Univerzita Pardubice

Fakulta ekonomicko-správní

Bezpečnost informačních systémů v prostředí počítačových sítí

Jiří Helvich

Bakalářská práce
2016

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2015/2016**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jiří Helvich**
Osobní číslo:	**E13207**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Název tématu:	**Bezpečnost informačních systémů v prostředí počítačových sítí**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování:

Cílem je popsat a vysvětlit principy ochrany dat v prostředí sítí a navrhnout praktickou ukázku nastavení zabezpečení serverového OS Windows jako řadiče domény s Active directory.
Osnova:
- Úvod do problematiky
- Bezpečnost sítí a ochrana dat
- Návrh řešení na konkrétním případu
- Vyhodnocení

Rozsah grafických prací:

Rozsah pracovní zprávy: **cca 35 stran**

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

Seznam odborné literatury:

HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. 3., aktualiz. vyd. Brno: Computer Press, 2006, 211 s. ISBN 80-251-0892-9.
DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Vyd. 1. Brno: Computer Press, 2004, 190 s. ISBN 80-251-0106-1
TVRDÍKOVÁ, Milena. Aplikace moderních informačních technologií v řízení firmy : nástroje ke zvyšování kvality informačních systémů. 1. vyd. Praha : Grada, 2008. 173 s. ISBN 978-80-247-2728-8.
STANEK, William R. Mistrovství v Microsoft Windows Server 2008: [kompletní informační zdroj pro profesionály]. Vyd. 1. Brno: Computer Press, 2009, 1364 s. ISBN 978-80-251-2158-0.
RUSSEL, Charlie a Sharon CRAWFORD. Microsoft Windows Server 2008: velký průvodce administrátora. Vyd. 1. Brno: Computer Press, 2009, 1271 s. Administrace (Computer Press). ISBN 978-80-251-2115-3.

Vedoucí bakalářské práce: **Ing. Pavel Jirava, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **29. září 2015**

Termín odevzdání bakalářské práce: **29. dubna 2016**

L.S.

doc. Ing. Renáta Myšková, Ph.D.
děkanka

prof. Ing. Jan Čapek, CSc.
vedoucí ústavu

V Pardubicích dne 29. září 2014

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 27. 5. 2016 Jiří Helvich

PODĚKOVÁNÍ:

Touto cestou bych rád poděkoval vedoucímu práce Ing. Pavlu Jiravovi, Ph.D. za jeho odbornou pomoc a cenná doporučení, která mi pomohla při zpracování mé bakalářské práce.

ANOTACE

Tato bakalářská práce se zabývá problematikou bezpečnosti informačních systémů v prostředí počítačových sítí. Práce řeší bezpečnost v oblasti informatiky, architekturu sítí, možné kybernetické útoky a protiopatření a operační systémy pro řízení bezpečnosti IS. V textu je poukázáno na slabá místa a chyby v zabezpečení, časté útoky a účinnou prevenci. Praktická část této práce je zaměřena na nastavení zabezpečení OS Windows Server 2008 R2.

KLÍČOVÁ SLOVA

Bezpečnost, Internet, LAN, servery, sítě, software, WAN, Windows

TITLE

Security of information systems in networked environment

ANNOTATION

This bachelor's thesis deals with the security of information systems in network environment. The thesis copes with security in computer science, network architecture, possible cyber attacks and countermeasures and operating systems for security control. There is the frequent attacks, weaknesses, vulnerabilities and effective prevention pointed out in the text. The practical part of the thesis is focused on the security settings of Windows Server 2008 R2.

KEYWORDS

Security, Internet, LAN, servers, networks, software, WAN, Windows

Obsah

SEZNAM TABULEK

SEZNAM ILUSTRACÍ

ÚVOD

Cílem této práce je popsat a vysvětlit principy ochrany dat v síťovém prostředí a vytvořit praktickou ukázku nastavení zabezpečení serverového OS Windows jako řadiče domény s Active Directory.

V úvodu této práce je popsána historie, která se vztahuje k bezpečnosti informací a vývoji počítačových sítí. Dále jsou popsány možné kybernetické útoky a opatření proti nim. Kybernetické útoky a protiopatření budou zkoumány z pohledu vnitřního zabezpečení a vnějších rizik, jako jsou vnější útoky z internetu a vnitřní útoky z lokální či uzavřené sítě. Kybernetické útoky většinou vznikají za účelem poškodit integritu, dostupnost a důvěrnost informací. Je třeba si uvědomit, že informační systém se skládá nejen ze softwaru, ale i z hardwaru, dat a lidí. V textu je popisován serverový operační systém MS Windows a služby, které nabízí.

Bezpečnost informací v oblasti ICT (Information and Communication Technologies) je v dnešní době kybernetických a teroristických útoků velmi aktuální téma. Tato bezpečnost je klíčovým faktorem pro sítě i informační systémy. Přestože je jedním z hlavních požadavků na nově vznikající a vyvíjející se sítě, existuje značný nedostatek snadno implementovatelných metod a strategií zabezpečení.

Svět, ve kterém žijeme, se vyznačuje digitalizací a elektronizací. Vlivem Internetu se svět zmenšuje, avšak Internet má své světlé i stinné stránky. Zejména v oblasti ochrany informací a identity je velmi nebezpečný. V oblasti ochrany informací lze považovat za velice nebezpečné útoky hackerů a špionážních škodlivých kódů. Naopak vzhledem k ochraně identity jsou nebezpečné zejména sociální sítě. Neustále stoupající počet útoků vyžaduje kvalitnější a náročnější ochranu v oblasti hardwaru i softwaru.

Tato práce popisuje zabezpečení a sítě založené na standardech IEEE 802.11 a IEEE 802.3. První norma definuje standardy sítě Ethernet a druhá bezdrátové sítě [11].

Motto:

Myslím, že počítačový virus má hodně společného se životem. Vypovídá to něco o lidské povaze, když si uvědomíme, že jediná forma života, jíž jsme stvořili, je čistě destruktivní.

Stephen Hawking

1 ÚVOD DO PROBLEMATIKY

Počítačové sítě a bezpečnost informací mají jako každá jiná problematika svojí historii. Historie je vždy důležitou součástí pro pochopení stavu v přítomnosti a je dobrým zvykem se s ní seznámit. Právě první kapitola je věnována historii komunikace, kryptologie a počítačových sítí.

1.1 Historie komunikačních sítí

V evoluci sítí lze považovat za počátek výměny informací poštovní síť, kterou lze definovat jako první komunikační síť. Historie této komunikační sítě sahá až do starověku (Perská říše, starověké Řecko), kdy pomocí fyzické výměny zpráv docházelo ke komunikaci. [10][19] První prakticky využitelné zařízení (telegraf) k přenosu informací na základě elektromagnetického principu sestrojil Carl Friedrich Gauss a Wilhelm Eduard roku 1836 v Mnichově. Dne 25. května 1844 odeslal americký malíř Samuel Morse zprávu "What hath God wrought?", která byla odeslána na vzdálenost 50 km z Washingtonu do Baltimoru. V následujících letech vznikaly bezdrátové telegrafy a radioamatérské telegrafie. [31][37] Již v této době byla řešena bezpečnost vzhledem k úniku a dostupnosti informací. Telegraf, který používal k přenosu kabelové spoje, byl jednoduše odposlouchávatelný a znemožnění komunikace se provádělo přerušením linky. Na základě potřeby skrytí významu zprávy se začíná dostávat do popředí kryptologie.

1.2 Historie kryptologie

Kryptologie je věda, která se zabývá utajováním významu přenášených zpráv a naopak. Slovo kryptologie pochází z Řeckého slova kryptós, což znamená skrytý. Dělíme ji na kryptografii a kryptoanalýzu. Kryptografie se zabývá utajováním významu zpráv. Naopak kryptoanalýza se zabývá ziskem obsahu šifrovaných zpráv bez znalosti informace nutné pro dešifrování. [12][6] První známky kryptologických metod pocházejí ze středověkého Egypta, přibližně z roku 1900 před n. l. Pokud chtěli staří Egypťané utajovat význam psaných zpráv, používali hieroglyfy, které byly odlišné od běžně používaných. Za průkopníka modernější kryptografie je považován Johannes Trithemius (1462-1516), což byl benediktinský opat ze Sponheimu, který napsal knihu Steganographia. Velké pozornosti se kryptologie těšila v období první a druhé světové války, kdy byla poměrně masivně využívána. Jeden z nejznámějších šifrovacích strojů je Enigma, kterou používala za druhé světové války německá vojska k šifrování utajovaných informací. Moderní kryptologii započal Claude Shannon (1916-2001)

a díky své práci „Communication Theory of Secrecy Systems“ je pokládán za otce matematické kryptografie. [9][4][8]

1.3 Historie počítačových sítí

Historie počítačových sítí sahá až do šedesátých let minulého století. Na základě vynálezu přepínané paketové sítě a stanovení standardů sítí odolných proti výpadku jednotlivých komunikačních uzlů, dochází k průlomu vědeckotechnického pokroku v oblasti digitální komunikace. Rozvojem komunikačních technologií vzniká potřeba integrované komunikace, na kterou vědci odpovědí vývojem protokolu TCP/IP (Transmission Control Protocol / Internet Protocol). [2][23] Za průkopníka v oblasti přepojování paketů lze považovat Leonarda Kleinrocka z MIT (Massachusetts Institute of Technology), který v červenci 1961 publikoval první knihu na téma přepojování paketů. Prvním autorem uceleného konceptu síťové komunikace byl J.C.R. Licklider, jenž byl také z MIT. [2][14]

RAND Corporation v roce 1964 v rámci utajeného projektu navrhla pro ministerstvo obrany USA řešení rozlehlé odolné sítě, která nepotřebuje žádnou centrální složku a její funkčnost byla zaručena i v případě výpadku některé její části. Princip sítě byl postaven na rovnocennosti všech uzlů a vlastních autoritách pro předávání, přijímání a vytváření zpráv. Na vývoji odolné sítě spolupracovala RAND s univerzitami MIT a UCLA (University of California, Los Angeles). Technika této sítě byla označena jako technika přepojování paketů (packet switching) ve variantě, kterou dnes nazýváme datagramová služba (datagram service). Metoda přepojování paketů byla poprvé použita v roce 1968 v rámci experimentální sítě National Physical Laboratory (Národní laboratoř pro fyziku) ve Velké Británii, kde se problematikou přepínané paketové sítě zabýval Donald W. Davies. Čtyřuzlová síť ARPANET (Advanced Research Project Agency Network) vzniká jako výsledek výzkumu počítačových sítí roku 1969. Projekt sítě ARPANET měl za úkol ověřit techniku přepojování paketů v praxi a umožnit dálkový přístup k tehdejším superpočítačům. [14][2][18]

ARPANET obsahovala v roce 1971 patnáct uzlů a v roce 1973 po připojení Velké Británie a Norska již obsahovala třicet sedm uzlů. Přenosová rychlost díky IMP (Interface Message Processor) a přenosovému protokolu NCP (Network Control Protocol) byla z původní rychlosti 2,4 kb/s zvýšena na 50 kb/s. Z výše uvedených informací vyplývá, že lze považovat ARPANET za předchůdce Internetu. První pokusy komunikace na základě protokolu TCP probíhaly souběžně v mezinárodním měřítku na třech místech: ve Stanfordu, u firmy BBN (Bolt, Beranek and Newman) a v Londýně na University College. Na základě výsledků praktických zkoušek byla potvrzena životaschopnost nového protokolu TCP. V roce 1978 dochází k oddělení

IP protokolu od TCP. V následujících letech ARPANET rychle roste a dochází k propojení s ostatními sítěmi, jako jsou CSNET (Computer Science Network) a EUnet (The European Network). V roce 1983 vzniká oddělením části ARPANETu vojenská síť s názvem MILNET. V roce 1985 vznikla nová topologie počítačové sítě NSFNET (National Science Foundation Network). NSFNET postavený na platformě protokolu TCP/IP postupem času přejímá původní roli ARPANETu. Síť NSFNET v dnešní době slouží jako páteřní síť Internetu ve Spojených státech. Na základě uvolňování pravidel pro připojování do těchto sítí a souběžně s rychlým rozvojem komunikačních technologií a osobních počítačů, došlo k obrovskému nárůstu propojenosti počítačových sítí a rozvoji WAN/MAN/LAN až do dnešní podoby Internetu. [14][18][2]

Internet jako globální datová síť, je soustava registrovaných sítí, které mají schopnost vyměňovat si pakety protokolu IP. Internet jaký dnes známe, započal svoji éru na podzim roku 1990, kdy byl spuštěn první WWW (World Wide Web) server. Tehdy vědci Tim Berners Lee a Robert Cailliau použili princip hypertextu (soubor textů navzájem propojených odkazy), který poprvé definoval Ted Nelson v roce 1965 a přidali k tomu komunikační protokol HTTP (Hyper Text Transfer Protocol). První WWW server fungoval v CERNu na počítači NeXT Computer a sloužil pro komunikaci vědců. [32][16] Počet připojení k Internetu postupně narůstal a v roce 2015 bylo připojeno kolem 3,4 miliardy lidí. Od roku 2000 do roku 2015 vzrostl počtu připojených obyvatel o 832%, viz tabulka 1 [15].

Z této kapitoly vyplývá, že lidé již od starověku mají potřebu komunikace na dálku a zároveň se snaží význam obsahu přenášené zprávy chránit před kompromitací. S vývojem komunikačních a informačních technologií a rozvojem celosvětové datové sítě se tato potřeba stává nedílnou součástí každodenního života, jak pracovního tak soukromého. S vývojem ICT je spojeno snižování komunikace prostřednictvím fyzických entit, jako jsou například kurýři. Rovněž poštovnictví zaznamenalo obrovský úbytek poštovních zásilek. Využívání komunikace prostřednictvím celosvětové datové sítě Internet a neustále rostoucí počet zařízení, komunikujících prostřednictvím této sítě, zvyšuje riziko kompromitace a dostupnosti dat, ukradení identity dat a dalších škodlivých událostí. Toto riziko hrozí ve státním, firemním i soukromém sektoru.

Tabulka 1: Počet připojení k Internetu v roce 2015

WORLD INTERNET USAGE AND POPULATION STATISTICS NOVEMBER 30, 2015 – Update						
World Regions	**Population 2015 Est.**	**Population % of World**	**Internet Users 30 Nov 2015**	**Penetration % Population**	**Growth 2000-2015**	**Users % of Table**
Africa	1,158,355,663	16.0 %	330,965,359	28.6 %	7,231.3%	9.8 %
Asia	4,032,466,882	55.5 %	1,622,084,293	40.2 %	1,319.1%	48.2 %
Europe	821,555,904	11.3 %	604,147,280	73.5 %	474.9%	18.0 %
Middle East	236,137,235	3.3 %	123,172,132	52.2 %	3,649.8%	3.7 %
North America	357,178,284	4.9 %	313,867,363	87.9 %	190.4%	9.3 %
Latin America / Caribbean	617,049,712	8.5 %	344,824,199	55.9 %	1,808.4%	10.2 %
Oceania / Australia	37,158,563	0.5 %	27,200,530	73.2 %	256.9%	0.8 %
WORLD TOTAL	7,259,902,243	100.0 %	3,366,261,156	46.4 %	832.5%	100.0 %

Zdroj: upraveno podle [15]

2 ARCHITEKTURA SÍTÍ

Než se budeme zabývat dělením počítačových sítí, musíme si říci, k čemu sítě vlastně slouží. Pojmem počítačová síť se rozumí spojení dvou a více zařízení, které mají schopnost komunikovat prostřednictvím síťového prostředí. Vlastní komunikace je realizována prostřednictvím síťových karet, metalických či optických kabelů a bezdrátových spojů. Počítačové sítě jsou vytvářeny proto, aby mohli uživatelé komunikovat na dálku, sdílet data, aplikace a HW (hardware) vybavení. HW vybavení může být například tiskárna, modem, osobní počítač, ale i smart telefon nebo smart televizor. Za HW vybavení můžeme ve své podstatě považovat jakékoli zařízení, které má síťový interface a schopnost vzdálené komunikace. Pod pojmem komunikace můžeme vnímat zasílání, přijímání, nebo sdílení dat prostřednictvím nějaké aplikace či HW, jako jsou například e-mail klienti, IM (Instant messaging) klienti, VoIP telefonie nebo také online aplikace v Internetu.

Při prvním pohledu na síť jako celek ji můžeme rozdělit na prvky, které členíme do tří skupin. První skupinou prvků jsou síťová koncová zařízení. Sem můžeme začlenit osobní počítače, tiskárny, smart telefony apod. Dalším skupinou je síťový HW. Tuto kategorii můžeme ještě rozdělit na dvě podskupiny a to na aktivní a pasivní HW. Za aktivní prvky považujeme síťové periferie výše uvedených koncových zařízení. Tyto prvky nám spojují kabeláže, krabičky, patch panely a nazýváme je pasivní částí. Do pasivní části síťového HW řadíme i technologické skříně, ve kterých jsou osazeny jak pasivní, tak i aktivní prvky. Poslední třetí skupinou je síťové programové vybavení, které je nainstalováno na zařízeních v počítačové síti. Spoje můžeme realizovat metalickými a optickými kabely nebo bezdrátovým způsobem. [11][20]

2.1 Referenční model ISO/OSI

Model ISO/OSI (International Standardization Organization / Open System Interconnection) je sedmivrstvý referenční model a můžeme ho porovnat se známějším modelem TCP/IP v tabulce 1. Tento model byl v roce 1984 vytvořen organizací ISO, se záměrem vytvořit standard pro přenosy v sítích. Model definuje celkovou funkci každé vrstvy a principem je převzetí úkolů vyšší vrstvy od nižší. Model OSI doporučuje, jak mají vrstvy fungovat horizontálně mezi sítěmi. [11][1]

2.2 Síťový model TCP/IP

Jak již bylo uvedeno v kapitole „Historie sítí a bezpečnosti“, protokol TCP/IP vznikl na základě požadavku amerického ministerstva obrany, které chtělo vytvořit robustní síť odolnou proti výpadkům důležitých uzlů sítě.

Architekturu modelu tvoří vrstvy a existují dva pohledy na tento model. Máme formální čtyř a neformální pětivrstvé pojetí tohoto síťového modelu, viz tabulka 2. Stejně jako u modelu OSI, každá vrstva reprezentuje určitou funkci, neboli protokol, který musí být v síti zajištěn. Tato architektura je pojmenována na základě dvou primárních protokolů TCP/IP, který společně navrhli vědci Robert Elliot Kahn a Vinton Cerf. [20][14]

Tabulka 2: Model TCP/IP a ISO/OSI

<table>
<tr><th>Vrstva</th><th>Síťový model TCP/IP (neformální)</th><th>Vrstva</th><th>Síťový model TCP/IP (formální)</th><th>Vrstva</th><th>Model OSI</th><th>Protokoly TCP/IP</th></tr>
<tr><td rowspan="3">5</td><td rowspan="3">Aplikační</td><td rowspan="3">4</td><td rowspan="3">Aplikační</td><td>7</td><td>Aplikační</td><td rowspan="3">HTTP, SMTP, POP3, DHCP, DNS</td></tr>
<tr><td>6</td><td>Prezentační</td></tr>
<tr><td>5</td><td>Relační</td></tr>
<tr><td>4</td><td>Přenosová</td><td>3</td><td>Přenosová</td><td>4</td><td>Přenosová</td><td>TCP, UDP</td></tr>
<tr><td>3</td><td>Internetová</td><td>2</td><td>Internetová</td><td>3</td><td>Síťová</td><td>IP</td></tr>
<tr><td>2</td><td>Datové Spoje</td><td rowspan="2">1</td><td rowspan="2">Síťové rozhraní</td><td>2</td><td>Spojová (linková)</td><td rowspan="2">Ethernet, frame relay, PPP</td></tr>
<tr><td>1</td><td>Fyzická</td><td>1</td><td>Fyzická</td></tr>
</table>

Podle názvu protokolu můžeme určit, do jaké vrstvy v určitém modelu protokol patří.

Zdroj: upraveno podle [20]

2.3 Funkce jednotlivých vrstev modelu ISO/OSI

Jak již bylo uvedeno, každá vrstva reprezentuje určitou funkci. U modelu TCP/IP dochází ke spojení více vrstev z modelu ISO/OSI, proto je z tohoto důvodu dále popisován vícevrství model. Veškeré podkapitoly k tomuto tématu jsou čerpány z uvedené literatury pod [11][1][28].

2.3.1 Aplikační vrstva

Tato vrstva je vrstvou nejvyšší a je nejvíce vnímána ze strany uživatelů. Realizuje aplikační služby za účelem zpřístupnění síťových služeb uživatelům. Jednoduše řečeno tuto vrstvu využívají síťové aplikace pro zpřístupnění služeb, jako jsou například elektronická pošta (POP3 – Post Office Protokol, SMTP – Simple Mail Transfer Protokol), přenos souborů (FTP – File Transfer Protokol), překlad IP adres na názvy (DNS – Domain Name System)

a webové stránky (HTTP – Hypertext Transfer Protokol). V této vrstvě se nenacházejí uživatelské aplikace.

2.3.2 Prezentační vrstva

V rámci této vrstvy jsou převáděna data mezi různým formáty kódování dat jako je například ASCI (American Standard Code for Information Interchange) pocházejících z různých sítí. Data jsou dále komprimována z důvodu snížení zatížení sítě a mohou být i šifrována / dešifrována vzhledem k požadovanému zabezpečení přenosu dat.

2.3.3 Relační vrstva

Jak již z názvu vyplývá, tato vrstva navazuje a ukončuje relace mezi dvěma komunikujícími entitami vyšší vrstvy. Další schopností je ověřování uživatelů a zabezpečení zařízení. Mezi hlavní představitele patří služby, jako jsou RPC (Remote Procedure Call) a protokoly QOS (Quality of Service)

2.3.4 Transportní (přenosová) vrstva

Transportní (přenosová) vrstva má podle standardů odpovědnost za spolehlivost a integritu dat při přenosu. Připravuje segmenty dat, které mají být přeneseny a následně sestaveny. Pokud jsou pakety doručeny ve špatném pořadí, tak právě tato vrstva zodpovídá za jejich správné sestavení. Do segmentů jsou přidávány údaje o koncovém zařízení neboli adresování. Typickým představitelem transportní vrstvy je již zmiňovaný protokol TCP.

2.3.5 Síťová vrstva

V této vrstvě nalezneme protokol IP, který zodpovídá za směrování paketů (datagramů) v síti. Mezi základní vlastnosti této vrstvy patří adresování, což je stanovení trasy mezi zdrojem a cílem. Trasa je volena pomocí směrování, které zabezpečují v lokální síti přepínače (switche) a mezi sítěmi přepínače (routery) za pomocí routovacích tabulek. V této vrstvě nenajdeme mechanismus na detekci či opravu chyb.

2.3.6 Spojová (linková) vrstva

Druhá nejnižší vrstva určuje strategii pro sdílení fyzických prostředků a uskutečňuje přenos datových rámců po fyzickém médiu. Aby mohl být tento přenos uskutečněn, musí vrstva zpracovat informace, které obdrží z vyšších vrstev. Zároveň rovněž rozhoduje, zda jim budou přijaté rámce od jiných zařízení předány. V této vrstvě je využívána MAC adresa, což je jedinečná fyzická adresa zařízení. Další částí protokolu je LLC (Logical Link Control).

Ten definuje způsob použití linky, synchronizaci rámců, řetězení toku a detekci chyb. Pro úspěšné doručení musí být splněny dvě podmínky. První podmínkou je ověření integrity rámce na straně příjemce a druhou je potvrzení této informace na straně odesílatele.

2.3.7 Fyzická vrstva

Fyzická vrstva určuje elektrické, optické, mechanické vlastnosti sítě a popisuje reprezentaci binární soustavy v signálu. Jak již samotný název napovídá, jedná se o fyzické prostředky sítě, kterými proudí informace. V této vrstvě platí i fyzikální vlastnosti o přenosu elektrických a optických, popřípadě bezdrátových impulsů. Pro dosažení delší vzdálenosti se využívají opakovače. V této vrstvě neexistuje mechanismus ke zjištění významu odeslaných nebo přijatých bitů.

2.4 Logická přilehlost

Princip komunikace podle modelu OSI lze popsat jako posloupnost událostí, které jsou potřeba v rámci síťové komunikační relace. Logická přilehlost znamená nefyzickou schopnost přímé komunikace mezi protokoly dvou a více uzlů. Jedná se například o zdánlivou schopnost komunikace protokolů IP na dvou počítačích. Jak je vidět v tabulce 3, vertikální komunikace probíhá skrz přilehlé vrstvy a protokoly. [28]

Tabulka 3: Logický tok vrstvených komunikací

Vrstva	Model OSI		Model OSI
7	Aplikační		Aplikační
6	Prezentační		Prezentační
5	Relační		Relační
4	Přenosová	Logický tok	Přenosová
3	Síťová		Síťová
2	Spojová (linková)		Spojová (linková)
1	Fyzická	Skutečný tok	Fyzická

Zdroj: upraveno podle [28]

2.5 Síťové protokoly a služby

V síťovém prostředí jsou protokoly jedním ze základních stavebních prvků sítí. Jedná se o protokoly, které patří do třetí a čtvrté vrstvy v modelu ISO/OSI, viz tabulka 2. V historii mezi nejznámější a v dnešní době již skoro nepoužívané protokoly patří IPX/SPX (Internet Packet

Exchange / Sequenced Packet Exchange) vyvinutý firmou Novell a NetBEUI protokol od firmy IBM. [11][1]

Jelikož jsou protokoly IPX/SPX a NetBEUI téměř nevyužívané, proto je v dalším textu pracováno pouze se skupinou protokolů TCP/IPv4 a s navazujícími protokoly vyšších vrstev. Jen pro upřesnění je přidána poznámka o adresování v sítích IPX/SPX, které je prováděno v hexadecimálním tvaru.

Internet protokol je v dnešní době nejrozšířenějším protokolem ve verzi 4 a 6. TCP patří do čtvrté (přenosové) vrstvy a IP se řadí do třetí (síťové) vrstvy. Zjednodušený princip přenosu dat v sítích TCP/IP můžeme popsat následujícím způsobem. Síťová aplikace, která požaduje spojení, osloví aplikační vrstvu, z které putuje požadavek do vrstvy přenosové. V této vrstvě je zorganizován přenos dat a poté vlastní přenos zabezpečí vrstva síťová. Pro tuto práci je však podstatná problematika adresování v síti, kterou musí každý administrátor ovládat. Jedná se o problematiku adresování v rámci jedné sítě, lépe řečeno, jednoho uzlu a komunikace mezi různými uzly. [11][1]

2.5.1 Internet protokol – IPv4

Strukturu IPv4 definuje dokument RFC 791. Každá adresa IP se skládá ze dvou částí a každá část se skládá z oktetů, jejichž počet závisí na velikosti sítě. První část udává adresu sítě a druhá část udává adresu klienta, viz tabulka 4. Sítě dělíme do tří základních tříd, které můžeme používat při standardním a nestandardním maskováním v 32 bitové adresaci. Třída A má rozsah prvního oktetu 0-127 a adresuje 126 sítí. Třída B má rozsah prvního oktetu 128-191 s adresací pro 16 tisíc sítí. Poslední třída C má rozsah prvního oktetu 192-223 a adresuje 2 milióny sítí. Maskování sítě je udáváno počtem bitů, které jsou zapisovány za poslední oktet sítě (např. /8). Pro lepší přehled je přiložena tabulka 5, která obsahuje třídy sítí. [11][20][1]

Při adresování v sítích IPv4 je nutné pamatovat na sítě, které jsou vyloučeny z volného používání. Jedná se o sítě třídy D, které mají interval od 224.0.0.0.1 do 239.255.255.255.255 a jsou určené pro skupinové adresování (multicast). Další třída E s prvním oktetem od 240 do 254 je určena pro experimentální účely. Poslední, ale významná síť je s prvním oktetem 127, která slouží jako loopback (localhost). [28]

Nástupcem IP verze 4, která je přes 30 let stará, je IP verze 6. Ta vznikla v první polovině devadesátých let minulého století a je založena oproti 32 bitové adresaci IPv4 na 128 bitové adresaci. Vznikla jako reakce na možné vyčerpání adresního prostoru verze 4 a chybějící zabezpečení síťové vrstvy. Sdružení IANA (Internet Assigned Numbers Authority – autorita

pro přidělování čísel v Internetu) v únoru 2011 rozdělilo všechny bloky centrálního registru IPv4 lokálním registrům světových regionů. Protokol IPv6 je rozšíření verze 4. Stávající aplikace potřebují minimální, nebo žádné úpravy, aby mohly využívat verzi 6. Rozdíl v počtu adres je značný, protože IPv4 nabízí přibližně 4 miliardy adres (232), naproti tomu IPv6 jich nabízí 3,4x1038. Jak vidíme, nárůst počtu sítí je citelný. Dalším popisem IPv6 se nebudeme zabývat, protože praktická část je postavena na IPv4. [28][25]

Tabulka 4: Ukázka adresace IPv4

Síť	Maska	Zkrácený zápis	IP adresa koncového klienta
192.168.2.0	255.255.255.0	192.168.2.0 / 24	192.168.2.10
11000000.10101000. 00000010.00000000	11111111.11111111. 11111111.00000000		11000000.10101000. 00000010.00001010

Tabulka obsahuje zápis v decimální a binární soustavě.

Zdroj: vlastní zpracování

Tabulka 5: Třídy sítí IPv4

Třída	Rozsah adres prvního čísla	Počet čísel vyhrazených pro adresu sítě	Počet čísel vyhrazených pro adresu koncových zařízení (uzlů)	Počet bitů sítě (maska)	Použití
A	0 – 127	1 (adresuje 126 sítí)	3 (adresuje asi 17. mil uzlů)	8 (255.0.0.0)	rozsáhlé sítě
B	128 – 191	2 (adresuje 16 tis. sítí)	2 (adresuje asi 65 tis. Uzlů)	16 (255.255.0.0)	středně velké sítě
C	192 – 223	3 (adresuje 2 mil. sítí)	1 (adresuje asi 254 uzlů)	24 (255.255.255.0)	menší sítě

Zdroj: upraveno podle [11]

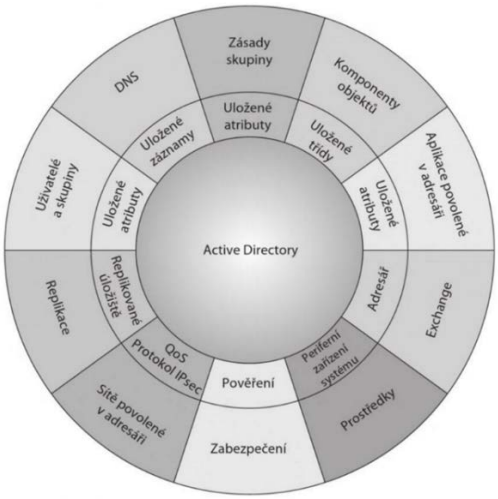
2.5.2 Protokol TCP a UDP

Protokoly TCP a UDP (User Datagram Protocol) patří do přenosové vrstvy a jsou to protokoly spojované. Přebírají data od aplikační vrstvy, které rozdělí na segmenty, očíslují je a seřadí podle požadavku na odeslání. Následným krokem je u TCP logické spojení s přenosovou vrstvou protějšku podle tabulky 3. Vlastní odesílání je realizováno síťovou vrstvou a naopak při příchodu datových segmentů jsou tyto segmenty předány zpět vrstvě přenosové. Rozdíl mezi TCP a UDP je ve spolehlivosti. TCP navazuje a ukončuje relaci, rovněž

je spolehlivý, oproti tomu UDP relaci nenavazuje ani neukončuje a je nespolehlivý. UDP bývá využíván aplikacemi, jako jsou DHCP, FTP, SNMP, DNS a BOOTP. Využívá se tam, kde je potřeba šetřit objem síťového provozu. [11][23]

2.5.3 Active Directory

Active Directory je založeno na protokolu LDAP a obsahuje velmi mnoho objektů, které lze spravovat. Doména v rámci AD je považována za množinu systémů, které jsou vzájemně seskupeny pomocí databáze SAM, viz obrázek 1. [27]



Obrázek 1: Objekty ve službě Active Directory

Zdroj: upraveno podle [27]

2.5.4 Protokol DNS a DHCP

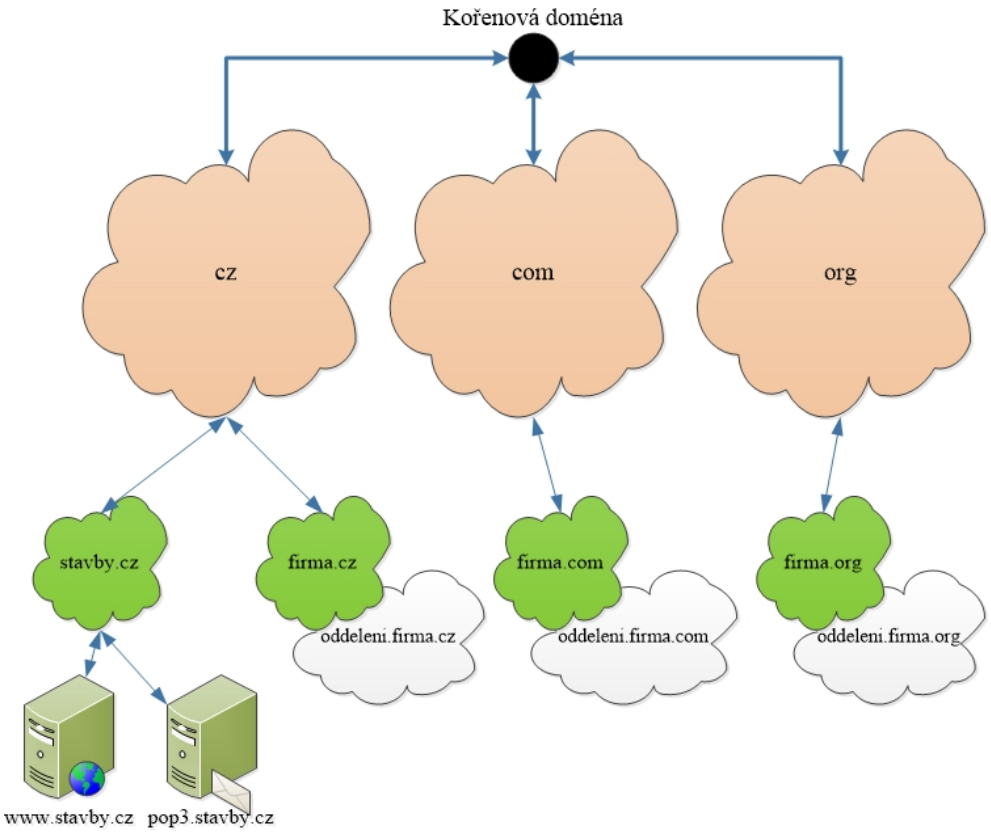
Protokoly DNS (Domain Name Systém) a DHCP (Dynamic Host Configuration Protokol) patří do aplikační vrstvy. Oba tyto protokoly slouží k práci s IP adresami. Prostřednictvím DHCP jsou adresy distribuovány síťovým klientům, navíc i třemi možnými způsoby. Prostřednictvím DHCP lze nastavit klientům nejen IP adresy, ale také informace o síti a službách, jako jsou maska, brána, DNS atd. Prvním způsobem distribuce je dynamická konfigurace, kterou je přidělena IP adresa z adresního rozsahu a to po určitou dobu. Po uplynutí doby rezervace je přidělena nová adresa. Druhým způsobem je ruční konfigurace, kterou se přiřazuje určitá adresa danému síťovému zařízení tzv. rezervace. Třetím způsobem je automatická konfigurace, kterou je IP adresa přidělena trvale, ale až po prvním připojení k síti. Přidělování IP adres prostřednictvím DHCP má více stavů. V prvním kroku klient vysílá DHCPDISCOVER pro zjištění dostupných DHCP služeb. Tento krok je nazýván inicializací. V druhém kroku dochází k výběru nejvhodnějšího DHCP serveru a klient odesílá tzv. DHCPREQUEST. V třetím kroku server DHCP přijme požadavek a po schválení zahájí

zápůjčku odesíláním DHCPPACK. Čtvrtá v pořadí je vazba, v které klient začíná používat přidělenou adresu. Pro předčasné ukončení používání přidělené adresy, server odesílá klientovi zprávu DHCPRELEASE. V rámci času zápůjčky máme tři stavy. Prvním stavem je obnovení, ve kterém dochází / nedochází k souhlasu s obnovením IP adresy. Pokud server nesouhlasí, klient se vrací do kroku inicializace. Druhým stavem je obnovení vazeb, ve kterém klient předpokládá, že DHCP server je nedostupný a klient začne vysílat zprávy DHCPREQUEST na všechny servery. Pokud je odpověď kladná, vrací se klient do kroku vazby. V případě záporné nebo žádné odpovědi se vrací do kroku inicializace. Třetím časovačem je vypršení, které v případě nedostupnosti DHCP serveru ve stavu obnovení vazeb klienta převede do stavu inicializace. Pokud DHCP správně distribuuje všechny potřebné informace o síti, tak již nic nebrání v používání DNS. DNS slouží k překladům IP adres na názvy a zpět. DNS byl původně vyvinut pro Internet, ale je používán i v uzavřených sítích (Intranet). Jedná se o pomocníka uživatelů, kteří si nemusí pamatovat IP adresy, ale pouze názvy. V rámci DNS jsou síťové zařízení rozděleny do zón, které nazýváme domény. První doména, nazývaná kořenová, je zapisována pouze tečkou. Další v pořadí je doména nejvyšší úrovně nebo také známá jako doména prvního řádu. Ta udává typ domény (TLD – Top Level Domain). Z praxe známe domény cz, sk, org, com atd. Další, nižší doména je oddělena tečkou a známe ji pod názvem doména druhého řádu. Tyto domény si subjekty registrují prostřednictvím firem, které tuto službu nabízí. Příklad členění domény je uveden v tabulce 6. Doménový strom je znázorněn na obrázku 2. Správu kořenových DNS serverů zabezpečuje nekomerční organizace ICANN (Internet Corporation For Assigned Names and Numbers). Protokoly DNS a DHCP jsou popsány v jedné kapitole, protože spolu úzce souvisí. Mezi těmito protokoly je vazba zvaná DDNS (Dynamic DNS), jenž zabezpečuje aktuálnost DNS při přidělování adres prostřednictvím DHCP. [11][23][1]

Tabulka 6: Členění domén

Kořenová doména	**Doména prvního řádu (TLD)**	**Doména druhého řádu**	**Doména třetího řádu (subdoména)**
.	cz	firma	oddeleni
.	com	firma	oddeleni
Zápis			
oddeleni.firma.cz oddelení.firma.com			

Zdroj: vlastní zpracování



Obrázek 2: Doménový strom

Zdroj: vlastní zpracování

2.5.5 Ostatní protokoly a služby

Při aplikování sítě řízené službou Active Directory přijdeme do styku s dalšími protokoly aplikační vrstvy, které si v rychlosti popíšeme. [23][1]

- služba WINS (Windows Internet Name Service) – předchůdce DNS, ponechává se z důvodu kompatibility pro služby a aplikace vyžadující překlad adres NetBIOS na IP;
- protokol HTTP / HTPPS (Hypertext Transfer Protocol / Hypertext Transfer Protocol Secure) – zprostředkovává výměnu hypertextových odkazů a sdílení informací;
- protokol FTP (File Transfer Protocol) – slouží pro vyměňování souborů;
- protokol SMTP (Simple Mail Transfer Protokol) – slouží pro odesílání a příjem pošty mezi servery MTA;
- protokol POP3 / IMAP (Post Office Protocol version 3 / Internet Message Access Protocol) – slouží pro stahování zpráv ze vzdáleného serveru MTA (mail transport agent) do MUA (Mail User Agent);
- protokol NTP (Network Time Protocol) – slouží pro synchronizaci času síťových klientů. [23][1]

2.6 Dělení sítí

Počítačové sítě můžeme rozčlenit do několika skupin. Můžeme je dělit podle rozlohy, poskytovaní služeb, topologie a účelu. Další možností dělení je podle přepojování, druhu přenosových technologií, přenosových médií, mobility apod. [23]

2.6.1 Dělení podle rozlohy

Podle velikosti a účelu můžeme rozdělit sítě do několika následujících skupin. Jedná se o rozdělení sítí vzhledem ke geografické rozloze.

2.6.1.1 PAN (Personal Area Network)

Toto označení sítě je velice málo známé a označujeme jím nejmenší sítě jak rozlohou, tak počtem zařízení. Jedná se o druh sítí, který slouží spíše jako dočasné sítě nebo k propojení osobních zařízení, jako jsou osobní počítače, mobilní telefony, PDA (Personal Digital Assistant) atd. Spojení je převážně realizováno prostřednictvím bezdrátového přenosu použitím WiFi, Bluetooth, IrDA (Infrared Data Association) a ZigBee . [23][34]

2.6.1.2 LAN (Local Area Network)

Jak již z názvu vyplývá, LAN je poměrně malá síť, ve které nejsou zařízení této sítě příliš vzdálené. Prvky jsou rozmístěné převážně v určitém objektu, místnosti nebo podniku. Hlavním úkolem této sítě je sdílení místních prostředků, jako jsou tiskárny data a aplikace. Jedná se o zařízení, která jsou zapojené do sítě na malém geografickém území v rozmezí stovek metrů, popřípadě pár kilometrů. Jako přenosové médium v těchto sítích mohou být použity metalické, optické nebo bezdrátové spoje. Rychlost přenosu je v rozmezí 10Mbps až 10Gbps. LAN má dobu vysílání a šíření danou vztahem podle obrázku 3. [23][11][7]

2.6.1.3 MAN (Metropolitan Area Network)

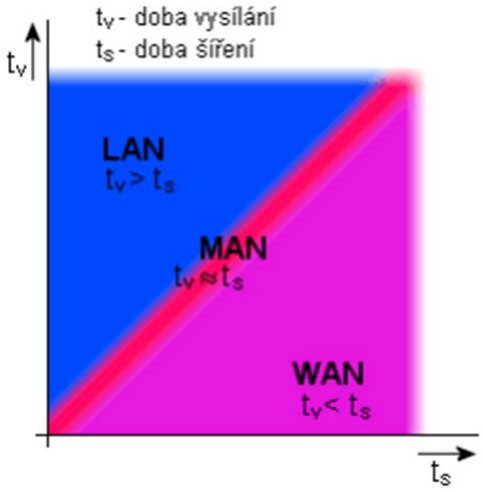
Jedná se o specifický název sítě o geografické rozloze města, popřípadě několika budov. Propojuje LAN, která se na tomto území nacházejí, do jedné sítě. MAN můžeme považovat za síť, která je menší než WAN a větší než LAN. Slouží pro přenos dat, zvuku a obrazu do vzdálenosti desítek kilometrů. Technologie použitých spojů je stejná jako u WAN. Rychlost přenosu je v rozmezí 100kbps až 1Gbps. MAN má dobu vysílání a šíření danou vztahem podle obrázku 3. [23][11][34][7]

2.6.1.4 WAN (Wide Area Network)

Ve své podstatě se jedná o množinu sítí LAN a MAN, která je navzájem propojené po celém světě. Vzdálenost spojů je neomezená a propojení těchto sítí se zprostředkovává všemi typy přenosových médií. Pro přenos jsou využívány speciální linky, jako jsou například technologie ATM, ISDN, Frame Relay. Ve výjimečných případech je využita i technologie Ethernetu. Rozlehlost se může podstatně lišit, čímž nebereme jenom vzdálenost, ale i počet spojovaných zařízení. Za WAN můžeme považovat jak firemní sítě s malou i velkou vzdáleností poboček, tak i městské sítě. Rychlost přenosu je v rozmezí 100kbps až 1Gbps. WAN má dobu vysílání a šíření danou vztahem podle obrázku 3. [23][11][7]

2.6.1.5 Internet

Internet můžeme vnímat jako systém navzájem propojených počítačových sítí LAN, MAN a WAN. [23]



Obrázek 3: Vysílání a šíření dat v síti

Zdroj: [7]

2.6.2 Dělení podle poskytovaní služeb

Následující dělení sítí je odvozeno od postavení uzlů a poskytování služeb. Velké sítě, do kterých je zapojeno větší množství navzájem komunikujících síťových zařízení, jsou realizovány na principu klient-server (počítačové sítě řízené serverem). Menší sítě, zejména domácí nebo účelové sítě, jsou realizovány na principu peer-to-peer (p2p). Sítě p2p jsou vzhledem k pořizovacím nákladům levné a nepotřebují žádné speciální síťové programové vybavení.

2.6.2.1 Peer-to-peer

Počítačové sítě založené na typu peer-to-peer, jak je vidět na obrázku 4, jsou sestavené ze skupiny síťových klientů (počítače, tiskárny, aktivní a pasivních prvky sítě). Princip komunikace je takový, že každý počítač je zároveň klientem i serverem. Jinak řečeno, dochází k přímé komunikaci klientů, neboť službu serveru i klienta obhospodařuje dané koncové zařízení. Tento typ sítě se využívá pro velmi malé sítě s celkovým počtem zařízení přibližně do 10 kusů. V této síti nenalezneme centrální ověřovací autoritu a sdílení služeb může nabídnout každý klient. Tento stav přináší problémy s přihlašováním ke sdíleným prostředkům a aktuálností dat, která jsou nositeli informací. Dalším problematickým faktorem je lokalizace dat, jelikož jsou data uložena na více počítačích. Tento problém některé firmy řeší nasazením takzvaného Pseudo Serveru (sdílení služeb desktopovým OS). Výhodou této sítě je fakt, že pro realizaci můžeme využít libovolnou platformu operačního systému a síťového prostředí. Velmi slabou stránkou je zabezpečení sítě a síťových klientů, protože si za zabezpečení ručí každý klient sám. [11][26][1]

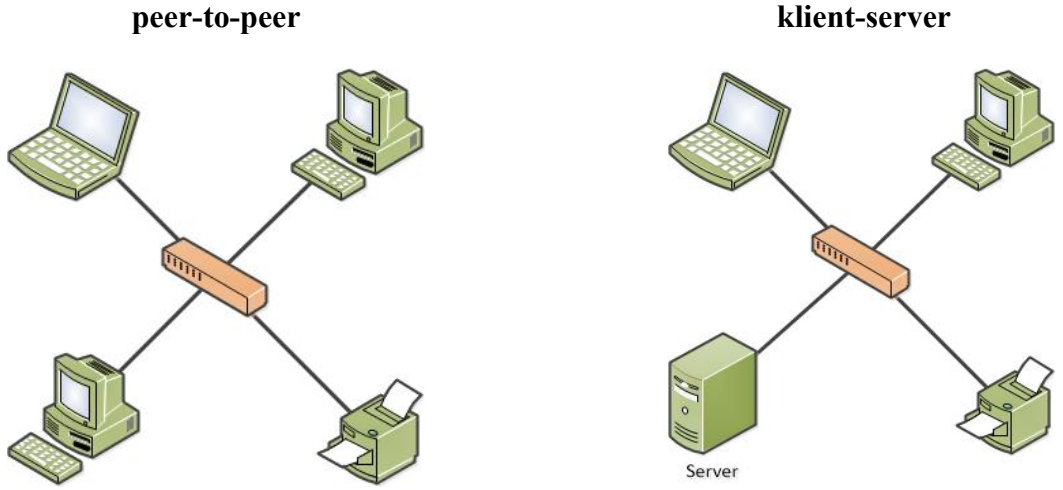
Pokud shrneme vlastnosti tohoto druhu sítě, můžeme říci, že se jedná o síť bez centra řízení a že všichni členové sítě jsou si rovni. Využívá se zejména z důvodu pořizovací ceny a jednoduchosti nastavení.

2.6.2.2 Počítačové sítě řízené serverem

Tento druh sítí je také znám pod názvem klient-server, viz obrázek 4. Tato kapitola je zaměřená pouze na popis této sítě a ne na služby, které jsou servery zprostředkovány.

Počítačové sítě řízené serverem jsou založeny na řízení z jednoho či více center a někdy jsou označovány také jako dvouvrstvé architektury. Tento druh sítě odstraňuje nedostatky p2p sítí v oblasti zabezpečení a správy. Rozdíl mezi p2p a klient-server je pouze v aplikování síťových operačních systémů a síťového programového vybavení. Hardwarové propojení prostřednictvím aktivních a pasivních prvků je identické u obou sítí. Jako centrum sítě můžeme považovat minimálně jeden fyzický server, který bývá zpravidla vyhrazený (dedicated). Tento server je využíván pouze pro účely řízení, sdílení a správy prostředků. Běžně se nevyužívá jako klient nebo pracovní stanice. K serveru přistupují klienti, jenž jsou autorizováni uživatelským účtem a heslem. V případě pozitivní autorizace mají povolen přístup ke sdíleným prostředkům. Klientské zařízení používá síťový software a data jsou ve většině případů ukládána na pevný disk serveru. Serverový hardware a software je na rozdíl od desktopového optimalizován pro rychlé vyřizování požadavků. [1][23][26]

Řízení v síti klient-server, je nejčastěji realizováno prostřednictvím serverů postavených na platformě OS Windows, Linux popřípadě Unix.



Obrázek 4: Sítě p2p a klient-server

Zdroj: upraveno podle [26]

2.6.3 Dělení podle topologie sítě

Topologií sítě se rozumí způsob, jakým jsou různé prvky sítě propojeny a jak jsou data prostřednictvím sítě přenášena. Lze ji tedy vnímat jako určitý tvar či strukturu sítě s danými vlastnostmi. Výsledné vlastnosti sítě jsou určovány topologií, která je prvkem síťového standardu [11]. Topologii sítí můžeme dělit na fyzickou a logickou.

2.6.3.1 Fyzická a logická topologie

Fyzickou topologií popisujeme reálnou konstrukci dané sítě. Konstrukcí je myšleno fyzické zapojení a rozložení zařízení včetně přenosových tras. Logickou topologií se rozumí, jak jsou data přenášena a kudy jsou přenášena. Tato topologie nemusí kopírovat fyzickou. [21]

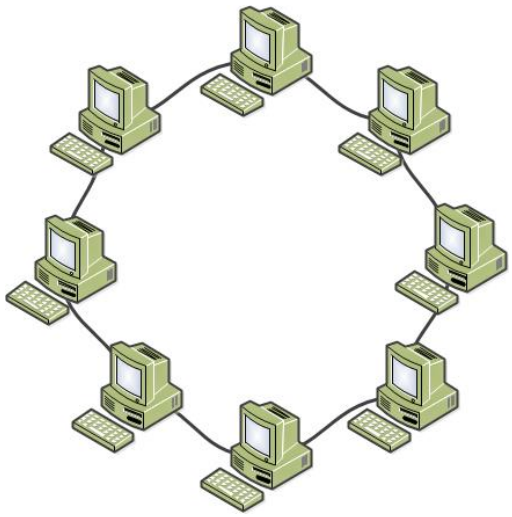
2.6.3.2 Základní topologie sítí

V této kapitole jsou popsány základní typy síťových topologií. Některé z nich se již v dnešní době masivně nevyužívají.

2.6.3.2.1 Kruhová topologie

Kruhová topologie (Ring Topology) je síť typu token, což značí, že síť vytváří souvislý kruh a zprávy jsou postupně předávány. Znamená to, že každý počítač je propojen s dalšími dvěma počítači, viz obrázek 5. Nevýhodou této sítě je stav nefunkčnosti, v případě přerušení spoje. Odstranění této nevýhody spočívá v použití zdvojeného kabelu (IBM Token Ring). Dalšími

nevýhodami jsou komunikace přes mezilehlé počítače, výpadek sítě v případě přidání dalšího klienta. Rovněž se špatně hledají / opravují poruchy. Naopak výhodou je přijatelná (nízká) cena, absence kolizí a jednoduchý přenos dat. [11][21]

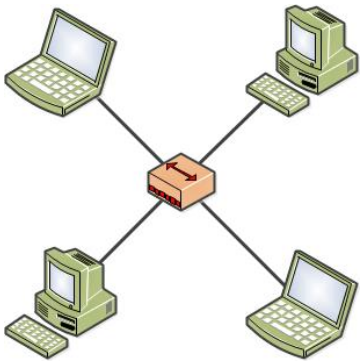


Obrázek 5: Kruhová topologie (ring)

Zdroj: upraveno podle [21]

2.6.3.2.2 Hvězdicová topologie

Hvězdicová topologie (Star topology) je nejvíce používaný způsob spojení síťových prvků, protože je jednoduchá a není náchylná na chyby. Centrem připojení v této topologii je aktivní prvek. Aktivním prvkem může být koncentrátor, HUB, nebo přepínač (switch). Každé zařízení je k centru připojeno vlastním spojem, jak je vidět na obrázku 6, nejčastěji však kroucenou dvoulinkou. Jedná se o jednocestné spojení mezi dvěma uzly. Výhodami této sítě jsou nízké náchylnosti k chybám, výpadek síťového klienta nemá vliv na funkčnost sítě, jednoduchost hledání / oprav poruch a nastavení sítě. Nevýhodou této sítě je větší spotřeba kabeláže a centrální zel, který jakmile vypadne, má za následek kolaps celé sítě. [11][21]

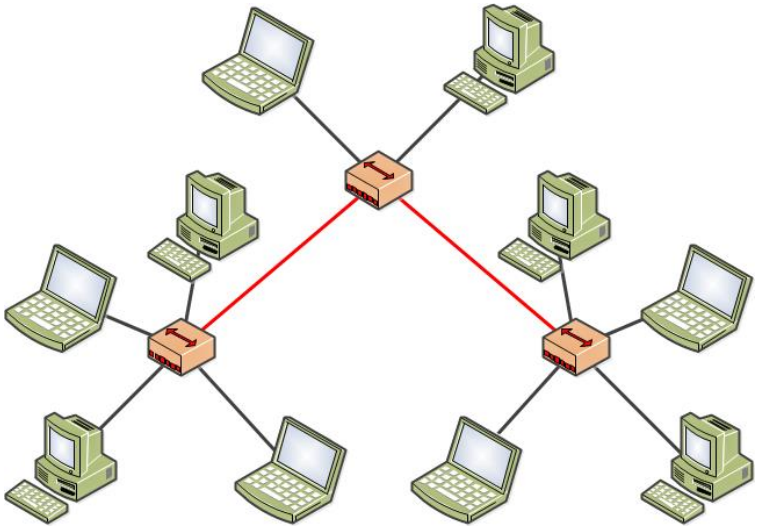


Obrázek 6: Hvězdicová topologie (star)

Zdroj: upraveno podle [21]

2.6.3.2.3 Stromová topologie

Tato topologie (tree topology) je také známá pod názvem hierarchická hvězdicová topologie a používá se pro spojení jednotlivých aktivních prvků zapojených do hvězdicové topologie. Využívá se zejména u rozsáhlých počítačových sítí a připomíná tvar stromu. Jednotlivé hvězdicové sítě jsou propojeny prostřednictvím kabelu připojeného ke speciálnímu vzestupnému portu uzlu, viz obrázek 7. Nevýhodou této topologie je částečná nefunkčnost dále položených uzlů při výpadku uzlu, který je v topologii blíže u kořenového uzlu. Jednoduše řečeno, ovlivněny jsou pouze uzly, které jsou za poškozeným uzlem. Výhodou této topologie je menší ovlivnění celé sítě v případě výpadku dílčího prvku, snížená spotřeba komunikačních kabelů a také zvýšená bezpečnost. [1][21].

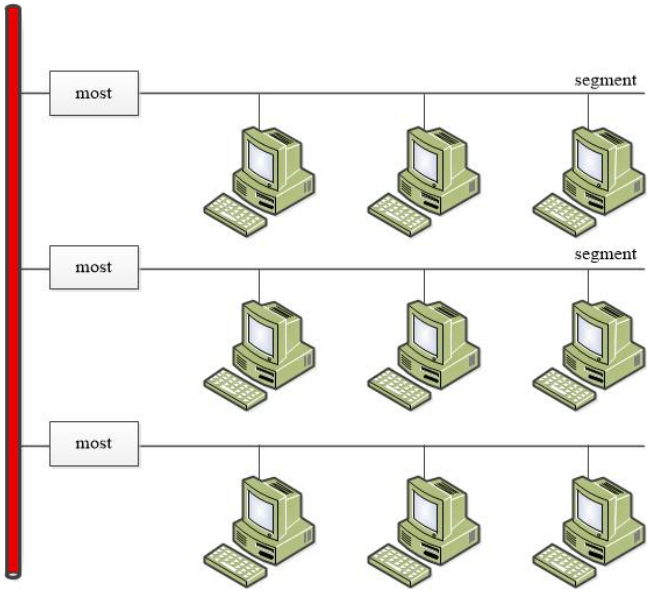


Obrázek 7: Stromová topologie (tree)

Zdroj: upraveno podle [21]

2.6.3.2.4 Páteřní vedení

Ve své podstatě se jedná o spojení prvků dané sítě známé také jako backbone. Jakákoli komunikace zařízení mimo jeden síťový segment je přenášena prostřednictvím páteřního vedení, jak je vidět na obrázku 8. Na páteřní vedení je kladen požadavek na větší přenosovou rychlost, minimálně 100Mp/s a optimálně 1 a více Gb/s. Jako spoje jsou používány metalické a optické kabely nebo bezdrátové spoje. [11][23]

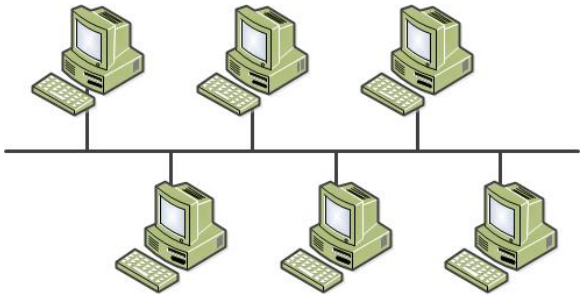


Obrázek 8: Páteřní vedení (backbone)

Zdroj: upraveno podle [35]

2.6.3.2.5 Sběrnicová topologie

Topologie této sítě je založena na zapojení spojovacího kabelu (sběrnice - bus) od zařízení k zařízení. Stanice jsou připojovány ke kabelu pomocí BNC T-konektorů, známých také jako Terminátor. Pro spojení se používá médium v podobě koaxiálního kabelu. Topologie je znázorněna na obrázku 9. Výhoda této topologie je v menší spotřebě kabeláže, nízké ceně a možnosti snadného rozšíření. Nevýhoda je v havárii celé sítě v případě přerušení vedení, principiální nespolehlivost, omezení délky kabelu sběrnice, velký počet spojů a lokalizace závad. [11][21]



Obrázek 9: Sběrnicová topologie (bus)

Zdroj: upraveno podle [21]

2.6.4 Dokumentace k sítím

Jako u každé jiné problematiky, která prochází vývojem, výstavbou a následně je nějakým způsobem spravována, tak i u sítí musí být vytvořena použitelná dokumentace. Základním

kamenem pro vývoj, výstavbu a správu sítě je nezbytná aktualizovaná dokumentace v podobě fyzických a logických map.

2.6.4.1 Fyzické mapy

Fyzické mapy zobrazují fyzickou implementaci sítě. Bývají podrobnější než logické a mohou být z důvodu velkého objemu informací rozděleny na dílčí části. To znamená, že větší sítě mohou být rozkresleny po budovách, odděleních atd. Tyto mapy zobrazují kompletní vedení a umístění všech HW prvků. [1]

2.6.4.2 Logické mapy

Logické mapy jsou ve své podstatě organizační diagramy, které znázorňují primární zařízení a jejich vliv na funkčnost toku dat. Dále znázorňují oboustrannou závislost zařízení vzhledem k funkčnosti. Logické mapy mohou obsahovat i koncová zařízení, ale na nich provoz sítě neleží. Avšak servery a routery v této mapě být zahrnuty musí. U rozsáhlých sítí je vykreslována „vysoká úroveň“ samostatně a dílčí oblasti jsou vykreslovány zvlášť. [1]

3 BEZPEČNOST SÍTÍ A OCHRANA DAT

Tímto jsme se dostali k hlavní kapitole této práce, která popisuje způsoby útoků a ochrany sítí nebo dat. Pro správné pochopení problematiky je důležité vnímat data v informatice, jako nositele informací. Ochrana těchto informací bývá dosti finančně nákladná, a také může být poměr ceny vůči možné škodě dosti nevyvážený. Z tohoto vyplývá, že je potřeba chránit data, která obsahují důležité informace. Rovněž poměr nákladů na ochranu vs. kompromitace informací by měl být vyvážený. Dále je nutné rozlišovat datovou a síťovou bezpečnost. Data chráníme především kryptografií a síť zvolenou bezpečnostní technikou. Hlavní otázkou však vždy zůstává, před kým a jakým způsobem data či síť chránit. Za základ bezpečnosti můžeme považovat dodržování stanovených pravidel a vynucování postihů při jejich nedodržení.

Jelikož je dané téma velmi objemné, není možné jej v této práci celé obsáhnout. Zaměříme se proto na bezpečnostní politiku, bezpečnost informací a mechanismy, útoky na informační technologie, škodlivý programový kód, časté chyby zabezpečení a ochranu možným útokům.

3.1 Základ bezpečnosti

Informační bezpečnost jako obor, který se zabývá zabezpečením informací v rámci počítačových technologií, pochází přibližně z první poloviny osmdesátých let. V této době se informace začaly přesouvat do privátních center výpočetních systémů. Tato centra představovala soustředění informací nesmírných hodnot. Finanční domy zde vedly evidence účtů svých klientů, podniky je využívaly pro řízení výroby a armády v nich soustřeďovaly nejutajovanější informace. V současnosti je hlavním cílem zabezpečení IS komplexnost a provázanost jednotlivých dílčích opatření. Pro zabezpečení maximálního užitku je nutná spolupráce informační bezpečnosti s dalšími druhy bezpečnosti dané organizace. Bezpečnost informačních systémů, například ve firemním prostředí, je chápána jako komplexní zajištění přístupů, manipulace s hodnotami, zálohování, antivirové ochrany atd. Je důležitou součástí koncepce, následného vývoje a význam tohoto zabezpečení neustále roste. Pro správné pochopení dané problematiky je důležité si uvědomit, že informační systémy se skládají z hardware, software, dat a také lidí. [17][33][6] Jinak řečeno jedná se o soubor technických prostředků, metod a lidí [3].

3.2 Bezpečnost informačních systémů

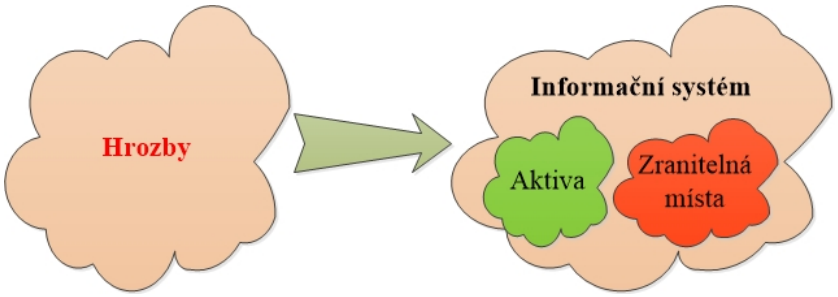
Budeme-li se bavit o firemním prostředí, tak každá firma by měla mít v rámci ISMS (Information Security Management System) pracovníka, který má pravomoci na prosazení

rozhodnutí vzhledem k bezpečnosti CIS (Communications and Information Systems). Tento pracovník mívá označení CISO (Chief Information Security Officer). Jeho úkolem je vypracování bezpečnostní politiky firmy, na jejíž vytvoření se podílí okruh kvalifikovaných osob a tato bezpečnostní politika by měla být schválena nejvyšším vedením firmy. Bezpečnostní politika je, obecně vzato, vize firmy v oblasti CIS bezpečnosti. Měla by obsahovat také analýzu rizik. Analýzou rizik se rozumí ohodnocení aktiv a jejich ohrožení. Mezi další dokumenty, které vytváří CISO patří havarijní plány a směrnice. Havarijní plány slouží jako návod postupů v případě bezpečnostního incidentu či katastrofy. Jelikož je vždy největším rizikem člověk, je nutné sledovat životní cyklus zaměstnance a CISO musí definovat postupy při přijetí zaměstnance, změně pracovního místa, či propuštění zaměstnance. Dokumentace je sice podstatná, ale při její tvorbě se musí vždy vycházet z individuálních podmínek a zájmů dotčených subjektů. Aby toto bylo dodrženo, tak je možné si položit základní otázky: zda a co má být chráněno, před čím má být daná věc chráněna a jakými prostředky a způsoby ochranu realizovat. [33][17][6]

Ve státních organizacích typu AČR, jsou v každém informačním systému rozděleny role mezi skupinu zaměstnanců, tak aby byl eliminován střet zájmů. Bezpečnostní management je definován od nejvyšší role „gestor IS“ po nejnižší pracovníky v rámci bezpečnostního managementu „místní bezpečnostní správci, lokální administrátoři“.

3.2.1 Bezpečnostní politika

Bezpečnostní politika je relativně neměnný základní dokument, který řeší bezpečnost daného IS. Rovněž by měl být závazný pro celou společnost. Hlavní oblasti politiky se rozpracovávají do detailní podoby formou bezpečnostních standardů a závazných interních dokumentů společnosti. Tato politika by měla odpovídat na tyto základní otázky: co potřebujeme chránit, proč to potřebujeme chránit, jakým způsobem to budeme chránit, jak ověříme funkční ochranu a postup při haváriích. Informační systém je nutné chránit před hrozbami, které ohrožují aktiva IS prostřednictvím zranitelných míst, viz obrázek 10. [17][6]



Obrázek 10: Aktiva a hrozby

Zdroj: upraveno podle [6]

Bezpečnostní politiku můžeme rozdělit na bezpečnost fyzickou, personální, informačních technologií, administrativní a procedurální. Jejím základem je identifikování dat a prostředků nacházejících se v IS. Data a prostředky, které potřebujeme chránit, můžeme obecně nazvat aktivem. Další dva kroky řeší určení aktiv, které je nutné chránit, přičemž volba ochrany musí být přiměřená k hodnotě aktiva. Následné zavedení ochrany IS je nutné zkontrolovat, a také je nutné vytvořit plán kontrol se zaměřením na funkčnost této ochrany. Dále je nutné vytvořit havarijní plány, které stanovují kroky v případě bezpečnostního incidentu či katastrofy. [33][6]

Struktura bezpečnostní politiky firmy

- popis – popis organizace, cíle bezpečnostní politiky;
- CISO – personální zajištění;
- analýza rizik – aktiva a jejich cena;
- návrh opatření – určení aktiv a způsobu ochrany;
- havarijní plány – reakce na bezpečnostní incidenty a katastrofy;
- administrativní část – periodické prověřování bezpečnostní politiky. [6]

3.2.2 Analýza rizik

Klíčovou aktivitou při sestavování bezpečnostní politiky je právě analýza rizik. Tato analýza se skládá z identifikace aktiv, hrozeb a vlastní analýzy rizik, kde výstupem je dokument, který obsahuje popis systému a výsledky analýzy. Identifikací aktiv zjišťujeme aktiva, která se v systému nacházejí. Identifikace hrozeb hledá hrozby, které IS hrozí. V rámci vlastní analýzy rizik je přiřazena konkrétním aktivům konkrétní hrozba. [17][6]

3.2.3 Návrh vhodné ochrany

Právě vhodná ochrana je navrhována vzhledem k ceně daného aktiva. V rámci tohoto návrhu lze použít několik přístupů k vypořádání s daným rizikem. Při snížení rizika jsou eliminovány slabiny a hrozby. Postoupením rizika jsou přemístěny náklady na ztrátu k jinému subjektu (pojištění). Akceptování rizika znamená smíření se se ztrátou. Ignoranci rizika považujeme za nesprávné rozhodnutí, při kterém je spoléháno na to, že riziko nenastane. Jednotlivé části bezpečnostních prostředků ochrany mohou zabezpečovat jedno i více dvojic (aktivum-hrozba). Vždy při návrhu odpovídající ochrany je nutné vyčíslit náklady na zavedení a udržování této ochrany. Postupnými kroky se zjišťuje, které dvojice daná ochrana chrání a v případě potřeby je tento postup opakován až do doby, kdy jsou všechny dvojice chráněné. [6][12]

3.2.4 Havarijní plán

Havarijní plán obsahuje postupy, které by měly popisovat činnost při selhání bezpečnostních opatření či katastrofě a dále obsahuje personální zajištění v případě krizového stavu. Cílem je co nejdříve obnovit chod systému a tento proces se skládá z několika kroků, viz tabulka 7. Havarijní plán jako dokument je vyhotovován ve dvou výtiscích, přičemž první je součástí bezpečnostní politiky a druhý je uložen na bezpečném a snadno dostupném místě. [6]

Tabulka 7: Kroky obnovy podle havarijních plánů

Krok	Název kroku	Popis
1	Odstranění akutního nebezpečí	odčerpání vody, uhašení požáru, odpojení systému od počítačové sítě atd.
2	Obnovení důležitých částí systému	výměna poškozených součástí, instalace SW a konfigurace
3	Obnovení poškozených dat	obnovení ze záložní kopie, v případě úmyslného poškození připojit IS k Internetu až po změně zabezpečení
4	Zavedení příslušných protiopatření	změna ochrany (požární hlásiče, firewall, antivir apod.)

Zdroj: upraveno podle [6]

3.2.5 Personální bezpečnost

Součástí informačního systému jsou i lidé, u kterých hrozí úmyslné či neúmyslné porušení bezpečnosti IS. Proto je u každého zaměstnance sledován životní cyklus. Životní cyklus zaměstnance začíná přijetím do firmy. Na další fázi pohlížíme jako na běžný život zaměstnance a v poslední fázi dochází k odchodu zaměstnance. V první fázi dochází k podepsání smlouvy, která by měla obsahovat mimo běžných náležitostí i bezpečnostní politiku a důsledky při její porušení. V rámci běžného života jsou nastavovány příslušné úrovně práv podle zastávané pozice a je prováděno školení. Poměrně důležitou fází je odchod zaměstnance, který můžeme vnímat jako přátelský, nepřátelský a konkurenční. V této fázi by mělo bezprostředně po zániku potřeby držení některého bezpečnostního prvku dojít k jejímu odebrání. Za bezpečnostní prvek můžeme považovat přístupové karty, klíče, účty v IS atd. Podstatné je, aby personální oddělení informovalo důležité pracoviště o nástupu či odchodu zaměstnance. [6][12]

3.3 Bezpečnost informací a mechanismy

Jak již bylo uvedeno, předpokladem pro vytvoření bezpečného prostředí je bezpečnostní politika. Při řešení bezpečnosti je potřeba předvídat možné hrozby a na základě predikce nastavovat bezpečnost celého systému, jak v oblasti síťového prostředí, serverů, tak

i koncových zařízení. To znamená zabezpečení komunikačních kanálů z pohledu logického a fyzického. K dosažení požadované bezpečnosti informací využíváme bezpečnostní mechanismy. Podle zjednodušeného pohledu je prostředí tak bezpečné, jak zabezpečené je nejslabší místo. Dalším podstatným faktorem bezpečnosti je uživatelský komfort neboli user friendly.

3.3.1 Základní požadavky na bezpečnost informací

Mezi základní požadavky na bezpečnost informací patří důvěrnost, dostupnost a integrita.

- důvěrnost – informace jsou přístupné pouze oprávněným uživatelům;
- dostupnost – informace jsou oprávněným uživatelům dostupné v okamžiku potřeby;
- integrita – data jsou kontrolována na nežádoucí modifikaci, která může vzniknout během transportu sítí, chybou v úložišti, nebo úmyslně. [12][33]

3.3.2 Bezpečnostní mechanismy

Bezpečnostní mechanismy můžeme dělit na slabé, střední a silné. Struktura mechanismů by měla být stupňovitá (sériová), a ne široká a mělká, jako je paralelní koncept bezpečnostního mechanismu. Překonáním jednoho bezpečnostního mechanismu sériového konceptu nemá takové fatální následky jako překonání mechanismu u paralelního konceptu. [12]

Typy bezpečnostních mechanismů

- fyzické zabezpečení – (trezory, zámky, ochranka, jmenovky, záložní generátory, chráněná úložiště pro zálohy dat a programů, …);
- logické zabezpečení – SW prostředky (řízení přístupu, využití kryptografie, antivirové produkty, elektronické podpisy, SW firewally, …);
- technické zabezpečení – HW prostředky (identifikační karty a čipy, firewally, archivační média, …);
- administrativní zabezpečení – (bezpečnostní směrnice IS, procedury, školení, hesla, právní normy, etické normy, analýza rizik konfigurace systému, …);
- personální zabezpečení – (prověření osob, kontakty, výpisy z rejstříku trestů, …). [12]

3.4 Útoky na informační technologie

Útoky můžeme dělit na cílené a náhodné. Jde o to, zda se útočníkovi jedná o úmyslné využití slabiny informačního systému ke způsobení škod nebo ztrát, nebo jde jen o náhodný střet slabiny a uskutečněné akce, která vede ke škodám nebo ztrátám. Následně můžeme hodnotit, zda se jedná o útok s velkou či malou škodou a jestli je veden na hardware, software nebo data.

Útočníky můžeme rozdělit na vnitřní a vnější podle logické polohy. Vnější útočí z vně systému a vnitřní naopak. Dalším nejnebezpečnějším útočníkem je celý svět, kdy jeden člověk zneužívá velké množství počítačů. Všichni využívají zranitelných míst systému, která vznikají selháním při návrhu, specifikaci požadavků, řešení projektu, konstrukci a při provozu. Při cílených útocích, útočník hledá nejslabší místo v zabezpečení systému s cílem způsobit škody nebo ztráty. Za narušení bezpečnosti můžeme považovat přerušení nebo odcizení, odposlech, změnu a přidání funkcí nebo dat. Škoda bývá většinou adekvátní ke schopnostem útočníka, a proto dělíme útočníky do tří skupin: amatéři, hackeři a profesionálové. Amatéři využívají dostupných postupů pro prolomení bezpečnosti a jen zkouší jaké to je. Jejich nebezpečnost je mizivá. Hackeři mají dostatek znalostí a často jen zkouší, či sbírají zkušenosti. Jsou limitováni časem a financemi. Byť pronikají do zabezpečených systémů bez záměru uškodit, tak je jejich nebezpečnost vcelku vysoká a informační systémy jsou chráněny právě proti nim. Profesionálové, kteří jsou vysoce kvalifikovaní a používají výborné vybavení, útočí převážně na systémy, které jsou objektem jejich zájmu. Nebezpečnost jejich útoků je vysoká a ochrana velmi nákladná. [6][33][12]

3.4.1 Druhy útoků

Tato podkapitola se zabývá druhy možných útoků z různých úhlů pohledů. Útoky můžeme rozdělit podle druhu provedení na útok přerušením, odposlechem, modifikací a přidáním hodnoty. Následky těchto útoků jsou popsány v tabulce 8. Podle jiné literatury můžeme útoky dělit na útoky pasivní, aktivní, na dostupnost služeb a převzetí moci. [12][6]

Tabulka 8: Útoky podle druhu provedení a jejich následky

Útoky	Následek
Útok přerušením	následkem je ztráta dostupnosti
Útok odposlechem	následkem je ztráta důvěrnosti
Útok modifikací	následkem je ztráta důvěryhodnosti dat (integrita)
Útok přidáním hodnoty	následkem je ztráta autenticity a integrity

Zdroj: upraveno podle [12]

3.4.1.1 Pasivní útoky

Pasivní útok spočívá v prostém získávání dat bez modifikace probíhající komunikace ze strany útočníka. Útoky mohou probíhat vzdáleně, nebo v místě uložení komunikačních zařízení. Mezi SW nástroje útoků patří například trojský kůň nebo jiný nástroj, který provádí skryté operace před uživatelem. Mezi uživatelem nechtěné operace patří přijímání a odesílání dat, rozesílání spamu, zaznamenávání stisku kláves, otevírání zadních vrátek, atd. Jako ochranu

proti trojskému koni je možné využít logické zabezpečení v podobě šifrování dat, antiviru a firewallu. Druhým způsobem je fyzický odposlech, při kterém útočník musí získat fyzický přístup ke komunikačnímu zařízení. Za komunikační zařízení lze v tomto případě považovat jak aktivní, tak pasivní prvky sítě. K zařízení či médiu je připojeno odposlouchávací zařízení přímo fyzicky, nebo například při bezdrátovém přenosu je odposlouchávací zařízení v dosahu šíření radiových vln. Ochranou proti tomuto typu útoku je šifrování dat, fyzická, administrativní a personální bezpečnost. [6][12]

3.4.1.2 Aktivní útoky

Těmito útoky je zasahováno do komunikace, při které dochází k modifikování přenosu dat ve prospěch útočníka nebo předstírání jiné identity útočníkem. Jedná se o útok na integritu dat, při kterém může například útočník změnit číslo bankovního účtu při převodu peněz nebo změní e-mailovou adresu atd. Ochranou proti těmto útokům jsou kontrolní součty přenášených dat, které však musejí být chráněné kryptografickým aparátem z důvodu zamezení modifikace. V druhém případě se útočník snaží podvržením autentizace předstírat, že je někdo jiný. Použití správných protokolů a důsledné autentizace může útočníkovi zabránit v modifikaci přenosu nebo útoku ze středu (útočník se nachází mezi oběma komunikujícími stranami). Pro tento druh útoků jsou využívány metody slovníkových útoků, útoků hrubou silou a sniffingu. Slovníkový útok je využíván k prolomení autentizačních údajů, přičemž je zjišťováno heslo prostřednictvím softwaru, který využívá určitý slovník. Útok hrubou silou spočívá v hledání hesla prostřednictvím postupně generovaného řetězce alfanumerických znaků. Sniffing slouží k zachytávání paketů, jenž jsou nositeli hesel a šifrovacích klíčů. [6][12]

3.4.1.3 Útoky na dostupnost služeb

Při těchto útocích dochází k zabránění dostupnosti služeb. Jsou využívané dvě metody útoků, přičemž první metoda spočívá ve zničení komunikace a druhá metoda přetěžuje systém nebo jeho části. Zničením komunikace se rozumí modifikace komunikace mezi příjemcem a odesílatelem s cílem poškodit smysluplnost přenášených dat. Přetížení sytému, nebo jeho částí má za následek odmítání legitimních požadavků. Pro tyto útoky jsou využívány metody spoofingu a DoS (Denial of Service). Spoofing slouží k falšování záhlaví datagramu, kde jsou změněny údaje o odesílateli, a příjemce vyřizuje velký počet dotazů, které podle něho pocházejí od různých odesílatelů. Je nejčastěji využíván pro DoS útoky. DoS útoky využívají techniku zaplavení, což je zasílání velkého počtu požadavků příjemci. Nebo využívají techniku zneužití chyb, která zneužívá chyb a slabin systému. DoS má mnoho verzí, ale hlavní jsou DoS a dDoS

(Distributed DoS). Základní DoS útok spočívá v útoku jednoho systému na jeden cílový systém. V dnešní době dochází k rozložení zátěže mezi více zařízení, a to umožňuje ochranu proti základnímu útoku. dDoS je distribuovaná verze jeho předchůdce, která zneužívá více systémů (Slave, Zombie) pro útok na jeden či více obětí. Přibližný princip spočívá v tom, že útočník získá kontrolu nad velkým počtem systémů a následně vydá příkaz k útoku na oběť. [6][12]

3.4.1.4 Útok na převzetí moci

Při tomto útoku není získání kontroly nad systémem prostředkem pro další útok, ale cílem. Důvodem útoku může být získání dat, nebo jejich zničení. Útok je možné provést fyzickým, nebo vzdáleným přístupem k systému, popřípadě útokem na spuštěné programy. Ochranou proti fyzickému přístupu k systému je fyzické, technické, administrativní a personální zabezpečení. Útok prostřednictvím vzdáleného přístupu spočívá v získání přístupových údajů například prostřednictvím trojského koně. Útok na spuštěné programy zneužívá chyb v programech s otevřenými síťovými porty. [6]

3.4.1.5 Sociotechnika

Sociotechnice se také říká sociální inženýrství a je využívána pro ovlivňování a přesvědčování lidí s cílem vyzvědět určité informace. Jelikož jsou lidé nejslabším článkem zabezpečeného systému, je nutné tomuto inženýrství věnovat pozornost. Pro útočníka je jednodušší získat informace od člověka, nežli se snažit prolomit zabezpečený systém, přičemž v sociotechnice jsou využívány lidské vlastnosti, jako je autorita, důslednost, společenský souhlas, sympatie, vzácná příležitost a vzájemnost. [12]

3.5 Škodlivý programový kód

Škodlivý software obecně nazýváme malware, který slouží k modifikaci, poškození počítačového systému nebo obtěžování uživatele. Následující seznam je výčet nejčastěji vyskytujících se škodlivých kódů. Historie počítačových virů je datována do roku 1988, kdy student americké university Robert Tappan vytvořil slavného červa, který díky chybě v kódu poškodil řadu systémů a velkou část Internetu [6].

Seznam malware

- počítačový virus slouží k nakažení spustitelného programu, který následně nakazí ostatní aplikace (replikuje se) s cílem ovládnout počítačový systém, ale nešíří se samovolně po síti;

- počítačový červ je programový kód, který má schopnost rozesílání sama sebe na jiné zařízení v síti, nad kterými převezme kontrolu;
- spam je nevyžádané sdělení hromadně šířené internetem, které nejčastěji obsahuje reklamní záležitosti;
- hoax je druhem nevyžádané zprávy, která má za účel pobavit, vystrašit, nebo vyvést v omyl adresáta;
- logická bomba je druh programového kódu, jenž má za účel aktivovat nežádoucí činnost nebo provést destrukci počítačového programu;
- trojský kůň je část počítačového programu, která vykonává jinou a hlavně skrytou nežádanou činnost. Není schopen replikace sama sebe;
- adware není nebezpečný programový kód pro operační systém, ale je to aplikace, která obtěžuje uživatele například reklamou;
- keylogger zaznamenává stisky kláves do logovacího souboru, který je odesílán prostřednictvím internetu;
- hijacker je opět programový kód, který je určený k obtěžování uživatele změněnou domovské stránky v WWW prohlížeči;
- sniffer je poměrně závažný škodlivý počítačový kód, který zachytává síťovou komunikaci a získává z ní hesla, čísla platebních karet apod.;
- spyware je podobný trojskému koni, protože odesílá data bez vědomí uživatele prostřednictvím internetu a šíří se v rámci shareware, freeware atd. [12][13]

3.6 Časté chyby zabezpečení

Mezi nejslabší místa zabezpečení patří slabá hesla, neaktualizovaný SW, spuštěné služby a otevřené porty, špatně nastavená ochrana firewallů, nezabezpečené sdílení dat, nezabezpečený přístup pro vzdálenou správu, nezabezpečené přípojné body ethernetu, absence fyzické ochrany prvků informačních technologií, neexistující bezpečnostní dokumentace a únik informací o zabezpečení.

3.7 Ochrana proti možným útokům

Významnou prevencí proti útokům je využití monitoringu, auditu, firewallu, antiviru, kryptologie, elektronického podpisu, fyzické bezpečnosti, analýzy rizik a bezpečnostní dokumentace. [6][12]

3.7.1 Monitoring a auditní systém

Monitoring slouží k zjišťování aktivit v informačním systému prostřednictvím systémů pro detekci útoků. Auditní záznamy počítačového systému uchovávají informace o zajímavých událostech v počítači, serveru či jiných zařízení. Oboje slouží pro detekci, uchovávání a následnou rekonstrukci zájmové události. Výstupy lze je využít například pro trestní stíhání nebo analýzu problému. [12][6]

3.7.1.1 Systémy a nástroje monitoringu

Základním systémem pro detekci útoků jsou dataminingové nástroje, které analyzují auditní záznamy v reálném čase. Dataminingové nástroje primárně detekují útoky, ale mohou také podávat informace o selhání systému, špatné autentizaci uživatele apod. Auditní záznam by měl obsahovat přesný čas, identifikaci programu, který záznam provedl a identifikaci uživatele. Reakce systémů pro detekci útoků na útok může být aktivní, pasivní, nebo hybridní. Aktivní reakce přímo ovlivňuje nežádoucí aktivitu. Pasivní je opakem aktivní a slouží k zasílání informací o incidentu. Hybridní je kombinací aktivní a pasivní reakce na útok. Dále rozlišujeme lokální a síťové systémy pro detekci útoků. Lokální systémy pro detekci útoků sledují aktivity na jednom počítačovém systému. Síťové systémy sledují aktivitu v celé počítačové síti zachytáváním a analýzou síťových paketů. [6][12]

Systémy pro detekci útoků spolupracují s nástroji, které slouží pro ochranu systému, dat a sítí. Honeypot a padded cel slouží pro odvedení pozornosti útočníka od skutečného systému, kdy honeypot je účelově vytvořený počítač, nebo počítačová síť, která obsahuje podvržená data. Nástroj padded cell funguje stejně jako honeypot, s rozdílem, že útočník je po identifikaci automaticky přesunut do této sítě. Vulnerability scanner je využíván pro testování systému vůči známým hrozbám a může být aktivní, nebo pasivní. [12][36]

3.7.2 Firewall a proxy server

Firewall a proxy server může být v podobě programového vybavení, jež je nainstalováno na počítači nebo serveru anebo v podobě hardwarového vybavení, které má vlastní systém. Firewall je centrální přístupový bod sloužící k propojení sítí s různou úrovní bezpečnosti a důvěryhodnosti. Můžeme ho rozdělit do třech skupin podle technologie. Do první skupiny patří jednoduchý IP filtr, který pracuje na základě sad pravidel, které zakazují určitý provoz na daných portech. Nevýhodou tohoto firewallu je absence schopnosti analýzy procházejících dat a obtížná nastavitelnost pro eliminaci všech možných nebezpečí. Stavový IP filtr je vylepšený jednoduchý IP filtr, jenž monitoruje síťový provoz a upravuje podle něj tabulku stavů, díky

které následně povoluje, či zakazuje provoz podle nastavených pravidel. Aplikační proxy server je určený pro jeden konkrétní protokol a filtruje pakety podle toho, která aplikace a na kterém portu s nimi pracuje. Jednoduše řečeno proxy server je prostředník mezi koncovým zařízením a cílovým serverem, kdy odděluje lokální síť od Internetu. [33][6]

3.7.3 Antivirus

Antivirus je počítačový program, který chrání počítače a servery před virovou nákazou a dalším škodlivým programovým kódem. Pro správnou funkci musí být aktualizovaná databáze virů, zapnuté pravidelné testování, zapnuté testování příchozích souborů a další služby jako je například zasílání reportů. Při použití antivirové ochrany by měl být aktualizovaný i operační systém, jelikož většina virů využívá bezpečnostních děr v OS. Antiviry dělíme podle způsobu vyhledávání na heuristické a signaturové. Signaturové antiviry využívají databáze virů, které obsahují část virů a popis jejich odstranění. Heuristické využívají virtuální oblast, ve které program spustí a zkoumají neobvyklé činnosti. Při používání antivirů ve větším množství počítačů je vhodné využít centrální správu. Z centrální správy můžeme na dálku ovládat antivirové programy síťových klientů, jako jsou osobní počítače a servery. [6][1]

3.7.4 Kryptologie

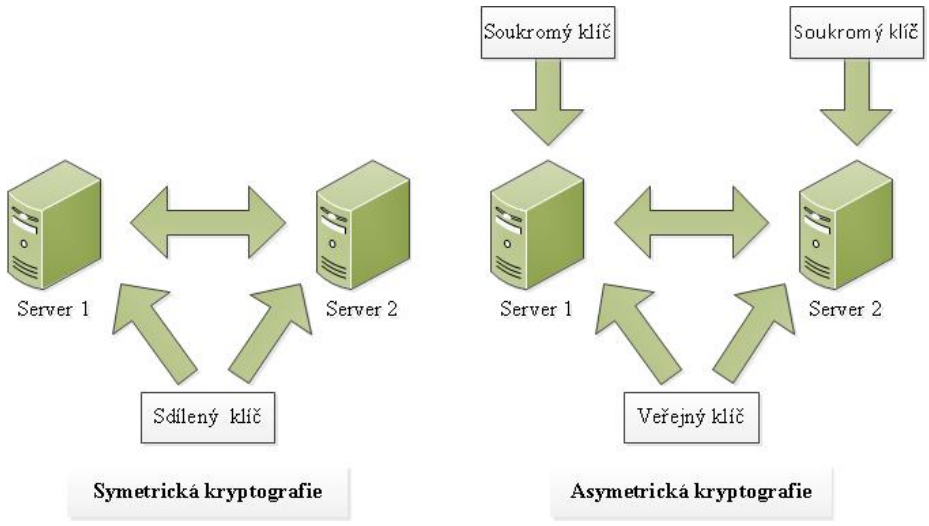
Jak již bylo na začátku práce napsáno, kryptologie je věda, která se zabývá utajováním významu přenášených zpráv a naopak. Dělíme ji na kryptografii, která se zabývá utajováním významu zpráv a kryptoanalýzu, která se zabývá ziskem obsahu šifrovaných zpráv bez znalosti informace nutné pro dešifrování. Budeme se zabývat pouze kryptografií, která slouží k šifrování a dešifrování dat. Šifrování znamená transformaci srozumitelného textu prostřednictvím šifrovacího algoritmu a klíče do nesrozumitelné podoby. Dešifrování znamená zpětnou transformaci nesrozumitelného textu prostřednictvím dešifrovacího algoritmu a klíče do srozumitelné podoby. Prostředky kryptografie můžeme šifrovat a dešifrovat data jako jsou ASCI text, databázové soubory, programy, video a audio soubory atd. Kryptografii dělíme na klasickou, moderní, symetrickou, asymetrickou, blokovou a proudovou. Klasická kryptografie je dělena podle substitučních a transpozičních algoritmů, které spadají do kategorie symetrické kryptografie, viz tabulka 9. Dělení na blokové a proudové je podle množství znaků, která jsou v jednom okamžiku šifrovány. Proudové využívají šifrování po jednom znaku a blokové po blocích znaků. [12][17][6]

Tabulka 9: Klasická kryptografie

Algoritmus	Popis
Substituční	Algoritmy nahrazují každý znak srozumitelného textu jiným znakem šifrovaného textu a jsou lehce prolomitelné.
monoalfabetické	Každý stejný znak srozumitelného textu je vždy nahrazen jedním znakem šifrovaného textu. (A→X; B→Y) Zástupcem této metody je Caesarova šifra.
homofonní	Každý stejný znak srozumitelného textu může být nahrazen jedním znakem ze skupiny znaků šifrovaného textu. (A→11, nebo 15, nebo 19; B→23, nebo 25, nebo 28)
polyalfabetické	Využívají současně několik monoalfabetických algoritmů, podle určitého klíče, jako je například sudé a liché písmeno apod. Zástupcem této metody je Vigenèrova a Vernamova šifra.
polygramové	Každá skupina znaků srozumitelného textu je vždy nahrazena jinou skupinou znaků šifrovaného textu. (ABC→DEF; ABD→DKP)
Transpoziční	Algoritmy pouze mění pořadí znaků v srozumitelném textu a jsou lehce prolomitelné.

Zdroj: upraveno podle [12]

Moderní kryptografii dělíme na symetrickou a asymetrickou. Symetrická kryptografie používá jeden klíč společně pro šifrování a dešifrování. Asymetrická kryptografie využívá pár klíčů, přičemž jedním klíčem je text šifrován a druhým je dešifrován. Klíčem, kterým byl text zašifrován, již nelze tento text dešifrovat. Rozdíl mezi symetrickou a asymetrickou kryptografií je znázorněn na obrázku 11. Mezi nejznámější symetrické šifrovací algoritmy patří DES (Data Encryption Standard), 3DES (Triple – DES), IDEA, BlowFish, CAST a AES. Mezi proudové patří FISH a RC4. Nejznámější asymetrické šifrovací algoritmy jsou RSA, Eliptické kryptosystémy (ECC), Hash algoritmy, ElGamal, Diffie-Hellman atd. [6][17][12]



Obrázek 11: Symetrická a asymetrická kryptografie

Zdroj: upraveno podle [6]

3.7.5 Řízení přístupu

Řízení přístupu se skládá z identifikace, autentizace a autorizace. Identifikací se rozumí tvrzení subjektu o své identitě. Při identifikaci jsou zadávané přihlašovací údaje. Autentizací se rozumí ověření identity prostřednictvím hesel apod. Autorizace je výsledkem předchozích dvou kroků a může být pozitivní, nebo negativní. Pro autentizaci je možné využívat autentizační předměty, jako jsou čipové karty, USB tokeny anebo biometrické informace. Lze ji rozdělit podle použitých identifikačních znaků na znalostní, biometrickou, vícefaktorovou autentizaci a autentizaci prostřednictvím autentizačního předmětu. [6][12]

Identifikační znaky

- znalostní – znalost daného subjektu (hesla, otázky, …);
- biometrický – jedinečné znaky lidského těla (otisk prstu, obličej, oko, dynamika psaní na klávesnici, …);
- autentizace prostřednictvím autentizačního předmětu – (čipová karta, USB token, …);
- vícefaktorová autentizace – kombinace více způsobů autentizace (čipová karta a PIN, …). [12]

V rámci autentizace jsou vytvořeny autentizační protokoly, na které jsou často vedené útoky. Mezi nejčastější útoky patří útok opakováním, ze středu, na hesla a na integritu zpráv. Útok opakováním je založen na odposlechu části komunikace a následné zopakování. Útok ze středu je založen na odposlouchávání komunikace mezi oběma komunikujícími stranami. Při útoku na integritu zpráv se útočník snaží vytvořit takové správy, které můžou dostat komunikující program do nestabilního stavu. [6][12]

4 NÁVRH ŘEŠENÍ NA KONKRÉTNÍM PŘÍPADU

Praktická část se zabývá instalací a nastavením zabezpečení serverového operačního systému MS Windows 2008 R2 jako řadiče domény s Active Directory a to ve firemním prostředí. Ukázka instalace OS je vytvořena ve virtualizační technologii hypervizor HYPER-V. V návrhu řešení je počítáno se dvěma kusy serverů, nicméně tato praktická ukázka se týká pouze nastavení prvního serveru jako hlavního řadiče domény.

4.1 Výchozí situace

Pro praktickou ukázku byla vybrána hypotetická společnost o 20 počítačích a 2 velkokapacitních tiskárnách. Firma se zabývá konkurenčním zpravodajstvím (CI – Competitive intelligence) a požaduje vytvoření bezpečného doménového prostředí jako základ informačního systému. Strukturovanou síť (kabeláž) již má vybudovanou a aktivní prvky jsou nakoupeny, osazeny a zkonfigurovány. Veškerý přístup k síti je realizován metalickými kabely a zásuvky LAN jsou aktivovány na základě požadavku a vždy musí být propojeny se zařízením.

4.2 Specifikace požadavku

Firma vytvořila základní požadavek na služby serveru. V požadavku klade důraz na výběr HW serveru a implementaci zabezpečení serverového operačního systému. Síťová a fyzická bezpečnost je řešena prostřednictvím externí firmy, která vybudovala a nastavila celou síť. Topologie této sítě a zapojení zařízení je patrné z obrázku 12.

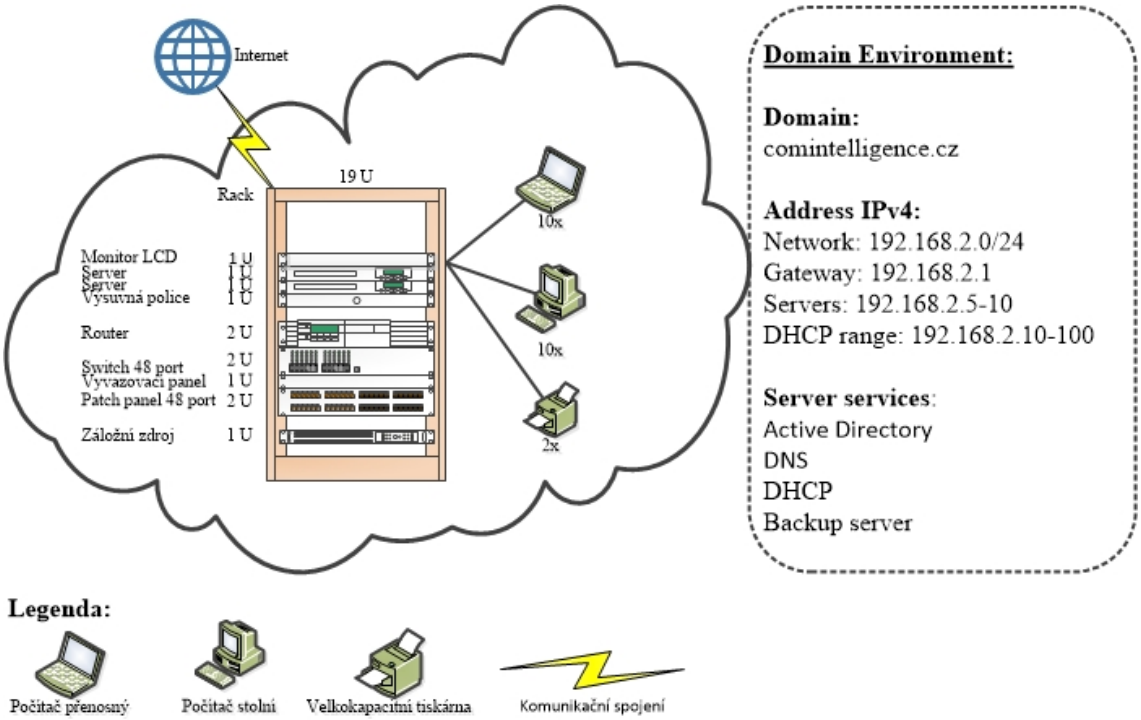
V rámci zabezpečení serveru AD je požadováno nastavení s cílem omezení přístupu počítačům, které nemají nastaveny a aktualizovány základní prvky zabezpečení, jako je například firewall, antivirus a aktualizace OS. Pro případ fyzického neautorizovaného přístupu je požadováno nastavení šifrování disků a zálohování dat, které také slouží k obnově dat a stavu systému při havárii. Pro dosažení většího výkonu a dostupnosti ke sdíleným prostředkům je server vybaven a nastaven příslušným typem řadiče disků. V doménové politice firma požaduje nastavení základních požadavků na doménové účty a audity.

Fáze projektu

1) specifikace požadavků na IS;
2) analýza;
3) návrh;
4) implementace;

5) testování;
6) zavedení;
    a) registrace domény;
    b) výběr verze serverového OS Windows a HW podle požadavku;
    c) instalace serverového OS;
    d) počáteční konfigurace;
    e) instalace a nastavení funkcí;
    f) instalace a nastavení rolí;
    g) připojení počítačů do domény;
    h) vytvoření bezpečnostní politiky;
    i) vytvoření směrnic a proškolení uživatelů;
7) údržba. [3]

V praktické ukázce jsou plněny pouze body b až f, které patří do plánu projektu.



Obrázek 12: Schéma sítě a nastavení

Zdroj: vlastní zpracování

4.3 Výběr verze serverového OS Windows a HW

Firma Microsoft nabízí Windows Server 2008 v několika verzích a je nutné vybrat správnou variantu podle požadavků. Pro účel firmy je vybrána verze Windows Server R2 Standard a operační systém je instalován na server od společnosti DELL (PowerEdge R515 - 2U) [5].

4.4 Instalace Windows Server 2008

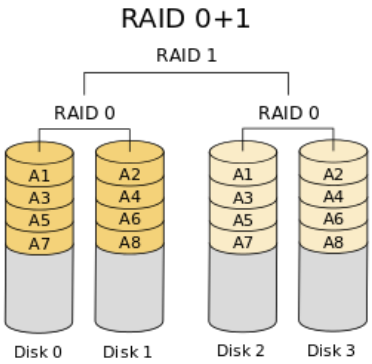
V prvním kroku je nutné nastavit řadič serveru, který je vybavený technologií RAID (Redundant Array of Inexpensive/Independent Disks). RAID technologie může být nakonfigurována s cílem dosáhnout většího výkonu, kapacity nebo dostupnosti. V našem případě je zvolena metoda nastavení, jenž má za účel zvýšit dostupnost a výkon. RAID technologie existuje v HW nebo SW verzi. Hardwarový RAID oproti softwarovému nezatěžuje server, přičemž může zajistit vyšší výkon a existuje v populárním, víceúrovňovém a nestandardním typu. Poměrně dobře jsou popsány úrovně RAIDu na Wikipedii pod URL *https://cs.wikipedia.org/wiki/RAID#Popul.C3.A1rn.C3.AD_typy_RAID*. [30][22]

Pro náš účel je vybrán RAID 01, který zvyšuje přístupovou dobu a dostupnost. Jedná se o dvouúrovňové pole, které potřebuje čtyři disky a využije z jejich kapacity 50%, viz vzorec (1). RAID 01 je kombinací RAID 0, což je spojení více členů do jednoho disku a RAID 1, který disky zrcadlí, viz obrázek 13. Data jsou ukládána prokládaným způsobem na disky (A/B) a (C/D). [24][22]

$$velikost = \frac{n \times c}{2} \tag{1}$$

kde: n=počet disků;

c=kapacita disků.



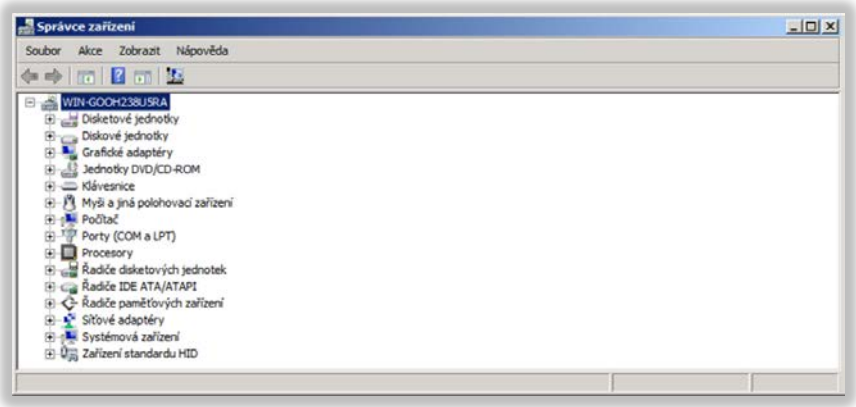
Obrázek 13: RAID 01

Zdroj: upraveno podle [22]

V rámci vlastní instalace je prvním krokem výběr lokalizace OS. Zde je doporučováno, pokud to licence umožňuje, zvolit lokalizaci v jazyce, v kterém vlastníme odbornou literaturu. Instalaci lze provádět lokálně nebo vzdáleně prostřednictvím služby pro nasazení systému Windows [24].

Jednotlivé kroky instalace:

1. výběr lokalizace OS;
2. výběr verze OS – Windows Server 2008 R2 Standard (úplná instalace);
3. přijmutí licenční politiky;
4. výběr typu instalace – vlastní;
5. výběr disku pro instalaci operačního systému;
6. vlastní instalace operačního systému;
7. 2x restart;
8. požadavek na zadání hesla administrátorského účtu (silné heslo – 15 až 20 znaků);
9. kontrola zavedení všech ovladačů a instalace SW dodaného k HW, viz obrázek 14;
10. zadání licenčního klíče a provedení aktivace;
11. instalace antivirové ochrany;
12. stažení a nainstalování aktualizací ze serveru Microsoftu. [24][30]

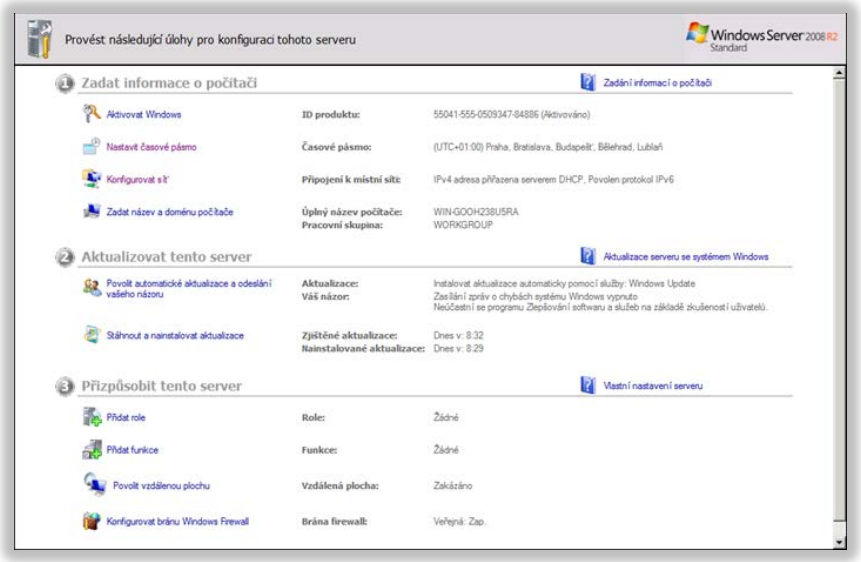


Obrázek 14: Kontrola zavedení všech ovladačů

Zdroj: vlastní zpracování

4.5 Počáteční konfigurace

Dalším krokem po instalaci je nastavení hardwaru a údajů, které jsou nezbytné pro zavedení rolí serveru. Pro nastavení můžeme použít konzoli pro počáteční konfiguraci, viz obrázek 15, která vyvolá požadovanou konzoli nebo je možné přímo využívat konzole jednotlivých služeb. Další možností konfigurace je využití Ovládacích panelů, Správce serveru, prostředí Windows PowerShell. Windows PowerShell je plně vybavený příkazový řádek, který umožňuje pracovat s integrovanými příkazy (rutiny). [30][24]

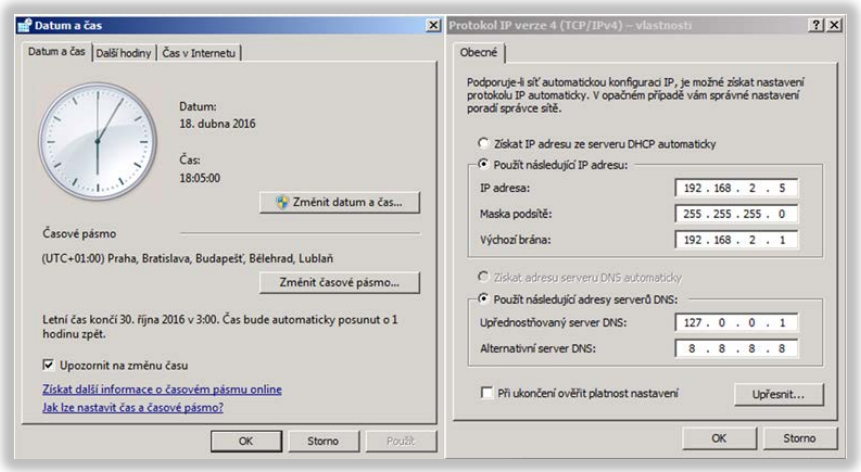


Obrázek 15: Konzole pro počáteční konfiguraci

Zdroj: vlastní zpracování

4.5.1 Nastavení síťového prostředí a časového pásma

Pokud nebylo nutné nastavit síťové prostředí hned po instalaci, tak nyní přišel čas na nastavení. Adresaci nastavujeme podle obrázku 16. Dalším důležitým krokem je zvolení data, času a automatické synchronizace, které je také znázorněno na obrázku 16. Výchozí hodnota, kterou ponecháme pro synchronizaci, je nastavena na hodnotu *time.windows.com*. [24][30]

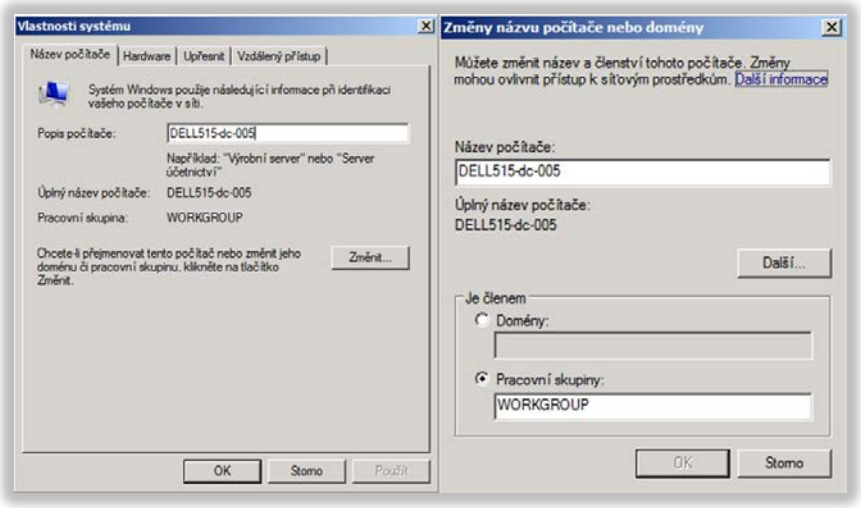


Obrázek 16: Nastavení síťového prostředí a časového pásma

Zdroj: vlastní zpracování

4.5.2 Nastavení názvu a domény

Název serveru je dost důležitý údaj, který musí být jedinečný v naší doménové struktuře a měl by splňovat požadavky na DNS a NetBIOS. Délka názvu by neměla přesáhnout 15 znaků a není doporučené používat hvězdičky, tečky a mezery. Konvence názvů by měla být ucelená pro celou síť. V našem případě je použita následující konvence (název serveru-funkce serveru-poslední oktet IP adresy) *DELL515-dc-005*, který můžeme změnit i po instalaci role AD, viz obrázek 17. Doménu nastavujeme jen v případě, pokud je funkční řadič domény. [24][30]



Obrázek 17: Nastavení názvu a domény

Zdroj: vlastní zpracování

4.5.3 Nastavení aktualizací a odesílání informací

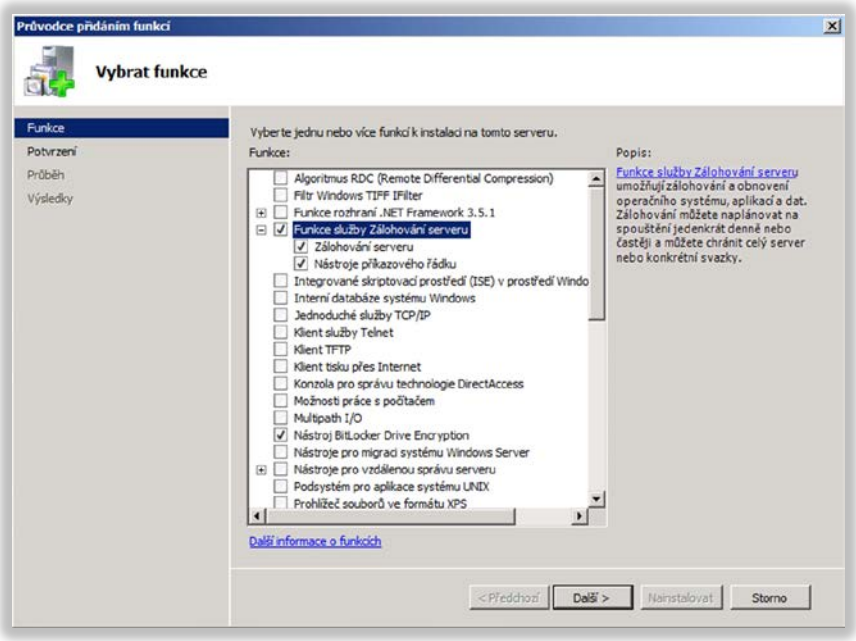
Poslední krok spočívá v nastavení způsobu stahování a instalování aktualizací. Zde jsou tři použitelné možnosti stahování a instalací aktualizací, přičemž jedna je nevhodná. Pro náš účel je příhodná druhá varianta, která povoluje stahovat aktualizace, ale na instalaci aktualizací se dotazuje. Z důvodu dostupnosti není možné použít automatické stahování a instalace, protože po zavedení některých aktualizací je vyžadován restart operačního systému. U služby zasílání zpráv o chybách je ponecháno výchozí nastavení, při kterém je správce dotazován na odeslání hlášení. Poslední nastavení se týká programu na zlepšování služeb, kterého neúčastníme. Postup nastavení je následující *Úlohy počáteční konfigurace → Povolit automatické aktualizace a odesílání vašeho názoru → Ručně konfigurovat nastavení.* Zde provedeme výše uvedené nastavení. [24]

4.6 Instalace funkcí

V této části můžeme přidat požadované funkce serveru. Funkcí rozumíme nějakou funkčnost serveru, při které není požadována instalace role. Jedná se o softwarovou komponentu, která nabízí další funkčnost. Po ukončení instalace funkcí je zobrazen dialog potvrzující správné nainstalování. Funkce lze přidávat a odebírat prostřednictvím konzole Správce serveru nebo Úlohy počáteční konfigurace. Samotný výběr funkcí je patrný z obrázku 18. [24][29]

Instalace požadovaných funkcí

- BitLocker – poskytuje zabezpečení prostřednictvím šifrování dat uložených na discích serveru;
- Zálohování systému Windows (Windows Server Backup) – služba umožňuje zálohovat a obnovovat systém a data. [30][29]



Obrázek 18: Instalace funkcí

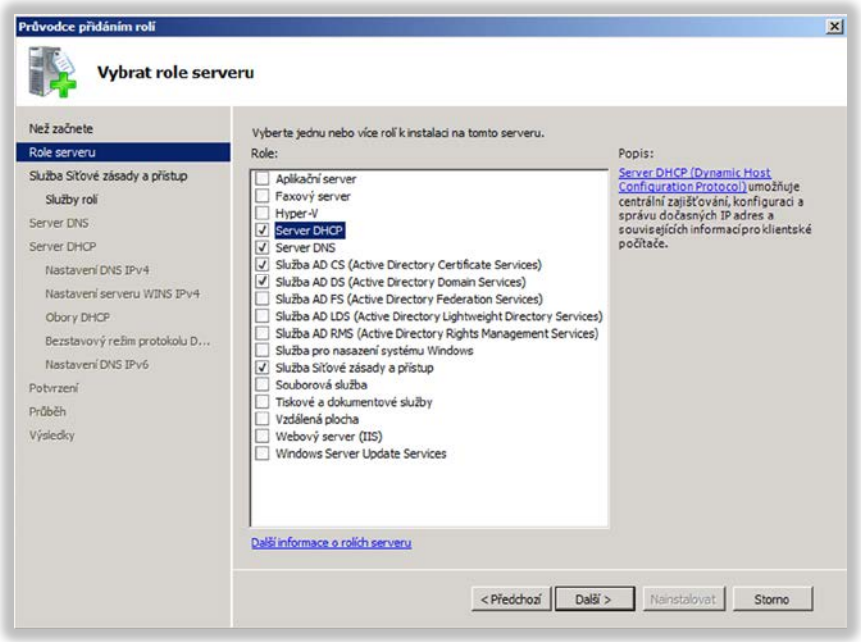
Zdroj: vlastní zpracování

4.7 Instalace rolí

Role u Windows Serveru znamenají soubor funkcí, kterými je definován účel serveru. Každá role obsahuje jednu nebo více služeb rolí. Služba role je konkrétní funkčnost, která slouží pro roli, pro kterou slouží jako služba role. Konzolu pro správu rolí lze aktivovat prostřednictvím konzole Správce serveru nebo Úlohy počáteční konfigurace. Vlastní konzole pro správu rolí je vidět na obrázku 19. [24]

Požadované role

- Active Directory + DNS
  - Domain Services (AD DS) – slouží pro ukládání a zpřístupnění informací o uživatelích, skupinách a dalších objektech v síti;
  - DNS Server – slouží pro překlad názvů na IP a zpět (je automaticky nainstalován při zavedení AD);
- DHCP server – nabízí centrální kontrolu nad adresováním IP;
- Služba síťové zásady a přístup (NPAS – Network Policy and Access Services) – slouží ke správě zabezpečeného přístupu k síti. [24]



Obrázek 19: Instalace rolí

Zdroj: vlastní zpracování

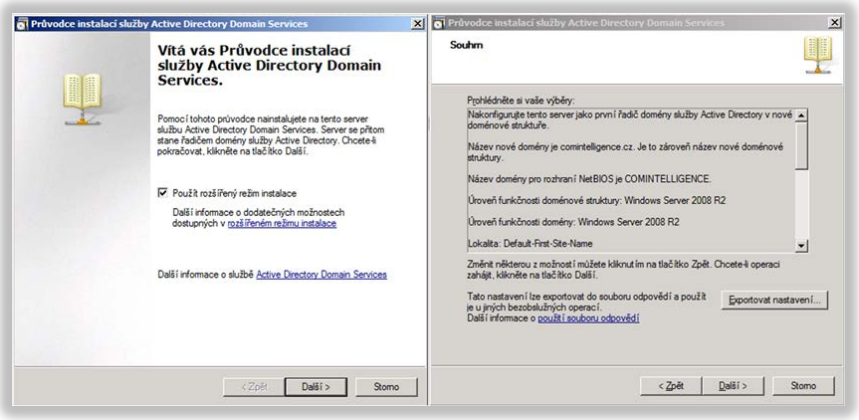
4.8 Instalace a konfigurace adresářových služeb

Po instalaci role Active Directory Domain Services (AD DS) je nutné server nastavit jako první řadič domény. Průvodce nastavením služby Active Directory lze spustit příkazem *dcpromo.exe*. Po otevření okna s průvodcem nastavení pokračujeme podle popisu jednotlivých kroků konfigurace adresářových služeb. [30][24]

Popis jednotlivých kroků konfigurace adresářových služeb

1. v úvodní obrazovce průvodce vybereme hodnotu pro použití rozšířeného režimu instalace podle obrázku 20;
2. informaci o kompatibilitě přejdeme dál;
3. v konfiguraci nastavení vybereme *Vytvoření nové doménové struktury*;

4. do pole plně kvalifikovaného názvu domény zapíšeme *comintelligence.cz*;
5. název domény pro rozhraní NetBIOS ponecháme v předvyplněném stavu *COMINTELLIGENCE*;
6. v úrovni funkčnosti doménové struktury zvolíme *Windows Server 2008 R2*, a to z důvodu zajištění všech funkcí.
7. další možnosti řadiče domény ponecháme v předvoleném nastavení i se serverem DNS;
8. umístění databáze, souborů protokolu a služeb SYSVOL ponecháme ve výchozím nastavení;
9. zadáme silné heslo správce;
10. souhrn nastavení pouze potvrdíme tlačítkem *Další*, viz obrázek 20. [30][24]



Obrázek 20: Instalace služby Active Directory

Zdroj: vlastní zpracování

4.9 Instalace a konfigurace DHCP

Při instalaci role DHCP dochází ke konfiguraci, kterou můžeme později změnit či doplnit. V první části je popsána instalace, v druhé je popsáno nastavení hodnot, které jsou určené pro distribuci prostřednictvím DHCP.

Popis jednotlivých kroků instalace serveru DHCP

1. po označení role serveru pokračujeme tlačítkem *Další*;
2. přeskočíme úvod k serveru DHCP;
3. ve vazbě síťového připojení ponecháme statickou adresu serveru v přednastaveném stavu *192.168.2.5*;
4. nastavení DNS IPv4 ponecháme ve výchozím nastavení nadřazenou doménou pro *comintelligence.cz* a IPv4 pro upřednostňovaný DNS změníme na *192.168.2.5*;
5. server WINS IPv4 není požadován;
6. obory DHCP nastavíme na hodnoty podle tabulky 10;

7. bezstavový režim protokolu DCPv6 ponecháme povolený;
8. nastavení DNS IPv6 ponecháme ve výchozím stavu;
9. ověření serveru DHCP je nutné pro další funkčnost a je nutné použít účet, který má příslušná práva;
10. v potvrzení, kde je i zpráva s požadovaným nastavením potvrdíme instalaci tlačítkem *Nainstalovat*. [30][24]

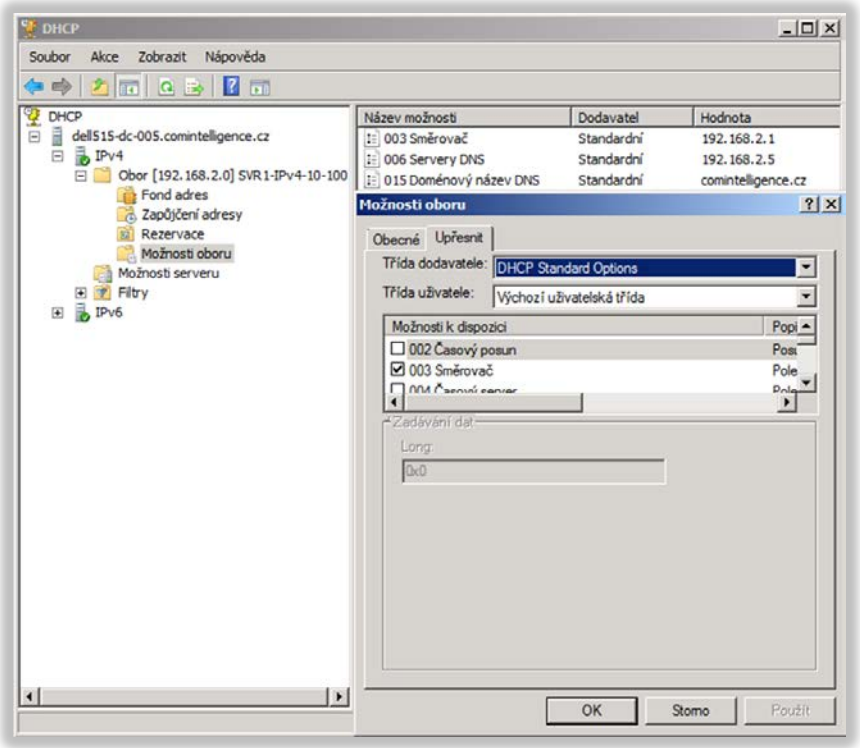
Tabulka 10: Výstup požadovaného nastavení serveru DHCP

Vazby síťového připojení	192.168.2.5 (IPv4)
Nastavení DNS IPv4	
Nadřazená doména DNS	comintelligence.cz
Servery DNS	192.168.2.5
Servery WINS	Žádné
Obory	
Název	SVR1-IPv4-10-100
Výchozí brána	192.168.2.1
Maska podsítě	255.255.255.0
Rozsah IP adres	192.168.2.10 - 192.168.2.100
Typ podsítě	Drátová síť (doba trvání zapůjčení bude 8 dnů)
Aktivovat obor	Ano
Bezstavový režim protokolu DHCPv6	Povoleno
Nastavení DNS IPv6	
Nadřazená doména DNS	comintelligence.cz
Servery DNS	::1
Ověřování serveru DHCP	Autorizace pomocí pověření přidružených k COMINTELLIGENCE\Administrator

Zdroj: vlastní zpracování

Popis konfigurace serveru DHCP

V konzole DHCP musí být nastaveny minimální údaje o službách a síťovém prostředí podle obrázku 21, které server DHCP bude předávat klientům.



Obrázek 21: Nastavení oboru DHCP

Zdroj: vlastní zpracování

4.10 Instalace a konfigurace služby síťových zásad a přístupů

Tato role obsahuje důležitou službu NPS (Network Policy Server), kterou integrujeme do služby DHCP;

Popis jednotlivých kroků instalace služby NPS

1. označíme roli *Služba Síťové zásady a přístup*;
2. úvod do služby potvrdíme tlačítkem *Další*;
3. ve službě rolí označíme *Server NPS (Network Policy Server)*;
4. na obrazovce potvrzení klikneme na *Nainstalovat*.

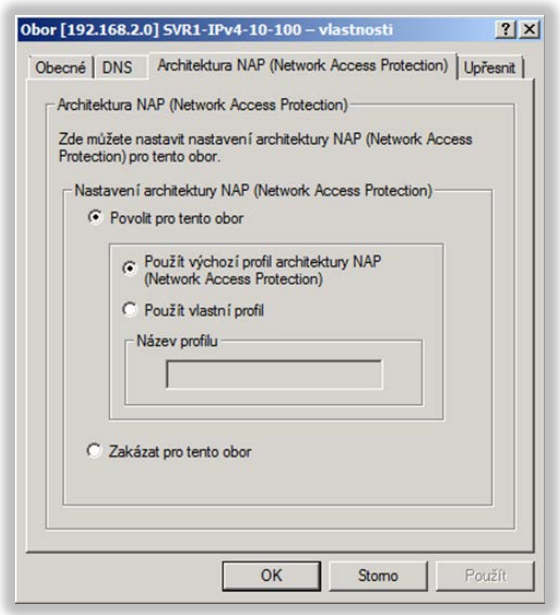
Popis jednotlivých kroků konfigurace služby NPS

1. ve správci serveru rozklikneme *Služba Síťové zásady a přístup → Server NPS (Místní)* a v prostředním okně zvolíme *Konfigurovat architekturu NAP*;
2. nyní musíme vybrat způsob připojení k síti, který je v našem případě DHCP, a proto vybereme v roletovém menu *Pomocí protokolu DHCP*;
3. jelikož je server DHCP provozován na tomto serveru společně s NAP, tak ponecháme pole *Klienti RADIUS* volné;
4. aplikování zásad požadujeme pro všechny obory DHCP, proto necháme pole *Obory DHCP* volné;

5. *Skupiny počítačů* opět ponecháme volné, protože požadujeme platnost zásad pro všechny;
6. jelikož nemáme nápravné servery, které ukládají aktualizace softwaru pro klienty NAP v případě potřeby, pole ponecháme ve výchozím stavu *Žádné*;
7. v okně *Definovat zásadu stavu architektury NAP* ponecháme označený *Validátor stavu zabezpečení systému Windows* a *Odepřít klientským počítačům neumožňujícím architekturu NAP úplný přístup k síti a povolit pouze přístup k síti s omezením*;
8. v posledním okně jsou uvedeny námi předvolené zásady, které potvrdíme tlačítkem *Dokončit*. [30][29]

4.10.1 Konfigurace DHCP pro použití NAP

Cílem této konfigurace je nastavení architektury NAP pro vytvořený obor serveru DHCP. Architekturu lze nastavovat pro každý obor DHCP zvlášť nebo globálně pro celé DHCP. Nastavení provedeme ve vlastnostech oboru, viz obrázek 22. [30]



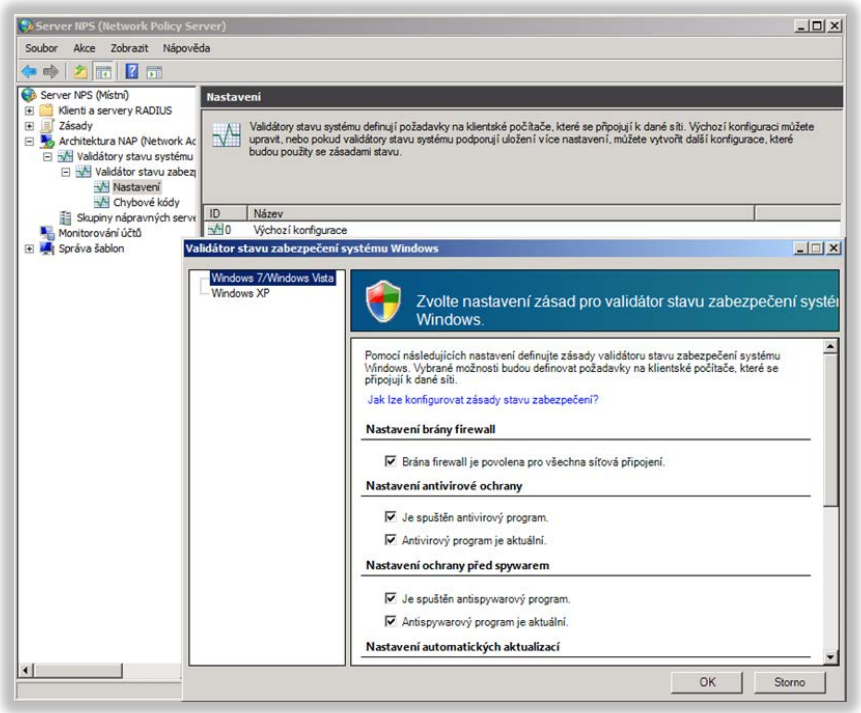
Obrázek 22: Nastavení oboru DHCP pro NAP

Zdroj: vlastní zpracování

4.10.2 Určení zásad stavů

Cílem předchozího nastavení je povolit klientům pouze přístup k síti s omezením, pokud nesplňují určité podmínky. Tyto podmínky nyní nastavíme pro OS Windows 7 a XP ve validátoru stavu sítě. Toto nastavení provedeme v konzole *Server NPS → Architektura NAP → Validátor stavu zabezpečení → Nastavení* v pravém okně zvolíme vlastnosti konfigurace *Výchozí konfigurace* a zaškrtneme všechny volby kromě *Windows Server Update Services*.

Typ požadovaných aktualizací nastavíme na *Důležité a vyšší* s časovou prodlevou posledního vyhledání aktualizací *72 hodin*. Část nastavení je vidět na obrázku 23. [24]



Obrázek 23: Validátor stavu zabezpečení systému Windows

Zdroj: vlastní zpracování

4.11 Implementace zabezpečení diskových oddílů serveru

BitLocker slouží k zašifrování disku za pomoci či bez TPM (Trusted Platform Module Management) čipu. Při spuštění operačního systému je schopný ověřit, zdali bylo s disky manipulováno. V případě podezřelé změny, kterou tato služba může zjistit z diagnostiky spouštěcích a systémových souborů a šifrovaných svazků, zakáže uvolnění klíče a normálního spuštění operačního systému. V případě restrikce je systém spuštěn v režimu obnovení (Recovery mode). Pro spuštění této služby bez čipu TPM je využívána například klíčenka USB, po příslušném nastavení objektu zásad.

Popis jednotlivých kroků konfigurace služby BitLockeru

1. v ovládacích panelech vybereme položku *Nástroj BitLocker Drive Encryption*;
2. u požadovaného disku vybereme *Zapnout nástroj Bitlockeru*, viz obrázek 24;
3. klikneme na volbu *Pokračovat v šifrování …;*
4. na kartě *Uložit heslo pro obnovení* provedeme uložení hesla na USB disk a vytištění;
5. v tomto kroku provedeme kontrolu označení volby *Spustit kontrolu systému nástroje BitLocker*;

6. po restartování a přihlášení k serveru pod stejným uživatelským se šifrování samo spustí. [30][24]

Obrázek 24: Nastavení funkce BitLocker

Zdroj: vlastní zpracování

4.12 Nastavení zásad skupin

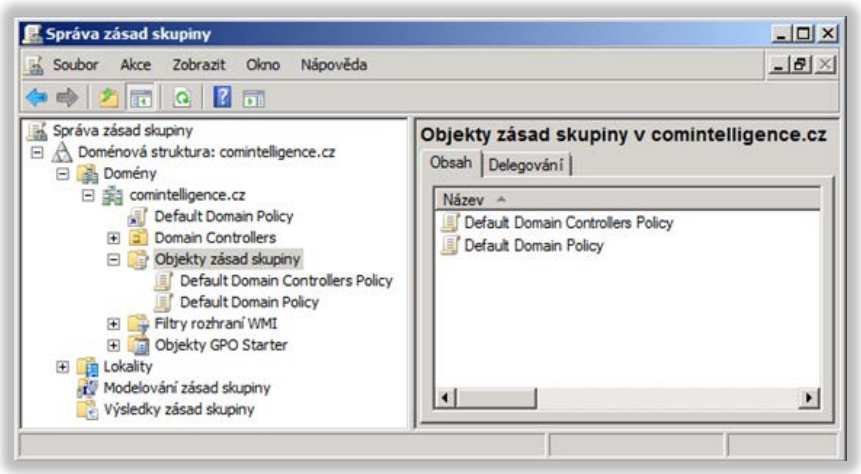
Zásady skupin nám slouží k centralizovanému nastavení uživatelů a počítačů ve službě AD DS. Pomáhá nám automatizovat klíčové úkoly správy s cílem zvýšit produktivitu správců, uživatelů, a také zvýšit bezpečnost jak koncových zařízení, tak celé domény. Nastavení zásad je ukládáno do Objektu zásad skupin (GPO). U počítačů je prostřednictvím zásad nastavováno zabezpečení, nastavení aplikací, přiřazení aplikací a spouštění skriptů a spouštění skriptů při vypnutí počítače. U uživatelů jsou nastavované vlastnosti týkající se nastavení aplikací, přesměrování složek, přiřazení a publikování aplikací, přihlašovacích a odhlašovacích skriptů uživatelů a nastavení zabezpečení. U nastavení zásad můžeme využít dědění, což znamená přebírání nastavení z nadřízených kontejnerů anebo potlačení dědění. Explicitně udělené oprávnění má přednost před zděděným, dokonce i při volbě odepřít. Pořadí implementace zásad skupin je v následujícím pořadí. [30][24][29]

Pořadí implementace

1. místní GPO;
2. GPO sítě;
3. GPO domény;
4. GPO organizační jednotky;
5. GPO podřízené organizační jednotky. [24][29]

4.12.1 Nastavení dílčích zásad skupin

Při tvorbě zásad by mělo být co nejméně zasahováno do zásad *Default Domain Policy* a *Default Domain Controllers Policy*. V zásadách domény se nastavují zejména zásady účtů a aplikace na řadičích, které vyžadují změnu zásad auditu. Zásady je vhodné rozdělit po logických celcích. Objekty GPO jsou nastavována prostřednictvím konzole *Správa zásad skupiny*, viz obrázek 25. Jednotlivé GPO nastavujeme v konzole *Ovládací panely → Nástroje pro správu → Správa zásad skupin → výběr dané zásady*. [30][24]



Obrázek 25: Konzola správa zásad skupin

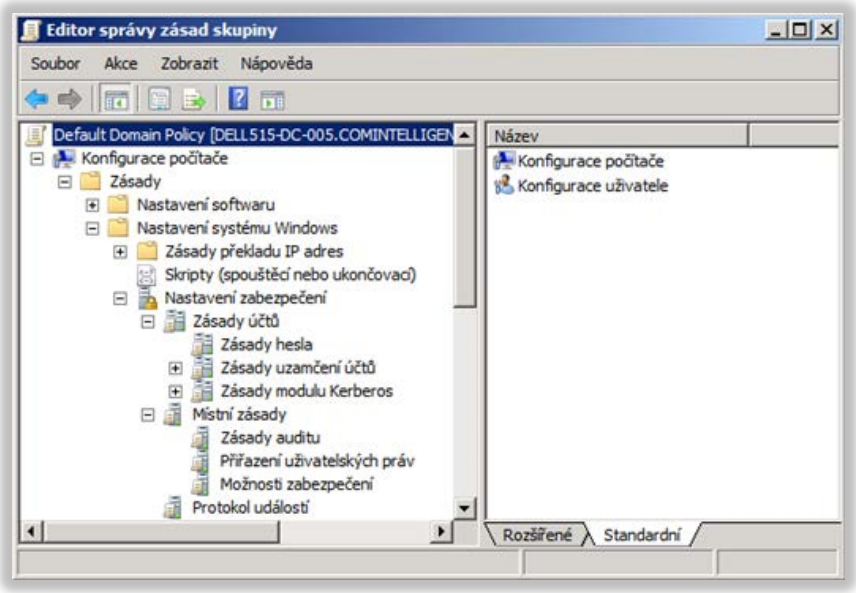
Zdroj: vlastní zpracování

Popis kroků nastavení základních požadavků na zásady účtů

1. ve správci zásad nalezneme *Objekty zásad skupiny* podle obrázku 25;
2. pravým tlačítkem myši klikneme na *Default Domain Policy* a vybereme *Upravit*;
3. v konzole *Editor správy zásad skupiny*, který je vidět na obrázku 26, vybereme příslušnou zásadu podle tabulky 11. [30][24]

Popis kroků nastavení základních požadavků na zásady auditů

1. ve správci zásad nalezneme *Objekty zásad skupiny* podle obrázku 25;
2. pravým tlačítkem myši klikneme na *Default Domain Policy* a vybereme *Upravit*;
3. v konzole *Editor správy zásad skupiny* vybereme příslušnou zásadu podle tabulky 12, obdobně jako na obrázku 26. [30][24]



Obrázek 26: Editor správy zásad skupiny

Zdroj: vlastní zpracování

Tabulka 11: Nastavení objektů zásad pro doménu

Default Domain Policy	
Konfigurace počítače → Zásady → Nastavení systému Windows → Nastavení zabezpečení → Zásady účtů	
Zásady hesla	
Heslo musí splňovat požadavky na složitost	Povoleno
Maximální stáří hesla	90 dnů
Minimální délka hesla	12 znaků
Minimální stáří hesla	1 den
Ukládat hesla pomocí reverzibilního šifrování	Zakázáno
Vynutit použití historie hesel	24 hesel pamatováno
Zásady uzamčení účtů	
Doba uzamčení účtu	0 (dokud jej správce neodemkne)
Prahová hodnota pro uzamčení účtu	3 chybných pokusů o přihlášení
Vynulovat čítač uzamčení účtu po	99999min (hodnota má význam při zadání nastavení hodnoty pro uzamčení účtu)

Zdroj: vlastní zpracování

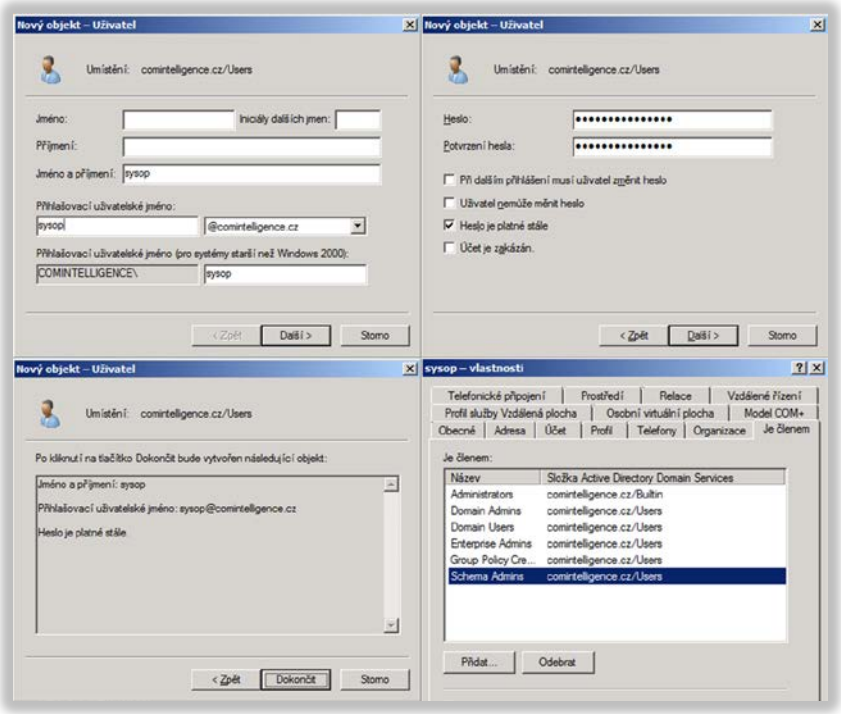
Tabulka 12: Nastavení objektů zásad pro řadiče domény

Default Domain Controllers Policy	
Konfigurace počítače → Zásady → Nastavení systému Windows → Nastavení zabezpečení → Místní zásady	
Zásady auditu	
Auditovat přístup k adresářové službě	Úspěšné a Neúspěšné
Auditovat správu účtů	Úspěšné a Neúspěšné
Auditovat systémové události	Úspěšné a Neúspěšné
Auditovat události přihlášení	Úspěšné a Neúspěšné
Auditovat změny zásad	Úspěšné a Neúspěšné
Protokol událostí	
Doba uchování aplikačního protokolu	30 dnů
Doba uchování protokolu zabezpečení	30 dnů
Doba uchování systémového protokolu	30 dnů
Maximální velikost aplikačního protokolu	40064 KB
Maximální velikost protokolu zabezpečení	150016 KB
Maximální velikost systémového protokolu	60032 KB
Metoda uchovávání aplikačního protokolu	Podle dnů
Metoda uchovávání protokolu zabezpečení	Podle dnů
Metoda uchovávání systémového protokolu	Podle dnů

Zdroj: vlastní zpracování

4.13 Zakázání předdefinovaných účtů

Na konci konfigurace je nutné zakázat zabudované účty správce a hosta. Toto nastavení provedeme v konzole pro správu účtů. Před nastavením daného objektu zásad je nutné vytvořit nový účet správce podle následujícího postupu: *Ovládací panely → Uživatelé a počítače služby Active Directory → comintelligence.cz → Users.* V levém okně klikneme pravým tlačítkem myši a vybereme *Nová položka → Uživatel.* Dále pokračujeme podle obrázku 27, včetně zařazení účtu do skupin s vyššími právy. Po vytvoření účtu nového správce klikneme pravým tlačítkem na účet administrátora a vybereme volbu *Zakázat účet*. Tímto způsobem přidáváme a zakazujeme také běžné uživatele. [24]



Obrázek 27: Editor správy zásad skupiny

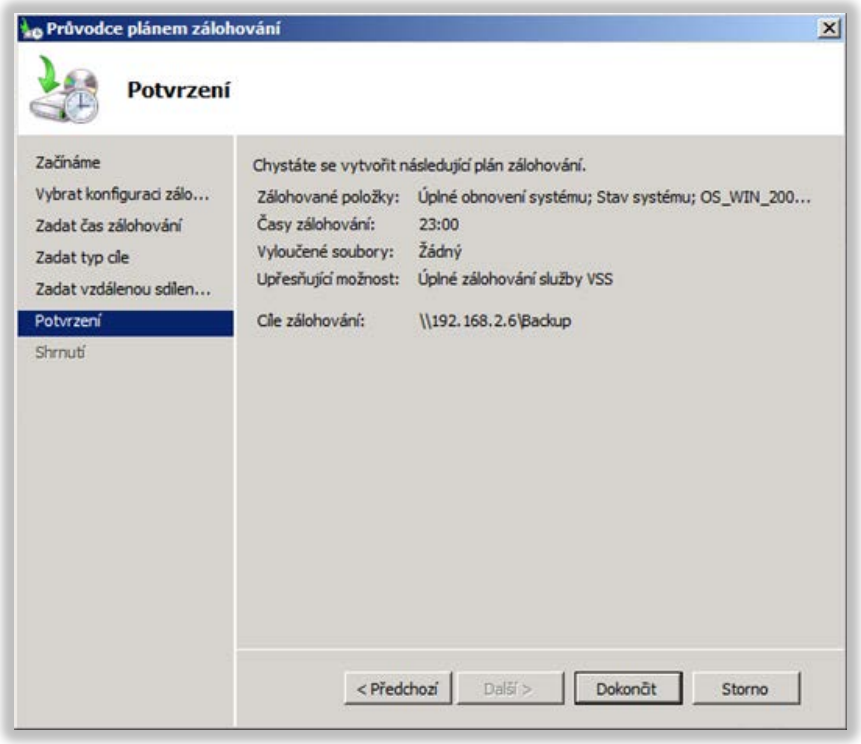
Zdroj: vlastní zpracování

4.14 Zálohování serveru

Posledním krokem je vytvoření automatických záloh serveru. Zálohování serveru zabezpečuje *Funkce služby Zálohování serveru*. Po nainstalování této funkce provedeme konfiguraci automatické zálohy celého serveru.

Popis kroků nastavení základních požadavků na zásady účtů

1. Spustíme funkci zálohování serveru *Nástroje pro správu* → *Ovládací panely* → *Zálohování serveru*;
2. V pravém okně vybereme *Plán zálohování…*;
3. V průvodci první okno potvrdíme tlačítkem *Další*;
4. V okně *Vybrat konfiguraci zálohování* označíme *Celý server* a potvrdíme tlačítkem *Další*;
5. Nyní zadáme čas denního zálohování na 23:00 hod;
6. V části *Zadat typ cíle* vybereme *Zálohovat do sdílené složky* a potvrdíme tlačítkem *Další*;
7. Nyní zadáme vzdálenou adresu sdílené složky ve tvaru *\\192.168.2.6\Backup*;
8. Po potvrzení jsme vyzváni k zadání účtu, který má právo zápisu do sdílené složky, a také k provedení zálohy na serveru v podobě *comintelligence.cz\sysop*;
9. V předposledním okně je uvedeno požadované nastavení zálohování, které potvrdíme tlačítkem *Dokončit*, viz obrázek 28. [24]



Obrázek 28: Nastavení zálohování serveru

Zdroj: vlastní zpracování

4.15 Vyhodnocení

Nastavení serverového operačního systému v kapitole 4 můžeme považovat za lehký úvod do problematiky implementace bezpečnostních prvků počítačové bezpečnosti v doménovém prostředí. Ukázka nastavení Windows Server 2008 R2, je pouze demonstrací schopností operačních systémů od firmy Microsoft. V průběhu dalšího konfigurování doménové politiky by byly nastaveny firewally, certifikační služby, VPN přístupy apod. Postupy nastavení existují ve formě standardních a individuálních metod. Standardní postupy jsou uceleně popsané v odborné literatuře k danému SW produktu. Individuální metody jsou výsledkem kreativního přístupu administrátora, který řeší nepopsané činnosti jak operačního systému, tak uživatelů. V případě aplikování těchto metod je nutné vést podrobnou dokumentaci těchto nastavení. V této ukázce byly použity standardní metody popsané v odborné literatuře.

ZÁVĚR

Cílem této práce bylo prostudovat, popsat a vysvětlit bezpečnost v oblasti ochrany dat v síťovém prostředí a vytvoření praktické ukázky nastavení zabezpečení serverového OS Windows jako řadiče domény s Active Directory.

V části historie byla popsána problematika sítí, kryptologie a počítačových sítí. Historie je vždy základním kamenem pro pochopení problematiky a nelze ji opomíjet. Podstatná část textu se týká Internetu, jako největší hrozby vzhledem k ochraně dat, hardwaru a sítí.

V další kapitole byla objasněna problematika topologií, standardů, protokolů a druhů sítí, která je podstatná pro plánování bezpečnosti jak síťové, tak i celého informačního systému. Podstatné je rozeznávat logickou a fyzickou topologii, která vždy nemusí být stejná. Každý administrátor či správce sítě nebo informačního systému by se měl orientovat v této problematice, protože stavět doménové prostředí nebo celý informačního systém na nezmapovaném či nepochopeném síťovém prostředí, převážně vede k následným fatálním problémům a obtížnému docílení kvalitního zabezpečení.

Kapitola bezpečnosti sítí a ochrany dat lehce popisuje problematiku správného zabezpečení. Z textu je zřejmé, že u větších informačních systémů se neobejdeme bez standardizované dokumentace. Bezpečnostní politika je hlavním z nich a měla by obsahovat popis subjektu, podstatné části určující povinnosti uživatelů a administrátorů informačního systému, popis ochrany aktiv a hrozící nebezpečí. Havarijní plány lze považovat za samostatný dokument, který obsahuje souhrn krizových opatření a postupů stanovených k řešení krizových situací. V dané kapitole byly postány druhy známých útoků, škodlivých programových kódů a ochran proti nim. V oblasti informatiky je to podobné jako u virů v přírodě. Na každý bezpečnostní problém se snažíme vyvinout účinnou ochranu, která je následně prolomena nebo vytvořena jiná bezpečnostní hrozba. U virových organismů se snažíme vyvíjet vakcíny, které jsou v některých případech účinné do doby mutace viru. Rovněž vznikají nové formy těchto virů. Tento cyklus ochrany a útoků je nekonečný koloběh vývoje ochranných prostředků.

Praktická část této práce měla ukázat nastavení operačního systému MS Windows 2008 R2 jako řadiče domény s Active Directory. Problematika nastavení byla realizována podle požadavku hypotetické firmy. Prvky bezpečnosti byly nastaveny minimálně, s cílem ukázat možnosti tohoto serverového produktu, které lze dále rozšiřovat podle požadavků. Produkty firmy Microsoft mají poměrně precizně vytvořené grafické rozhraní pro nastavení bezpečného prostředí, jak v oblasti samostatných počítačů, tak i v oblasti síťového a doménového prostředí.

Závěrem je nutné poukázat na skutečnost, že většina provozovatelů sítí a informačních systémů preferuje levnější variantu zabezpečení, aniž by si uvědomovali, že únik informací či jejich destrukce může poškodit jejich ekonomickou a funkční stabilitu.

POUŽITÁ LITERATURA

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

[2] Brief History of the Internet. Internet Society [online]. 2016 [cit. 2016-03-14]. Dostupné z: http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet#Origins

[3] BUCHALCEVOVÁ, Alena. Metodiky budování informačních systémů. Vyd. 1. Praha: Oeconomica, 2009. ISBN 978-80-245-1540-3.

[4] Crypto-world.info [online]. Pavel Vondruška, 2013 [cit. http://crypto-world.info]. Dostupné z: http://crypto-world.info/

[5] DELL: Rackový server PowerEdge R515 s výškou 2U | Dell. DELL [online]. 2016 [cit. 2016-04-16]. Dostupné z: http://www.dell.com/cz/domacnosti/p/poweredge-r515/pd

[6] DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Vyd. 1. Brno: Computer Press, 2004, 190 s. ISBN 80-251-0106-1

[7] DOSEDLA, Martin. Základy výpočetní techniky [online]. Pedagogická fakulta Masarykovy univerzity: Katedra technické a informační výchovy, 2007 [cit. 2016-03-27]. Dostupné z: http://www.ped.muni.cz/wtech/elearning/zvt.pdf

[8] EDITOR, Burton Rosenberg. Handbook of financial cryptography and security [online]. Boca Raton: Chapman, 2010 [cit. 2016-03-14]. ISBN 978-142-0059-823. Dostupné z: https://books.google.cz/books?id=_d7RUNF-2tcC&pg=PR19&lpg=PR19&dq=http://crypto-world.info/+%22Trithemius%22+steganographia&source=bl&ots=ezKetKda9L&sig=I67waIRS9OjCGhwjiLs_aMqEKwE&hl=cs&sa=X&ved=0ahUKEwi8iMuIvsDLAhXENpoKHQM-CLkQ6AEIOTAE#v=onepage&q=http%3A%2F%2Fcrypto-world.info%2F%20%22Trithemius%22%20steganographia&f=false

[9] Historie kryptografie. WIKIPEDIE: Otevřená encyklopedie [online]. [cit. 2016-03-13]. Dostupné z: https://cs.wikipedia.org/wiki/Historie_kryptografie

[10] Historie poštovnictví. JABLKO poznání [online]. [cit. 2016-03-13]. Dostupné z: http://www.jablko.cz/Zajimavosti/Udalosti/Zajim_udalo_2.htm

[11] HORÁK, Jaroslav a Milan KERŠLÁGER. Počítačové sítě pro začínající správce. 3., aktualiz. vyd. Brno: Computer Press, 2006, 211 s. ISBN 80-251-0892-9.

[12] HUB, Miloslav. Bezpečnost a ochrana informací v prostředí internetu. Vyd. 1. Pardubice: Univerzita Pardubice, 2013, 89 s. ISBN 978-80-7395-701-8.

[13] IKAROS: Informačné systémy a škodlivé kódy od A po Z. IKAROS: elektronický časopis o informační společnosti [online]. 2007 [cit. 2016-04-09]. Dostupné z: http://ikaros.cz/informacne-systemy-a-skodlive-kody-od-a-po-z

[14] Internet History. Living Internet [online]. 2015 [cit. 2016-03-14]. Dostupné z: http://www.livinginternet.com/i/ii.htm

[15] Internet World Stats: World Stats. Internet World Stats [online]. ©2001-2016 [cit. 2016-03-16]. Dostupné z: http://www.internetworldstats.com/stats.htm

[16] Jak na Internet: Historie Internetu. CZ.NIC [online]. CZ.NIC, z. s. p. o., ©2012-2014 [cit. 2016-03-16]. Dostupné z: http://www.jaknainternet.cz/page/1205/historie-internetu

[17] JAŠEK, Roman. Informační a datová bezpečnost. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006. ISBN 80-731-8456-7.

[18] Krátce z historie Internetu. Masarykova univerzita: Ústav výpočetní techniky [online]. [cit. 2016-03-14]. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/22.html

[19] NÝVLT, Marek. Počítačové sítě [online]. In: . s. 119 [cit. 2016-03-13]. Dostupné z: http://www.clatrutnov.cz/index.php/ke-stazeni/category/10-stredni-skola?download=47%3Apocitacove-site

[20] ODOM, Wendell. Počítačové sítě bez předchozích znalostí. Vyd. 1. Brno: CP Books, 2005, 383 s. ISBN 80-251-0538-5.

[21] PALATINUS, Lukáš. Topologie sítí. PALATINUS, Lukáš. BANAN.CZ: WEBHOSTING [online]. 2014 [cit. 2016-03-28]. Dostupné z: http://blog.banan.cz/Internet/Topologie-siti

[22] RAID. WikipediE: Otevřená Encyklopedie [online]. [cit. 2016-04-16]. Dostupné z: https://cs.wikipedia.org/wiki/RAID#Popul.C3.A1rn.C3.AD_typy_RAID

[23] RUKOVANSKÝ, Imrich. Počítačové sítě. Kunovice: Evropský polytechnický institut, 2011. ISBN 978-80-7314-231-5.

[24] RUSSEL, Charlie a Sharon CRAWFORD. Microsoft Windows Server 2008: velký průvodce administrátora. Vyd. 1. Brno: Computer Press, 2009. Administrace (Computer Press). ISBN 978-80-251-2115-3.

[25] SATRAPA, Pavel. IPv6: internetový protokol verze 6. 3., aktualiz. a dopl. vyd. Praha: CZ.NIC, c2011. CZ.NIC. ISBN 978-80-904248-4-5.

[26] Sítě typu Peer-to-peer vs. sítě založené na serveru. Microsoft: Microsoft Developer Network[online]. 2016 [cit. 2016-03-28]. Dostupné z: https://msdn.microsoft.com/cs-cz/library/cc527483(v=ws.10).aspx

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

[28] SPORTACK, Mark A. Směrování v sítích IP: [autorizovaný výukový průvodce : samostudium : kompletní zdroj informací o směrování a protokolech v sítích IP]. Vyd. 1. Brno: Computer Press, 2004. Cisco systems. ISBN 80-251-0127-4.

[29] STANEK, William R. Microsoft Windows Server 2008: kapesní rádce administrátora. Vyd. 1. Brno: Computer Press, 2008. Knihovnička administrátora (Computer Press). ISBN 978-80-251-1936-5.

[30] STANEK, William R. Mistrovství v Microsoft Windows Server 2008: [kompletní informační zdroj pro profesionály]. Vyd. 1. Brno: Computer Press, 2009. ISBN 978-80-251-2158-0.

[31] Telegrafie. WIKIPEDIE: Otevřená encyklopedie [online]. [cit. 2016-03-13]. Dostupné z: https://cs.wikipedia.org/wiki/Telegrafie

[32] The World Wide Web (WWW). Living Internet [online]. 2015 [cit. 2016-03-16]. Dostupné z: http://www.livinginternet.com/w/w.htm

[33] TVRDÍKOVÁ, Milena. Aplikace moderních informačních technologií v řízení firmy: nástroje ke zvyšování kvality informačních systémů. 1. vyd. Praha: Grada, 2008. Management v informační společnosti. ISBN 978-80-247-2728-8.

[34] Typy sítí. EStránky.cz [online]. 2014 [cit. 2016-03-27]. Dostupné z: http://www.pcsit.estranky.cz/clanky/typy-siti/

[35] Vzájemné propojování sítí - I. PETERKA, Jiří. EArchiv.cz: Archiv článků a přednášek Jiřího Peterky [online]. 2011 [cit. 2015-06-01]. Dostupné z: http://www.earchiv.cz/a92/a228c110.php3

[36] WHITMAN, Michael E a Herbert J MATTORD. Principles of information security. 4th ed. Boston, MA: Course Technology, c2012. ISBN 978-1-111-13821-9.

[37] Zajímavosti: Pošta - telegraf - poslové. Světový tisk [online]. [cit. 2016-03-13]. Dostupné z: http://www.thunder-bolt.cz/zajimavosti/0-obsah.html