Metodiky zabezpečení operačního systému Microsoft Windows

Methodology of the Microsoft Windows operating system security

Bc. Lucie Pivničková

Diplomová práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

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

Jméno a příjmení:	**Bc. Lucie PIVNIČKOVÁ**
Osobní číslo:	**A08467**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Metodika zabezpečení operačního systému Microsoft Windows.**

Zásady pro vypracování:

1. **Vypracujte literární rešerši na zadané téma.**
2. **Navrhněte lokální a síťové zabezpečení OS Microsoft Windows 7. Popište hrozící rizika a obranu proti nim.**
3. **Vytvořte sadu doporučení a postupů zabezpečení daného OS. Jako výchozí konfiguraci uvažujte počítač s běžnou konfigurací.**
4. **Aplikujte navržená doporučení na operační systém Windows 7 v síťovém prostředí s využitím Active Directory. Použijte server Windows Server 2008 R2.**
5. **Prakticky otestujte navržené řešení.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **SMITH, Ben, KOMAR, Brian. Zabezpečení systému a sítě : Microsoft Windows. Brno : Computer Press, a.s., 2006. 700 s. ISBN 80-251-1260-8.**
2. **BOTT, Ed, SIECHERT, Carl. Mistrovství v zabezpečení Microsoft Windows 2000 a XP. Brno : Computer Press, 2004. 696 s. ISBN 80-7226-878-3.**
3. **MOSKOWITZ, Jeremy. Zásady skupiny profily a IntelliMirror : ve Windows 2000, 2003 a XP . Brno : Computer Press, a. s., 2005. 524 s. ISBN 80-251-0806-6.**
4. **MCCLURE, Stuart, SCAMBRAY, Joel, KURTZ, George. Hacking bez tajemství. Brno : Computer Press, a.s, 2003. 632 s. ISBN 80-722-6948-8.**
5. **HOWARD, Michael, LEBLANC, David. Bezpečný kód. Brno : Computer Press, a.s., 2008. 888 s. ISBN 978-80-251-2050-7.**
6. **TULLOCH, Mitch, NORTHRUP, Tony, HONEYCUTT, Jerry. Microsoft Windows Vista : Resource Kit. Brno : Computer Press, a.s., 2008. 1432 s. ISBN 978-80-251-1990-7.**
7. **Microsoft [online]. 2010 [cit. 2010-01-31]. Dostupný z WWW: www.microsoft.com/cs/cz/.**

Vedoucí diplomové práce: **doc. Ing. Martin Sysel, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání diplomové práce: **19. února 2010**

Termín odevzdání diplomové práce: **8. června 2010**

Ve Zlíně dne 19. února 2010

prof. Ing. Vladimír Vašek, CSc.
děkan

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

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

ABSTRAKT

Tato diplomová práce ukazuje metodiky zabezpečení, které jsou aplikovány na v současnosti nejnovější operační systémy firmy Microsoft. Konkrétně se jedná o systémy Windows Server 2008 R2, Standard Edition a Windows 7, Professional.

V jednotlivých částech diplomové práce jsou popsány služby, které jsou obsaženy ve Windows Server 2008 R2 a v praxi jsou často využívané. Jedná se především o služby ADDS (Active Directory Domain Services), ADCS (Active Directory Certificate Services), DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), Remote Desktop Services (dříve označována jako Terminálová služba) a v neposlední řadě NAP (Network Access Protection). Všechny zmiňované služby jsou instalovány a využívány s ohledem na bezpečnost, k jejíž aplikaci je využit převážně nástroj GPMC (Group Policy Management Console), který slouží pro správu zásad skupiny v prostředí Active Directory. Proto, aby bylo zabezpečení kompletní, je nutné, aby klienti využívající služeb serveru splňovali bezpečnostní podmínky k přístupu na daný server, to je mimo jiné také aplikováno prostřednictvím zásad skupiny.

V praktické části práce jsou formou podrobných postupů ukázána vhodná nastavení jednotlivých služeb a zásad zabezpečení při tvorbě jednoduché, ale zabezpečené počítačové sítě s operačními systémy Microsoft Windows.

Klíčová slova: Windows Server 2008 R2, Windows 7, metodiky zabezpečení, ADDS, ADCS, DNS, DHCP, Remote Desktop Services, NAP, zásady skupiny, GPMC

ABSTRACT

This diploma thesis shows the available methods for securing computer systems and their application in Microsoft Windows systems. Specifically, the Windows Server 2008 R2, Standard Edition, and Windows 7 Professional were used which are currently the latest operation systems released by Microsoft Corporation. The thesis describes the services included (and therefore widely used) in default configuration of Windows Server 2008 R2 and focuses on these services: ADDS (Active Directory Domain Services), ADCS (Active Directory Certificate Services), DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), Remote Desktop Services (formerly known as Terminal Services) and also the NAP (Network Access Protection). All these services are installed and used with regard to safety. This thesis also presents GPMC (Group Policy Management Console), which is used to manage Group Policy in Active Directory environment.

In order to ensure complete security, it is necessary that the clients using the server services meet the security requirements for accessing this server. This is ensured by applying Group Policy.

In the practical part of this work the appropriate settings for each service and security policies are illustrated in the form of detailed step-by-step instructions to create a simple but secure computer network with Microsoft Windows operating systems.

Keywords: Windows Server 2008 R2, Windows 7, security methodologies, ADDS, ADCS, DNS, DHCP, Remote Desktop Services, NAP, group policy, GPMC

Děkuji vedoucímu práce doc. Ing. Martinu Syslovi, Ph.D. za odborné vedení a pomoc v průběhu řešení této práce.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracovala samostatně a použitou literaturu jsem citovala. V případě publikace výsledků budu uvedena jako spoluautorka.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Společnost Microsoft již řadu let vyvíjí serverové operační systémy (označované Microsoft Windows Server) a klientské operační systémy (označované Microsoft Windows), které jsou celosvětově velmi populární a právě díky tomu jsou také lákavým cílem útočníků. Společnost Microsoft klade na bezpečnost veliký důraz a své produkty podrobuje řadě změn, které zvyšují jejich bezpečnost. Nejnovějšími produkty z řad operačních systémů společnosti Microsoft jsou nyní Windows Server 2008 R2 a Windows 7, jež obsahují novinky a vylepšení na poli bezpečnosti a při správném použití se dá tvrdit, že jsou bezpečnější než jejich předchůdci. Bohužel však stále existují bezpečnostní problémy, proti nimž neexistuje stoprocentní ochrana. Jejich definici v roce 2000 publikoval Scott Culp ze společnosti Microsoft v soupisu deseti neměnných zákonů zabezpečení (10 Immutable Laws of Security).

Myšlenkou této diplomové práce je nejen popsat možná rizika plynoucí z nedostatečně zabezpečeného počítače, ale hlavně nabídnout ucelený postup zabezpečení operačních systémů Windows Server 2008 R2 a Windows 7.

V diplomové práci je uvažována modelová situace, kdy je třeba připravit jednoduchou počítačovou síť s jedním serverem a dvěma klientskými počítači. V této modelové situaci máme k dispozici tři počítače. Jeden (server), na němž je nainstalován Windows Server 2008 R2, Standard Edition, který bude sloužit jako řadič domény a dva klientské počítače, na nichž se nachází Windows 7, Professional. Všechny počítače mají po instalaci výchozí konfiguraci a z té bude tato práce vycházet. Server obsahuje dvě síťové karty, jedna je využívána výhradně pro komunikaci v lokální síti a druhá umožňuje přístup k síti internet.

Tato diplomová práce popisuje jak instalovat a plně využívat služeb obsažených ve Windows Serveru 2008 R2, jež jsou v praxi hojně využívané s ohledem na bezpečnost serveru samotného i klientů využívajících daných služeb. Práce ukazuje jak využít službu Active Directory Domain Services, která slouží k usnadnění centralizované správy a aplikaci zabezpečení pomocí zásad skupiny.

I. TEORETICKÁ ČÁST

1 BEZPEČNOSTNÍ HROZBY

V roce 1995, když byl Internet ještě ve svém raném stádiu, vůdčí referenční autorita v oblasti počítačové bezpečnosti, Koordinační centrum CERT, ohlásilo nalezení 171 zranitelných míst, které mohli zloději a vandalové využít k útokům na nejčastěji používané operační systémy a aplikace. V roce 2000 počet nově objevených zranitelných míst vzrostl na 1090 a v roce 2001 celkový počet vyskočil na více než 2500, z nichž 37 závad bylo považováno za natolik závažné, že vedly ke zveřejnění oficiálních bezpečnostních výstrah.[2]

Počet nových zranitelných míst v operačních systémech stále narůstá, neboť každý nový operační systém sebou přináší i přes řadu vylepšení a novinek slabá místa, která mohou být zneužívána útočníky. V současné době jsou osobní počítače nedílnou součástí života a počítačová gramotnost patří téměř k základním lidským dovednostem, díky tomu také vzrůstají potencionální škody.

Operační systémy společnosti Microsoft patří k nejpopulárnějším operačním systémům a díky tomu jsou také lákavým cílem útočníků. V nedávné době společnost přišla s novými operačními systémy, kterými se zabývá tato diplomová práce a to Windows Server 2008 R2 a Windows 7. I přesto, že tyto operační systémy obsahují řadu vylepšení a z hlediska spolehlivosti a výkonu patří k nejlepším na trhu, již v průběhu svého krátkého života zaznamenaly řadu oprav.

Tato část práce popíše možné hrozby, které je při tvorbě komplexního zabezpečení třeba mít vždy namysli a proti kterým je důležité systémy chránit.

1.1 Obecná rizika

Jeden z nejčastějších problémů se kterým se uživatelé často setkávají, je malware. Pojem malware vznikl složením anglických slov „malicious“ (zákeřný) a „software“. Tento pojem je v podstatě souhrnným označením pro škodlivý (nežádoucí) software jako jsou trojské koně, viry, červy, spyware nebo adware.

Některé z těchto škodlivých programů mohou způsobit velké škody v provozu počítače, proto je tedy nutné se chránit, ale aby bylo možné počítače a sítě před viry a červy nebo trojskými koňmi ochránit, je dobré vědět, jak tyto programy fungují.

Virus je programový kód, který se replikuje tak, že se sám připojí k nějakému jinému objektu. Virus ale nemusí být programem sám o sobě, ve skutečnosti může být šíření

zdánlivě nových virů způsobeno jen přepsanými a jinak zabalenými verzemi staršího virového kódu. Virus, který infikuje počítač, může převzít kontrolu nad programy pro elektronickou poštu, zničit nebo poškodit datové soubory, vymazat nainstalované programy nebo porušit samotný operační systém. [2, 4]

Červ je nezávislý program, který se replikuje tak, že se sám kopíruje z jednoho počítače na druhý, obvykle přes síť nebo prostřednictvím příloh elektronické pošty. Mnoho moderních červů navíc obsahuje i virový kód, který dokáže poškodit data nebo spotřebovává tolik systémových zdrojů, že se operační systém stane nepoužitelným. [2, 4]

Trojský kůň je program, který má podobu skrytého serveru, umožňující vetřelci převzít kontrolu nad vzdáleným počítačem, aniž by o tom jeho uživatel věděl. Počítače, které byly napadeny programem v podobě trojského koně, se někdy označují jako zombie. Zástupy takto ovládnutých počítačů mohou vyvolat drastické útoky proti webovým serverům. [2, 4]

Mnoho nejběžnějších počítačových virů a dalších nebezpečných programů se šíří prostřednictvím příloh elektronické pošty. Elektronická pošta nemusí sloužit jen pro přenos různých škodlivých programů, ale existují zde i jiné bezpečnostní problémy. Temnou stránkou elektronické pošty je tzv. nevyžádaná pošta v dnešní době označována jako spam. Pro většinu lidí spam představuje pouze nepříjemnost než skutečné ohrožení bezpečnosti počítače. Spam však s sebou může nést viry a jiný nepřátelský software.

Možnou obranou proti těmto rizikům je neustálé instalování aktualizací systému, konfigurace brány firewall a samozřejmě instalace antivirového programu. Popis těchto možností je popsán v kapitole Metodiky zabezpečení Microsoft Windows.

1.1.1 Sociální inženýrství

Sociální inženýrství je běžně používaný termín označující podvodné jednání neboli manipulaci lidí za účelem provedení určité akce nebo získání určité utajené informace. Ve většině případů útočník nepřichází do osobního kontaktu s obětí a přesto je schopný přesvědčit svou oběť, aby mu poskytla veškeré nutné informace.

Obranou proti sociálnímu inženýrství je vzdělání uživatelů, nedůvěra, ověřování zdroje a odmítnutí.

1.2 Specifická rizika služeb Windows Server 2008 R2

Počítači, který zastává funkci serveru, hrozí specifická rizika spojená s poskytováním služeb klientům. S každou nově instalovanou službou vznikají určitá rizika a těmi se bude zabývat tato část práce.

1.2.1 Bezpečnostní hrozby řadiče domény (Domain Controller)

Řadič domény (DC) je v podstatě počítač, na kterém je uložen adresář služby Active Directory. Řadič domény Windows musí být správně zabezpečený, neboť je pravděpodobným cílem útoku, při němž může dojít k ohrožení databáze Active Directory a objektů v ní uložených. Řadič domény se systémem Windows Server 2008 R2 může čelit následujícím hrozbám: [11]

- Modifikace nebo přidávání objektů služby AD
- Útoky na heslo
- Útoky s odepřením služeb (DoS)
- Útoky s vyřazením replikací
- Zneužití známých zranitelných míst

1.2.1.1 Modifikace nebo přidávání objektů služby AD

V případě napadení řadiče domény (DC) může útočník ve službě Active Directory (AD) provádět jakékoliv změny např. odstraňovat či modifikovat stávající objekty AD nebo naopak přidávat nové.

1.2.1.2 Útoky na heslo

Útočník, který získá přístup k DC, může na takovém řadiči domény zavést jiný operační systém a následně pomocí zálohy System State (Stavu systému) zálohovat celou databázi služby AD, nebo může zkopírovat databázi a protokoly služby AD na jiný počítač. Takto vytvořenou zálohu řadiče domény může následně obnovit na vzdáleném počítači a v odpojeném, offline stavu z něj vést útok na heslo.

1.2.1.3 Útoky s odepřením služeb (DoS)

Pomocí útoku zvanému DoS (Denial of Service) může útočník zabránit v provádění běžného ověřování uživatelů nebo může vést útoky proti službě DNS (Domain Name System), což způsobí, že klienti nebudou moci v síti vyhledat řadiče domény.

1.2.1.4 Útoky s vyřazením replikací

V případě, že útočník dokáže přerušit chod replikací mezi řadiči domény, může tím zabránit i v aplikaci objektů Group Policy (Zásad skupiny), které by mohly řadiče domény chránit před vyřazením z činnosti.

1.2.1.5 Zneužití známých zranitelných míst

Řadič domény, který není udržován v aktuálním stavu, může být snadným cílem útočníků.

1.2.2 Bezpečnostní hrozby DNS (Domain Name System)

Server názvového systému DNS (Domain Name System) zajišťuje vyhodnocování názvů DNS a jejich převod na IP adresy, a naopak vyhodnocování IP adresy na názvy DNS. I služba AD je na službě DNS závislá a využívá ji v roli výchozí služby pro vyhodnocování názvů.[3] Služba DNS může čelit následujícím hrozbám: [11]

- Změny v záznamech služby DNS
- Přenosy zón s daty DNS do neoprávněného serveru
- Útoky s odepřením služeb (DoS) proti službám DNS
- Vyřazení přístupu k záznamům prostředků DNS v kořeni doménové struktury

1.2.2.1 Změny v záznamech služby DNS

Servery DNS podporují dynamické aktualizace DNS, a proto jsou v případě nesprávné konfigurace zabezpečení ohroženy modifikací záznamů prostředků DNS. Útočníkovi, kterému se podaří tyto záznamy modifikovat, může přesměrovat klienty do jiného serveru, který napodobuje činnost původního serveru a přebírá jeho identitu.

Útočníci také mohou zanést „znečistit“ mezipaměť cache serveru DNS falešnými informacemi. V případě úspěšného útoku bude server DNS odesílat klientům pozměněné odpovědi a nespojí s autoritativním serverem DNS.

1.2.2.2 Přenosy zón s daty DNS do neoprávněného serveru

Zóna DNS obsahuje záznamy prostředků SRV a IP adresy, z nichž útočník může dobře odhadnout rozložení vnitřní sítě a umístění služeb AD. Pokud se útočníkovi podaří získat data zóny DNS, může si snadno sestavit topologický diagram sítě.

1.2.2.3 Útoky s odepřením služeb (DoS) proti službám DNS

Útoky typu DoS (Denial of Service) mohou klientům znemožnit přístup ke službám DNS v síti. Při takovém útoku přestane server DNS reagovat na dotazy. Služba AD je na službě DNS také závislá, což znamená, že v případě úspěšného napadení dojde k vyřazení služby DNS z činnosti a přestane v síti fungovat ověřování a vyhodnocování hostitelských názvů v síti.

1.2.2.4 Vyřazení přístupu k záznamům prostředků DNS

Zóna DNS kořenové domény struktury obsahuje záznamy prostředků DNS včetně záznamů prostředků SRV s globálně jedinečnými identifikátory GUID. V případě, že nelze přistupovat k těmto záznamům v kořeni doménové struktury, může se stát, že řadič domény nenalezne záznamy SRV s identifikátory GUID svých partnerů pro replikaci a tím celá replikace selže.

1.2.3 Bezpečnostní hrozby DHCP (Dynamic Host Configuration Protocol)

Protokol DHCP se využívá pro automatické přidělování IP adres klientským počítačům a dalším síťovým zařízením v počítačových sítích na bázi TCP/IP. Protokol DHCP je v síťovém prostředí vystaven následujícím hrozbám: [11]

- Neoprávněné servery DHCP
- Server DHCP přepíše platné záznamy prostředků ve službě DNS
- Neoprávněný klient DHCP

1.2.3.1 Neoprávněné servery DHCP

Útočníkovi, kterému se podaří připojit do vnitřní sítě, může uvést do provozu falešný (neoprávněný) server DHCP, ten následně klientům podává nesprávné IP adresy a další informace.

Poznámka: V případě provozování služby AD je riziko zavlečení neoprávněného serveru DHCP sníženo neboť servery DHCP se musí autorizovat (ověřovat) v adresářové službě AD.

1.2.3.2 Server DHCP přepíše platné záznamy prostředků ve službě DNS

Proces registrace záznamů prostředků DNS na serveru DNS je ve výchozím nastavení rozdělen mezi server a klient DHCP. Server DHCP zaregistruje záznamy prostředků PTR

(Pointer), zapisované do zóny zpětného vyhledávání, a je také jejich vlastníkem, zatímco klient DHCP registruje svůj záznam prostředku A v zóně dopředného vyhledávání.[3]

Při úspěšné změně konfigurace serveru DHCP, může server zaregistrovat oba záznamy prostředků (PTR, A) a následně se stát jejich vlastníkem. V takovém případě může server DHCP přepsat informace o klientu, který již nebude moci aktualizovat svoji IP adresu ve službě DNS neboť není již jeho vlastníkem.

Poznámka: Systémy podporující dynamické aktualizace DNS zajišťují, že modifikaci záznamů prostředků DNS může vykonat výhradně jeho vlastník.

1.2.3.3 Neoprávněný klient DHCP

Server DHCP přiřazuje IP adresu libovolnému klientovi, který si jí vyžádá. Jedinou podmínkou je, aby ve fondu IP adres pronajímaných serverem DHCP byla volná adresa IP. To znamená, že IP adresu a informace o konfiguraci protokolu TCP/IP může získat i neoprávněný klient. Takovýto klient poté může komunikovat s veškerými službami TCP/IP v síti a s dalšími službami AD.

1.3 Fyzické útoky

Tento typ útoku nevyžaduje od útočníka žádné technické znalosti. V případě, že je počítač zanechán, byť jen na několik sekund bez dohledu může dojít k jeho odcizení. To se týká převážně notebooků, ale ani u stolních počítačů to není ničím neobvyklým. Ve chvíli, kdy má útočník počítač ve své moci má dostatek času na to, aby se do něj dostal a získal veškerá osobní data případně hesla, která v něm byla uložena.

Útočníkům nemusí jít výhradně o zcizení hardwarových součástí, ale o získávání citlivých dat bez vědomí uživatelů. Mohou například využít nedbalosti uživatelů, jež ponechají počítače bez dozoru v přihlášeném stavu. V takovém případě má útočník volnou cestu ke zkopírování dat na nějaký externí disk nebo může data zaslat přes internet na nějaký jiný počítač nebo také může pozměnit některá data a tím znehodnotit práci uživatelů. Dobře vybavený útočník také může nainstalovat sledovací program, které běží na pozadí systému a zasílá informace o veškeré činnosti na nějaký cizí počítač.

Jsou také typy útočníků, kterým nejde ani o zcizení hardwarových součástí ani o získávání citlivých dat, ale pouze a jedině o znehodnocení daného počítače například tím, že poškrábají nebo jinak znehodnotí display počítače, přestřižením kabelů, politím nebo popsáním klávesnice atd.

Tyto fyzické útoky je možné minimalizovat například, tak že počítače s citlivými informacemi budou za zamčenými dveřmi, v případě, že jde o velice citlivé informace šifrovat soubory a složky systému nebo použití externích zámků k upevnění počítače k pracovnímu stolu.

2 SLUŽBY SYSTÉMU MICROSOFT WINDOWS SERVER 2008 R2

Windows Server 2008 R2 obsahuje řadu služeb, které jsou v praxi využívány a dle zakoupené edice jsou omezeny dostupností, viz Obr. 1. Na obrázku je také vyznačena edice, která byla v praktické části diplomové práce využita.

V této části diplomové práce budou popsány služby, které byly v práci využívány a na něž bylo aplikováno zabezpečení.

Legenda: ○ = Nedostupné ◐ = Dostupné částečně/omezeně ✔ = Plně dostupné

Server Role	Enterprise	Datacenter	Standard	Itanium	Web	Foundation	HPC
Active Directory Certificate Services	✔	✔	◐1	○	○	◐1	◐ 1
Active Directory Domain Services	✔	✔	✔	○	○	✔	✔
DHCP Server	✔	✔	✔	○	○	✔	✔
DNS Server	✔	✔	✔	○	✔	✔	✔
Fax Server	✔	✔	✔	○	○	✔	○
File Services	✔	✔	◐2	○	○	◐2	◐ 2
Network Policy and Access Services	✔	✔	◐3	○	○	◐5	◐ 3
Print and Document Services	✔	✔	✔	○	○	✔	○
Remote Desktop Services	✔	✔	◐4	○	○	◐6	◐ 4
Web Services (IIS)	✔	✔	✔	✔	✔	✔	✔
Windows Server Update Services (WSUS)	✔	✔	✔	○	✔	✔	✔

1 Omezeno na vytváření certifikačních autorit – bez dalších funkcí ADCS (NDES, Online Responder Service). Více informací naleznete v dokumentaci role ADCS na webu TechNet.

2 Omezeno na 1 samostatný kořenový adresář (standalone DFS root).

3 Omezeno na 250 RRAS připojení, 50 IAS připojení a na 2 IAS Server Groups.

4 Omezeno na 250 připojení Remote Desktop Services.

5 Omezeno na 50 RRAS připojení, 10 IAS připojení.

6 Omezeno na 50 připojení Remote Desktop Services.

Obrázek 1: Porovnání jednotlivých rolí (převzato z [1])

2.1 Active Directory Domain Services (AD DS)

Adresářová služba Active Directory Domain Services je jednou z rolí obsažených ve Windows Serveru 2008 R2. Jedná se o rozšiřitelnou adresářovou službu, která umožňuje centralizovanou správu síťových prostředků. V podstatě to znamená, že tato adresářová služba ukládá veškeré informace potřebné k použití a správě distribuovaných prostředků na jednom místě. Umožňuje například snadno přidávat, odebírat nebo přemísťovat účty pro

uživatele, skupiny a počítače, nastavovat politiku, instalovat programy, stejně jako jiné typy prostředků. Téměř každá úloha správy nějakým způsobem ovlivní službu Active Directory.

K tomu abychom mohli využívat službu ADDS (Active Directory Domain Services) je nutné splňovat následující požadavky:

- V síti by měla být dostupná služba překladu jmen DNS (Domain Name System). Server DNS nemusí být provozován na platformě společnosti Microsoft, ale při instalaci služby Active Directory přináší provoz DNS serveru na platformě společnosti Microsoft určité výhody např. schopnost přijímat žádosti o dynamické záznamy.
- Server, který bude sloužit jako řadič domény a rovněž fungovat jako server DNS, by měl mít přiřazenou statickou adresu IP.
- Souborový systém na discích serveru musí být typu NTFS.

2.2 Domain Name System (DNS)

Systém DNS je systém pro názvy počítačů a síťových služeb, které jsou uspořádány do hierarchie domén. Názvy DNS se používají v sítích TCP/IP, například v síti Internet, k vyhledání počítačů a služeb pomocí popisných názvů. Pokud uživatel zadá v aplikaci název DNS počítače, klienti a servery služby DNS spolupracují na vyhledání názvu a poskytují jiné informace spojené s tímto počítačem, například jeho adresu IP nebo službu, kterou v síti zajišťuje. Tento proces je označován jako překlad adres IP.

Role serveru DNS umožňuje serveru se systémem Windows Server 2008 R2, aby se mohl chovat jako server pro překlad adres IP v síti TCP/IP. Síť může obsahovat počítače se systémem Windows stejně jako počítače s jinými operačními systémy. Služba DNS v systému Windows Server 2008 R2 je těsně spojena s protokolem DHCP (Dynamic Host Configuration Protocol) tak, aby klienti DHCP se systémem Windows a servery DHCP se systémem Windows automaticky registrovaly názvy hostitelů a adresy IP na serveru DNS pro příslušnou doménu.

Obvykle je služba DNS systému Windows Server 2008 integrována se službou AD DS. V tomto prostředí obor názvů DNS zrcadlí doménové struktury a domény služby Active Directory v organizaci. Síťoví hostitelé a služby jsou konfigurovány s názvy DNS, aby je

bylo možné vyhledat v síti, a jsou také konfigurovány se servery DNS, které překládají adresy řadičů domén služby Active Directory.

Služba serveru DNS systému Windows Server 2008 podporuje a splňuje standardy, které jsou specifikovány v sadě dokumentů RFC (Request for Comments) služby DNS. Z tohoto důvodu je plně kompatibilní s jakýmkoli jiným serverem DNS, který odpovídá standardům RFC. Služba DNS Client Resolver je obsažena ve všech klientských a serverových verzích operačního systému Windows. [7, 15]

2.3 Dynamic Host Configuration Protocol (DHCP)

Při nasazení serverů DHCP (Dynamic Host Configuration Protocol) v síti automaticky poskytujete klientským počítačům a jiným síťovým zařízením používajícím protokol TCP/IP platné adresy IP. Těmto klientům a zařízením lze také poskytnout další parametry konfigurace (označované jako možnosti DHCP), které jim umožní připojit se k dalším síťovým prostředkům, jako jsou servery DNS, servery WINS a směrovače.

Funkce poskytované serverem DHCP

Protokol DHCP je technologie typu klient-server, která serverům DHCP umožňuje přiřadit (zapůjčit) adresy IP počítačům a jiným zařízením, které jsou klienty DHCP. Pomocí serveru DHCP lze provádět následující akce: [7, 15]

- zapůjčení adres IP klientům DHCP na určitou dobu a jejich automatické obnovení na žádost klienta,
- automatická aktualizace parametrů klientů DHCP změnou možnosti serveru nebo oboru na serveru DHCP namísto provedení akce u jednotlivých klientů DHCP,
- rezervace adres IP pro určené počítače či jiná zařízení, aby měla vždy stejnou adresu IP a také nejaktuálnější možnosti DHCP,
- vyloučení adres IP nebo rozsahů adres z distribuce serverem DHCP za účelem jejich možného použití pro staticky konfigurované servery, směrovače a jiná zařízení vyžadující statické adresy IP,
- poskytování služeb DHCP mnoha podsítím za předpokladu, že všechny směrovače mezi serverem DHCP a podsítí, pro kterou chcete poskytovat služby, jsou konfigurovány pro předávání zpráv DHCP,
- konfigurace serveru DHCP pro poskytování služby registrace názvů DNS klientům DHCP,

- přiřazení adres vícesměrového vysílání klientům DHCP založeným na protokolu IP.

2.4 Active Directory Certification Services (AD CS)

Služba AD CS (Active Directory Certificate Services) poskytuje služby pro vydávání a správu certifikátů veřejných klíčů, které jsou využívány v systémech softwarového zabezpečení založených na technologii veřejných klíčů.

Funkce služby AD CS

Pomocí nástroje Správce serveru je možné instalovat následující součásti služby AD CS: [7, 15]

- **Certifikační autority (CA):** Kořenové a podřízené certifikační autority jsou používány k vydávání certifikátů uživatelům, počítačům a službám a ke správě platnosti certifikátů.
- **Webový zápis certifikační autority:** Webový zápis umožňuje uživatelům připojit se k certifikační autoritě prostřednictvím webového prohlížeče za účelem vyžádání certifikátů a získání seznamů odvolaných certifikátů (CRL).
- **Online respondér:** Služba online respondéru přijímá požadavky na stav odvolání pro konkrétní certifikáty, hodnotí stav těchto certifikátů a odesílá zpět podepsanou odpověď obsahující požadované informace o stavu certifikátu.
- **Služba zápisu síťových zařízení:** Služba zápisu síťových zařízení umožňuje, aby směrovače a další síťová zařízení, která nemají účet domény, mohla získávat certifikáty.
- **Webová služba Zápis certifikátů:** Webová služba Zápis certifikátů povoluje uživatelům a počítačům provést zápis certifikátu, který používá protokol HTTPS. Společně s webovou službou Zásady zápisu certifikátů povoluje zápis certifikátu na základě zásad, pokud klientský počítač není členem domény nebo pokud člen domény není připojen k doméně.
- **Webová služba Zásady zápisu certifikátů:** Webová služba Zásady zápisu certifikátů povoluje uživatelům a počítačům získat informace o zásadách zápisu certifikátů. Společně s webovou službou Zápis certifikátů povoluje zápis certifikátu na základě zásad, pokud klientský počítač není členem domény nebo pokud člen domény není připojen k doméně.

2.5 Vzdálená plocha (Remote Desktop Services)

Vzdálená plocha, dříve označovaná jako Terminálová služba, je role serveru v systému Windows Server 2008 R2, jež poskytuje technologie, které uživatelům umožňují používat aplikace založené na systému Windows nainstalované na serveru Hostitel relací vzdálené plochy (hostitel relací VP) nebo získat přístup k celé ploše systému Windows. Pomocí služby Vzdálená plocha mohou uživatelé získat přístup k serveru Hostitel relací VP z podnikové sítě nebo z Internetu.

Služba Vzdálená plocha umožňuje efektivně nasazovat a spravovat software v podnikovém prostředí. Programy lze snadno nasadit z centrálního umístění. Vzhledem k tomu, že programy jsou nasazovány na server Hostitel relací VP a nikoli do klientských počítačů, je snazší je upgradovat a spravovat.

Když uživatel získá přístup k programu na serveru Hostitel relací VP, je program spuštěn na serveru. Každý uživatel vidí pouze svou individuální relaci. Relace je transparentně spravována operačním systémem serveru a je nezávislá na všech ostatních klientských relacích. Službu Vzdálená plocha lze dále konfigurovat tak, aby byly pomocí technologie Hyper-V přiřazeny virtuální počítače uživatelům nebo aby služba Vzdálená plocha dynamicky přiřazovala dostupné virtuální počítače uživatelům při připojení. [7, 15]

Služby rolí služby Vzdálená plocha

Vzdálená plocha je role serveru, která sestává z několika služeb rolí. V systému Windows Server 2008 R2 se služba Vzdálená plocha skládá z následujících služeb rolí: [7, 15]

- **Hostitel relací VP:** Hostitel relací vzdálené plochy (hostitel relací VP), dříve označovaný jako Terminálový server, umožňuje serveru hostovat programy založené na systému Windows nebo celou plochu systému Windows. Uživatelé se mohou připojit k serveru Hostitel relací VP a spustit programy, uložit soubory nebo používat síťové prostředky daného serveru.
- **Webový přístup k VP:** Webový přístup k vzdálené ploše (RD Web Access), dříve označovaný jako program TS Web Access, umožňuje získat přístup k programu Připojení k aplikacím RemoteApp a vzdálené ploše prostřednictvím nabídky Start v počítači se systémem Windows 7 nebo prostřednictvím webového prohlížeče. Program Připojení k aplikacím RemoteApp a vzdálené ploše uživatelům poskytuje přizpůsobené zobrazení vzdálených aplikací Programy aplikací RemoteApp a virtuálních ploch.

- **Licencování VP:** Služba Licencování vzdálené plochy (Licencování VP), dříve označovaná jako Licencování TS, spravuje licence pro klientský přístup ke službě Vzdálená plocha (licence VP CAL), které jsou požadovány pro připojení každého zařízení nebo uživatele k serveru Hostitel relací VP. Služba Licencování VP slouží k instalaci, vystavování a sledování dostupnosti licencí VP CAL na licenčním serveru vzdálené plochy.
- **Brána VP:** Služba Brána vzdálené plochy (Brána VP) (dříve označovaná jako Brána TS) umožňuje autorizovaným vzdáleným uživatelům připojit se k prostředkům v interní podnikové síti z libovolného zařízení připojeného k Internetu.
- **Zprostředkovatel připojení k VP:** Zprostředkovatel připojení k vzdálené ploše (Zprostředkovatel připojení k VP), dříve označovaný jako Zprostředkovatel relací TS, podporuje vyrovnávání zatížení relací a opětovné připojení k relaci v serverové farmě Hostitel relací VP s vyrovnáváním zatížení. Zprostředkovatel připojení k VP se také používá k poskytnutí přístupu k aplikacím Programy aplikací RemoteApp a virtuálním plochám prostřednictvím programu Připojení k aplikacím RemoteApp a vzdálené ploše.
- **Hostitel virtualizace VP:** Služba Hostitel virtualizace vzdálené plochy (hostitel virtualizace VP) v integraci s technologií Hyper-V hostuje virtuální počítače a poskytuje je uživatelům jako virtuální plochy. Každému uživateli v organizaci můžete přiřadit jedinečnou virtuální plochu nebo můžete uživatelům poskytnout sdílený přístup do fondu virtuálních ploch.

2.6 Síťové zásady a přístup (Network Policy and Access Services)

Služba Síťové zásady a přístup poskytuje následující řešení možnosti připojení k síti: [7, 15]

- Architektura NAP (Network Access Protection). Architektura NAP je technologie vytváření, vynucení a nápravy problémů zásad stavu klienta, která je zahrnuta v klientském operačním systému Windows 7 a v operačním systému Windows Server 2008 R2. S využitím architektury NAP mohou správci systému vytvořit a automaticky vynutit zásady stavu počítače, mezi které patří požadavky na software, požadavky na aktualizace zabezpečení, požadované konfigurace počítače a další nastavení. Klientským počítačům, které nesplňují zásady stavu, může být přidělen

omezený přístup k síti, dokud nebude jejich konfigurace aktualizována a zásady splněny. V závislosti na zvoleném způsobu nasazení architektury NAP mohou být klienti neodpovídající zásadám automaticky aktualizováni, aby uživatelé mohli rychle znovu získat úplný přístup k síti bez nutnosti ruční aktualizace nebo změny konfigurace počítačů.

- Zabezpečený bezdrátový a drátový přístup. Pokud nasadíte bezdrátové přístupové body 802.1X, poskytne zabezpečený bezdrátový přístup uživatelům bezdrátových sítí metodu zabezpečeného ověřování pomocí hesla, jejíž nasazení je snadné. V případě nasazení ověřovacích přepínačů 802.1X umožňuje drátový přístup zabezpečení sítě tím, že zajistí ověření intranetových uživatelů před jejich připojením k síti nebo získáním adresy IP pomocí protokolu DHCP.
- Řešení vzdáleného přístupu. Díky řešení vzdáleného přístupu je možné uživatelům poskytnout virtuální privátní síť (VPN) a tradiční přístup k síti vaší organizace pomocí telefonického připojení. Můžete také pomocí řešení VPN připojit pobočky k síti, nasadit do sítě plnohodnotné softwarové směrovače a sdílet připojení k Internetu v rámci intranetu.
- Centrální správa síťových zásad pomocí serveru a proxy serveru RADIUS. Není třeba konfigurovat zásady přístupu k síti na jednotlivých serverech pro přístup k síti, jako jsou bezdrátové přístupové body, ověřovací přepínače 802.1X, servery VPN a servery pro telefonické připojení. Zásady, které určují všechny aspekty požadavků na připojení k síti, včetně určení, kdo a kdy se může připojit a jakou úroveň zabezpečení je nutné k připojení k síti použít, můžete vytvořit na jediném místě.

Služby rolí pro službu Síťové zásady a přístup

Při instalaci služby Síťové zásady a přístup jsou k dispozici následující služby rolí: [7, 15]

- Server NPS (Network Policy Server). Server NPS představuje implementaci serveru a proxy serveru RADIUS vytvořenou společností Microsoft. Pomocí serveru NPS je možné centrálně spravovat přístup k síti prostřednictvím řady různých serverů pro přístup k síti, k nimž patří bezdrátové přístupové body, servery VPN, servery pro telefonické připojení a ověřovací přepínače 802.1X. Server NPS můžete dále použít k nasazení zabezpečeného ověřování hesla protokolem PEAP (Protected Extensible Authentication Protocol)-MS-CHAP v2 u bezdrátových

připojení. Server NPS obsahuje také důležité součásti pro nasazení architektury NAP v síti.

Po instalaci služby rolí NPS lze nasadit následující technologie: [7, 15]

- Server zásad stavu architektury NAP. Pokud nakonfigurujete server NPS jako server zásad stavu architektury NAP, vyhodnotí server NPS prohlášení o stavu (Statement of Health) odeslaná klientskými počítači s podporou architektury NAP, které chtějí komunikovat v síti. Na serveru NPS je možné nakonfigurovat zásady architektury NAP, které klientským počítačům umožní aktualizaci konfigurace na úroveň odpovídající síťovým zásadám v organizaci.
- Bezdrátové připojení standardu IEEE 802.11. Pomocí modulu snap-in NPS konzoly MMC můžete nakonfigurovat zásady požadavků na připojení založená na protokolu 802.1X pro přístup klientů k bezdrátové síti IEEE 802.11. V modulu snap-in NPS je také možné nakonfigurovat bezdrátové přístupové body jako klienty služby RADIUS (Remote Authentication Dial-In User Service) a server NPS použít jako server RADIUS ke zpracování požadavků na připojení i k ověřování, autorizaci a monitorování účtů pro bezdrátová připojení protokolem 802.11. Po nasazení bezdrátové infrastruktury ověřování 802.1X lze bezdrátový přístup standardu IEEE 802.11 úplně integrovat s architekturou NAP a umožnit tak ověřování stavu bezdrátových klientů pomocí zásad stavu před povolením jejich připojení k síti.
- Drátové připojení standardu IEEE 802.3. Pomocí modulu snap-in NPS konzoly MMC můžete nakonfigurovat zásady požadavků na připojení založená na protokolu 802.1X pro přístup klientů připojených kabelem k síti Ethernet standardu IEEE 802.3. V modulu snap-in NPS je také možné nakonfigurovat přepínače vyhovující protokolu 802.1X jako klienty služby RADIUS a server NPS použít jako server RADIUS ke zpracování požadavků na připojení i k ověřování, autorizaci a monitorování účtů pro připojení k síti Ethernet protokolem 802.3. Pokud nasadíte drátovou infrastrukturu ověřování 802.1X, můžete úplně integrovat přístup klientů připojených kabelem k síti IEEE 802.3 s architekturou NAP.
- Server RADIUS. Server NPS provádí centralizované ověřování připojení, autorizaci a monitorování účtů pro bezdrátová připojení, ověřovací přepínače, vzdálený přístup pomocí telefonického připojení a připojení VPN. Pokud použijete server NPS jako server RADIUS, je třeba v modulu snap-in NPS

nakonfigurovat servery pro přístup k síti, například bezdrátové přístupové body a servery VPN, jako klienty RADIUS. Je třeba nakonfigurovat také zásady sítě, které server NPS použije k autorizaci požadavků na připojení, a můžete také nakonfigurovat monitorování účtů RADIUS tak, aby server NPS protokoloval informace o monitorování účtů do souborů protokolů na místním pevném disku nebo v databázi serveru Microsoft SQL Server.

- Proxy server RADIUS. Pokud použijete server NPS jako proxy server RADIUS, je třeba nakonfigurovat zásady požadavků na připojení, jež umožní serveru NPS určit, které požadavky na připojení mají být předávány jiným serverům RADIUS a kterým serverům RADIUS chcete požadavky na připojení předávat. Na serveru NPS můžete také nakonfigurovat předávání protokolování dat o monitorování účtů nejméně jednomu počítači ve vzdálené skupině serverů RADIUS.

- Směrování a vzdálený přístup. Služba Směrování a vzdálený přístup umožňuje nasadit služby VPN a vzdáleného přístupu pomocí telefonického připojení a služby směrování pro více protokolů mezi místními sítěmi LAN, mezi sítěmi LAN a WAN a v sítích VPN a pro překlad síťových adres (NAT).

  Během instalace služby rolí služby Směrování a vzdálený přístup lze nasadit následující technologie: [7, 15]

  - Služba vzdáleného přístupu. Pomocí služby Směrování a vzdálený přístup můžete nasadit připojení sítí VPN používající protokol PPTP (Point-to-Point Tunneling Protocol), SSTP (Secure Socket Tunneling Protocol) nebo L2TP (Layer Two Tunneling Protocol) s protokolem IPsec (Internet Protocol security), která uživatelům poskytnou vzdálený přístup k síti vaší organizace. Můžete vytvořit také připojení VPN mezi lokalitami mezi dvěma servery v různých umístěních. Na jednotlivých serverech je pomocí služby Směrování a vzdálený přístup nakonfigurováno zabezpečené odesílání privátních dat. Připojení mezi dvěma servery může být trvalé (vždy zapnuté) nebo na vyžádání (vyžádané volání).
  - Služba vzdáleného přístupu umožňuje také vzdálený přístup pomocí tradičního telefonického připojení a podporuje tak mobilní nebo domácí uživatele, kteří se k intranetům organizace připojují telefonicky. Příchozí požadavky na připojení klientů telefonického připojení k síti přijímá zařízení pro telefonické připojení,

které je nainstalováno na serveru se spuštěnou službou Směrování a vzdálený přístup. Server vzdáleného přístupu přijme volání, ověří a autorizuje volajícího a přenese data mezi klientem telefonického připojení k síti a intranetem organizace.

- Směrování. Služba směrování poskytuje plnohodnotný softwarový směrovač a otevřenou platformu pro směrování a propojení sítí. Tato služba nabízí služby směrování společnostem v prostředí místních sítí LAN a rozlehlých sítí WAN.
- Pokud nasadíte překlad síťových adres (NAT), bude server se službou Směrování a vzdálený přístup nakonfigurován na sdílení připojení k Internetu s počítači v privátní síti a na překlad přenosů mezi svou veřejnou adresou a privátní sítí. Díky překladu síťových adres (NAT) získají počítače v privátní síti určitou míru ochrany, protože směrovač s nakonfigurovanou funkcí překladu síťových adres (NAT) nepředává přenosy z Internetu do privátní sítě, pokud není předání vyžádáno klientem privátní sítě nebo pokud nejsou přenosy výslovně povoleny.
- Pokud nasadíte síť VPN a překlad síťových adres (NAT), bude server se službou Směrování a vzdálený přístup nakonfigurován k poskytování překladu síťových adres (NAT) pro privátní síť a k příjmu připojení VPN. Počítače v Internetu nebudou moci určit adresy IP počítačů v privátní síti. Klienti VPN se však budou moci připojit k počítačům v privátní síti, jako kdyby byli fyzicky připojeni ke stejné síti.

- Autorita pro registraci stavu (Health Registration Authority). Autorita pro registraci stavu je součást architektury NAP, která vydává certifikáty stavu klientům, u nichž server NPS úspěšně provede ověření zásad stavu pomocí prohlášení o stavu (SoH) klienta. Autorita pro registraci stavu se používá pouze s metodou vynucení protokolu IPsec architektury NAP.

- Protokol HCAP (Host Credential Authorization Protocol). Protokol HCAP umožňuje integraci řešení architektury NAP společnosti Microsoft se serverem pro řízení přístupu k síti společnosti Cisco. Pokud nasadíte protokol HCAP se serverem NPS a architekturou NAP, může server NPS provádět vyhodnocování stavu klientů a autorizaci klientů přístupu protokolem 802.1X společnosti Cisco.

2.7 Služba Windows Server Update Services

Služba WSUS umožňuje správcům informačních technologií nasazovat nejnovější aktualizace produktů společnosti Microsoft do počítačů, ve kterých běží podporované operační systémy této společnosti.

Pomocí služby WSUS mohou správci plně spravovat distribuci aktualizací vydaných prostřednictvím služby Microsoft Update do počítačů v jejich síti. Služba WSUS poskytuje infrastrukturu správy, která se skládá z následujících částí. [7, 15]

- **Microsoft Update:** Web společnosti Microsoft, který distribuuje aktualizace produktů této společnosti.
- **Server Windows Server Update Services:** Tato součást je nainstalována na serveru uvnitř podnikové brány firewall. Server WSUS umožňuje správcům spravovat a distribuovat aktualizace prostřednictvím konzoly pro správu služby WSUS, kterou je možné nainstalovat do každého počítače se systémem Windows v doméně. Kromě toho může být server WSUS zdrojem aktualizací pro další servery WSUS v organizaci. Nejméně jeden server WSUS v síti musí být připojen k serveru Microsoft Update, aby získával informace o dostupných aktualizacích. Správce může určit na základě konfigurace a zabezpečení sítě, zda se budou ostatní servery připojovat přímo k serveru Microsoft Update.
- **Automatické aktualizace:** Tato součást je součástí podporovaných operačních systémů. Automatické aktualizace umožňují, aby serverové i klientské počítače získávaly aktualizace ze serveru Microsoft Update nebo ze serveru WSUS.

3 ZÁSADY SKUPINY (GROUP POLICY)

Zásady skupiny umožňují správci systému definovat různé součásti pracovního prostředí uživatelů. Pro plnou funkčnost prostředků zásad skupiny je nezbytná instalace služby Active Directory Domain Services.

3.1 Vlastnosti zásad skupiny

Zásady skupiny obsahují tyto základní funkce:

- Nastavení zabezpečení,
- šablony pro správu,
- skripty,
- instalace software,
- přesměrování složek,
- údržba aplikace Internet Explorer,
- zásady zabezpečení protokolu IP,
- zásady omezení software,
- zásady bezdrátové sítě (IEEE 802.11),
- služba vzdálené instalace.

Zásady skupiny (Group Policy) máme dvojího typu:

- Zásady skupiny bez služby Active Directory, jež se označují jako Místní zásady skupiny. Při využívání Místních zásad skupiny může být nevýhodou fakt, že omezují všechny uživatele, kteří se přihlásí k danému počítači, takže nejen obyčejné uživatele, ale také administrátory.
- Zásady skupiny se službou Active Directory, jež využívá tato diplomová práce, poskytují téměř neomezené využívaní objektů zásad skupiny (GPO – Group Policy Object). Díky GPO je možné aplikovat jednotlivá pravidla na vybrané uživatele či počítače.

K tomu aby jednotlivé zásady byly správně aplikovány, je třeba znát strukturu Active Directory. Ta se skládá ze tří hlavních úrovní:

- sídlo
- doména

- organizační jednotka (OU)

Úrovňové dělení v tomto případě znamená, že zásady nastavené na vyšší úrovni prostředí Active Diretory automaticky ovlivní všechny nižší úrovně. Jinak řečeno zásady nastavené na určité úrovni zdědí všechny nižší úrovně. [9]

- Pokud GPO budou nastaveny na úrovni sídla, všechna nastavení zásad skupiny z tohoto objektu ovlivní všechny účty přihlášené do tohoto sídla. Samozřejmě, účty se nachází v doméně (nebo/a v OU), ale účet patří do určitého sídla, proto ho ovlivňují jen tato nastavení zásad.
- Pokud GPO budou nastaveny na úrovni domény, ovlivní všechny prvky této domény a všechny OU na nižších úrovních.
- Pokud GPO budou nastaveny na úrovni OU, ovlivní všechny prvky této OU a další OU na nižších úrovních.

Ve chvíli, kdy si dvě zásady odporují, má přednost zásada nastavená na nižší úrovni. To znamená, že zásada nastavená na úrovni domény a jiná, která ji ruší na úrovni organizační jednotky má přednost, vyhrává tedy organizační jednotka. Stejně tak nastavení zásad na úrovni domény přebíjí všechny konfliktní zásady nastavené na úrovni sídla.

Důležité je vědět, že každý, kdo se přihlásí na některou pracovní stanici, je omezován prvně místním nastavením zásad a až poté se použije nastavení zásad prostředí Active Directory (úrovně sídla, domény a OU). V takovém případě je řeč o čtyřech úrovních Zásad skupiny a to místním počítači, sídle, doméně a OU. V případě nějakého konfliktu, GPO nastavené v prostředí Active Directory mají přednost před místními zásadami skupiny.

Zásady skupiny obsahují dvě části a to část uživatele neboli Konfigurace uživatele a část počítač neboli Konfigurace počítače. Týkají se jak místních zásad skupin, tak i objektů zásad skupin, které se vytvářejí při používání Active Directory. V případě, že v Konfiguraci uživatele i Konfiguraci počítače jsou nastaveny zásady, které si odporují, použije se nastavení, které je součástí Konfigurace počítače.

3.2 Propojení Objektů zásad skupiny

V případě, že je vytvořen GPO na úrovni sídla, domény nebo OU pomocí grafického uživatelského prostředí, systém tento objekt automaticky připojí k úrovni, na které byl vytvořen.

Objekty zásad skupiny vytvořené v prostředí Active Directory jsou občas přirovnávány k dětem plavajícím ve velkém bazénu. Každé dítě má kolem pasu upevněný provaz, jehož druhý konec drží jeho dospělý ochránce. Ve skutečnosti, kolem každého dítěte může být upevněno více provazů a každý ochránce může hlídat více dětí. Smutné je, když některé dítě plave v bazénu jen tak, bez ochránce. V této analogii je k bazénu přirovnaný jeden kontejner prostředí Active Directory, který se nazývá Zásady. Všechny GPO se narodí a žijí v této konkrétní doméně. Odtud se pak zkopírují na všechny řadiče domény. Ochránce z této analogie nám pak reprezentuje některou z úrovní prostředí Active Directory - sídlo, doménu nebo OU. [9]

V příkladu s bazénem mohlo být několik ochránců připojeno k jednomu dítěti. V prostředí Active Directory může být s jedním GPO propojeno také více úrovní. Tudíž i každá úroveň Active Directory může obsahovat několik GPO, které zůstávají v doméně připravené na použití.

Je důležité si pamatovat, že nezáleží na tom, jestli GPO je propojený se sídlem, doménou nebo OU. Objekt si jen tak plave v bazénu (analogie domény), kde čeká, až jej někdo bude potřebovat. [9]

4 METODIKY ZABEZPEČENÍ MICROSOFT WINDOWS

Společnost Microsoft klade na bezpečnost veliký důraz a své produkty podrobuje řadě změn, které zvyšují jejich bezpečnost.

V této části práce budou popsány metodiky zabezpečení, které byly v práci využity a jež zvyšují bezpečnost počítačů.

4.1 Aktualizace systému

Každá verze systému Windows, která kdy byla vydána, obsahuje určité chyby a nedostatky, které mohou oslabit bezpečnost systému. V průběhu času, jak se tyto bezpečnostní problémy identifikují, firma Microsoft zveřejňuje opravné balíčky a aktualizace, které problémy odstraňují. Service Pack jenž je souhrnem doposud zveřejněných aktualizací obsahuje veškeré opravy chyb a bezpečnostní aktualizace spolu s rozšiřujícími součástmi systému.

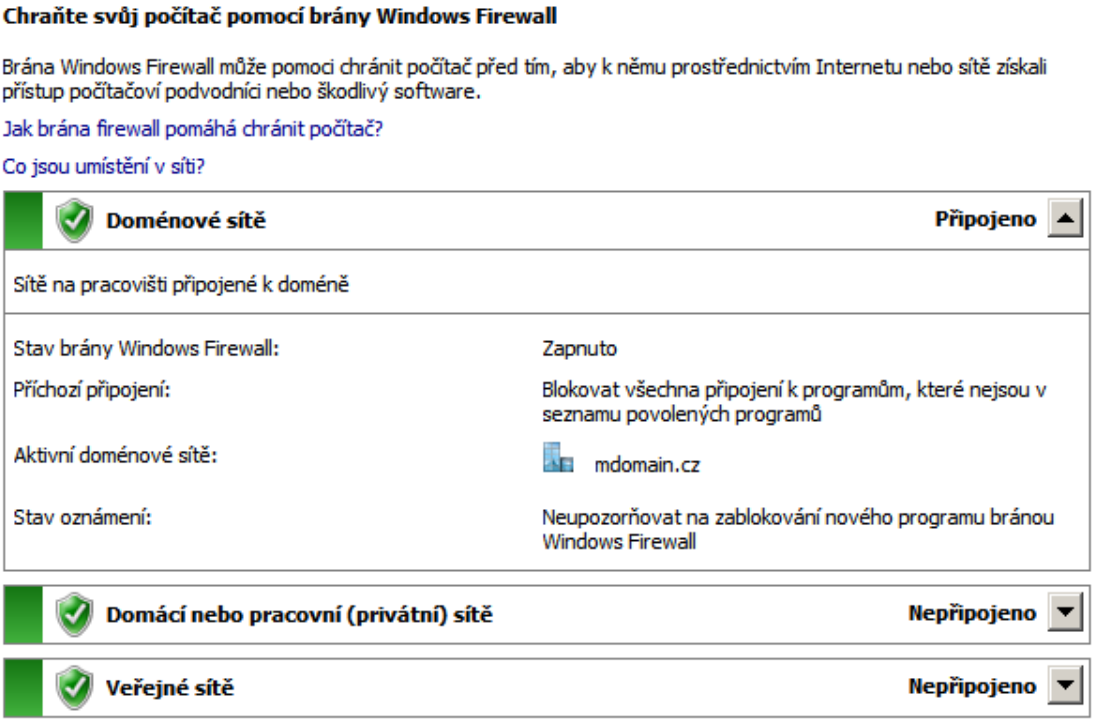
4.2 Firewall

Brána firewall je systém nebo software, který řídí datový tok mezi dvěma počítačovými sítěmi, přičemž chrání počítač nebo síť před vnějšími útočníky. Počítače připojené k síti Internet by měli využívat tuto metodu zabezpečení. Brány firewall se obecně dělí na softwarové a hardwarové. Jedná-li se o jediný počítač je vhodnější, využít softwarovou bránu firewall, ale v případě, že jde o skupinu počítačů, měla by být využita hardwarová brána firewall. Vyššího zabezpečení lze dosáhnout kombinací těchto dvou firewallů. V žádném případě není vhodné kombinovat dva softwarové firewally. V takovém případě muže dojít k problému připojení k síti Internet nebo k jiným neočekávaným chybám.

Brána firewall operačních systému Windows Server 2008 R2 a Windows 7

Brána firewall je integrovanou součástí Windows Server 2008 R2 a Windows 7.

Windows Firewall si podle profilu síťového umístění určuje výchozí nastavení při prvním připojení do jakékoliv sítě.



Obrázek 2: Windows Firewall, umístění v síti

Ve Windows Firewall je možnost povolení nebo zablokování programů a portů, kde je také možné dávat výjimky programům pro jednotlivé profily umístění v síti, tedy už ne jen jednu výjimku pro jeden program, ale pro každý program dvě (privátní, veřejné – v případě domény budou možnosti tři). To významně zlepšilo chování při připojení do VPN. Nastavení výjimek programů a služeb je rozšířeno o možnost jejich upravení pro jednotlivé profily umístění v síti. V záložce 'Upřesnit nastavení' je podrobné nastavení Windows Firewall. Ve vlastnostech brány firewall je možné upřesnit nastavení jednotlivých profilů, doménového, veřejného i soukromého, což zahrnuje pravidla pro příchozí a odchozí připojení pro každý profil, ale i možnost IPSec. Užitečné mohou být filtry, díky kterým je možné si zobrazit momentálně hledaná pravidla a jejich nastavení. Filtrovat je možné dle profilu, stavu a skupiny.

4.3 Antivirový software

Antivirový program je počítačový software, který slouží k identifikaci, odstraňování a eliminaci počítačových virů a jiného škodlivého software (malware). Antivir využívá převážně dvou technik:

Prohlíží soubory na lokálním disku a má za cíl nalézt sekvenci odpovídající definici některého počítačového viru v databázi.

Detekuje podezřelé aktivity nějakého počítačového programu, který může značit infekci. Tato technika zahrnuje analýzu zachytávaných dat, sledování aktivit na jednotlivých portech či jiné postupy. [11]

Operační systémy Windows ve výchozí konfiguraci neposkytují ochranu tohoto typu. Proto je důležité nainstalovat antivirový program hned po instalaci operačního systému.

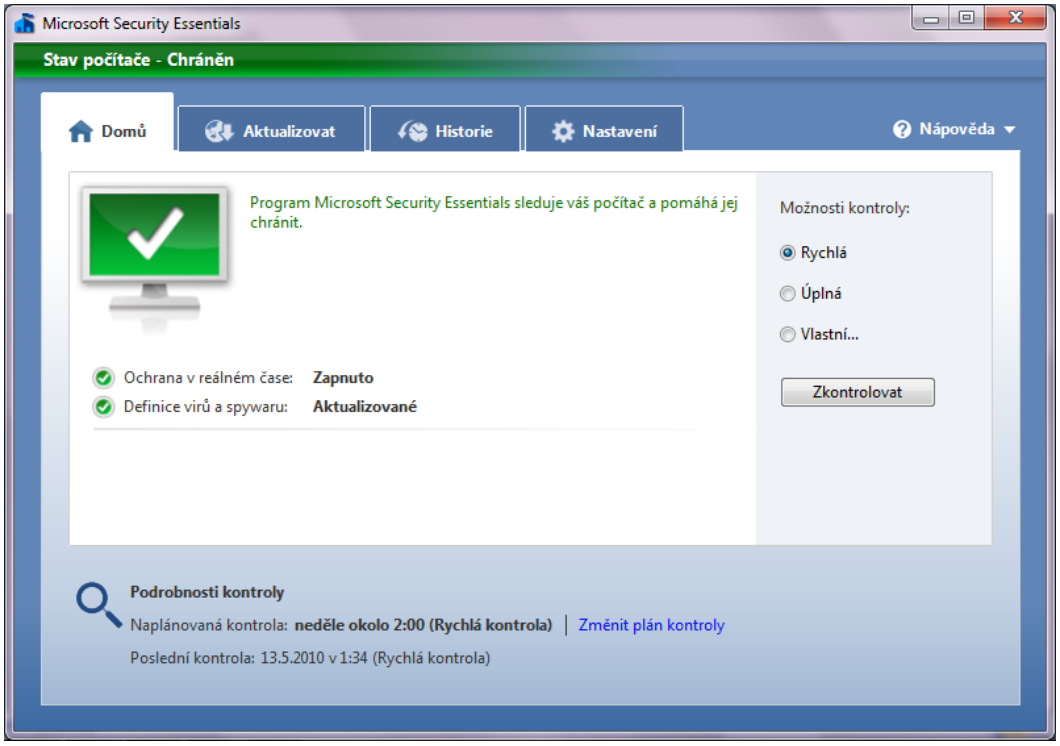
Existuje celá řada antivirových programů poskytující kvalitní ochranu systému. Z této široké škály je možno si vybrat antivirový program, který bude co nejefektivněji vyhovovat stanoveným podmínkám.

Microsoft Security Essentials

Společnost Microsoft nedávno na trh uvedla nový antivirový program zvaný Microsoft Security Essentials, který nabízí kvalitní ochranu počítačů proti virům, spyware, trojským koním a dalším nebezpečím, které se nachází v síti. Výhodou použití zmiňovaného programu je stoprocentní kompatibilita se systémem Windows 7 a fakt, že daný program je zdarma. Program je vybaven i jinými přednostmi a to jest nenáročností na výkon počítače a také snadná obsluha a nastavení.

Uživatelské rozhraní obsahuje čtyři záložky:

- Home – základní přehled, jež obsahuje poslední kontrolu systému, plán další kontroly a typ skenování
- Update – umožňuje stahování nových aktualizací
- History – přehled všech položek, které byly antivirem detekovány jako hrozba
- Settings – různá nastavení programu



Obrázek 3: Microsoft Security Essentials

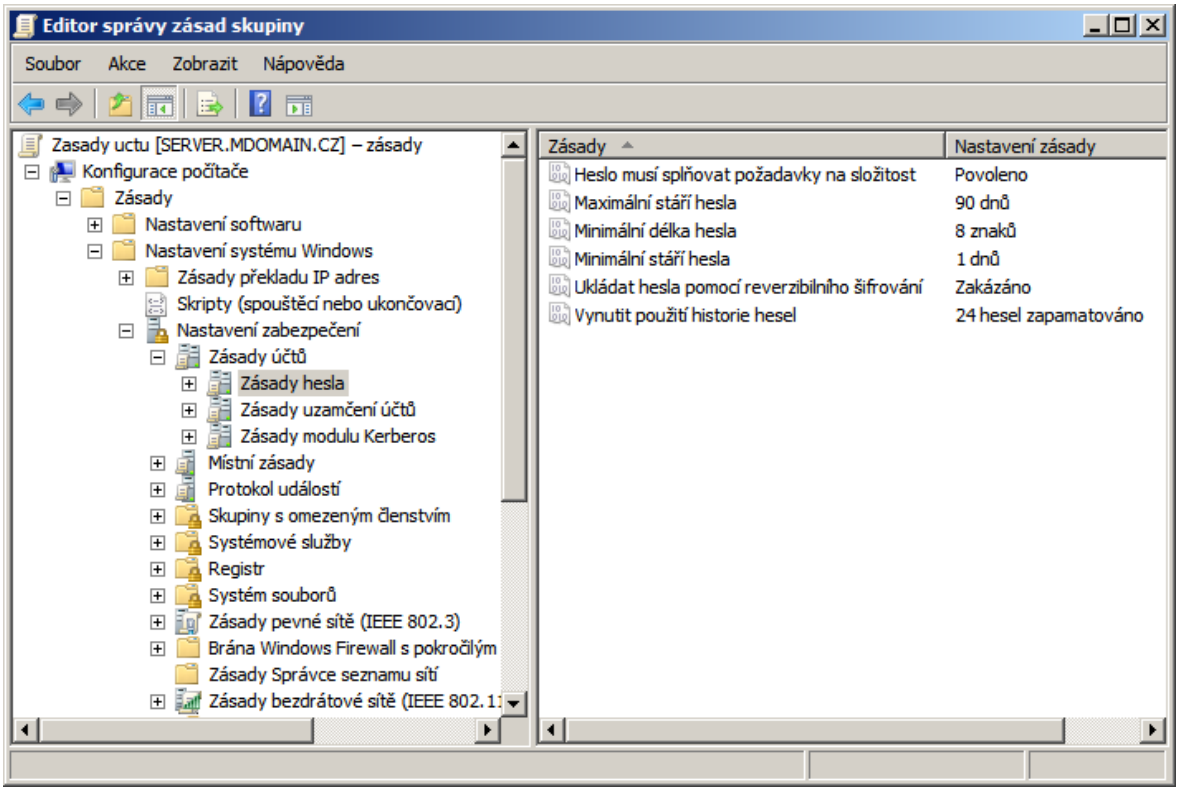
4.4 Nastavení zásad hesla

Nastavení zásad hesla patří mezi základní stavební kameny zabezpečení domény Active Directory.

Ve chvíli kdy je vytvořena doména je také vytvořena organizační jednotka Domain Controllers a dva standardní objekty zásad skupiny, kdy GPO Default Domain Policy je propojen na úroveň domény a GPO Default Domain Controllers Policy je propojen na úroveň OU Domain Controllers.

GPO Defalut Domain Policy slouží k nastavení výchozí konfigurace pro Zásady účtů, která obsahuje tři klíčová nastavení zabezpečení domény:

- Zásady hesla
- Zásady uzamčení účtů
- Zásady modulu Kerberos



Obrázek 4: Editor správy zásad skupiny, nastavení Zásad hesla

Pomocí GPO Default Domain Policy je také možné uplatnit speciální zásady na úrovni domény a to:

- Automaticky odpojit uživatele po uplynutí doby přihlášení
- Přejmenovat účet správce
- Přejmenovat účet hosta

Výchozí konfiguraci Zásad účtů je možné upravovat dvěma způsoby:

- Přímá změna GPO Default Domain Policy
- Vytvoření nového GPO (Group Policy Object) na úrovni domény a změna priority objektu

Obě možnosti úpravy Zásad účtů má své výhody avšak v této práci byla využita druhá možnost a to Vytvoření nového GPO na úrovni domény. Výhodou tohoto postupu je, že nechává GPO Default Domain Policy beze změn a veškerá nastavení jsou uložena v nově vytvořeném objektu zásad skupiny. Při využití této možnosti je velmi důležité nezapomnět zvýšit prioritu nového objektu. V případě kdy by měl nový GPO nižší prioritu uplatnilo by se výchozí nastavení v GPO Default Domain Policy.

4.4.1 Zásady hesla

Slouží k nastavení zásad hesel doménových účtů. Pomocí Zásad hesla definujeme požadavky na složitost hesla: [15]

Heslo musí splňovat požadavky na složitost - povolením této zásady, musí heslo splňovat následující minimální požadavky:

- Nesmí obsahovat název účtu uživatele ani části celého jména uživatele přesahující dva sousední znaky
- Musí obsahovat alespoň 6 znaků
- Musí obsahovat znaky ze tří z následujících čtyř kategorií:
  - Velká písmena anglické abecedy (A až Z)
  - Malá písmena anglické abecedy (a až z)
  - Základních 10 číslic (0 až 9)
  - Jiné než alfanumerické znaky (například !, $, #, %)

Požadavky na složitost jsou prosazovány při změně nebo vytvoření hesla.

Maximální stáří hesla - povolení této zásady zabezpečení určuje dobu (ve dnech), po kterou může být heslo používáno, než systém požádá uživatele o jeho změnu. Zadáním hodnoty v rozsahu 1 až 999 je možné určit počet dnů, po jejichž uplynutí má vypršet platnost hesla, zadáním hodnoty 0 je možné určit trvalou platnost hesla. Pokud je maximální stáří hesla mezi 1 a 999 dny, musí být minimální stáří hesla menší než tato hodnota. Pokud je maximální stáří hesla nastaveno na hodnotu 0, lze minimální stáří hesla nastavit na libovolnou hodnotu mezi 0 a 998 dny.

Minimální délka hesla - povolení této zásady zabezpečení určuje nejmenší počet znaků, které musí heslo uživatele obsahovat. Lze nastavit hodnotu mezi 1 a 14 znaky, případně nastavením hodnoty 0 určit, že není požadováno žádné heslo.

Minimální stáří hesla - povolení této zásady zabezpečení určuje dobu (ve dnech), po kterou musí být heslo používáno, než je uživatel může změnit. Je možné nastavit hodnotu mezi 1 a 998 dny, nastavením hodnoty 0 je umožněna bezprostřední změna hesla. Minimální stáří hesla musí být menší než maximální stáří hesla, pokud není maximální stáří hesla nastaveno na hodnotu 0, která značí trvalou platnost hesel. Pokud je maximální stáří hesla nastaveno na hodnotu 0, lze minimální stáří hesla nastavit na libovolnou hodnotu mezi 0 a 998.

Ukládat hesla pomocí reverzibilního šifrování - povolení této zásady zabezpečení určuje, zda operační systém bude ukládat hesla pomocí reverzibilního šifrování. Tato zásada poskytuje podporu aplikací používajících protokoly, které vyžadují znalost hesla pro účely ověření. Ukládání hesel pomocí reverzibilního šifrování je v podstatě stejné jako uložení hesel ve formě prostého textu. Z tohoto důvodu by tato zásada neměla být nikdy povolena, pokud požadavky aplikace nepřevažují nad potřebou ochrany hesel.

Tato zásada je vyžadována při použití ověřování pomocí protokolu CHAP (Challenge-Handshake Authentication Protocol) prostřednictvím vzdáleného přístupu nebo služeb IAS (Internet Authentication Services). Je také zapotřebí při ověřování algoritmem Digest u Internetové informační služby (IIS).

Vynutit použití historie hesel - povolení této zásady zabezpečení určuje počet jedinečných nových hesel, která musí být přidružena k uživatelskému účtu, než lze znovu použít některé staré heslo. Hodnota musí být mezi 0 a 24 hesly. Tato zásada umožňuje správcům zvýšit zabezpečení tím, že zabraňuje opětovnému používání starých hesel.

4.4.1.1 Tvorba silných hesel

Silné heslo je takové, které nelze snadno uhodnout ani prolomit. Silné heslo je alespoň osm znaků dlouhé, neobsahuje název uživatelského účtu ani jeho část a obsahuje alespoň tři znaky z následujících čtyř kategorií znaků: velká písmena, malá písmena, číslice a speciální znaky. [15]

Typ pro tvorby a zapamatování hesla: [7]

- je dobré si zvolit snadno zapamatovatelné slovní spojení např.: "Amerika je daleko"
- nahradit písmena nebo slova ze snadno zapamatovatelného slovního spojení číslicemi, symboly a pravopisnými chybami např.: "Amerika je daleko" může po nahrazení vypadat "@mer|4@je |)ale4o"
- pro snadnější zapamatování je dobré volit speciální znaky a číslice tak, aby připomínaly skutečné písmeno ze slovního spojení (A-@, D-|), O-(), K-4)

Takto vytvořené heslo lze považovat za dostatečně silné a to díky tomu, že neobsahuje úplná slova, neboť některá z nich jsou nahrazena číslicí či speciálním znakem a také obsahuje mezery.

Výhodou využití mezer je, že je možné vytvořit slovní spojení skládající se z většího počtu slov, což je povětšinou snazší k zapamatování než běžné heslo a díky své délce je také těžší ho uhodnout.

Nevýhodou využívání mezer může být fakt, že nelze zaručit, že všechny systémy poskytující ochranu heslem budou mezeru podporovat.

Poznámka: V heslech je také možnost využívat diakritiku, což se obecně nedoporučuje, neboť nevýhodou může být, že ne každý počítač má nainstalovanou českou klávesnici.

Pro tvorbu silných hesel je možné také využít nástroje pro tvorbu hesel např. Safetica Business, Password Generator Professional aj.

4.5 Auditování událostí

Auditování slouží ke sledování činností uživatelů a změn v systému, které mají vliv na zabezpečení systému. Auditování probíhá tak, že se zvolené události zaznamenávají do protokolů. [2]

Účelem auditování je schopnost zpětně prozkoumat události a stavy počítačového systému a odvodit tak informace potřebné pro řešení chyb, problémů se zabezpečením, identifikaci trendů a v neposlední řadě také učinit proaktivní opatření, jež zabrání výskytu problémů v budoucnosti. [1]

Aby zaznamenaná informace měla pro správce systému skutečnou hodnotu, měla by obsahovat následující údaje:

Každá položka protokolu je označena typem a obsahuje informace v hlavičce a popis události.

Hlavička události obsahuje následující informace o události:[7]

- Datum - Datum výskytu události.
- Čas - Čas výskytu události.
- Uživatel - Uživatelské jméno uživatele, který byl přihlášen při výskytu události.
- Počítač - Název počítače, ve kterém došlo k výskytu události.
- ID události - Číslo události, které identifikuje typ události. Na základě ID události mohou pracovníci oddělení technické podpory porozumět tomu, co se v systému stalo.

- Zdroj - Zdroj události. Může to být název programu, součásti systému nebo jednotlivé součásti většího programu.
- Typ - Typ události. Může to být jeden z následujících pěti typů: Chyba, Upozornění, Informace, Auditovat úspěšné provedení operací a Auditovat neúspěšné provedení operací.
- Kategorie - Klasifikace události podle zdroje události. Používá se především v protokolu zabezpečení.

Typy událostí

Popis každé zaprotokolované události závisí na typu události. Každá událost v protokolu může být zařazena do jednoho z následujících typů:[7]

- Informace - Událost, která popisuje úspěšnou operaci úlohy, například aplikace, ovladače nebo služby. Událost typu Informace se zaprotokoluje například tehdy, pokud se úspěšně načte síťový ovladač.
- Upozornění - Událost, která nemusí být nutně závažná, může však naznačovat možnost výskytu budoucích potíží. Událost typu Upozornění se zaprotokoluje například tehdy, pokud začíná být málo místa na disku.
- Chyba - Událost, která popisuje závažný problém, například selhání kritické úlohy. Událost typu Chyba může zahrnovat ztrátu dat nebo ztrátu funkčnosti. Událost typu Chyba se zaprotokoluje například v případě, že se nezdaří načtení služby během spouštění.
- Auditovat úspěšné provedení operací (protokol zabezpečení) - Událost, která popisuje úspěšné dokončení auditované události zabezpečení. Událost typu Auditovat úspěšné provedení operací se zaprotokoluje například tehdy, pokud se uživatel přihlásí k počítači.
- Auditovat neúspěšné provedení operací (protokol zabezpečení) - Událost popisující auditovanou událost zabezpečení, která se nedokončila úspěšně. Událost typu Auditovat neúspěšné provedení operací se může zaprotokolovat například tehdy, pokud uživatel nemůže získat přístup na síťovou jednotku.

Operační systém Microsoft Windows Server 2008 definuje několik kategorií auditu bezpečnostních událostí: [1, 2, 7, 11]

- Události přihlášení k účtu

- Správu účtu
- Přístup k adresářové službě
- Události přihlášení
- Přístup k objektům
- Změny zásad
- Používání privilegií
- Sledování procesů
- Systémové události

Soubor protokolu, který je možné prohlížet pomocí konzoly Prohlížeč událostí (Event Viewer).

4.6 Architektura NAP (Network Access Protection)

Architektura NAP (Network Access Protection) je nová technologie, která byla zavedena v systému Windows 7 a Windows Server 2008. Architektura NAP obsahuje klientské a serverové součásti umožňující vytvoření a vynucení zásad požadavků na stav, které definují požadovanou softwarovou a systémovou konfiguraci počítačů, jež se připojují k síti. Architektura NAP vynucuje požadavky na stav prověřením a vyhodnocením stavu klientských počítačů, přičemž omezí přístup k síti, pokud klientské počítače považuje za nekompatibilní a provede nápravu nekompatibilních klientských počítačů tak, aby měly neomezený přístup k síti. Architektura NAP vynucuje požadavky na stav u klientských počítačů, které se snaží připojit k síti. Jakmile se kompatibilní klientský počítač připojí k síti, zajišťuje architektura NAP trvalou kompatibilitu jeho stavu. [7]

K vynucení architektury NAP dojde v okamžiku, kdy se klientské počítače pokusí připojit k síti prostřednictvím serveru pro přístup k síti, jako je například server virtuální privátní sítě (VPN) se službou Směrování a vzdálený přístup, nebo pokud se klientské počítače pokusí komunikovat s jinými síťovými prostředky. Postup vynucení architektury NAP závisí na vybrané metodě vynucení. Architektura NAP vynucuje požadavky na stav pro následující položky:[1]

- komunikace chráněná protokolem IPsec (Internet Protocol security) - při využití tohoto způsobu nasazení se bude NAP starat o to, aby se do sítě nepřipojil žádný počítač, který nesplňuje požadavky na komunikaci pomocí protokolu IPSec

- připojení ověřená standardem zabezpečení IEEE (Institute of Electrical and Electronics Engineers) 802.1X) - zde jsou zase ostře sledována zařízení typu ethernetových přepínačů a bezdrátových přístupových bodů, které pokud nesplní definované podmínky, nebudou moci komunikovat se zbytkem sítě
- připojení virtuálních privátních sítí (VPN) - v tomto případě jsou hlídány počítače využívající VPN jakožto formy vzdáleného přístupu do sítě. Tento způsob nasazení je vhodný zejména tam, kde se např. zaměstnanci firmy připojují do firemní sítě z domu ze svých vlastních počítačů, nad kterými nemá správce sítě kontrolu. NAP pohlídá, aby do firemní sítě byly vpuštěny třeba jen ty počítače, na kterých je nainstalován antivirus, mají povolené automatické aktualizace, atd.
- konfigurace protokolu DHCP (Dynamic Host Configuration Protocol) - tento způsob vynucení NAPem je asi nejzranitelnější. NAP zde ve spolupráci se serverem DHCP zajišťuje, aby plnohodnotná adresa IP byla přidělena jen počítačům, které splňují požadavky na jejich stav. Pokud žádající počítač tyto požadavky nesplňuje, může mu být přidělena jiná adresa IP a počítač tak bude umístěn do tzv. nápravné sítě (remediation network). V této nápravné síti je místo totálního odpojení od sítě počítači poskytnuta jakási možnost zjednat nápravu. Např. zde může z intranetového webu stáhnout a nainstalovat antivirovou aplikaci, aktualizace Windows apod.
- připojení prostřednictvím služby Brána Vzdálené plochy (Brána VP).

4.7 Zabezpečení síťového provozu pomocí protokolu IPSec

Mnohé síťové protokoly neposkytují vůbec žádné nebo jen minimální zabezpečení naproti tomu protokol IPSec (IP Security) poskytuje zabezpečení dvěma základními způsoby:

- Šifrování - IPSec umí šifrovat datové pakety nebo jen data v těchto paketech díky protokolu ESP (Encapsulating Security Payload) a tím zajišťuje bezpečný přenos dat přes nezabezpečenou část sítě (např. Internet)
- Integrita - IPSec poskytuje také mechanizmy, které slouží k ověření dat díky protokolu AH (Authentication Header) a tím zajišťuje jejich autentičnost

Mechanizmy ověřování protokolu IPSec:

- Kerberos - pokud je protokol IPSec nasazen v doméně Active Directory je protokol Kerberos k dispozici a je tedy možné ho využít bez nutnosti instalace dalších služeb

- Certifikáty - jestliže se v síti nachází služby používané pro provoz infrastruktury veřejných klíčů hlavně tedy certifikační autorita CA, je možné zvolit tento způsob ověřování
- Sdílený klíč - tento způsob ověřování je vhodný použít pro zajištění komunikace mezi několika málo počítači. Pracuje se zde s jediným tajným klíčem, který musí být znám všem komunikujícím stranám

Operační systém Windows Server 2008 R2 obsahuje dvě možnosti, jak nasadit komunikaci chráněnou protokolem IPSec v síti:

- Zabezpečení komunikace prostřednictvím zásad IPSec
- Zabezpečení komunikace pomocí Pravidel zabezpečení připojení

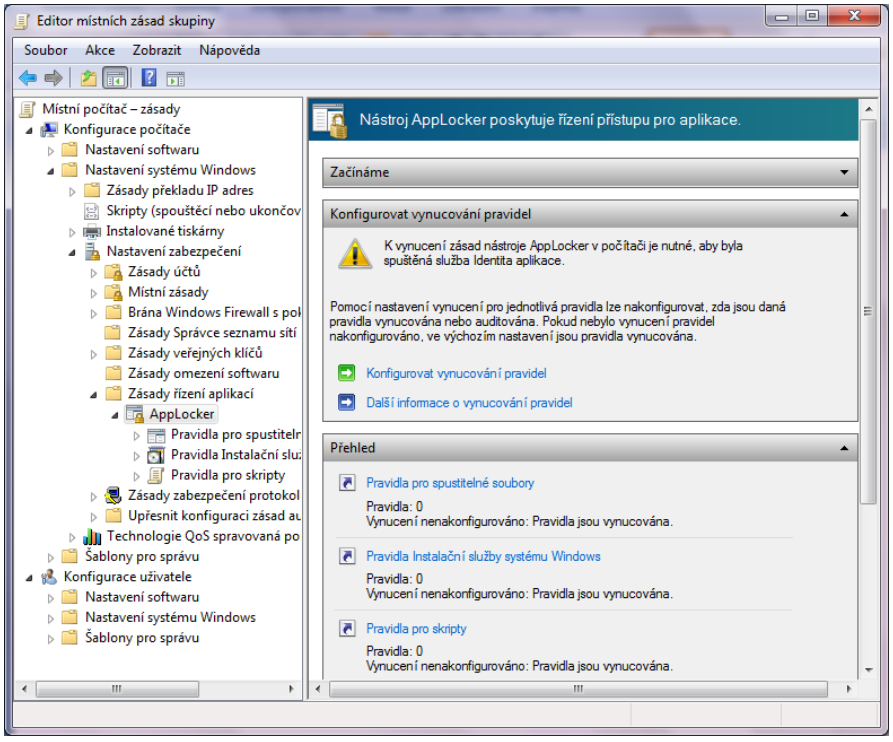
Výchozí zásady IPSec:

- Client (Respond Only) - tato zásada funguje tak, že hostitel vždy navazuje nešifrované spojení a pouze je-li komunikace zahájena jiným hostitelem, který vyžaduje šifrování, dohodnou se obě strany na používání šifrované komunikace
- Secure Server (Require Security) - komunikace bude probíhat jen tehdy, pokud je možnost ji zašifrovat. V opačném případě nebude spojení navázáno
- Server (Request Security) - hostitel se pokusí při navazování spojení vyjednat šifrované spojení, ale není-li to možné (druhá strana jej nepodporuje), spokojí se hostitel i s nešifrovanou komunikací

4.8 AppLocker

Je flexibilní a pro administraci snadný mechanizmus poskytující IT profesionálům možnost přesně specifikovat co je dovoleno spouštět v desktopu a tak vnutit uživateli, aby byly spouštěny pouze aplikace, instalace programů a skripty které jsou odsouhlaseny.

Navíc je zde možnost blokování aplikací dle informací o vydavateli nebo podle verze softwaru. Pokud například bude vyžadováno zablokovat všechny aplikace od Mozilly, nebude nutné jednu po druhé instalovat a poté blokovat jejich spuštění. Stačí z jednoho spustitelného souboru získat informace o příslušném vydavateli. Stejně tak může být zablokováno spouštění starých verzí programů.



Obrázek 5: Nástroj AppLocker

II. PRAKTICKÁ ČÁST

5 INSTALACE A KONFIGURACE SLUŽEB WINDOWS SERVER 2008 R2 S OHLEDEM NA BEZPEČNOST

Hlavním cílem praktické části je definovat skupinu postupů a nastavení Windows Server 2008 R2 a klientských systémů Windows 7, tak aby společně vytvářely celek, který bude nejen odpovídat současným standardům bezpečnosti, ale také poskytne dostatečné prostředky pro snadnou a efektivní administraci.

Nástroje a služby využité v této části budou vycházet ze současných prostředků daných operačních systémů. Budou rovněž prezentovány některé vlastnosti, které dřívější verze operačních systému firmy Microsoft neposkytovaly a které značně zvyšují užitnou hodnotu systému. S novými vlastnostmi jsou však spojena i nová rizika a tedy i nezbytnost aplikace nových prostředků zabezpečení.

Popsané nastavení je aplikováno v omezeném prostředí, kdy jsou k dispozici tři počítače, z nichž jeden slouží jako server a dva jsou v roli klientů využívající služeb serveru. Na serverovém počítači je nainstalován Windows Server 2008 R2 na němž jsou postupně aplikovány vybrané služby s ohledem na zabezpečení. Důležitou rolí a součástí systému Windows Server 2008 R2 je adresářová služba AD a konzola GPM, díky čemuž jsou centrálně spravovány klientské počítače a aplikovány zásady zabezpečení přičemž uživatelé těchto počítačů jsou dvojího typu, z nichž jeden má výraznější omezení.

Tato část práce tedy nabídne řadu postupů, které provedou instalací, konfigurací, zabezpečením jednotlivých služeb a klientských stanic.

5.1 Příprava serveru s ohledem na bezpečnost

Tato část diplomové práce se zabývá popisem přípravy jednotlivých služeb systému Windows Server 2008 R2 s ohledem na bezpečnost. Byla zde popsána instalace a konfigurace služeb:

- Active Directory Domain Services včetně DNS Serveru
- DHCP (Dynamic Host Configuration Protocol) Server
- Active Directory Certificate Services
- Vzdálená plocha (Remote Desktop Services)
- Windows Server Update Services

Základním předpokladem zabezpečení je, že počítače obsahují aktualizace systému, zapnutou a nakonfigurovanou bránu firewall a nainstalovaný antivirový program.

5.1.1 Instalace Active Directory Domain Services

ÚČEL: Instalace služby Active Directory Domain Services je nezbytností ve chvíli, kdy chceme plně využívat Zásady skupiny, jež jsou základním pilířem zabezpečení a usnadní centralizovanou správu systému.

Určitou výhodou tohoto postupu je že není nutné mít v síti dostupnou službu DNS neboť tento nedostatek je v průběhu instalace odstraněn. Nezbytnou podmínkou však je, aby počítač (server) byl připojen k síti.

POSTUP 1: Připojení serveru k síti

1. *Spravce serveru (Server Manager) – Zobrazit síťová připojení (Network Connections)*
2. *Připojení k místní síti (Local Area Connection) - pravé tlačítko myši - Vlastnosti (Properties)*
3. *Protokol TCP/IPv4 (Internet Protocol Version 4) - Vlastnosti (Propertis)*
4. *Zde byla nastavena adresu IP, síťová maska, ale výchozí brána a DNS byly ponechány nevyplněné – OK - Zavřít (Close)*
5. *Nastavení bylo ověřeno v Příkazovém řádku pomocí příkazu Ipconfig*

Poznámka: IP adresa byla nastavena na hodnotu *10.0.0.1* a síťová maska na hodnotu *255.0.0.0*.

POSTUP 2: Instalace binárních souborů služby AD DS

1. *Správce serveru (Server Manager) - v levý panel položka Role (Roles) - pravý panel tlačítko Přidat role (Add Roles)*
2. *Vybrat role serveru (Select Server Roles) - služba AD DS (Active Directory Domain Services) - Další (Next) - Instalovat (Install)*

POSTUP 3: Instalace služby Active Directory Domain Services

1. *Klávesová zkratka Windows + R - příkazem dcpromo.exe byl vyvolán průvodce instalací služby AD DS (AD DS Installation Wizard) – Další (Next)*

2. *Vyberte konfiguraci nasazení (Choose A Deployment Configuration) - volba Vytvořit novou doménu v nové doménové struktuře (Create a new domain in a new forest) – Další (Next)*
3. *Zde byl zadán plně kvalifikovaný název domény na stránce Název kořenové domény doménové struktury (Name the Forest Root Domain) – Další (Next)*

Poznámka: V této diplomové práci byla doména pojmenována *mdomain.cz*, jedná se o kořenovou doménu doménové struktury, tudíž se celá doménová struktura se jmenuje *mdomain.cz*.

4. *Úroveň funkčnosti doménové struktury byl zvolen na Windows Server 2008 – Další (Next)*

Poznámka: Úroveň funkčnosti Windows Server 2008 se nastavuje v případě, že v celé doménové struktuře budou nasazeny pouze doménové řadiče s operačním systémem Windows Server 2008, v opačném případě se volí nižší úroveň funkčnosti (Windows Server 2000 nebo Windows Server 2003).

5. *Na serveru se služba DNS nenachází, proto byla položka Server DNS (DNS Server) ponechána zatrhnutá - Další (Next)*

Poznámka: V případě, že počítač obsahuje více síťových adaptérů nebo má přiřazenu pouze statickou adresu IPv4, ale IPv6 nikoli, objeví se varování, že počítač má dynamicky přiřazenou adresu IP.

6. *Byla vybrána volba Ano, počítač bude používat dynamicky přiřazenou adresu IP (nedoporučuje se), (Yes, this server will use a dynamically assigned IP address (not recommended))*

Poznámka: V závislosti na zvoleném plně kvalifikovaném názvu domény se může objevit hláška, která upozorňuje, že na lokální síti neexistuje delegace v doméně vyšší úrovně, tedy cz. To však v lokální síti není nutné řešit, proto byla zvolena možnost Ano (Yes).

7. *Na další obrazovce bylo ponecháno defaultní umístění databáze a souborů protokolů služby Active Directory a také složky SYSVOL - Další (Next)*
8. *Poté bylo zadáno heslo správce režimu obnovení adresářových služeb - Další (Next) - Dokončit (Finish)*

Poznámka: Tento účet administrátora je odlišný od účtu doménového administrátora a je dostupný jen tehdy, když spustíme doménový řadič v režimu obnovení adresářových služeb. V takovém případě lze na doménovém řadiči použít lokální a nikoliv doménový uživatelský účet.

POSTUP 4: Synchronizace času v doméně

Server pro emulaci primárního řadiče domény v doménové struktuře byl nastaven na synchronizaci času s externím časovým serverem a to spuštěním příkazu:

w32tm /config /computer:server.mdomain.cz /manualpeerlist:time.windows.com /syncfromflags:manual /update

5.1.2 Zabezpečení adresářové služby

5.1.2.1 Zálohování a obnovení adresářové služby

POSTUP 5: Instalace Funkce služby Zálohování serveru

1. *Správce serveru (Server Manager) – levý panel Funkce – pravý panel Přidat funkce*
2. *Vybrat funkce – Funkce služby Zálohování systému – Další – Nainstalovat*

POSTUP 6: Záloha adresářových služeb pomocí příkazového řádku

1. *Start - Všechny programy (All Programs) - Příslušenství (Accessories) - pravé tlačítko na Příkazový řádek (Command Line) - Spustit jako správce (Run As Administrator)*
2. *V okně příkazového řádku následujícím příkazem byly vypsány připojené disky a tím zjištěny jejich identifikátory*

   C:\>wbadmin get disks

3. *Poté byl použit příkaz, který naplánoval úlohu zálohování na konkrétní čas, určil zálohovaná data a také cílový disk pro zálohu.*

   C:\>wbadmin enable backup -addtarget:{identifikátor} - schedule:23:00 –allcritical

Poznámka: Záloha byla naplánována na 23h a v tomto časovém úseku bude zálohovat všechna důležitá systémová data a cílem bude disk určený dříve získaným identifikátorem.

POSTUP 7: Běžná obnova adresářových služeb

1. *Restart řadiče domény pro obnovení - klávesa F8 - nabídka Rozšířené možnosti spuštění (Advanced Boot Options) - Režim obnoveni adresářových služeb (Directory Services Restore Mode) - Enter*

2. *Po objevení přihlašovacího okno, bylo zadáno jméno a heslo administrátora pro režim DSRM.*

Poznámka: Nejedná se o stejného administrátora jako administrátora domény. Heslo administrátora pro režim DSRM bylo zadáno v průběhu povýšení serveru na řadič domény.

3. *Příkazový řádek s oprávněními správce – příkaz vypisující dostupné sady záloh*

   C: \> wbadmin get versions

   V seznamu byla vyhledána záloha a uchován identifikátor verze.

4. *Zahájení operace obnovení stavu systému s určené verze zálohy pomocí příkazu*

   C:\>wbadmin start systemstaterecovery -version:verze

5. *Poté byla potvrzena obnova stavu systému klávesou A (Y). Po obnovení byl řadič restartován do normálního stavu*

5.1.3 Instalace role DHCP (Dynamic Host Configuration Protocol)

ÚČEL: Služba DHCP (Dynamic Host Configuration Protocol) poskytuje automatické přidělování IP adres jednotlivým klientským počítačům v počítačových sítích, čímž zjednodušuje jejich správu. Výhodou nasazení služby DHCP může být také fakt, že snižuje riziko chyby lidského faktoru neboť každý server DHCP si udržuje databázi adres IP a díky tomu ví, které adresy může klientům zapůjčit, které jsou zapůjčeny a které zapůjčeny nikdy nebudou.

POSTUP 8: Instalace role DHCP Server

1. *Správce serveru (Server Manager) - levý panel uzel Role (Roles) - pravý panel odkaz Přidat role (Add Roles) - Vybrat role serveru (Select Server Roles) – DHCP Server - Další (Next)*
2. *Na následující obrazovce byla ze seznamu síťových připojení vybrána statická adresa IP, která bude použita pro službu DHCP*

Poznámka: Statická adresa IP: 10.0.0.1.

3. *Na obrazovce Zadat nastavení protokolu IPv4 serveru DNS (Specify IPv4 DNS Server Settings) byly ponechány informace o serveru DNS – Další (Next)*

Poznámka: Nadřazená doména: mdomain.cz, IPv4 adresa upřednostňovaného serveru DNS: 10.0.0.1.

4. *Služba WINS byla ponechána nevyplněná, neboť nebude využívána – Další (Next)*
5. *Přidat nebo upravit obory DHCP (Add or Edit DHCP Scopes) - Další (Next) – Nainstalovat (Install) – Zavřít (Close)*
6. *Ověřit server DHCP – Použít aktuální pověření (*MDOMAIN\Administrator*)*

POSTUP 9: Autorizace serveru DHCP v doméně Active Directory

1. *Start – Nástroje pro správu (Administrative Tools) – DHCP*
2. *Levý panel konzoly DHCP – pravé tlačítko myši na název serveru – možnost Autorizovat (Authorize)*

POSTUP 10: Vytvoření oboru DHCP

1. *Start – Nástroje pro správu (Administrative Tools) – DHCP*
2. *Pravé tlačítko na IPv4 – položka Nový obor (New Scope) - Průvodce vytvořením oboru – Další (Next) - dále byl zadán název oboru – Další (Next)*
3. *Na obrazovce Rozsah adres IP (IP Address Range) byla zadána počáteční a koncová adresa IP a síťová maska – Další (Next)*

Poznámka: Název oboru: Obor, Počáteční adresa IP: 10.0.0.1, Koncová adresa IP: 10.0.0.254, Maska podsítě: 255.0.0.0, Výchozí brána: 10.0.0.1, Typ podsítě: Pevná síť (doba trvání zapůjčení bude 6 dnů).

4. *Na obrazovce Rozsah vyloučení (Add Exclusions) do polí Počáteční adresa IP (Start IP address) a Koncová adresa IP (End IP address) byla zadána statická adresa přidělená serveru – Přidat (Add) – Další (Next)*

Poznámka: Tím, že bylo do Rozsahu vyloučení (Add Exclusions) přidána statická adresa, jež byla přidělena severu, bylo zajištěno, že tato adresa se nebude přiřazovat klientům. Počáteční adresa IP: 10.0.0.1, Koncová adresa IP: 10.0.0.1.

5. *Doba zápůjčky adres IP byla nastavena na 1 týden – Další (Next)*
6. *Dále byla vybrána volba Ne, změním tyto možnosti později (No, I will configure these options later) – Další (Next) – Dokončit (Finish)*
7. *Pravé tlačítko myši na název oboru – Aktivovat (Activate)*

POSTUP 11: Nastavení možností DHCP

1. *Start – Nástroje pro správu (Administrative Tools) – DHCP*
2. *V levém panelu byl rozbalen název serveru DHCP – IPv4 – obor*
3. *Pravé tlačítko na Možnosti oboru (Scope Options) – položka Konfigurovat možnosti (Configure Options)*
4. *V okně Možnosti oboru (Scope Options) byla vybrána možnost Směrovač neboli výchozí brána – OK*

POSTUP 12: Vytvoření rezervace klienta DHCP

1. *Start – Nástroje pro správu (Administrative Tools) – DHCP*
2. *Byla rozbalena hierarchie DHCP až na úroveň oboru – Rezervace (Reservations) – pravé tlačítko myši na položku Nová rezervace (New Reservation)*
3. *Do nového dialogového okna byla zadána adresa IP, která bude vždy přidělena dále fyzická adresa neboli MAC adresa a název rezervace – Přidat (Add)*

Poznámka: Fyzická adresa neboli MAC adresa byla zjištěna na lokálním počítači pomocí příkazu *ipconfig /all*.

5.1.4 Zabezpečení role DHCP Server

Vzhledem k tomu, že DHCP není ověřovaný protokol, jsou adresy IP zapůjčeny každému uživateli připojenému k síti, který o ni zažádá. Neověřený uživatel tak může získat zápůjčku od libovolného klienta DHCP vždy, když server DHCP může zápůjčku poskytnout.

Jak již bylo popsáno v kapitole Bezpečnostní hrozby v části věnované hrozícím rizikům služby DHCP všichni nepovolaní uživatelé, kteří mají fyzický přístup do sítě využívající protokol DHCP, mohou na serverech DHCP vyvolat útok přetížením systému DoS (Denial

of Service) požadováním velkého počtu zápůjček ze serveru, čímž vyčerpají zápůjčky, které by byly jinak dostupné jiným klientům DHCP.

Vzhledem k těmto a dalším hrozícím rizikům je důležité se zabývat zabezpečením této služby, tak aby se rizika minimalizovala.

5.1.4.1 Záloha a obnovení serveru DHCP

ÚČEL: Služba DHCP Server obsahuje množství informací jako např. konfigurace serveru, vlastnosti oborů a aktuální zápůjčky. Výhodou jejich zálohování je možnost při jejich ztrátě obnovení do původního stavu.

POSTUP 13: Záloha serveru DHCP

1. *Start – Nástroje pro správu (Administrative Tools) – DHCP*
2. *V levém panelu byl vybrán server, který bude zálohován – pravé tlačítko myši byla vybrána možnost Zálohování (Backup)*
3. *V dialogovém okně Vyhledat složku (Browse For Folder) bylo vybráno umístění na jiném fyzickém disku, než na kterém ukládá automatické zálohy služba DHCP a tím byla vytvořena složka s názvem New a soubor DhcpCfg*

POSTUP 14: Obnovení serveru DHCP

1. *Start – Nástroje pro správu (Administrative Tools) – DHCP*
2. *V levém panelu byl vybrán server, na který budou obnovena zálohovaná data – pravé tlačítko myši - možnost Obnovení (Restore)*
3. *V dialogovém okně Vyhledat složku (Browse For Folder) byla vybrána složka s aktuální zálohou – poté klepnutím na tlačítko Ano (Yes) byl odsouhlasen restart služby DHCP*

5.1.5 Instalace role serveru NPS

ÚČEL: Služba Síťové zásady a přístup poskytuje architekturu NAP, což je technologie vytváření, vynucení a nápravy problémů zásad stavu klienta.

Konfigurace protokolu DHCP (Dynamic Host Configuration Protocol) - tento způsob vynucení NAPem je asi nejzranitelnější. NAP zde ve spolupráci se serverem DHCP zajišťuje, aby plnohodnotná adresa IP byla přidělena jen počítačům, které splňují požadavky na jejich stav. Pokud žádající počítač tyto požadavky nesplňuje, může mu být přidělena jiná adresa IP a počítač tak bude umístěn do tzv. nápravné sítě (remediation

network). V této nápravné síti je místo totálního odpojení od sítě počítači poskytnuta jakási možnost zjednat nápravu. Např. zde je možné z intranetového webu stáhnout a nainstalovat antivirovou aplikaci, aktualizace Windows apod.

POSTUP 15: Instalace role serveru NPS (Network Policy Server)

1. *Správce serveru (Server Manager) - levý panel uzel Role (Roles) - pravý panel tlačítko Přidat role (Add Roles) - Další (Next)*
2. *V seznamu byla vybrána role Služba Síťové zásady a přístup (Network Policy and Access Server) - Další (Next)*
3. *Na obrazovce Vybrat služby rolí (Select Role Services) - položka Server NPS (Network Policy Server) - Další (Next) - Nainstalovat (Install) - Zavřít (Close)*

5.1.5.1 Konfigurace serveru NAP pomocí průvodce

POSTUP 16: Konfigurace serveru NAP

1. *Start - Nástroje pro správu (Administrative Tools) - Server NPS (Network Policy Server)*
2. *V sekci Standardní konfigurace (Standard Configuration) - položka Architektura NAP (Network Access Protection) - Konfigurovat architekturu NAP (Configure NAP)*
3. *Na obrazovce Vybrat způsob připojení k síti, který bude použit s architekturou NAP (Select Network Connection Method for Use with NAP), byla vybrána možnost Pomocí protokolu DHCP (Dynamic Host Configuration Protocol (DHCP)) a v poli Název zásady (Policy name) byl ponechán automaticky vygenerovaný název - Další (Next)*
4. *Na obrazovce Zadat servery vynucení architektury NAP, na kterých je spuštěn produkt server DHCP (Specify NAP Enforcement Servers Running DHCP Server) je nutné zadat server DHCP, který bude spolupracovat se systémem NAP.*

Poznámka: V této diplomové práci je server DHCP umístěn na stejném serveru jako server NPS proto zde není nutné cokoliv zadávat. V případě, že by služba DHCP byla provozována na jiném serveru, bylo by nutné tento server přidat.

5. *Na obrazovce Zadat obory DHCP (Specify DHCP Scopes) byl seznam ponechán prázdný – Další (Next)*

Poznámka: Možnost Zadat obory DHCP (Specify DHCP Scopes) slouží pro definici oboru DHCP pro práci s NAP. Vzhledem k tomu, že obor není nastaven pro spolupráci se

systémem NAP, bude seznam ponechán prázdný, což způsobí, že později budou použity všechny obory DHCP, které mají povolenou spolupráci s NAP.

Seznam Skupiny počítačů (Machine Groups) byl ponechán také prázdný a díky tomu se později zásada použije na všechny počítače i uživatele.

6. *Skupina nápravných serverů (Remediation Server Group) - Další (Next)*
7. *Definovat zásady stavu architektury NAP (Define NAP Health Policy) – možnost Validátor stavu zabezpečení systému Windows (Windows Security Health Validator)*

   Ve spodní části téže obrazovky Omezení přístupu k síti pro klientské počítače neumožňující architekturu NAP (Network Access Restrictions for NAP-Ineligible client computers) byla vybrána možnost Odepřít klientským počítačům neumožňujícím architekturu NAP úplný přístup k síti a povolit pouze přístup k síti s omezením (Deny full network access to NAP-ineligible computers. Allow access to a restricted network only) - Další (Next) - Dokončit (Finish)

5.1.5.2 Povolení architektury NAP na oboru DHCP

POSTUP 17: Povolení architektury NAP na oboru DHCP

1. *Start - Nástroje pro správu (Administrative Tools) – DHCP - levý panel konzoly DHCP – obory - pravé tlačítko myši - Vlastnosti (Properties)*
2. *Záložka Architektura NAP (Network Access Protection) - Povolit pro tento obor (Enable for this scope) - Použít výchozí profil architektury NAP (Use default Network Access Protection profile) - OK*

5.1.5.3 Nastavení tříd DHCP pro použití s architekturou NAP

POSTUP 18: Nastavení tříd DHCP pro použití s architekturou NAP

1. *Start - Nástroje pro správu (Administrative Tools) – DHCP*
2. *Levý panel konzoly DHCP – obory - pravé tlačítko myši na Možnosti oboru (Scope Options) - Konfigurovat možnosti (Configure Options) - záložka Upřesnit (Advanced) - Třída uživatele (User class) - položka Výchozí uživatelská třída (Default User Class)*

   V seznamu Možnosti k dispozici (Available Options) - položka 006 Servery DNS (DNS Servers) - do pole Adresa IP (IP Address) byla zadána adresa IP serveru DNS - položka 015 Doménový název DNS (DNS Domain Name) - do pole Hodnota

řetězce (String value) byl zadán název DNS domény, který bude přidělován prověřeným klientům

Poznámka: V této diplomové práci byla použita IP adresa DNS serveru *10.0.0.1* a název domény DNS *mdomain.cz*.

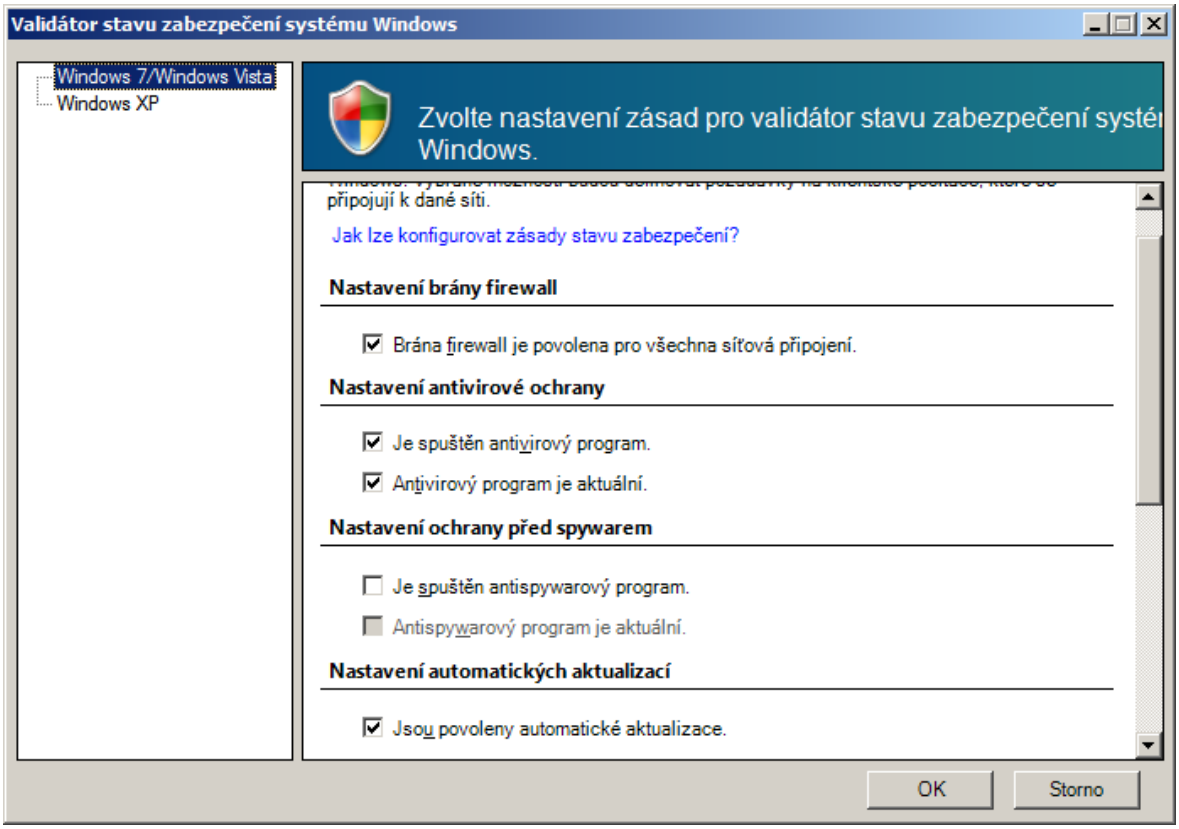
3. *Možnosti oboru (Scope Options) - Třída uživatele (User class) - Výchozí třída architektury NAP (Default Network Access Protection Class) - 006 Servery DNS (DNS Servers) - do pole Adresa IP (IP Address) byla zadána adresa serveru DNS - 015 Doménový název DNS (DNS Domain Name) - do pole Hodnota řetězce (String value) byl zadán odlišný název domény DNS pro klienty, kteří nesplňují požadavky validátoru stavu systému – OK*

Poznámka: IP adresa DNS serveru: *10.0.0.1* a název domény DNS: *restricted.mdomain.cz*.

5.1.5.4 Vytvoření validátoru stavu systému

POSTUP 19: Vytvoření validátoru stavu systému

1. *Start - Nástroje pro správu (Administrative Tools) - Server NPS (Network Policy Server)*
2. *Levý panel konzoly uzel Architektura NAP (Network Access Protecttion) - Validátory stavu systému (System Health Validators) - Validátor stavu zabezpečení systému Windows (Windows Security Health Validator) – Nastavení – Výchozí konfigurace - OK*



Obrázek 6: Nastavení validátoru stavu zabezpečení systému Windows

Poznámka: V nastavení validátoru stavu zabezpečení byly definovány požadavky, které musí klienti splňovat. Definované požadavky: Nastavení brány firewall, Nastavení antivirové ochrany a Nastavení automatických aktualizací.

5.1.5.5 Konfigurace klienta systému NAP prostřednictvím zásad skupiny

POSTUP 20: Konfigurace klienta systému NAP prostřednictvím zásad skupiny

1. *Start - Nástroje pro správu (Administrative Tools) - Správa zásad skupiny (Group Policy Management) - Objekty zásad skupiny (Group Policy Objects) - pravé tlačítko myši - Nový (New) - do políčka Název (Name) byl zadán název objektu - OK*

Poznámka: Nový objekt zásad skupiny v doméně byl propojen s organizační jednotkou Zamestnanci. Pojmenování nového objektu zásad: Zásady NAP.

2. *Pravé tlačítko na objekt Zásady NAP - Upravit (Edit) - v editoru zásad – Konfigurace počítače (Computer Configuration) - Zásady (Policies) - Nastavení systému Windows (Windows Settings) - Nastavení zabezpečení (Security Settings) - Systémové služby (System Services) – pravý panel – pravé tlačítko myši na službu Agent architektury NAP (Network Access Protection), (Network Access Protection*

Agent) - možnost Vlastnosti (Properties) - Definovat toto nastavení zásad (Define these policy settings) - Automaticky (Automatic) - OK

3. *Network Access Protection - Konfigurace klienta NAP (NAP Client Configuration) - Klienti vynucení (Enforcement Clients) – pravý panel – pravé tlačítko myši na položku Součást DHCP Quarantine Enforcement Client (DHCP Quarantine Enforcement Client) - Povolit (Enable) – levý panel – pravé tlačítko myši na položku Konfigurace klienta NAP (NAP Client Configuration) - Aktualizovat*
4. *Editor zásad - Konfigurace počítače (Computer Configuration) - Zásady (Policies) - Šablony pro správu (Administrative Templates) - Součásti systému Windows (Windows Components) - Centrum zabezpečení (Security Center) – pravý panel – pravé tlačítko myši na položku Zapnout centrum zabezpečení (pouze počítače v doméně) (Turn On Security Center (Domain PCs only)) - Upravit (Edit) – Povoleno (Enabled) - OK*

5.1.6 Instalace role AD CS (Active Directory Certificate Services)

POSTUP 21: Instalace role AD CS

1. *Správce serveru (Server Manager) - levý panel - Role (Roles) - pravý panel - Přidat role (Add Roles) - Služba AD CS (Active Directory Certificate Services) - Další (Next)*
2. *Vybrat služby rolí (Select Role Services) - Certifikační autorita (Certification Authority) - Webový zápis k certifikační autoritě (Certification Authority Web Enrollment)*

Poznámka: Při výběru služby role Webový zápis k certifikační autoritě (Certification Authority Web Enrollment) bude zobrazen dotaz na instalaci potřebných služeb rolí a funkcí.

3. *Přidat požadované služby rolí (Add Required Role Services) - Další (Next)*
4. *Na obrazovce Zadat typ instalace (Specify Setup Type) - Rozlehlá síť (Enterprise) - Další (Next)*

   Dále byla vybrána volba Kořenová certifikační autorita (Root CA), neboť je to první CA v síti - Další (Next)
5. *Na obrazovce Nastavit privátní klíč (Set Up Private Key) - Vytvořit nový privátní klíč (Create a new private key) - Další (Next)*

6. *Na obrazovce Konfigurovat kryptografii pro certifikační autoritu (Configure Cryptography for CA) byly nastaveny možnosti zprostředkovatele kryptografických služeb, délku klíče a algoritmus hash - Další (Next)*

Poznámka: Zprostředkovatel kryptografických služeb: RSA#Microsoft Software Key Storage Provider, Délka klíče: 4096, Algoritmus hash: sha1

7. *Na obrazovce Konfigurovat název certifikační autority (Configure CA Name) - Další (Next)*
8. *Nastavit období platnosti (Set Validity Period) – Další (Next)*

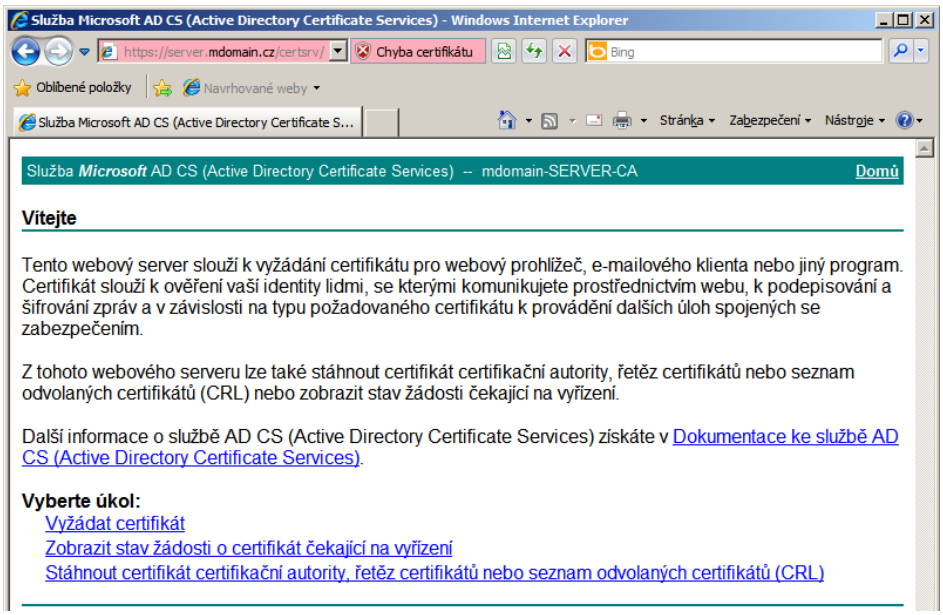
Poznámka: Hodnota platnosti byla nastavena na dobu 10 let, neboť CA nemůže vydat certifikát s platností delší, než je její vlastní platnost.

9. *Na obrazovce Konfigurovat databázi certifikátů (Configure Certificate Database) - Další (Next) - Nainstalovat (Install) - Zavřít (Close)*

5.1.6.1 Vygenerování uživatelského certifikátu prostřednictvím webu

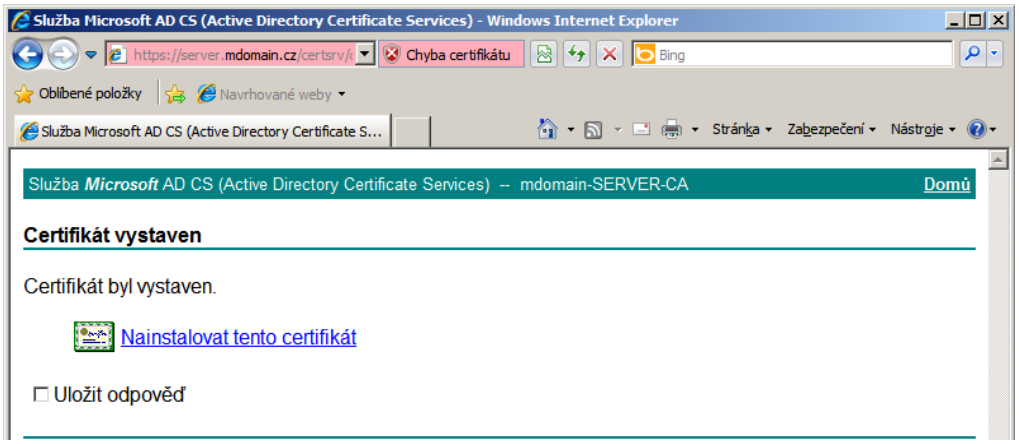
POSTUP 22: Vygenerování uživatelského certifikátu prostřednictvím webu

1. *Do internetového prohlížeče byla zadána adresa URL serveru CA: https://server.mdomain.cz/certsrv*



Obrázek 7: Vygenerování uživatelského certifikátu

2. *Vyžádat certifikát (Request Certificate) - Uživatelský certifikát (User Certificate) - Odeslat (Submit) - Ano (Yes) - Nainstalovat tento certifikát (Install this certificate) – Ano (Yes)*



Obrázek 8: Vystavení a instalace certifikátu

5.1.6.2 Povolení automatického přidělování certifikátů

POSTUP 23: Povolení automatického přidělování certifikátů

1. *Start – Nástroje pro správu (Administrative Tools) – Správa zásad skupiny (Group Policy Management)*
2. *Pravé tlačítko myši na objekt zásad skupiny s názvem Default Domain Policy – Upravit (Edit)*
3. *Editor správa zásad skupiny (Group Policy Management Editor) – Konfigurace počítače (Computer Configuration) – Zásady (Policy) – Nastavení systému Windows (Windows Settings) – Nastavení zabezpečení (Security Settings) – Zásady veřejných klíčů (Public Key Policies)*
4. *Pravý panel – pravé tlačítko myši na Klient certifikační služby-automatický zápis (Certificate Services Client-Auto-Enrollment) – Vlastnosti (Properties) – Povolit (Enabled) – volby „Obnovovat certifikáty, jejichž platnost vypršela, aktualizovat čekající certifikáty a odebírat odvolané certifikáty“ a „Aktualizovat certifikáty, které používají šablony certifikátů“ – OK*
5. *Start – Nástroje pro správu (Administrative Tools) – Certification Authority – levý panel – pravé tlačítko myši na název certifikační autority – Vlastnosti (Properties)*
6. *Modul zásad (Policy Module) – Vlastnosti (Properties) – „Pokud je to možné postupovat podle nastavení v šabloně certifikátů, jinak automaticky vydat certifikát*

(Follow the settings in the certificate template, if applicable. Otherwise, automatically isme the certificate)“ – OK

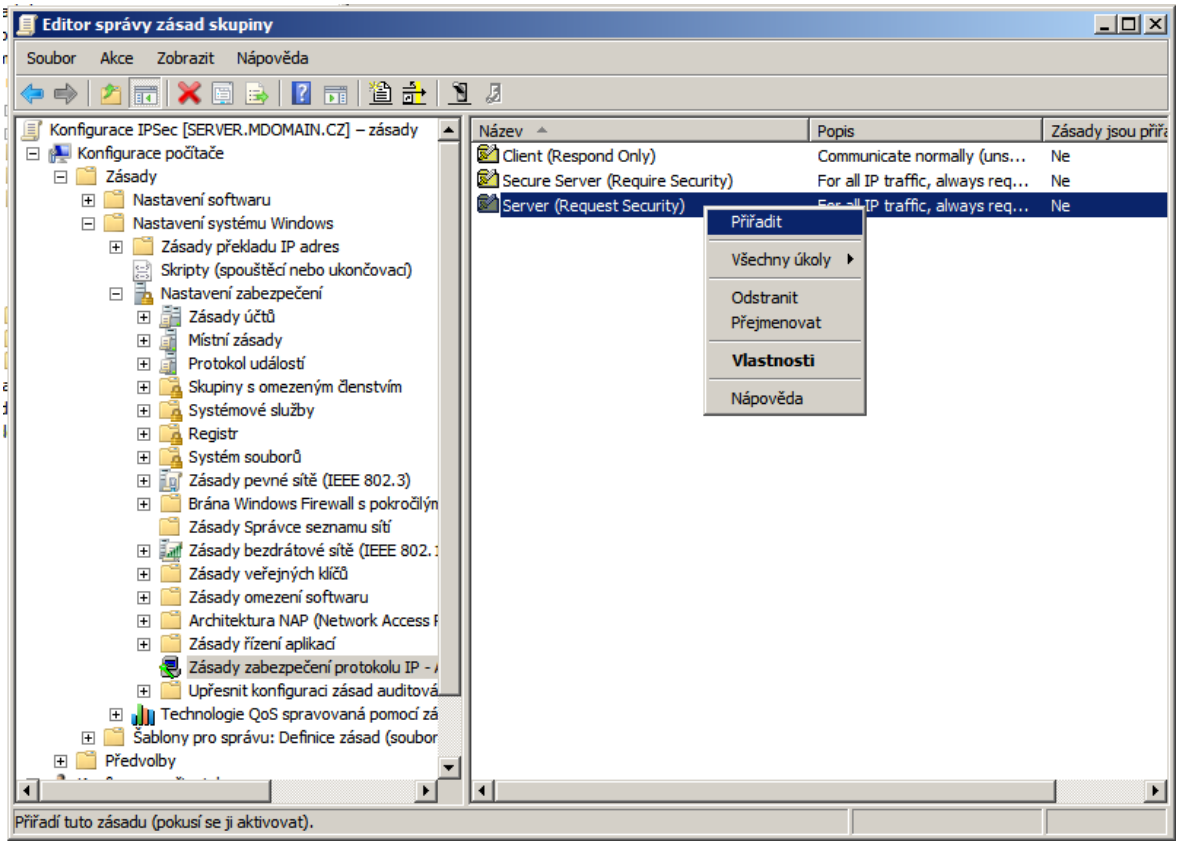
5.1.7 Zabezpečení síťového provozu pomocí protokolu IPSec

5.1.7.1 Nasazení zabezpečené komunikace prostřednictvím zásad skupiny

1. *Start - Nástroje pro správu (Administrative Tools) - Správa zásad skupiny (Group Policy Management) – levý panel – pravé tlačítko myši na organizační jednotku, v níž jsou umístěni uživatelé - Vytvořit objekt zásad skupiny v této doméně a propojit jej sem (Create a GPO in this domain and Link it here)*

Poznámka: Nově vytvořený objekt zásad skupiny byl pojmenován Konfigurace IPSec pro klienty.

2. *Pravé tlačítko myši na nově vytvořený objekt zásad skupiny - Upravit (Edit)*
3. *V editoru zásad rozbalte - Konfigurace počítače (Computer Configuration) - Zásady (Policies) - Nastavení systému Windows (Windows Settings) - Nastavení zabezpečení (Security Settings) - Zásady zabezpečení protokolu IP - Active Directory (IP Security Policies on Active Directory) - Server (Request Security) – Přidělit (Assign)*



Obrázek 9: Nasazení zabezpečené komunikace prostřednictvím zásad skupiny

5.1.8 Instalace role Vzdálená plocha (Remote Desktop Services)

ÚČEL: Vzdálená služba operačního systému Microsoft Windows Server 2008 R2 je mechanizmus vzdáleného řízení, správy a využívání serverů. Výhodami instalace této služby je škálovatelnost, schopnost obsloužit větší množství připojení, poskytnutí vzdálených aplikací neboli RemoteApps, možnost přistupovat k vzdálené ploše i vzdáleným aplikacím prostřednictvím webového rozhraní serveru nebo přístup k počítačům umístěným na vnitřní síti (např. za branou firewall) prostřednictvím Hostitele relací VP s nainstalovanou komponentou Brána VP.

POSTUP 24: Instalace role Vzdálená plocha

1. *Správce serveru (Server Manager) - levý panel uzel Role (Roles) - pravý panel odkaz Přidat role (Add Roles) - Vybrat role serveru (Select Server Roles) – Vzdálená plocha (Remote Desktop Services) - Další (Next)*
2. *Na další obrazovce ze seznamu služeb rolí serveru Vzdálená plocha byl vybrán Hostitel relací vzdálené plochy (dříve označovaný Terminálový server)*
3. *Na obrazovce Zadat metodu ověření pro vzdálený server (Specify Authentication Method for Remote Desktop Server) byla vybrána volba Požadování ověření na*

úrovni sítě (Require Network Level Authentication), což je bezpečnější metoda ověřování

4. *Na další obrazovce Výběr režimu licencování byla zvolena položka Konfigurovat později (Configure later) - Další (Next)*

Poznámka: Po zvolení volby Konfigurovat později (Configure later) začne běžet 120denní „bezlicenční" období. Po uplynutí této doby přestane terminálový server fungovat jako terminálový server, neboť Připojení pomocí klienta vzdálené plochy bude omezen na dvě současná připojení. K tomu, aby mělo vůbec smysl službu Vzdálená plocha nasazovat, jsou potřeba klientské licence VP CAL.

5. *Dále bylo ponecháno výchozí nastavení tedy skupina Administrators, které je dovoleno vzdáleně se připojit k tomuto vzdálenému serveru - Další (Next) - Instalovat (Install)*

Poznámka: Toto nastavení bude později změněno tak, že přidáme uživatele do skupiny Remote Desktop Users.

5.1.8.1 Zveřejnění aplikací RemoteApp

ÚČEL: Výhodou aplikace RemoteApp je, že uživatelé ani administrátoři nemusejí instalovat aplikace na klientské počítače a tím se snižují nároky na hardwarové vybavení klientských počítačů a také jednou z dalších výhod převážně pro správce je, že aplikace jsou spravovány z jednoho umístění.

POSTUP 25: Zveřejnění aplikací RemoteApp

1. *Start – Nástroje pro správu (Administrative Tools) – Vzdálená plocha (Remote Desktop Service) – Správce vzdálených aplikací RemoteApp (RemoteApp Manager)*
2. *Pravý panel konzoly - Přidat aplikace RemoteApp (Add RemoteApp Programs) - Další (Next) a poté ze seznamu dostupných aplikací byly vybrány aplikace, které byly přidány do seznamu programů RemoteApp - Další (Next) - Dokončit (Finish)*

Poznámka: Vybrané aplikace pro demonstraci: WordPad, Malování, Kalkulačka

5.1.8.2 Vytvoření instalačního balíčku MSI

ÚČEL: Výhodou vytvoření instalačního balíčku MSI z pohledu správce je instalace těchto balíčků MSI pomocí zásad skupin a také je pomocí zásad skupin centrálně spravovat. Z pohledu uživatele je to hlavně fakt, že dané aplikace najde v nabídce Start.

POSTUP 26: Vytvoření instalačního balíčku MSI

1. *Start - Nástroje pro správu (Administrative Tools) - Vzdálená plocha (Remote Desktop Services) - Správce vzdálených aplikací RemoteApp (RemoteApp Manager)*
2. *Vybrané programy RemoteApp - tlačítko Vytvořit balíčky Instalační služby systému Windows (Create Windows Installer Package) – Zadat nastavení balíčků – Zadat umístění pro uložení balíčků - Další (Next)*
3. *Na obrazovce s názvem Konfigurovat distribuční balíček (Configure Distribution Package) bylo ponecháno výchozí umístění v nabídce Start, konkrétně v kategorii Vzdálené programy (Remote Programs) a zatrhnuta možnost Plocha – Další (Next) – Dokončit (Finish)*

Poznámka: Balíček MSI byl uložen do složky Packaged Programs na němž bylo nakonfigurováno sdílení, aby klienti mohli přistupovat k MSI balíčkům.

V možnostech nastavení je také možné změnit umístění nebo umožnit převzetí klientských přípon souborů, takže při povolení tohoto nastavení bude např. při otevření dokumentu s příponou .rtf spuštěna vzdálená aplikace namísto té místní.

5.1.8.3 Implementace jednotného přihlášení (Single Sign-On)

ÚČEL: Výhodou jednotného přihlášení (Single Sign-On) je, že uživatelé nemusí opakovaně zadávat uživatelská jména a hesla.

POSTUP 27: Nastavení jednotného přihlášení (Single Sign-On)

1. *Start - Nástroje pro správu (Administrative Tools) - Správa zásad skupiny (Group Policy Management)*
2. *Pravé tlačítko myši na Objekty zásad skupiny (Group Policy Objects) - Nový (New) – objekt zasad skupiny byl propojen s organizační jednotkou Zamestnanci*
3. *Do políčka Název (Name) zadáme název objektu - OK*

Poznámka: Pojmenování GPO (Objekt zásad skupiny): SingleSingOn

4. *Klepnutím na nově vytvořený objekt zásad skupiny pravým tlačítkem myši byla zvolena možnost Upravit (Edit) - Konfigurace počítače (Computer Conflguration) - Zásady (Policies) - Šablony pro správu (Administrative Templates) - Systém (System) - Delegování pověření (Credentials Delegation)*
5. *Byla vybrána zásada s názvem Povolit delegování výchozích pověření (Allow Delegating Default Credentials) - pravé tlačítko myši - Vlastnosti (Properties) - Povoleno (Enabled) - Zobrazit (Show)*

6. *Na následující obrazovce byl nadefinován vzdálený server ve tvaru TERMSRV/server, na kterém byl povolen přístup pomocí delegovaných výchozích pověření – OK*

Poznámka: TERMSRV/server.mdomain.cz.

7. *V následujícím dialogovém okně bylo ověřeno zatržení políčka Zřetězit výchozí operační systém s výše uvedeným vstupem (Concatenate OS defaults with input above) - OK*

5.1.9 Zabezpečení Vzdálené plochy (Remote Desktop Services)

Jak již bylo uvedeno v kapitole Bezpečnostní hrozby v oddílu Specifická rizika služeb Windows Server 2008 R2, ve chvíli kdy je na serveru nainstalována služba Vzdálená plocha (Remote Desktop Services) je poskytnuta klientům možnost vzdáleného připojení k serveru. Tuto možnost však mohou zkoušet využít i neoprávnění uživatelé a proto je nutné danou službu zabezpečit, tak aby minimalizovala možné riziko.

5.1.9.1 Konfigurace Brány Vzdálená plocha (Remote Desktop Gateway)

ÚČEL: Hlavní funkcí Brány Vzdálená plocha je umožnit přístup uživatelům z vnější sítě ke službám např. RemoteApps běžící na vnitřní síti, která je chráněna firewallem. Výhodou využití Brány Vzdálená plocha je že umožňuje zapouzdření datového provozu při jeho přenosu přes Internet do protokolu SSL (port 443) a po překonání vnějšího firewallu jsou tato data opět vybalena do původní podoby protokolu RDP (Remote Desktop Protocol), (port 3389) a dále předána cílovým vzdáleným serverům.

POSTUP 28: Konfigurace Brány Vzdálená plocha (Remote Desktop Gateway)

1. *Správce serveru (Server Manager) - levý panel uzel Role (Roles) - položka Vzdálená plocha (Remote Desktop Services)*
2. *Na obrazovce Vybrat služby rolí (Select Role Services) - Brána Vzdálená plocha (Remote Desktop Gateway) bylo potvrzeno přidání požadovaných doplňujících funkcí - Další (Next)*
3. *Byla zvolena možnost Vytvořit certifikát podepsaný svým držitelem pro šifrování SSL (Create a self-signed certificate for SSL ecryption) - Další (Next)*

Poznámka: Síťový provoz mezi klientem a Bránou TS probíhá v šifrované podobě pomocí SSL.

4. *Na stránce konfigurace zásad autorizace byla zvolena možnost Později (Later) - Další (Next) - Nainstalovat (Install)*

5.1.9.2 Nasazení certifikátu SSL pro bránu Vzdálená plocha

ÚČEL: SSL (Secure Sockets Layer) je protokol, který poskytuje zabezpečenou komunikaci šifrováním a autentizaci komunikujících stran. Vzhledem k tomu, že v předchozím postupu byla zvolena možnost Vytvořit certifikát podepsaný svým držitelem pro šifrování SSL (Create a self-signed certificate for SSL ecryption) je nutné přidat klientským počítačům certifikát serveru do seznamu důvěryhodných certifikačních autorit.

POSTUP 29: Nasazení certifikátu SSL pro bránu Vzdálená plocha

1. *Windows+R - příkaz mmc (Microsoft Management Console) - Soubor (File) - Přidat nebo odebrat modul snap-in (Add/ Remove Snap-in) - modul Certifikáty (Certificates) - tlačítko Přidat (Add) - Účet počítače (Computer account) - Další (Next)- v okně Vybrat počítač (Select Computer) - položka Místní počítač (Local Computer) - tlačítko Dokončit (Finish) - OK*
2. *Levý panel konzoly - Certifikáty (Místní), (Certificates (Local)) - Osobní (Personal) - Certifikáty (Certificates). Zde byl vybrán certifikát shodný s názvem serveru - pravé tlačítko myši - položka Všechny úkoly (All Tasks) - Exportovat (Export)*
3. *Na obrazovce s názvem Soubor pro export (File to Export) pomocí tlačítka Procházet (Browse) byl zadán název a umístění souboru, do kterého byl certifikát exportován - Další (Next) - Dokončit (Finish)*
4. *Start - Nástroje pro správu (Administrative Tools) - Správa zásad skupiny (Group Policy Management)*
5. *Pravé tlačítko na organizační jednotku OU, do které byly umístěny účty počítačů, na které bude aplikováno nastavení - položka Upravit (Edit)*
6. *Konfigurace počítače (Computer Configuration) - Zásady (Policies) - Nastavení systému Windows (Windows Settings) - Nastavení zabezpečení (Security Settings) - Zásady veřejných klíčů (Public Key Policies) - pravé tlačítko myši na Důvěryhodné kořenové certifikační úřady (Trusted Root Certification Authorities) - možnost Importovat (Import) soubor obsahující vyexportovaný certifikát*
7. *Na stránce Úložiště certifikátů (Certificate Store) je automaticky vybrána volba Všechny certifikáty v následujícím úložišti - Důvěryhodné kořenové certifikační úřady (Place all certificates in the following store-Trusted Root Certificate Authorities) - Další (Next) - Dokončit (Finish)*

5.1.9.3 Vytvoření zásady autorizace připojení a prostředků

ÚČEL: Při instalaci služby Brána Vzdálené plochy bylo určeno, že později budou nastaveny zásady autorizace připojení a zásady autorizace prostředků, díky nimž bude Brána Vzdálené plochy schopna určit, kdo se smí jeho prostřednictvím připojit a kdo ne.

POSTUP 30: Vytvoření zásady autorizace připojení a zásady autorizace prostředků

1. *Start - Nástroje pro správu (Administrative Tools) – Vzdálená plocha (Remote Desktop Services) - Správce brány Vzdálená plocha (Remote Desktop Gateway Manager)*
2. *Levý panel konzoly správce - Název serveru - Zásady (Policies) – pravé tlačítko myši na položku Zásady autorizace připojení (Connection Authorization Policies) - Vytvořit novou zásadu (Create New Policy) - Průvodce (Wizard)*
3. *Vytvořit zásady CAP ke Vzdálené ploše a VP pro autorizaci prostředků (doporučeno) - Další (Next) - na další obrazovce byl zadán název zásady - Další (Next)*
4. *Dále byly nadefinovány požadavky pro autorizaci připojení. Bylo nastaveno ověřování heslem a přístup povolen jen skupině Domain Admins – Další (Next)*
5. *Na obrazovce Přesměrování zařízení (Device Redirection) je možnost vybrat, u kterých zařízení bude povoleno jejich přesměrování. Byla vybrána možnost Povolit přesměrování pro všechna klientská zařízení - Další (Next)*
6. *Druhá polovina průvodce se věnuje nastavením zásad autorizace prostředků. Na první stránce byl zadán název zásady - Další (Next)*
7. *Na obrazovce s názvem Skupina počítačů (Computer Group) byla vybrána třetí možnost, která umožňuje připojení k libovolným síťovým prostředkům - Další (Next)*
8. *Na obrazovce Povolené porty (Allowed Ports) byla ponechána výchozí možnost, kdy připojení bude realizováno pomocí portu protokolu RDP, kterým je port 3389 - Další (Next) - Dokončit (Finish)*

Poznámka: Název zásady autorizace připojení: CAP, název zásady autorizace prostředků: VP

5.1.10 Instalace role Windows Server Update Services

ÚČEL: Pomocí služby WSUS mohou správci plně spravovat aktualizace vydané prostřednictvím služby Microsoft Update do počítačů v síti.

POSTUP 31: Instalace role WSUS

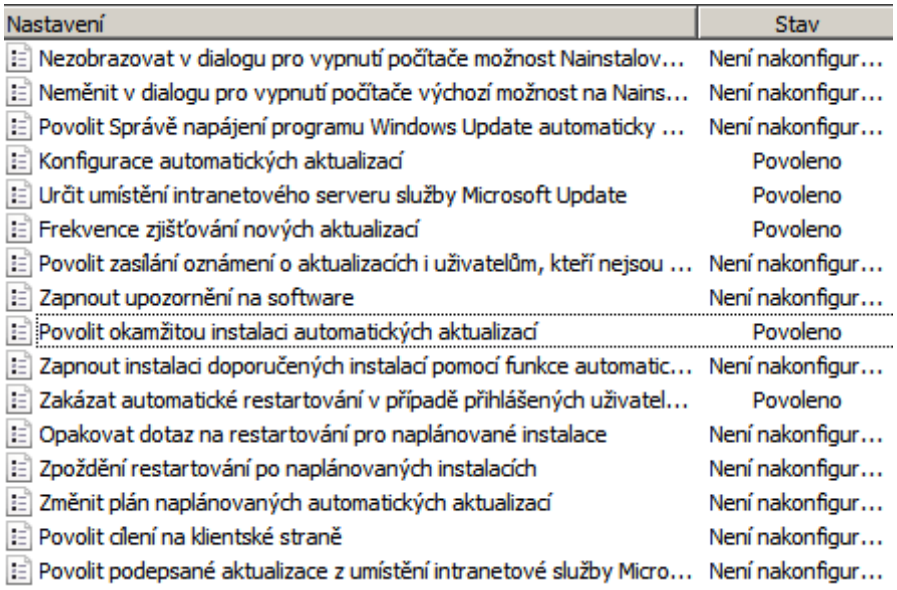
1. *Správce serveru (Server Manager) - levý panel uzel Role (Roles) - pravý panel odkaz Přidat role (Add Roles) - Vybrat role serveru (Select Server Roles) – WSUS (Windows Server Update Services) - Další (Next) - S podmínkami licenční smlouvy souhlasím – Další*
2. *Na stránce Vyberte zdroj aktualizace - Ukládat aktualizace místně (D:/WSUS) – Další*
3. *Na stránce Možnosti databáze – Další – Dokončit*

POSTUP 32: Konfigurace WSUS

1. *Start – Nástroje pro správu – Windows Server Update Services*
2. *Levý panel - Možnosti – Průvodce konfigurací služby WSUS – Další – Připojit k serveru pro odeslání dat – Spustit připojení – stahovat aktualizace pouze v těchto jazycích – čeština – Další – Vybrat programy – Další – Aktualizace – Další – Synchronizovat automaticky – Další – Dokončit*
3. *Souhrnné hlášení – Nezahrnout stav ze serveru pro příjem dat replik – OK*
4. *Průvodce vyčištěním serveru služby WSUS – Další – Dokončit*
5. *Aktualizace schválení – Nové pravidlo – Pokud je aktualizace součástí určitého produktu – libovolný produkt – Windows 7 – všechny počítače – Název: Automatické schválení Windows 7 – OK*

POSTUP 33: Konfigurace GPO WSUS v zásadách skupiny

1. *Start – Nástroje pro správu – Správce zásad skupiny – Vytvoření GPO na úrovni domény – Název: WSUS – OK*
2. *Pravé tlačítko myši na WSUS – Upravit – Šablony pro správu – Součásti systému Windows – Windows Update – Konfigurace – automatické aktualizace – Povoleno – Automaticky stahovat a plánovat instalaci (Každý den v 12hod)*
3. *Určení umístění intranetové služby Microsoft update – Povoleno – bylo vepsáno http://server:8530 – opět zopakovat – OK*
4. *Zakázat automatické restartování u přihlášených uživatelů po plánovaných instalacích automatických aktualizací – Povoleno – OK*
5. *Frekvence zjišťování nových aktualizací – Povoleno – OK*
6. *Povolit okamžitou instalaci automatických aktualizací – Povoleno – OK*



Nastavení	Stav
Nezobrazovat v dialogu pro vypnutí počítače možnost Nainstalov…	Není nakonfigur…
Neměnit v dialogu pro vypnutí počítače výchozí možnost na Nains…	Není nakonfigur…
Povolit Správě napájení programu Windows Update automaticky …	Není nakonfigur…
Konfigurace automatických aktualizací	Povoleno
Určit umístění intranetového serveru služby Microsoft Update	Povoleno
Frekvence zjišťování nových aktualizací	Povoleno
Povolit zasílání oznámení o aktualizacích i uživatelům, kteří nejsou …	Není nakonfigur…
Zapnout upozornění na software	Není nakonfigur…
Povolit okamžitou instalaci automatických aktualizací	Povoleno
Zapnout instalaci doporučených instalací pomocí funkce automatic…	Není nakonfigur…
Zakázat automatické restartování v případě přihlášených uživatel…	Povoleno
Opakovat dotaz na restartování pro naplánované instalace	Není nakonfigur…
Zpoždění restartování po naplánovaných instalacích	Není nakonfigur…
Změnit plán naplánovaných automatických aktualizací	Není nakonfigur…
Povolit cílení na klientské straně	Není nakonfigur…
Povolit podepsané aktualizace z umístění intranetové služby Micro…	Není nakonfigur…

Obrázek 10: Nastavení aktualizací v zásadách skupiny

5.2 Příprava organizačních jednotek a uživatelů v AD DS

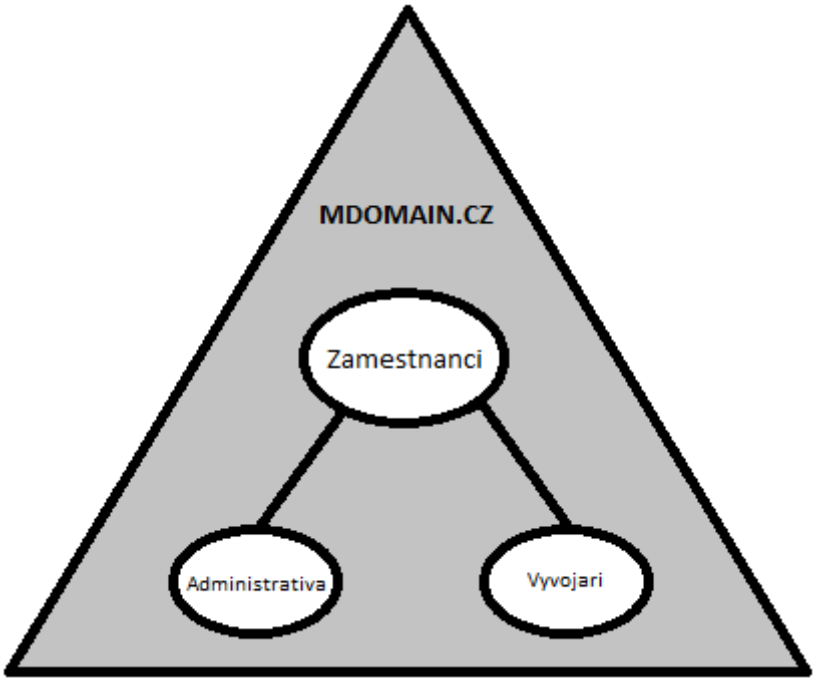
Tato část praktické části se zabývá strukturou a tvorbou organizačních jednotek a uživatelů. Bude vytvořena organizační jednotka Zamestnanci v níž budou dvě vnořené organizační jednotky nazvané Administrativa a Vyvojari. Součástí OU Administrativa bude uživatel Sekretarka, na nějž budou aplikovány takové zásady zabezpečení, aby tento uživatel měl menší oprávnění než uživatel Vyvojar, jež bude součástí OU Vyvojari.

5.2.1 Vytvoření organizačních jednotek

POSTUP 34: Vytvoření organizačních jednotek (OU)

1. *Start - Nástroje pro správu (Administrative Tools) - Uživatelé a počítače služby Active Directory (Active Directory Users and Computers)*
2. *Levý panel – pravé tlačítko myši na doménu – Nová položka (New) – organizační jednotka – Název – Chránit kontejner před náhodným odstraněním*

Poznámka: Pomocí tohoto postupu byla vytvořena organizační jednotka Zamestnanci do níž byly stejným způsobem vytvořeny další dvě organizační jednotky nazvané Administrativa a Vyvojari. Znázorněno na Obrázku 11.



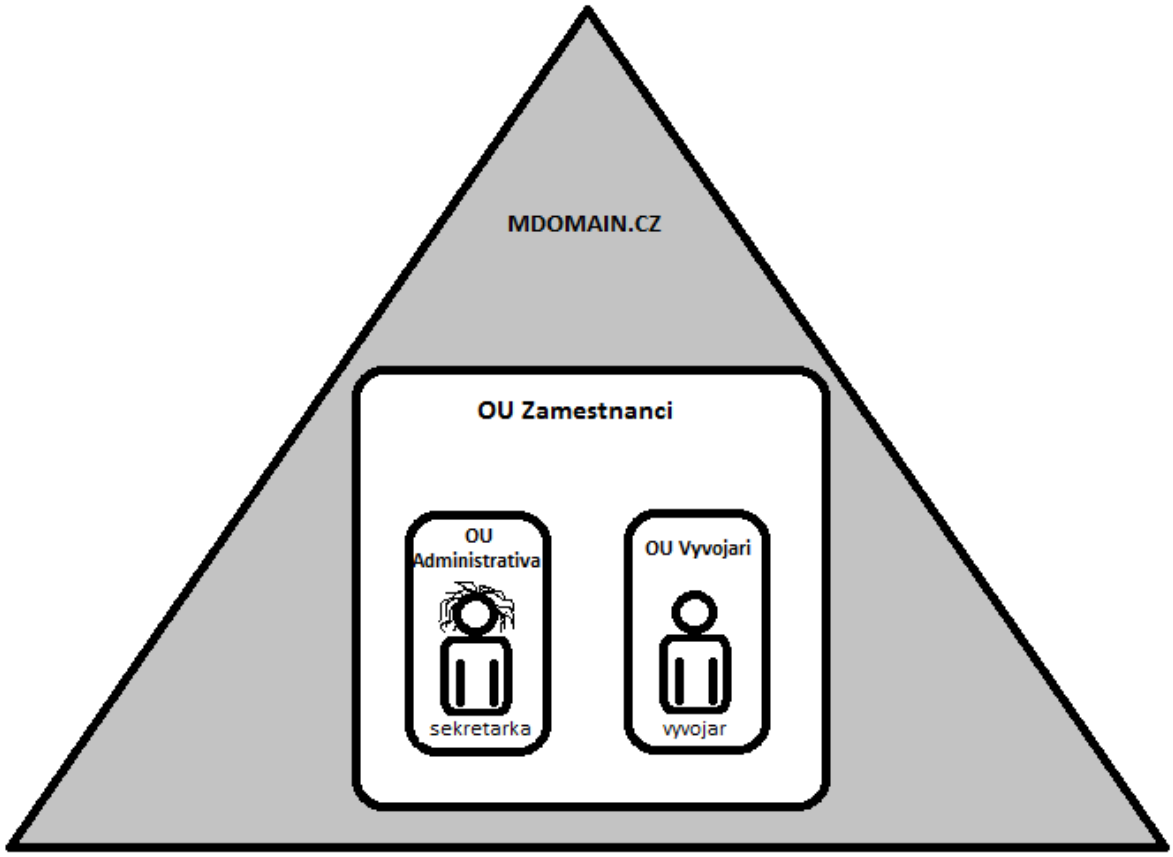
Obrázek 11: Organizační jednotky v rámci domény

5.2.2 Vytvoření uživatelských účtů

POSTUP 35: Vytvoření uživatelských účtů

1. *Start - Nástroje pro správu (Administrative Tools) - Uživatelé a počítače služby Active Directory (Active Directory Users and Computers)*
2. *V levém panelu v struktuře domény byla označena organizační jednotka Zamestnanci – pravé tlačítko na Administrativa - Nová položka (New) - Uživatel (User)*
3. *V dialogovém okně Nový objekt-Uživatel (New Object-User) bylo vyplněno přihlašovací uživatelské jméno a Jméno (First name) - Další (Next)*

Poznámka: Pomocí tohoto postupu byly vytvořeny účty *sekretarka* v organizační jednotce Administrativa a *vyvojar* v organizační jednotce Vyvojari. Znázorněno na Obrázku 12.



Obrázek 12: Struktura prostředí v Active Directory

4. *Na další obrazovce bylo zadáno heslo a do pole Potvrzení hesla (Password Confirmation) bylo zadáno opětovně - Další (Next) – Dokončit (Finish)*

Poznámka: Zadané heslo musí splňovat požadavky na komplexitu hesla. Ve výchozím stavu to znamená, že heslo musí obsahovat alespoň 3 z celkového počtu 4 kategorií znaků (malá písmena, velká písmena, číslice, speciální znaky) a také má alespoň 7 znaků. Také by nemělo obsahovat uživatelské jméno ani jeho část.

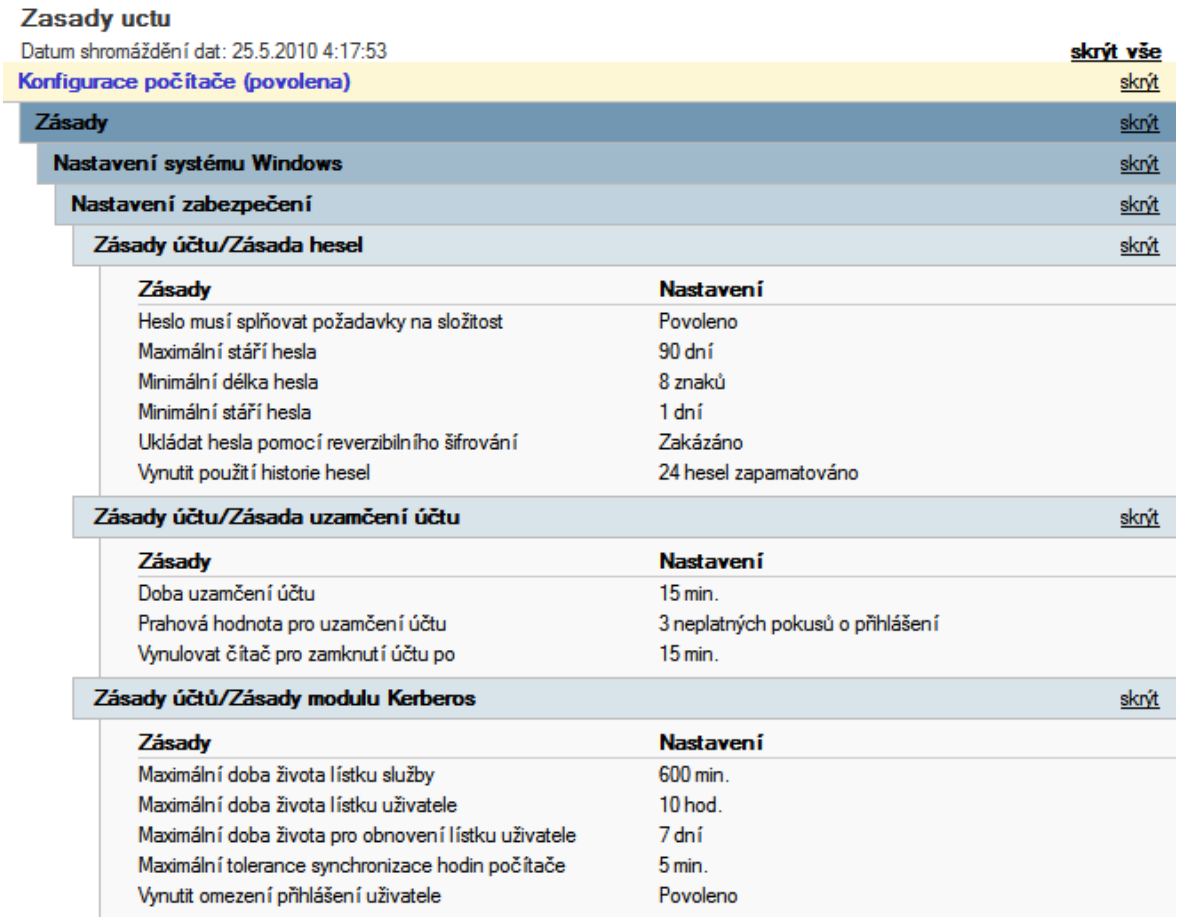
5.3 Aplikace zabezpečení pomocí GPMC

5.3.1 Nastavení zásad hesla

POSTUP 36: Nastavení zásad hesla na úrovni domény

1. *Start - Nástroje pro správu (Administrative Tools) - Správa zásad skupiny (Group Policy Management)*
2. *Objekt zásad skupiny – pravé tlačítko myši - Default Domain Policy - Upravit (Edit)*
3. *V Editoru správy zásad skupiny (Group Policy Management Editor) - Konfigurace počítače (Computer Configuration) - Zásady (Policies) - Nastavení systému*

Windows (Windows Settings) - Nastavení zabezpečení (Security Settings) - Zásady účtů (Account Policies) - Zásady hesla (Password Policies)



Zasady uctu

Datum shromáždění dat: 25.5.2010 4:17:53 skrýt vše

Konfigurace počítače (povolena) skrýt

Zásady skrýt

Nastavení systému Windows skrýt

Nastavení zabezpečení skrýt

Zásady účtu/Zásada hesel skrýt

Zásady	Nastavení
Heslo musí splňovat požadavky na složitost	Povoleno
Maximální stáří hesla	90 dní
Minimální délka hesla	8 znaků
Minimální stáří hesla	1 dní
Ukládat hesla pomocí reverzibilního šifrování	Zakázáno
Vynutit použití historie hesel	24 hesel zapamatováno

Zásady účtu/Zásada uzamčení účtu skrýt

Zásady	Nastavení
Doba uzamčení účtu	15 min.
Prahová hodnota pro uzamčení účtu	3 neplatných pokusů o přihlášení
Vynulovat čítač pro zamknutí účtu po	15 min.

Zásady účtů/Zásady modulu Kerberos skrýt

Zásady	Nastavení
Maximální doba života lístku služby	600 min.
Maximální doba života lístku uživatele	10 hod.
Maximální doba života pro obnovení lístku uživatele	7 dní
Maximální tolerance synchronizace hodin počítače	5 min.
Vynutit omezení přihlášení uživatele	Povoleno

Obrázek 13: Nastavení zásad účtu

5.3.2 Povolení auditování

ÚČEL: Auditování slouží ke sledování činností uživatelů a změn v systému, které mají vliv na zabezpečení systému.

Poznámka: Nastavení auditování se týkají počítačů, proto jsou všechny v kategorii Konfigurace počítače (Computer Configuration). Pro úpravu nastavení auditování pro řadiče domény se využívá objekt zásad skupiny s názvem Default Domain Controllers Policy.

5.3.2.1 Auditovat přístup k adresářové službě

ÚČEL: Toto nastavení zabezpečení určuje, zda bude operační systém auditovat pokusy uživatele o přístup k objektům služby Active Directory.

POSTUP 37: Audit přístupu k adresářové službě

1. *Windows+R - příkaz mmc (Microsoft Management Console) - Soubor (File) - Přidat nebo odebrat modul snap-in (Add/ Remove Snap-in) - modul Správa zásad skupiny (Group Policy Management)*
2. *Pravé tlačítko myši na Objekty zásad skupiny (Group Policy Objects) - Nový (New) – do políčka Název (Name) zadáme název objektu – OK - objekt zásad skupiny byl propojen s organizační jednotkou Zamestnanci*
3. *V konzole Editoru správy zásad skupiny (Group Policy Management Editor) - Konfigurace počítače (Computer Configuration) – Zásady (Policies) - Nastavení systému Windows (Windows Settings) - Nastavení zabezpečení (Security Settings) - Místní zásady (Local Policies) - Zásady auditu (Audit Policies)*
4. *Pravý panel konzoly - pravé tlačítko myši na zásadu Audit přístupu k adresářové službě - volba Definovat toto nastavení zásad (Define these policy settings) - auditovat Úspěšné události*

Nastavení akce a objektů:

1. *Uživatelé a počítače Active Directory (Active Directory Users and Computers) - pravé tlačítko myši - Zobrazit (View) - Upřesňující funkce (Advanced Features)*

Poznámka: Díky tomu nastavení je možné ve vlastnostech objektu vidět záložku Zabezpečení (Security).

2. *Pravé tlačítko myši na objekt pro audit „Zamestnanci“ - Vlastnosti (Properties) - Zabezpečení (Security) - Upřesnit (Customize) - Auditování (Auditing)*
3. *Přidat (Add) - uživatelé nebo skupina, jejichž akce s tímto objektem budou auditovány – dále byly ze seznamu speciálních oprávnění zaškrtnuty akce pro auditování – OK*

5.3.2.2 Auditovat správu účtů

ÚČEL: Toto nastavení zabezpečení určuje, zda se bude auditovat každá událost správy účtů v počítači. K těmto událostem dochází například tehdy, když je vytvořen, změněn nebo odstraněn uživatelský účet, když je uživatelský účet přejmenován, povolen nebo zakázán, nebo když je nastaveno nebo změněno jeho heslo.

POSTUP 38: Audit správy účtů

1. *Windows+R - příkaz mmc (Microsoft Management Console) - Soubor (File) - Přidat nebo odebrat modul snap-in (Add/ Remove Snap-in) - modul Správa zásad skupiny (Group Policy Management)*
2. *Pravé tlačítko myši na Objekty zásad skupiny (Group Policy Objects) - Nový (New) – do políčka Název (Name) zadáme název objektu – OK - objekt zásad skupiny byl propojen s organizační jednotkou Zamestnanci*
3. *V konzole Editoru správy zásad skupiny (Group Policy Management Editor) - Konfigurace počítače (Computer Configuration) – Zásady (Policies) - Nastavení systému Windows (Windows Settings) - Nastavení zabezpečení (Security Settings) - Místní zásady (Local Policies) - Zásady auditu (Audit Policies)*
4. *Pravý panel konzoly - pravé tlačítko myši na zásadu Auditovat správu účtů - volba Definovat toto nastavení zásad (Define these policy settings) - auditovat Úspěšné události i Neúspěšné události*

Nastavení akce a objektů:

5. *Uživatelé a počítače Active Directory (Active Directory Users and Computers) – pravé tlačítko myši - Zobrazit (View) - Upřesňující funkce (Advanced Features)*

Poznámka: Díky tomu nastavení je možné ve vlastnostech objektu vidět záložku Zabezpečení (Security).

6. *Pravé tlačítko myši na objekt pro audit „Zamestnanci“ - Vlastnosti (Properties) - Zabezpečení (Security) - Upřesnit (Customize) - Auditování (Auditing)*
7. *Přidat (Add) - uživatelé nebo skupina, jejichž akce s tímto objektem budou auditovány – dále byly ze seznamu speciálních oprávnění zaškrtnuty akce pro auditování – OK*

5.3.2.3 Auditovat systémové události

ÚČEL: Toto nastavení zabezpečení určuje, zda bude operační systém auditovat systémové události, ke kterým dochází například tehdy, když uživatel restartuje nebo vypíná počítač, nebo když nějaká událost ovlivňuje zabezpečení systému nebo protokol Zabezpečení.

POSTUP 39: Audit systémových událostí

1. *Windows+R - příkaz mmc (Microsoft Management Console) - Soubor (File) - Přidat nebo odebrat modul snap-in (Add/ Remove Snap-in) - modul Správa zásad skupiny (Group Policy Management)*
2. *Pravé tlačítko myši na Objekty zásad skupiny (Group Policy Objects) - Nový (New) – do políčka Název (Name) zadáme název objektu – OK - objekt zásad skupiny byl propojen s organizační jednotkou Zamestnanci*
3. *V konzole Editoru správy zásad skupiny (Group Policy Management Editor) - Konfigurace počítače (Computer Configuration) – Zásady (Policies) - Nastavení systému Windows (Windows Settings) - Nastavení zabezpečení (Security Settings) - Místní zásady (Local Policies) - Zásady auditu (Audit Policies)*
4. *Pravý panel konzoly - pravé tlačítko myši na zásadu Auditovat systémové události - volba Definovat toto nastavení zásad (Define these policy settings) - auditovat Úspěšné události i Neúspěšné události*

Nastavení akce a objektů:

5. *Uživatelé a počítače Active Directory (Active Directory Users and Computers) – pravé tlačítko myši - Zobrazit (View) - Upřesňující funkce (Advanced Features)*

Poznámka: Díky tomu nastavení je možné ve vlastnostech objektu vidět záložku Zabezpečení (Security).

6. *Pravé tlačítko myši na objekt pro audit „Zamestnanci“ - Vlastnosti (Properties) - Zabezpečení (Security) - Upřesnit (Customize) - Auditování (Auditing)*
7. *Přidat (Add) - uživatelé nebo skupina, jejichž akce s tímto objektem budou auditovány – dále byly ze seznamu speciálních oprávnění zaškrtnuty akce pro auditování – OK*

5.3.2.4 Auditovat události přihlášení

ÚČEL: Toto nastavení zabezpečení určuje, zda má operační systém auditovat jednotlivé pokusy uživatele o přihlášení k počítači nebo odhlášení.

POSTUP 40: Audit událostí přihlášení

1. *Windows+R - příkaz mmc (Microsoft Management Console) - Soubor (File) - Přidat nebo odebrat modul snap-in (Add/ Remove Snap-in) - modul Správa zásad skupiny (Group Policy Management)*
2. *Pravé tlačítko myši na Objekty zásad skupiny (Group Policy Objects) - Nový (New) – do políčka Název (Name) zadáme název objektu – OK - objekt zásad skupiny byl propojen s organizační jednotkou Zamestnanci*
3. *V konzole Editoru správy zásad skupiny (Group Policy Management Editor) - Konfigurace počítače (Computer Configuration) – Zásady (Policies) - Nastavení systému Windows (Windows Settings) - Nastavení zabezpečení (Security Settings) - Místní zásady (Local Policies) - Zásady auditu (Audit Policies)*
4. *Pravý panel konzoly - pravé tlačítko myši na zásadu Auditovat události přihlášení - volba Definovat toto nastavení zásad (Define these policy settings) - auditovat Úspěšné události i Neúspěšné události*

Nastavení akce a objektů:

5. *Uživatelé a počítače Active Directory (Active Directory Users and Computers) – pravé tlačítko myši - Zobrazit (View) - Upřesňující funkce (Advanced Features)*

Poznámka: Díky tomu nastavení je možné ve vlastnostech objektu vidět záložku Zabezpečení (Security).

6. *Pravé tlačítko myši na objekt pro audit „Zamestnanci“ - Vlastnosti (Properties) - Zabezpečení (Security) - Upřesnit (Customize) - Auditování (Auditing)*
7. *Přidat (Add) - uživatelé nebo skupina, jejichž akce s tímto objektem budou auditovány – dále byly ze seznamu speciálních oprávnění zaškrtnuty akce pro auditování – OK*

5.3.2.5 Auditovat změny zásad

ÚČEL: Toto nastavení zabezpečení určuje, zda bude operační systém auditovat jednotlivé události pokusů o změnu zásad přiřazení uživatelských práv, zásadách auditu, zásadách důvěry nebo zásadách hesla.

POSTUP 41: Audit změn zásad

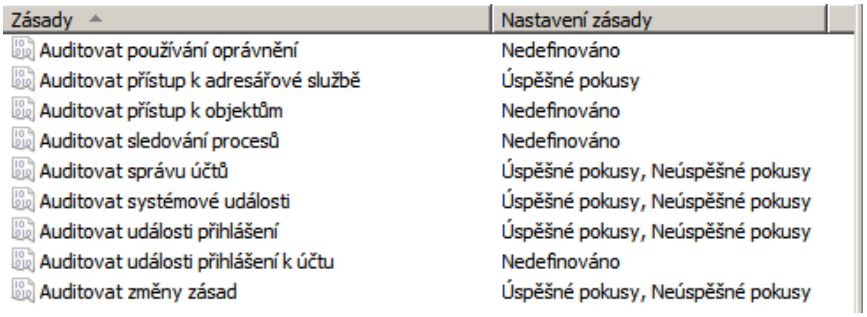
1. *Windows+R - příkaz mmc (Microsoft Management Console) - Soubor (File) - Přidat nebo odebrat modul snap-in (Add/ Remove Snap-in) - modul Správa zásad skupiny (Group Policy Management)*
2. *Pravé tlačítko myši na Objekty zásad skupiny (Group Policy Objects) - Nový (New) – do políčka Název (Name) zadáme název objektu – OK - objekt zásad skupiny byl propojen s organizační jednotkou Zamestnanci*
3. *V konzole Editoru správy zásad skupiny (Group Policy Management Editor) - Konfigurace počítače (Computer Configuration) – Zásady (Policies) - Nastavení systému Windows (Windows Settings) - Nastavení zabezpečení (Security Settings) - Místní zásady (Local Policies) - Zásady auditu (Audit Policies)*
4. *Pravý panel konzoly - pravé tlačítko myši na zásadu Auditovat změny zásad - volba Definovat toto nastavení zásad (Define these policy settings) - auditovat Úspěšné události i Neúspěšné události*

Nastavení akce a objektů:

5. *Uživatelé a počítače Active Directory (Active Directory Users and Computers) – pravé tlačítko myši - Zobrazit (View) - Upřesňující funkce (Advanced Features)*

Poznámka: Díky tomu nastavení je možné ve vlastnostech objektu vidět záložku Zabezpečení (Security).

6. *Pravé tlačítko myši na objekt pro audit „Zamestnanci“ - Vlastnosti (Properties) - Zabezpečení (Security) - Upřesnit (Customize) - Auditování (Auditing)*
7. *Přidat (Add) - uživatelé nebo skupina, jejichž akce s tímto objektem budou auditovány – dále byly ze seznamu speciálních oprávnění zaškrtnuty akce pro auditování – OK*



Zásady	Nastavení zásady
Auditovat používání oprávnění	Nedefinováno
Auditovat přístup k adresářové službě	Úspěšné pokusy
Auditovat přístup k objektům	Nedefinováno
Auditovat sledování procesů	Nedefinováno
Auditovat správu účtů	Úspěšné pokusy, Neúspěšné pokusy
Auditovat systémové události	Úspěšné pokusy, Neúspěšné pokusy
Auditovat události přihlášení	Úspěšné pokusy, Neúspěšné pokusy
Auditovat události přihlášení k účtu	Nedefinováno
Auditovat změny zásad	Úspěšné pokusy, Neúspěšné pokusy

Obrázek 14: Nastavení auditů

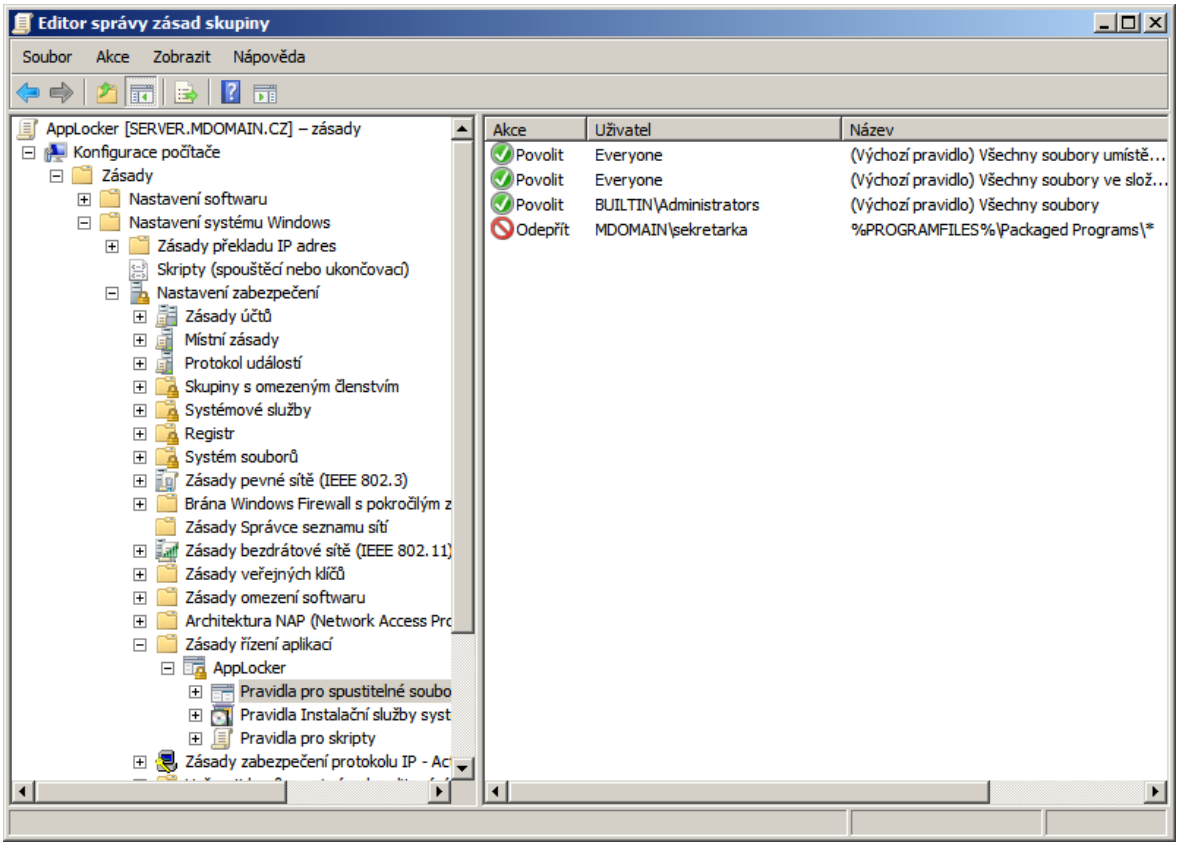
5.3.3 Omezení spouštění aplikací pomocí zásad AppLockeru

POSTUP 42: Omezení spouštění aplikací pomocí zásad AppLockeru

1. *Start – Nástroje pro správu (Administrative Tools) – Správa zásad skupiny (Group Policy Management)*
2. *Pravé tlačítko myši na organizační jednotku „Administrativa“ – Vytvořit nový objekt zásad skupiny a propojit jej sem (Create a GPO in this domain, and Link it here)*

Poznámka: Název nového objektu zásad: AppLocker

3. *Pravé tlačítko myši na nový objekt zásad – Upravit (Edit)*
4. *V editoru zásad skupiny – Konfigurace počítače (Computer Configuration) – Zásady (Policies) – Nastavení systému Windows (Windows Settings) – Nastavení zabezpečení (Security Setings) – Zásady řízení aplikací (Application Control Policies) – levý panel položka AppLocker*
5. *Pravý panel odkaz Nastavit vynucení pravidel (Configure rule enforcement) – Nastaveno (Configured) – Pravidla spustitelných souborů (Executable rules) – OK*
6. *Levý panel AppLocker – pravé tlačítko na položku Pravidla spustitelných souborů (Executable Rules) – Vytvořit nové pravidlo (Create New Rule) – Další (Next)*
7. *Na obrazovce Oprávnění (Permissions) – byla vybrána možnost Zakázat (Deny) – Vybrat (Select) – uživatel sekretarka – Další (Next)*



Obrázek 15: Omezení spouštění aplikací pomocí AppLocker

8. *Na obrazovce Podmínky (Conditions) – Cesta (Path) – Další (Next) – Procházet složky (Browse folders) - byla vybrána složka „Packaged Programs“ - Další (Next)*

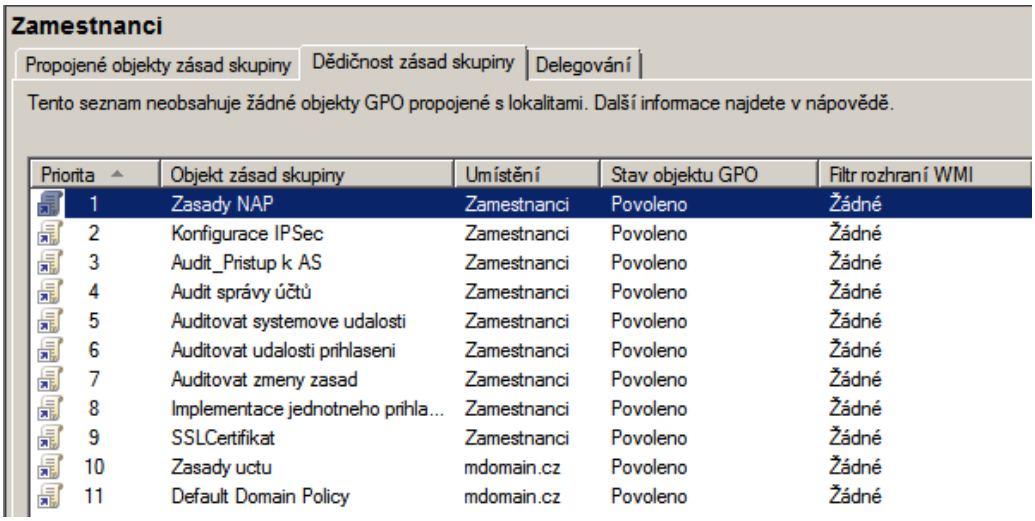
Poznámka: V diplomové práci byla vybrána složka D:\Program Files\Packaged Programs ze které bylo zakázáno spouštět programy.

9. *Na obrazovce Výjimky (Exceptions) byla pomocí tlačítka Přidat (Add) definována výjimka – Další (Next) – Dokončit (Finish)*
10. *Vygenerovat výchozí sadu pravidel – Ano (Yes)*

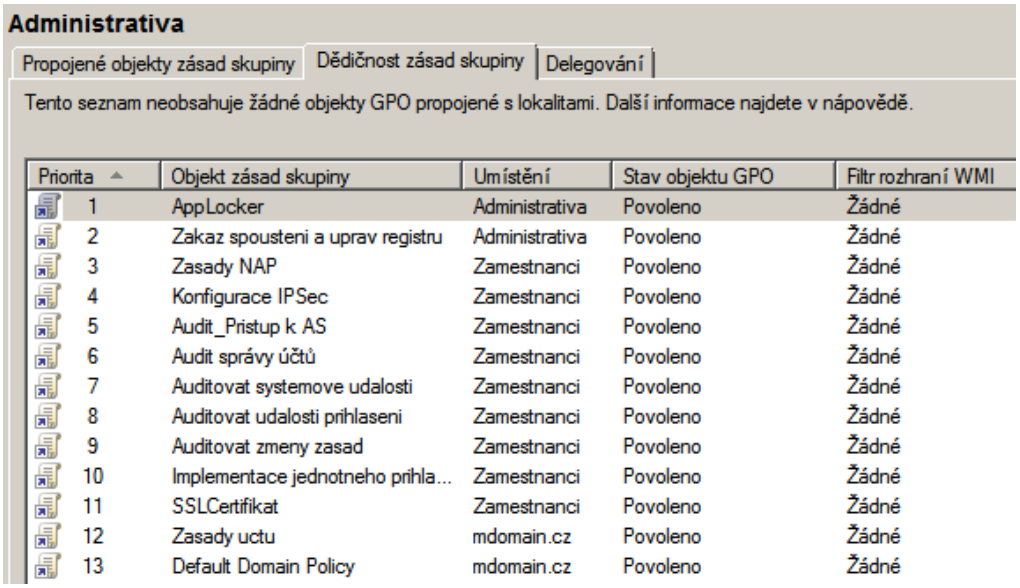
5.3.4 Aplikace a porovnání objektů zásad skupiny v OU

Na obrázcích je vidět aplikace GPO propojené na úrovni „OU Zamestnanci“. Vzhledem k tomu, že se tato organizační jednotka nachází v doméně mdomain.cz zdědila veškerá aplikovaná GPO propojené na úrovni domény. Důvod je ten, že je aktivní Dědičnost zásad skupiny, což znamená, že každá nižší jednotka zdědí GPO aplikované na vyšší úrovni. „OU Zamestnanci“ obsahuje dvě vnořené OU a to „Administrativa“ a „Vyvojari“ to znamená, že veškeré GPO v „OU Zamestnanci“ zdědí tyto vnořené OU. OU

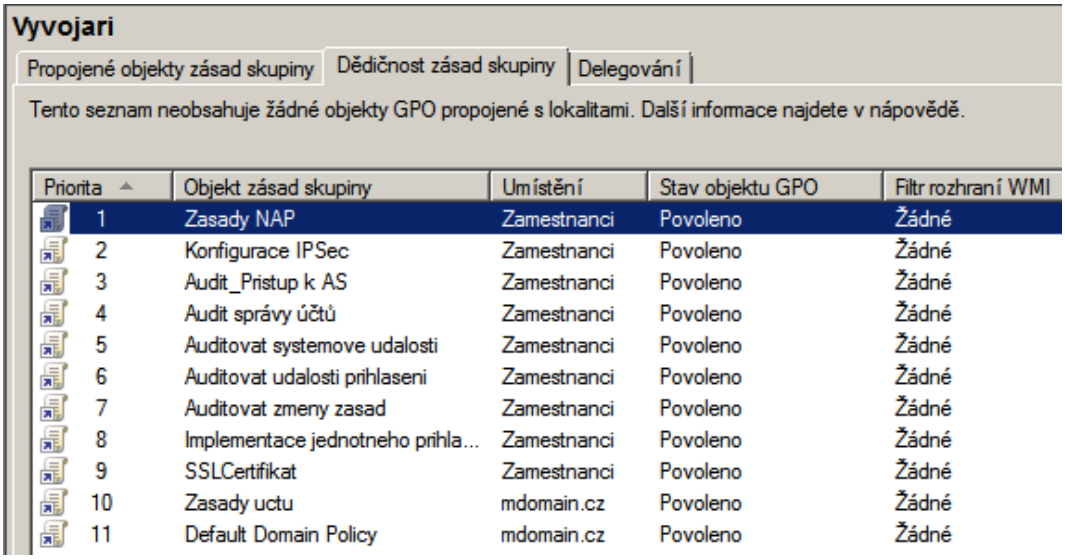
Administrativa však obsahuje GPO propojené právě na tuto organizační jednotku, to tedy znamená, že neovlivní „OU Zamestnanci“ a „OU Vyvojari“.



Obrázek 16: Propojené GPO v rámci OU Zamestnanci



Obrázek 17: Propojené GPO v rámci OU Administrativa



Priorita	Objekt zásad skupiny	Umístění	Stav objektu GPO	Filtr rozhraní WMI
1	Zasady NAP	Zamestnanci	Povoleno	Žádné
2	Konfigurace IPSec	Zamestnanci	Povoleno	Žádné
3	Audit_Pristup k AS	Zamestnanci	Povoleno	Žádné
4	Audit správy účtů	Zamestnanci	Povoleno	Žádné
5	Auditovat systemove udalosti	Zamestnanci	Povoleno	Žádné
6	Auditovat udalosti prihlaseni	Zamestnanci	Povoleno	Žádné
7	Auditovat zmeny zasad	Zamestnanci	Povoleno	Žádné
8	Implementace jednotneho prihla...	Zamestnanci	Povoleno	Žádné
9	SSLCertifikat	Zamestnanci	Povoleno	Žádné
10	Zasady uctu	mdomain.cz	Povoleno	Žádné
11	Default Domain Policy	mdomain.cz	Povoleno	Žádné

Obrázek 18: Propojené GPO v rámci OU Vyvojari

5.4 Konfigurace klientských počítačů s ohledem na bezpečnost

5.4.1 Konfigurace připojení klientského počítače k síti

POSTUP 43: Připojení klienta k síti

1. *Spravce serveru (Server Manager) – Zobrazit síťová připojení (Network Connections)*
2. *Připojení k místní síti (Local Area Connection) - pravé tlačítko myši - Vlastnosti (Properties)*
3. *Protokol TCP/IPv4 (Internet Protocol Version 4) - Vlastnosti (Propertis)*
4. *Zde byla nastavena adresu IP, síťová maska, ale výchozí brána a DNS byly prozatím ponechány nevyplněné - OK - Zavřít (Close)*
5. *Nastavení bylo ověřeno v Příkazovém řádku pomocí příkazu Ipconfig*

Poznámka: IP adresa byla nastavena na hodnotu *10.0.0.2* a síťová maska na hodnotu *255.0.0.0*.

5.4.2 Přihlášení klienta do domény

POSTUP 44: Přihlášení klienta do domény

1. *Start – pravé tlačítko na Počítač – Vlastnosti (Properties) – Název počítače, doména a nastavení pracovní skupiny – Změnit nastavení*

2. *Ve vlastnostech systému – ID sítě – Připojit se k doméně nebo pracovní skupině – možnost Tento počítač je součástí podnikové sítě a je používán k připojení k dalším počítačům v práci – Společnost používá síť s doménou*
3. *Na další stránce bylo zadáno Uživatelské jméno, Heslo a Název domény*
4. *Dále byl zadán Název počítače a Doména počítače*

Poznámka: Uživatelské jméno: sekretarka, Název domény: mdomain.cz, Název počítače: LP-PC2, Doména počítače: mdomain.cz.

5.4.3 Konfigurace připojení klientského počítače k síti se službou DHCP

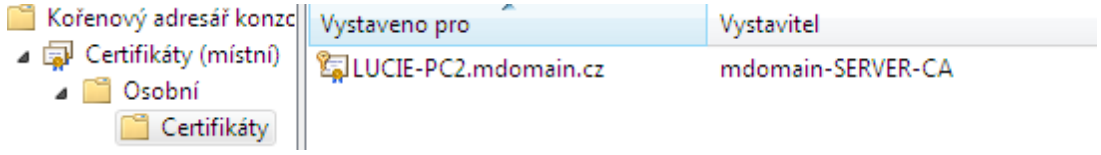
POSTUP 45: Připojení klienta k síti s aktivní službou DHCP

1. *Spravce serveru (Server Manager) – Zobrazit síťová připojení (Network Connections)*
2. *Připojení k místní síti (Local Area Connection) - pravé tlačítko myši - Vlastnosti (Properties)*
3. *Protokol TCP/IPv4 (Internet Protocol Version 4) - Vlastnosti (Propertis)*
4. *Zde bylo nastaveno Získat IP adresu ze serveru DHCP automaticky a Získat adresu serveru DNS automaticky - OK - Zavřít (Close)*

5.4.4 Vyžádání certifikátu počítače na klientském počítači

1. *Windows + R – příkaz mmc – Soubor (File) – Přidat nebo odebrat modul snap-in (Add/Remove Snap-in) – Certifikáty (Certificates) – Přidat (Add) – Účet počítače (Computer account) – Místní počítač (Local computer) – Dokončit (Finish) – OK*
2. *Levý panel konzoly – Certifikáty (Certificates) – pravé tlačítko myši na položku Osobní (Personal) – Všechny úkoly (All Tasks) – Vyžádat nový certifikát (Request New Certificate)*
3. *Zápis certifikátu (Certificate Enrollment) – Další (Next) – typ certifikátu – Počítač (Computer) – Zapsat (Enroll)*

Poznámka: Po úspěšném získání certifikátu je tento certifikát uložen v konzole Certifikáty (Certificates).



Obrázek 19: Úspěšné vystavení certifikátu počítače

5.4.5 Instalace balíčku MSI na klientském počítači

Výhodou instalace balíčků MSI je, že jsou klientům poskytnuty programy serverem, které jsou součástí nabídky Start a jsou také zobrazeny na Ploše.

POSTUP 46: Instalace balíčku MSI

1. *Start – Počítač (Computer) - levý panel – Síť (Network) – Server – Packaged Programs – instal balíčku MSI*

Poznámka: Při spuštění vzdáleného programu musí uživatel zadat Uživatelské jméno a Heslo. Díky implementaci jednotného přihlášení se stačí autentizovat jen jednou.

5.4.6 Konfigurace klienta pro připojení pomocí Brány VP

POSTUP 47: Konfigurace klienta pro připojení pomocí Brány VP

1. *Start – Všechny programy (All Programs) – Příslušenství (Accessories) – Připojení ke vzdálené ploše (Remote Desktop Connection)*
2. *Do pole název Počítače (Computer) byla zadána IP adresa serverového počítače*
3. *Možnosti (Options) – Upřesnit (Advanced) – Nastavení (Settings)*
4. *V dialogovém okně Nastavení serveru brány služby Vzdálená plocha byl do pole Název serveru uveden název serveru s rolí Brána Vzdálené plochy a zrušeno políčko Nepoužívat server služby Brána VP pro místní adresy*

5.4.7 Vyžádání aktualizace zásad skupiny na klientském počítači

Pro okamžitou aplikaci změn v nastavení zásad využijeme jeden z dvou možných příkazů *Gpupdate /force a Gpupdate /forte.* Jediným rozdílem těchto dvou příkazů je, že *Gpupdate /forte* je z hlediska priority na vyšší úrovni. Pro aktualizaci zásad se tyto příkazy využívají na klientských počítačích nikoliv serverových

ZÁVĚR

Ve chvíli kdy jsou počítače součástí domény, bývají spravovány přes síťové rozhraní prostřednictvím serveru. Tento server poskytuje svým klientům služby nebo aplikuje zabezpečení. Proto je velmi důležité zabezpečit daný server, tak aby minimalizace hrozících rizik jak ze strany vnější sítě, tak ze strany samotných klientů vnitřní sítě byla co možná největší.

Tím se zabývala tato diplomová práce, která si kladla za cíl popsat možná rizika plynoucí z nedostatečně zabezpečeného počítače, ale hlavně nabídnout ucelený postup zabezpečení operačních systémů Windows Server 2008 R2 a Windows 7.

Součástí teoretické části práce je nejen popis obecných a fyzických rizik, ale také rizik, které jsou specifické pro serverové počítače. Dále se práce zabývala obecným popisem vybraných služeb serverového operačního systému Microsoft Windows Server 2008 R2 s čímž souvisí další část práce, jež popisuje metodiky zabezpečení vybraných služeb a systému jako celku. Zásady skupiny (Group Policy) jakožto základnímu pilíři celého zabezpečení byla věnována samostatná kapitola, která si kladla za cíl popsat a vysvětlit aplikaci jednotlivých zásad zabezpečení na počítače.

Nejdůležitější částí diplomové práce je bezesporu její praktická část. Zde byly ukázány postupy instalace a konfigurace vybraných služeb s ohledem na bezpečnost. Práce na příkladu sítě se třemi počítači - serverovým, se systémem Windows Server 2008 R2 a dvěma klientskými se systémem Windows 7, ukazuje jak vhodně instalovat služby Active Directory Domain Services, díky níž je daný server povýšen do role řadiče domény. Následně je ukázáno, jak prostřednictvím této služby, na klienty připojené do sítě tohoto, aplikovat řadu vhodných zabezpečení. Pro správnou funkci domény je nezbytná i síťová služba DNS Server, jejíž instalace byla rovněž v praktické části popsána. Stejně tak byl server doplněn o službu DHCP Server. Služba DHCP Server byla nakonfigurována, tak aby spolupracovala s architekturou NAP, díky čemuž bylo zajištěno, že adresy IP umožňující plnohodnotný přístup k prostředkům sítě budou přiděleny jen počítačům, které splňují předem definované požadavky. Byl tedy kladen důraz i na vhodné nastavení klientských počítačů se systém Windows 7 Professional nebo lépe řečeno vhodné nastavení jejich uživatelských účtů s určitými omezeními, které mají významný podíl pro minimalizaci rizik plynoucích z neodborného nebo úmyslného zásahů do konfigurace počítače. Součástí praktické časti je také popis instalace a konfigurace služby Remote

Desktop Service, ve které se práce zaměřuje na využití jejich rolí RemoteApps a Brány VP (Vzdálená plocha).

Celá praktická část je zpracována formou praktického průvodce, který postupnými kroky provede instalací a konfigurací systému Windows Server 2008 s ohledem na zabezpečení před aktuálními hrozbami. Samozřejmě je nutné upozornit, že práce je velmi úzce pojatá, neboť faktem zůstává, že zabezpečení serverových a klientských počítačů nebo celkově bezpečnost je velmi rozsáhlé téma. Pro řešení této práce by bylo vhodnější, kdyby se server nacházel v reálném prostředí pokud možno s větším počtem serverů, kdy by bylo možné aplikovat některé druhy zabezpečení, a také klientů. Tím by jakékoliv nastavené zabezpečení prošlo plným testovacím procesem a práce by tedy mohla reagovat na skutečné a aktuální problémy se kterými se správci dennodenně setkávají.

Při praktické realizaci z důvodu některých omezení, jakým bylo například využití pouze jediného serveru, došlo ke vzniku několika bezpečnostních prohřešků. Použití jediného serveru, na kterém by běžela služba AD DS současně se službou Remote Desktop Service není rozhodně doporučováno, neboť při této konfiguraci je dovolen přístup klientům na serverový počítač, který je řadičem domény a tím dochází ke značnému bezpečnostnímu riziku.

Výsledné řešení prezentuje postupy instalace a konfigurace významných služeb serverového počítače, například AD DS (Active Directory Domain Services), ale také řadu prostředků, jak prostřednictvím operačních systému Microsoft Windows vytvořit dobře fungující bezpečnou počítačovou síť.

ZÁVĚR V ANGLIČTINĚ

The best option to maintenance computers which are part of the domain is through the network interface of the server.

The server provides services to its clients, allows applying security and so on. Therefore, it is very important to secure the server to minimize risks threatening from both sides - from the side of the external network, and also from the clients inside its own network.

This thesis deals with all above mentioned risks. At the beginning, it describes the potential risks arising from poorly secured computers, and then it tries to offer comprehensive security approach for Windows Server 2008 R2 and Windows 7 network.

The theoretical part of this thesis is not just a general description of the physical risks but also focuses on the specifics of the server computer. This work also deals with a general description of selected Microsoft Windows Server 2008 R2's services, which is linked to the another part, which shows the methodology of securing these selected services and links the security options to one solid complex. A separate chapter is dedicated to the Group Policy, which is a basic pillar of the Windows Server security. The chapter tries to describe and explain the application of security policies on the individual computer or its group in the Windows Server network.

The most important part of the thesis is certainly its practical part. There are given examples how to install and configure the selected server services with regard to its safety. The work on the example of the network with three computers - server, Windows Server 2008 R2 and the two clients running Windows 7, shows how to properly install the Active Directory Domain Services, through which the server is promoted to the role of the domain controller and it becomes able to offer series of security options to its clients. For proper function of the domain it is necessary to install DNS Server service, whose installation is also shown in the practical part of this thesis. Likewise, the server has been promoted to the DHCP Server. DHCP Server role has been configured to cooperate with the NAP architecture, thereby the IP addresses to allow full access to network resources will be provided only to computers that meet the predefined requirements. Presented configuration focused on the appropriate settings on client computers with Windows 7 Professional or better. Preparation of suitable settings of their user accounts with certain restrictions has a significant contribution to minimizing the risks from improper or intentional interference with computer configurations. The practical part also contains a description of the

installation and configuration of the Remote Desktop Service, which is focused on its roles RemoteApps and Remote Desktop.

Whole practical part is presented as a practical guide, which shows successive steps to install and configure Windows Server 2008 with regard to protection against current threats. Of course, it should be noted that the work is very narrowly conceived, because the fact remains that the security of server and client computers or the total security of whole network is a very broad topic. To deal with this task it would have been preferable if the server was located in a real environment, with more servers, which could carry more security options, as well as clients. This would let the security setting undergo full testing process and should therefore work to respond to real and actual problems which administrators face daily.

Due to certain restrictions, such as usage of only a single server, there were several safety violations, which should be avoided in practical implementation. Using a single server that is running the AD DS and Remote Desktop Service as well, is definitely not recommended, because in this configuration, clients are allowed to access server computer, which is also a domain controller, and this is a significant security risk.

The resulting solution presents procedures for installing and configuring the server computer with most of it important services, for example AD DS (Active Direcotry Domain Services) but also presents a way how to create an efficient and securely working computer network based on Microsoft Windows operating systems.

SEZNAM POUŽITÉ LITERATURY

[1] BABARÍK, Martin. Microsoft Windows Server 2008 : Hotová řešení. 2008. Brno: Computer Press, a.s., 2009. 432 s. ISBN 978-80-251-2207-5.

[2] BOTT, Ed, SIECHERT, Carl. Mistrovství v zabezpečení Microsoft Windows 2000 a XP. Brno: Computer Press, 2004. 696 s. ISBN 80-7226-878-3.

[3] BICKEL, R., et al. Guide to Securing Microsoft Windows XP : Operational Network Evaluations Division of the Systems and Network Attack Center (SNAC). SNAC [online]. 2002 [cit. 2002-10-31], s. 1-128.

[4] HATCH, Brian; LEE, James; KURTZ, George. *Linux Hackerské Útoky : Bezpečnost Linuxu - tajemství a řešení*. Praha : SoftPress, 2002. 576 s. ISBN 80-86497-17-8.

[5] HOWARD, Michael, LEBLANC, David. Bezpečný kód. Brno : Computer Press, a.s., 2008. 888 s. ISBN 978-80-251-2050-7.

[6] MCCLURE, Stuart, SCAMBRAY, Joel, KURTZ, George. Hacking bez tajemství. Brno: Computer Press, a.s, 2003. 632 s. ISBN 80-722-6948-8.

[7] Microsoft.com/cs/cz/ [online]. 2010 [cit. 2010-03-20]. Microsoft. Dostupné z WWW: <http://www.microsoft.com/cs/cz/>.

[8] *Microsoft TechNet* [online]. 2000 [cit. 2010-05-23]. 10 Immutable Laws of Security. Dostupné z WWW: <http://technet.microsoft.com/en-us/library/cc722487.aspx>.

[9] MOSKOWITZ, Jeremy. Zásady skupiny profily a IntelliMirror : ve Windows 2000, 2003 a XP . Brno : Computer Press, a. s., 2005. 524 s. ISBN 80-251-0806-6.

[10] Mstv.cz [online]. 2010 [cit. 2010-03-20]. MSTV. Dostupné z WWW: <www.mstv.cz>.

[11] SMITH, Ben, KOMAR, Brian. Zabezpečení systému a sítě: Microsoft Windows. Brno: Computer Press, a.s., 2006. 700 s. ISBN 80-251-1260-8.

[12] STANEK, William R. Microsoft Windows Server 2008 : Kapesní rádce administrátora. 2008. Brno: Computer Press, a.s., 2008. 704 s. ISBN 978-80-251-1936-5.

[13] TULLOCH, Mitch, NORTHRUP, Tony, HONEYCUTT, Jerry. Microsoft Windows Vista: Resource Kit. Brno: Computer Press, a.s., 2008. 1432 s. ISBN 978-80-251-1990-7.

[14] Windows 7 Product Guide. Microsoft. 2009, no. 1, s. 1-140. Dostupný z WWW: http://www.microsoft.com/downloads/details.aspx?FamilyID=b3c68ec2-e726-4830-ac89-31c71d6be5f3&displayLang=en.

[15] Nápověda a podpora pro systém Windows Server 2008 R2 [offline]. 2009 [cit. 2010-04-15]. Microsoft

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

A-záznam	Převádí jmenný název na IP adresu. Obsahuje vždy číselnou hodnotu IP adresy.
ADCS	Active Directory Certification Services je služba, která poskytuje služby pro vydávání a správu certifikátů veřejných klíčů, které jsou využívány v systémech softwarového zabezpečení založených na technologii veřejných klíčů
ADDS	Active Directory Domain Services je rozšiřitelná adresářová služba, která umožňuje centralizovanou správu síťových prostředků
CA	Certifikační autorita slouží k vydávání certifikátů uživatelům, počítačům a službám a ke správě platnosti certifikátů
CRL	Certificate Revocation List je seznam zneplatněných certifikátů, ve kterém jsou zapsány informace o certifikátech, které jejich vlastníci prohlásili za neplatné (nechali je zneplatnit)
DC	Domain Controller neboli řadič domény je počítač, na kterém je uložen adresář služby Active Directory
DHCP	Dynamic Host Configuration Protocol slouží pro automatické přidělování IP adres klientským počítačům a dalším síťovým zařízením v počítačových sítích na bázi TCP/IP
DNS	Domain Name System slouží k vyhodnocování názvů DNS a jejich převod na IP adresy, a naopak vyhodnocování IP adresy na názvy DNS
DoS	Denial of Service nebo DDoS (Distributed Denial of Services) spočívá v zahlcení serveru (resp. počítače) nadměrným množstvím požadavků, nejde tedy prvořadně o získávání dat
GPMC	Group Policy Management Console) je nástroj, který slouží pro správu zásad skupiny v prostředí Active Directory
GPO	Group Policy Object neboli objekt zásad skupiny umožňuje aplikovat jednotlivá pravidla na vybrané uživatele či počítače v prostředí Active Directory

GUID	Globálně jedinečný identifikátor je speciální typ identifikátoru používaný v softwarových aplikacích poskytující jedinečné referenční číslo
HTTPS	Hypertext Transfer Protocol Secure je nadstavba síťového protokolu HTTP, která umožňuje zabezpečit spojení před odposloucháváním, podvržením dat a umožňuje též ověřit identitu protistrany
IP adresa	Je v informatice číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti
Licence VP CAL	Licence VP CAL (Client Access License) jsou softwarové licence, které jsou požadovány pro připojení každého zařízení nebo uživatele k serveru Hostitel relací VP
Malware	Souhrnné označení zahrnující počítačové viry, trojské koně, spyware a adware
NAP	Network Access Protection je technologie vytváření, vynucení a nápravy problémů zásad stavu klienta
NAT	Network Address Translation umožňuje nakonfigurovat sdílení připojení k Internetu s počítači v privátní síti a překlad přenosů mezi svou veřejnou adresou a privátní sítí
NPS	Network Policy Server umožňuje centrálně spravovat přístup k síti prostřednictvím řady různých serverů pro přístup k síti, k nimž patří bezdrátové přístupové body, servery VPN, servery pro telefonické připojení a ověřovací přepínače 802.1X
OU	Organization Unit slouží k uspořádání objektů v doméně k usnadnění správy účtů pro uživatele, skupiny a počítač a pro správu ostatních prostředků (tiskárny, sdílené složky atd.)
PTR	Reverzní záznam PTR slouží k převodu IP adresy na názvy
RFC	Request For Comments jsou označením řady standardů a dalších dokumentů popisujících Internetové protokoly, systémy atd. RFC jsou oficiálně považovány spíše za doporučení, než normy přesto se

	podle nich řídí většina Internetu
SRV	Service record je záznam obsahující hostitelský název serverů, na nichž příslušné služby AD běží, a podle nichž se klienti DNS mohou k požadované službě AD připojit
TCP/IP	Transmission Control Protocol/Internet Protocol obsahuje sadu protokolů pro komunikaci v počítačové síti a je hlavním protokolem celosvětové sítě Internet
VPN	Virtual Private Network slouží k virtuálnímu spojení více fyzicky vzdálených počítačů, takže se chovají, jako by byly přímo propojené jednou sítí
WINS	Windows Internet Naming Service slouží pro překlad názvů NetBIOS
WSUS	Windows Server Update Services slouží ke správě aktualizací vydaných prostřednictvím služby Microsoft Update

SEZNAM OBRÁZKŮ

SEZNAM POSTUPŮ