Ochrana firemních dat

Protection of company information

Bc. Radim LUKEŠ

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. Radim LUKEŠ**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Ochrana firemních dat**

Zásady pro vypracování:

1. **Analyzujte hlavní důvody ochrany firemních dat.**
2. **Popište základní způsoby ochrany firemních dat.**
3. **Navrhněte a proveďte implementaci monitorovacího systému System Center Operations Manager na servery platformy Windows.**
4. **Vyhodnoťte.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **THOMAS, M. Thomas. Zabezpečení počítačových sítí bez předchozích znalostí. Brno : Computer Press, a.s., 2005. 338 s. ISBN 80-251-0417-6.**
2. **MLÝNEK, Jaroslav. Zabezpečení obchodních informací : Výběr a realizace bezpečnostních opatření k zajištění důvěrnosti, celistvosti a dostupnosti informací. [s.l.] : Computer Press, a.s., 2007. 160 s. ISBN 978-80-251-1511-4.**
3. **SMITH, Ben, KOMAR, Brian, MICROSOFT Security Team. Zabezpečení systému a sítě Microsoft Windows. Brno : Computer Press, a.s., 2006. 700 s. ISBN 80-251-1260-8.**
4. **DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat . Brno : Computer Press, 2004. 200 s. ISBN 80-251-0106-1.**
5. **LUDVÍK, Miroslav, ŠTĚDROŇ, Bohumír. Teorie bezpečnosti počítačových sítí. Computer Media, 2008. 98 s. ISBN 80-86686-35-3.**
6. **ŘEPA, Pavel . Jak na . . . instalaci agenta SCOM 2007 a řešení případných problémů [online]. 2009 , Monday, October 19, 2009 [cit. 2010-01-06]. Dostupný z WWW: http://blogs.technet.com/technetczsk/pages/jak-na-instalaci-agenta-scom-2007-a-reseni-pripadnych-problemu.aspx.**
7. **MICROSOFT. System Center Operations Manager 2007 (SCOM) -- Platform Monitoring [online]. 2009 , 2009 [cit. 2010-01-06]. Dostupný z WWW: http://www.microsoft.com/systemcenter/operationsmanager/en/us/default.aspx.**

Vedoucí diplomové práce: **doc. Ing. Ivan Zelinka, Ph.D.**
Ústav informatiky a umělé inteligence

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

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

prof. Ing. Vladimír Vašek, CSc.
ředitel ústavu

ABSTRAKT

Diplomová práce se zabývá problematikou ochrany firemních dat. Klade si za cíl seznámit čtenáře s hlavními důvody ochrany dat a popsat základní způsoby, jak se co nejlépe vypořádat s těmito riziky. V praktické části je řešena implementace monitorovacího systému System Center Operations Manager od firmy Microsoft na vybrané servery ve společnosti Home Credit International, a.s.

Klíčová slova: bezpečnostní politika, informace, riziko, útok, antivir, firewall, monitorování

ABSTRACT

The diploma thesis deals with the protection of corporate data. It aims to ascquaint the reader with the main reasons of data protection and describe the basic ways to best cope with these risks. The practical part is designed to implement a monitoring system, System Center Operations Manager from Microsoft at selected servers in the Home Credit International, Inc.

Keywords: security policy, information, risk, attack, antivirus, firewall, monitoring

Poděkování

Rád bych poděkoval doc. Ing. Ivanu Zelinkovi, Ph.D., za ochotu a trpělivost. Dále chci poděkovat mé manželce Vlaďce, dcerám Klárce a Darjence za neustálou podporu, kterou mi věnují.

Motto: „Není moudrý ten, kdo ví mnoho, ale ten kdo ví, co je třeba.“

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 pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně ……

podpis diplomanta

OBSAH

ÚVOD

Dnešní společnost lze bez nadsázky označit jako společnost informační. Drtivá většina dnešních firem intenzivně využívá prostředky výpočetní techniky ke své každodenní práci.

Informace mají v současné době hodnotu zlata a víceméně všichni jsme na informacích přímo závislí. Bez ohledu na obor podnikání, všichni s informacemi pracujeme a uvědomujeme si fakt, že v byznysu jsou informace klíčem k úspěchu.

Proto je důležité se k informacím chovat tak, aby byly naše informace v bezpečí, a to s vynaložením minimálních nákladů. Ve své práci se tedy pokusím seznámit čtenáře s principem zachování důvěrnosti, integrity a dostupnosti informací. Dále je zde uveden přehled několika základních opatření vedoucích k ochraně dat.

V praktické části je proveden návrh a implementace monitorovacího produktu Microsoft System Center Operation Manager na vybrané servery.

I. TEORETICKÁ ČÁST

1 BEZPEČNOSTNÍ POLITIKA

1.1 Bezpečnost a počítačové sítě

V dnešní době se za pomoci informační technologie zpracovává stále více informací. Pokud hovoříme v souvislosti s informačními technologiemi o zpracování informací, pak máme zejména na mysli použití těchto technologií k uchovávání, přenosu, vyhodnocování a prezentaci informací. Často se jedná o informace s nezanedbatelnou hodnotou (například bankovní účty, informace o zaměstnancích, databáze klientů, obchodní záměry, výsledky vývoje či výzkumu) musí být chráněny tak, aby:

- k nim měly přístup pouze oprávněné osoby,
- se zpracovávaly nefalšované informace,
- se dalo zjistit, kdo tyto informace vytvořil, změnil nebo odstranil,
- byly dostupné tehdy, když jsou potřebné,
- nebyly nekontrolovaným způsobem vyzrazeny.

1.2 Zabezpečení informace

Ochrana informace je složitý proces, který může mít různou podobu, ale vždy by měl směřovat k zajištění důvěrnosti, integrity a dostupnosti požadované informace.

1.2.1 Důvěrnost

Pojmem důvěrnost je myšlena prevence proti neoprávněnému užití informace. Cílem tohoto zajištění je zajistit, aby informace byly přístupné nebo aby byly sděleny pouze těm, kteří jsou k tomu oprávněni.

Většina firem pracuje se spoustou informací, které je potřeba rozdělit podle tohoto kritéria. Příkladem takového rozdělení mohou být následující klasifikační stupně:

- Veřejné – informace pro veřejnost (e-mailové adresy, telefonní čísla)
- Interní – informace pro zaměstnance dané společnosti
- Důvěrné – informace pouze pro vybrané zaměstnance
- Soukromé – informace pouze pro vybrané zaměstnance

- Přísně důvěrné – informace pouze pro vybrané zaměstnance (strategické plány, zdrojové kódy)

Toto rozdělení je pouze vzorové a může se lišit, ale je podstatné, aby společnost měla ke každé informaci, kterou bude vytvářet, zpracovávat nebo uchovávat, přiřazen odpovídající klasifikační stupeň a na základě tohoto rozdělení dodržovala určité zásady.

1.2.2 Integrita

Termínem integrita rozumíme zajištění správnosti a úplnosti informací. Snahou je zabránit nežádoucí změně dat, ke které by mohlo dojít technickým selháním, náhodou nebo úmyslně.

1.2.3 Dostupnost

Nejčastěji bývá dostupnost definována jako zajištění přístupu k informaci pro oprávněného uživatele v okamžiku, kdy to uživatel potřebuje. [11]

Dostupnost systému bývá často označována termíny RTO (Recovery Time Objective) a RPO (Recovery Point Objective).

Recovery Time Objective označuje dobu, za jak dlouho po výpadku musí být systém funkční. Naproti tomu Recovery Point Objective znamená, kolik dat může být ztraceno v případě výpadku systému.

1.3 Motivace pro zabezpečení

Motivací, proč zabezpečit svůj informační systém, může být jednoduchá rovnice. Bezpečnost rovná se peníze. Počítačové viry, spam, cílené útoky vedené po Internetu a zneužívání počítačové infrastruktury jsou stále častějšími případy narušení chodu firem a představují mnohdy i nemalé finanční ztráty.

Tyto škody způsobené narušením síťové a informační infrastruktury firmy mohou výrazně převýšit náklady na zabezpečení proti těmto rizikům.

Prvním a velice důležitým krokem při ochraně dat je mít stanovenou bezpečnostní politiku, někdy taky nazývanou zásady zabezpečení. Tyto zásady pomáhají předcházet bezpečnostním hrozbám a snaží se o minimalizaci případných ztrát vzniklých v důsledku bezpečnostních incidentů. Zjednodušeně řečeno se zásady zabezpečení podobají příkazům,

pravidlům a zákonům, kterými se řídíme v našem životě. Bezpečnostní politika tedy určuje, jaké chování je a není přípustné. Bývá vyjádřena písemnou formou a dává odpovědi na základní otázky:

- co se snažíme chránit,
- proti jakým hrozbám se snažíme chránit,
- jakým způsobem budeme ochraňovat to, co vyžaduje ochranu,
- jak pravděpodobná jsou jednotlivá rizika.

1.4 Analýza organizace

Jinak bude k otázce bezpečnosti přistupovat malá firma a jinak velká organizace se spoustou poboček. Protože se bezpečnostní politika různých firem liší, je nutné vždy provést nejprve analýzu dané firmy, která se skládá z následujících bodů:

1.4.1 Analýza aktiv

V tomto bodu se vymezuje, co chce firma chránit. Může se jednat o následující aktiva:

- Informace – dokumenty, databáze
- Hardware – servery, pracovní stanice, síťové prvky, tiskárny, kabely
- Software – operační systémy, programy
- Budovy – ve kterých se nacházejí výše uvedená aktiva

1.4.2 Analýza hrozeb

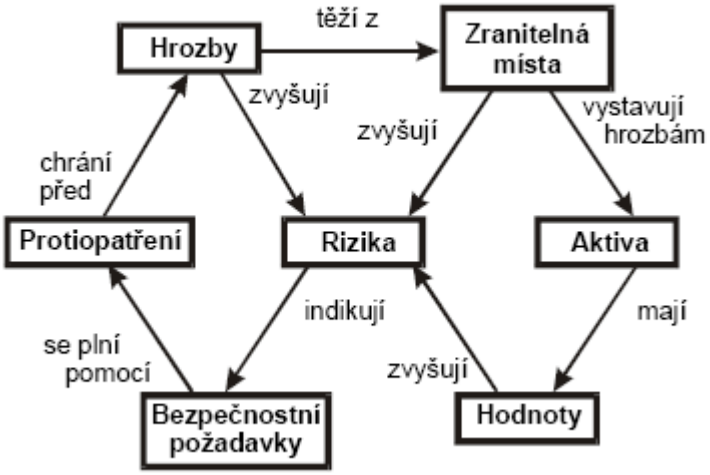
V tomto kroku se definují hrozby, proti kterým chce firma ochránit svá aktiva. Hrozby jsou úmyslné či náhodné okolnosti, jenž mohou vést k poškození aktiv. Může se jednat o zneužívání technických prostředků informačního systému, vyzrazení, zničení, znepřístupnění informací a podobně.

U jednotlivých hrozeb se stanovuje úroveň hrozby, její pravděpodobnost a úroveň zranitelnosti aktiva vůči hrozbě.

1.4.3 Analýza rizik

U této analýzy se určuje, jaká rizika hrozí aktivům a jak velká jsou tato rizika. Dále se zjišťuje, zda jsou pro firmu tato rizika přijatelná, nebo naopak, která rizika je nutno eliminovat.

Následující obrázek nám ukazuje vzájemné vztahy mezi pojmy používanými při analýze rizik.



Obr. 1 Vzájemné vztahy při analýze rizik

Díky kompletní analýze poznáme detailně celou organizaci. Zjistíme možné hrozby, které mohou působit na zranitelná místa. Výsledkem zhodnocení těchto analýz je návrh různých protiopatření, která slouží k eliminaci hrozeb. Díky provedené analýze vznikne bezpečnostní dokumentace, ve které se zohlední specifikace dané organizace.

Tato dokumentace je závazná pro celou organizaci, včetně pracovníků externích společností, kteří využívají informační prostředky společnosti, a stává se základním pilířem řešení bezpečnosti.

Tato bezpečnostní dokumentace pokrývá oblasti od základních zásad a principů zajištění bezpečnosti, přes pracovní postupy, až po technické detaily (nastavení a konfigurace různých zařízení).

1.5 Zásady zabezpečení

Bezpečnostní dokumentace se používá pro bližší určení bezpečnostní politiky. V této dokumentaci jsou podrobněji definovány zásady pro jednotlivé oblasti bezpečnosti tak, aby jejich dodržování bylo možné zkontrolovat.

1.5.1 Tvorba hesla

Jako příklad si můžeme uvést dokument nazvaný zásady pro tvorbu a používání hesel. Hesla se používají k autentizaci uživatele, kdy uživatel zadá svůj uživatelský kód (login), kterým se identifikuje v systému, a heslo (password), které slouží k ověření jeho totožnosti.

Uživatelé mají obecně tendenci si vytvářet hesla lehce zapamatovatelná. Ve většině případů se jedná o hesla kratší než osm znaků, jednoduchá slova, jako jsou jména blízkých osob, domácích mazlíčků, názvy měsíců, data narození a podobně. Taková hesla jsou zcela nevhodná, protože jsou snadno uhodnutelná, například za pomoci slovníkového útoku.

1.5.2 Požadavky na heslo

Pro přihlášení do systémů je tedy vhodné použít silné heslo, které lze charakterizovat takto:

- délka hesla je nejméně deset alfanumerických znaků
- obsahuje malá i velká písmena
- obsahuje číslice a speciální znak (například @ # $ % & * / +)
- není tvořeno žádným slovem z běžného slovníku
- není odvozeno z žádných osobních údajů uživatele

Rozdíl mezi slabým a silným heslem je patrný z uvedeného příkladu:

- slabé heslo – „franta123“, „micinka“, „heslo“, „cervenec2010“
- silné heslo – „Kg*gr7uG9vnqvKj“, „HD/331j2SgM1*ph“

Dále je vhodné zajistit pravidelnou změnu hesla po určitém časovém období a zajistit, aby si uživatelé nemohli zadat stejné heslo, případně aby si nestřídali pouze dvě hesla.

Použitím zásad pro tvorbu a používání hesel určíme pro uživatele standard pro vytváření silných hesel a způsob jejich změny.

Jiným příkladem vypracované zásady zabezpečení může být dokument s názvem zásady pro práci s elektronickou poštou nebo pravidla pro práci s výpočetní technikou.

1.6 Vypracování bezpečnostní dokumentace

Při tvorbě bezpečnostní dokumentace může firma narazit na množství problémů. Ne každá firma má dostatek zkušeností s tvorbou takové dokumentace. Úskalím může být nepřehlednost, přílišná detailnost nebo naopak povrchnost.

Z tohoto důvodu může podnik požádat o pomoc konzultační firmu. Tyto firmy mají s vypracováváním bezpečnostní dokumentace bohaté zkušenosti.

Pokud má firma ustanoveny klíčové bezpečnostní dokumenty, je nutné zajistit dodržování definovaných pravidel a zásad. Je důležité také zajistit zpětnou vazbu, která způsobí, že se případné změny promítnou do příslušné dokumentace a do procesu řízení bezpečnosti.

Změny okolního prostředí, změny priorit organizace, stejně jako reakce na nově se objevující rizika mohou vyvolat potřebu vrátit se k některému z předchozích kroků řešení bezpečnosti, a provést tak například doplňkovou analýzu rizik nebo doplnit chybějící bezpečnostní standard nebo směrnici.

1.7 Typy bezpečnostních politik

Bezpečnostní politika se dělí na čtyři základní typy podle požadované úrovně zabezpečení.

1.7.1 Promiskuitní bezpečnostní politika

Jedná se o bezpečnostní politiku, která nikoho neomezuje, protože každému v zásadě povoluje dělat všechny činnosti, tedy i takové, které by dělat neměli.

Výhody: nízké náklady na provoz

Nevýhody: zajišťuje pouze minimální nebo vůbec žádnou bezpečnost, ta musí být

případně zajištěna mimo informační systém

1.7.2 Liberální bezpečnostní politika

Umožňuje uživateli dělat vše, co není explicitně zakázáno. Tato bezpečnostní politika je často uplatňována v prostředí, ve kterém se považují potencionální hrozby za málo až průměrně závažné.

Výhody: vyšší bezpečnost než u promiskuitní bezpečnostní politiky, nízká cena

Nevýhody: nelze použít v systémech s vyšším rizikem

1.7.3 Racionální bezpečnostní politika

Tato bezpečnostní politika zakazuje dělat vše, co není explicitně povoleno.

Výhody: zaručuje vysoký stupeň bezpečnosti

Nevýhody: nákladnější na zavedení

1.7.4 Paranoidní bezpečnostní politika

Použitím této bezpečnostní politiky je zaručen nejvyšší stupeň bezpečnosti, protože zakazuje dělat vše, co je potencionálně nebezpečné, včetně toho, co by nemuselo být explicitně zakázáno.

Výhody: maximální bezpečnost

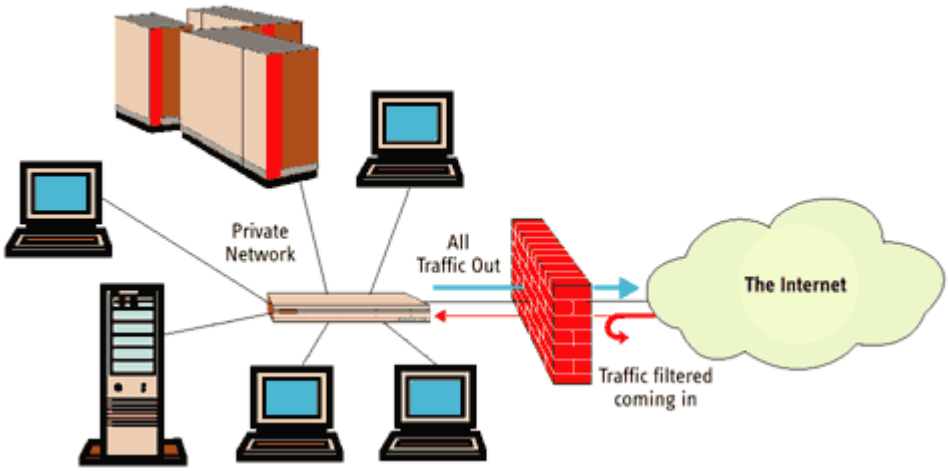
Nevýhody: omezení funkčnosti systému, v extrémních případech může vést k izolaci celého systému

2 METODY OCHRANY DAT

2.1 Firewall

Firewall je důležitou součástí při zabezpečení síťového provozu. Termín firewall se dá volně přeložit jako protipožární zeď, i když skutečný význam je spíše bezpečnostní brána.

Běžným příkladem použití je ochrana firemní sítě proti nepovoleným přístupům z Internetu. Jak je patrno z níže uvedeného obrázku, jedná se totiž o zařízení či software oddělující provoz mezi dvěma sítěmi, přičemž propouští dovnitř sítě nebo ven ze sítě data podle určitých, předem definovaných pravidel. [8]



Obr. 2 Funkce firewallu

Nastavení pravidel pro komunikaci přes firewall se běžně označuje termínem bezpečnostní politika firewalu. Tato bezpečnostní politika zahrnuje nejen samotná pravidla komunikace mezi sítěmi, ale u většiny dnešních produktů také různá globální nastavení, překlady adres (NAT – Network Address Translation), pokyny pro vytváření šifrovaných spojení mezi šifrovacími branami (VPN – Virtual Private Networks) nebo vyhledávání protokolových anomálií (IDS – Intrusion Detection System).

2.1.1 Softwarový firewall

Tento firewall se někdy rovněž označuje jako personální firewall. Mívá obvykle podobu speciálního software, který bývá nainstalován na počítači, který je připojen k Internetu.

Většina společností vyrábějících zabezpečovací software prodává firewally jako samostatné programy nebo jako součást jiného zabezpečovacího programu, například antiviru.

Příkladem takového spojení může být produkt Symantec Endpoint Protection od firmy Symantec[1].

Obr. 3 Softwarový firewall a antivir Symantec Endpoint Protection

Dalším příkladem softwarového typu firewallu může být Windows Firewall, který firma Microsoft zaintegrovala přímo do operačního systému.

[1] http://www.symantec.com/index.jsp

2.1.2 Hardwarový firewall

Bývá realizován jako samostatné zařízení, ale často je též součástí jiné hardwarové síťové komponenty, jako je například router[2] nebo switch[3]. Tento druh firewallu poskytuje zabezpečení proti napadení opravdu na vysoké úrovni.

Jedním zařízením lze chránit více počítačů současně, což u velkých sítí usnadňuje nároky na jejich konfiguraci. Další výhodou je rovněž fakt, že fungují nezávisle na operačním systému nainstalovaném na jednotlivých počítačích v síti. [13]

Obr. 4 Hardwarový firewall CISCO

[2] zařízení, které se používá ke spojení alespoň dvou sítí

[3] aktivní síťový prvek, propojující jednotlivé segmenty sítě

2.2 Antivirová ochrana

Další neméně důležitou součástí zabezpečení je antivirová ochrana. Počítačové viry patří mezi nejstarší hrozby a jejich historie je skoro stejně stará jako historie samotných počítaců.

Vznik prvního viru, jenž nesl jméno Brain, se datuje do roku 1986. Napsali ho dva bratři Basit a Amjad Alvi z Pákistánu. Autoři viru se zabývali prodejem softwaru a v těle viru zanechali textovou zprávu se svými jmény, adresou a telefonním číslem. Nutno podotknout, že virus Brain neměl žádné destruktivní účinky, obsahoval pouze následující reklamu:

Welcome to the Dungeon

(c) 1986 Basit & Amjad (pvt) Ltd.

BRAIN COMPUTER SERVICES

730 NIZAB BLOCK ALLAMA IQBAL TOWN

LAHORE-PAKISTAN
PHONE :430791,443248,280530.

Beware of this VIRUS....

Contact us for vaccination..... $#@%$@!!

V dřívějších dobách byly nejčastějším zdrojem pro šíření virů diskety, jejich úlohu však s rozvojem technologií v dnešní době převzal Internet.

Škodlivý kód se dnes z větší části přenáší prostřednictvím e-mailů, různých programů stahovaných z Internetu nebo třeba návštěvou webových stránek s pornografií či warezem[4].

[4] autorská díla, se kterými je nakládáno v rozporu s autorským právem

2.2.1 Typy počítačových virů

Když už hovoříme o virech, bylo by vhodné seznámit se s definicí, co je to počítačový vir. Jedná se o vědomě vytvořený program, který je schopen sám sebe, bez vědomí uživatele, šířit dále.

Většinou je vytvořen za účelem narušení fungování počítače, nahrání, porušení či smazání dat, případně k dalšímu šíření do jiných počítačů a po Internetu. [14]

2.2.1.1 Backdoor

Představuje škodlivý kód, který v infikovaném počítači otevírá zadní vrátka pro vzdáleného útočníka a umožní mu přístup do počítače bez vědomí uživatele. Takto napadený stroj pak může útočník využít ke skladování a distribuci nelegálního obsahu, k šíření spamu nebo k útokům typu DoS a DDoS na další počítače.

Útoky DoS a DDoS probíhají v praxi většinou tak, že provoz na síti je zaplaven množstvím náhodných dat, je narušeno konfigurační nastavení a cílový server je extrémně vytížený. Výsledkem bývá v lepším případě nedostupná služba či web, v horším případě pak zhroucení služby, pád operačního systému a nutný restart serveru, případně i obnovení nastavení. [15]

Zatímco útok typu DoS provádí útočník z jediného počítače, u distribuovaného DoS útoku je do akce zapojeno více počítačů. Útočník si nejprve vybírá server, síť nebo službu, kterou chce z nějakého důvodu vyřadit z provozu, a svou roli zde hraje i zranitelnost daného serveru, tedy slabá či nechráněná místa systému.

2.2.1.2 Trojský kůň

Toto označení získaly programy podle řecké báje o dobytí města Trója. Na první pohled se vydávají tyto trojské koně za neškodný program, užitečnou utilitu nebo hru, ale skrytě provádí jinou škodlivou činnost.

2.2.1.3 Keylogger

Program skrytě monitoruje jednotlivé stisky kláves, které ukládá do logu a následně odesílá na předem dané e-mailové adresy. Díky tomu může dojít třeba k vyzrazení hesla.

2.2.1.4 Worms

Nazývané také červi, jsou specifickým typem škodlivého kódu. Neinfikují soubory, ale šíří se prostřednictvím počítačové sítě. Díky tomu se vyznačují velmi vysokou rychlostí šíření.

2.2.1.5 Makroviry

Makroviry využívají toho, že dokumenty určitého formátu mohou obsahovat kód, který je spuštěn při práci s dokumentem a který může být virem infikován. Nejčastěji jsou makroviry infikovány aplikace Word a Excel z kancelářského balíku Microsoft Office.

2.2.1.6 Souborové viry

Souborové viry napadají spustitelné soubory typu (COM, BAT, EXE).

2.3 Speciální případy infiltrace

Kromě virů a červů se můžeme setkat se specifickou skupinou programů, které nemají destruktivní charakter, ale mohou značně znepříjemňovat práci uživatelům a správcům počítačových sítí.

2.3.1 Spyware

Svůj název získal od anglického slovíčka spy, což v českém jazyce znamená špión. Tento software odesílá z počítače data, často bez vědomí jeho uživatele. Obsahem těchto dat může být přehled navštívených webových stránek nebo nainstalovaných programů. Tyto informace pak mohou být zneužity k nevyžádané reklamě.

2.3.2 Adware

Jedná se o aplikaci, která má co do činění s reklamou. V některých případech se může jednat o specifický způsob licencování programu, kdy je uživatel při instalaci programu na existenci adware upozorněn a musí s ním souhlasit.

Během použití takového programu je zobrazována reklama ve formě banneru nebo vyskakujících pop-up oken.

2.3.3 Spam

Jedná se o nevyžádané masově šířené sdělení nejčastěji reklamního charakteru. Problém spamu spočívá především v tom, že zatěžuje síť a zbytečně snižuje kapacitu emailové schránky.

2.3.4 Hoax

Tímto termínem se v počítačovém světě nejčastěji označuje zpráva, která varuje před neexistujícím nebezpečným virem a zároveň žádá o předání této zprávy co největšímu počtu uživatelů. Snaží se přesvědčit příjemce o tom, že varování přišlo z důvěryhodných zdrojů, například z některé velké společnosti jako je Microsoft nebo IBM.

Jako hoax můžeme také označit šířenou zprávu, která obsahuje nepřesné, zkreslující informace, účelově upravené polopravdy nebo směsku polopravd a lží. [16]

V praxi se můžeme setkat s těmito hoaxy:

- popisy jiného nebezpečí – většinou se jedná o smyšlené nebezpečí z běžného života (infikované jehly na sedadlech v MHD, nová funkčnost bankomatu)
- falešné prosby o pomoc – typickým případem jsou prosby o darování krve pro nemocného člověka
- fámy o mobilních telefonech – vymyšlené nebo zkreslené informace o mobilních telefonech
- petice a výzvy – v případě připojení osobních údajů k těmto zprávám, hrozí jejich zneužití
- pyramidové hry a nabídky na snadné výdělky – nabídky na odměnu nebo slevu
- řetězové dopisy štěstí – jedná se o různé modlitby, poselství nebo žertovné zprávy

2.3.4.1 Příklad poplašné zprávy č.1

Oficiálně z banky:

Jakmile se ocitnete v situacii a musíte pod nátlakem vybrat peníze z bankovního automatu na požádáni/přinuceni nasilnikem, zadejte svůj PIN opačně: to je od konce - např. máte-li 1234, tak zadáte 4321, automat vám peníze přesto vydá, ale též současně přivolá policií,

která vám přijde na pomoc. Tato zpráva byla před nedávnem vysílaná v TV, protože málo lidí využívalo tuto skutečnost, protože o tom nevěděli.

Přepošlete toto co nejvíce lidem. [16]

2.3.4.2 Příklad poplašné zprávy č. 2

Subject: Pošli dál, záleží na tom život dítěte

Obdržel jsem od polských přátel níže uvedený text: Je to důležitá zpráva. Stručný překlad: Tomek má 14 let a v posledním měsíci byl nalezen na mozku nádor. Každým dnem se jeho stav zhoršuje. Jeho rodina je chudá a nemá peníze na složitou operaci, která ho může zachránit. Z tohoto důvodu se rozhodl Portál Onet.pl chlapci Tomkovi pomoci. Za každý e-mail bude platit na konto symbolickou částku 1 ZL(cca 7,5CZK).Na oparaci vystačí, když e-mail obdrží 7500 osob. Záleží na Vaší dobré vůli a dobrém úmyslu poslat zprávu všem, které máte v adresáři.. Možná, že díky právě Vám bude Tomek žít.

Konec konců...může se to přihodit komukoliv.... [16]

Na první pohled se může zdát, že šíření takových zpráv nemůže být škodlivé. Ale opak je pravdou. Stejně jako u spamu, rozesíláním těchto zpráv dochází k zbytečnému zatěžování linek a poštovních serverů.

Také pro mnohé uživatele je nepříjemné, pokud dostanou takové zprávy opakovaně.

2.3.5 Phishing

Phishingem se označuje e-mailová zpráva, jejímž cílem je vylákat z příjemce jeho důvěrná data (PIN, informace o kontech, číslo platební karty), která se dají dobře zneužít.

Nemusí jít jenom o účty přímo bankovní, ale také ostatních organizací, kde dochází k manipulaci s penězy nebo je možné jakýmkoliv způsobem zneužít jejich služeb. Příkladem můžem být PayPal, eBay, Skype, Google.

Text může vypadat jako informace o neprovedení platby, výzva k aktualizaci bezpečnostních údajů, oznámení o dočasném zablokování účtu či platební karty, výzkum klientské spokojenosti nebo jako elektronický bulletin pro klienty. [17]

Nejlepší ochranou proti phishingu je zdravý rozum a ostražitost.

2.3.5.1 Příklad phishingu č.1

Rádi bychom Vás informovali, že jsme v současné době provádí pravidelnou údržbu a modernizaci našeho účtu služby a jako výsledek této vaše účty musí být modernizovány.

Omlouváme se za způsobené nepříjemnosti.

Pro udržení svého účtu, musíte odpovědětTento e-mail okamžitě a zadejte informace níže: jméno ::.....

Heslo: .....

Nestane-li se do 48 hodin bude okamžitě učinit váš účet deaktivován z naší databáze. Děkujeme Vám za využití našich služeb!

"WEBMAIL SUPPORT

© WEBMAIL ACCOUNT ABN 31 088 377 860 Všechna práva vyhrazena. E-mailový účet údržba. [17]

2.3.5.2 Příklad phishingu č.2

Vazeni klienti,

radi bychom Vas upozornili na novou verzi podvodneho e-mailu (tzv. phishingu). Nova verze e-mailu ma jako ty predesle vzbudit dojem, ze byla odeslana z e-mailove adresy Ceske sporitelny, tentokrat vsak z oficialni e-mailove adresy banky csas@csas.cz. Obsahuje odkaz v tele na udajne webove stranky internetoveho bankovnictvi banky a uzivatel je vyzvan k prihlaseni, tedy zadani osobnich bankovnich udaju.

Prosim, verifikujte tuto emailovou adresu kliknutim na spojeni nize: http://www.csas.cz/banka/appmanager/portal/banka

Verifikovaci spojeni je platne do 24 hodin. [17]

2.4 Antivirové programy

Když už tedy víme, s čím vším se lze setkat na poli virů, můžeme se podívat také na to, jakými prostředky se lze bránit. K tomuto účelu slouží antivirové programy. Ty chrání počítače před nepříjemnými následky infiltrace škodlivých programů.

Antivir provádí kontrolu proti infiltraci pomocí následujích metod:

- porovnání s virovou databází
- heuristická analýza
- kontrola integrity

2.4.1 Virová databáze

Antivir porovnává skenovaná data s databází známých virů, důležitá je pravidelná aktualizace této virové báze.

2.4.2 Heuristická analýza

Základem této metody je emulátor kódu a existence virtuálního prostředí. Emulátor kódu dokáže spustit soubor a nasimuluje ve virtuálním prostředí spuštění kódu, jako kdyby ho spustil uživatel sám.

Protože emulátor tuto činnost provádí ve virtuálním prostředí, nemůže tak v případě spuštění infikovaného souboru dojít k ohrožení.

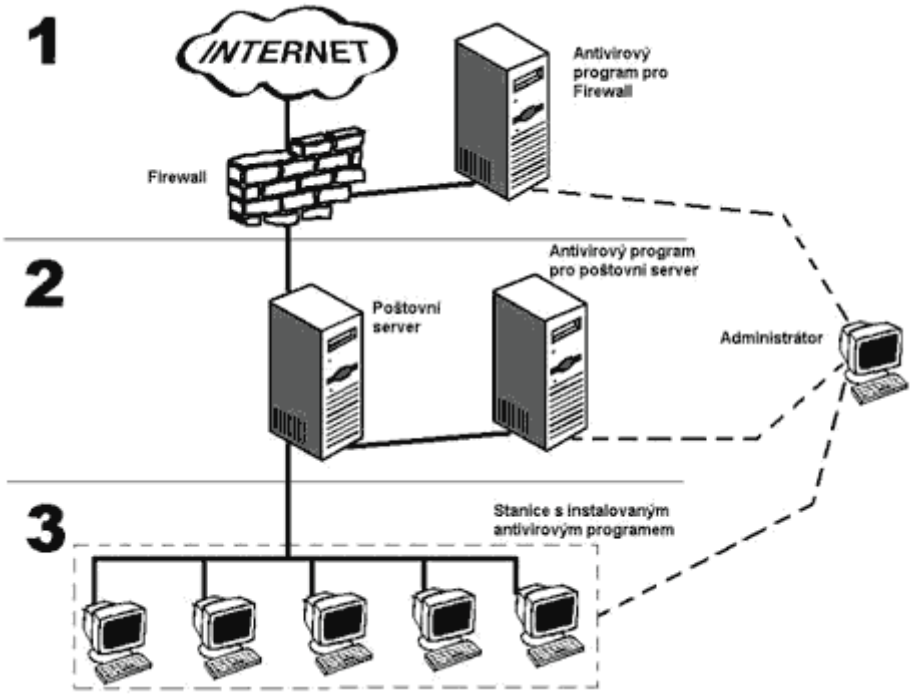
2.4.3 Kontrola integrity

Kontrola integrity je založena na porovnávání aktuálního stavu souborů a oblastí na disku s informacemi, které si kontrolní program (integrity checker) uschoval při posledním spuštění, popřípadě při jeho instalaci. Jestliže se do takto chráněného počítače dostane virus, zdvořile na sebe upozorní změnou některého z kontrolovaných objektů a může být zachycen kontrolou integrity. [18]

2.5 Centrální správa a víceúrovňová ochrana

V případě antivirové ochrany je vhodné nespoléhat se pouze na jednu úroveň, ale vybudovat tuto ochranu ve více úrovních. V případě počítačové sítě je základní úroveň představována antivirovým programem nainstalovaným na pracovní stanici nebo notebooku. Další úrovně mohou být řešeny antivirem na internetové vstupní bráně, poštovním nebo souborovém serveru.

Výhodou je fakt, že v případě selhání některé z úrovní zbývá minimálně jedna další, která je schopná škodlivý kód zachytit a případně eliminovat.



Obr. 5 Víceúrovňové řešení antivirové ochrany

Nezbytným a neméně důležitým prvkem komplexního antivirového řešení je také účinná centrální správa, která administrátorovi umožňuje spravovat celý provázaný systém z jednoho místa v lokální síti nebo dokonce přímo ze vzdáleného počítače umístěného mimo chráněné sítě. [19]

2.6 Šifrování

Použití kryptografie (šifrování) nám pomůže vyřešit spoustu problémů v mnoha oblastech počítačové bezpečnosti. Pokud hovoříme o šifrování, pak máme na mysli proces, který na základě určitého algoritmu a šifrovacího klíče šifruje data do nečitelné podoby. V případě opětovného použití lze data vrátit zpět do čitelné podoby.

Šifrovací metody lze rozdělit na:

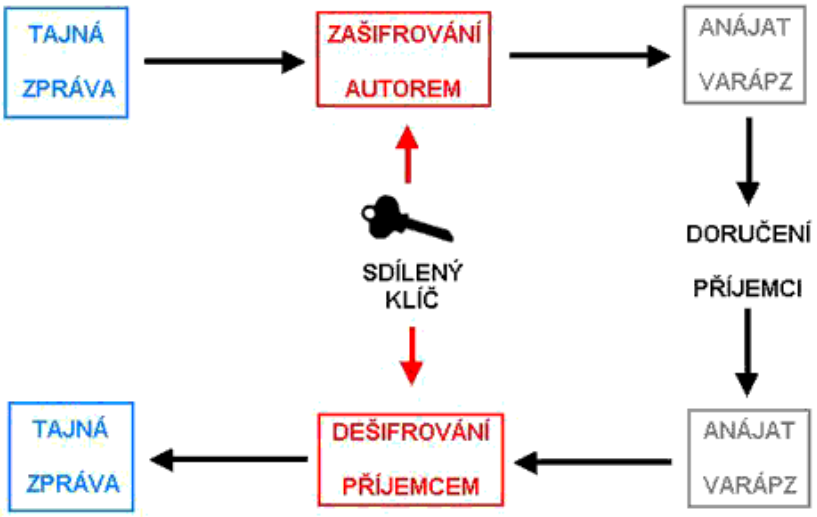
- jednosměrné – používá pouze proces zašifrování, nelze tedy provést zpětný proces odšifrování
- obousměrné – po zašifrování lze za pomoci správného klíče dešifrovat výsledek a získat zpět originál

Jiné možné rozdělení je podle druhu klíče na:

- šifrování s privátním klíčem (symetrické)
- šifrování s veřejným klíčem (asymetrické)

2.6.1 Šifrování s privátním klíčem

Při tomto druhu šifrování se používá pouze jediný klíč, který použijeme jak pro zašifrování, tak pro dešifrování. Výhodou tohoto způsobu je nízká výpočetní náročnost. Nevýhodou je, že autor zprávy a její příjemce se musí dohodnout na bezpečném předání sdíleného klíče.

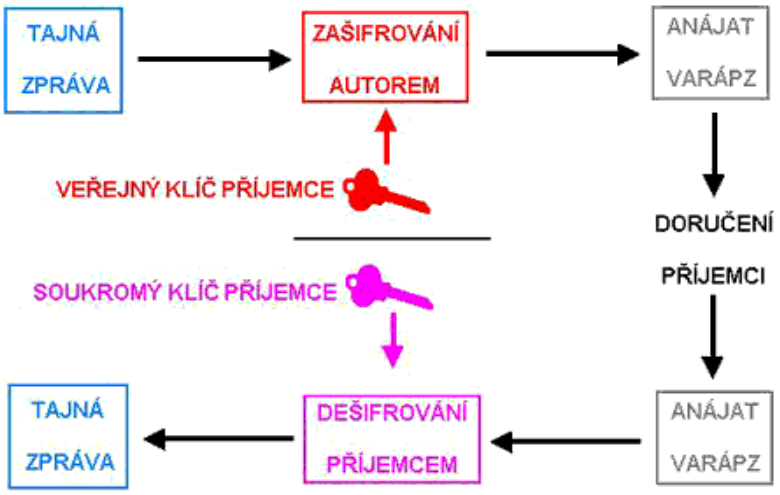


Obr. 6 Symetrické šifrování

2.6.2 Šifrování s veřejným klíčem

Při asymetrickém šifrování se používá dvojice klíčů – veřejný a soukromý. Použitím dvojice klíčů se eliminuje potřeba předání klíčů, jako tomu bylo v případě symetrického šifrování. Veřejný klíč je určen k volnému šíření narozdíl od soukromého, který je potřeba

chránit. Veřejným klíčem příjemce se zašifruje jemu určená zpráva, kterou má možnost dešifrovat pouze majitel přislušného soukromého klíče.



Obr. 7 Asymetrické šifrování

2.7 Zálohování

Zálohováním rozumíme vytvoření kopie dat na jiném datovém nosiči nebo místě. Záložní data jsou poté využívána v případě ztráty nebo poškození zazálohovaných dat. O tom, že zálohování je důležitý proces, se určitě přesvědčil každý, kdo někdy čelil ztrátě dat.

Způsoby poškození dat si můžeme rozdělit do několika skupin:

- poškození vlivem lidského faktoru – neúmyslné smazání, nedbalost
- poškození způsobené selháním systému – výpadek elektrického proudu, selhání hardware
- poškození s úmyslem data zničit – sabotáž, krádež, virová nákaza
- poškození přírodními vlivy – požár, voda

Typy záloh:

- plná
- inkrementální
- rozdílová

2.7.1 Plná záloha (full backup)

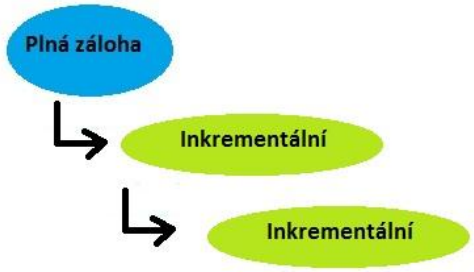
U plné zálohy jsou zvolená data zazálohována kompletně celá. Při další záloze je opět provedena kompletní kopie všech zvolených dat. Výhodou plné zálohy je, že každá záloha je nezávislá a samostatná. Na druhou stranu plná záloha zabírá nejvíce místa.

Obr. 8 Plná záloha

2.7.2 Inkrementální záloha (incremental backup)

U inkrementální zálohy je na začátku provedena plná záloha. V následujícím kole zálohování je provedena pouze záloha těch dat, u kterých proběhla změna oproti plné či předchozí inkrementální záloze.

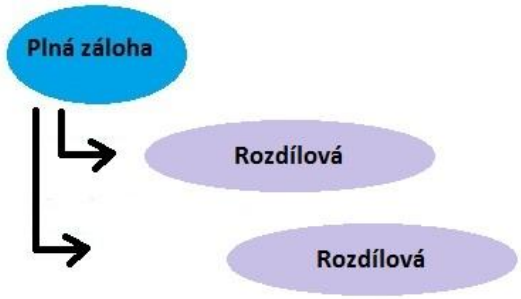
Výhodou tohoto typu záloh je úspora místa při zálohování. Naopak nevýhodou je, že při obnově je potřeba mít k dispozici celý řetezec záloh. Pokud je některá inkrementální záloha poškozena, pak není možno obnovit následující zálohy za touto poškozenou.



Obr. 9 Inkrementální zálohování

2.7.3 Rozdílová záloha (differential backup)

U rozdílové zálohy se zaznamenávají změny, které proběhly od plné zálohy. Pro případnou obnovu dat je potřeba mít plnou a příslušnou rozdílovou zálohu. Pokud dojde k poškození některé z rozdílových záloh, tak to nemá vliv na žádnou jinou rozdílovou zálohu.



Obr. 10 Rozdílové zálohování

3 BEZPEČNOSTNÍ MONITORING

Důležitou součástí kompletního zabezpečení je rovněž bezpečnostní monitoring. Jeho úkolem je detekce bezpečnostních událostí, které mají povahu útoku proti informačnímu systému.

3.1 IDS/IPS

Pod těmito zkratkami se skrývají dva systémy napomáhající lépe chránit firemní data, a to systém pro detekci narušení IDS (Intrusion Detection System) a pro prevenci průniku IPS (Intrusion Prevention System).

Systém IDS dokáže odhalit probíhající útok a s pomocí systému IPS zajistí přiměřenou reakci za účelem eliminace tohoto útoku. Systémy IDS/IPS jsou vhodným doplněním k ochraně za pomocí firewallu.

Metody detekce neoprávněného vniknutí:

- detekce vzoru – tato metoda porovnává datový tok na síti s databází signatur již známých útoků. Mezi výhody patří rychlost, přesnost a jednoduchost. Nevýhodou je problematická detekce nových útoků. Záleží totiž na tom, zda již existuje popis daného útoku v databázi signatur. Obvykle se tato metoda omezuje pouze na kontrolu jediného datového paketu.
- stavová detekce vzoru – jedná se o rozšíření předchozí metody, kdy je umožněno analyzovat datový tok, tím je umožněno detekovat i útoky rozdělené do více paketů.
- detekce anomálií – systémy, které používají tuto metodu, detekují odchylky od typického chování počítačové sítě. Systém může pracovat následujícím způsobem. V průběhu zavedení se IDS systém seznámí se sítí, zjistí informace o službách a protokolech, zavede si statistiku chování. Po tomto seznámení IDS systém sleduje provoz v síti a detekuje odchylky od typického chování. Nevýhodou mohou být falešné útoky. Naopak výhodou je schopnost zachytit nové, dosud neznámé útoky.

Systémy IDS obvykle využívají kombinaci těchto metod.

Dále si popíšeme architekturu systému IDS. Ten se zpravidla skládá ze dvou komponent – senzorů, které provádějí detekci a z dohledového systému. Senzory se dělí dle umístění na host-based a network-based IDS senzory.

3.1.1 Host-based IDS senzory

IDS systémy založené na těchto senzorech hledají útoky na úrovni operačního systému. Jedná se o softwarové produkty, které jsou instalovány na koncové stanice, kde monitorují systémová volání, chybová hlášení, logy a změna souborového systému. [20]

3.1.2 Network-based senzory

Tyto systémy sledují veškerý provoz v síti. K tomuto účelu mohou používat síťovou kartu v promiskuitním režimu. Tato síťová karta porovnává všechny pakety s databází známých útoků. Výhodou tohoto řešení je skutečnost, že tyto senzory jsou v síti velmi nenápadné a díky tomu jsou těžko zranitelné. [20]

3.1.3 Dohledový systém

Dohledový systém IDS má za úkol správu IDS senzorů. Má za úkol komunikovat s jednotlivými IDS senzory, které mu předávájí informace o realizovaných útocích. Dohledový systém IDS umožňuje konfiguraci senzorů IDS nebo aktualizaci databáze signatur, která obsahuje charakteristiky známých útoků. [20]

3.2 Počítačová návnada

Počítačová návnada představuje zajímavé rozšíření rodiny bezpečnostních produktů. Bývá realizována pomocí honeypot[5] neboli též decoy serverů. Jedná se v podstatě o přídavný server nebo celý počítačový systém, který se tváří jako atraktivní cíl útoku.

Cílem je nalákat potencionálního útočníka. K tomuto účelu je honeypot nastaven tak, aby vypadal, že je hůře zabezpečený, často má zvoleno provokativně lákavé jméno.

[5] Honeypot – z anglického jazyka, český překlad hrneček s medem

Počítačová návnada nám zajišťuje tyto důležité věci:

- pomáhá nám vyhodnotit, zda je navržené zabezpečení sítě dostatečné
- pomáhá nám poznat nepřítele, jeho techniky a metody, čímž nám umožní lépe se bránit proti dalšímu případnému zneužití
- odvádí pozornost útočníka od cennějších prostředků počítačové sítě

3.3 Bezpečnostní audit

Úkolem bezpečnostního auditu je zhodnotit zranitelnost našeho informačního systému. Jeho cílem je prozkoumat a identifikovat bezpečnostní slabiny a zjistit, jakým způsobem a v jakém rozsahu by bylo možné tyto chyby využít. Toto hodnocení může nabídnout detailní přehled o momentálním stavu bezpečnosti.

Bezpečnostní audit má několik základních typů, jenž se dělí podle svého konkrétního zaměření a rozsahu působnosti na:

- audit organizace bezpečnosti
- audit bezpečnosti komunikační infrastruktury
- audit bezpečnosti informačního systému
- audit bezpečnosti serverů
- audit bezpečnosti koncových stanic

3.3.1 Audit organizace bezpečnosti

Tento audit slouží ke komplexnímu posouzení celkového zajištění ochrany informací v organizaci. Jeho součástí je revize bezpečnostní dokumentace v celém jejím rozsahu, zhodnocení postupů souvisejících s provozem informačních technologií a účinnost krizových plánů.

3.3.2 Audit bezpečnosti komunikační infrastruktury

Zahrnuje zhodnocení celkové koncepce zabezpečení počítačové sítě. Pozornost je věnována zabezpečení komunikace, především komunikace prostřednictvím Internetu, klíčovým síťovým prvkům a zařízením zajišťujícím bezpečnost komunikace.

3.3.3 Audit bezpečnosti informačního systému

Posoudí zajištění ochrany informací, které zpracovává daný informační systém, včetně jejich ochrany před vstupem do systému a následně poté, když jsou jako výstup předány dále.

3.3.4 Audit bezpečnosti serverů

Je zaměřen na odhalení slabých míst v konfiguraci, v nastavení operačního systému

a v provozovaných aplikacích.

3.3.5 Audit bezpečnosti koncových stanic

Hodnotí zabezpečení provozovaných pracovních stanic a notebooků. Jsou při něm identifikovány případné slabiny v nastavení instalovaných operačních systémů a je rovněž posouzena úroveň zabezpečení provozovaných aplikací.

3.4 Penetrační testy

Praktickým způsobem, jak ověřit odolnost našich informačních technologií je penetrační test. Tento test reálně simuluje aktivity zkušeného útočníka. Penetrační testy lze rozdělit podle několika hledisek.

Podle testovaného prostředí:

- externí penetrační test – prověří systém proti útokům z Internetu
- interní penetrační test – slouží k prověření zabezpečení vnitřní sítě vůči útokům zevnitř firmy

Podle informovanosti:

- skrytou formou – subjekty, které mají zodpovědnost za správu prověřovaných zařízení nejsou předem o testu informovány. Kromě samotného prověření zařízení dojde také k prověření reakčních mechanismů odpovědných osob
- otevřenou formou – subjekty zodpovědné za správu testovaných zařízení jsou o testu informovány předem

Podle množství poskytnutých informací:

- bez znalosti prostředí – firma, která provádí penetrační test nemá žádné vstupní informace o testovaném prostředí, test je tak proveden bez jakýchkoli informací, tím dojde k plnohodnotné simulaci útoku hackera
- se znalostí prostředí – před samotným penetračním testem dojde k seznámení s testovaným prostředím

Jak penetrační testy, tak bezpečnostní audit mohou být prováděny jednorázově nebo opakovaně v pravidelných intervalech.

Na provádění bezpečnostních auditů se většinou firmy najímají externí společnosti. Ty nabízí, narozdíl od interního oddělení auditu, vyšší objektivitu a přináší možnost srovnání s jinými provozovanými systémy.

II. PRAKTICKÁ ČÁST

4 NÁVRH A IMPLEMENTACE SYSTEM CENTER OPERATIONS MANAGER

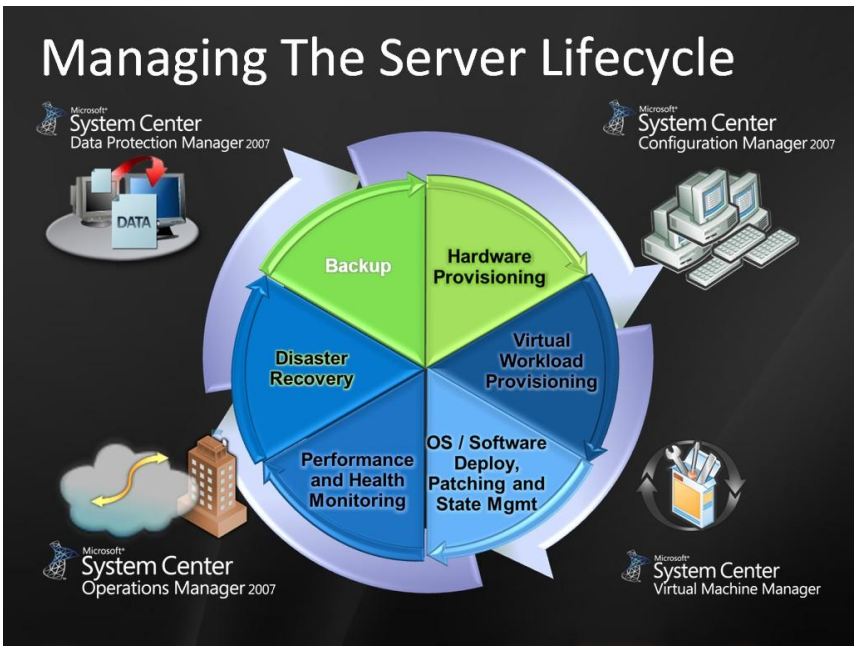
Cílem praktické části diplomové práce bylo navrhnout a následně provést implementaci monitorovacího systému System Center Operations Manager 2007 na vybrané servery provozované na platformě Microsoft Windows ve firmě Home Credit International, a.s.

4.1 Rodina System Center produktů

Řešení System Center od firmy Microsoft pomáhá správcům informačních technologií při správě jejich prostředí tak, aby mohli být schopni optimalizovat IT struktury s cílem snížit náklady, zlepšit poskytované služby a zvýšit dostupnost aplikací. [9]

Produkty System Center obsahují nástroje a funkce, kterými jsou schopny pokrýt životní cyklus každého serveru:

- nasazení
- správa
- monitorování
- zálohování



Obr. 11 Životní cyklus serveru

Životní cyklus serveru má několik částí a jak již bylo řečeno, na každou tuto část je zacílen některý z produktů System Center.

V následujícím přehledu si představíme jednotlivé produkty System Center.

4.1.1 System Center Configuration Manager (SCCM)

Microsoft System Center Configuration Manager 2007

Tento produkt je určen pro nasazení a správu koncových stanic a serverů. Umožňuje centrální plně automatizované nasazení případně reinstalaci všech podporovaných MS operačních systémů na fyzický HW.

Dále lze pomocí SCCM provádět hardwarovou a softwarovou inventarizaci, distribuovat a aktualizovat software či měřit využití softwaru uživateli. Umožňuje tak získat lepší přehled o IT systému a kontrolu nad ním.

4.1.2 System Center Virtual Machine Manager (SCVMM)

Microsoft System Center Virtual Machine Manager

System Center Virtual Machine Manager je určen pro správu fyzických a virtuálních počítačů. Umožňuje provést konsolidaci málo využívaných fyzických serverů a rychle vytvářet nové virtuální počítače.

4.1.3 System Center Operations Manager

Microsoft System Center Operations Manager 2007

System Center Operations Manager je schopen monitorovat IT prostředí. Pomocí SCOM je možno monitorovat stav serverů, klientských stanic, síťových prvků, služeb a aplikací. Protože implementací tohoto nástroje se zabývá i tato práce, detailněji si funkci tohoto produktu představíme později.

4.1.4 System Center Data Protection Manager (SCDPM)

Microsoft System Center Data Protection Manager 2007

Produkt System Center Data Protection Manager je produkt, který má na starost zálohování a disaster řešení. Zajišťuje nepřetržitou ochranu dat pro aplikace a souborové servery. SCDPM představuje centrální bod, kde se zálohují data, která se sbírají prostřednictvím agentů na produkčních serverech a zasílají se k archivaci.

4.2 Profil firmy HCI, a.s.

Společnost Home Credit International, a.s., je součástí skupiny Home Credit, která je poskytovatelem spotřebitelského financování na trzích střední a východní Evropy a střední Asie.

Skupina Home Credit náleží do silné mezinárodní finanční skupiny PPF, která se zabývá spotřebitelským financováním a retailovým bankovnictvím.

Home Credit International, a.s., je poradenskou a servisní společností orientovanou na členy skupiny Home Credit. Součástí Home Credit International je IT centrum, umístěné v Brně a Ostravě, které je zodpovědné za kompletní IT podporu včetně vývoje a provozu centrálních aplikací, kritických pro obchodní aktivity jednotlivých společností skupiny Home Credit. V současné době poskytuje podporu pro společnosti Home Credit v České republice, Slovenské republice, Ruské federaci, Kazachstánu, Bělorusku, Číně a Vietnamu.

4.2.1 Oddělení provozu

Provoz je jedním z oddělení ve firmě Home Credit International, a.s. Hlavní činností provozního oddělení je správa technologického prostředí, infrastruktury a provoz aplikací pro podporu finančních aktivit skupiny Home Credit. Patří sem správa technologií a jejich architektury v oblastech databází, aplikačních a webových serverů, operačních systémů (UNIX, Linux, Windows) a síťové infrastruktury. Dále spravuje hlavní a záložní datová centra v Brně a v Praze.

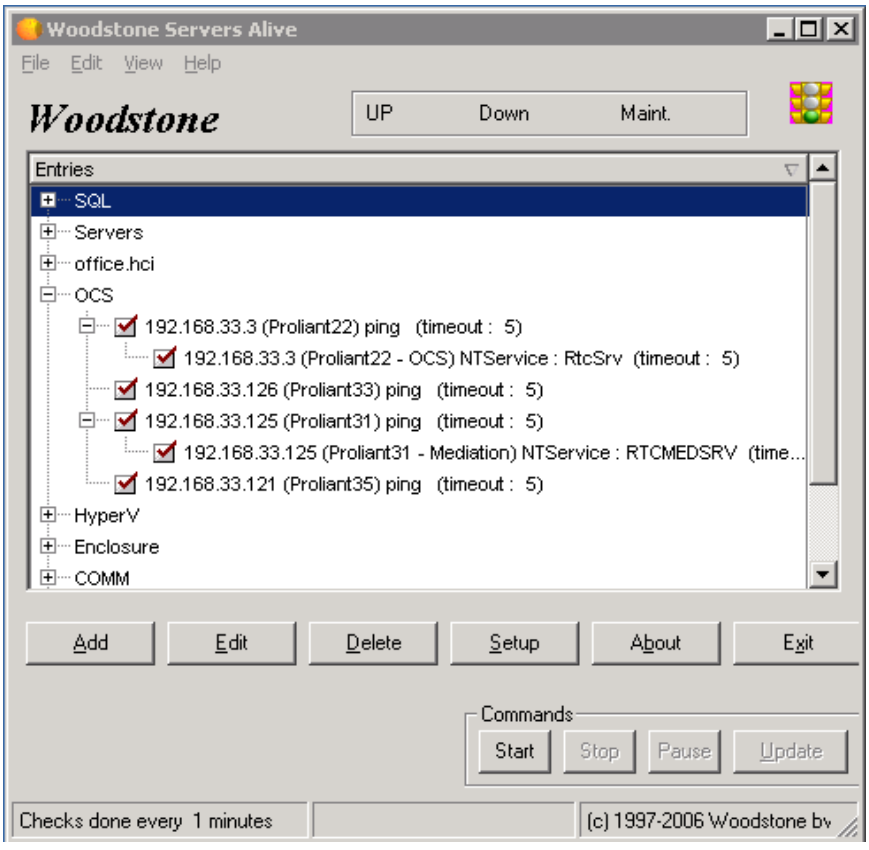
4.2.2 Windows team

Windows team je součástí oddělení provozu. Jeho hlavní náplní je podpora koncových uživatelů, instalace HW a SW pro tyto uživatele, instalace a provoz serverů na platformě MS Windows.

4.3 Monitorování serverů platformy MS Windows

4.3.1 Woodstone Servers Alive

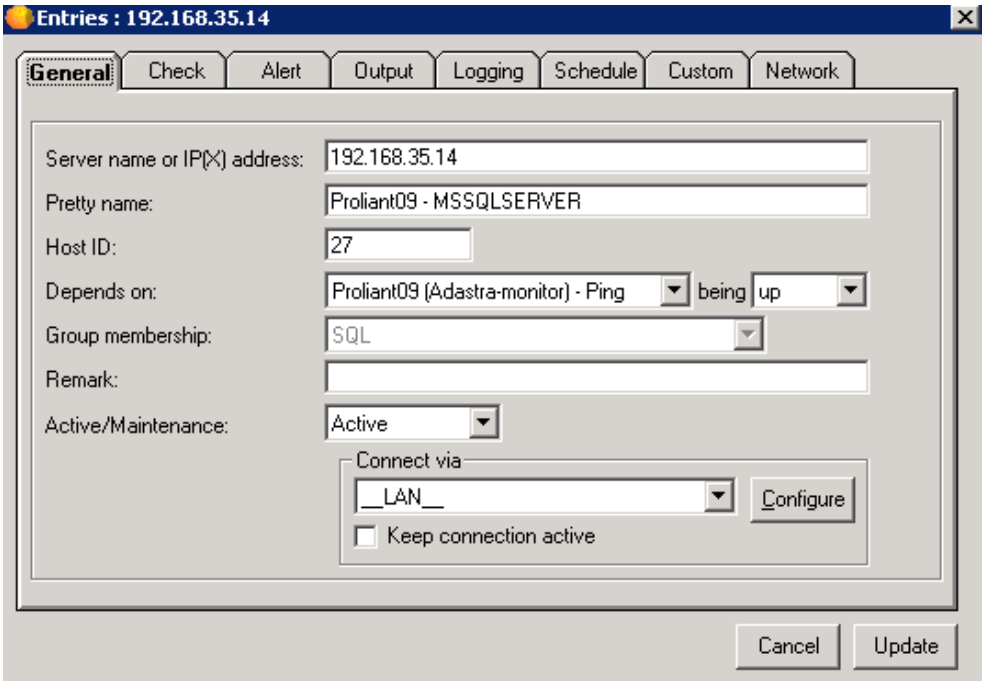
Před implementací monitorovacího nástroje SCOM používal Windows team na monitorování vybraných serverů aplikaci Woodstone Servers Alive[6].



Obr. 12 Monitorovací nástroj Woodstone Servers Alive

[6] http://www.woodstone.nu/salive/

Tento nástroj umožňuje nadefinovat jednoduché monitorovací a kontrolní úlohy, jako například ping hostitelského stroje, monitorování volného místa na disku vzdáleného počítače nebo kontrolu, zda je spuštěna určitá služba.



Obr. 13 Nastavení ping checku na dostupnost serveru

Tento nástroj sloužil velice dobře v době, kdy se Windows team staral o servery, jejichž počet nepřevyšoval dvě desítky. Vzhledem ke zvyšujícímu se počtu serverů ve firmě vyvstala potřeba nasazení nového monitorovacího prostředku.

4.3.2 System Center Operations Manager

Nasazením System Center Operations Manager se splnily požadavky, které byly kladeny na nový monitorovací nástroj:

- změna dohledu nad systémy z pasivního na proaktivní
- informace přijímané z monitorování jsou uloženy do databáze
- reportovací funkce
- flexibilnější řešení případných problémů při nasazení a provozování aplikace SCOM díky Microsoft Premier Support

5 IMPLEMENTACE SYSTEM CENTER OPERATIONS MANAGER

5.1 HW požadavky

Jako hardwarový základ pro nový monitorovací systém byl zvolen blade server ProLiant BL460c G1 od firmy Hewlett-Packard, který byl umístěn v hlavním datovém centru, které je vybaveno klimatizací, záložním zdrojem UPS a diesel generátorem pro případ výpadku elektrické energie.

Obr. 14 Blade server HP

ProLiant BL460c G1

HW konfigurace serveru:

Počet procesorů:	2
Procesor :	CPU Intel Xeon 2.66 Ghz
Pamět:	16 GB RAM DDR2
Harddisk:	2 x 146 GB 10k RPM nastavené v RAID 1 (mirroring)
Síťový adaptér:	2 x integrovaný 1Gb/s multifunční serverový adaptér

Z diskového pole byl připojen přes Fibre channel adaptér logický disk o celkové velikosti 300 GB, který byl určen jako úložiště pro SQL databáze, jenž potřebuje SCOM ke své činnosti.

5.2 SW požadavky

5.2.1 Operační systém

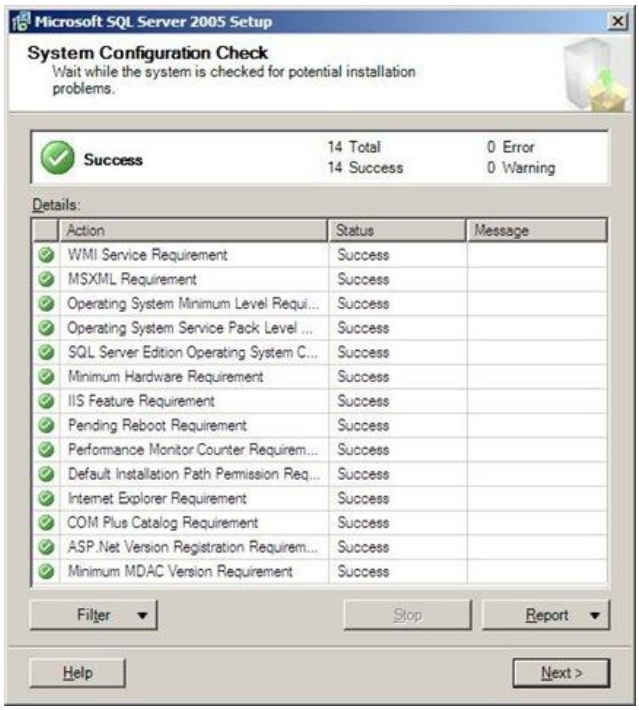
Na fyzický server byl nainstalován operační systém Microsoft Windows Server 2003 R2 Enterprise Edition SP 2. Po instalaci operačního systému a nezbytné konfiguraci sítě byly nainstalovány bezpečnostní záplaty. Následně byl server vložen do domény OFFICE.

5.2.2 SQL server

Protože SCOM využívá pro ukládání dat technologii SQL bylo potřeba provést instalaci Microsoft SQL Server 2005. U SQL Serveru je potřeba uvědomit si, že SQL má licenční podmínky, a že je potřeba pokrýt jeho použití licencemi Per Processor, nebo kombinací licencí pro server a klientskou přístupovou licencí CAL.

Microsoft však umožňuje u některých produktů, ke kterým patří i SCOM, zakoupit si tento produkt ve variantě „with SQL Technology“. Pokud se tedy rozhodneme zakoupit tuto verzi, není již nutné kupovat klientské licence SQL CAL.

Bohužel již však tento SQL server nelze použít k žádnému jinému účelu, než pro potřeby nástroje, k němuž byl pořízen.



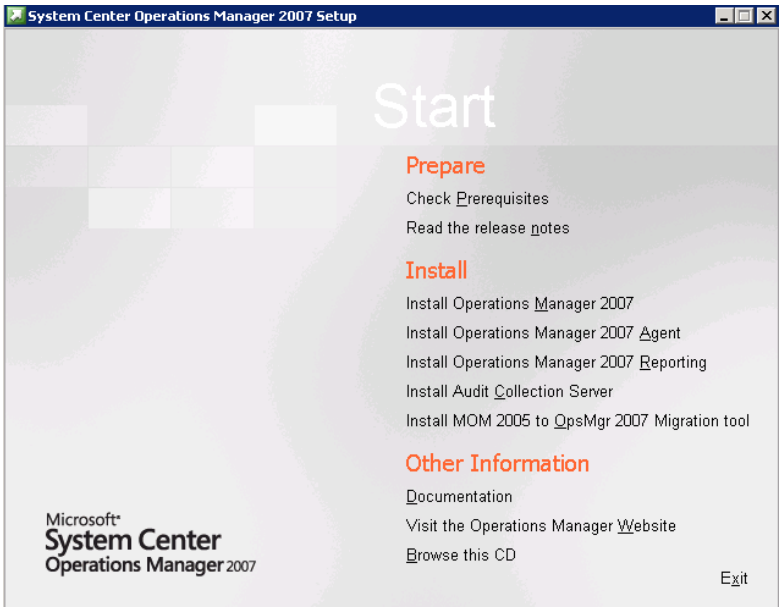
Obr. 15 Instalace MS SQL Serveru 2005

5.2.3 System Center Operations Manager

Po instalaci MS SQL Serveru bylo potřeba provést instalaci samotného nástroje System Center Operations Manager. Z licenčního hlediska je nutno při nákupu tohoto produktu pořídit serverovou licenci a licenci pro spravovaná zařízení. Licenční schéma je tedy velmi podobné tomu, co známe u jiných serverových produktů, jako je například již zmiňovaný SQL Server a CAL licence. Jediným rozdílem je, že místo CAL se používá označení ML (Management License).

Instalace se spouští z instalačního zdroje příkazem SetupOM.exe.

Instalace probíhá pomocí klasického GUI.



Obr. 16 Instalace SCOM 2007

V průběhu instalace System Center Operations Manageru se nastavuje instance SQL Serveru.

5.3 Instalace agentů System Center Operations Manager

Po úspěšné instalaci System Center Operations Manageru následuje instalace agenta na vybrané servery, které chceme pomocí SCOMu monitorovat. Pro každého monitorovaného klienta je třeba mít zakoupenu management licenci. Pro licenční politiku je třeba si osvětlit pojem OSE – Operating System Environment. Stručně řečeno je OSE operační systém a aplikace, které se na něm spouští. [10]

OSE se dělí na:

- Fyzické – physical operating system environment POSE
- Virtuální – virtual operating system environment VOSE

Management License je potřeba pořídit pro každý spravovaný operační systém (dále jen OSE), jak pro fyzický, tak pro virtuální. V licencování System Center je potřeba ještě rozlišit klientský a serverový OSE.

Jak je z názvu patrné klientský OSE je prostředí s jiným, než serverovým operačním systémem.

Podle typu monitorovaného OSE je třeba vybrat vhodný typ management licence. V našem případě se jedná o Operations Management License, která se dělí na tři různé typy:

- Client OML
- Standard Server OML
- Enterprise Server OML

5.3.1 Client OML

Tato licence slouží k monitorování jiného než serverového operačního systému.

5.3.2 Standard Server OML

Umožnuje monitorovat základní služby serverového operačního systému.

5.3.3 Enterprise Server OML

Monitoruje služby serverového operačního systému jako Standard server OML, ale navíc umožnuje získat dohled nad aplikacemi či službami (např. monitoring Exchange nebo SQL Serveru).

Pro monitorování byly vybrány servery, které zajišťují důležité funkce a u kterých je potřeba v případě problémů, co nejrychleji zjistit příčinu tohoto problému a provést nápravu tak, aby výpadek byl co nejkratší.

Vybrané servery jsou znázorněny v následující tabulce.

Název serveru	Použití serveru
P10	Primární doménový řadič PDC
P23	Záložní doménový řadič BDC
P201	Záložní doménový řadič BDC
P101	Záložní doménový řadič BDC v disaster centru
P11	SQL server pro analytické oddělení
P26	SQL server pro analytické oddělení
P14	VMWare server pro testovací účely
P22	Office Communications Server - FrontEnd
P24	SQL server
P25	VMWare pro servery Business Objects
P29	HYPER-V server
P31	Office Communications Server - Mediation
P32	Mail server – Exchange 2007
P33	Office Communications Server - WebAccess
P35	Office Communications Server - GroupChat
P38	Hyper-V server
P39	Hyper-V server
Intranet1	Sharepoint
P20	Cisco Secure Access Control Server
P21	Cisco Secure Access Control Server
P02	WSUS server

Tab. 1 Seznam serverů monitorovaných pomocí SCOM

5.4 Management pack

Dalším krokem k úspěšné implementaci SCOM je instalace management packů (MP). Tyto management packy jsou vlastně popisem informací o monitorovaných službách. Jedná se o balík předem definovaných pravidel, která jsou určena pro dohled nad službou, systémem, aplikací nebo hardware.

V management packu jsou také předpřipraveny základní reporty o monitorovaném zařízení či službě, a dále informace o konkrétních chybách a možnostech jejich řešení.

Každý management pack se skládá z několika základních prvků:

- Attributes – pravidla pro členění objektů do skupin dle definovaných atributů
- Rules – pravidlo pro monitorování stavu, výkonu, události
- Monitors – souhrn pravidel, vztahujících se k určitému monitorovanému objektu
    - Availability - dostupnost
    - Configuration - konfigurace
    - Performance - výkon
    - Security - zabezpečení
- Object discoveries – pravidla pro vyhledávání objektů a vztahů mezi nimi
- Tasks – předdefinované úkoly pro správu, které lze použít přímo z operační konzole
- Views – určené pro zobrazení stavů a alertů

Management pack tak obsahuje doporučené postupy ke zjišťování, monitorování a řešení potíží specifické součásti, ke které je určen.

Tyto management packy vytváří jednak přímo firma Microsoft pro své produkty a služby (Active Directory, SQL, Exchange, Sharepoint aj.), ale jsou také k dispozici management packy pro produkty třetích stran (Oracle, Linux, serverový HW), které vytváří partneři společnosti Microsoft.

V následujícím přehledu si uvedeme některé management packy, které byly nasazeny:

- Windows Server Operating System SystemCenterOperationsManager 2007 MP
- Windows Group Policy 2003 System Center Operations Manager 2007 MP
- SQL Server System Center Operations Manager 2007 MP
- Microsoft Windows DNS Server 2000 and 2003 System Center Operations Manager 2007
- Active Directory System Center Operations Manager 2007 MP
- Microsoft Exchange 2007 System Center Operations Manager 2007 MP

- Microsoft Windows File Replication Service System Center Operations Manager 2007 MP
- MICROSOFT Windows Server 2000 2003 and 2008 DHCP MP
- MICROSOFT Windows Server 2000 2003 and 2008 DNS MP
- Windows Server Hyper-V MP
- OCS2007_R2_SCOM2007

5.5 Konfigurace SCOM

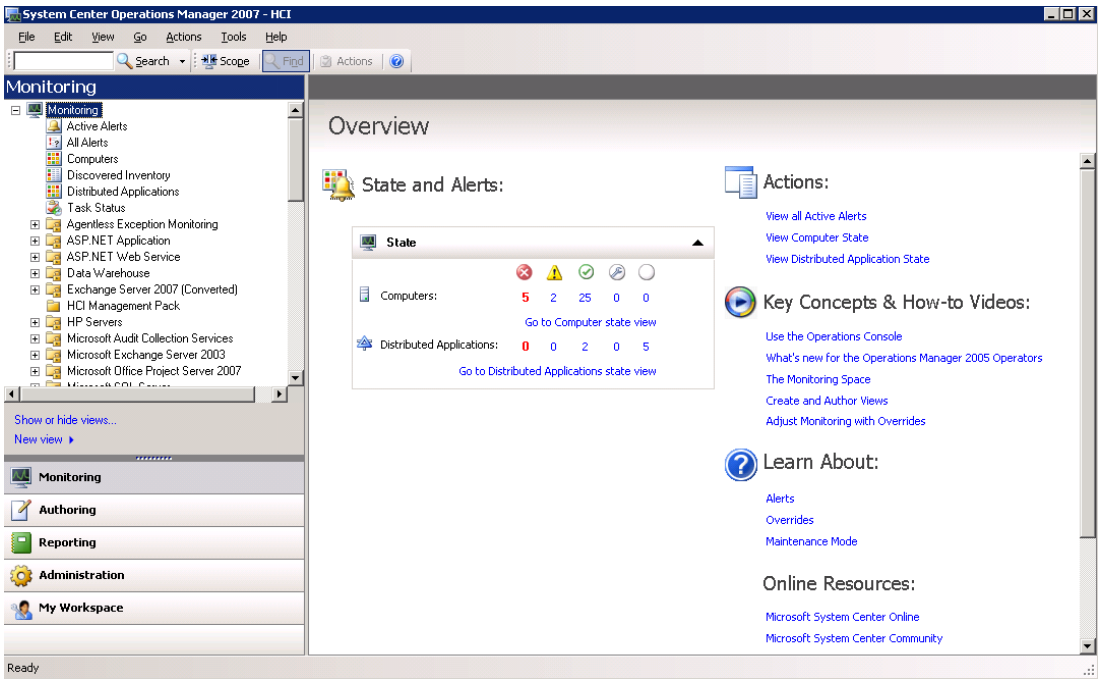
Po instalaci vybraných management packů začnou agenti na monitorovaných serverech sbírat data a zasílat je na management server.

5.5.1 Konzole SCOM

Konzole SCOM je určena pro správu a práci s prostředím SCOM. Skládá se z několika panelů, které si popíšeme.

5.5.1.1 Monitoring

V tomto panelu je možné sledovat všechny monitorované součásti.



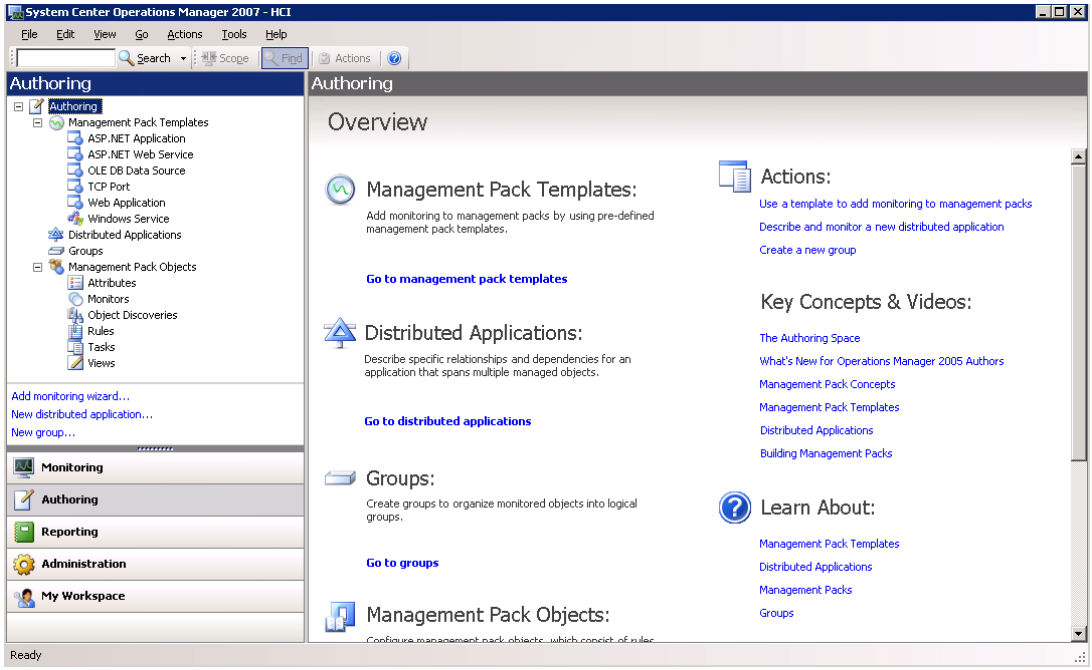
Obr. 17 Konzole System Center Operations Manager – monitoring panel

Základními kameny monitorování jsou tzv. health modely (model zdraví). Tento health model je ve skutečnosti množina atributů a jejich hodnot popisující zdravou komponentu (entitu). Spojením několika souvisejících health modelů vzniká model distribuované aplikace.

Pod ditribuovanou aplikací si můžeme představit např. elektronickou poštu. Její model by se skládal z health modulů Exchange, Active Directory, příslušného HW atd. Jednotlivé health modely a již hotové modely distribučních aplikací jsou součástí volně stažitelných management packů. Navíc si můžeme vytvořit svůj vlastní model distribuované aplikace.

5.5.1.2 Authoring

Tento panel slouží k editaci jednotlivých monitorovacích komponent.



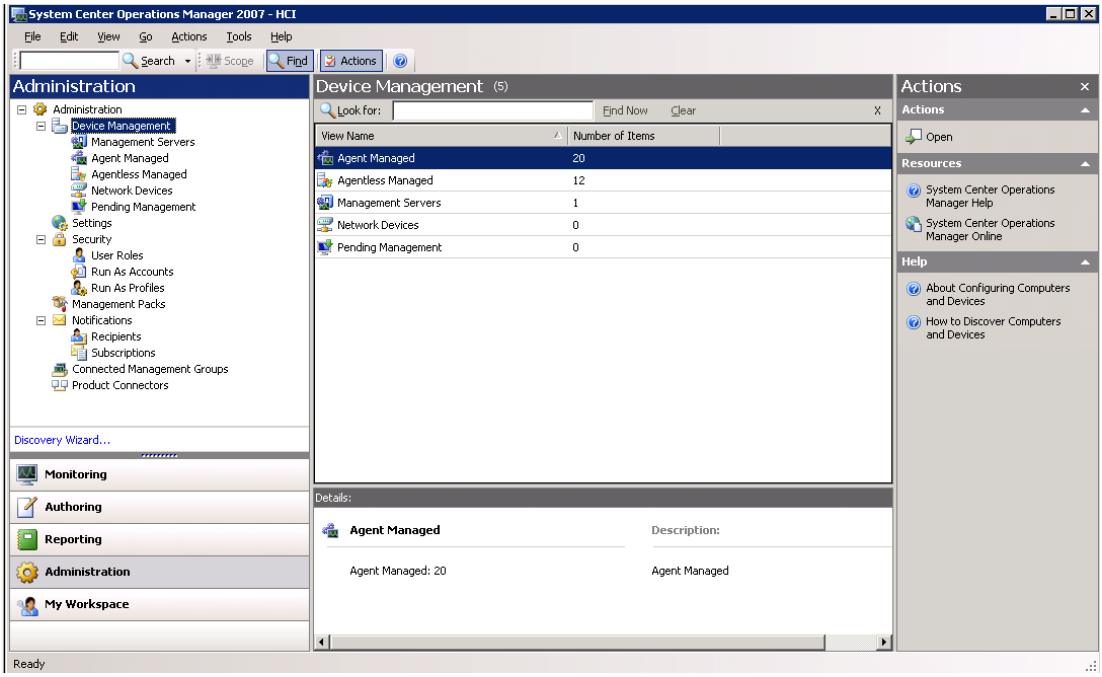
Obr. 18 Konzole System Center Operations Manager – authoring panel

5.5.1.3 Reporting

V tomto panelu jsou soustředěny reportovací nástroje. Zde je na výběr spousta předdefinovaných reportů.

5.5.1.4 Administration

Tento panel je určen pro administraci SCOM. Umožňuje nastavit různé konfigurace, uživatelské přístupy, notifikace apod.



Obr. 19 Konzole System Center Operations Manager – administration panel

5.5.1.5 My workspace

Poslední panel SCOM konzole umožňuje nastavit osobní oblíbené pohledy.

5.6 Shrnutí

Microsoft System Center Operations Manager je nástroj určený pro manažery, administrátory a operátory IT prostředí. Umožňuje vykonávat proaktivní sledování dostupnosti služeb provozovaných v rámci IT infrastruktury organizace.

SCOM je serverový produkt založený na principech klient-server, kde klientem bývá monitorovaný systém (server, stanice, aktivní prvky, jiné HW zařízení). Informace z tohoto systému jsou pomocí agenta přenášeny do centrálního bodu řízení (management server), kde mohou být dále vyhodnocovány. Informace jsou z této databáze následně prezentovány pomocí uživatelských rozhraní pracovníkům IT. [21]

Nebylo záměrem vyčerpávajícím způsobem podrobně popsat kompletní produkt, ale spíše nastínit koncepci a princip správy za pomoci tohoto nástroje.

ZÁVĚR

Obsahem této práce byla otázka ochrany dat. Toto téma je velmi rozsáhlé a určitě by si zasloužilo mnohem detailnější zpracování. Cílem této práce bylo uvést hlavní bezpečnostní principy a řešení týkající se bezpečnosti. Bezpečnost musí být chápána jako komplexní řešení, pouze v ojedinělých případech lze posuzovat její části odděleně. Všechna řešení jsou jedinečná a musí být výsledkem analýzy specifických bezpečnostních požadavků a podmínek dané organizace.

Důležitým poznatkem, kterého bychom si měly být vědomi, je fakt, že žádné bezpečnostní opatření nemůže zaručit stoprocentní ochranu. Všechna opatření mohou rizika pouze snižovat. To platí i při vzájemné kombinaci více bezpečnostních opatření. Cílem všech bezpečnostních opatření je snížit riziko na co nejnižší možnou míru.

Základem všech opatření by měla být v každé organizaci bezpečnostní politika, která musí vzniknout na základě důkladné analýzy aktiv, hrozeb a rizik. Tvorbě bezpečnostní politiky by se měly zúčastnit všechny zainteresované strany, tj. management, security oddělení a informační specialisté. V případě potřeby je možné využít služeb externích konzultantů.

Nedílnou součástí bezpečnostní politiky musí být také definice kontrolních mechanismů a pravidelné přezkoumávání jejích částí.

V praktické části diplomové práce je navržena a popsána implementace monitorovacího systému System Center Operations Manager na vybrané servery platformy Windows. Nasazením tohoto produktu se snadněji identifikují a řeší problémy, které mají vliv na stav poskytovaných IT služeb. Díky použití management packů se System Center Operations Manager snadno přizpůsobuje potřebám firmy a zvyšuje úroveň poskytovaných IT služeb. System Center Operations Manager se díky těmto vlastnostem stal efektivním pomocníkem Windows teamu firmy HCI. V současné době probíhá implementace dalšího produktu z řady System Center a to System Center Configuration Manager, od kterého očekáváme další zkvalitnění poskytovaných služeb.

Z toho vyplývá, že je potřeba v oblasti IT neustále sledovat vývoj, který je velmi dynamický.

CONCLUSION

The content of this thesis is the question of data protection. This topic is very extensive and certainly deserves more detailed elaboration. The aim of this study is to describe the major principles of security nad safety solutions. Security must be viewed as a complete solution, only in rare cases can its parts be considered separately. All solutions are unique and must be the result of analysis of specific security requirements and conditions of the organization.

An important finding, which we should be aware of, is the fact that no security measures can guarantee one hundred percent protection. All the measures can only reduce the risk. This is true even in the case of combining more security measures. The aim of all safety precautions is to reduce risk to the lowest level possible.

The basis of all measures in every organization should be security policy, which must arise from a thorough analysis of the assets, threats and risks. Security policy should include all stakeholders – management, security departments and information specialists. If necessary, the services of external consultants can be used.

An integral part of security policy must also be the defined controls and periodic reviews of its parts.

The practical part of this thesis is designed and described to implement a monitoring system, System Center Operations Manager at selected servers which are running on the Windows platform. The deployment of this product brings about easier identification and solution of problems that affect the provision of IT services. Thanks to using the Management Pack, the System Center Operations Manager easily adapts to the needs of businesses and increases the level of IT services provided. Currently, the implementation of another product of System Center and System Center Configuration Manager is being carried out, from which we expect to further improve the services.

To condude there is a need for IT to constantly monitor developments that are very dynamic.

SEZNAM POUŽITÉ LITERATURY

[1] THOMAS, M. Thomas. Zabezpečení počítačových sítí bez předchozích znalostí. Brno : Computer Press, a.s., 2005. 338 s. ISBN 80-251-0417-6.

[2] MLÝNEK, Jaroslav. Zabezpečení obchodních informací : Výběr a realizace bezpečnostních opatření k zajištění důvěrnosti, celistvosti a dostupnosti informací. [s.l.] : Computer Press, a.s., 2007. 160 s. ISBN 978-80-251-1511-4.

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

[4] DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat . Brno : Computer Press, 2004. 200 s. ISBN 80-251-0106-1.

[5] LUDVÍK, Miroslav, ŠTĚDROŇ, Bohumír. Teorie bezpečnosti počítačových sítí. Computer Media, 2008. 98 s. ISBN 80-86686-35-3.

[6] ŘEPA, Pavel . Jak na … instalaci agenta SCOM 2007 a řešení případných problémů [online]. 2009 , Monday, October 19, 2009 [cit. 2010-05-21]. Dostupný z WWW: http://blogs.technet.com/technetczsk/pages/jak-na-instalaci-agenta-scom-2007-a-reseni-pripadnych-problemu.aspx.

[7] MICROSOFT. System Center Operations Manager 2007 (SCOM) – Platform Monitoring [online]. 2009 , 2009 [cit. 2010-05-21]. Dostupný z WWW: http://www.microsoft.com/systemcenter/operationsmanager/en/us/default.aspx.

[8] *Antivirové centrum* [online]. 2006 [cit. 2010-05-21]. Firewall. Dostupné z WWW: <http://antivirovecentrum.cz/firewally.aspx>.

[9] PETRŽELA, Radim. *Zive.cz* [online]. 4.2.2009 [cit. 2010-05-21]. System Center: pro serverové profíky. Dostupné z WWW: <http://www.zive.cz/clanky/system-center-pro-serverove-profiky/sc-3-a-145517/default.aspx>.

[10] VODRÁŽKOVÁ, Darina. T*echnet.com* [online]. 21.5.2008 [cit. 2010-05-21]. Licence v rodině System Center. Dostupné z WWW: <http://blogs.technet.com/b/technetczsk/archive/2008/05/21/licence-produkty-system-center-family.aspx>.

[11] *Clever and smart* [online]. 2009 [cit. 2010-05-21]. CIA: Důvěrnost-Integrita-Dostupnost. Dostupné z WWW: <http://www.cleverandsmart.cz/duvernost-integrita-dostupnost/>.

[12] BITTO, Ondřej . *Lupa* [online]. 25. 1. 2006 [cit. 2010-05-21]. Počítačové viry: 20 let tam a zpátky. Dostupné z WWW: <http://www.lupa.cz/clanky/pocitacove-viry-20-let-tam-a-zpatky/>.

[13] *Tech-Life in Pink* [online]. 31. 3. 2009 [cit. 2010-05-21]. Cisco PIX Firewall Basics. Dostupné z WWW: <http://techlifeinpink.com/tag/cisco/>.

[14] HÁK, Igor. *Moderní počítačové viry* [online]. 15.9.2005 [cit. 2010-05-21]. Dostupné z WWW: <http://viry.cz/go.php?p=viry&t=clanek&id=23>.

[15] KOPECKÝ, Luboš. *ITBiz* [online]. 9.10.2009 [cit. 2010-05-21]. Útoky DOS/DDOS. Dostupné z WWW: <http://www.itbiz.cz/utoky-dos-ddos>.

[16] DŽUBÁK, Josef. *Hoax* [online]. 2004 [cit. 2010-05-21]. Co je to hoax. Dostupné z WWW: <http://hoax.cz/hoax/co-je-to-hoax>.

[17] DŽUBÁK, Josef. *Hoax* [online]. 2006 [cit. 2010-05-21]. Co je to phishing. Dostupné z WWW: <http://hoax.cz/phishing/co-je-to-phishing>.

[18] *Eset* [online]. 2006 [cit. 2010-05-21]. Rejstřík pojmů. Dostupné z WWW: <http://www.eset.cz/podpora/rejstrik>.

[19] NÁDENÍČEK, Petr. *Svět sítí* [online]. 25.10.2002 [cit. 2010-05-21]. Moderní antivirová ochrana v kostce. DostupnézWWW: <http://www.svetsiti.cz/view_list.asp?rubrika=Tutorialy&temaID=188>.

[20] PANÁČEK, Petr. *Systemonline.cz* [online]. 7.8.2003 [cit. 2010-05-21]. Systémy pro detekci neoprávněného průniku. Dostupné z WWW: <http://www.systemonline.cz/clanky/systemy-pro-detekci-neopravneneho-pruniku.htm>.

[21] *DIGITRADE* [online]. 2007 [cit. 2010-05-21]. Microsoft System Center Operations Manager. Dostupné z WWW: <http://www.pc-ware.com/pcw/cz/cz/nase_sluzby/podpora/dohledove_centrum/scom/main.htm>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AD	Active Directory
BDC	Backup domain controller
CAL	Client Access License
CPU	Central Processing Unit
DDoS	Distribute Denial of Service
DDR	Double Data Rate
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
GUI	Graphical User Interface
HCI	Home Credit International
HP	Hewlett-Packard
HW	Hardware
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
IT	Information Technology
MHD	Městská Hromadná Doprava
ML	Management License
MP	Management Pack
MS	Microsoft
NAT	Network Address Translation
OCS	Office Communications Server
OML	Operations Management License
PDC	Primary domain controller

PIN	Personal Identification Number
POSE	Physical Operating System Environment
RAID	Redundant Array of Independent Disks
RAM	Random Access Memory
RPM	Revolutions Per Minute
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SCCM	System Center Configuration Manager
SCDPM	System Center Data Protection Manager.
SCOM	System Center Operations Manager
SCVMM	System Center Virtual Machine Manager
SP	Service Pack
SQL	Structured Query Language
SW	Software
UPS	Uninterruptible Power Supply
VOSE	Virtual Operating System Environment
VPN	Virtual Private Networks
WSUS	Windows Server Update Services

SEZNAM OBRÁZKŮ

SEZNAM TABULEK