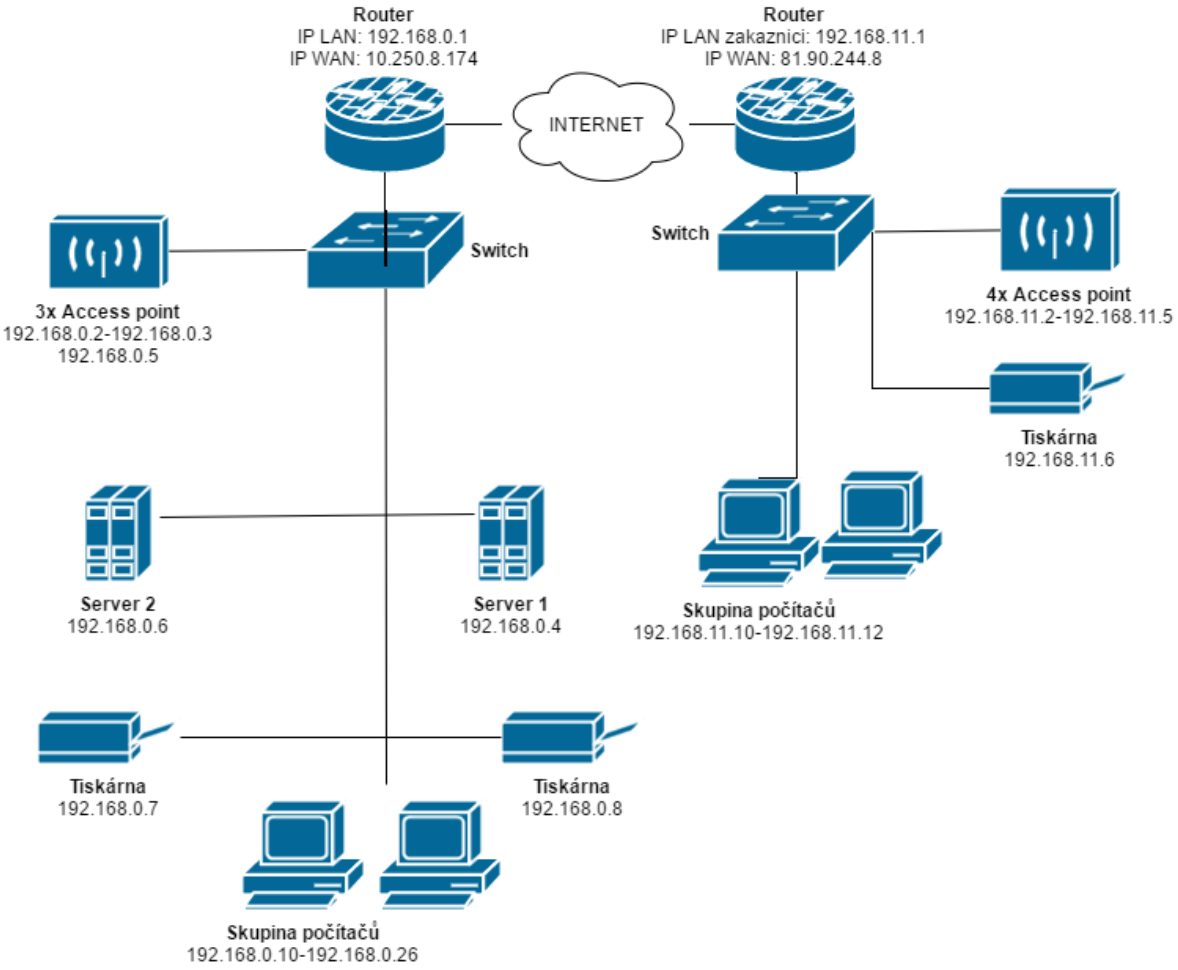
1) **Analýza a základní přehled o současném stavu ICT –** poskytnout přehled a popis aktuálního řešení ICT v dané společnosti. V rámci tohoto úkolu analyzovat následující oblasti ICT:
    - LAN/WAN síť
    - Servery
    - Aplikace a OS
    - Pracovní stanice
    - Zálohovací strategie

2) **Analýza stavu bezpečnosti –** na základě stavu ICT a konfigurace sítě, analyzovat veškeré bezpečností hrozby, zjistit nedostatky v současné konfiguraci sítě, zařízení či postupů a navrhnout jejich změnu k implementaci. Součástí úkolu je zhodnocení následujících oblastí:
    - Fyzická bezpečnost
    - Přístupová hesla
    - Antivirový program a firewall
    - Školení zaměstnanců
    - Zabezpečení vzdálených přístupů do firemní sítě
    - Ochrana před útoky z internetu a lokální sítě
    - Bezdrátová síť
    - Šifrování dat

4.3. Počítačová síť

V počítačové síti se nachází 20 koncových stanic, dva počítačové servery, tři síťové tiskárny, dvě bezdrátové sítě a aktivní a pasivní prvky pro propojení zařízení v rámci podnikové sítě. V rámci sítě je vytvořena pracovní skupina, která slouží k vzájemnému sdílení dat mezi zařízeními v síti. Všechna zařízení v síti mají přiřazenou IP adresu staticky, v rámci bezdrátové sítě je nabízeno 20 IP adres pomocí DHCP serveru, který běží na routeru. Firma využívá 2 nezávislé připojení k síti internet, první slouží pro potřeby

zaměstnanců, druhé pro přístup k internetu pro zákazníky. V případě výpadku internetu v podnikové síti se lze napojit na druhé připojení, k tomu je nutné vždy přepojit kabel a přiřadit správnou IP adresu. Celá počítačová síť je postavena na 1 Gbit/s. Veškerá zařízení v počítačové síti jsou chráněna přepěťovou ochranou a záložním zdrojem elektrické energie.



Obrázek 9: Schéma zapojení počítačové sítě LAMPS, a.s.

Zdroj: Vlastní

Doporučené změny v rámci počítačové sítě:

- Nahradit dva routery jedním, nastavit konfiguraci, aby při výpadku internetu došlo k přepojení na záložní připojení
- V rámci podnikové sítě nasadit doménu, pro správu sdílení souborů a prostředků, autentizaci a autorizaci uživatelů

4.3.1 Bezdrátová síť

Při stavbě budovy došlo k vhodnému rozmístění access pointů po budově. Signál je dostatečný ve všech místech budovy, kde se předpokládá možné připojování k síti. Nakonfigurovány jsou 2 nezávislé bezdrátové sítě, jedna pro zákazníky, pouze s přístupem na internet, druhá pro potřeby zaměstnanců s přístupem do LAN.

Tabulka 1: Konfigurace Wi-Fi

Název sítě:	LAMPS-zakaznici	LAMPS-WiFi
Zabezpečení:	WPA2	WPA2
Složitost hesla:	dostatečné	dostatečné
Využití:	Přístup k internetu pro zákazníky, využíváno během výstav společnosti	Přístup do LAN pro zaměstnance, není příliš využíváno
Zařízení:	4x PLANET WNAP-1110	3x ASUS RT-N16
Pokrytí:	Vnitřek budovy, část venkovního prostoru	Vnitřek budovy

Zdroj: Vlastní

Z bezpečnostního hlediska je současné nastavení bezdrátové sítě dostatečné a nejsou vyžadovány žádné změny.

4.3.2 Vzdálený přístup

Pro potřeby zaměstnanců je nakonfigurováno šifrované připojení v rámci VPN, využívající řešení OpenVPN s autentizací certifikátu, na routeru je dále nakonfigurováno

přesměrování portů, pro služby, které by mohly být vyžadovány zaměstnanci mimo síť. Mezi tyto služby patří zejména vzdálená plocha, FTP připojení a připojení ke kamerovému systému. Zaměstnanci využívají pouze připojení přes směrování portů.

Bude nutné zakázat směrování portů a využívat pro vzdálený přístup do firemní sítě výhradně zabezpečené spojení, aby byla zajištěna bezpečnost komunikace.

4.4. Přehled stavu ICT

4.4.1 Aktivní prvky

Routery

Největším problém v oblasti aktivních prvků jsou nevhodně zvolené routery, které neumožňují pokročilé možnosti konfigurace a jsou určeny na domácí využití. V sítí jsou aktivní 2 routery TP-LINK TL-WR1043ND. Oba tyto routery je nutné nahradit pokročilejším zařízením, které by zastalo práci obou a zvládlo i pokročilou konfiguraci.

Switche

Pro propojení uzlů v síti jsou ve firmě využívány 2 switche TL-SG1048. Switche poskytující očekávanou rychlost sítě. Nevýhodou je nemožnost konfigurace, zejména určení, které zařízení může využívat jaký port, aby se nemohl připojit útočník do naší sítě pomocí počítačových zásuvek ve zdi. Tento problém je částečně vyřešen vhodným fyzickým zapojením v serverovně, kde jsou propojeny do switche jen ty zásuvky, kde se nachází zařízení společnosti. Tato ochrana je dostatečná, neboť se nepředpokládá, že by útočník dokázal proniknout k síťové zásuvce v prostorách firmy a nahradit některé využívané zařízení.

Bezdrátové AP

V síti jsou využívány pro účely bezdrátově sítě dva druhy AP 4x PLANET WNAP-1110 a 3x ASUS RT-N16. Oba typy zařízení poskytují aktuální standard v oblasti zabezpečení bezdrátových sítí a jejich rychlost je dostatečná pro účely společnosti.

4.4.2 Koncové stanice

V počítačové síti podniku je 17 pracovních stanic a 3 stanice určené pro zákazníky k případnému nákupu zboží. Všechny pracovní stanice jsou počítačové sestavy různých hardwarových parametrů. Firma nakupuje počítače od různých dodavatelů vždy podle potřeby, z tohoto důvodu jsou velké rozdíly mezi sestavami. Na 15 počítačích je nainstalován operační systém Windows 10, neboť firma využila bezplatného přechodu z operačního systém Windows 7. Na dalších stanicích je stále nainstalován zastaralý operační systém Windows XP, na těchto stanicích je již práce nekomfortní, neboť jde o zastaralá zařízení a některé služby již nefungují pod tímto operačním systémem. V každém počítači je připojena sdílená složka ze serveru jako disk S:/, kterou zaměstnanci využívající k ukládání dat do svých složek. V rámci této služky mají přístup všichni zaměstnanci do všech složek. Na každé stanici jsou nainstalovány následující programy:

- **Adobe Acrobat Reader**
- **Eset Smart Security**
- **OpenOffice**
- **MRP – účetní a skladový program**
- **Windows Live Mail**
- **VLC media player**
- **Google Chrome**

U těchto programů, kromě antivirové ochrany Eset, není nastavena automatická aktualizace programu.

Další aktualizace a instalace programů je na stanicích zakázána pomocí místních práv, kde jsou na počítačích nastavena uživatelům pouze omezená práva. Na některých stanicích je vypnuta automatická aktualizace Windows.

Doporučením v této oblasti je přesunutí nastavení systému oprávnění na doménový řadič, nalezení vhodného systému automatických aktualizací software a Windows. U antivirové ochrany je vhodné nainstalovat centrální službu pro správu licencí, automatickou konfiguraci stanic, abychom každou změnu nemuseli provádět na všech zařízeních. Nahrazení počítačů využívajících systém Windows XP za nové je výrazně doporučeno. Poslední doporučenou změnou je nastavení sdílené složky přes doménový řadič a využívat i možnosti zabezpečení v rámci podnikové sítě.

4.4.3 Servery

V síti jsou využívány 2 servery s rozdílnými účely. Na prvním serveru je nainstalována serverová část účetního a skladového programu MRP a je zde využíván operační systém Windows 7. Druhý server s operačním systém Windows Server 2008 slouží jako datový, OpenVPN, ftp server, dále je zde nainstalován software na monitoring a záznam kamer. Webový server firma v síti nepoužívá, svou webovou prezentaci má uloženou na externím hostingu. Na obou serverech se nachází disk o velikosti 2 TB, u druhého serveru je navíc připojen další disk o velikosti 2 TB pro ukládání kamerových záznamů. Druhý server je vhodné využít jako doménový řadič a využít všech výhod, které nabízí zapojení do domény. Přidání disků do serverů a jejich zapojení do RAID by výrazně snížilo problémy s vyřazením některého disku.

4.5. Zaměstnanci

Ve firmě pracuje 13 zaměstnanců a majitel společnosti. Během diskuze se zaměstnanci bylo zjištěno, že mají dobré znalosti základních pravidel, většina přiznala, ale že je příliš nedodržují. Hlavním problém je neexistující bezpečností dokument, který by zaměstnancům poskytl základní přehled o problémech, které je mohou potkat a ohrozit tím celou síť. Tyto základní body by měly být zaměstnancům připomínány na pravidelných školeních, která by byla vždy doplněna novými poznatky od posledního školení, případně případy, které nastaly v mezidobí. Zaměstnanci mají v současném stavu vysoké oprávnění k přístupu ke zdrojům v síti. Je vhodné celou síť upravit tak, aby zaměstnanec měl přístup pouze ke zdrojům, které potřebuje k vykonávání své práce v podniku.

4.6. Fyzická bezpečnost

4.6.1 Budova

Budova společnosti je zabezpečena několika mechanismy. Prvním je automatické uzamknutí brány a vchodových vrat do areálu mimo pracovní hodiny. Dále je zde nainstalován bezpečnostní systém, který v případě průniku do budovy spustí alarm. Tento systém je rozdělen do několika zón a zaměstnanec vypíná alarm pouze v místech, ve kterých pracuje. Při vstupu a odchodu z budovy se zaměstnanec identifikuje čipem. Posledním prvkem ochrany budovy je bezpečnostní agentura, která provádí pravidelné kontroly mimo pracovní dobu, v případě poplachu se k budově dostaví okamžitě, čímž je zajištěna rychlá reakce v případě vniknutí. Všechny přístupy do budovy jsou zaznamenávány na kamerový záznam. Celková bezpečnost budovy je tedy na vysoké úrovni a nepředpokládá se, že by byl útočník schopen se připojit k firemní síti nebo provádět jinou činnost v rámci budovy.

4.6.2 Serverovna

Serverovna je zabezpečena vlastním okruhem v rámci alarmu. Přístup do této místnosti mají pouze klíčoví zaměstnanci, kteří pro vstup mají povoleno vypnutí zabezpečovacího alarmu a mají požadovaný klíč. Fyzický přístup k nejdůležitějším datům v serverovně je dostatečně chráněn a není nutné provádět změny v této oblasti.

4.7. Ostatní oblasti

4.7.1 Zálohování dat

Zálohování dat v rámci tohoto podniku je na vysoké úrovni, neboť před několika lety došlo k poškození disků na serveru a ztrátě důležitých dat. Každé zařízení v rámci sítě, u kterého je možnost zálohování dat je prováděno automaticky každý den přírůstkově. Zálohovány jsou veškeré dokumenty a emaily. Všechna zařízení jsou zálohována na disk na serveru. Nepostradatelná data, účetní záznamy, jsou zálohovány 2x týdně na externí server mimo firmu pro případ většího poškození budovy.

4.7.2 Politika hesel

Politika hesel není v současném stavu nastavena u žádného programu v podniku, zaměstnanci nemají ani poskytnutý doporučený postup pro vytvoření svého hesla. Složitost hesel tedy není kontrolována a zaměstnanci mohou používat i jednoduchá hesla. U programů, kde lze nastavit složitost hesla je doporučeno provést změny, dále je vhodné do dokumentu pro zaměstnance přidat i základní pravidla pro vytvoření hesla.

4.7.3 Šifrování

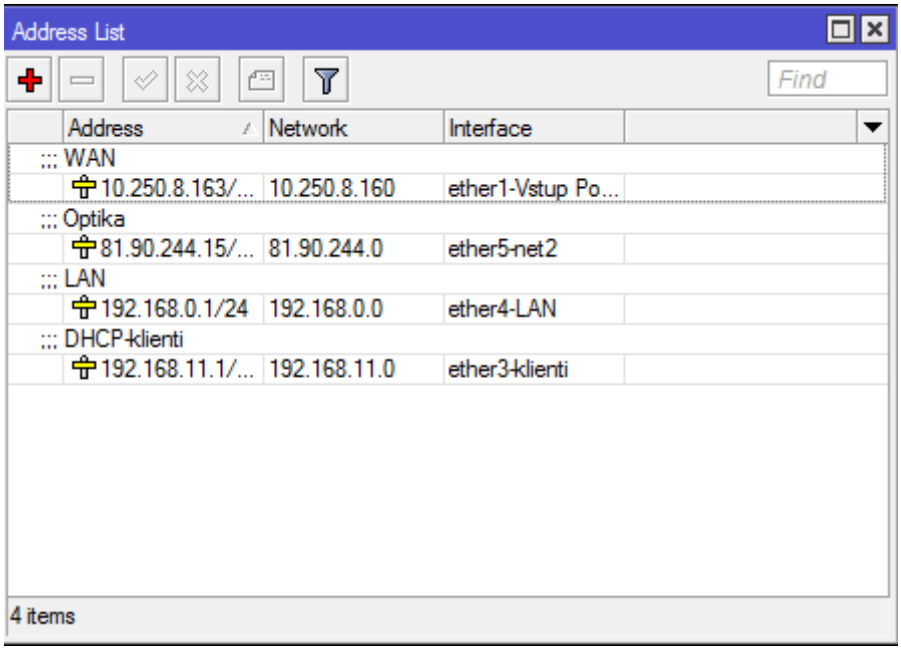
Šifrování dat na discích se ve společnosti nevyužívá. V rámci podniku jsou citlivá data účetnictví uložena na serveru. Tato data by mělo smysl šifrovat, ale jejich zcizení je vysoce nepravděpodobné kvůli vysokému zabezpečení serverovny a zamezení přístupu k datům v rámci sítě. Šifrování na jednotlivých stanicích není potřebné, jelikož se tam nenachází citlivé údaje podniku. Byla vyžádána možnost elektronického podpisu emailu, jelikož některé zahraniční firmy tuto metodu po firmě požadují.

4.8. Návrh a provedené změny

4.8.1 Výměna routeru

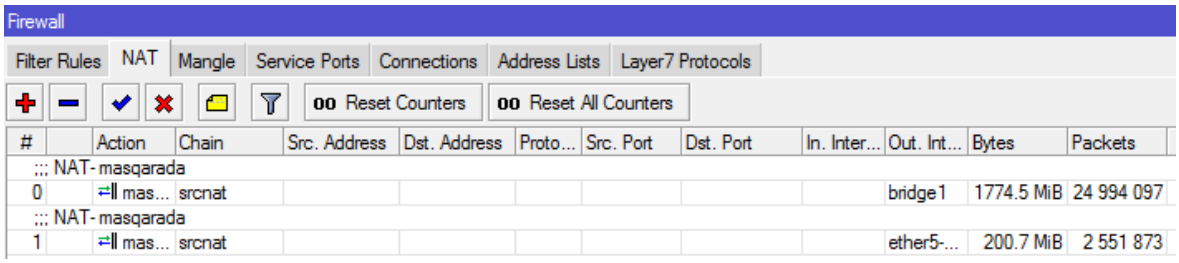
Firmě byla doporučena výměna dvou routerů za jeden, který zvládne současnou funkci obou, navíc bude mít více možností konfigurace. Nabídnut je router firmy Mikrotik RB951G-2HnD. Veškeré změny byly nakonfigurovány a vyzkoušeny v daném podniku na zapůjčeném Mikrotiku. Na Mikrotiku jsou doporučeny následující nastavení:

- **Standardní nastavení sítě** – nastavit zařízení, tak aby bylo v souladu s předchozím nastavením IP adresace



Obrázek 10: Přehled IP adresace

Zdroj: Vlastní



Obrázek 11: Nastavení NAT maškarády

Zdroj: Vlastní

- **OpenVPN** – provést konfiguraci OpenVPN přímo na tomto zařízení, aby nemusely být požadavky směrovány na server v rámci LAN, tato služba je součástí routeru Mikrotik, není třeba instalovat, pouze je nutné provést nastavení. Parametry a příkazy, které byly provedeny jsou charakterizovány na webu společnosti Mikrotik. [48]

Postup nastavení OpenVPN serveru:

Vytvoření certifikační autority (PC):

openssl genrsa -des3 -out ca.key 4096

openssl req -new -x509 -days 3650 -key ca.key -out ca.crt

Vytvoření certifikátu pro OpenVPN (PC):

openssl genrsa -des3 -out server.key 4096

openssl req -new -key server.key -out server.csr

openssl x509 -req -days 3650 -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out server.crt

Import certifikátu na Mikrotiku po nahrání do složky Files (Mikrotik):

import file-name=server.crt

import file-name=server.key

Vytvoření rozsahu ip adres pro připojené uživatele (Mikrotik):

/ip pool add name=ovpn-pool ranges=192.168.0.100-192.168.0.150

Definování profilu připojení (Mikrotik):

/ppp profile add change-tcp-mss=default comment="" bridge=vpn-bridge \

name="lamps" only-one=default remote-address=ovpn-pool \

use-compression=default use-encryption=required use-vj-compression=default

Postup nastavení OpenVPN serveru:

OpenVPN server konfigurace:

/interface ovpn-server server set auth=sha1,md5 certificate=router_cert \

cipher=blowfish128,aes128,aes192,aes256 default-profile=lamps \

enabled=yes keepalive-timeout=disabled max-mtu=1500 mode=ethernet netmask=24 \

port=1194 require-client-certificate=yes

Postup nastavení OpenVPN klienta:

Na klientech je nutné nainstalovat program OpenVPN, který je dostupný pro většinu operačních systémů a následně provést nastavení.

Generování certifikátu pro klienty (PC – stejné ve kterém jsme vytvořili cert. autoritu při nastavení serveru):

openssl genrsa -des3 -out client.key 4096

openssl req -new -key client.key -out client.csr

openssl x509 -req -days 3650 -in client.csr -CA ca.crt -CAkey ca.key -set_serial 01 -out client.crt

Nastavení konfiguračního souboru:

client

dev tun

proto tcp-client

remote 188.175.124.128 1194

resolv-retry infinite

nobind

persist-key

persist-tun

ca ca.crt

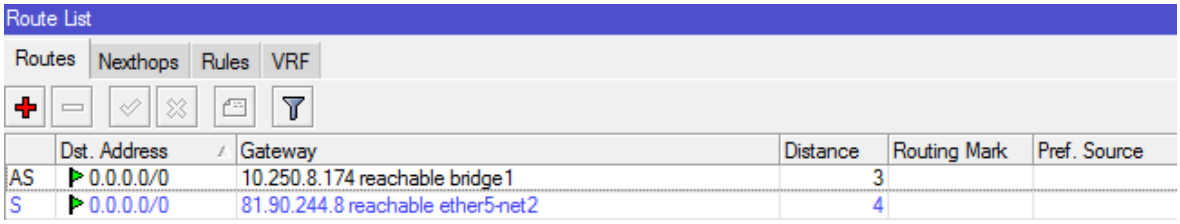
cert client.crt

key client.key

comp-lzo

verb 3

- **Záložní připojení WAN** – provést konfiguraci dvou internetových připojení, tak aby v případě výpadku hlavního připojení došlo k automatickému přepojení. Nejprve se nastaví výchozí brány s různým parametrem Distance, což je preferenční hodnota. Následně se u preferovaného spojení výchozí brány nakonfiguruje ověření spojení pomocí příkazu ping (Check Gateway), při výpadku spojení následně dojde k automatickému přepojení na záložní konektivitu.



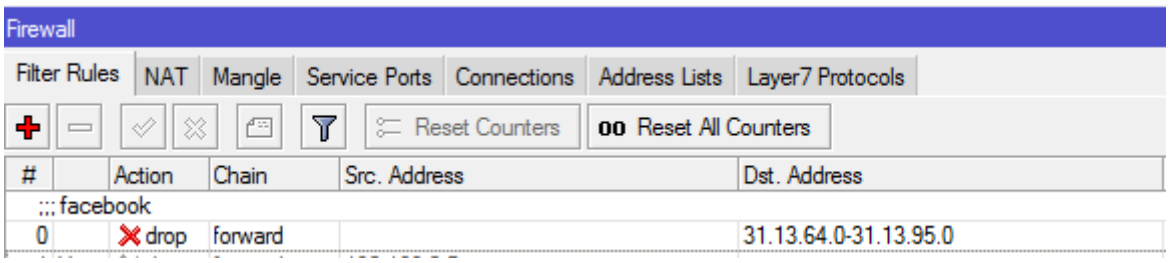
Obrázek 12: Nastavení výchozích bran

Zdroj: Vlastní

Obrázek 13: Nastavení kontroly gateway pomocí ping

Zdroj: Vlastní

- **Firewall** – nakonfigurovat firewall, aby nebyl možný přístup do sítě LAN z vnější sítě. Vedení společnosti si vyžádalo také blokaci přístupu na facebook. Blokace facebooku je dosažena pomocí zablokování IP adres, které pro svou činnost využívá společnost v Evropě. Do sítě LAN byl zakázán veškerý provoz, není nastaveno ani žádné směrování portů do této sítě.



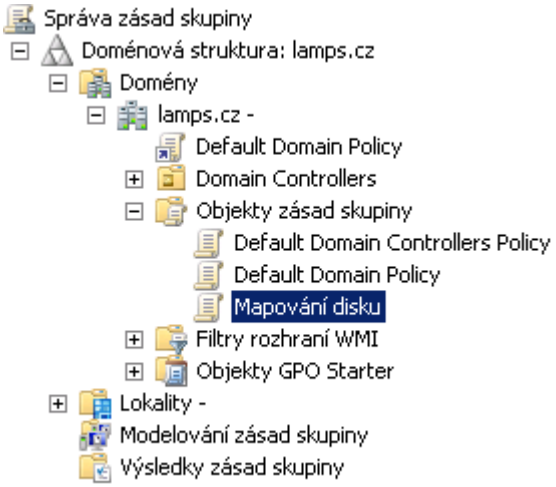
Obrázek 14: Zakázání facebooku

Zdroj: Vlastní

4.8.2 Nasazení domény

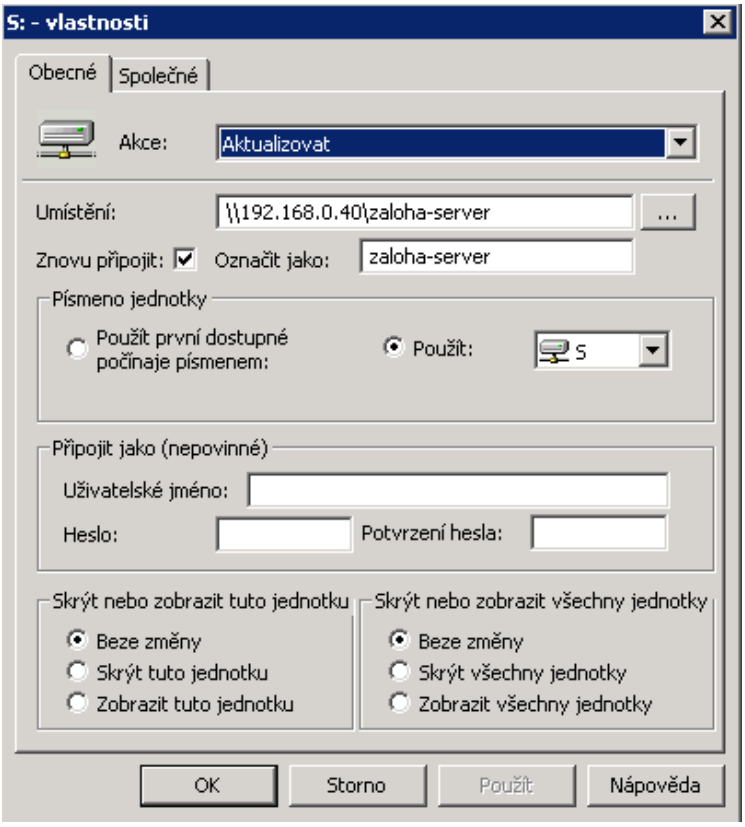
Pro snadnější konfiguraci stanic a zlepšení správy počítačové sítě byla nainstalována doména na jeden ze serverů. Tento server bude sloužit jako doménový řadič, server pro záznam kamerového systému, terminálový server a file server. Byla nainstalována doména lamps.cz. Následně byly do domény přidány veškeré počítače a tiskárny. Následně bylo provedeno požadované nastavení ze zadání.

- V konzoli Uživatelé a počítače Active Directory byly vytvořeny uživatelské účty pro zaměstnance, kteří ve společnosti pracují. Pracovní skupiny nebyly v rámci práv vytvořeny, neboť nebylo nalezeno vhodné uplatnění z hlediska práv.
- Byly připojeny všechny počítače do domény lamps.cz.
- Byl vytvořen startovací skript, který na stanicích namapuje síťový disk ze serveru a označí ho S:/. Mapování disku bylo dosaženo pomocí vytvoření zásady GPO, viz Obrázek 15, v rámci této GPO bylo nakonfigurování mapování disku viz Obrázek 16 a proběhlo mapování GPO na doménu viz Obrázek 17. tomto disku byla nastavena práva jednotlivých uživatelů, dle dohody s vedením společnosti. V rámci podniku bylo také zamezeno sdílení souborů a složek mezi počítači.



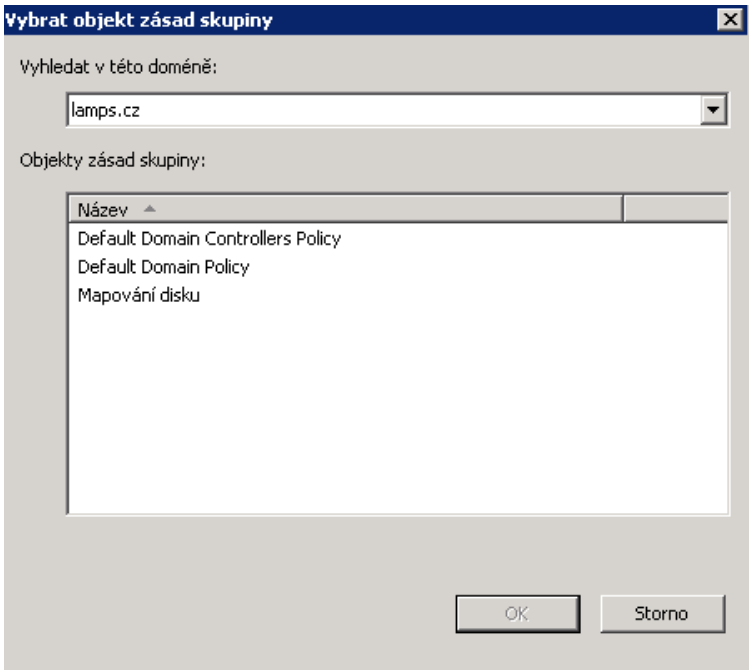
Obrázek 15: Vytvoření GPO Mapování disku

Zdroj: Vlastní



Obrázek 16: Nastavení Mapování disku

Zdroj: Vlastní

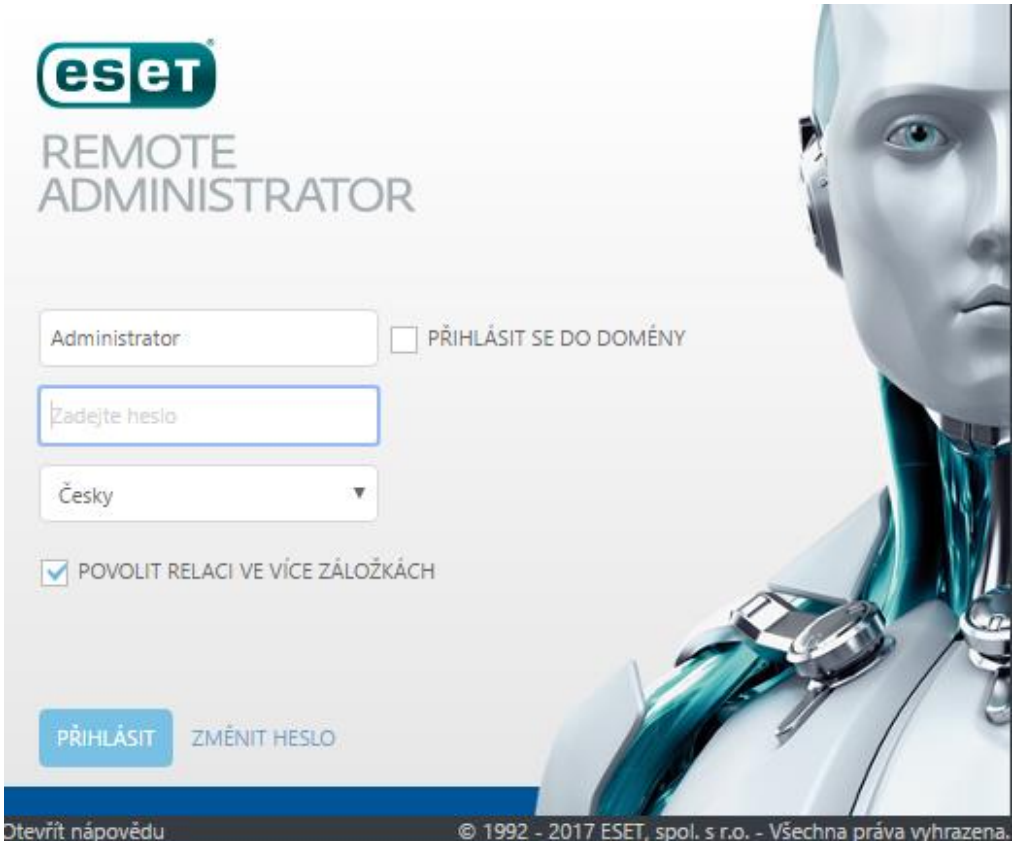


Obrázek 17: Přiřazení GPO k dané doméně

Zdroj: Vlastní

4.8.3 Konfigurace serveru

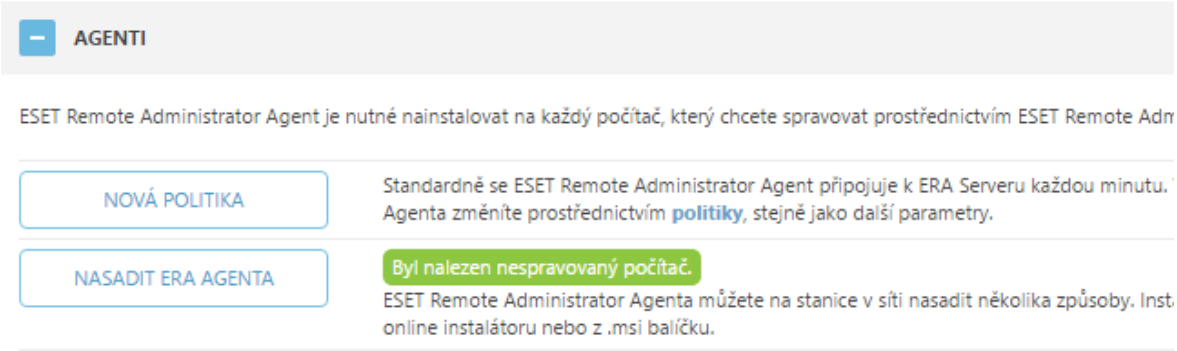
- **Centralizovanost antivirového programu** – na serveru byl nainstalován program ESET Remote Administrator pro centralizovanou správu produktu firmy Eset, který je zdarma pro držitele licencí na stanice. Tento produkt se spravuje pomocí webového prohlížeče viz Obrázek 18. Pro nastavení na stanicích je potřeba na serveru vytvořit bezpečností politiku tohoto software viz Obrázek 19, následně tuto politiku distribuovat společně s ERA agentem, což je agent spojující stanici a server. Instalace byla provedena manuálně na každé stanici.



Obrázek 18: Přihlašovací obrazovka ESET Remote Administrator

Zdroj: Vlastní

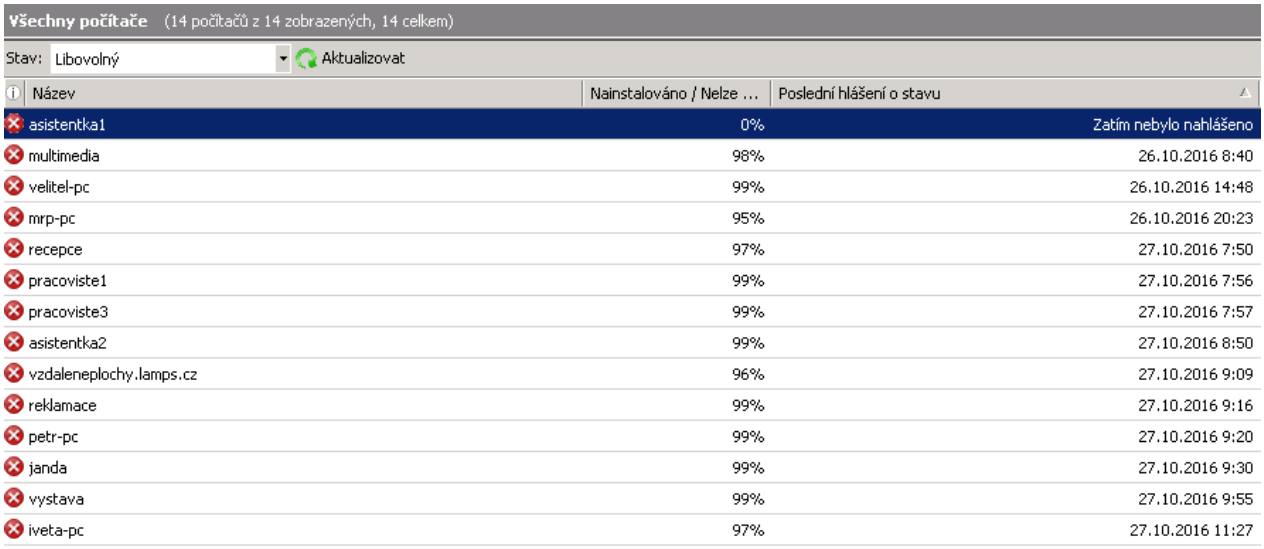
- **Vytvoření balíčků pro klienty** – spárování s ESET Remote Administrator, nastavení politik a určení



Obrázek 19: Přidání nové politiky

Zdroj: Vlastní

- **Windows Server Update Services** – Kvůli nepřehlednosti aktualizací Windows, byl nainstalován na server Windows Server Update Services, což je služba pro vytvoření lokálního serveru pro aktualizace Windows. V rámci této služby lze aktualizovat velké množství aplikací od společnosti Microsoft. Výsledkem je přehled aktualizací, které stanice mají nainstalovány, nutnost stahovat aktualizace pouze jednou pro celou síť. Na obrázku Obrázek 20 je znázorněn stav po nainstalování této služby. Veškeré stanice byly následně aktualizovány.



Obrázek 20: Zjištěný stav aktualizací Windows

Zdroj: Vlastní

- **RAID** – v rámci obou serverů bylo doporučena zakoupení disků o velikosti 6 TB WD Gold, které by byly v RAID1. Tento typ RAIDu lze nastavit přímo ve Windows bez nutnosti nákupu dalšího software.

4.8.4 Zaměstnanci

- Bezpečnostní dokument – Byl vytvořen bezpečnostní dokument, kterým se mají všichni zaměstnanci řídit a dodržovat ho.

- Školení – Bylo provedeno školení se zaměstnanci, na kterém byl prezentován bezpečností dokument a vysvětleny všechny body. Následně bylo doporučeno provádět následující školení vždy s novým zaměstnancem a pravidelně 1x ročně hromadně se všemi zaměstnanci. Po konci prvního školení byl bezpečnostní dokument upraven, o poznatky získaného z tohoto školení o oblasti, na které se zaměstnanci dotazovali.

4.8.5 Výměna PC s Windows XP

Bylo doporučeno provést náhradu starších počítačů s Windows XP za nové. V posledních letech firma již takto vyměnila několik počítačů, jelikož u starších nestačil výkon. Z hlediska bezpečnosti a praktičnosti je již vhodné kompletně tyto počítače nahradit. Byly nabídnuty 2 sestavy v celkovém počtu 5 počítačů. První sestava se liší od druhé diskem s menší velikostí, pomalejším procesorem a menší operační pamětí. Tato sestava je dostatečná pro aktuální účely firmy. Druhá sestava poskytuje celkově vyšší výkon, který prodlouží životnost počítače z hlediska výkonosti o pár let.

Tabulka 2: Varianta 1 – Nové PC

Kategorie	Produkt	Cena bez DPH
Skříň	+ Akyga PC skrín Micro ATX cerná	299.00
Zdroj	+ Akyga ATX Zdroj 400W Basic ventiláror 12cm P4 3xSATA	320.00
Základní deska	+ ASUS H81M-K soc.1150 H81 DDR3 mATX 1xPCIe USB3 GL iG D-Sub DVI	974.00
Procesor	+ INTEL Celeron Procesor G1840 2.8GHZ/LGA1150/2MB/Haswell	985.00
Operační paměť	+ Kingston DDR3 2GB DIMM 1333MHz CL9 SR x16	362.00
Pevný disk	+ Seagate BarraCuda 3,5" - 1TB/7200rpm/SATA-6G/64MB	1 096.00
Optická mechanika	+ ASUS DVDRW DRW-24D5MT/BLK/B/AS, 24x, SATA, cerná, bulk	308.00
Operační systém	+ MS OEM Windows 10 Pro x32 CZ 1pk DVD	3 358.00
Montáž	+ Montáž PC	401.00

Výsledná cena této sestavy je 8 103 Kč bez DPH. Konfigurace byla navržena Konfigurátorem PC společnosti ASBIS dne 15.3.2017. [49]

Tabulka 3: Varianta 2 – Nové PC

Kategorie	Produkt	Cena bez DPH
Skříň	+ Akyga PC skrín Micro ATX cerná	299.00
Zdroj	+ Akyga ATX Zdroj 400W Basic ventiláror 12cm P4 3xSATA	320.00
Základní deska	+ ASUS H81M-K soc.1150 H81 DDR3 mATX 1xPCIe USB3 GL iG D-Sub DVI	974.00
Procesor	+ INTEL Core i3-4170 3.7GHz/3MB/LGA1150/HD4400/Haswell Refresh	2 743.00
Operační paměť	+ Kingston DDR3 4GB DIMM 1333MHz CL9 SR x8	624.00
Pevný disk	+ Seagate BarraCuda 3,5" - 1TB/7200rpm/SATA-6G/64MB	1 096.00
Optická mechanika	+ ASUS DVDRW DRW-24D5MT/BLK/B/AS, 24x, SATA, cerná, bulk	308.00
Operační systém	+ MS OEM Windows 10 Pro x64 CZ 1pk DVD	3 376.00
Montáž	+ Montáž PC	401.00

Výsledná cena této sestavy je 10 141 Kč bez DPH. Konfigurace byla navržena Konfigurátorem PC společnosti ASBIS dne 15.3.2017. [49]

4.8.6 Stanice

Na všech stanicích byly provedeny úpravy v rámci předcházejících změn. Na počítači majitele byla nastavena možnost digitálního podpisu emailu, který je občas vyžadován zahraničními subjekty, daný certifikát firma již vlastnila. Provedené změny na stanicích:

- Omezení přístupu ke složkám a souborům na PC v rámci LAN
- Připojení počítače do domény
- Nainstalování ERA agenta ESET a přenesení správy na server
- Mapování sdíleného disku pomocí GPO
- Instalace digitálního podpisu
- Zapnutí automatických aktualizací nainstalovaného software

5. Výsledky a diskuse

Byla provedena důkladná analýza bezpečnosti a ochrany dat v dané pražské společnosti. Během této analýzy bylo zjištěno, že firma disponuje kvalitním hardware v některých oblastech, nad kterým lze aplikovat změny pro zvýšení bezpečnosti. Toto zjištění celkovou cenovou kalkulaci výrazně snížilo, jelikož nebylo nutné nakupovat nové vybavení do dané společnosti. Změny nad současným hardware byly provedeny v rámci diplomové práce zdarma, ale jejich ohodnocení je znázorněno v Tabulka 6. Dále byly vypracovány dvě varianty pro nákup nového hardware do dané společnosti.

Tabulka 4: Cenová kalkulace č. 1

Typ zařízení	Varianta	Cena Kč bez DPH
Router	Mikrotik RB750Gr3	1 313,-
Disk – RAID	WD Gold 4TB	4 x 4 892,-
Nové PC	Viz Tabulka 2: Varianta 1 – Nové PC	5 x 8 103,-
Celková cena		**61 396,-**

Zdroj: Vlastní, ceny převzaty ze stránek Alza.cz [50] a Asbis.cz [49] k 15.3.2017

Tabulka 5: Cenová kalkulace č. 2

Typ zařízení	Varianta	Cena Kč bez DPH
Router	Mikrotik RB951G-2HnD	1 726,-
Disk – RAID	WD Gold 6TB	4 x 6 710,-
Nové PC	Viz Tabulka 3: Varianta 2 – Nové PC	5 x 10 141,-
Celková cena		**79 271.-**

Zdroj: Vlastní, ceny převzaty ze stránek Alza.cz [50] a Asbis.cz [49] k 15.3.2017

Mezi sestavami není velký cenový rozdíl pro danou společnost, proto byla po diskusi s vedením společnosti zvolena k zakoupení varianta číslo 2, nabízející kromě zvýšené bezpečnosti i očekávanou delší životnost z hlediska výkonu zakoupeného hardware.

Tabulka 6: Přehled změn nad současným hardware

Typ změny	Popis	Časová dotace
Analýza stavu	Analýza současného stavu zabezpečení	30 hodin
Nastavení routeru	Konfigurace nového routeru	2 hodiny
Nasazení domény	Instalace a konfigurace domény	4 hodiny
Nasazení ESET	Instalace a konfigurace centrálního prvku	2 hodiny
Nasazení WSUS	Instalace a konfigurace služby WSUS	3 hodiny
Školení zaměstnanců	Příprava a provedení školení zaměstnanců	6 hodiny
Změny na stanicích	Aplikování změn na stanicích	8 hodin
Celkový čas		**55 hodin**

Zdroj: Vlastní

Celkový strávený čas analýzou a provedením změn nad současným hardware je dle tabulky 6 vypočten na 55 hodin. Tato práce nebyla firmě účtována, jelikož byla provedena v rámci diplomové práce. Při současné průměrné hrubé mzdě 28 297 Kč [51] by plat správce počítačové sítě při této časové dotaci činil 9 727 Kč. Toto je částka za plat vlastního zaměstnance, jelikož by firma musela najmout externího zaměstnance, jeho mzda by byla navýšena o provizi jeho společnosti a případně o dopravu zaměstnance.

Firmě bylo závěrem doporučeno provádět pravidelný audit nastavení a kontroly využívaného hardware a software externím zaměstnancem, jelikož firma nemá vlastního správce počítačové sítě.

6. Závěr

Cílem práce bylo představení moderních trendů v oblasti bezpečnosti a ochrany dat v malém firemním prostředí. Představeny byly hlavní oblasti, které byly analyzovány a zhodnoceny v existujícím firemním prostředím v pražské firmě LAMPS, a.s. V první polovině praktické části bylo cílem zhodnocení nynějšího stavu zabezpečení v rámci této firmy. Zjištěné nedostatky byly charakterizovány a byla navržena jejich úprava v rámci druhé poloviny praktické částí diplomové práce. Některé navržené změny byly provedeny ihned po analyzování dané oblasti po dohodě s vedením společnosti.

Výsledkem analýzy a následného návrhu zabezpečení bylo vytvoření cenové nabídky na provedené změny, které již proběhly nebo jsou plánovány. S vedením společnosti byla vybrána jedna z navržených možností. Nákup hardware a provedení dalších plánovaných změn, s tím spojených, je plánován na druhou polovinu roku. Výsledkem provedených změn je zvýšení celkového zabezpečení daného podniku. Veškerých plánovaných cílů bylo tedy dosaženo.

7. Seznam použitých zdrojů

1. ČECH, Jaroslav. *Analýza a demonstrace vybraných síťových útoků*. Praha, 2005. Bakalářská práce. VYSOKÁ ŠKOLA FINANČNÍ A SPRÁVNÍ.

2. KABELOVÁ, Alena a Libor DOSTÁLEK. *Velký průvodce protokoly TCP/IP a systémem DNS.* 5., aktualiz. vyd. Brno : Computer Press, 2008. 978-80-251-2236-5.

3. O'REGAN, Gerard. *Introduction to the History of Computing.* Berlín : Springer, 2016. 978-3-319-33138-6.

4. PETERKA, Jiří. Rodina protokolů TCP/IP [online]. [cit. 2.1.2017]. Dostupný na WWW: http://www.earchiv.cz/a96/gifs/p632k151.gif

5. PETERKA, Jiří. Síťový model TCP/IP. *Archiv článků a přednášek Jiřího Peterky.* [Online] [cit. 2016-12-20] http://www.earchiv.cz/a92/a231c110.php3.

6. KLIMEŠ, Cyril. *Principy výstavby počítačů a operačních systémů*. Ostrava: Kovosil, 2007. ISBN 978-80-903694-1-2.

7. PLUMMER, David. *An Ethernet Address Resolution Protocol* [online]. 1982 [cit. 2016-12-20]. Dostupné z: https://tools.ietf.org/pdf/rfc826.pdf

8. POSTEL, Jon. Internet Control Message Protocol [online]. 1981 [cit. 2016-12-20]. Dostupné z: http://www.rfc-base.org/txt/rfc-792.txt

9. INTERNET ENGINEERING TASK FORCE. *Requirements for Internet Hosts -- Communication Layers* [online]. 1989 [cit. 2016-12-21]. Dostupné z: http://www.rfc-base.org/txt/rfc-1122.txt

10. DROMS, Ralph. *Dynamic Host Configuration Protocol* [online]. 1993 [cit. 2016-12-21]. Dostupné z: https://tools.ietf.org/html/rfc1531

11. MICROSOFT. ALS Microsoft® Windows® 2000 Network Infrastructure Administration, Second Edition [online]. [cit. 5.1.2017]. Dostupný na WWW: https://www.microsoft.com/mspress/books/sampchap/6371/0735618704-04.gif

12. DROMS, Ralph a Ted LEMON. *DHCP Příručka administrátora*. Brno: Computer Press, 2004. ISBN 80-251-0130-4.

13. W3C a MIT. Hypertext Transfer Protocol -- HTTP/1.1 [online]. 1999 [cit. 2016-12-22]. Dostupné z: http://www.rfc-base.org/txt/rfc-792.txt

14. PASSERI, Paolo. 2016 Cyber Attacks Statistics [online]. [cit. 12.1.2017]. Dostupný na WWW: https://i1.wp.com/www.hackmageddon.com/wp-content/uploads/2017/01/2016-Motivations-Behind-Attacks.png

15. VALENTINO, Vishnu. *Kali Linux Man in the Middle Attack* [online]. [cit. 2017-01-05]. Dostupné z: http://www.hacking-tutorial.com/hacking-tutorial/kali-linux-man-middle-attack/#sthash.3Dd1Qo2r.dpbs

16. MCMASTER UNIVERSITY. Man in the Middle Attack [online]. [cit. 12.1.2017]. Dostupný na WWW: https://www.hackingloops.com/wp-content/uploads/2016/06/owasp-man_in_the_middle.jpg

17. MOOS, Jiří. *Laboratoř hackera – vaše lokální wifi síť nemusí být bezpečná* [online]. [cit. 2017-01-05]. Dostupné z: http://cdr.cz/clanek/hacking-lokalni-wifi-site-arp-spoofing-utok

18. DIMITRIOS, Tournas. ARP cache poisoning / ARP spoofing (MIT) [online]. [cit. 17.1.2017]. Dostupný na WWW: https://tournasdimitrios1.files.wordpress.com/2011/02/arp-spoofing.png

19. BALOCH, Rafay. Ethical hacking and penetration testing guide. ISBN 1482231611.

20. TETZ, Edward. *Cisco networking all-in-one for dummies*. Hoboken, NJ: John Wiley & Sons, c2011. --For dummies. ISBN 9781118137857.

21. CISCO SYSTEMS. *IP Source Guard* [online]. [cit. 2017-01-08]. Dostupné z: http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/12-2SY/configuration/guide/sy_swcg/ip_source_guard.html

22. HALLER, Martin. *Bráníme se odposlechu: ARP Cache Poisoning a připojení počítače k síti* [online]. [cit. 2017-01-08]. Dostupné z: http://www.lupa.cz/clanky/arp-cache-poisoning-a-pripojeni-pocitace-k-siti/

23. KHALIMONENKO, Alexander; STROHSCHNEIDER, Jens; KUPREEV, Oleg. Kaspersky DDOS intelligence report for Q3 2016 [online]. [cit. 23.1.2017]. Dostupný na WWW: https://cdn.securelist.com/files/2016/10/ddos_q3_en_5.jpg

24. BEAL, Vangie. *DDoS attack - Distributed Denial of Service* [online]. [cit. 2017-01-09]. Dostupné z: http://www.webopedia.com/TERM/D/DDoS_attack.html

25. WAGNON, John. BIG-IP LTM SYN Check [online]. [cit. 23.1.2017]. Dostupný na WWW: https://devcentral.f5.com/Portals/0/images/metapost/News-Articles/ltwagnon/2013/Apr/Windows-Live-Writer-74c02fc9b247_F599-Presentation1_2.jpg

26. KRAUSE, Michal. *Noční můra jménem SYN flooding* [online]. [cit. 2017-01-09]. Dostupné z: https://www.root.cz/clanky/nocni-mura-jmenem-syn-flooding/

27. HOUSER, Robert. *Priority bezpečnostní politiky v malých a středních firmách* [online]. [cit. 2017-01-14]. Dostupné z: https://www.systemonline.cz/it-security/priority-bezpecnostni-politiky-v-malych-a-strednich-firmach.htm

28. PETŘÍČEK, Miroslav. *Stavíme firewall* [online]. [cit. 2017-01-14]. Dostupné z: https://www.root.cz/clanky/stavime-firewall-3/

29. PETERKA, Jiří. *Proxy brány* [online]. [cit. 2017-01-14]. Dostupné z: http://www.earchiv.cz/b01/b0100025.php3

30. VÁVRA, Tomáš. *Bezpečnost podnikových sítí* [online]. [cit. 2017-01-14]. Dostupné z: http://computerworld.cz/securityworld/bezpecnost-podnikovych-siti-46405

31. KUGLER, Zdeněk. *Proxy Firewall*. Brno, 2009. Diplomová práce. VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ. Vedoucí práce Radim Pust.

32. AMENIT S.R.O. *Antivirový program* [online]. [cit. 2017-01-15]. Dostupné z: https://www.antivirovecentrum.cz/antiviry.aspx

33. VAIDYA, Harendra, Shahrukh MIRZA a Nayan MALI. *International Journal of Advance Research in Engineering, Science & Technology* [online]. 2016 [cit. 2017-01-15]. ISSN 2393-9877.

34. REAL TIME ENTERPRISES. *Network Intrusion Detection System* [online]. [cit. 2017-01-15]. Dostupné z: http://www.real-time.com/linuxsolutions/nids.html

35. KEIJSER, Jan Just a Eric F. CRIST. *Mastering OpenVPN. Packt Publishing,* 2015. ISBN 978-1783553136.

36. MAREK, Michal. Jak bezpečně surfovat na veřejné Wi-Fi? Pomůže VPN [online]. [cit. 27.1.2017]. Dostupný na WWW: http://jablickar.cz/wp-content/uploads/2016/12/VPN_explained_transparent_grey-640x320.png na WWW: http://jablickar.cz/wp-content/uploads/2016/12/VPN_explained_transparent_grey-640x320.png

37. BOUŠKA, Petr. VPN 1 - IPsec VPN a Cisco [online]. [cit. 2017-01-21]. Dostupné z: http://www.samuraj-cz.com/clanek/vpn-1-ipsec-vpn-a-cisco/

38. KÖHRE, Thomas. *Stavíme si bezdrátovou síť Wi-fi*. Brno: Computer Press, 2004. ISBN 80-251-0391-9.

39. JAHODA, Bohumil. *Přechod na HTTPS* [online]. [cit. 2017-01-21]. Dostupné z: http://jecas.cz/https

40. MICROSOFT. *How EFS Works* [online]. [cit. 2017-01-22]. Dostupné z: https://technet.microsoft.com/library/Cc962103

41. ORMAN, Hilarie. *Encrypted Email: The History and Technology of Message Privacy*. Springer, 2015. ISBN 978-3-319-21344-6.

42. HLADKÁ, Eva; FOUSEK, Jan. Šifrování emailu [online]. [cit. 30.1.2017]. Dostupný na WWW: https://is.muni.cz/do/1492/el/sitmu/law/html/images/asymcrypto.png

43. PRVNÍ CERTIFIKAČNÍ AUTORITA, A.S. *Elektronický podpis* [online]. [cit. 2017-01-22]. Dostupné z: http://www.ica.cz/Elektronicky-podpis

44. HLADKÁ, Eva; FOUSEK, Jan. Elektronický podpis [online]. [cit. 30.1.2017]. Dostupný na WWW: https://is.muni.cz/do/1492/el/sitmu/law/html/images/elpodpis.png

45. MICROSOFT. *BitLocker Drive Encryption Overview* [online]. [cit. 2017-01-22]. Dostupné z: https://technet.microsoft.com/en-us/library/cc732774(v=ws.11).aspx

46. BITTO, Ondřej. *1001 tipů a triků pro Microsoft Windows 8*. Brno: Computer Press, 2013. ISBN 978-80-251-3806-9.

47. *web společnosti LAMPS, a.s.* [online]. Praha, 2009 [cit. 2017-03-28]. Dostupné z: http://hracky.lampshracky.cz/sortiment-hracek.html

48. *MikroTik Wiki* [online]. Mikrotik, 2016 [cit. 2017-03-28]. Dostupné z: https://wiki.mikrotik.com/wiki/Main_Page

49. *Konfigurátor PC* [online]. ASBIS CZ, 2016 [cit. 2017-03-15]. Dostupné z: http://www.asbis.cz/default.asp?show=configallnew&scatag=pc

50. *Web Alza.cz* [online]. ALZA CZ, 2017 [cit. 2017-03-15]. Dostupné z: http://www.alza.cz

51. *Web platy.cz* [online]. Profesia CZ, spol. s r.o., 2017 [cit. 2017-03-15]. Dostupné z: http://www.alza.cz

8. Přílohy

Příloha 1 : Seznam použitých zkratek.....67

Příloha 1 : Seznam použitých zkratek

AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
ARP	Address Resolution Protocol
ARPA	Advanced Research Projects Agency
BOOTP	Bootstrap Protocol
CCMP	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol
DDoS	Distributed Denial of service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Systém
EFS	Encrypted File System
FAT	File Allocation Table
HIDS	Host-based intrusion detection systém
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IDS	Intrusion detection system
IP	Internet Protocol
ISO	International Organization for Standardization
OSI	Open Systems Interconnection model
LAN	Local area network
MAC	Media Access Control
MBR	Master Boot Record
NTP	Network Time Protocol
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VPN	Virtual Private Network

WINS Windows Internet Naming Service

WPA2 Wi-Fi Protected Access 2