Bezpečnostní řešení IT společnosti

Libor Housírek

Bakalářská práce
2006

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektrotechniky a měření
akademický rok: 2005/2006

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Libor HOUSÍREK**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Bezpečnostní řešení IT společnosti**

Zásady pro vypracování:

1.) Seznámení s možným nebezpečím, které hrozí při provozování lokální počítačové sítě.
2.) Seznámení s technikami a nástroji, které se přitom používají.
3.) Obrana proti těmto hrozbám.
4.) Stanovení základní bezpečnostních pravidel práce s PC pro uživatele a administrátora.
5.) Vzorový příklad zabezpečení.

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

Knižní literatura:
Joel Scambray, Suart McClure, Georgie Kurz; Hacking bez Tajemství; Computer press, Praha 2002
Tomáš Doseděl; Počítačová bezpečnost a ochrana dat; Computer press, Praha 2004
Michal Matějka; Počítačová kriminalita; Computer press, Praha 2002

Časopisecká literatura:
PC WORD Serurity; IDG Czech, a.s., čtvrtletník 2005/2006
PC WORD; IDG Czech, a.s., měsíčník 2005/2006
CHIP; Vogel Burda Comunications, s.r.o., měsíčník 2005/2006

Vedoucí bakalářské práce: **Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a statistiky

Datum zadání bakalářské práce: **14. února 2006**

Termín odevzdání bakalářské práce: **13. června 2006**

Ve Zlíně dne 14. února 2006

L.S.

prof. Ing. Vladimír Vašek, CSc.
pověřený děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Cílem této práce je základní seznámení s použitím a využitím bezpečnostních informačních technologií jako základního prostředku bezpečnosti. Uvědomit si vzrůstající problém neoprávněného vniknutí do datových souborů. Využívat prevence pro znesnadnění přístupu neoprávněné osoby. Předcházet a čelit útokům, které mohou vést k totálnímu poškození dat a tím znehodnotit naši práci. Mít vždy na zřeteli základní zásady bezpečného stahování a internetové komunikace.

Klíčová slova: Bezpečnostní politika, Firewall, Antiviry, Bezpečnostní záplaty, Zabezpečení

ABSTRACT

The purpose of this work is providing the basic knowledge of the use and taking advantage of safety information technologies as a principal means of security. To become aware of increasing problems with unauthorized accesses to data files. To utilize preventive means, which will make difficult any access of any unauthorized person. To prevent and counteract attacks, which could lead to total destruction of data and so to undermine our work. To keep in view all and any fundamental principles of safe downloads and Internet communications.

Keywords: Security policy, Firewall, Sntivirus commands, Security patches, Safeguard

Prohlašuji, že bakalářskou práci jsem zpracoval samostatně, a že jsem uvedl všechny literární a odborné zdroje.

V Bystrovanech dne 18.5.2006 ……

OBSAH

ÚVOD

Není to tak dávno, co připojení k internetu znamenalo bezpečné připojení k obrovskému zdroji informací a zábavy. Ne že by bylo hrozilo menší nebezpečí, ale mnohem větší roli zde hrál fakt, že jedinců znalých těchto problémů bylo méně a většina z nich patřila ke světlé straně "síly". S rychle rostoucím rozšiřováním internetu, jeho služeb, programů pro ně určených a v neposlední řadě také jeho rychlosti se začaly jako první množit klasické viry. Výměna souborů několikanásobně vzrostla a také se zrychlila. V obrovské rychlosti začaly růst FTP servery, různé druhy výměnných sítí a objevily se první nesmělé pokusy o výměnu (větších) souborů e-mailem. Opravdový boom nebezpečí je doménou posledních tří let. Objevila se nová generace programátorů, která rychlostí blesku detekuje slabá místa a nemá výčitky svědomí okamžitě jich využít. Svou vinu v tomto nárůstu útoků přiznal nedávno i Microsoft, který potvrdil, že nevěnoval bezpečnosti svých produktů dostatečnou pozornost.

Pro uživatele PC to znamená jedno, musí být podezřívavý, a tím nemám na mysli jen naivní nigerijské dopisy "Pošlete mi milion a já vám dám deset", nebo různé druhy hoaxů . Ty ve své podstatě nejsou nebezpečné, alespoň ne přímo. Mnohem nebezpečnější jsou E-Maily prošpikované různými červy nebo trojskými koňmi, které ke své aktivaci nepotřebují ani jakoukoliv reakci ze strany uživatele, stačí řádně nezáplatovaný počítač, neaktualizovaný antivir nebo nenainstalovaný firewall.

Další Nebezpečí může číhat na každém kroku - ať už klikáte na nenápadné tlačítko na internetové stránce, stahujete zajímavý program, nebo si jen čtete e-maily od přátel.

Posledním a ne zanedbatelným nebezpečím jsou hackeři, kteří jsou schopni využít jakékoliv bezpečností slabiny nainstalovaného softwaru a zneužít ji k odcizení privátních či jiných dat, nebo k ovládnutí počítače a tím jeho možného zneužití k dalším útokům na jiné cíle.

I. TEORETICKÁ ČÁST

1 PŘEHLED JEDNOTLIVÝCH RIZIK

V reálném světě během svého života průběžně poznáváme různá rizika. Buď je známe a připravíme se na ně, snažíme se toto riziko snížit na minimum, nebo jim jednoduše předejdeme. Při připojení počítačové sítě nebo jen jednoho PC je to obdobné. Nejdříve se seznámíme s těmito hrozbami, pojmenujeme je a stručně uvedeme jejich charakteristiku.

1.1 Nebezpečný software

Viry

Viry jsou počítačové programy vytvořené se zlým úmyslem, které se snaží infikovat počítače a šíří se z jedné stanice na druhou různými způsoby:

- Jako příloha e-mailů.
- Ze zavirovaných přenosných médií jako je disketa, CD-ROM, DV-ROM…
- Přímo po Internetu z jednoho počítače na druhý (červ).
- Jako soubory ke stažení na stránkách vytvořených se zlým úmyslem. V některých případech pouhé navštívení stránky může zahájit stahování viru. Jindy mohou být viry ukryty uvnitř zdánlivě neškodných programů, které si z Internetu stáhnete.

Takto zasažený počítač může rozesílat desetitisíce e-mailů, z nichž každý s sebou nese virus. Tyto viry často využívají k vyhledání dalších osob, jejichž počítače by mohly napadnout, náš e-mailový adresář. Mohou předstírat, že jsou něčím jiným ("trojský kůň"). Např. soubor, který zdánlivě obsahuje fotografii známé osobnosti. Mohou být ukryty v dokumentech (makroviry). Jakmile je počítač zasažen, prohledává vir Internet, aby objevil nedostatečně zabezpečené počítače, které by mohl napadnout a zaslat jim kopii sebe sama. Jelikož k šíření virů jsou používány různé metody, potřebujeme různé nástroje k zajištění účinné ochrany - antivirový software, firewall a zdravý rozum.Těmto virům, trojským koňům a wormům se často souhrnně říká malware (maligní, tedy škodlivý software), známější je běžně užívaný termín "viry", kterým budeme označovat všechny tři kategorie.

Kromě toho, že se viry rozmnožují, nesou s sebou, další hrozby:

- rozesílání nevyžádané pošty,
- otevírání zadních vrátek do naší sítě nebo našemu počítači pro počítačové zločince,
- vyhledávání osobních informací, jako jsou hesla,
- zobrazování nevyžádané reklamy,
- přesměrování našeho prohlížeče,
- vypínání vaší bezpečnostní ochrany,
- vytváření prostoru pro phishing (rhybaření) k podvedení ostatních uživatelů,
- vedení útoků směřujících k odmítnutí služeb na jiných internetových serverech.

Spyware

Poslední roky se rozšířila hrozba špiónských spyware prográmků. Cílem činnosti těchto záškodníků je nepozorované usazení na disku uživatelova pevného disku a následné monitorování jeho činnosti. Nejedná se o klasické keyloggery v pravém slova smyslu, ale spíše o menší prográmky, které mohou shromažďovat rozličné informace, a ty zasílat svému tvůrci nebo zneuživateli. Pod společný pojem spyware bývá většinou zařazováno hned několik variant elektronických škůdců, ne všechny však dělají totéž. Jak již bylo nastíněno, klasický spyware sbírá informace o uživateli, které následně zasílá přes internet dále. Trochu jinak funguje adware, jenž automaticky zobrazuje reklamu – k výběru portfolia nabízených produktů navíc může s úspěchem využívat výsledků předchozího monitorování. Spyware kategorie pod křídla své definice může schovat také takzvané dialery. Tedy ty prográmky, které dokáží změnit vlastnosti vytáčeného spojení prostřednictvím klasické telefonní linky, a tak zařídit surfování v rámci nesrovnatelně dražšího tarifu.

Spyware způsobuje např. následující problémy:

- nepříjemná vyskakovací reklama,
- převzetí kontroly nad vaším prohlížečem,
- vyhledávání osobních informací, jako jsou hesla,
- zpomalování počítače a připojení na Internet,
- stahování virů,
- obtíže s odstraněním.

Nevyžádané e-maily

Spam se postupně mění z malé nepříjemnosti ve velký problém. Více než polovinu všech e-mailů na Internetu představuje nevyžádaná pošta, což znamená, že platíme za datovou kapacitu spammera.

Jelikož spammeři vydělávají, pokud si koupíme jejich zboží, ať již je to lék, pornofilm, nebo hazardní hry hrané on-line, mají dostatek důvodů k tomu, aby byli dostatečně přesvědčiví a neústupní.

1.2 Hacking, odposlech, podvody a krádeže identity

Hacking

Díky automatizovaným nástrojům, virům a spywaru není nabourávání se do cizích počítačů náročnou činností vyžadující nejmodernější nákladné zařízení, stačí nezabezpečený počítač a nebo uživatel, který může obejít vnější bezpečnostní opatření . Poměrně známa metoda je sociální inženýrství, kdy pod záminkou je vylákáno uživatelské heslo a to zneužito při útoku na server. Další metoda kdy po instalaci neznámého software je instalován další skrytý program (např. key logger) který zaznamenává všechny stisknuté klávesy a ty po určité době odešle na FTP nebo e-mail útočníka. Pro hackery jsou peníze silnou motivací a zcizení informací o vašem bankovním účtu nebo platební kartě jim stojí za trochu námahy.

Ohroženi jsou sice všichni, ale malé podniky a nebo organizace jsou pro hackery zvláště atraktivním cílem, neboť mívají databáze osobních informací, jež je možné zneužít ke krádeži identity ve velkém.

Odposlech

Sniffery slouží pro zachytávání a čtení paketů procházejících sítí. Útočník tak díky nim může zjistit řadu zajímavých informací o komunikaci ostatních uživatelů, například přihlašovací jméno a heslo služeb FTP, POP3 atd. Pokud pakety oprávněně analyzuje administrátor, může mimo jiné zjistit, co zapříčiňuje sníženou propustnost sítě.

Při normální síťové komunikaci přijímá počítač pouze ty pakety, které jsou mu určeny. To logicky není dobrá situace pro účely sniffování, takže síťová karta bývá přepnuta do takzvaného promiskuitního módu. V něm pak zachytává všechny pakety sítě. V případě sítě, která je tvořena počítači, které jsou navzájem propojeny ethernetovým kabelem musí útočník svůj sniffer nainstalovat na nějaký počítač v síti. Ovšem v případě užití bezdrátové sítě např. Wi-Fi (ta nám umožňuje širokopásmové připojení pomocí rádiových vln s dosahem několika stovek metrů) může, pokud naše síť není zabezpečena, se na naše internetové připojení nebo na naši vnitřní síť napojit, je-li v dosahu.

Podvody

Podvody na Internetu jsou stále větším problémem. Podvodníci se často skrývají za internetovými adresami. Mezi běžné triky patří:

- phishing, tedy rhybaření, při němž je využit falešný bankovní server nebo server, který po nás vyžaduje zadání soukromých informací (např. čísla kreditních karet), jež jsou posléze zneužity k vašemu okradení,
- podvody se zálohami mezi klasické příklady patří úhrada správního poplatku za účelem vyzvednutí neexistující výhry v loterii nebo zaslání peněz, které umožní získat část prostředků ze švýcarského konta jistého afrického diktátora (nigerijské dopisy).

Krádež identity

Krádež identity je skutečně velmi závažným problémem. Pachatelé využívají kombinace sociálního působení (tedy podvodů), záludných hackerských postupů, např. virů, a informací z reálného života, jakými jsou bankovní výpisy vytažené z popelnice, aby se za nás vydávali.Tímto způsobem mimo jiné mohou:

- vybrat náš bankovní účet,
- vyčerpat limit na naší kreditní kartě nákupem zboží pro vlastní potřebu,
- nakupovat auta na dluh naším jménem,
- vydávat se za nás na Internetu, např. zneužít naší totožnosti při on-line aukcích nebo

  na e-komerce serveru.

1.2.1 Fyzická krádež

Každý rok jsou ukradeny desítky tisíc přenosných počítačů. Jakmile se zločinec zmocní našeho laptopu, získává přístup ke všem datům na pevném disku. Platí to i o ukradených domácích stolních počítačích nebo o kapesních počítačích a mobilních telefonech. Nejvíce nebezpečná je krádež serveru na nichž jsou uložena citlivé informace.

1.2.2 Krádež dat

Malá zařízení, která se vejdou do dlaně, mají dnes paměť, která mnohonásobně převyšuje paměť počítačových pevných disků před deseti lety.

Například:

- Přenosný MP3 přehrávač může v sobě mít uloženo až 60 GB dat - což stačí ke zkopírování běžného pevného disku.
- Malinký paměťový modul velikosti palce může v sobě mít uloženo 512 MB - což stačí na zkopírování personální databáze a stovek dokumentů MS Word. To odpovídá paměti 364 disket.
- Mnohé telefony, kapesní počítače (PDA), fotoaparáty lze dnes připojit k počítači pomocí kabelu nebo infračerveného spojení a použít k přenosu počítačových dat.
- Mnoho počítačů má CD-ROM vypalovačky, které mohou vypálit 640 MB dat na prázdné CD.
- Díky širokopásmovému připojení na Internet mohou zaměstnanci poslat e-mailem velká množství dat z firmy, aniž by o tom někdo věděl.

2 PŘEHLED JEDNOTLIVÝCH ZABEZPEČENÍ

Pořídit si kvalitní antivir a případně i personální firewall nestačí. Je nutné bezpečnost brát komplexně. Tedy dodržování bezpečnostní politiky, instalace antiviru, antispywaru a firewallu. Nutná je jejich aktualizace včetně instalací posledních verzí oprav ke všem nainstalovaným programům včetně operačního systému.

2.1 Bezpečnostní politika

Jaké jsou typické cíle bezpečnostní politiky IT? V reálném prostředí se nevyhneme tlaku na zajištění potřebné úrovně důvěrnosti, autentizace, integrity dat a prevence před viry a jinými škodlivými programy, nepopiratelnosti odpovědnosti a potřebné velikosti výpočetního a paměťového výkonu. V distribuovaném prostředí, jakým síť Internet je, se k uvedeným cílům přidává požadavek bezpečnosti transakcí, např. mezi webovskými klienty a servery.

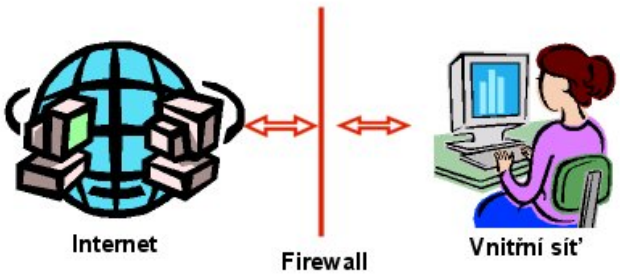
Na webovských serverech se uchovávají jak veřejně dostupné soubory, tak soubory citlivé a důvěrné, a ty je třeba ochránit. Na webovském klientu je třeba přijmout opatření proti virové nákaze, prohlížeč by neměl spouštět žádné nedůvěryhodné aplikace. K provedení programu, dovezeného do klientské stanice z WWW, by měl uživatel dát explicitní souhlas po zvážení potřeby prověření certifikace takového objektu. Takže, které vlastnosti IS vlastně představují bezpečnost IS? Které požadavky na bezpečnost zpracování komerčních a legislativně citlivých informací můžeme považovat za přirozené? Určitě je takovým bezpečnostním požadavkem poskytnutí potřebného rozsahu důvěrnosti. Důvěrnost má zásadní význam z hlediska ochrany soukromých dat, a to jak z hlediska zachování soukromí, tak i z hlediska možnosti zneužití informačních služeb. Důvěrnost IS lze zabezpečit pomocí šifrování, skrýváním identit počítačů organizace za firewally nebo řízením přístupu k souborům, např. na WWW serverech. Přirozeným požadavkem na šifrovací systém je dostupnost operace dešifrování. K šifrování a dešifrování je třeba znát jistá tajemství. Prokázání totožnosti pomocí znalosti těchto tajemství se využívá i při implementaci bezpečnostní funkce autentizace a nepopiratelnosti. Šifrování se může provádět na různých úrovních distribuovaného systému podle požadované úrovně transparentnosti takové operace, náročnosti na výkon procesoru a na prostor paměti.

Dalším možným bezpečnostním požadavkem může být uplatnění řízení přístupu**.** Může být žádoucí, aby byla neviditelná pouze část nějaké transakce, zatímco její zbytek může být veřejně dostupný. Takové výběrové řízení přístupu k transakcím, např. při elektronickém obchodování, umožní zákazníkovi „zabalit“ svoje identifikační informace o platební kartě do elektronické obálky, kterou může otevřít pouze jeho banka, tuto přiložit k objednávce a zaslat obchodníkovi. Obchodník obálku předá bance, která obchodníkovi potvrdí solventnost zákazníka, a tento může pokračovat v prodeji, aniž by mu zákazník svoje soukromá data zpřístupňoval. Dalším přirozeným požadavkem je požadavek zajištění integrity. Integrita musí zajišťovat, aby aktiva, dostupná autorizovaným uživatelům, byla úplná a věrná, tj. odpovídající své specifikaci. Data při přenosu nemohou být neautorizovaně měněna. Pro zajištění integrity dat lze použít např. mechanismů kryptografických kontrolních součtů, elektronického podpisu a certifikátů na bázi asymetrické kryptografie. Pro zajištění integrity softwaru je přirozeně nutné používat také adekvátní aktuální antivirové nástroje. Zajištění autentičnosti je dalším generickým požadavkem bezpečnosti IT. Komunikující strany by měly důvěřovat tomu, že komunikují s tím partnerem, se kterým komunikovat chtěly. K silné autentizaci je třeba obvykle použít mechanismů elektronického podpisu a certifikátů. Dostatečně důvěryhodné prokázání identity lze (podle výsledků analýzy rizik) také dosáhnout např. jednoduchým používáním hesel. Požaduje-li se zajištění nepopiratelnosti, pak žádná ze spolupracujících stran nesmí mít možnost svoji účast v transakci popřít, a to i po jejím ukončení. Aby bylo možné použít nějaký mechanismus pro implementaci funkce nepopiratelnosti, je třeba ho vybavit vlastností prokazatelnosti autorství. Takovým mechanismem je např. certifikovaný elektronický podpis. Nedílnou součástí bezpečnostní politiky on-line provozovaných IS musí být opatření zajišťující trvalou dostupnost jeho informatických služeb, tj. zamezující neoprávněnému vyčerpání zdrojů vnějším útočníkem nebo nedokonale vyškoleným vlastním zaměstnancem organizace.Tato opatření se realizují např. definicí mezí dostupného paměťového prostoru, omezením délek elektronicky vyměňovaných zpráv nebo dílu dostupného procesorového výkonu.

2.2 Firewally

Firewall je soubor pravidel, jež chrání vnitřní síť LAN před útokem "zvenčí" - v praxi především z Internetu. Může být pouze na jednom PC a nebo na síťovém serveru, přes který jsou všechna ostatní PC napojena. Chrání tak počítače před útokem hackerů, před viry a wormy (červy). Firewall tedy obsahuje pravidla, jež řídí komunikaci z vnitřní sítě směrem ven, komunikaci soustřeďuje do jednoho uzlu, odfiltrovává nebezpečné služby, blokuje nepřátelské monitorování sítě apod.

Z hlediska bezpečnosti představuje nejnižší kategorii tzv. paketový filtr. Ten dokáže na základě zdrojové a cílové IP adresy eventuálně TCP portu blokovat jednotlivé pakety. To dnes umí v podstatě průměrný směrovač a úroveň bezpečnosti je minimální. Problém je v tom, že nedokáže z jednotlivých paketů sestavit spojení. To umí až stavový firewall (statefull inspection). Umí přiřadit pakety příslušnému spojení, viz obr.2. Díky tomu například rozpozná, že se jedná o pakety vracející se do sítě v rámci spojení, které bylo navázáno zevnitř. Úroveň bezpečnosti je mnohem vyšší. Dokáže odhalit například spoofing, tj. útok založený právě na tom, že se pakety odeslané útočníkem "vracejí" do sítě. Třetí kategorii podle klasického dělení je proxy neboli aplikační brána. Toto zařízení pracuje na aplikační úrovni. Jinými slovy rozumí konkrétním aplikacím (http, telnet, ftp atd.), ukončují spojení od klienta a směrem k serveru navazují úplně nové. Znamená to, že musí obsahovat jak klienta tak i server pro všechny podporované aplikace. Míra bezpečnosti pro konkrétní aplikace je velice vysoká. Nevýhodou je podpora omezené množiny aplikací a menší výkon. Nelze obecně říct, že aplikační brána je lepší nebo horší než stavový firewall. Aplikační brána může poskytovat menší ochranu před útoky na síťové vrstvě. Jde o to, co je potřeba řešit. Obě řešení se často kombinují.



Obr. 1. Ilustrační obrázek firewallu

2.2.1 Druhy osobních firewallů

Sunbelt Kerio Personal Firewall

Výkonný firewall pro zkušenější uživatele. Pro osobní a nekomerční použití zdarma, ovšem po 30 dnech se přepne do "omezené verze", která nenabízí některé dodatečné funkce. V současné době je aktuální verze 4.2.3.

http://www.sunbelt-software.com/Kerio-Download.cfm

Obr. 2. Sunbelt Kerio firewall

Outpost Firewall

Jednodušší, ale plně funkční firewall, bohužel bez oficiální češtiny. V současné době je aktuální verze 3.51

http://www.agnitum.com/products/outpost/index.php

Obr. 3. Outpost firewall

Zone Alarm

Známý produkt od firmy Zonelabs, vhodný především pro začátečníky. Výhodou je automatické nastavení základních pravidel pro provoz. Existuje v několika verzích. Nejednoduší je pro nekomerční užití zdarma V současné době je aktuální verze 61.744

http://www.zonelabs.com

Obr. 4. Zone alarm firewall

Norton Internet Security 2006

Balík se skládá z pěti klíčových komponent. Norton AntiVirus patří mezi nejuznávanější antivirové produkty, dostupné na trhu. Nabízí rozšířené zjišťování hrozeb upozorňuje uživatele na některé nevirové hrozby, jako je spyware a programy pro zaznamenávání stisknutých kláves, automaticky odstraňuje viry, červy a trojské koně. Vedle toho prověřuje a čistí přílohy rychlých zpráv, příchozí a odchozí e-maily a další soubory. Funkce Norton Internet Worm Protection blokuje některé nebezpečné internetové červy ihned při vstupu.

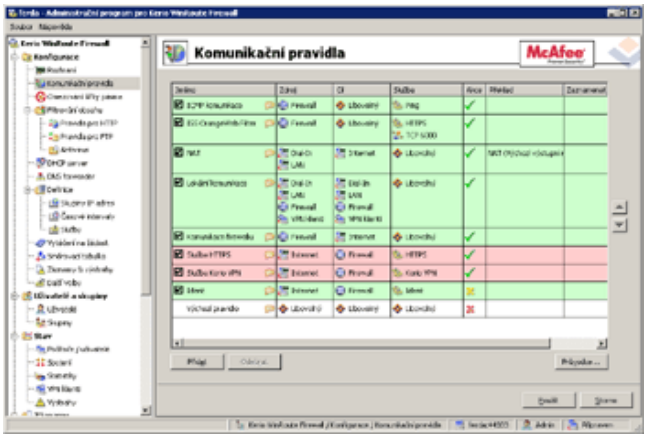
Obr. 5. Norton Internet security

2.2.2 Síťové firewally

Kerio Win Route firewall

WinRoute je komplexní nástroj pro připojení lokální sítě do Internetu a její ochranu proti průniku zvenčí. Jeho základní funkce jsou : filtrování protokolů, antivirová ochrana, DHCP server, DNS server, VPN server a klient ……V současné době je aktuální verze 6.21

http://www.kerio.cz/kwf_firewall.html



Obr. 6. Kerio Win Route firewall

MS ISA Server 2004

ISA Server 2004 obsahuje komplexní bránu firewall na aplikační vrstvě, která umožňuje bránit organizace všech velikostí před externími i interními útoky a ohroženími. Integrovaná architektura brány firewall a VPN podporuje stavové filtrování a kontrolu veškeré komunikace VPN. V současné době je aktuální verze 2004 SP2

http://www.microsoft.com/cze/windowsserversystem/isaserver/

Obr. 7. ISA server 2004

2.2.3 Jednoduché otestování firewallu

Když nainstalujeme firewall, začíná další fáze a tou je přesné stanovení pravidel .Na níže uvedených stranách lze provést jednoduché testy našeho firewallu.

Qualys,http://www.qualys.com). Bezpečnostní experti Qualysu chrání systémy bank a velkých IT firem – nabízejí ale také několik bezplatných funkcí. Na hlavní stránce klikněte pod »Resources« na »Free Tools«. Tam můžete otestovat dvacet nejohroženějších míst vašeho počítače, použít různé detektory trójských koní nebo spustit kompletní bezpečnostní prověrku vašeho systému.

StevenGibson,(http://www.grc.com). Bezpečnostní stránka Stevena Gibsona nabízí pod odkazem „Shields UP" dva různé testy vašeho firewallu. Zatímco „Test my Shields" prověřuje známé slabiny, testuje „Probe my Ports" část komunikačních portů vašeho počítače.

Audit My PC,(http://www.auditmypc.com) I na této stránce máte možnost provést sken portů (portscan) vašeho počítače. Vyhodnocení sice nějakou dobu trvá, ale za podrobnou analýzu firewallu to čekání opravdu stojí za to.

2.2.4 Nejběžnější používané porty

Na jeden počítač může být současně kladeno mnoho požadavků na různé jeho služby. Každá služba (jako například WWW, FTP…) pracuje na tzv. portu. Portů je celkem 65535. Některá čísla portů jsou rezervována pro určité služby. Pár základních uvádím níže seznam dalších můžete najít například v souboru *%SystemRoot%\drivers\etc\services*.

7 Echo	13 Daytime	21 FTP	23 Telnet	25 SMTP	53 DNS
80 HTTP	110 POP3	139 Net Bios	443 HTTPS	8080 Proxy	

2.3 Antiviry

Nejletitější hrozbou počítačů všeho druhu jsou počítačové viry .Počítačový virus ve své podstatě není ničím jiným než škodlivým programovým kódem, který je schopen šíření sebe sama bez vědomí uživatele. Různé viry s sebou přinášejí různá rizika, takže se lze

setkat i s více méně neškodnými žertovnými variantami, které svou infekční činnost završí prostým vypsáním nějakého textíku na obrazovku. Hrozbou jsou však destruktivní viry, které smažou veškerá data, nebo v poslední době druhem, který napadnuté počítače využívá k útoku na další cíle tzv. DOS útok.

Jednu z nejsnadnějších zbraní proti nákaze počítačovým virem představuje nepoužívání podezřelého softwaru. Častým zdrojem virů jsou totiž data z pochybných zdrojů typu warez stránek a jim podobných. A tak by si uživatel měl dvakrát rozmyslet, než z těchto lokalit něco stáhne. Systém Windows XP v sobě sám o sobě neobsahuje žádný antivirový program. Proto by po jeho instalaci měl následovat výběr vhodného antiviru. Prakticky všechny kvalitnější antivirové programy poskytují ochranu hned na několika úrovních a různými funkcemi. Tou nejzákladnější funkcí je testování souborů na požádání. Nejčastěji se praktikuje porovnávání podle v databázi uložených virových sekvencí, případně takzvaná heuristická analýza. Pokud použijete prvně jmenovanou variantu, testování většinou proběhne rychleji. Heuristická analýza zase dovoluje odhalit i některé dosud neznámé viry (analýzou chování programového kódu). Člověk je tvor zapomnětlivý, takže byste raději měli ihned po instalaci antivirového programu naplánovat automatické testování pevných disků. Některé antiviry poskytují i tu možnost, že pokud v plánované době počítač neběží, zahájí test okamžitě po jeho spuštění. Důležitou komponentu představuje také ochrana počítače v reálném čase, která dokáže virus zachytit ještě před tím, než se usadí na disku a v paměti počítače. V době rozmachu internetu a jeho aplikací nachází také odůvodněné uplatnění e-mailový skener, který testuje přílohy elektronické pošty na přítomnost virů.

Obr. 8. Centrum zabezpečení hlídá přítomnost antivirového programu.

Mezi fundament počítačové bezpečnosti patří samozřejmě pravidelná aktualizace všech softwarových produktů, v případě antivirových systémů toto pravidlo platí dvojnásob. Úspěšnost odhalení viru na základě porovnávání sekvencí stojí a padá s aktuálností vzorků, takže jen díky nejnovější databázi budete chráněni i před posledními odhalenými škůdci.

Používáte-li trvalé připojení k internetu, určitě využijte možnost automatického stahování aktualizací.

Posledním novinkou antivirové ochrany představuje technologie TruePrevent. Program sleduje chování všech procesů, které v počítači běží. Pokud některou aplikaci vyhodnotí jako nebezpečnou, ukončí ji a propříště ji zablokuje.Aby mohl sledovat programy spuštěné pod Windows, usazuje se podobně jako rootkit přímo v operačním systému. Nejlepším místem je API. Ve Windows totiž programy nekomunikují s hardwarem přímo, nýbrž předávají své příkazy operačnímu systému právě prostřednictvím rozhraní API. TruePrevent zasahuje do tohoto procesu. Sleduje každou komunikaci s rozhraním API a zaznamenává jí do protokolu. Potom svůj protokol porovnává se souborem záznamů vytvořený autorem programu a odhaduje nebezpečnost procesů. Jakmile se nějaký program pokusí porušit důležité pravidlo, TruePrevent ho okamžitě zablokuje.

2.3.1 Než začneme odstraňovat vir

Použití jednoúčelových antivirů

Před použitím jednoúčelových antivirů je vhodné vypnout stávající antivirový systém a to především on-access skener (často označován jako rezidentní štít).

Adresář Systém volume Information & _RESTORE

Ve Windows XP a ME je taktéž vhodné vypnout funkci OBNOVA SYSTÉMU (RESTORE SYSTEM), která by později bránila smazání infikovaných souborů, které "uvízly" v adresářích _RESTORE (Windows ME) nebo SYSTEM VOLUME INFORMATION (Windows XP).

Postup pro Windows ME:

1. Klikněte pravým tlačítkem myši na ikonu TENTO POČÍTAČ (MY COMPUTER) a zvolte z nabídky VLASTNOSTI (PROPERTIES).

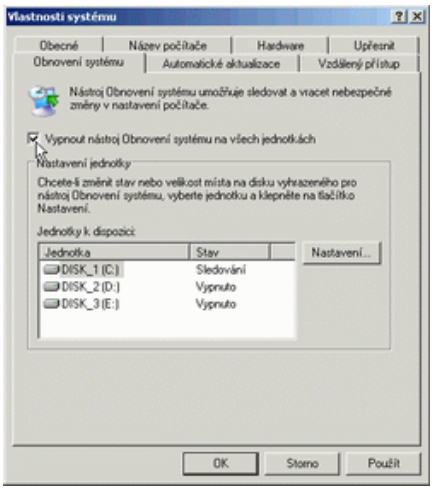
2. Přepněte se do záložky VÝKON (PERFORMANCE) a stiskněte tlačítko SOUBOROVÝ SYSTÉM (FILE SYSTEM).

3. Zde se přesuňte na záložku PŘI POTÍŽÍCH (TROUBLESHOOTING) a zaškrtněte poslední volbu - ZAKÁZAT OBNOVU SYSTÉMU (DISABLE SYSTEM RESTORE).

4. Vše potvrďte tlačítkem OK, Windows se restartuje.

Postup pro Windows XP:

1. Klikněte pravým tlačítkem myši na ikonu TENTO POČÍTAČ (MY COMPUTER).
2. Zvolte VLASTNOSTI (PROPERTIES) a nalistujte záložku OBNOVENÍ SYSTÉMU (SYSTEM RESTORE).
3. Zatrhněte volbu VYPNOUT NÁSTROJ OBNOVENÍ SYSTÉMU NA VŠECH JEDNOTKÁCH.
4. Potvrďte, Windows provede restart.



Obr. 9. Vypnutí obnovení systému

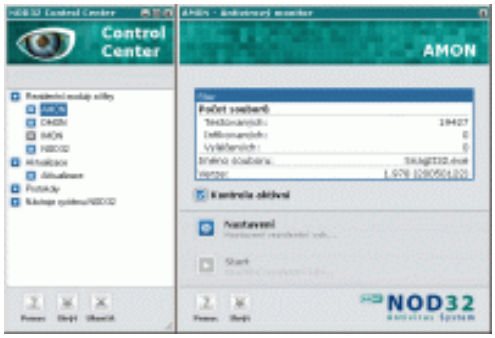
2.3.2 Přehled nejznámějších antivirů

NOD32 Antivirus system

Velmi uživatelsky příjemný antivir, který obstál v uznávaném testu 100% Virus Bulletin již několikrát po sobě. Ten zkoumá, zda antivirus dokáže odstranit všechny viry, které jsou na

seznamu aktivních virů . Obsahuje všechny běžné typy ochrany: rezidentní štít s názvem AMON, heuristická analýza, detekce virů v archívech ZIP, ARJ, RAR a automatická aktualizace virové databáze. Existuje ve čtyřech verzích: Standard, Professional, Enterprise , Server . Pokrývá tedy celé spektrum, od domácích uživatelů až po instalaci na serveru a spolupráci s např. Exchange.

http://www.eset.cz/cz

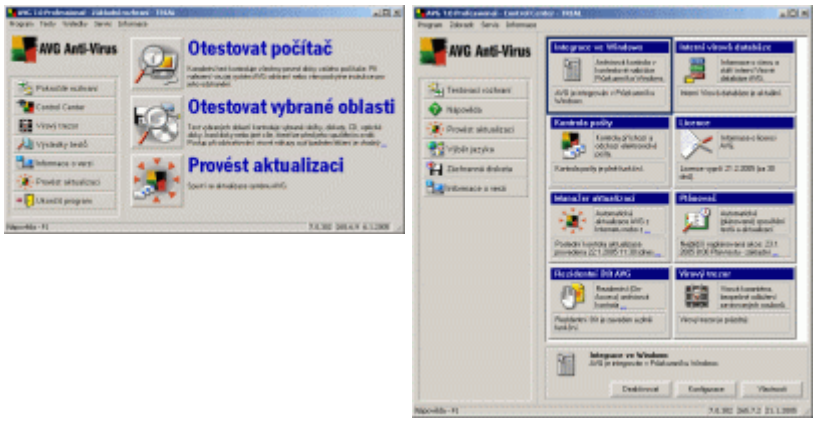


Obr. 10. NOD 32

AVG 7.1

AVG pro pracovní stanici zajišťuje automatickou a komplexní ochranu uživatele před útoky počítačových virů. Je k dispozici jako AVG Professional pro jednoho uživatele, nebo jako AVG SoHo (Small office - Home office) pro potřeby domácností a malých firem. Antivirový systém AVG svým propracovaným spojením detekčních technik a nabídkou několika úrovní ochrany (kontrola pošty, kontrola souborů na disku, rezidentní ochrana při práci se soubory) představuje pro uživatele spolehlivou ochranu jeho počítače před virovým nebezpečím. Kvalitní fungování systému je podpořeno vždy dostupnými pravidelnými i mimořádnými aktualizacemi a nepřetržitou technickou podporou.

http://www.avg.cz/doc/1



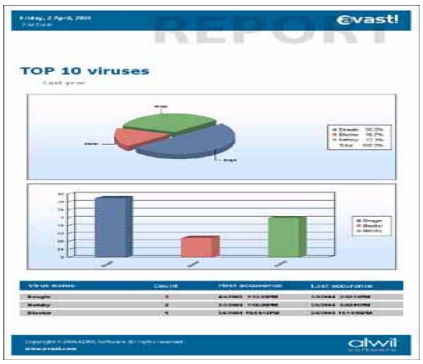
Obr. 11. AVG

Avast 4.7

Jeden ze dvou předních českých antivirových systémů, který je ve verzi pro domácí užívání zcela zdarma. Od verze 4 jsou varianty Home Edition a Professional Edition rozdílné - verze Pro obsahuje některé nadstandardní funkce jako prohledávání archívů .CAB, rozšířené

uživatelské prostředí Skript Blocker. Dále existuje verze Server edition, která je učena k instalaci na server. Zde je schopna kontrolovat všechny soubory na serveru, HTTP provoz nebo kontrolovat elektronickou poštu. Zajímavostí je PDA verze určená pro kapesní počítače. Verze 4.6 obsahuje zajímavé novinky jako je například "Webový štít", což je vlastně transparentní proxy schopná monitorovat a filtrovat veškerý HTTP provoz. "NNTP skener" kontroluje provoz používaných diskuzních skupiny proti nežádoucím přílohám. "Podpora rozbalování archivů programu Outlook Express" dokáže dekomprimovat a odvirovávat archivy programu Microsoft Outlook Express (dbx). V neposlední řadě pak v nové verzové řadě nalezneme vylepšenou ochranu proti malweru - škodlivým kódům jako jsou dialery, spyware či adware.

http://www.avast.cz/index_cze.html



Obr. 12. AVAST

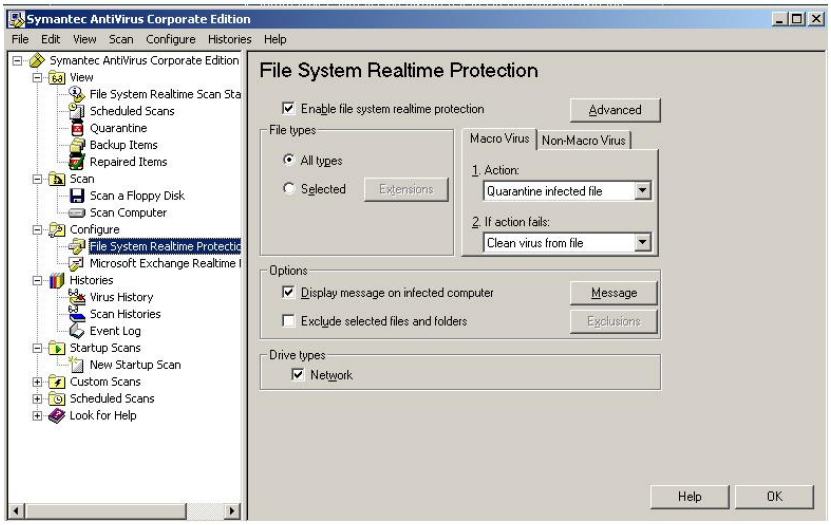
Symantec antivirus

Norton AntiVirus je již dlouhou dobu považován za jeden z nejlepších antivirů vůbec. Program pochopitelně dokáže provádět antivirovou kontrolu celého systému na povel nebo podle předem stanoveného plánu. Všechny testy si můžete přesně nakonfigurovat, vybrání adresářů, které chcete kontrolovat, přípon na které dávat pozor. Norton AntiVirus obsahuje funkci LiveUpdate, která automaticky kontroluje po Internetu, zda máte nejnovější definice, a nabídne vám stažení aktuálních.

Existuje i verze pro mobilní zařízení s operačním systémem Symbiant. Což může ocenit hodně uživatelů používající chytré mobilní telefony.

Pro firemní řešení jako je ochrana souborového, poštovního nebo proxy serveru je určena verze Small Business Edition 10.0. Ta nabízí ochranu nejen před viry, ale i spywarem adwarem dále může plnit i funkci firewallu.

http://www.symantec.com/index.htm



Obr. 13. Symantec antivirus

Existují samozřejmě antivirové programy od dalších firem, ale vzhledem k jejich malé rozšířenosti v naší republice je zde neuvádím.

2.3.3 Hodnocení jednotlivých antivirových programů

Hodnocení jednotlivých antivirových programů je velmi složité a vyžaduje podrobné testy a znalosti dané problematiky. Osobně bych doporučil navštívit na internetu stránky, které se věnují tomuto tématu na vysoce odborné úrovni.

Z českých www stránek bych zmínil asi nejznámější stranu http://www.viry.cz/go.php , která se dopodrobna věnuje tématice antivirových programů a virů. Další strana je http://www.hoax.cz/cze/, jenž se věnuje problematice šíření hoaxů tedy poplašných správ. Další www stránky v českém jazyce jsou www.grisoft.cz, www.avast.cz nebo www.no32.cz.

Ze zahraničních webů bych rád zmínil stránku http://www.icsa.net/icsa/icsahome.php zabývající se certifikací jednotlivých antivirových programů nebo firewallů. Stránka časopisu Virus Buletin http://www.virusbtn.com/index zabývající se testováním jednotlivých antivirových programů. Jako poslední ještě zmíním stránku www.eicar.com, kde se zasloužili o vytvoření tzv. Eicar Test File. Zbytek odkazů na další www strany naleznete na http://www.viry.cz/go.php?p=viry&t=listodkazy.

Co je to soubor Eicar.com

EICAR je institutem (European Institute for Computer Antivirus Research) pořádající různé konference a ostatní akce. Pro nás je ovšem nejdůležitější existence tzv. „The Anti-Virus test file" právě od institutu EICAR. Onen „The Anti-Virus test file" je zcela neškodný soubor (nejčastěji EICAR.COM) o velikosti 68 bajtů. Několik antivirových společností se dříve dohodlo, že pokud bude antivirovým skenerem nalezen právě takový, 68 bajtů veliký soubor se specifickým řetězcem, antivirus ho identifikuje jako virus. Jedinou podmínkou je, že ze strany antivirového skeneru je tento soubor podporován (dnes je tomu v naprosté většině případů). Soubor dle popisu se stal významným pomocníkem při zjišťování, zda funkčně vyhlížející antivirus je opravdu funkční a dokáže detekovat reálné viry (k tomuto nemusí docházet například při vzájemné kolizi s jiným antivirovým systémem atd.). Co se týče řetězce, je složen tak, že ho lze utvořit i na klávesnici a navíc je spustitelný (vypíše „EICAR-STANDARD-ANTIVIRUS-TEST-FILE").

2.4 Spyware

Podobně jako u virové hrozby také v případě spyware spočívá základ obrany v používání zdravého rozumu během surfování po internetu. Webové warez stránky a jejich obsah totiž poskytují výborné podhoubí pro šíření tohoto SW a využití naivity některých uživatelů. Analogie s obranou před čistě virovými hrozbami dále pokračuje i pořízením některé z antispyware utilit, které dokáží nejen testovat pevný disk a další známé lokace na přítomnost špionů, ale v některých případech také proaktivní ochranou v reálném čase

2.4.1 Přehled neznámějších antispywarových programů

Spybot S&D

Je to program, jenž lze mít zdarma. Jeho poslední verze 1.4 má už bohužel zastaralé jádro a tak ho lze doporučit již jen jako doplněk k některým níže uvedeným programům. Spybot S&D identifikovat a odstranit. Vedle této základní skupiny vás Spybot chrání i proti dialerům, přesměrovávajícím modemové připojení přes drahé linky, trojským koním, programům zaznamenávajícím stisky kláves a mnoha dalším nebezpečím. Samozřejmostí je možnost aktualizace přes Internet. Program obsahuje i českou lokalizaci základního menu a ovládání. Nápověda je bohužel jen v angličtině.

http://www.safer-networking.org/

Obr. 14. Spybot 1.4

Windows defender 2

Nástupce Microsoft AntiSpyware, nyní pod označením Beta 2. Nový vzhled a uživatelské menu, lepší skenování a ochrana před napadením spyware a jiným malware. Má být mnohem lepší než stávající Microsoft AntiSpyware. Nejnovější verze opravuje chyby, drobné změny se týkají i uživatelského rozhraní. Vylepšena byla technologie SpyNet, která umožňuje uživatelům odesílat Microsoftu reporty o novém malware a pomáhat tak udržovat databázi co nejaktuálnější.

http://www.microsoft.com/athome/security/spyware/software/default.mspx

Obr. 15. MS Defender 2

Ad – Avare SE

Pravděpodobně nejznámějším zástupcem skupiny programů bojujících proti spyware je aplikace Ad-aware od společnosti Lavasoft. Tu lze ve verzi Personal používat pro osobní potřeby zdarma, k dispozici jsou ale také pokročilejší, avšak placené verze Professional a Plus. Ty navíc dovolují například odhalovat spyware v reálném čase při surfování, a ne až po jeho napadení počítače.

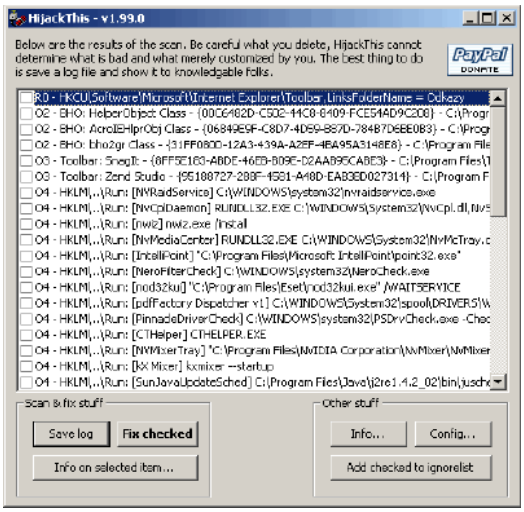
http://www.lavasoft.com/

Obr. 16. Ad- Avare SE

2.4.2 Hijack This

HijackThis slouží k získání sourhnu informací, ze kterých lze ve většině případů "vyčíst" případnou infekci. HijackThis po stisku tlačítka "Scan" vypíše běžící procesy v paměti, zobrazí instalované BHO, důležité položky registrů, linky na ActiveX programy atd. Většinu záležitostí je možné rovnou vyřešit.

Pozor! Zobrazené výsledky nemusí mít nic společného se spyware! Užití tohoto programu je spojeno se znalostí na úrovní alespoň „velmi pokročilý uživatel“.



Obr. 17. Hijack This

2.5 Aktualizace software a pravidla bezpečnosti

V dnešní době je nejvíce užívaným operačním systémem Windows XP, pominu-li firemní prostředí, kde se stále používá Windows 2000 a dnes již nepodporovaný pro domácí prostředí určený Windows 98 a jeho varianty, budu se zde zmiňovat jen o aktualizaci Windows XP. Vynechám ostatní operační systémy založené na linuxu, unixu, Mac OS a další....

V počítači je instalován software od různých firem a ten je třeba také aktualizovat. Proces aktualizace u každého produktu je odlišný, ale nezbytně nutný. Protože tento instalovaný software tvoří na každém počítači celek. A každý neaktualizovaný program by se mohl stát potencionálním nebezpečím.

2.5.1 Windows XP update

Windows XP jsou na tom poměrně dobře. Koncem minulého roku byl totiž vydán Service Pack 2, který ve Windows XP opravuje ty nejzávažnější problémy a přináší i aktualizace řady součástí systému. Nové je například centrum zabezpečení systému Windows, kde můžete na jednom místě sledovat a spravovat nastavení zabezpečení počítače. Změněna byla brána Windows Firewall, která je ve výchozím nastavení nainstalována a povolena. Přibyla i ochrana stahování pro aplikaci Internet Explorer, která zobrazuje upozornění na potenciálně nebezpečné stahované položky a umožňuje blokovat nechtěné programy. Novinkou je i blokování automaticky otevíraných oken v aplikaci Internet Explorer. Jinými

slovy, Windows XP Service Pack 2 je nutností. Pokud jste si ho ještě nenainstalovali, doporučuji tuto chybu co nejdříve napravit.

Obr. 18. Zde aktivuje automatická aktualizace windows

Windows www update

Alternativy k automatickým aktualizacím jsou dvě. První z nich je služba Windows Update, která se ovládá přes webové rozhraní. Kromě kontroly stavu systému vám pak může nabídnout i aktualizace certifikovaných ovladačů pro vybraná zařízení. Je to ideální nástroj pro kontrolu chybějících záplat a na rozdíl od automatických aktualizací vám nabídne i updaty pro komponenty systému. Je nutné ovšem podstoupit ověření pravosti Windows.

http://windowsupdate.microsoft.com/

Obr. 19. Windows www update

Služba stažení software

Pokud potřebujete přímo instalační soubory jednotlivých záplat, je tato stránka ideální volbou. Přes vyhledávání podle klíčových kategorií (verze operačního systému nebo technologie) sice najdete poslední záplaty pro svůj systém, vzhledem k jejich rozdělení to ale bude chvíli trvat. U některých aktualizací je navíc stažení podmíněno poměrně dlouhým ověřovacím procesem.

http://www.microsoft.com/downloads/Search.aspx?displaylang=cs

Obr. 20. Služba stažení software

2.5.2 Pravidla bezpečnosti

Pravidla pro heslo

Takzvané power-on heslo a heslo pro pevný disk slouží k autorizaci uživatele již při spuštění počítače. Těmito hesly jsou vybaveny téměř všechny počítače. I toto heslo se dá prolomit, nicméně již ne tak jednoduše. Na prolomení obou hesel je třeba odborníka, který provede zásah přímo na jednotlivých komponentách počítače. Jako další vrstva slouží hesla na přihlášení uživatele kdo systému.

Nicméně je nutné dodržet několik pravidel:

- alespoň 8 znaků
- nesmí být smysluplné slovo
- žádné spojení s uživatelem
- obsahuje malá a velká písmena
- obsahuje číslice a spec. znaky
- různá hesla pro různé systémy
- své heslo nikomu nesdělovat
- toto heslo pravidelně měnit

Ideální z hlediska uživatele je možnost nahradit tato hesla biometrickou autentizací uživatele

.

Autentizace dalšími zařízeními

Jako možné prvky autentizace uživatele do počítače se využívají nejvíce čtečky čipových karet, tokeny (podobné USB klíčům) a snímače otisků prstů. Každá možnost má své výhody i nevýhody. Například snímače otisků prstů jsou dnes dostupné ve dvou variantách - bud je snímán otisk jako reliéf prstu, podobně jako například v policejní kartotéce, nebo snímač snímá obraz povrchového napětí prstu . V tomto případě nefungují útoky určené pro první druh snímače, tj. podstrčení „mrtvého" prstu (kopie), neboť prst po oddělení od ruky ztrácí při-

bližně po deseti minutách svojí standardní povrchovou vodivost a snímač tedy nemůže autentizaci provést.

Zapnout firewall

Pokud nepožíváte ochranný program od třetího výrobce, je nutné aktivovat Personal firewall ze ServicePacku2.

Instalovat Updaty

Windows se standardně spojují s webovou stránkou Microsoft a zjišťují, zda jsou k dispozici aktualizace systému.Tuto funkci je nutné nechat aktivovanou.

Ve Windows XP používat výstrahy zabezpečení

V service packu 2 jsou Výstrahy zabezpečení systému Windows (Windows Security Center), které vás upozorní ve chvíli, kdy je firewall nebo antivirová ochrana vypnutá či není aktualizovaná.

Nepoužívat počítač jako administrátor

Při přihlašování k počítači uživatelským účtem s administrátorskými právy se zvyšuje riziko napadení virem. Je tedy nutné založit uživatelský účet s omezenými právy.

Nastavit vyšší stupeň bezpečnosti v IE

V internet exploreru by rozhodně měl být nastaven stupeň bezpečnosti na střední. Ovšem při navštěvování stránek s pochybným obsahem bych doporučil tento stupeň bezpečnosti nastavit na vysoký. nastavení IE na vysokou úroveň zabezpečení může bohužel vést k tomu, že prohlížeč nás bude obtěžovat záplavou varování a zákazů. To lze vyřešit tím, že stránky, které navštěvujete často zařadíte na seznam důvěryhodných serverů.

Užití alternativního WWW prohlížeče

Z důvodu velkého rozšíření Internet exploreru, který je součástí operačního systému je hodně stránek obsahující nebezpečný kód určena jemu. Proto doporučuji používat alternativního prohlížeče např. Mozilla FireFox nebo Opera.

Šifrování e-mailové korespondence

Šifrovat e-maily je možné pomocí řady produktů. Patří sem jednak celopodnikové infrastrukturní systémy s veřejným klíčem vhodné pro nadnárodní společnosti, jednak bezpečné webmailové systémy pro jednotlivce. Jako příklad uvádím PGP desktop „www.pgp.com“

Zablokovat a zašifrovat adresáře

Počínaje Windows NT nabízí Microsoft souborový systém NTFS, který dovoluje zablokovat přístup pro určité uživatele, a dokonce i zašifrovat soubory a složky. Pomocí technologie EFS lze zašifrovat soubory a složky v režimu offline. K dispozici jsou také nové možnosti sdílení šifrovaných souborů a zákazu agentů obnovení šifrovaných dat. Systém Windows XP Professional rovněž usnadňuje správu systému EFS ve vaší společnosti prostřednictvím zásad skupiny a nástrojů příkazového řádku.

Nastavit zobrazení přípon souborů

Některé viry se maskují jako neškodné typy souborů tím, že doplní na konec svého názvu falešnou příponu, jako např. „fotka.jpg.exe“

Vypnout automatický náhled

Některým zavirovaným zprávám stačí k aktivaci automatický náhled v poštovním klientu. Z tohoto důvodu doporučuji jej zavřít.

Zacházet opatrně s URL odkazy obsažených v e-mailech

Abychom snížili nebezpečí virové infekce e-mailem, URL odkaz obsažený ve zprávě vložte ručně do webového prohlížeče. Jelikož tento odkaz může skrýt skutečnou webovou adresu.

Číst e-maily ve formátu prostého textu

Mnoho virů potřebuje ke své aktivaci kód HTML v textu zprávy. Můžeme tomuto předejít, že e-maily si budeme číst jako prostý text.

II. PRAKTICKÁ ČÁST

3 POPIS SITUACE A ZADÁNÍ ÚKOLU

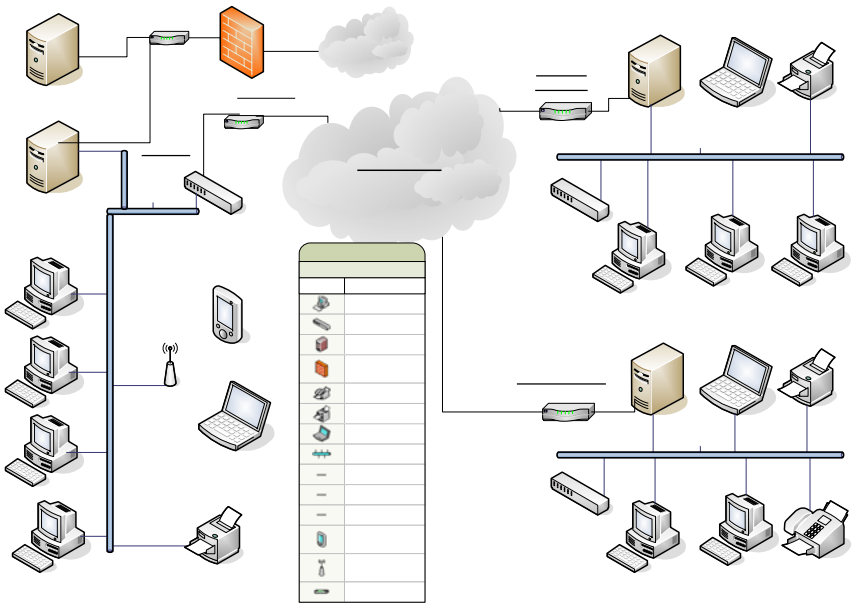
Pro tento účel jsem zvolil firmu, která má jedno ředitelství a dvě pobočky umístěné v naší republice. Jedna pobočka sídlí v tomtéž městě jako ředitelství . Operační systém na stanicích je použit od firmy Microsoft a jedná se o verze Windows 98, 2000 a XP Pro. Na serverech je instalován operační systém Windows 2003. Instalovaným kancelářským softwarem na jednotlivých stanicích je MS Office. V sídlu firmy je bezdrátová síť tvořena jedním AP a několika klientskými stanicemi. Ve firmě pracuje několik mobilních uživatelů a tak je nutné je bezpečným způsobem připojit vzdáleně do sítě.

Požadavek zadavatele zní:

- Propojit dvě pobočky zadavatele s ředitelstvím
- tuto firemní síť připojit k internetu
- zabezpečit vzdálený přístup do sítě
- provést zabezpečení včetně bezdrátové sítě na ředitelství
- vytvořit bezpečností politiku

4 PRAKTICKÝ NÁVRH ZABEZPEČENÍ

Návrh je rozložen do jednotlivých bodů. V těchto bodem vysvětlím jakým způsobem daný úkol vyřeším. Pro osvědčenou spolehlivost jsem zvolil směrovače firmy CISCO. Směrovače jsem doplnil záložním spojením ISDN. Spojení s internetem slouží pevná datová linka na které je umístěn Firewall plnící zároveň funkci VPN koncentrátoru.



Obr. 21. Blokové schéma návrhu řešení

4.1 Propojení poboček s ředitelstvím

Propojení poboček bude realizováno pomocí směrovačů CISCO, pevných datových okruhů a pomocí služby Frame Relay. Protokol Frame Relay využívá pro datová propojení pevných virtuálních kanálů PVC. Typická rychlost se bohybuje v rozmezí 64 kbps - 2 Mbps. Z hlediska uživatele se virtuální kanál Frame Relay s garantovanou propustností CIR nastavenou na požadovanou hodnotu jeví jako podstatně rychlejší linka, a to nejen z hlediska dosahované skutečné propustnosti spojení, ale i z hlediska odezvy.

Jako směrovače na jednotlivé pobočky je použit typ CISCO 1712-VPN/K9 (router s ISDN BRI zálohou). Na ředitelství CISCO 2620 XM doplněné o 1 x CISCO WIC 1T a 1 x WIC 1B –S/T.

Celé síť je zálohovaná u poskytovatele. Navíc je použito záložní spojení přes linky ISDN. Směrovače v případě ztráty spojení automaticky navážou komunikaci a konektivita zůstane zachována.

CISCO 1712 VPN/K9

Bundle - směrovač (32MB Flash, 64MB DRAM a IOS IP Plus/ADSL/Firewall/IDS/IPSEC 3DES) - 4-port switch 10/100Base-TX (LAN), 1x ISDN BRI (záloha WAN připojení), 1 port 10Base-T (WAN - xDSL, kabelový modem), 1 AUX port (připojení modemu pro vzdálenou správu - až 115kbps asynchronně), 1 modul VPN modul a 1 port konsoly (správa zařízení).

CISCO 2620 XM

Směrovač (30 kpps) s podporou hlasových funkcí (16MB Flash, 32MB DRAM a IOS IP) - 1 port 10/100Base-TX (LAN), 2 sloty pro WIC/VIC moduly (WAN), 1 slot pro NM modul, 1 interní slot pro AIM kompresní modul (HW šifrování DES, 3DES (AIM-VPN/BP) nebo HW komprese dat s poměrem 4:1 pro 8Mbps (AIM-COMPR2)), 1 AUX portem (připojení modemu pro vzdálenou správu nebo záložní spojení - až 115kbps asynchronně) a 1 port konsoly (správa zařízení).

Cisco WIC-1B-S/T

WIC modul vybavený 1 rozhraním ISDN BRI (euroISDN2 - rozhraní S/T). Konektor RJ-45. Modul určen pro 1600, 1700, 2600 a 3600. WIC-1B-S/T.

Cisco WIC-1T

WIC modul vybavený 1 sériovým WAN portem sync/async (2,048 Mbps/115,2 kbps), asynchronně jen v 1600 a 1720. Konektor DB-60 (RS-232, RS-449, RS-530, V.35, X.21) - DTE nebo DCE mód. Modul určen pro 1600 (pouze v async. režimu), 1700 (u 1720 pouze v async. režimu), 2600 (pouze v sync. režimu) a 3600 (pouze v sync. režimu). WIC-1T.

Stupeň ochrany	Access Rate (kbs)	CIR (kbs)
Ředitelství	1024	512
Pobočka vzdálená	512	256
Pobočka místní	512	256

Tabulka 1. Virtuální kanály FR

4.2 Připojení firemní sítě k internetu

Přístup k síti internet bude řešen pomocí pevného digitálního datového okruhu. Vzhledem k velikosti firemní sítě a využití jednotlivých uživatelů postačí rychlost 1 Mbps. Rychlost tohoto spojení je garantována a linka má 24 hod. dohled. ISP dále poskytuje službu zálohování DNS, Mail serveru a WWW serveru. Jako směrovač je použit CISCO PIX 506 E-BUN – K9 .

CISCO PIX 506

Bundle - HW firewall + 3DES/AES licence pro malé/střední kanceláře. DHCP klient/server, PPPoE, SNMP, PAT for IPsec.Firewall: Stateful inspection, DoS (Denial-of-Service) a AAA (TACACS+ a Radius), podpora NAT/PAT.VPN: IKE a IPsec; 56-bit DES, 168-bit 3DES a 256-bit AES. Propustnost bez šifrování 100Mb/s, s IPSec 20Mb/s (DES), s IPSec 17Mb/s (3DES), s IPSec 30Mb/s (128-bit AES). Hardware VPN client (Easy VPN Remote), VPN concentrator services (Easy VPN Server) pro až 25 remote uživatelů, Site-to-site VPN. Max. 25.000 současných TCP/UDP spojení, max. 25 VPN současně.Rozhraní: 2x 10/100Base-TX (LAN + WAN)

4.3 Vzdálený přístup

Vzdálený přístup do sítě či k aplikaci je metoda zajišťující přímou nebo nepřímou komunikaci klienta (uživatele) se vzdáleným systémem (často umístěným v interní síti nebo DMZ).
Komunikace je zajištěna pomocí několika mechanismů:

- Autentizace a Autorizace
- Ochranné prvky (firewall a VPN koncentrátor) zajišťující komunikaci

V tomto případě jsou klienti připojeni pomocí (vytáčené) linky ke svému ISP, čímž je jim umožněn přístup k Internetu. Klienti mají nainstalovaného klienta Kerio VPN , který jim zajišťuje VPN připojení k bráně, kterou je v našem případě FireWall-1.

1. Uživatel naváže VPN komunikaci buď pomocí transparentního režimu, tzn. snaží se navázat spojení se serverem za firewallem, nebo manuálně – zvolí Connect a klient se připojí k firewallu.

2. Uživatel je dotázán na autentizační údaje – autentizace může proběhnout jménem a heslem nebo silnější autentizační metodou.

3. Firewallem může (a nemusí) být klientovi přidělena IP adresa interní sítě nebo DMZ, takže ten se pak při komunikaci chová, jako by byl uživatel připojen do dané sítě. Zároveň je možné díky nastavení bezpečnostní politiky klienta zabezpečit, že uživatel během připojení může komunikovat pouze s povolenými servery.

Obr. 22. Vzdálený přístup

Stupeň ochrany	**Metoda**	**Popis**
Základní	Jméno a heslo	Autentizace pomocí statického uživatelského jména a hesla
Střední	Jméno a jednorázové heslo	Autentizace pomocí jména a jednorázově platného hesla (například S/Key)
Standardní ochrana	Dvoufaktorová autentizace bez interakce uživatele	Uživatel vlastní autentizační předmět generující jednorázová hesla bez nutnosti vložení PIN, předmět je vázán na uživatelské jméno.
Silná ochrana	Dvoufaktorová autentizace s interakcí uživatele	Uživatel vlastní autentizační předmět generující jednorázová hesla s vazbou na své přihlašovací jméno. Pro použití předmětu musí navíc zadat PIN. (například řešení SecurID, Vasco, Cryptocard)
Velmi silná ochrana	Dvoufaktorová autentizace s interakcí uživatele a kryptografickými funkcemi.	Kryptografická autentizace za použití certifikátů a předmětu chránícího privátní klíč na základě hesla (např. Smart Card).

Tabulka 2. Bezpečnostní požadavky

4.4 Zabezpečení sítě

Fyzická bezpečnost

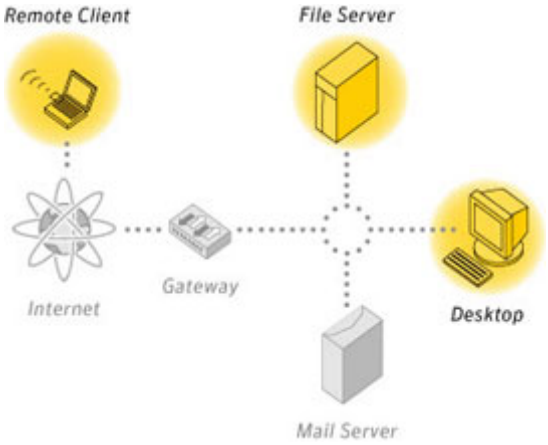
Instalace kvalitních mechanických zábran v celém objektu doplněného o elektronický poplašný systém, případně doplněný o požární systém. Servery a aktivní síťové prvky musí být v jedné vyhrazené místnosti s omezeným přístupem osob. Jednotlivé servery doplníme o vlastí zámek a odpojíme nepoužívané síťové zásuvky. Vybavíme kanceláře skartovacími zařízeními a důsledně dbáme na ochranu informací, které jsou vytištěny na papíře. Důležité je nenechávat návštěvníky uvnitř zabezpečených prostor bez dozoru. Toto opatření se týká i externích pracovníků. Při likvidaci starších záznamových médií jako jsou počítačové harddisky, pásky se zálohami, diskety nebo CDROM zkontrolovat a smazat veškeré informace. Posledním krokem je evidence všech zařízení, které se připojují k firemní síti. Tyto zařízení vybavit evidenční nálepkou a o každém zařízení mít informace jako je hardwarová a softwarová konfigurace.

Kontrola přístupu

Zde ve spolupráci s bezpečnostní politikou určíme oprávnění přístupu k jednotlivým zdrojům. Zkontrolujeme sílu používaných hesel, jejich universálnost a jejich pravidelnou obměnu. K tomuto nám nejlépe poslouží systémová politika, kde přesně stanovíme pravidla. Tyto pravidla se netýkají jen serverů a síťových zařízení, ale primárně všech počítačů ve firemní síti. Na jednotlivých počítačích dále zkontrolujeme zda běžní uživatelé nemají administrátorský přístup, instalaci nelegálního software a zda používají vyměněná paměťová média. Pokud ano tak ji omezit, nebo zakázat ve spolupráci s bezpečnostní politikou.

Ochrana proti škodlivému software

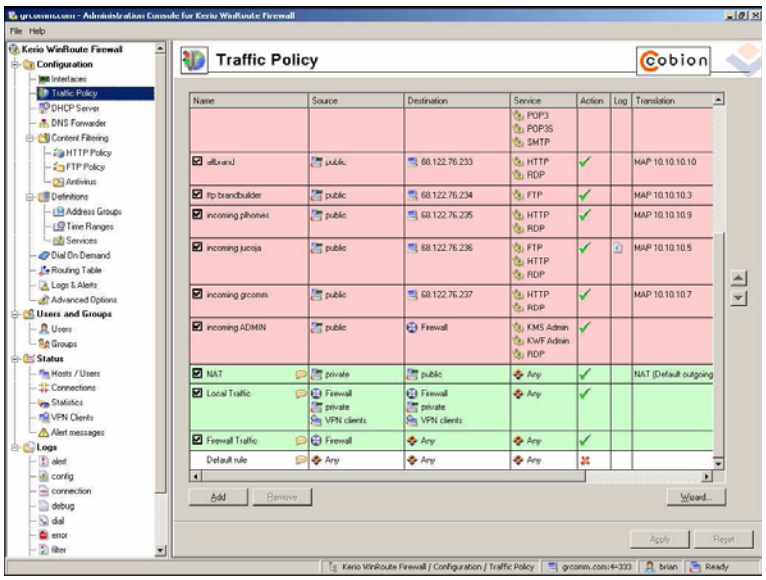
Na hlavním serveru je instalován Symantec Antivirus. Ten je také instalován na dalších dvou serverech na pobočkách organizace . Klienti nainstalovaní na jednotlivých počítačích se tak mohou rovnoměrně připojovat a zbytečně nezvyšovat provoz na síti Frame Relay. Tento antivir je integrován s instalovaným MS Exchange a firewallem Kerio WinRoute.Vytváří nejen antivirovou ochranu, ale i ochranu před adwarem a spywarem.



Obr. 23. Symantec antivirus

Firewall

Primární ochranu firemní sítě zajišťuje CISCO PIX 506. Má vestavěn HW Firewall s ochranou proti DOS útokům. Dále má integrovaný VPN koncentrátor. Jako sekundární firewall je použit Kerio WinRoute. Ten obsahuje VPN server, který je použit pro vzdálené připojení zaměstnanců k firemní síti. Je integrován s instalovaným antivirovým programem Symantec Antiviru. To mimo jiné umožňuje kontrolu obsahu veškeré webové komunikace, včetně HTML stránek. Kontrolovány jsou rovněž soubory stahované přes http nebo FTP.



Obr. 24. Kerio WinRoute

4.5 Bezpečnostní politika

Stanovení bezpečnostní politiky je velmi specifické. Záleží na konkrétní situaci v organizaci kde má být vytvořena a posléze i uplatňována. Představím tedy obecnější pravidla, která by měla být při zavádění bezpečností politiky (BP) dodržena. Při vytváření BP nám může pomoci mezinárodní standardy, jako např. (International Organization for Standardization) ISO/IEC 17799:2005 Kodex praxe řízení informační bezpečnosti , ISO/IEC 13335 Management bezpečnosti informačních a komunikačních technologií. nebo ISF (Information Security Forum) The Standard of Good Practice for Information Security. Jako první musíme stanovit pravidla BP, provést analýzu rizik a vytvoření bezpečnostního týmu.

Vytvoření pravidel

Organizace musí určit, jaká úroveň bezpečnosti je pro ni vhodná a dosažitelná vzhledem k její organizační struktuře, zaměstnanců, již definovaných politik, vztah mezi jednotlivými odděleními a úrovní přístupů jednotlivých pracovníků na všech úrovních. Na základě toho můžeme stanovit role jednotlivých uživatelů, jejich odpovědnost a stanovit obecná pravidla. Zde stanovíme kategorie uživatelů, definujeme jednotlivé uživatelské účty a určíme odpovědnost za užívání účtu. Zároveň ve spolupráci s vedením organizace stanovíme sankce za nedodržení těchto pravidel.

Analýza rizik

Provedení analýzy rizik je základním procesem, z jehož výsledků lze vyjít při výstavbě bezpečnostních struktur ve firmě. Účelem analýzy rizik je identifikace bodů vstupu do sítě a možné způsoby útoku na síť zvnějšku i zvnitřku. To vyžaduje identifikaci všech síťových zdrojů a následné přiřazení odpovídajících rizik. Zde tedy určíme velikost rizika v případě napadení firemního firewallu nebo routeru. Dále vymezíme okruhy lidí na běžné uživatele, uživatele s vyššími právy a administrátory. Přesně určíme kdo má přístup k jakým zdrojům.

Dále je třeba zjistit způsob identifikace, jeho zneužití a případné slabiny. Zde můžeme využít různých softwarových utilit na prolamování hesel, nebo sniferů na sledování sítě.

Bezpečnostní tým

Zde budou pracovníci ze všech oddělení organizace. Tento tým bude odpovědný za povědomí o BP a za její vynucování. Dále bude odpovědný za reakci na narušení bezpečnosti a bude podávat zprávy nejvyššímu managementu. Tato skupina bude informována o všech aspektech BP a bude se účastnit na jejím dalším vývoji. V tomto týmu musí být pracovník, který má na starost IT v organizaci. Ten bude mít za úkol monitorování bezpečnosti sítě a vytváření definic jako reakce na různé bezpečnostní incidenty.

Organizace BP

Při stanovení bezpečností politiky, provedení analýzy bezpečnosti a vytvoření bezpečnostního týmu si definujeme jednotlivé zdroje např. použitý operační systém, instalované aplikace, databáze nebo další síťová zařízení. Využijeme skutečnosti, že v bezpečnostním týmu máme pracovníky ze všech oddělení organizace a stanovíme priority řešení zjištěných problémů. Postup řešení spočívá v rozdělení na několik dílčích úloh, které se navzájem doplňují. Při hledání a řešení jednotlivých úloh je vhodné začít kategoriemi s největšími riziky a poté po seznamu postupovat dolů.

Realizace

Po předchozí přípravě přistoupíme k realizaci. Je třeba si uvědomit, že distrubuované systémy není možné zabezpečit zcela. Cílem je vytvořit povědomí o bezpečnosti, minimalizovat riziko za využití dostupných technologií.

Opakování

Po realizaci přichází ke slovu naplánování pravidelných revizí. Tyto revize by se měli pravidelně opakovat po 6 až 12 měsících. Nebo pokud organizace projde zásadními změnami, které by měli vliv na BP.

Penetrační test

Je to test bezpečnostní politiky. Pomůže nám zjistit slabá místa a tak zkvalitnit zavedené bezpečnostní opatření. Můžeme ho provést svépomocí, nebo jej přenechat auditorské firmě.

Havarijní plán

Součástí bezpečnostní politiky je i Havarijní plán IS **.** Výpadek informačního systému může znamenat velkou hrozbu pro chod společnosti. Plán kontinuity IS připravuje organizaci na potenciální havárie, omezuje jejich dopady na fungování informačního systému a stanoví postupy, jak řešit nestandardní situace. Jednotlivá narušení mohou být nejrůznějšího typu, například:

- přírodní nebo technologické havárie,
- cílené útoky na informační systém,
- neúmyslné selhání obsluhy s důsledkem výpadku informačního systému,
- nedostatek obslužného personálu,
- výpadek subdodavatele např. elektrické energie, plynu, Internet providera, atp

Plán kontinuity by měl zahrnovat:

- Prevenci
- Reakci na mimořádnou událost
- Obnovu kritických funkcí organizace
- Zotavení z mimořádné události
- Obnova původního stavu

Prevence

Znamená přípravu plánů a jejich realizačních opatření, přípravu lidí i technických prostředků pro případ havárie. Na její kvalitě závisí četnost a doba výpadků a náklady na obnovu funkčnosti.

Reakce mimořádnou událost

Prioritním zájmem každé společnosti je, aby škody vzniklé v případě havárie byly co nejmenší a co nejméně narušily chod společnosti. Do této fáze spadá také ochrana zdraví a lidských životů. Probíhají činnosti k zastavení, omezení rozsahu či zpomalení události.

Obnova kritických funkcí organizace

Po prvotní reakci následuje obnova kritických procesů. Tato fáze má pro organizace velký význam, neboť zde se rozhoduje o velikosti následných škod, případně o samotné existenci organizace. Činnosti pracovníků se přitom řídí dle havarijních procedur. Jejich součástí je např. přesun provozu do náhradních prostor a náhradního zařízení, obnova provozu v nouzovém, havarijním stavu, atp.

Zotavení z mimořádné události

Další fází procesu obnovy je obnova podpůrných činností a celkové zotavení organizace z narušení. Obnovují se především takové funkce, které z hlediska časové dostupnosti a významu nejsou kritické, ale přesto se značnou měrou podílejí na kvalitě služeb, které organizace poskytuje.

Obnova původního stavu

V této fázi se obnovuje původní stav provozu IS, je zjištěn rozsah škod, jsou rekonstruovány budovy místnosti, zajištěna technika, SW prostředky a přechod provozu z havarijního do normálního stavu.

ZÁVĚR

Pokud počítač není při připojení k Internetu chráněný, hackeři mohou získat přístup k vašim osobním informacím v počítači, mohou do něj nainstalovat kód, který ničí soubory nebo způsobuje poruchy, případně mohou váš počítač zneužít k působení problémů jiným domácím a firemním počítačům připojeným k Internetu. Firewall pomáhá zachytit mnoho druhů útoků z Internetu ještě dříve, než dosáhnou vašeho systému.

Brána firewall nezabezpečí počítač stoprocentně. Představuje však nejúčinnější první linii obrany. Proto je nutné mít neustále aktualizovaný operační systém, antivirový program, antispyware program a dodržovat bezpečnostní politiku.

SEZNAM POUŽITÉ LITERATURY

Monografie:

[1]NÁDENÍČEK, P. PŘIBYL, T. PŘIKRYLOVÁ, O. VOBRUBA, T. *Chip Special*, Vogel Publishing, 2002

[2] HÁK, I. Moderní počítačové viry, II vydání, el.podob

[3] SCAMBRAY, J. MC CLURE, S. KURTZ, G. Hacking bez tajemství, II aktualizované vydání Computer Press 2002 ISBN 80-7226-644-6

[4] Doseděl, T. Počítačová bezpečnost a ochrana dat, Computer press, Praha 2004 ISBN 80-251-0106-1

[5]] Matějka, M. Počítačová kriminalita, Computer press, Praha 2002

[6] PC WORD Security, IDG Czech, a.s. čtvrtletník 2005/2006 ISSN 1214-794X

[7] PC WORD, IDG Czech, a.s. měsíčník 2004/2006

[8] CHIP, Vogel Burda Comunications s.r.o., měsíčník 2004/2006

Internetové zdroje:

[9] Symantec Antivirus 10 [online], [cit. 2006-05-12]. Dostupný z WWW: <http://www.symantec.cz/region/cz/product/savsmb_index.html>.

[10] Kerio: Kerio WinRoute 6.0 [online], [cit. 2006-05-12]. Dostupný z WWW: <http://www.kerio.cz/kwf_home.html>.

[11] Subelt Kerio Personal Firewall [online], [cit. 2006-05-12]. Dostupný z WWW: <http://www.sunbelt-software.com/Kerio-Download.cfm>.

[12] Outpost Firewall PRO [online], [cit. 2006-05-10]. Dostupný z WWW: <http://www.agnitum.com/products/outpost/index.php>.

[13] Zone Aarm [online], [cit. 2006-05-10]. Dostupný z WWW: <http://www.zonelabs.com/store/content/home.jsp>.

[14] Microsoft: ISA server 2004 [online], [cit. 2006-05-17]. Dostupný z WWW: <http://www.microsoft.com/cze/windowsserversystem/isaserver/>.

[15] Esset: Nod32 [online], [cit. 2006-05-09]. Dostupný z WWW:
<http://www.eset.cz/cz>.

[16] alvil: avast! antivirus v 4.7 [online], [cit. 2006-05-09]. Dostupný z WWW:
<http://www.avast.cz/index_cze.html>.

[17] Grisoft: AVG antivirus [online], [cit. 2006-05-09]. Dostupný z WWW:
<http://www.avg.cz/doc/1>.

[18] SPYBOT [online], [cit. 2006-05-09]. Dostupný z WWW:
<http://www.safer-networking.org/en/index.html >.

[19] Microsoft: Windows Defender beta 2 [online], [cit. 2006-05-15]. Dostupný z WWW:
<http://www.microsoft.com/athome/security/spyware/software/default.mspx>.

[20] Lavasoft [online], [cit. 2006-05-09]. Dostupný z WWW:
<http://www.lavasoft.com/>.

[21] HOAX: Čím hoax škodí [online], [cit. 2006-05-09]. Dostupný z WWW:
<http://www.hoax.cz/cze/index.php?action=hoax_damages >.

[22] Igiho stránka o virech [online], [cit. 2006-05-12]. Dostupný z WWW:
<http://www.viry.cz/go.php>.

[23] Igiho stránka o virech: Odkazy [online], [cit. 2006-05-12]. Dostupný z WWW:
<http://www.viry.cz/go.php?p=viry&t=listodkazy>.

[24] Microsoft: Windows update [online], [cit. 2006-05-05]. Dostupný z WWW:
<http://windowsupdate.microsoft.com/ >.

[25] Microsoft: služba stažení softwaru [online], [cit. 2006-05-05]. Dostupný z WWW:
<http://www.microsoft.com/downloads/Search.aspx?displaylang=cs>.

[26] CISCO: Produkty a služby [online], [cit. 2006-05-14]. Dostupný z WWW:
<http://www.cisco.cz/index.sub.php?pid=products>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

Antivirový software	Software speciálně vytvořený na detekci a prevenci známých virů.
API	Rozhraní pro programování aplikací
Autentifikace	Proces zjišťování, zda někdo nebo něco je skutečně tím, za co či za koho se vydává. V soukromých a veřejných počítačových sítích (včetně Internetu) se ověřování obvykle provádí pomocí hesel.
Bezpečnostní mezera	Jakákoli vada produktu, administrativního procesu nebo kroku, popř. fyzické vlivy, které vystavují počítač útokům uživatele se zlým úmyslem.
Biometrie	Používání tělesných měr, jako jsou otisky prstů nebo duhovky, jako prostředku autentizace.
CD-ROM	CD-ROM je datová verze hudebního CD umožňující uložení až 700 MB dat. Pomocí vypalovací mechaniky CD je možné vytvářet nový CD-ROM.
CIR	Commited Information Rate. Rychlost (bit/s) garantovaná sítí Frame Relay pro přenos informací za normálních podmínek.
Cyberslacking	Plýtvání časem, obvykle v zaměstnání, brouzdáním po Internetu.
Červ	Druh počítačového viru. Červ se obvykle šíří bez přičinění uživatele a rozšiřuje po sítích své úplné (eventuálně upravené) kopie. Červ může využít paměť nebo datovou kapacitu, takže počítač přestává odpovídat.
Dešifrování	Proces převádění zašifrovaných dat zpět do jejich původní podoby.
E-mailový podvrh	Jinak neškodný e-mail, jehož cílem je příjemce vystrašit nebo jej přimět k přeposlání zprávy dalším uživatelům (případně oboje). Příkladem může být falešné varování před virem nebo řetězová zpráva (dopis).
Falšování	Pozměňování obsahu balíčků přenášených přes Internet nebo upravování dat na počítačových discích při narušení sítě.
Firewall	Hardware nebo software, který chrání počítač nebo síť před neoprávněnými přístupy z Internetu.

Hacker	Hackeři jsou techničtí mistři. Většina z nich jsou nevinní nadšenci, které baví pracovat s počítačem. Někteří však využívají svých dovedností k nekalým účelům: nezákonnému nabourávání systémů nebo vytváření virů či jiného softwaru se zlým úmyslem.
Hardwarový firewall	Firewall, který funguje jako samostatné zařízení, například router, namísto spouštění jako software na počítači.
IPSec	IP Security (IPSec) zajišťuje bezpečnost přenosu citlivých informací přes nechráněné sítě, jako je Internet. IPSec se chová jako síťová vrstva a chrání a autentizuje IP pakety mezi zúčastněnými IPSec zařízeními.
ISDN	Integrated Services Digital Network. Technologie určená k přenosu hlasových a datových informací.
ISP	Internet Service Provider. Společnost, která poskytuje přístup k Internetu.
Krádež identity	Trestný čin vydávání se za někoho pomocí jeho soukromých informací za účelem finančního zisku.
LAN	Lokální počítačová síť (Local Area Network - LAN) určená ke komunikaci mezi počítači.
LDAP	Lightweight Directory Access Protocol je standardizovaný protokol pro přístup k adresářovým službám, definuje komunikaci mezi serverem a klientem.
L2TP	Protokol L2TP zajišťuje bezpečnost přenosu citlivých informací přes nechráněné sítě, jako je Internet.
Makrovirus	Makrovirus využívá makra běžných aplikací, jako jsou textové editory, k provádění škodlivých/nežádoucích činností.
Modem	Zařízení, které propojuje počítač s veřejnou telefonní sítí, obvykle za účelem připojení na Internet.
MP3	MPEG-1 Audio Layer-3 je standardní zařízení pro komprimování a ukládání zvukových souborů, využívá se obvykle pro hudbu.
MP3 přehrávač	Zařízení na přehrávání hudebních souborů MP3.
Odmítnutí odpovědnosti	Například nákup zboží na internetové aukci, při němž nakupující nezaplatí. Vymazání nebo pozměnění souboru způsobem, který nelze dohledat a je možné ho popřít.

Paket	Základní jednotka datového přenosu na síti.
Peer – to - Peer	Síť, ve které může každý počítač fungovat zároveň jako server a jako klient; obvykle se používá ke sdílení hudebních souborů po Internetu.
Penetrační testování	Simulovaný útok důvěryhodných hackerů na počítačový systém ve snaze najít bezpečnostní mezery a zjistit možnosti zlepšení bezpečnosti.
Pevný disk	Pevná magnetická disková jednotka používaná k ukládání dat na osobních počítačích.
Phishing	Phishing (česky také rhybaření) je pokus o krádež identity, při němž zločinci oslovují uživatele Internetu s cílem získat od nich soukromé informace jako např. uživatelské jméno nebo heslo.
Pirátství	Ilegální používání nebo rozmnožování materiálů, na které se vztahují zákony o duševním vlastnictví, například autorské právo.
Port	Každá síťová služba na daném počítači má vlastní port, jako například telefonní přípojka.
Prohlížeč	Program, který umožňuje uživatelům číst a prohlížet stránky na internetové síti (World Wide Web), jako je Mozilla Firefox nebo Microsoft Internet Explorer.
Přístupová práva	Možnost uživatelů číst, měnit nebo mazat soubory.
RAID	Z angl. "Redundant Array of Inexpensive Discs". Namísto používání jednoho velkého nákladného disku používá většina serverů tzv. diskové pole RAID. Existují zde různé úrovně redundance, takže RAID úroveň 5 je nejvyšší úroveň bezpečnosti. Jeden disk v rámci pole může selhat, nebo být dokonce vyjmut, ale data přesto zůstávají v bezpečí.
Root kit	Software, který modifikuje principy, na nichž pracuje operační systém. Velice často (ne vždy!) je zneužívaný hackery ke skrývání programů apod. před antivirovými a dalšími aplikacemi.
Router	Zařízení které, dokáže díky znalosti topologie sítě zvolit pro příchozí paket nejvhodnější další cestu. Směrovače pracují s logickými adresami.
Server	Počítač, který poskytuje službu jiným počítačům prostřednictvím sítě.

Síť	Určitý počet vzájemně propojených počítačů.
Sociální inženýrství	Triky používané hackery, jejichž cílem je přístup do zab. systémů, například předstíráním, že jsou pracovníci technické podpory
Spoofing	Například falšování e-mailových zpráv nebo skenování internetových paketů za účelem získání platného hesla, se kterým je možné se "nabourat" do počítače.
Spyware	Nežádoucí software, který tajně monitoruje činnost uživatele, hledá soukromé informace nebo dává vnějším uživatelům kontrolu nad počítačem.
Stahovat	Přenášet kopii souboru ze vzdáleného počítače na svůj počítač pomocí modemu nebo sítě.
Šifrování	Proces převádění dat do šifrovaného textu, aby k nim neměly přístup neoprávněné osoby.
Token	Fyzický předmět, například čipová karta, který se používá k ověření uživatelů nebo uložení dat.
Trojský kůň	Počítačový program, který je na první pohled užitečný, ale ve skutečnosti páchá škody.
USB	Univerzální sériová sběrnice: standardní rozhraní k propojování počítačů a periferií.
Uživatelské jméno	Kódové jméno, které společně s heslem odemyká uživatelský účet.
Uživatelský účet	Soubor pravidel definujících přístup k souborům a systémům na počítači, který je vlastní jednotlivému uživateli.
Virová definice	Otisk prstu", který používá antivirový software při zjišťování napadení počítače virem.
VPN	Soukromá datová síť (Virtual Private Network, VPN), která využívá jakoukoliv veřejnou síť jako třeba internet tím, že zašifruje data na jednom uzlu a pomocí bezpečnostních procedur vytvoří "tunel", jímž mohou data přejít do místa určení.
Virus	Kód napsaný výslovně za účelem toho, aby se sám reprodukoval. Virus se pokouší šířit z počítače na počítač tím, že infikuje jiný soubor, obvykle program, který lze spustit. Kromě šíření

	může být virus použit k tomu, aby vás poškodil, nebo pro nezákonnou činnost. Viz také Trojský kůň (tzv. trojan), červ (worm) a spyware.
Worm	Worm = červ. Druh počítačového viru. Červ se obvykle šíří bez přičinění uživatele a rozšiřuje po sítích své úplné (eventuálně upravené) kopie. Červ může využít paměť nebo datovou kapacitu, takže počítač přestává odpovídat.
Webmail	E-mailový systém, který využívá ke čtení a posílání e-mailů internetový prohlížeč, a nikoli samostatný program e-mailového klienta.
Záloha	Kopírování uživatelských dat a systémových souborů na záložní médium.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: NÁZEV PŘÍLOHY