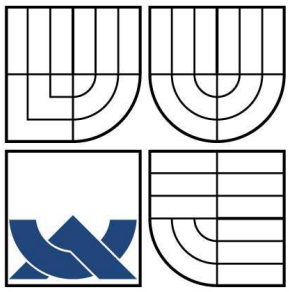
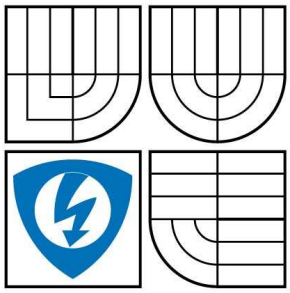


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA ELEKTROTECHNIKY A KOMUNIKAČNÍCH TECHNOLOGIÍ
ÚSTAV TELEKOMUNIKACÍ

FACULTY OF ELECTRICAL ENGINEERING AND COMMUNICATION
DEPARTMENT OF TELECOMMUNICATIONS

MODERNÍ POČÍTAČOVÉ VIRY
MODERN COMPUTER'S VIRUSES

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — LUKÁŠ MALINA
AUTHOR

VEDOUCÍ PRÁCE — ING. RADIM PUST
SUPERVISOR

BRNO 2008

Originální zadání (viz vytištěná verze)

LICENČNÍ SMLOUVA (viz vytištěná verze a příloha license.pdf)

Anotace

Bakalářská práce Moderní počítačové viry se skládá ze dvou hlavních cílů (Analýza počítačových virů a návrh zabezpečení střední počítačové sítě) rozdělených na tři části: Analýza počítačových virů, Vlastní návrh zabezpečení osobního počítače koncového uživatele (Terminálu) a Vlastní návrh zabezpečení střední počítačové sítě. V první části jsou analyzovány metody šíření a infekce, specifické vlastnosti a dopady počítačových virů na osobní počítače. V druhé části je uvedeno řešení zabezpečení osobních počítačů pomocí antivirového programu, osobní firewallu a antispamového softwaru. Dále jsou shrnuty výsledky testovaní některých volně dostupných antivirových softwarů a jiných bezpečnostních softwarů, s případnými postupy konfigurace a doporučení pro správný chod těchto programů.Třetí část pak uvádí komplexní návrh zabezpečení střední počítačové sítě, kde je uvedena struktura zabezpečení sítě. U jednotlivých použitých komponentů jsou naznačeny konfigurační postupy a doporučení pro maximální bezpečnost. Struktura je přizpůsobená pro aktivní síťové prvky firmy Cisco, které jsou v dnešní době nejpoužívanější. Celkový návrh zabezpečení sítě je orientován na hardwarový firewall Cisco PIX, u kterého jsou rozvedeny potenciální možnosti nastavení. Dále jsou v třetí části uvedeny některé důležité tipy a doporučení pro celkovou činnost sítě, včetně nastavení bezpečnostní politiky, bezpečných hesel a šifrování dat. Rovněž jsou popsány i různé techniky dohledu a monitorování správné a bezpečné činnosti sítě, při použití sond IDS (intrusion detection system) a IPS (intrusion prevention system), či použití obsáhlého monitorovacího softwaru MARS (Cisco security monitoring, analyzing and response system) od firmy Cisco.

Klíčová slova: virus, počítačový červ, útok odepření služby, antivirový program, firewall, návnada, sonda IDS

Abstract

Bachelor's thesis "Modern computer's viruses" is composed from two mainly object (analysis computer's viruses and suggestion of security middle computer network), separated for three parts: Analysis computer's viruses, Personal suggestion of security personal computer end-user (computer terminal) and Personal suggestion of security middle computer network. Methods of transmission and infection, specific properties of viruses and impact upon personal computers are examined in the first part. Resolution of personal suggestion of security personal computer with help of antivirus software, personal firewall and antispam software is inducted in the second part. Futher, results of testing some free AV software and other security software are summarized with possible progress of configuration and recommendation for correct running this software. Complex suggestion of security middle computer network is adduced in the third part, where is inducted structure of security network. Configuration progression and recommendation for maximum security is indicated on particular used components. Structure is adapted for active network Cisco components, which are most used around these days. Completely suggestion of security network is directed on hardware firewall Cisco PIX, where is unfolded potential possibility of options. Futher, the third part contain some important tips and recommendation for completely working network, including setting security preference, security passwords and data encryption. Also, there is described various techniques monitoring and supervision working security network using complex monitoring software MARS (Cisco security monitoring, analyzing and response system) from Cisco company.

Keywords: virus, worm, denial of service, antivirus software, firewall, honeypot, probe IDS

Metadata (viz vytištěná verze a příloha metadata.pdf)

Prohlášení

Prohlašuji, že svou bakalářskou práci na téma"Moderní počítačové viry" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že v souvislosti s vytvořením této bakalářské práce jsem neporušil autorská práva třetích osob, zejména jsem nezasáhl nedovoleným způsobem do cizích autorských práv osobnostních a jsem si plně vědom následků porušení ustanovení § 11 a následujících autorského zákona č. 121/2000 Sb., včetně možných trestněprávních důsledků vyplývajících z ustanovení § 152 trestního zákona č. 140/1961 Sb.“

V Brně dne …… ……..
(podpis autora)

Poděkování

Děkuji vedoucímu bakalářské Ing.Radimu Pustovi, za pomoc, cenné rady a celkovou podporu při zpracování bakalářské práce.

V Brně dne …… ……..
(podpis autora)

Seznam použitých zkratek

AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AES	Advance data Encryption Standard
AH	Authentication Header
API	Application Program Interface
ARP	Address Resolution Protocol
ASA	Adaptive Security Algorithm
ATM	Asynchronní Transportní Mód
AV	AntiVirus
AVP	AntiVirový Program
BIOS	Basic Input/Output System
CA	Certification Authority
COM	Component Object Model
CPU	Central Processing Unit
CSACS	Cisco Secure Access Control Server
CS-MARS	Cisco Security Monitoring, Analyzing and Response System
CSR	Certification signed request
DCOM	Distributed Component Object Model
DDoS	Direct Denial of Service
DES	Data Encryption Standard
DHCP	Domain Host Control Protocol
DLL	Dynamic Link Library
DMZ	DeMilitarizovaná Zóna
DNS	Domain Name Server
DoS	Denial of Service
DOS	Disk Operating System
EAP	Extensible Authentication Protocol
EAP-TTLS	EAP- Tunneling Transport Layer Security
ELF	Executable and Linkable Format
EPO	EntryPoint Obscuring
ESP	Encapsulating Security Payload
EXE	EXEcutable files

FAT	File Allocation Table
FTP	File Transfer Protocol
FWSM	FireWall Services Module
HFS	Hierarchical File System
HIPS	Host-based Intrusion Prevention System
HLL	High Level Language
HTML	Hyper Text Markup Language
HTTP	HyperText Transfer Protocol
IAT	Import Address Table
ICMP	Internet Control Message Protocol
IDEA	International Data Encryption Algorithm
IDS	Intrusion Detectional System
IDT	Interrupt Descriptor Table
IKE	Internet Key Exchange
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPS	Intrusion Preventional System
IPSec	Internet Protocol Security
ISAKMP	Ip Security Association Key Management Protocol
ISP	Internet Services Provider
IT	Informační Technologie
IVT	Interrupt Vector Table
JS	Java Skript
L2TP	Layer 2 Tunneling Protocol
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
MBR	Master Boot Record
MIME	Multipurpose Internet Mail Extensions
NAT	Network Address Translation
NDS	NetWare Directory System
NE	New Executable
NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Prevention System
NNTP	Network News Transfer Protocol

NTFS	New Technology File Systém
NTP	Network Time Protocol
OLE	Object Linking and Embedding
OS	Operační Systém
OSPF	Open Shortest Path First
PAT	Port Address Translation
PC	Personal Computer
PE	Portable Executable
PEAP	Protected EAP
PHP	Personal Home Page
POP3	Post Office Protocol version 3
PPPoE	Point to Point Protocol of Ethernet
PPTP	Point to Point Tunneling Protocol
QoS	Quality of Services
RADIUS	Remote Authentication Dial-In User Service
RC4	Ron's Code no.4
RFC	Request For Comments
RIP	Routing Information Protocol
RPC	Remote Procedure Call
RTSP	Real Time Streaming Protocol
RVA	Relative Virtual Address
SA	Security Association
SEH	Structured Exception Handling
SH	SHell skripty
SMC	Service control manager
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Manager Protocol
SP	Service Pack
SPT	SPanning Tree protocol
SSH	Secure SHell
SSID	Service Set IDentifier
SSL	Secure Sockets Layer
TACACS	Terminal Access Controller Access Control Systém
TCP	Transmission Control Protocol

TKIP	Temporal Key Integrity Protocol
TLS	Thread Local Storage
TLS	Transport Level Security
UDP	User Daragram Protocol
URL	Uniform Resource Locator
VBS	Visual Basic Scripts
VLAN	Virtual LAN
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VxD	Virtual device Drivers
WEP	Wired Equivalent Privacy
WLAN	Wireless Location Area Network
WPA	Wi-Fi Protected Access
WWW	World Wide Web
XML	eXtensible Markup Language
XSL	eXtensible Stylesheet Language

Obsah

Úvod

V posledních letech se stále častěji setkáváme s novými druhy IT kriminality. Klasické počítačové viry pomalu nahrazují nové, které mají za úkol ještě více škodit či jistým způsobem obohatit útočníka, čili autora škodlivého kódu. Tyto nové hrozby nám nepochybně přinesl nový fenomén posledních několika let, známý jako internet. Můžeme tedy již téměř zapomenout na viry, které se šířily po disketách či jiných multimédiích, přestože se stále vyskytují, nicméně nejsou tyto infekce hromadného charakteru a navíc jsou dnes snadnou záležitostí pro mnoho antivirových programů, které by již neměli chybět na žádném osobním počítači.

Jelikož malware (škodlivý software, program či kód) může nejvíce poškodit firmy či instituce, které jsou vnitřně protkány počítačovou sítí a napojeny na celosvětově přístupovou síť internet, je třeba se zabývat komplexnějším bezpečnostním systémem, který by již nezahrnoval pouze bezpečnostní software, ale byl by tvořen z několika bezpečnostních zón (hraniční směrovač, síťový firewall, systémy pro detekci průniku do sítě IDS a IPS, návnady (honeypots) atd.). Avšak pro plnohodnotné řešení zabezpečení firemní sítě je nutné nejprve porozumět možným útokům a hrozbám, které jsou v dnešních dobách a budou se vyskytovat nepochybně i v budoucnu. V této bakalářské práci jsou popsány principy šíření, infekce, maskování, útočné a obranné vlastnosti počítačových virů. Samozřejmě i tyto vlastnosti mají svůj vývoj a s postupem času se stávají více komplikovanější. Přispívá k tomu i dynamický růst softwarových produktů a evoluce operačních systémů. Přestože k pojmu moderní počítačový virus nelze přímo přiřadit nové verze malware, které mohou být dosti často ještě škodlivější, jsou uvedeny i tyto nové hrozby, čímž se myslí phishing, spam, 3Dspam, adware a spyware. I proti tomuto malware existuje celá řada bezpečnostních programů, které chrání své uživatele od nepříjemných problémů. Počítačovým sítím kromě škodlivých kódů hrozí také činnost crackerů, kteří neoprávněně vnikají do sítě, kde mohou získat cenné data či nějakým způsobem škodit.

V poslední době jsme svědky nového trendu síťových počítačových virů, které odborná veřejnost nazývá jako červi (angl. worms). Tyto škodlivé kódy zaznamenaly velký vzestup od roku 2004 a dnes jsou zodpovědné za nejrozšířenější útoky na uživatele internetu po celém světě. Lze tedy předpokládat, že vývoj počítačových virů na síťové úrovni se bude nadále rozšiřovat a je potřeba se zaměřit na dosud známé exploitace, spolu s hledáním zranitelných míst a připravovat se tak na nové druhy těchto červů, ačkoli předpokládat či předvídat nové typy útoků patří v tomto oboru za nejnáročnější, a proto se v dnešní době touto činností zabývá mnoho odborníků v těch největších světových IT firmách. Tyto firmy vyvíjejí komplexní bezpečnostní zařízení, které chrání sítě od linkové a síťové (průniky crackerů) až po aplikační vrstvu (viry, spamy a spyware). Příkladem může být např. zařízení Cisco ASA (adaptive security appliance), které sdružuje funkci aplikačního stavového firewallu, systému prevence průniku IPS, Antivirový software, spam a spyware moduly a VPN koncentrátory. Avšak je povinností každého dobrého administrátora, či správce sítě, ať už malé či větší organizace nebo firmy, sledovat nejnovější změny a trendy v bezpečnosti, což spočívá v implementaci nových bezpečnostních záplat a tak být připraven proti nejaktuálnějším virům či útokům na svou síť.

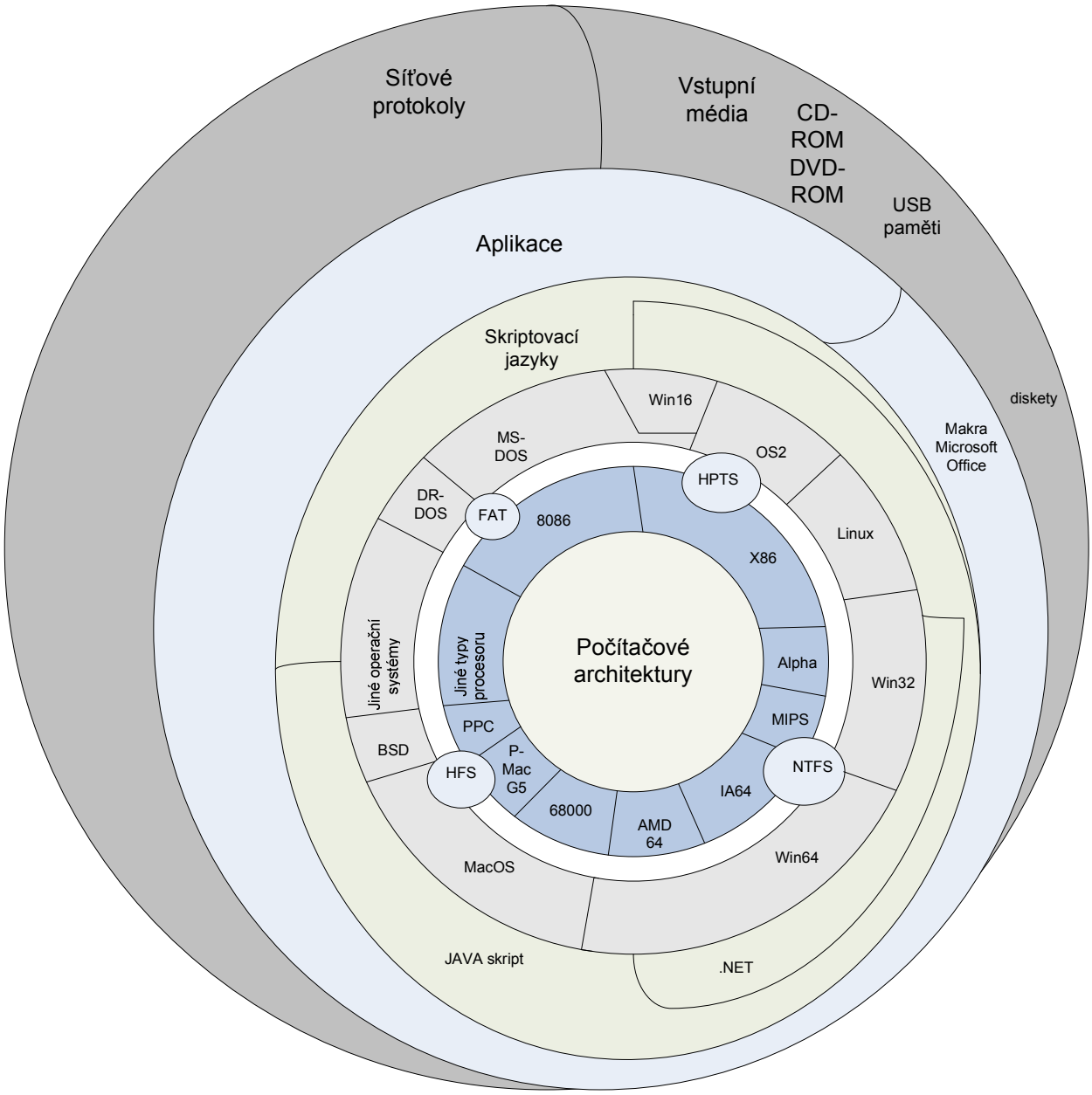
1 Analýza počítačových virů

Počítačové viry k dnešní podobě moderních poč.virů, prošly poměrně dlouhou evolucí. Za celou dobu svého vývoje přibývaly i nové trendy, které se přizpůsobovaly k novým technologiím a typům operačních systémů. Jelikož se operační systémy stávají více složitější a komplexnější, je pro autory virů o to větší výzvou, tyto systémy napadat. Škodlivý kód počítačového viru obvykle obsahuje tyto funkce: infiltrace (průnik do systému), infekce (napadení hostitele), útočné funkce (retro vlastnosti), obranné funkce (techniky stealth, polymorfismus), replikace a infekce (nákaza systému), payload (podepsaní či vizitka viru). V této kapitole budou popsány vlastnosti a techniky těchto funkcí, ale již novějších virů, které jsou hrozbou hlavně pro aktuální používané platformy (W32, W64, Mul, Linux, JS, W97M a jiné stále používané programy a operační systémy).

1.1 Infiltrace

Pod tímto pojmem si můžeme představit průnik škodlivého kódu do určitého systému. V podstatě tedy záleží o jaký systém se jedná, zda-li je pro virus hostinný či nehostinný. Funkce a životnost virů závisí hned na několik kritérií a prostředí: pc architektuře, procesoru, operačním systému, verze operačního systému, souborového systému, formátu souboru, překladači , HTML, času a datu, archivovaných formátech, příponách souboru, síťových protokolech, zdrojových kódech, atd. až po multiparitní viry, které však mají omezený rozsah své univerzálnosti.

Autoři virů se snaží o to, aby se jejich „umělecké dílo“ co nejvíce proslavilo a proto tedy se zaměřují na nejpoužívanější a nejrozšířenější typy prostředí. Z toho vyplývá, že se vyskytuje mnohem více virů na platformách IBM PC a jejich klonech, než-li například na Apple II. Dále také se nemá cenu příliš zabývat viry, které jsou funkční pouze v zastaralých operačních systémech a softwarech, ačkoliv některé staré viry dokáží „obživnout“ i na dnešních operačních systémech. Následující obr. 1.1 ukazuje působnost škodlivých kódů dle různých prostředí.



Obr. 1.1: infiltrace škodlivého kódu dle různých prostředí

1.1.1 Infiltrace v závislosti operačního systému

Infiltrace do prostředí WIN32

Zkratka platformy WIN32 značí viry napadající 32 bitové operační systémy(OS) Windows (Windows 9x, ME, NT, 2000 a XP na platformě x86). V tomto prostředí infikují soubory PE(portable executables-spustitelný formát souborů), které mají nejčastěji příponu exe. Formát souborů PE v těchto OS využívají binární programy, běžné systémové komponenty, aplikace, spořiče obrazovky, ovladače zařízení, nativní aplikace, dynamické knihovny a ovladače AktiveX.

Viry dále pro svojí infekci a replikaci používají API (Application Program Interface), tedy množinu funkcí operačních systémů Windows 9x a NT (včetně 2000, 2003, XP), díky kterých mohou pracovat s pamětí, vyhledávat a pracovat se soubory a adresáři.

Velmi populární se stal útok pomocí infektorů nativního kódu. Jelikož soubor PE je možné nahrát jako ovladač zařízení, konzolovou aplikaci či nativní aplikaci, může se pak nativní aplikace, jako je například autochk.exe, spouštět již v průběhu bootování, čímž nativní virus získává značný náskok k infekci v systému před odhalením bezpečnostními programy. Protože se spouští dříve než subsystémy, nemají k dispozici jejich knihovny DLL, jako například KERNEL32.DLL, ale mohou využít funkce nativní API z knihovny NTDLL.DLL, které mají mnoho funkcí pro práci se soubory a pamětí. Ukázka některých operací API, které nativní viry používají, jako například první virus tohoto druhu W32/Chiton z roku 2001:

RtlAllocateHeap()	- alokuje paměť
RtlFreeHeap()	- uvolní paměť
RtlSetCurrentDirectory_U()	- nastaví adresář
NtOpenFile()	- otevře soubor
NtCreateSection()	- vytvoří sekci

Některé viry dokáží napadat přímo soubory dynamických knihoven (DLL). Soubory DLL používají stejný systém uspořádání dat jako soubory portable executables (PE). Dynamické knihovny jsou navíc schopny exportu funkcí, které jsou použitelné dalšími aplikacemi. Rozhraní mezi aplikacemi a dynamickými knihovnami je zajištěno exportem z DLL a importem do spustitelných souborů, viz [3]. K zavěšení do knihoven využívají API connect() a send().

Infiltrace do prostředí WIN64

Pro nové 64 bitové architektury IA64, AMD64 a EM64T byl vytvořen i nový 64bitový formát spustitelných souborů PE+. Jeden z prvních virů, který se na této platformě vyskytl v březnu 2004, byl W64/Rugrat.3344 naprogramovaný v assembleru pro IA64, který používá malé množství funkcí Win64 API ze tří různých knihoven. Poté následoval virus W64/Shruggle, který již uměl infikovat soubory PE+ na architektuře procesorů AMD64, viz[3].

Infiltrace do prostředí UNIX a LINUX

Ani tyto poměrně bezpečné a spolehlivé systémy nejsou ušetřeny od útoků počítačových virů. Na rozdíl od prostředí OS W32 a W64, které používají formát souborů PE a PE+, používají nejčastěji formát ELF(kompatibilní pro 32bitové i pro 64bitové procesory), který nemá koncovku a identifikace probíhá dle interní struktury. Soubory ELF mají jen krátkou hlavičku a jsou dále rozděleny do logických sekcí. Většina virů na systémech Linux napadá právě tyto soubory. Viry jsou většinou jednoduché, jako je například vir Linux/Jac.8759, který může infikovat další soubory nacházející se pouze ve stejném adresáři jako virus. Zabezpečení pomocí udílení práv hraje v Linux a v Unix pro viry zásadní roli. Například rozmanitý virus {W32,Linux}/Simile.D nakazí v systému všechny soubory s povoleným právem zápisu.

Mezi nejnebezpečnější viry pro Linux a Unix jsou sofistikovaní počítačoví červi (například Linux/Slapper), kteří v kombinaci šíření po síťové vrstvě napadají i soubory ELF a

mohou k zvýšení své působnosti, tedy práv, dosáhnout exploitací síťových služeb a tak využít snadnějšího přístupu k binárním souborům, viz [3].

1.1.2 Infiltrace v závislosti na překladači programu

Infiltrace makro-virů Microsoft Office

Některé dnešní viry fungují jen díky programům ze sady Microsoft Office, a to zejména díky Microsoft Word, Microsoft Excel a Microsoft PowerPoint, které jsou dnes nejpoužívanější. Tyto viry nazýváme makro-viry, jelikož jsou založeny na makrech, které za normálních okolností usnadňují uživatelům Excelu, Wordu a PowerPointu práci. Protože makra ke své činnosti potřebují pracovat s daty dané aplikace, umějí tedy tyto data kopírovat a modifikovat a mohou tak zasahovat i do jiných dat na počítači. Makro, které je schopno zkopírovat sebe sama z jednoho dokumentu do druhého (tedy replikace), je označeno makro-virem.

K úspěšnému šíření makro-viru musí docházet k výměně dat(souborů typu *.doc, *.xls a *.ppt) včetně maker mezi jednotlivými uživateli a počítači. Proces šíření je však zcela omezen jazyky jednotlivých lokalizací. Například makro-virus pocházející z anglické verze použije v těle příkaz FileSave, ale např. španělská verze tohoto makro-viru by musela použít příkaz ArchivoGuardar. Pochopitelně jazyková odlišnost platí pro celé naprogramované tělo makra. Také některé příkazy mezi MSWord a MSExcel nejsou autentická a tak neumožňují kompatibilitu. Tyto omezení ale vynahrazuje skutečnost a sice,že Microsoft Office jsou komerčním softwarem, který může být používán na různých architekturách počítače (IBM PC, Macintosh, …) a taky na různých verzích operačního systému (W32, W64 a MacOs).

Makra a případné makro-viry se přenáší vždy v těle datového souboru *.doc či *.xls. Struktura těchto souborů, které Microsoft používá, je označena OLE2. Makra tedy vypadají jako streamy uvnitř dokumentu. Tento škodlivý kód je potom dobře ukryt hluboko v dokumentu a navíc se ještě dělí po 64 bajtech. Makro-viry se poté do nových souborů kopírují podle standardních kopírovacích příkazů, či mohu využít nějaký globální soubor např.NORMAL.DOT (pro MWord), ze kterého se zpětně kopíruje do dalších dokumentů.

Některé makro-viry používají pro vlastní potřebu volání funkcí API z Win32, čímž ale ztratí kompatibilitu se systémy Macintosh. Některé viry jako například {W32, W97M}/Heathen.12888 umí vystoupit z kontextu jako makro-virus a pomocí volaní API funkce CallBack12(),CallBack24() a CreateThread12() souboru KERNEL32.DLL se poté šíří jak v dokumentech, tak i ve spustitelných souborech, podrobněji v [2] a [3]. Trochu odlišným multiparitním virem je W32/Coke, který speciálně infikuje globální šablony pomocí malého zaváděcího kódu, čímž nahraje do globální šablony polymorfní kód makra v textovém souboru. Z toho plyne, že patří nejen pod skupinu polymorfních binárních virů, ale spadá i pod makro-viry. Jelikož jsou obecně polymorfní makro viry poměrně pomalé díky mnoha iteracím, ztrácejí tak na efektivitě své replikace. Ale protože vir Coke se generuje jako polymorfní makro-vir do textového souboru za použití Win32kódu, stává se z něj poměrně rychlejším polymorfním makro-virem, než prostí polymorfní makro-viry.

Dalším zajímavým jevem u makro-virů je jejich schopnost vývoje, či naopak degenerace. To je zapříčiněno především tím, jak makro-viry využívají ke své potřebě další sadu maker, které se nachází v patřičném dokumentu nebo si je prostě kradou z cizích dokumentů. Tímto potom můžou dosahovat nečekaného vývoje. Jestliže makra degenerují a tak ztrácejí funkci replikace, pak za touto skutečností stojí především jejich ztráta některých částí ze sady maker.

Speciálním druhem makro-virů jsou makra s rovnicemi (formula), které se neukládají spolu se standardními makry, ale Excel je uloží do prostoru pro makra Excelu 4. Mezi prvními viry tohoto druhu byl francouzský virus XF/Paix, viz [3].

Před lety ale Microsoft přišel s Office 2003, který umožňuje ukládat dokumenty v novém textovém formátu XML. Virus W32/Press využil myšlenku v proniknutí infekce do souboru XML za pomocí odkazu, který XML uchovává, na soubor XSL(Extensible Stylesheet Language) umístěný na webu, podrobněji v [3].

Infiltrace skriptovacích virů Visual Basic a Java

Tyto viry se rozšířili krátce po výskytu makro virů. Ke svému šíření využívají nejčastěji elektronickou poštu (e-maily). Modul Windows Script Host (nachází se v souboru WSCRIPT.EXE) umožňuje vykonávat VBScript (Visual Basic Scripts) a JScript (Java Scripts) a to podobně jednoduše, jako v případě klasických spustitelných souborů. Tyto soubory se používají k multimediálním aplikacím, které musí pracovat se širokou paletou příkazů a funkcí, tudíž není těžké vytvořit fungující skriptovací virus.

Jedním ze známých virů tohoto druhu je VBS/LoveLetter.A@mm, který obletěl svět již v roce 2000. Jestliže uživateli přišel elektronickou poštou tento virus, stačilo pak pouze kliknout na přílohu, která obsahovala dva soubory. První příloha obsahovala neškodný textový soubor a druhá příloha, soubor typu VBS, byla díky výchozímu nastavení systému Windows (skrýt příponu souborů známých typů) neviditelná, jelikož se naivně nepředpokládalo potenciální nebezpečí skriptovacího viru. Ten pak díky funkci Outlook MAPI a jeho následných příkazů CreateObjekt(“Outlook.Application“) a metodou NameSpace(“MAPI“), která sbírala příkazy pomocí AddressLists(), se zasílal (metodou send()) samovolně všem známým v seznamu uživatele.

VBS viry a JSkriptovací viry těží hlavně z rozsáhlé funkčnosti objektů ActiveX, které mají přístup k systémovým objektům a jiným aplikacím, které jsou spjaty s aplikacemi e-mail.

Velmi jednoduše můžeme předejít proti skriptovacím virům spuštěním zákazu jejich spouštění v nastavení prohlížeči. V dnešních moderních Java aplikacích se ale využívá digitálního podpisu autora aplikace, čímž se uživatel může rozhodnout, na základě vlastních zkušeností a také věrohodnosti autora, zda-li tuto aplikaci spustit nebo blokovat, čili nespouštět.

Další druhy infiltrace skriptovacích virů(SH,PHP,AplS a ActionSript)

Shell skripty (SH) jsou skriptovací jazyky, které používá většina systémů Unix. Používají se při instalací a dávkovém zpracování a proto je využívají i viry, které tak mohou aplikovat infekční techniky, jako přepisování souboru, nebo vložení na, před, či za programy. Známý červ SH/Reneto.A, který se objevil v roce 2004, využíval bash skript pro kopírování svého kódu do adresáře StartupItems na připojených discích systému Mac Os X, viz [3].

PHP hypertext preprocessor jsou otevřené skriptovací jazyky pod open source, které jsou určeny pro vytváření aplikací pro stránky html. Na rozdíl od JS tyto skripty neběží na klientském serveru, ale na domovském serveru. PHP viry mohou využít ke svému prospěchu tyto příkazy: fopen(), fread(), fputs(), fclose(), opendir(), readdir(), atd. Mezi známé PHP viry patří PHP/Caracula či PHP/Feast, který je navíc polymorfní a při šíření přepíše jiné soubory svým kódem vždy jinak sekvenčně sestavený.

Také na systému Macintosh existují skripty, které podporují lokální skriptování. AppleSkript není přímo standartní součástí systému Mac a proto se AplS viry tolik nešíří.

ActionScript se používá v aplikacích flash, který využívá rovněž dostatek funkcí potřebných k vytvoření funkčního viru.

1.1.3 Infiltrace dle jiných parametrů

Dle časových parametrů

Autor viru může dosti často do svého „díla“ vložit neprogramovanou podmínku, která bude spouštět a ukončovat činnost viru v jistém časovém rozmezí. Příkladem byl virus W32/Welchia, který konal činnost pouze do ledna 2004. Nebo například známý počítačový červ W32/CodeRed, byl aktivní pouze do roku 2001. Ale díky jeho úspěchu ho mnozí autoři pokusili modifikovat, tak že odstranili časové omezení, čímž dodali tomuto kódu neomezenou časovou působnost.

Dle archivovaných formátech

Některé viry umí napadat pouze archivované formáty ZIP,ARJ,RAR atd., přičemž ale většina virů dokáží primárně napadat nezkomprimované binární soubory. Útok na zkomprimované soubory se objevil náhle poté, co Microsoft přidal bezpečnostní záplaty do programu Microsoft Outlook. Tato modifikace nespouštěla spustitelné soubory, ale stále umožňovala stahovat, spouštět a posílat zkomprimované soubory, což využili autoři virů a vkládali své viry do archivovaných souborů ZIP pomocí hlavičky adresáře.

Dle síťového protokolu

V současnosti jde o nejnebezpečnější infiltraci. Protokoly TCP a UDP jsou využívány mobilním škodlivým kódem k útokům na nové cíle Internetu, viz [3]. Takové viry již označujeme jako červy. Tyto červy poté naslouchají na příslušných portech těchto protokolů a po přebrání řízení,vyhledávají nové cíle a poté se rychle replikují, čímž dosáhnou útoku DoS (Denial of Service-odmítnutí služby). K přebrání kontroly mohou využít exploit hlavičky MIME, která obecně načítá kód již při čtení nebo náhledu. Takhle se šířil například W32/Badtrans.B, nebo Win32/Bridex.

Naštěstí většina chyb v komunikačních službách, které byly zneužívány červy Win32/Blaster (nebo Win32/Lovsan) využívající bezpečnostní díru v DCOM RPC rozhraní, jsou dnes bezpečnostními záplatami odstraněny (př. SP1/SP2,SP3,SP4 pro Windows XP/2000). Nová rodina virů Stration/Warezov/Ramex se rozšiřuje nejen emailem, ale také odkazy přes ICQ, Skype a podobných instant messengerů.

Dle zdrojového kódu (Visual Basic,Visual Basic .NET, C , Pascal)

Tyto druhy škodlivých kódů potřebují ke svému šíření soubory vytvořené ve výše uvedených programových jazycích. Například W32/Subit umí infikovat zdrojové kódy VSB a VSB .NET.

Tyto viry se vytváří poměrně snadno. Tělo kódu základně obsahuje minimálně dvě funkce. První funkce vyhledává v prostoru disku další typové soubory (např. *.c) a druhou funkcí se virus infikuje do nalezeného souboru.

1.1.4 Infiltrace jiného druhu

Moderní počítačové viry směřují svoji působnost k těm nejpoužívanějším sdíleným prostředím a tím, je bezesporu internet. Budou se tedy šířit prostřednictvím sítě a k tomu vhodně využívat síťové protokoly a jejich bezpečnostní slabiny. Nejsofistikovanější z nich k obelstění kontroly integrity se nebudou nacházet na pevných discích, ale budou injektovat nové procesy v adresářových prostorech.

1.2 Metody Infekce

Tato sekce obsahuje popis různých metod, které viry po úspěšné infiltraci používají k přepisovaní, nebo nakažení různých formátů souborů či aplikací.

1.2.1 První typy infekce

Boot viry

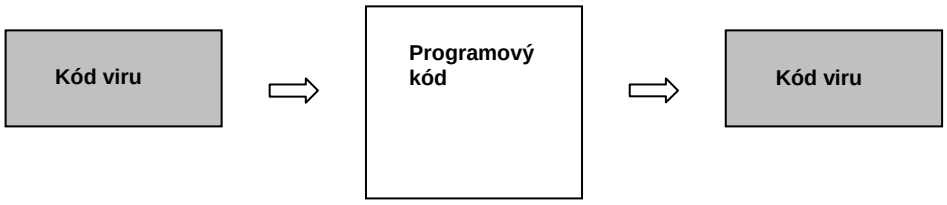
Tyto viry patří mezi nejstarší(virus Brain 1986). Na systém pronikly pomocí diskety a zneužily start operačního systému, který bootoval primárně z jednotky A: tedy disketové mechaniky, poté virus, který se nacházel na disketě, převzal kontrolu bootování a zkopíroval se do paměti na místo MBR(master boot record – zavaděč OS), který se ještě předtím přesune na jiné místo sektoru disku. Tuto techniku použil virus Stoned.

V dnešních dobách tyto viry jsou již minulostí, protože k zavedení operačního systému se nepoužívá disketa, která kdysi tyto viry vnášela do systému.

1.2.2 Techniky infekce obecných souborů

Přepisující technika(overwrite)

Jde o velice jednoduchou techniku infekce, která může však napáchat nejvíce škody, jelikož nakažené soubory či dokumenty jsou ve skutečnosti přepsány virovým kódem, budou původní data již zcela ztracena. Pokud virus najde vhodný soubor na diskovém prostoru, jednoduše ho pomocí přepisovacího příkazu nahradí vlastním souborem(obr 1.2).



Obr. 1.2: Virus přepíše tělo hostitele.

Tato dosti zákeřná metoda infekce je velmi nápadná, a proto ji používají spíše viry šířící se elektronickou poštou, čímž si zachovávají svoji replikaci. Nejznámějším virem byl VBS/LoveLetter.A@mm, který po infiltraci pomocí e-mailu na hostitelský počítač vyhledával soubory s příponami (.vbs, .vbe, .js, .jse, .css, .wsh, .sct, .hta, .jpg, .jpeg, .wav, .txt, .gif, .doc, .htm, .html, .xls, .ini, .bat, .com, .avi, .qt, .mpg, .mpeg, .cpp, .c, .h, .swf, .psd, .wri, .mp3, .mp2) a následně je přepsal svojí kopií. Před tímto skutečně ničivým procesem se stačil odeslat na adresy jiných emailů, které měl uživatel v adresáři.

Jinou škodlivou infekcí, je přepsání pouze počáteční části programového kódu souboru (obr 1.3). Po spuštění tohoto nakaženého souboru se virus znovu spustí a přepíše další soubor. Takto postupují malé viry o délce pár desítek bajtů. Jejich algoritmus musí být kvůli omezené délce jednodušší a je rozdělen do tří fází:

1.Nalezení vhodného souboru a to pouze v aktuálním adresáři
2.Otevřít soubor pro zápis
3 Zapsat kód viru na začátek nalezeného souboru

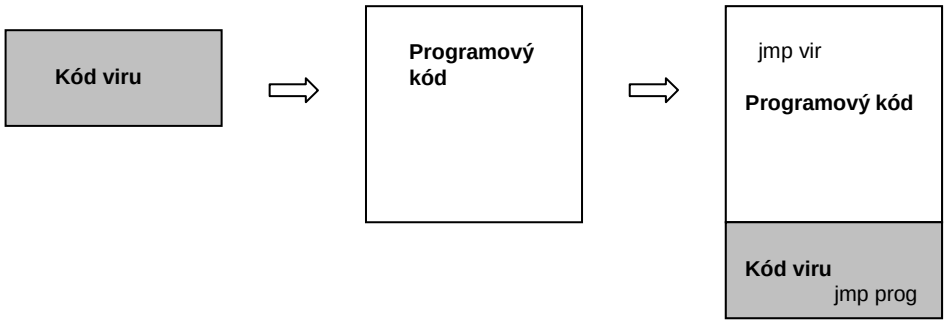
Obr. 1.3: Virus přepíše počátek hostitele.

Třetí méně obvyklou variantou je infekce náhodným přepsáním těla hostitele (obr 1.4). Virus si náhodně vybere oblast v programovém kódu hostitele a přepíše do dané oblasti svůj kód. Tímto původní kód znehodnotí a program může havarovat při spuštění.

Obr. 1.4: Virus náhodně přepíše hostitele.

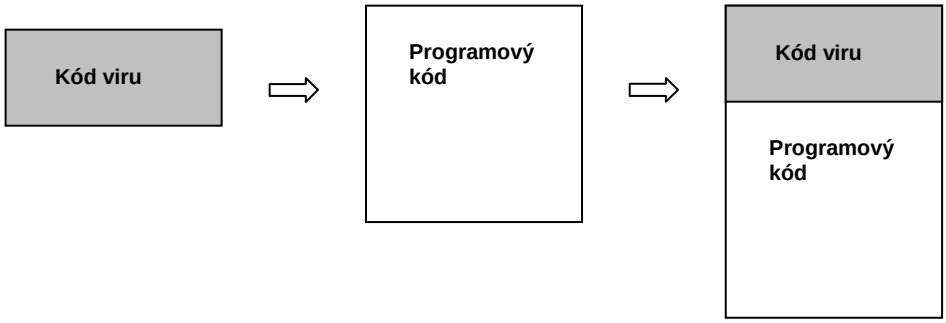
Připojující technika

Některé starší Dos viry se připojovali za hostitele(soubory COM) a pomocí vložení instrukce skoku JMP na začátek hostitele přebrali kontrolu, viz obr.1.5. Viry, které chtěli takto převzít kontrolu nad soubory EXE, je musely nejprve převést na soubory COM. Tato technika je použitelná pro formáty souborů EXE, NE, PE, ELF atd., které používají dosluhující operační systémy. Tyto soubory mají obvykle i hlavičky s metadaty o souboru, které virus vhodně využívá.



Obr. 1.5: Virus připojený za tělo programového kódu.

Častější technikou je však připojení těla škodlivého kódu na začátek hostitelského kódu. Tyto viry nazýváme Prependery, které se obvykle vytváří v programových jazycích C, Delphi nebo Pascal . Nejprve prepender vykoná svůj kód a pak předá řízení kódu hostitelskému programu, viz obr 1.6.



Obr. 1.6: virus (prepender)

Dutinová infekce

Tato technika infekce, stejně jako přepisující metoda, nemění velikost hostitele, ale virový kód si ke svému zápisu, do těla programového kódu, vybere bezpečné místo, které nezpůsobí havárii programu. Tato místa v kódu představují nuly a bloky 0xCC, což jsou zarovnávací znaky pro instrukce jazyka C. Navíc viry přidávají na začátek kódu hostitele skok (jmp) ukazující na začátek kódu viru a pak odskakují zpět na počátek programu hostitele (obr 1.7).

Známým virem využívající tuto metodu je Virus W32/Installer, který tak napadal PE soubory na Windows 2000.

Obr. 1.7: virus se vhodně přepsal do těla hostitele

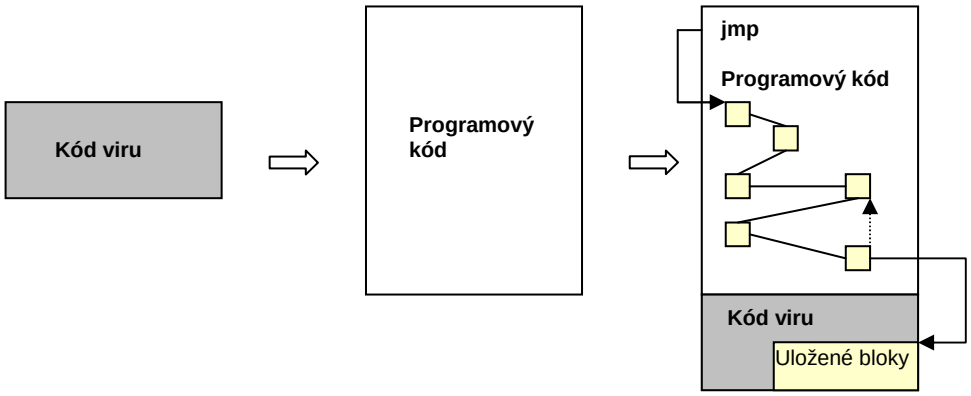
Viry jako W95/CIH využívají efektivnější metodu dutin, která spočívá v rozdělení viru na zaváděcí rutinu a určitý počet sekcí. Tyto části se pak zkopírují na různá bezpečná místa v těle kódu hostitelského programu. Podmínkou úspěšné infekce je dostatečná velikost volného místa pro uložení celého zavaděče. V souborech formátu PE jsou o mezerách údaje přímo v hlavičce sekcí.

Komprimující infekce

Viry, které tuto metodu používají, se nejprve přepíšou někam do volné dutiny hostitele, a potom binární komprimaci zmenší společný obsah. Virový kód si sebou přináší i dekompresor, čímž po infekci vrátí původní velikost napadeného souboru. Kompresní techniku používá virus W32/Redemption, který útočí na 32bitové PE soubory.

Technika přidání decryptoru

Tato metoda je o něco složitější než předcházející techniky. Spočívá ve vepsání tzv. decryptoru do těla hostitele, na který je přesměrován vstupní bod do programu. Decryptor, který je rozdělen na více části, začíná na náhodném úseku hostitelského programu a postupným kopírováním kousků těla hostitele vede až na počátek virového kódu, který tyto sekce hostitelského programu uchovává. Po spuštění takové infikované aplikace decryptor rozšifruje zašifrované tělo viru a předá mu řízení, a pak po další infekci předá řízení programovacího kódu, kterému postupně vrací uložené kousky kódu (obr 1.8). Příkladem této techniky je slovenský polymorfní virus One_Half.



Obr. 1.8: decryptor postupně šifruje tělo virového kódu

Ještě sofistikovanější je metoda, která využívá vložení decryptoru a virového těla přímo do těla hostitele. Přepsané bloky těla kódu hostitele kopíruje za jeho tělo kódu. K přístupu těchto částí se používá tabulka, kterou zná jen virus.

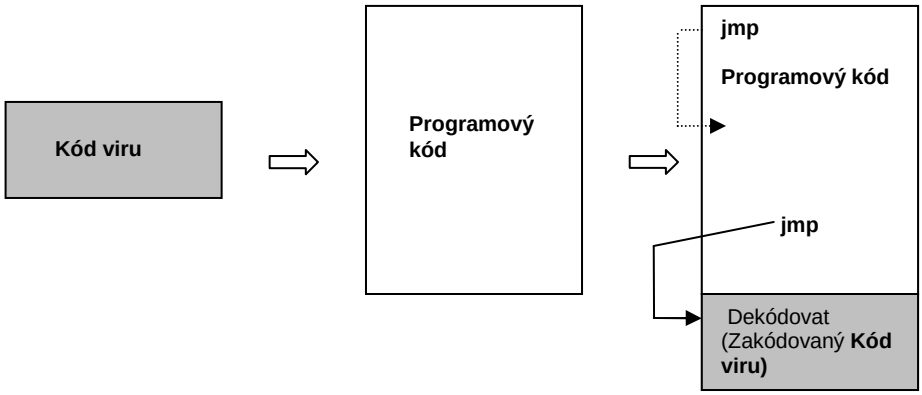
1.2.3 Technika infekce utajení vstupního bodu (EPO)

Technika EPO (EntryPoint Obscuring) utajení vstupního bodu se nesnaží měnit vstupní bod aplikace, ani kód viru, na který tento bod ukazuje. Pozměňuje, ale vnitřní kód hostitele tak, aby virus mohl převzít řízení v náhodný moment.

Základní EPO techniky infekce

Tuto techniku fungující pod DOSem využil virus Olivia v roce 1997. Ten infikuje soubory COM a EXE. Využívá k tomu vhodný okamžik(spuštění, přejmenování nebo změnu atribut). Nejdříve umaže jeho souborové atributy, pak ho otevře a analyzuje jeho strukturu. Hledá v něm vhodné instrukce typu(JMP, JMP short, NOP, CLC, STC, CLI STI, CLD a STD). Jestliže se mu podaří takovou instrukci najít, pak hledá na místě další takovou instrukci a pokud není umístěna v posledních 64 bajtech, virus jej přepíše na místě předešlé nalezené instrukce, viz [3].

Na obrázku 1.9 je vidět instrukce skoku JMP(ve vhodném místě v těle hostitele), která směřuje šipkou nakonec kódu programu, kde se nachází decryptor, který rozšifruje zakódovaný virus.



Obr. 1.9: DOSový EPO virus

Vylepšené EPO techniky infekce

U této velmi komplikované metody se viry nejprve zavěsí na obsluhu INT 1 (TRACE) pod DOSem. Takto pak trasují hostitelský program po prvních 256 instrukcí a zastaví se po maximálním počtu 2048 iterací. Pokud byla poslední trasovaná instrukce typu (CALL, JMP, ADD AL, …), pak tuto instrukci přepíší instrukcí CALL, která však směřuje na polymorfně zakódovaný virus. Tento postup prováděl virus Nexiv_Der, který napadal COM soubory a uměl infikovat i boot sektory.

EPO technika typu zavěšení na API volání ve Win32

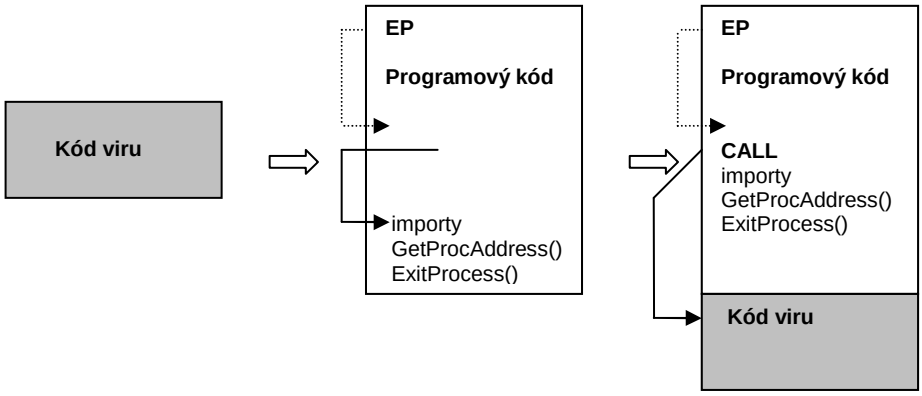
Systémy Win32 používají jako formát spustitelných souborů PE, který může být napaden pomocí přesměrování volání API. Win32 EPO viry totiž umějí vyhledávat instrukce CALL v kódové sekci hostitele a ty pak zařazují do adresáře importů. CALL instrukci pozmění tak, aby ukazovala na začátek virového kódu. Tělo viru se pak umísťuje například na konec souboru.

Oblíbené implementace volání API:

Od programů Microsoft	CALL DWORD PTR [ ]
Od Borlandu	JMP DWORD PTR [ ]

Některé viry čekají až na závěrečné volání API funkcí ExitProcess(), které volá každý PE soubor při svém ukončování (obr. 1.10). Virus se takto spolehlivě zavěsí na program,

který se již chtěl ukončit. Poté co virus vykoná svůj kód, spustí původní kód opravením přepsané funkce, viz [3].



Obr. 1.10: použití instrukce CALL volající kód viru

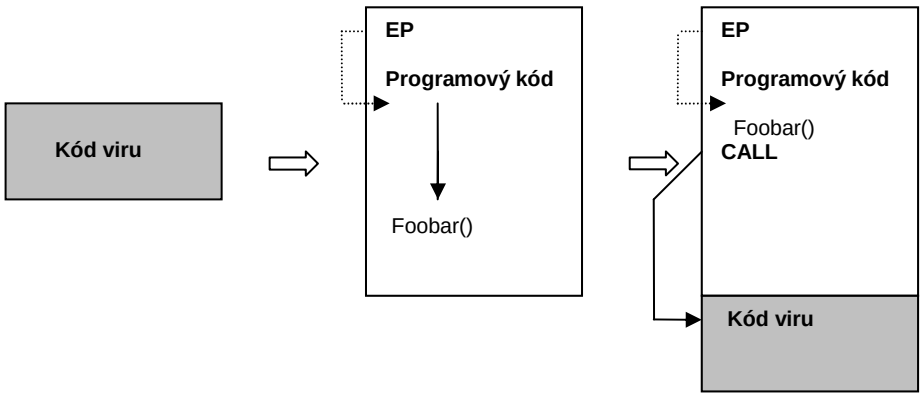
Spolehlivé využití funkcí Win32

Vyhledání v programovém kódu hostitele instrukci CALL, nemusí ještě znamenat, že tato instrukce volá funkci API, proto kód viru ještě provede kontrolu, zda-li se nejedná pouze o datovou část jiné funkce (tzn. Program instrukcí CALL volá nějakou svoji jinou funkci, např. podprogram). Aby měl virus jistotu, hledá v programu volání funkce Foobar (), na kterou tak zavěsí začátek svého škodlivého kódu. Funkce volání Foobar () začíná sekvencemi operačního kódu 0x55 0x89 0xE5.

```
CALL Foobar

Foobar:
PUSH EBP                                ;opkód 0x55
MOV EBP, ESP                            ; opkód 0x89E5
```

Takto se zavěšuje na program virus W32/RaingSong, viz obr 1.11.



Obr. 1.11: zavěšení na funkci Foobar()

1.2.4 Jiné využití instrukcí ve Win32

Tyto metody jsou již natolik sofistikované, že je dokáží využít jen ti nezdatnější autoři počítačových virů. Mezi známé metody, které se vyskytli jmenujme alespoň tyto:

Nahrazení tabulky importů(vstupů) ve Win32

Virus, který používá tuto techniku infekce, se nesnaží modifikovat či upravovat programový kód hostitelského souboru, ale pokouší se změnit adresy v tabulce importů hostitelského PE souboru. Pokud se po provedených změnách spustí hostitelský soubor a ve svém programovém kódu se pokusí zavolat nějakou funkci API, zavolá ve skutečnosti adresu směřující na tělo virového kódu, který je alokovaný někde ve volném paměťovém prostoru.

Použití „neznámých" vstupních bodů

Tato technika spočívá v tom, že kód viru se aktivuje po volaní nějaké méně známe funkci. Virus se zavěsí na hostitelský kód pomocí TLS entry point(vstupní bod thread local storage). Toto lokální úložiště toků načítá při spouštění souboru zavaděč v hlavičce PE ještě před spuštěním obvyklého vstupního bodu (který obvykle viry používají) PE.OptionalHeader.AddressOfEntryPoint.

Integrování kódu

Tato metoda je prozatím nejnáročnější technika infekce. Spočívá ve smíchání kódů programu hostitele a škodlivého kódu za použití EPO technik. Nejprve však virus musí hostitelský kód zdisassemblovat, což je pro paměť velká výpočetní zátěž. Pak se virus integruje do kódu hostitele tak, aby nenarušil celkovou funkčnost obou kódů. A následně se zase musí takto smíchaný kód zpětně zreassemblovat. Navíc se musí relokovat kódové a datové sekce hostitelského programu. Virové skenery musejí pak navíc hledat vstupní bod ukazující na polymorfní a metamorfní kód viru, který navíc může využít decryptor libovolně uložený v těle hostitele.

Tuto techniku zvládl jeden z největších autorů virů, ruský autor s nickem Zombie a jeho výtvor byl označen jako W95/Zmist.

Budoucí techniky infekce

Jedná se o metody založené na decryptorech a metod integrace do hostitele. Vir by se však neintegroval způsobem smíchání svého kódu s kódem hostitele, ale využíval by některé sady instrukcí, funkcí a podprogramů z hostitelova kódu, ze kterých by se pak sám sestavil. Tyto viry by se budovali přímo z kódu napadeného programu. Takový virus pak dokáže infikovat pouze vhodný soubor s potřebnou sadou instrukcí.

1.2.5 Techniky infekce souborů PE

V předchozích sekcí byli rozebrány techniky infekce obecných souborů, kde se již vyskytli i příklady infekce souborů formátu PE(portable executable). Tato podkapitola bude zaměřena přímo na soubory formátu PE, které viry infikují nejvíce.

Rozbor formátu PE

Tento formát souboru vytvořil Microsoft a implementoval ho poprvé ve Windows 95. Svojí strukturou se podobá unixovému formátu COFF. PE pracuje primárně s aplikacemi Win32, které volá pomocí instrukcí ze sady funkcí API Win32. Formáty PE se používají ve všech následujících operačních systémech Windows (Windows 9x, Windows 2000, Windows 2003 Server, Windows XP). S novými hardwarovými platformami (32bitů bylo rozšířeno na 64bitů) se Win32 rozšířilo na Win64 a formát PE se jen rozšířil na PE+. Kvůli kompatibilitě jsou obě sady API téměř stejné.

Základní položky formátu PE
-DOS stub
-hlavička
-tabulka sekcí
-tabulka importů
-tabulka exportů

Struktura formátu PE:

MS-DOS MZ hlavička
MS-DOSový stub
Signatura PE souboru
Povinná hlavička PE souboru
Nepovinná hlavička PE souboru
hlavička sekce.text
hlavička sekce.data
hlavička sekce.rsrc
hlavička sekce.reloc
hlavička sekce.debug
….
sekce.text
sekce.data
sekce.rsrc
sekce.reloc
….
sekce.debug

DOS stub

Starý DOS program, který roubuje jiné části kódu. Zobrazuje výpis chybové hlášky (This program cannot be run in DOS mode). V PE formátu tento program zůstal jen kvůli kompatibilitě.

Struktura hlavičky PE

Je rozdělena na povinné záhlaví a obsahuje také nepovinné atributy.
Zde jsou uvedeny atributy, které viry používají. První dvě atributy patří do povinné hlavičky, zbytek patří do nepovinné hlavičky:

-NumberOfSections

Počet sekcí v EXE(DLL) souboru. Pokud virus se infikuje na novou sekci, musí zvýšit tuto hodnotu.

-Charakteristic

Některé viry v té položce ověřují jaký má soubor příznak, zda-li je typu EXE či DLL. Některé hledají soubory EXE a některé pro změnu pouze knihovny DLL.

-SizeOfCode

Obsahuje zaokrouhlený údaj o velikosti všech sekcí, tedy celého kódu. Dobrý virus by měl tento údaj při infekci zvýšit, ale ve většině případů se tak neděje.

-AddressOfEntryPoint

Adresa, na které začíná spustitelný kód. Je vyjádřena relativně (RVA – Relative Virtual Address) a směřuje na první sekci textu. Oblíbená položka virů, kteří tak na sebe přesměrují vstupní bod.

-ImageBase

Při spuštění PE souboru je obraz zaveden linkerem na místo v paměti, které je specifikováno právě virtuální adresou, uvedenou v ImageBase. U programů Microsoft jde o hodnotu 0x400000. Viry používají tento údaj pro přesné vypočítání pozice některých prvků.

-SectionAlignment

Jedná se o zarovnání sekce v paměti. Každá sekce PE souboru začíná v paměti na virtuální adrese, která je násobkem tohoto atributu. Obvykle jde o 64 KB (0x10000). Viry používají tento údaj pro odvození vhodného místa pro uložení vlastního těla.

-FileAlignment

Jde o zarovnání sekce v souboru. Vlastní data souboru začínají na násobcích této hodnoty.

-SizeOfImage

Velikost modulu PE souboru v paměti, zaokrouhlena nahoru na nejbližší násobek SectionAlignment. Tuto hodnotu potřebuje linker pro zavedení částí souboru do paměti. Nesprávný hodnota po infekci souboru způsobí, že virus nebude schopen provozu pod Windows NT. Operační systém řady Windows 9x/Me totiž tuto hodnotu narozdíl od NT nekontroluje

-Checksum

Atributa kontrolní součet bývá v řadě případů prázdný. Infekce PE souborů je navíc usnadněna tím, že Windows 9x/Me tento atribut také nekontroluje.

Tabulka sekcí

Leží mezi hlavičkou PE a samotnými daty. Obsahuje informace o každé sekci (jméno sekce, velikost a umístění surových dat - raw dat). Jednotlivé sekce se používají k oddělení různých typů dat, jako například spustitelný kód, data, globální data, ladící informace, relace a podobně. Viry buďto přidávají novou sekci, nebo zvětší již vytvořenou sekci. Potom tedy musí přepsat i údaje, které právě uchovávají tyto hlavičky sekcí uloženy v tabulce sekcí. Zajímají je hlavně tyto položky:

-VirtualSize – Virtuální velikost sekce před zaokrouhlení podle FileAlignment.
-SizeOfRawData - Velikost sekce po zaokrouhlení podle FileAlignment.
-Characteristic -Uchovává příznaky, které popisují vlastnosti dané sekce: Readable (čitelná), writeable (zapisovatelná), code (kód), data.

Tabulka importů IAT

Pomocí tabulky importů IAT (Import address table) může většina virů infikovat soubor PE, tím že zamění adresu volaní API funkce za adresu počátku svého kódu. PE soubor tabulku používá k volání funkcí z příslušných knihoven DLL. Tabulka obsahuje jména importovaných DLL knihoven a jména importovaných funkcí z těchto knihoven. Mezi známé knihovny například patří ADVAPI32.DLL či KERNEL32.DLL. Používané importy jsou zaznamenané v sekci .date.

Může se stát, že aplikace nezná adresu na potřebnou API. Proto musí použít příkaz API LoadLibrary() a GetProcAddress(), kde z potřebné knihovny již najde příslušnou adresu.

U formátu souboru PE+, který se používá u 64bitových pc architekturách, se liší obsluha tabulky importů. Zde se namísto tabulky IAT používá PLABEL_DESCRIPTOR.

Tabulka exportů

Opačná funkce importu. Soubor formátu PE, nejčastěji jde o nějakou knihovnu DLL, zapisuje informace o exportovaných funkcích do sekce .edata. Například tabulka exportů KERNEL32.DLL se sestavuje ze struktury IMAGE_EXPORT_DIRECTORY, která uchovává tři různé tabulky:adresy funkcí, jejich jména a ordinální hodnoty.

Některé viry těží z toho, že použijí funkci GetProcAddress, kterou naleznou v druhé tabulce ze struktury IMAGE_EXPORT_DIRECTORY u KERNEL.DLL, k získání jiných API adres.

Infekce hlavičky PE

Tuto techniku mohou použít jen viry s krátkým kódem. Umístí se mezi konec hlavičky PE za tabulku sekcí a začátek první sekce. Musí modifikovat atribut AddressOfEntryPoint v PE hlavičce tak, aby neukazovala na první sekci ale na vstupní bod kódu viru. Tyto viry musí být menší než FileAlignment.

Infekce na začátek souboru PE

Tím že virus přepíše začátek souboru, například první tři datové sekce, poškodí tím soubor PE, který se již nespustí. Proto tuto metodu viry W95 nepoužívají. Viry HLL (high level language - C, Pascal) nakazí soubor PE a ten se pak spouští s EXE hlavičkou viru. Při

vracení řízení původnímu programu, musí virus zpětně vyextrahovat původní kód do dočasného souboru a pak ho spustit.

Infekce na konec souboru PE

Virus se zapíše do poslední sekce, kterou upraví tak, aby se do ní vešel. Musí tedy pozměnit položky VirtualSize, SizeOfRawData a upravit AddressOfEntryPoint. Nepřepisuje položku NumberOfSection (počet sekcí). Musí jen přepočítat údaje položky SizeOfImage. Příkladem může být virus W95/Anxiety.1358.

Některé viry nemění atributu AddressOfEntryPoint, ale přebírají řízení jinak. Výpočtem určí adresu vstupního bodu hostitele souboru PE a na tuto adresu připíšou instrukci JMP (jump-skoč), kterou odskočí na vlastní kód. Takové viry musí ale maskovat relokační záznamy, které do této oblasti kódu ukazují, jako například virus W32/Cabanas. Protože instrukce JMP by vzhledem k relokačním záznamům neměla být první v kódu, virus W95/Matburg umístí JMP až za blok náhodného smetí(nějaké zarovnávací znaky v kódu).

Infekce do dělených dutin

Tato infekce počítá s prázdnými místy v různých sekcí v souboru PE. Linker tyto mezery vyplňuje nulami nebo 0xCC. Prázdné místa vznikají následkem násobku souborového zarovnání. V tom také spočívá rozdíl raw-dat v souboru a dat alokovaných při spuštění ve virtuální paměti. Velikost prázdného místa je pak menší než 512 Bajtů. Proto se virus jednoduše rozděluje do prázdných míst různých sektorů. K jednotlivým blokům přiřazuje instrukce odskoků na další následující bloky kódu. Soubor po infekci nezvětší svou velikost. Tuto metodu používá virus W95/CIH, který většina veřejnosti zná pod jménem Černobyl.

Infekce VxD

VxD – Virtual device drivers (virtuální ovladač řízení), tento modul může přebírat řízení nad souborovým systémem. Virus Navrhar se například ukrývá v souboru formátu OLE2(např. .doc od MSWord), kde je na jeho konci ukryt jako infektor makro-viru, s použitím API volaní, které si stáhne importací knihovny KERNEL32.DLL, se spustí a poté infikuje známé ovladače VxD v jeho seznamu. Hned po restartování PC má jako VxD řízení a čeká na otevření dalšího dokumentu, který pak využije ke svému šíření. Virů tohoto druhu příliš mnoho není. Ale vzhledem k tomu, že PE soubory se mezi uživateli nešíří tolik, jako soubory DOC (například jako přílohy v e-mailu), lze očekávat že podobné metody infekce se budou rozvíjet tímto směrem.

1.2.6 Infekce paměťově rezidentních virů

Tyto viry se inicializují v paměti a existují jako aplikace, která žije svým škodlivým životem.

1. Vyhrazení místa v paměti pro svůj vlastní kód.
2. Přemístění kódu do daného místa.
3. Aktivace kódu.
4. Zavěšení kódu.
5. Infekce nových souborů či systémových oblastí.

Tyto techniky infekce jsou známé už v DOSovém prostředí, kde běžela vždy pouze jedna úloha „thread“. Kde virus používal k přebrání řízení nějakou instrukci přerušení IVT(Interrupt Vector Table-tabulka vektoru přerušení) typu INT ID. Tyto viry používali mnoho zavěšovacích technik, ale patří do minulosti a nebudou dále rozebírány.

U novějších operačních systémů Windows se tyto rezidentní viry již tolik neprosazují. Za prvé jsou snadným terčem antivirových skenerů. Za druhé je může samotný uživatel odhalit pomocí nástroje Správce úloh systému Windows v záložce Procesy. Tyto viry používají jinou strategii viz. 1.2.7.

Dočasně paměťové rezidentní viry

Tyto viry zůstávají v paměti po určitý čas nebo po dobu výskytu nějaké události. Událostí se může myslet například překročení naprogramovaného limitu infikovaných souborů.

1.2.7 Infekce v uživatelském režimu

Již dlouhou dobu operační systémy podporují multitasking. Multitasking je označení pro děj, kdy operační systém vykonává v jedné době více procesů. Jednotlivé procesy odebírají pro svou činnost část operační paměti. Obecně bývá paměťový prostor rozdělen na bezpečnostní okruhy. U nových operačních systémů se navíc odděluje paměť pro aplikace běžící v jádru samotného operačního systému,ovladačů a bezpečnostní datové struktury od aplikací pro uživatelské aplikace. Viry pak využívají různých již zmíněných metod, které využije infiltraci do paměti.

Viry v procesech(uživatelském režimu):

- mohou běžet jako svůj vlastní proces. Nevýhoda je snadné odhalení.
- se načítají s infikovaným procesem(např. WINWORD.EXE) jako podproces, získá řízení a v samotném procesu vytvoří thread, který běží v uživatelském režimu a infikuje soubory za pomoci technik přímé akce.
- se načítá ještě před infikovaným kódem hostitele a díky dočasného souboru na disku a jeho spuštěním infikuje další soubory a poté předá řízení zpět hostitelskému souboru.
- mohou být i rezidentní(per-process resident), kdy se zavěšují v uživatelském režimu na vhodné funkce API a tím se rozmnožit při jejich volání hostitelem.
- mohou být ve formě virové knihovny .DLL, kterou používá hostitelský proces.

1.2.8 Infekce v režimu jádra

Windows 9x/Me

Některé viry dokáží infikovat režim jádra tím, že se zavěsí na souborový systém pomocí VxD (ovladače W9x pro režim jádra) API IFSMgr_InstallFileSystemApiHook(), viz [3]. Některé viry mohou také používat funkce režimu jádra voláním skrze bránu(„call gate“). Známý vir Černobyl W95/CIH po přístupu do režimu jádra přepisoval Flash Biosu tak, že poškodil hardware.

Windows NT/2000/XP

První virus, který je paměťově rezidentní v režimu jádra ve formě ovladače, se nazývá Infis a je proveden základně ve dvou verzí (jedna verze napadá Windows NT, druhá verze Windows 2000). Takový virus pak disponuje velkým potenciálem a může s využitím různých obsluh přerušení infikovat jakýkoliv soubor. Jelikož takový virus zůstává v paměti jako ovladač pro režim jádra a zavěšuje se na hlavní obslužné přerušení NT systému INT 2Eh (systémové volání) takovým způsobem, že se dovede infikovat kdykoliv, jestliže se za běhu otevře nějaký soubor, podrobněji v [2], [3].

Virus Infis se po infekci extrahuje jako samotný ovladač INF.SYS a používá vhodný klíč potřebný pro načtení sebe jako ovladače po dalším restartu OS. Tento klíč, který má uschovaný každý ovladač v registrech, vyžaduje SMC (service control manager – správce řízení služeb), aby mohl daný ovladač po restartu načíst. Tímto pak po restartování systému Infis získá kontrolu a přepíše IDT (tabulka deskriptorů přerušení), tak že převezme řízení před funkcí KiSystemService() a tím i zachytí každé otevření souboru, viz [3]. Pak stačí už jen porovnat, zda-li se jedná o soubor PE s vhodnou příponou.

1.3 Obranné vlastnosti počítačových virů

Autoři virů pochopitelně přidávají do kódů svých virů mnohé vlastnosti a programové rutiny, které viry používají k oklamání uživatelů, antivirových softwarů a bezpečnostních opatření operačních systémů.

1.3.1 Techniky tunelovaní

Tuto techniku využívali především starší paměťově rezidentní viry. V podstatě jde o to, že virus se zavěsí na první článek volání, čímž obejde ostatní rezidentní aplikace, a tím v podstatě antivirový monitorovací program. K nalezení počátečních vstupních bodů původní obsluhy přerušení používali viry tyto druhy technik.

Skenovaní v paměti původní obsluhy

Tato technika byla používaná v DOS. Viry prohledávali fyzickou paměť, kde hledali krátký sled instrukcí začátku původní obsluhy přerušení např. INT 21h. Po získání adresy INT 21h se mohl zavěsit na toto přerušení. Většinou umístil na začátek rutiny INT 21h instrukci skoku JMP s odkazem na vstupní bod kódu viru.

Trasování pomocí ladícího rozhraní

Viry postupně trasovali cestu v ladícím rozhraní pomocí neškodného přerušení INT 1 a pokud narazí na příslušnou obsluhu např. INT 21h, uloží si adresu této obsluhy.

Využití emulátoru

Bezpečnější tunelovaní spočívá v používání emulátoru kódu, který simuluje chovaní procesoru. Tato technika je založena podobně jako trasovaní. Výhodou je, že vir nemusí používat poněkud složité ladící rozhraní.

Použití nedokumentovaných funkcí

Viry využívají k přístupu k původní obsluze nezdokumentované funkce volaní API, které nemusí znát příslušné antivirové systémy. Pokouší se získat seznam těchto volaní a pak je využít k zavěšení na původní obsluhu.

1.3.2 Techniky stealth

Tyto techniky používají všechny sofistikovanější viry. Takové viry se snaží různými modifikacemi a postrkováním falešných dat maskovat svoji přítomnost v systému. V systému se spouští různé kontrolní funkce, které stealth vir odposlouchává a vrací jim vhodně upravená data. Většina těchto technik byla využívána v systémech DOS a na OS typu W32 a W64 se již téměř nepoužívá.

Semi-stealth

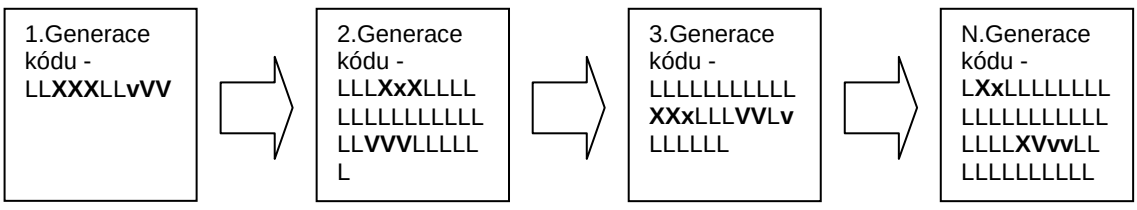
Tato technika spočívá v utajení velikosti infikovaného souboru. Vir tedy vrací hodnotu původní velikosti souboru. Aby se tento rezidentní virus nedostal do dezorientace a nezmenšoval velikost i nenakaženého souboru, musí proto přiřadit nakaženému souboru určitý příznak.

Tyto techniky adresářového stealth se v dnešních systémech příliš nepoužívají, protože si uživatel běžně nepamatuje přesné velikosti souborů či aplikací a taky se v používaných zobrazení tyto údaje často ani nezobrazují. Přesto tuto techniku použil například virus W32/Cabanas s kombinací zavěšení na tabulku importovaných adres IAT, ze kterých si stáhl adresy vhodných funkcí API.

1.3.3 Polymorfismus

Jedná se o maskovací techniku. Viry využívají změny decryptoru do velkého počtu odlišných instancí, které mohou mít až miliony různých forem, za pomocí zanášení tzv. datového smetí, což bývají většinou nepoužívané a nic neprovádějící instrukce, nebo nefunkční podprogramy. Takový virus měl pak bezpočet podob a klasickými srovnávacími metodami ho nebylo možné zachytit.

Tyto viry si zachovávají konstantní kód těla, které se mění v každé generaci na jinou podobu, čímž jsou moderními technikami poměrně dobře dekódovány a odhaleny. Na ilustrativním obr. 1.12 je vidět, jak je různě ke virovému kódu zanášeno datové smetí (znak L) a jak jednotlivá instrukce kódu (znaky X,x,v a V) může měnit své pořadí či pozici.



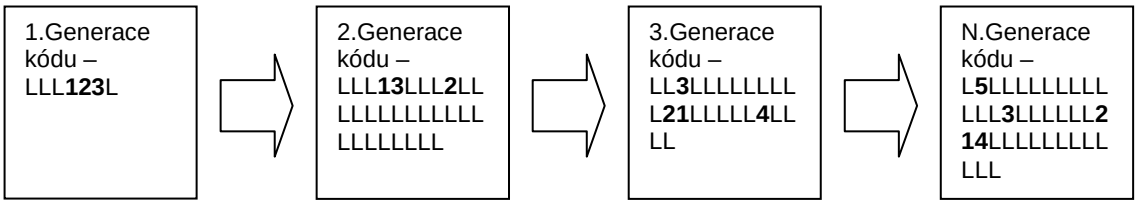
Obr. 1.12: Ukázka jak kód viru mění v jednotlivých generací svůj decryptor

1.3.4 Metamorfismus

Jde o další stupeň maskování virových kódů. Tyto viry vkládají do svých těl datové smetí a nové ekvivalentní instrukce, čímž v každých dalších generací mění svoji strukturu i tvar. Dokonce s využití skoků (JMP) mění svoje pořadí instrukcí tzv. permutační technikou. Tímto se stávají větším problémem pro bezpečnostní programy.

Na metamorfní engine se objevil také sofistikovaný virový kód pod označením W32/Evol, který nejen že mění svoji podobu a k tomu přidává smetí, čímž mění svůj tvar, ale dokáže měnit i DWORD hodnoty(SizeOfCode, SectionAlignment, atd.) používané v PE formátu souborů (obr. 1.13).

Kombinace polymorfních a metamorfních technik je hodně využívaná, kdy virus jako W95/Zmist náhodně používá přídavný polymorfní decryptor. Navíc kombinací utajení vstupního bodu EPO a metamorfnosti se stává dokonale utajeným virem pro heuristickou analýzu.



Obr. 1.13: Ukázka jak se kód viru mění v pořadí a v množství datových instrukcí

1.3.5 Obrana proti disassemblování

Virus se může proti disassemblovaní bránit několika způsoby. Tyto techniky jsou většinou založeny zakódování, polymorfismu, metamorfismu či matení kódu.

Zakódování dat

Mezi nejjednodušší techniky patří jednoduché zakódování dat v těle viru. V těle viru se pomocí nějakého kódovacího klíče zakódují všechny datové konstanty. Takto byl zakódovaný červ W95/Fix2001, aby neprozradil emailovou adresu útočníka, na který virus odesílal ukradené přihlašovací hesla a loginy.

Matení kódu

Další metodou proti disassemblovaní je matení kódu takovým způsobem, aby kód působil zmateně, a tím vyřadili heuristické analyzátory. Virus má ve svém kódu zaneseny například instrukce skoků, které mají nechat analyzátor skákat sem a tam, a tím ho dezorientovat.

1.3.6 Obrana proti ladění

Mnohé antivirové skenery a monitorovací systémy používají k odhalení virů ladění debuggerem, kterým trasují(krokují) kód viru na aplikační úrovni. Útočníci za dlouhá léta

vymysleli mnoho triků a technik k obraně proti této metodě analýzy. Mnohé tyto metody bývají dnešními lepšími debuggeremi prolomeny, a proto je nemá cenu zmiňovat.

Generování výjimek

Vir, který využije této techniky k oklamání debuggeru na aplikační úrovni, se jednoduše zavěsí na INT 0, která generuje výjimku dělení nulou a spouští instrukci jako „obsluhu“. Příkladem může být vir W95/SST.951.

Některé jiné viry používají vyvolání výjimky INT 3 na 32Win. Takto se poté spustí obsluha s volajícím API s ID funkcemi a parametry předanými na zásobníku.

Vypínání klávesnice

K trasování kódu se používá klávesnice. Virus pak musí zjistit, zda-li právě běží debugger. Tuto skutečnost zjistí dle těchto třech základních metod:

- použije API funkci IsDebuggerPresent(), po vracení hodnoty TRUE virus ví že debugger běží na aplikační úrovni
- hledání v klíčích registru pro detekci debuggeru
- detekce debuggeru přes seznam ovladačů nebo skenování paměti

Pak už stačí viru přednastavit obsah vhodného I/O portu a zablokovat klávesnici.

Matoucí souborové formáty a vstupní body

Některé debuggery nejsou zvyklé na nestandardní vstupní body uvnitř souborů formátu PE. Jestliže virus po infekci změní vstupní bod na nějaký alternativní, pak debugger při ladění tohoto souboru zhavaruje.

1.3.7 Obrana proti emulaci

Emulátor se obecně považuje za nejsilnější článek antivirového skeneru. Proto se autoři virů snaží uspět i v této fázi skenování a vymýšlí nejrůznější techniky k obelstění emulátoru.

Obsluha výjimek(SEH)

Virus nastavuje obsluhu výjimek tak, aby uvedl emulátor do pasti, za předpokladu že emulátor danou výjimku neumí obsloužit. Takto se snažil virus W95/Champ.5447.B setřást skener. Moderní viry dnes používají náhodné bloky smetí k vyvolání výjimky, což nemusí emulátor zaznamenat, jelikož by tak vznikali časté falešné poplachy.

Použití přerušení

Virus W95/Darkmil ve svém polymorfním decryptoru volá přerušení typu INT 2Bh, INT 08h, atd., čímž se emulace zastaví. Většina polymorfně zakódovaných virů nepoužívá přerušení až do chvíle úplného rozkódování.

Ostatní techniky

Pochopitelně obranných technik proti emulátorů je více. Některé zanikli vlivem neustálého zlepšování antivirových emulátorů. Některé techniky se snaží pouze emulátory zpomalit, za použití nějakého složitějšího zakódování a podobně.

1.3.8 Obrana proti heuristické analýze

Heuristická analýza má obecně za úkol detekovat nové existující varianty virů a existuje ve dvou módech (statická a dynamická). Statická heuristika obecně analyzuje fragmenty kódu těla viru a zkoumá souborový formát. Dynamická heuristika spočívá ve využití uzavřeného virtuálního prostředí, kde tedy simuluje činnost procesoru a operačního systému, do kterého nechá emulovat zkoumaný kód a detekuje podezřelé operace.

První generace heuristiky byla založena na statické analýze. Ta rozeznávala podezřelé struktury uvnitř PE souborů. Tato metoda zpočátku fungovala velmi úspěšně. Autoři virů vymysleli mnoho technik, které byli již naznačeny při rozboru infekce souborů PE, jako například:

- technika zatajení vstupního bodu
- infekce první sekce posunutím zbylých sekcí
- technika připojení na začátek hostitele a modifikace jeho hlavičky
- náhodný výběr vstupního bodu v kódové sekci
- využití prázdného místa díky zarovnání kompilátoru

Se známými technikami se nové viry jen těžko prosadí, a proto jejich autoři musí přicházet na nové, aby dokázali moderní heuristické analýzy překonat.

Nepoužívání API funkcí

Jedná se o velmi efektivní obranu proti heuristice a disassemblování. Tuto metodu používá mnoho moderních virů, jako například W32/Dengue. Tím že se vyhnou používání importů jmen API funkcí, které používají k práci se soubory např. OpenFile(), WriteFile(), a podobně, stávají se méně nápadnými pro heuristickou analýzu. Ale místo řetězců (jmen) používají jejich kontrolní součty, které se přepočítávají v tabulce exportů jednotlivých DLL knihoven.

1.3.9 Jiné obranné mechanismy

Mezi známé triky odchytávání virů je jejich nalákání na návnadu. Návnada je obecně jakýkoliv typový soubor, ze kterého lze snadno oddělit tělo viru od zbytku kódu a analyzovat jeho kód. Obvykle tyto soubory obsahují nic nedělající instrukce NOP a vrací činnost operačnímu systému bez zvláštní činnosti a bývají obvykle malé velikosti. Pro vyhýbání se návnadám musí kód viru obsahovat pár jednoduchých analytických rutin. Například bude v kódu infekce podmínka na nenapadání(nepřepisování) podezřele malých souborů s větším počtem instrukcí NOP a tak dále.

1.4 Útočné vlastnosti virů

Tyto vlastnosti viry používají proti nejčastěji největšímu protivníku v operačnímu systému. Jde pochopitelně o antivirové programy, monitory podezřelého chování (behavior - blockers), osobní firewally a jiné bezpečnostní programy.

Pro viry, kterým takto nestačí pouze defenzivní mechanizmy, se našlo označení retroviry.

Agresivní retroviry

Jelikož většina uživatelů Win32 a Win64 pracuje pod administrátorským právem, mají tyto viry značnou výhodu v útočení proti bezpečnostním systémům. Mezi tyto nejběžnější útoky patří:

-Vypnutí nebo odstranění antivirového programu z paměti či z disku.
-Vypnutí nebo obejití monitoru podezřelého chování (behavior - blocker).
-Vypnutí nebo odstranění osobního firewallu.
-Odstranění souborů ověřující integritu dat.
-Modifikace souborů ověřující integritu dat.
-Nasazení trojského koně do AV databáze.
-Blokování stahování nových AV aktualizací a databází.

1.5 Projevy virů

Projevy virů tzv. payloady značí jednoduše charakteristiku projevení či chovaní viru po jejich aktivaci. Dnes můžeme narazit na nejrůznější typy aktivačních rutin počítačových virů a na různé typy aktivačních událostí.
Mezi nejčastější typy aktivačních událostí patří:

-systémové datum nebo čas
-datové razítko souboru
-jméno souboru
-standardní nastavení systémového jazyka
-návštěva určité stránky
-IP adresa systému

Viry bez projevu

Tyto málo časté viry, bývají většinou ukryty v hostitelskému systému a nijak vědomě neohrožují, tedy nezasahují do systému, či nemažou data, a také na sebe neupozorňují různými výpisy či zobrazeními. Tyto viry se jednoduše pouze množí v hostitelském systému a mohou poškodit uživatele pouze při nechtěném zapříčinění pádu systému, kdy uživatel ztratí data v aktuálních otevřených prací. Tímto virem byl například WM/Koncept.

Nedestruktivní projev

Podle výzkumů, asi polovina virů patří do této kategorie. Tyto viry nemažou soubory a nijak nepoškozují systém. Pouze obtěžují uživatele různými aktivačními rutinami, jako například výpis zpráv, zobrazování různých multimediálních útvarů(obrázky, hry, spořiče obrazovky, hudební nahrávky - mp3 wav atd.). Jistě tyto viry jsou nežádoucí a otravné, ale pořád to není nejhorší.

Destruktivní projev

Jde o dost zákeřný útok počítačového viru. Tyto viry pak ničí data dle způsobů:

-Příležitostná destrukce dat. Takový virus útočí a ničí data s jistým omezením. Mezi tyto omezení patří například datum nebo jméno souboru. Nebo viry pouze modifikují určitý soubor.

-Totální destrukce dat. Tyto viry mažou přímo soubory z disku. V krajních případech formátují celé disky.

-Šifrování dat. Tyto viry uměly šifrovat data pomocích jednoduchých či složitějších šifrovacích metod. Například virus W32/Crypto byl jedním z posledních virů, které tento payload používali.

-Destrukce hardware. Další velmi nepříjemná záležitost a pro mnohé asi tou nejhorší možnost projevu viru. Takové viry se snaží přepisovat kód zavaděče pro BIOS a nastavit nebo-li taktovat, a tím přetížit procesor až k jeho zničení. Známým virem, který má tyto dovednosti, byl již zmiňovaný „Černobyl“ W95/CIH.

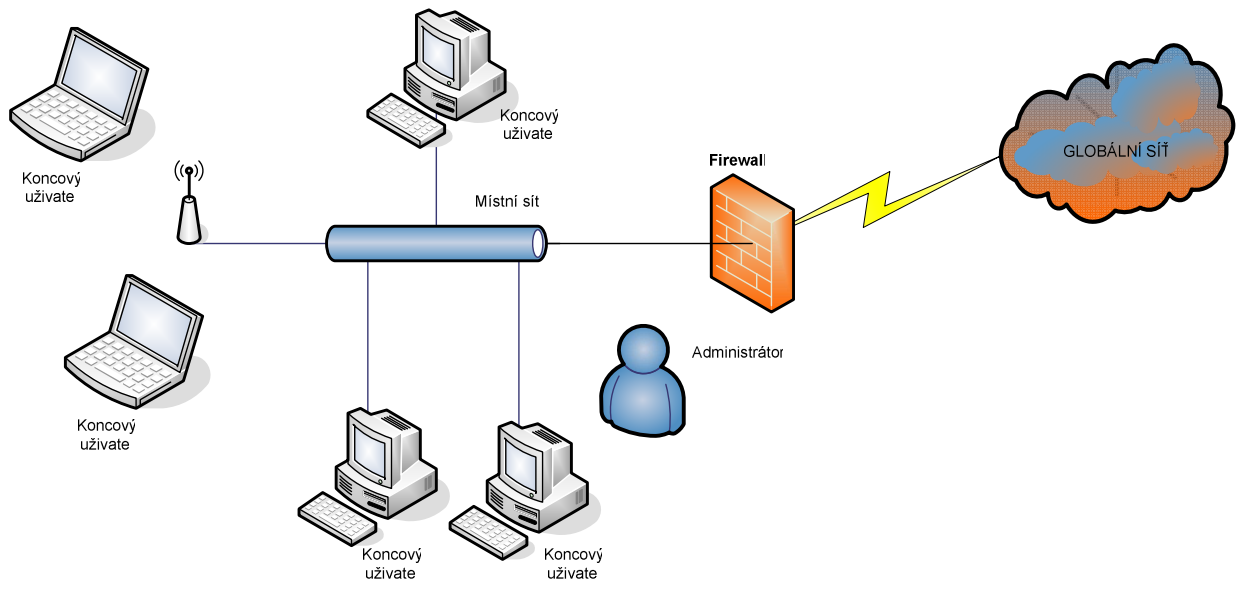
Útoky na počítačové sítě

Tyto útoky jsou jedny z nejaktuálnějších problémů dnešních dnů, co se týče této problematiky. Jde o útoky pomocí virů, které nazýváme počítačové červy. Počítačový červi mají většinou v povaze se šířit po celé síti na síťové vrstvě ve formě paketů, čímž snadno dokáží cíleně zahltit jakoukoliv síť. Tyto útoky mohou být směrovány náhodně, nebo z jistých důvodů. Například z politických důvodů, nebo dokonce z důvodů průmyslových „války konkurencí“, ačkoliv toto tvrzení by se mohlo mnoho lidem zdát jako konspirační.

Útok na DoS spočívá ve využití bezpečnostních slabin serverů či routerů, čímž se konkrétní síť pod těmito útoky přetížila tak, že začala zahazovat většinu paketů. Takto se projevil například virus W32/Slammer, který dokázal rozesílat pakety takovou rychlostí, že docházelo k výpadkům sítí ATM a v některých lokací sítí až na 90 % ztrátovost dat. Dalším slavným červem byl například W32/CodeRed, který útočil na stránky www.whitehouse.gov neustálým připojováním, čímž byli nuceni správci tohoto serveru rychle změnit svoji IP adresu, více o nových červech [11].

2 Vlastní návrh zabezpečení osobního počítače koncového uživatele (Terminálu)

Dobrý návrh zabezpečení PC koncového uživatele spočívá v ideální kombinaci ekonomických a kvalitativních faktorů. V dnešním světě je počítačová bezpečnost dat velkým obchodem a na trhu existuje velká konkurence. Každý osobní počítač by měl mít v dnešních dobách alespoň osobní firewall a základní antivirový program. Tato věc je drtivé většině uživatelů zcela známá. V mnoha případech se ale stane, že osobní počítač využívají i osoby, které postrádají základní informace o počítačové bezpečnosti. Toto je klasický případ různých firem či institucí, kde PC využívají ke své činnosti i právě tyto osoby. Z toho důvodu se na koncové terminály běžně zavádějí různé přístupové práva. Čili za bezpečnost dat na terminálu zodpovídá právě administrátor, často přímo správce počítačové sítě, který paušálně nastavuje zabezpečovací software na všechny terminály v počítačové síti, nebo na přiřazený úsek dané sítě, kterou má ve své kompetenci. Politika přístupových práv je samozřejmě velmi rozmanitá. Obecně tedy považujme administrátora za osobu, která má právo zasahovat a konfigurovat software na jednom či skupině terminálů, tedy PC vyskytující se v dané síti (obr. 2.1).

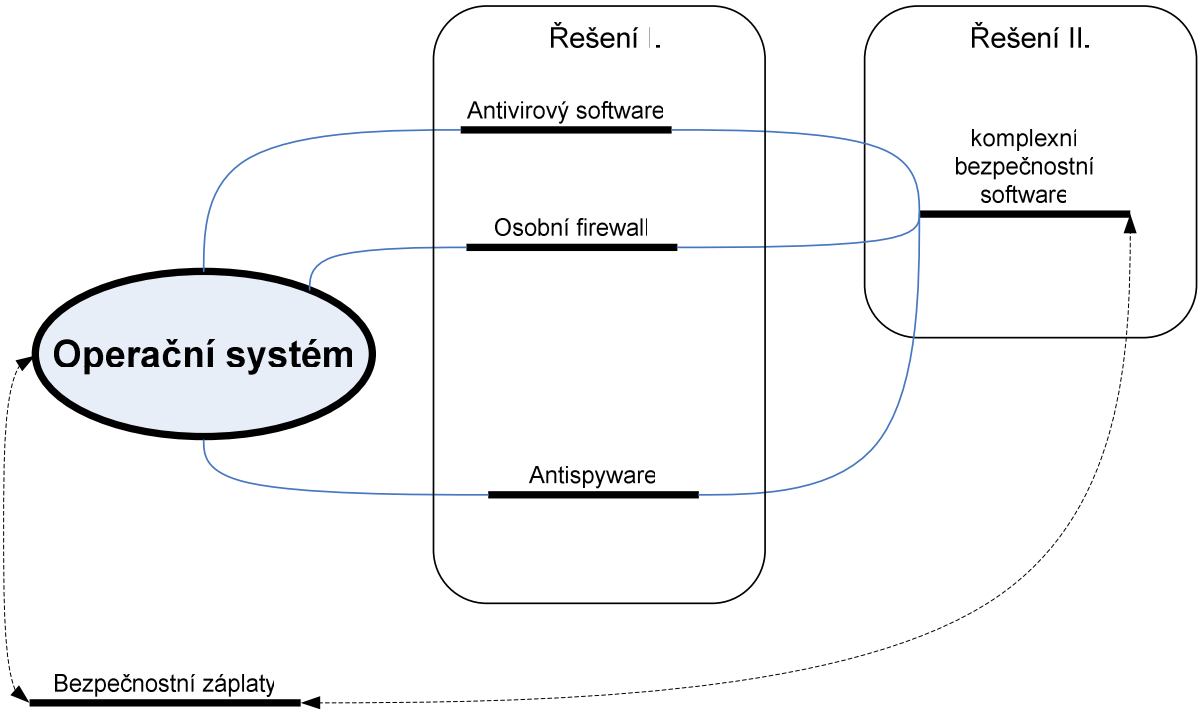


Obr. 2.1: obecné zapojení počítačové sítě

Práce administrátora, krom jiných činností, spočívá v bezpečnostní konfiguraci jednotlivých terminálů tj. osobních počítačů, které slouží koncovému uživateli či přímo administrátoru. Ve firemních sítích či sítích různých institucí nemá obvykle běžný uživatel práva k instalaci software a k různým modifikacím zasahující do systému, a proto veškerá práce na instalování software a nastavení zabezpečení zbývá na pověřené osoby s dostatečnými právy. V tomto návrhu bude tedy uveden postup a nezbytný software pro dobré zabezpečení koncového uživatele. Dále bude vedeno několik podpůrných programů a metod, které by měl mít administrátor v zásobě při případném selhaní bezpečnostních rutin a software, a jak by měl postupovat při léčení po napadení systému virem či červem.

2.1 Základní schéma základního zabezpečovacího software na terminálu

Základní kostra nezbytného software, která je zobrazena obr. 2.2, by neměla chybět na žádném počítači v síti. Tento návrh se zaměří na řešení I., které bude složeno z jednotlivých segmentů. Budou předvedeny jeho výhody a jeho nevýhody vůči řešení II., které spočívá v komplexní sdružení těchto základních bezpečnostních programů. V případě Antispyware však jde spíše o nadstandardní software, který se pomalu začíná prosazovat díky zvýšené aktivitě nevyžádaných reklam a jiných exploitů do uživatelského systému.



Obr. 2.2: základní prvky zabezpečení terminálu koncového uživatele

2.1.1 Výhody a nevýhody jednotlivých řešení I. a II.

Řešení I.

Tento návrh umožňuje rozmanitou kombinaci jednotlivých software a bude dále podrobně rozebrán, jelikož je levnější a tudíž perspektivní a hlavně snadno dostupný pro testovaní. Vhodnou kombinací a využití od každé skupiny bezpečnostního software toho nejoptimálnějšího programu či produktu lze dosáhnout občas kvalitnějšího zabezpečení, než nabízí některé levnější druhy komplexního bezpečnostního software.

Mezi jeho nevýhody však patří větší náročnost na údržbu a aktualizování jednotlivých programů, je tedy dosti komplikované implementovat a obsluhovat toto nastavení u většího počtu terminálů. Proto je toto řešení více vhodné pro počítačové sítě s menším počtem terminálů. Mezi další negativní vlastnosti lze zařadit fakt, že některé programy se v málo případech navzájem nedomluví na kontrole a nebo jsou někdy druhým programem zakazovány. Příkladem může být, jak některý Antispyware zakazuje aktualizace bezpečnostních záplat pro Windows XP.

V podstatě je toto řešení nejvhodnější pro jednotlivé uživatele zejména domácností, které svoji obranu mohou tímto způsobem poskládat ze freeware-programů, čili si zabezpečit osobní počítač zadarmo a to poměrně efektivně, nebo si některý software zaplatit např.

antivirový program, či využít jeho trial verze . Dále je vhodné pro menší firmy či instituce, které mohou toto řešení skombinovat s finančně výhodnými multilicenčními antivirovými balíčky s některými freeware firewally. Nebo využít jiných kombinací. Vše je jen otázkou financí, a také záleží na velikosti firmy či instituce, kde se výhodnost jednotlivých kombinací velmi liší.

+ nízká cena
+ možnost vlastního sestavení té nejvhodnější kombinace

- náročná obsluha a zdlouhavá konfigurace a nastavení

= vhodné pro jednoho uživatele či malý počet terminálů v síti (malé firmy a instituce)

Řešení II.

Komplexní ochrany sdružují více funkcí do jednoho softwarového balíčku, který bývá za nemalou cenu určen především větším firmám či institucí. Tyto balíčky bývají také často s narůstajícím počtem terminálů tzn. s větší objednávkou poskytovány za výhodnější ceny. Administrátor má pak jednotnou čili usnadněnou konfiguraci na všech terminálech. Dnes asi mezi nejznámější produkty patří Norton Internet Security, McAfee Internet Security Suite, AVG Internet Security aj. Většina těchto firem svým zákazníkům poskytuje také kompletní servis a nabízí nové bezpečnostní záplaty a aktualizace.

+ snadná konfigurace a rychlá implementace
+ jednotná kompletní integrita obrany
+ vše v jednom

- vysoká cena
- případné paušální selhaní všech terminálů

= vhodné pro větší počet terminálů v síti (větší firmy a instituce)

2.2 Antivirový software

Výběr vhodného antivirového programu je při dnešní pestré nabídce od nejrůznějších firem velmi variabilní. Pro obsluhu například domácí osobního počítače, tedy jednoho terminálu se zcela určitě doporučuje bezplatný AV software (trial verze či free verze, která nese základní funkce a má značná omezení). V případě uživatele, který pracuje s hodnotnými daty, by bylo však vhodnější přemýšlet o kvalitnějším antivirovém software a volba by padla na placený program z výběru některých předních značek softwarových výrobců AV programů. Uživatel má usnadněný výběr dle aktuálních testů těchto produktů například na internetu, kde své výsledky publikuje anglický časopis Virus Bulletin (www.virusbtn.com), který patří mezi nejuznávanější.

.

2.2.1 Antivirový program a jeho základní vlastnosti

Výhodou AVP od známých firem bývá kvalitní zpracování tohoto software, usnadněná obsluha, velmi časté aktualizace nových bezpečnostních dat, moderní techniky detekcí a dezinfekcí, a také odborné poradenství a veřejná diskusní fóra pro své zákazníky, viz [16]. Nevýhodou je pak pouze cena, a ta dnes u většiny uživatelů hraje hlavní roli. Uživatel by se

proto měl rozmyslet, jakou cenu je schopný zaplatit, a zda-li se mu to vyplatí v závislosti na důležitosti a hodnotě dat, se kterými pracuje. V následujících sekcích budou rozebrány určité vlastnosti těchto moderních antivirových programů, které obvykle mají i své stinné stránky. Ve výsledku budou uvedeny jednotlivé základní vlastnosti, a jaké by měli mít ideální parametry.

Detekce

Jestliže si zakoupíme antivirový program, máme plné právo očekávat, že náš AV software je schopen detekovat 100% známých virů. Otázkou však zůstává, do jaké míry bude detekce úspěšná při výskytu nového druhu počítačového viru. Kvalitní heuristická analýza je tedy velkou výhodou. Otázkou je, jak bude detekce adaptivní na nové a neznámé škodlivé kódy.

Rychlost skenovaní

Využití streamů pod NTFS znamená i několikrát rychlejší skenování. Jde tedy o vhodnou kombinaci s kontrolou integrity, která urychlí každé další nové skenování. Nevýhodou je, že připojení streamu ke každému souboru na disku nemusí každému uživateli vyhovovat, a taky musí být předpoklad, že systém byl na 100 % „čistý“. Dále rychlost skenování závisí na vytíženosti CPU, tím pádem se stává nepřímo úměrná k požadavku na náročnost na systém(hardware).

Standardní interval stahovaní aktualizací

Čím častěji tím lépe. Toto nemusí být vždy pravda. Záleží především na pružnosti a kvalitní podpoře od výrobce a na hodnotě aktualizovaných informací. Včasná aktualizace vůči novým infiltrací je v dnešní době podstatná.

Možnost kontroly při zavádění OS

Dobré AV programy by měli umožňovat kontroly při zavádění OS, které nejsou ovlivněny případnou infekcí. A tím včas zamezit dalšímu šíření počítačového viru.

Paketový skener

Jedná se o prevenci vůči narušení. V dnešní době rozmachu počítačových červů se tato funkce přidává již do většiny AV software.

Transparentní kontrola POP3, IMAP, SMTP, HTTP, NNTP

Rovněž nezbytná ochrana proti různým trojanům a počítačovým červům. Antivirová kontrola pošty v případě protokolů IMAP, SMTP a POP3, bez ohledu na použitý poštovní program, je vítanou vlastností.

Náročnost na systém

Antivirové programy by neměli příliš zatěžovat systém a tím omezovat práci uživatele. Mezi negativní projevy bývají rychlost CPU při skenování a pomalejší přístup k disku.
Ovládání a vzhled

Uživatelské prostředí by mělo být přehledné a ovládání by mělo být jasné. Popřípadě by měl uživatel mít možnost na výběr s obvyklých módů ovládacích funkcí a parametrů, které bývají rozděleny pro začátečníky, pokročilé a případně experty s plnou možností ovládání.

Další doplňkové vlastnosti

Samozřejmě se dnes snaží přidávat výrobci AVP do svých programů i další funkce, a tím více konkurovat jiným softwarům. Mezi tyto funkce patří moduly pro detekci aktivních rootkitů, hlídání významných částí registrů, antispam, antispyware a adware, osobní firewall a další. Tyto funkce se v různých kombinací a v různém množství implementují do antivirového programu, tak aby uživatelům zvýšili komfort. Samozřejmě tím roste i prodejní cena. Software, který sdružuje většinou těchto funkcí se nazývá komplexní bezpečnostní software (Internet security).

2.3 Komplexní bezpečnostní software (AVP, osobní firewall, Antispyware, atd.)

Produkty tohoto typu přináší pohodlné komplexní zabezpečení osobního počítače uživatele. Nevýhoda je, jak už bylo zmíněno větší finanční náročnost. Uživatel by měl očekávat kromě perfektních vlastností antivirového programu i tyto přídavné funkce:

Osobní firewall (Personal firewall)

Dobrý osobní firewall by měl mít co nejmenší požadavky na uživatele. Měl by se dynamicky přizpůsobovat a korektně rozeznávat aktuální nebezpečí na rozdíl od funkcí využívané uživatelem.

Antispyware, kontrola rootkitů a adware

Všechny tyto nevyžádané infiltrace by měl program dokonale detekovat a po rozhodnutí uživatele případně odstranit.

Antispam

Jedná se o odstranění nevyžádané pošty, která je hromadně rozesílána globální sítí (internet). V dnešní době jde o komplexnější řešení. Takový antispamový filtr pracuje s obsahem e-mailu a na základě známých signatur (např. viagra, atd.) ze slovníku a mezinárodních databází. Poté pomocí speciálních modulů by měl skenovat i přílohy (obrázky, texty a jiné informační podměty), ve kterých bývá často spam vložen. Moderním trendem jsou 3D spamy, které znesnadňují detekci tím, že sdělení v podobě obrázku je zobrazeno prostorově. Text je tak v podstatě zdeformován a rozpoznávání písmen (textu) je ze strany antispamových modulů daleko komplikovanější. Dále se přidává i "šum" na pozadí (různé čárky, tečky, jednoduchý vzorek...), podrobněji v [12].

Detekce rootkitů a kontrola známých knihoven

Tato vlastnost dokáže odhalit různé techniky stealth a podobně, které používá všemožný typ sofistikovaného malware.

2.4 Software osobního firewallu

Osobních firewallů je dnes k dispozici celá řada. Existuje hodně kvalitních freeware verzí, stejně tak i jako přídavné firewally, které jsou jako součást AV programu, či případně jako u řešení II., tedy situace, kdy máme firewall již jako součást programového balíčku (internet security). Některé free verze bývají jen zkušební a jsou omezeny určitou dobou(několik dnů) používání nebo bývají časově neomezeny, ale jejich některé funkce, často větší část z nastavení, bývají přístupné jen v plné verzi, která je již za poplatek (prodejní cenu).

2.4.1 Personal firewall 4 (Sunbelt/Kerio)

Tento firewall bude použit v první řadě v případě řešení I. Jedná se o nejpopulárnější firewall a bývá zcela doporučován hlavně pro začátečníky, tak i pokročilé, neboť při instalaci se uživatel rozhodne, jaký základní režim(mód) chce používat. Tyto režimy lze poté také měnit. Další výhodou tohoto programu je, že je kompletně v češtině. Mezi nevýhody patří, že free verze je omezena na 30 dnů od instalace. Administrátor ocení možnost zamčení nastavení firewallu díky loginu a hesla, které by měl k dispozici a tím koncovému uživateli znemožní měnit nastavení.

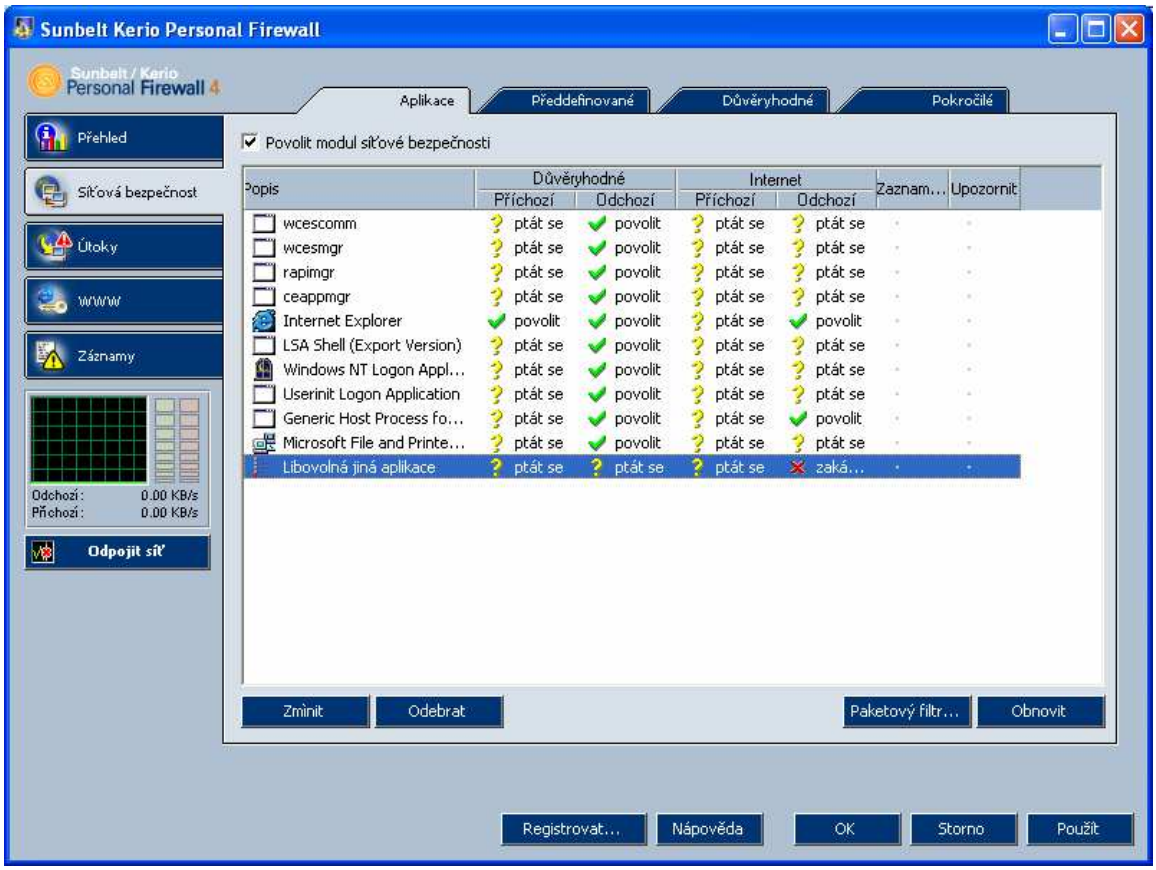
Módy

Simple (no popup mode- bez ptaní)
Firewall automaticky povoluje veškerou komunikaci z terminálu, čili komunikaci inicializovanou většinou uživatelem a blokuje veškerou příchozí komunikaci, pracuje podle výchozích pravidel uložených v nastavení firewallu. Výhodou je, že program nevyrušuje častými dotazy pro blokování či povolení aplikace. Vhodné pro začátečníky.

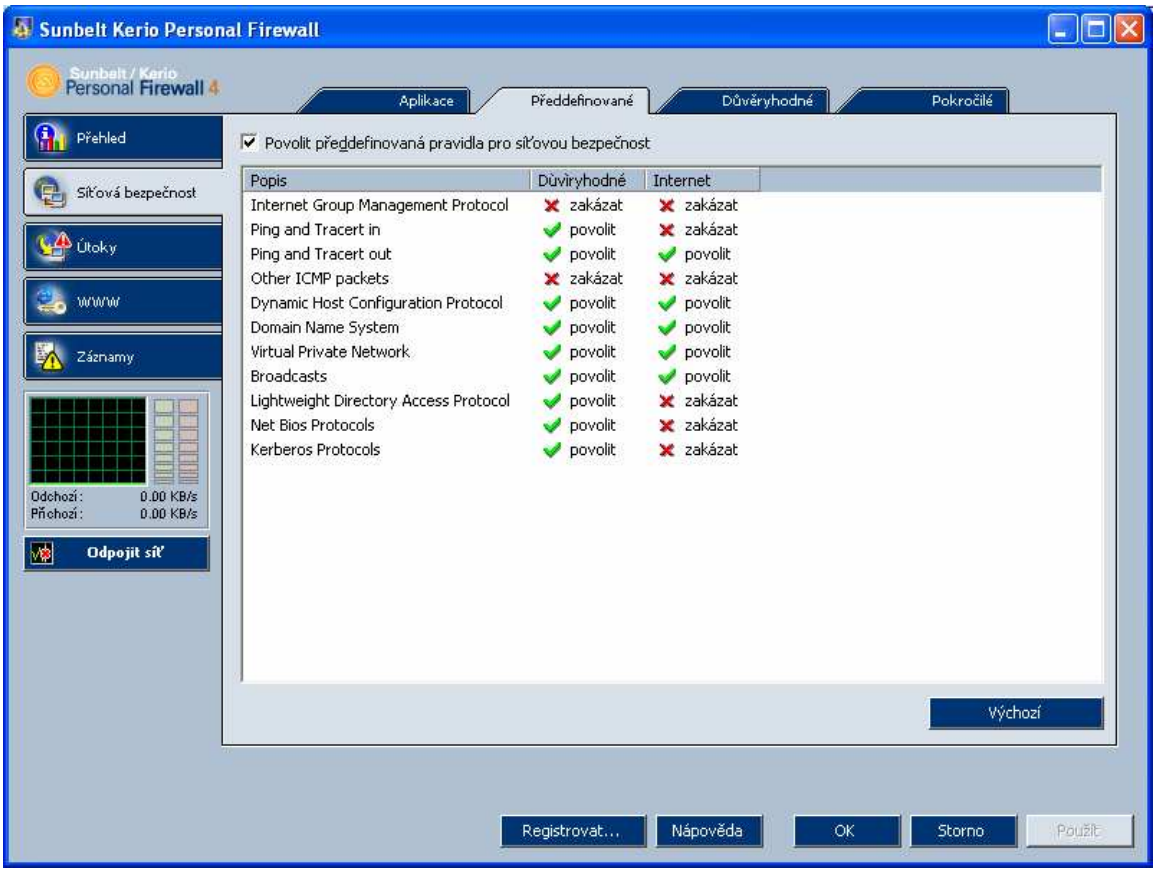
Advanced (learning mode – učící se režim)
Při zachycení neznámé komunikace, spuštění neznámé aplikace se dotazuje, jaká akce má být provedena a zda se má pro tuto akci vytvořit pravidlo. Tyto dotazy obvykle poté za chodu systému nabízí tři typy rozhodnutí (povolit , blokovat nebo se dotázat znovu).

Nastavení firewallu

Oprávněný uživatel by měl mít představu o legitimních aplikací, takovou aby firewall tyto aplikace omylem neblokoval. Nejprve si v položce Přehled/Předvolby nastaví vlastní profil tím, že zatrhne Povolit ochranu heslem a zvolí heslo. Poté tento uživatel, čím se myslí administrátor, který danou bezpečnost nastavuje, by měl modifikovat následující vlastnosti nastavení. Tyto nastavení najde v položce Síťová bezpečnost, která rozvíjí další nastavení, mezi kterými nechybí aplikace (Obr. 2.3) a předdefinované vlastnosti (Obr. 2.4). V této sekci se uživatel rozhoduje, které vlastnosti zakázat a které naopak povolit. Jestliže se jedná o vlastnost, ke které uživatel necítí důvěru, ale přesto ji využívá, nastaví režim dotazu, čím se jednotlivě rozhoduje při každém výskytu dané vlastnosti. V těchto dvou nastavení se uživatel ještě rozhoduje, zda-li ponechat povolení vlastnosti či aplikace pouze na důvěryhodném, či i na internetu, popřípadě obojí.



Obr. 2.3: nastavení zákazu u internet aplikace Odchozí

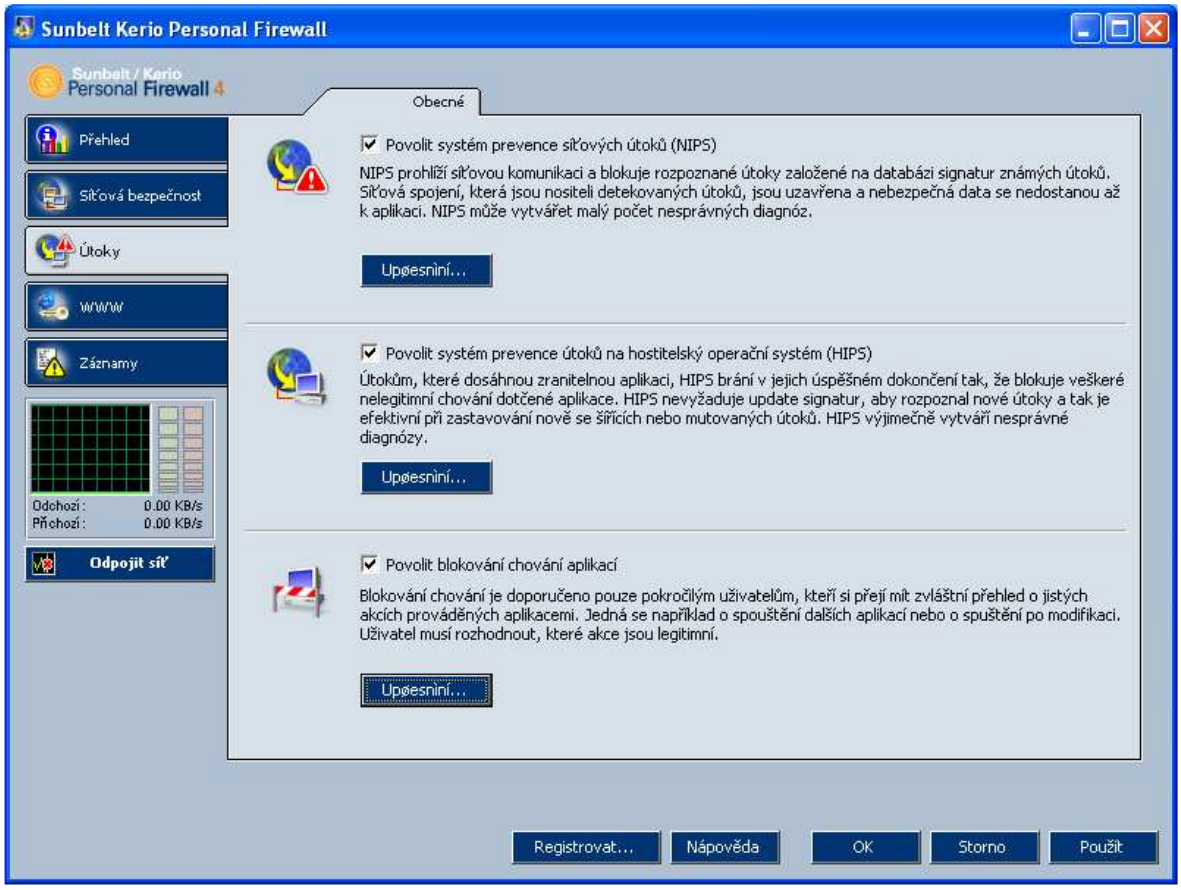


Obr. 2.4: předdefinované vlastnosti

Nastavení bezpečných nejčastěji tedy interních (místních-domácích) zařízení a terminálů do důvěryhodných patří do nastavení v záložce **Důvěryhodné**. Kde se zobrazí popis, IP adresa/tel.číslo a adaptér. Toto se nastavuje postupně s první komunikací daných okolních terminálů v síti, či přímým přidáním terminálu dle adresy přímo v záložce.

V záložce **Pokročilé** nastavuje tyto vlastnosti:
-Ochrana během startu a vypnutí OS (blokovaní pokusů za těchto situací)
-Režim internetové brány (použijeme v případě PC jako poskytovatele sdílení internetu)
-Rozšířené záznamy (monitorování paketů přicházející na neotevřené porty)

Dalším krokem v nastavení firewallu je konfigurace v položce **Útoky** (obr. 2.5).

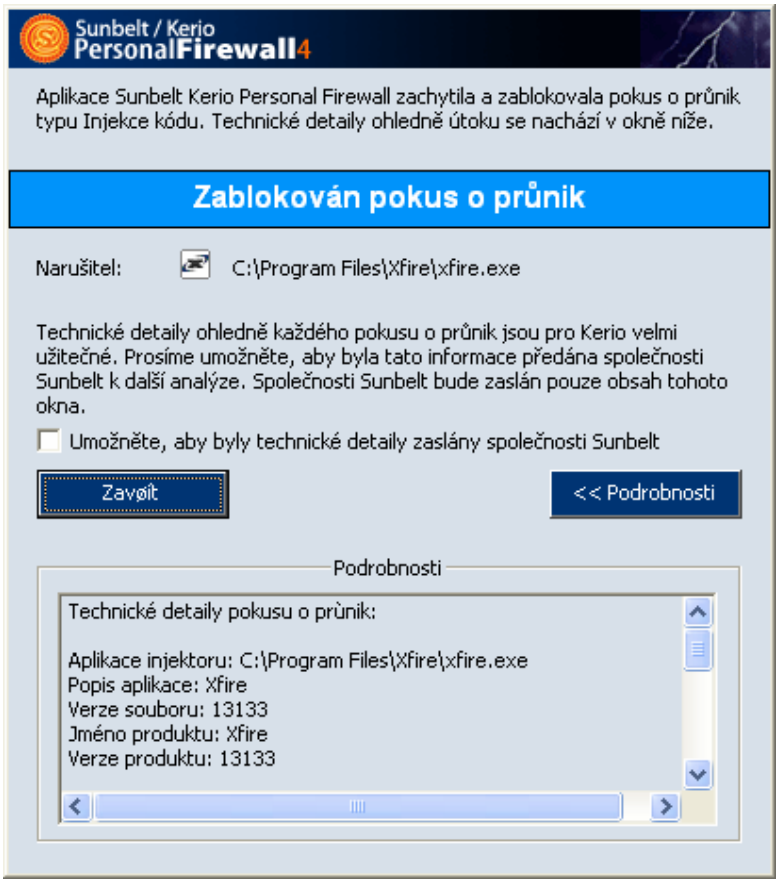


Obr. 2.5: nastavení prevencí NIPS, HIPS a blokování chování aplikací

Obvykle se doporučuje toto nastavení nechat implicitně nastavené výrobcem softwaru. Po kliknutí na tlačítko **Upřesnění** v případě **NIPS** se zobrazí nabídka s dílčími prioritami (nízká, střední a vysoká) různých útoků, které je možné zakázat. Povolením nízké priority předejdeme špatným diagnózám a blokovaní užitečných aplikací.

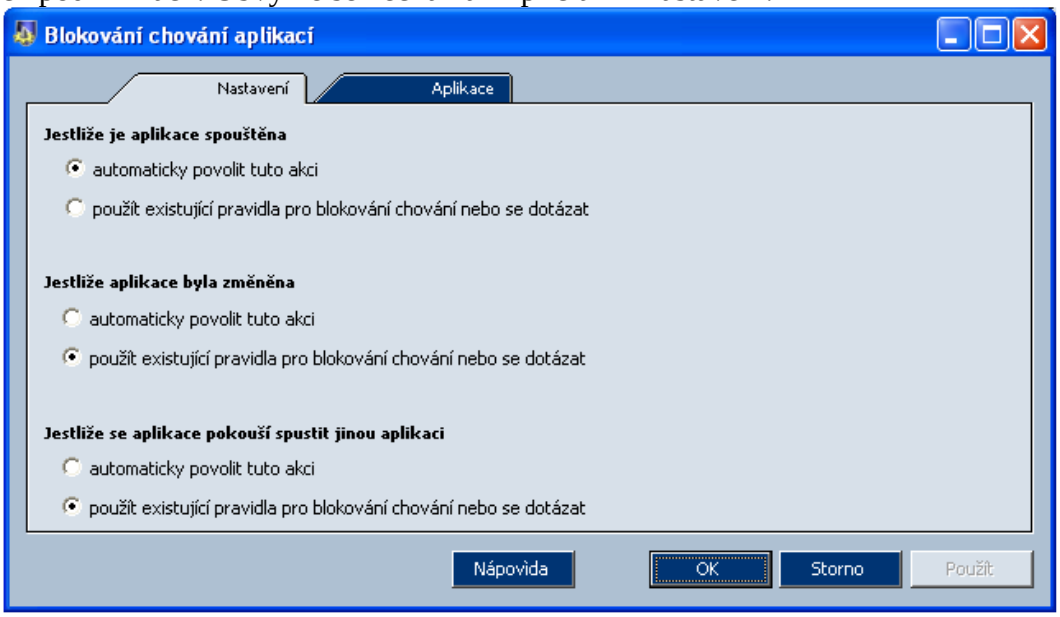
Po kliknutí na tlačítko **Upřesnění** v případě **HIPS** se zobrazí nabídka, kde se dají nastavit blokace pro rozběhnutí kódu po přetečení paměti, kterou využívají jak některé viry, tak některé aplikace, a proto je možné definovat výjimky. Rovněž zde nastavujeme blokace spustitelných injekcí kódu a také i nastavujeme výjimky. Je dobré ošetřit tyto výjimky, jelikož během chodu tohoto firewallu se může neustále spouštět hláška o blokaci injektoru, který představuje například neškodný Xfire (slouží ke komunikaci hráčů pc her po

internetu, monitoruje činnosti různých aplikací a zkoumá zdali se nejedná o pc hru), viz obr 2.6.



Obr. 2.6: výpis blokace injektoru (HIPS)

U poslední možnosti, kde povolujeme blokování aplikací, se po stisknutí tlačítka **Upřesnění** objeví okno (viz obr. 2.7), kde se řeší základní politika spouštění aplikací při různých podmínkách. Obvykle se nechá na implicitním nastavení.



Obr. 2.7: nastavení politiky spouštění aplikací

Třetím a posledním krokem je nastavení **WWW**, kde si uživatel může volně nastavovat **Blokovaní reklam** tj.zabezpečení proti adware, vyskakujícím oken (pop up, pop under) a zakazovat běžné skripty (JAVA, VBS) a objekty ActiveX.

V záložce **Soukromí**, pak lze nastavovat filtraci Cookie (bohužel pouze pro Microsoft Explorer) a trasování surfování po webu, pomocí Referer. Pokud si uživatel přeje mít co největší soukromí a používá jiný webový prohlížeč (mozilla, opera), tak mu vřele doporučuji také speciální program Delete Cookie, který již není součástí firewallu a je dostupný jako trial verze (bohužel na 3 dny).

Možnosti sledování dat

Uživateli Personal firewall 4 nabízí mnoho statistik a výpisů událostí. Dle těchto statistik pak může pružněji reagovat na změny různých exploitů a injektorů atd. Následující **statistiky** bývají jako záložka v položce **Přehled** a také zde lze sledovat i aktuální změny **spojení**. Tyto statistiky se ukládají do položky **Záznamy**.

Aby měl administrátor globální přehled o různých terminálech je vhodné nastavit v položce **Záznamy** v záložce **nastavení** IP adresu pracovního terminálu administrátora spolu s portem (např. 514), kde by chodili informace těchto záznamů o maximální nastavitelné velikosti.

+velmi mnoho nastavitelných funkcí
+konfigurace na heslo
+rozsáhlé nastavení bezpečnosti pro internet explorer
+lehká konfigurace (vhodná i pro začátečníky)
+dobré grafické zpracování má za důsledek lepší ovládání
+zabezpečení proti adware, vyskakujících oken atd.
+přítomnost NIPS, HIPS

-po skončení trial verze (30 dnů) se mnoho funkcí omezí
-při neúplném nastavení často vyvolává falešné poplachy (př. injektor Xfire)

=svou komplexností vhodné pro pokročilé uživatele i začátečníky

2.4.2 Jiný osobní firewall

Jako další alternativy se nabízejí i jiné kvalitní značky osobního firewall.

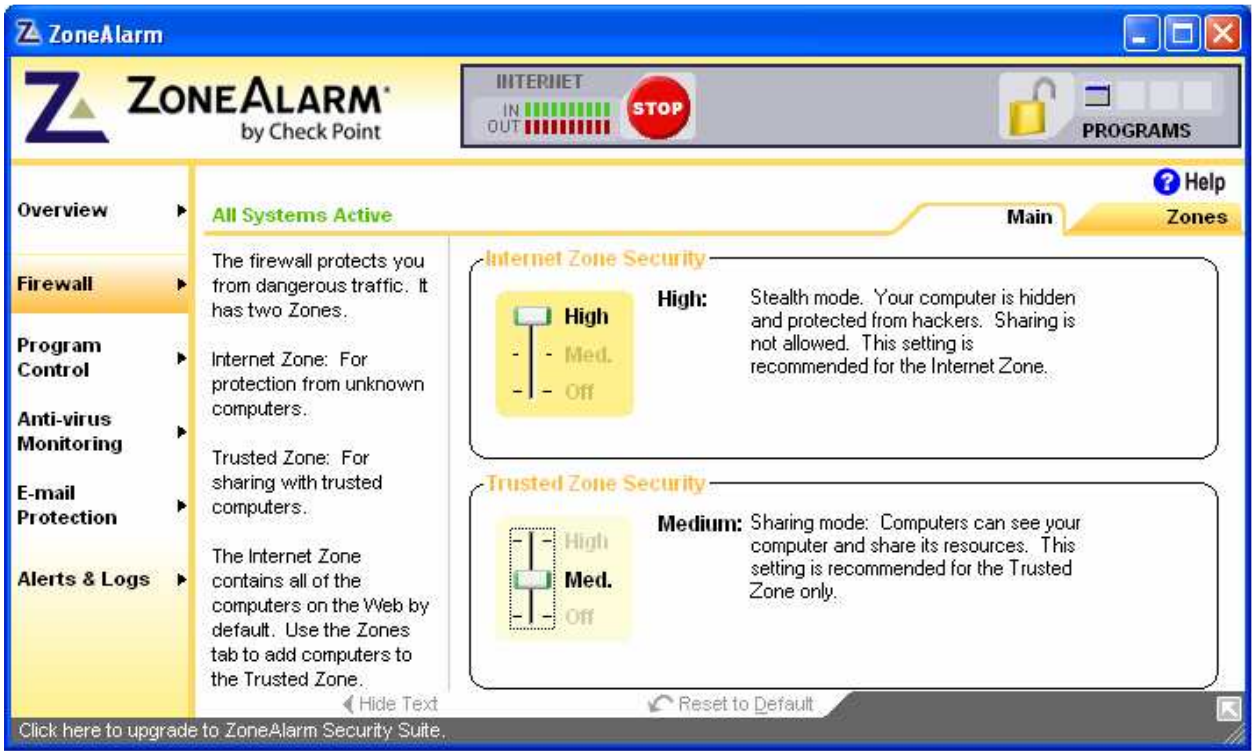
ZoneAlarm (test free verze)

Nejedná se o nekvalitní výrobek. Mezi jeho výhody patří volná dostupnost s poměrně snadným nastavením bezpečnosti. Pro větší stupeň nastavení je však potřeba placená verze ZoneAlarmPro. Není tedy časově omezen, tak jako Kerio PF4, ale nabízí méně funkcí a nastavitelných voleb. Jako nevýhoda se jeví i jeho ovládání v angličtině, což by někomu mohlo i vadit (viz obr. 2.8).

+ lehká konfigurace (vhodná i pro začátečníky)
+ free verze, časově neomezená

- slabá ochrana na úrovni e-mail (v této verzi pouze před .VBS)
- omezená konfigurace
- málo funkcí (nepřítomnost NIPS, HIPS)
- žádné nastavení soukromí (filtrace Cookies, zákaz trasování)
- žádné zabezpečení proti adware, vyskakujících oken atd.
- absence zamčení nastavení heslem

= vhodné tak pro domácí uživatele a začátečníky



Obr. 2.8: ukázka nastavení firewallu ZoneAlarm

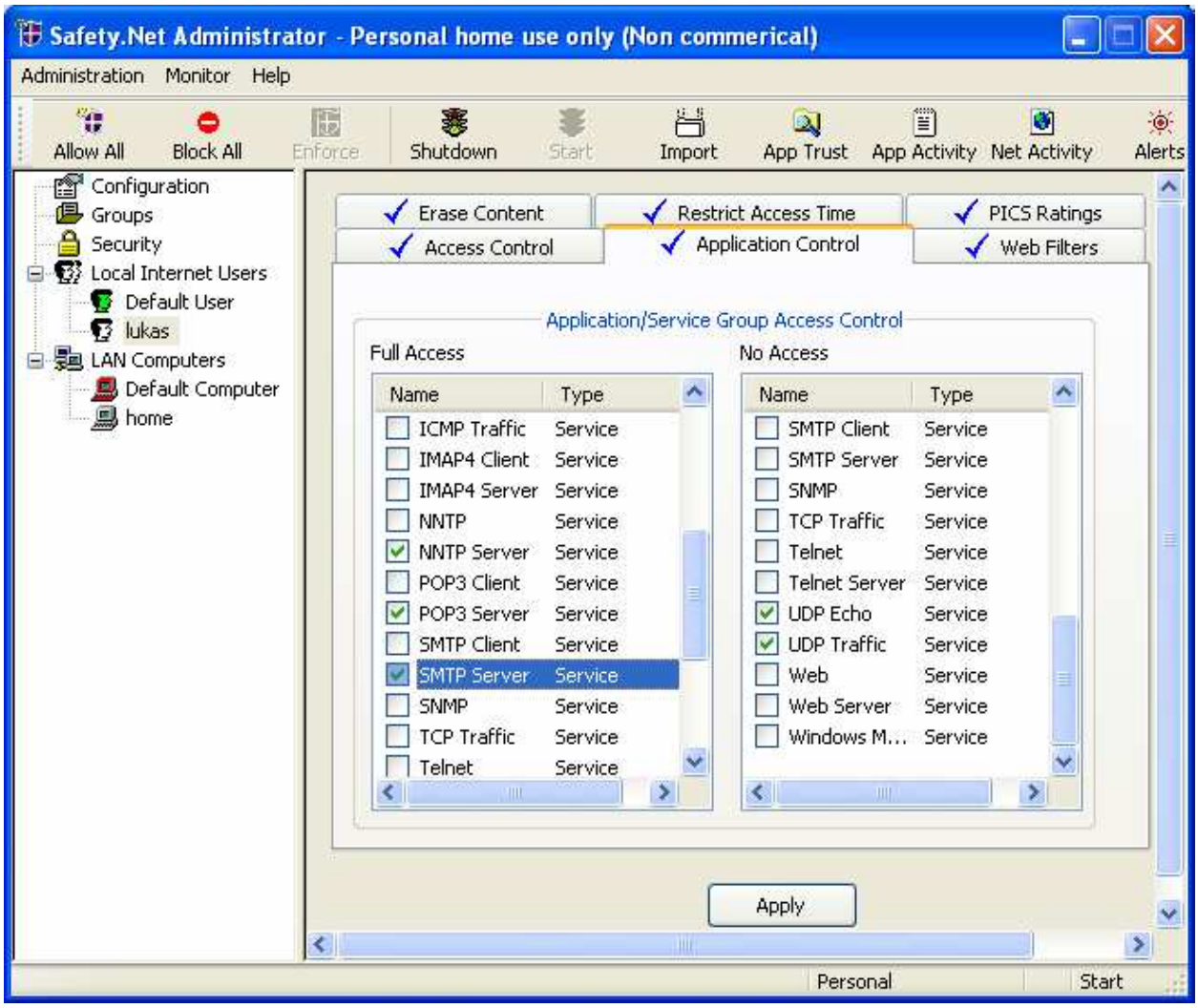
Safety.Net.Administrator – Personal home use only (no comercial)

Tento firewall již obsahuje o poznání více nastavitelných funkcí než firewall ZoneAlarm (free verze). Což přináší mnohé výhody. Mezi jedny z nevýhod patří jeho nepřehledné grafické prostředí a také pro některé angličtina.

+velmi mnoho nastavitelných funkcí
+konfigurace na heslo
+dobré nastavení bezpečnosti na internetu (security)
+možnost vytváření různých uživatelských nastavení(viz obr. 2.9)
+možnost vytváření různých konfigurací pro pc v síti

-horší grafické zpracování má za vinu horší ovládání
-chybí zabezpečení proti adware, vyskakujících oken atd.
-nepřítomnost NIPS, HIPS

=vhodné pro pokročilé uživatele a správce malých sítí

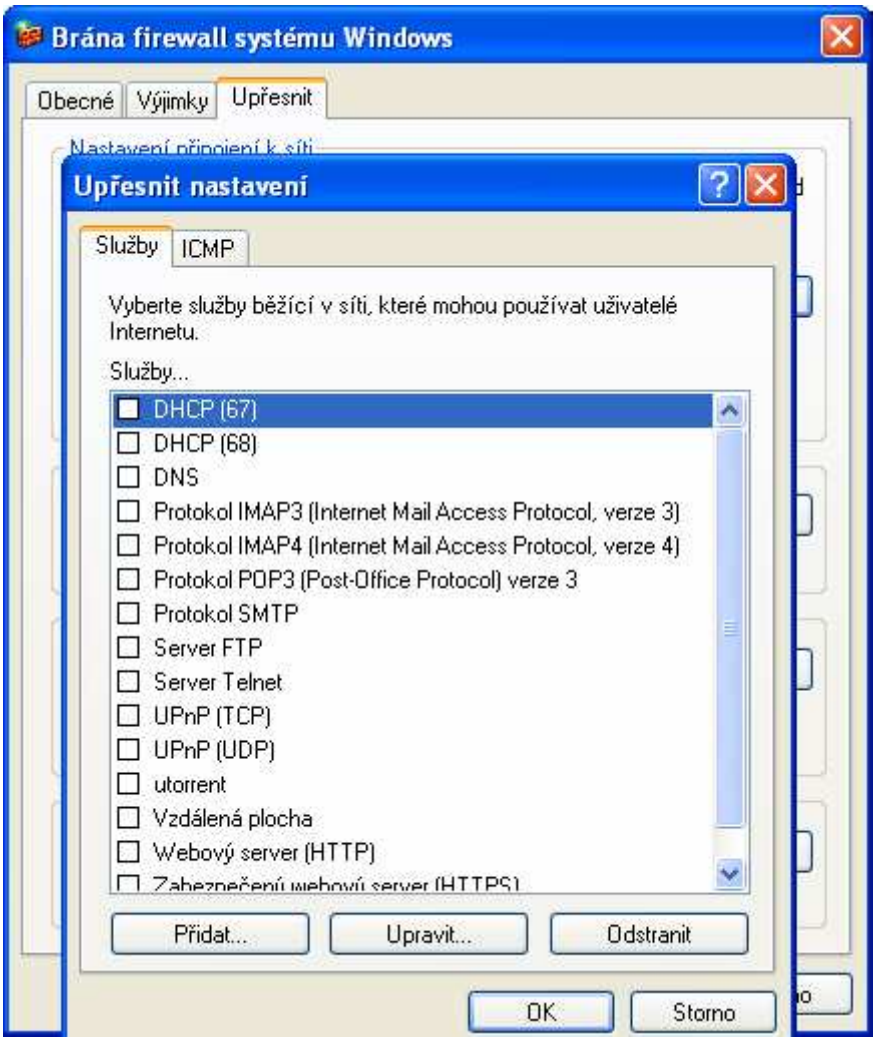


Obr. 2.9: nastavení plného přístupu (full Access) u uživatele lukas

Brána firewall systému Windows

Pokud uživatel má k dispozici systémy Windows XP, je potřeba si stáhnout navíc balíček oprav Service pack 2.

Firewall v SP2 je propracovanější a lepší než původní verze ve windows XP. Implicitně se po instalaci SP2 zapne a zakáže všechny funkce, podrobněji v [2]. Nabízí jen možnost povolení těchto služeb, které si vybereme a chceme používat (viz obr. 2.10).



Obr. 2.10: možnost povolení různých služeb, které firewall blokuje

\+ je součástí op.systému (nutný download SP2)
\+ uživatel op.systému, který se nevyzná v bezpečnosti nemusí nic nastavovat (firewall vše zakáže)

-velmi omezené možnosti, téměř žádné funkce navíc

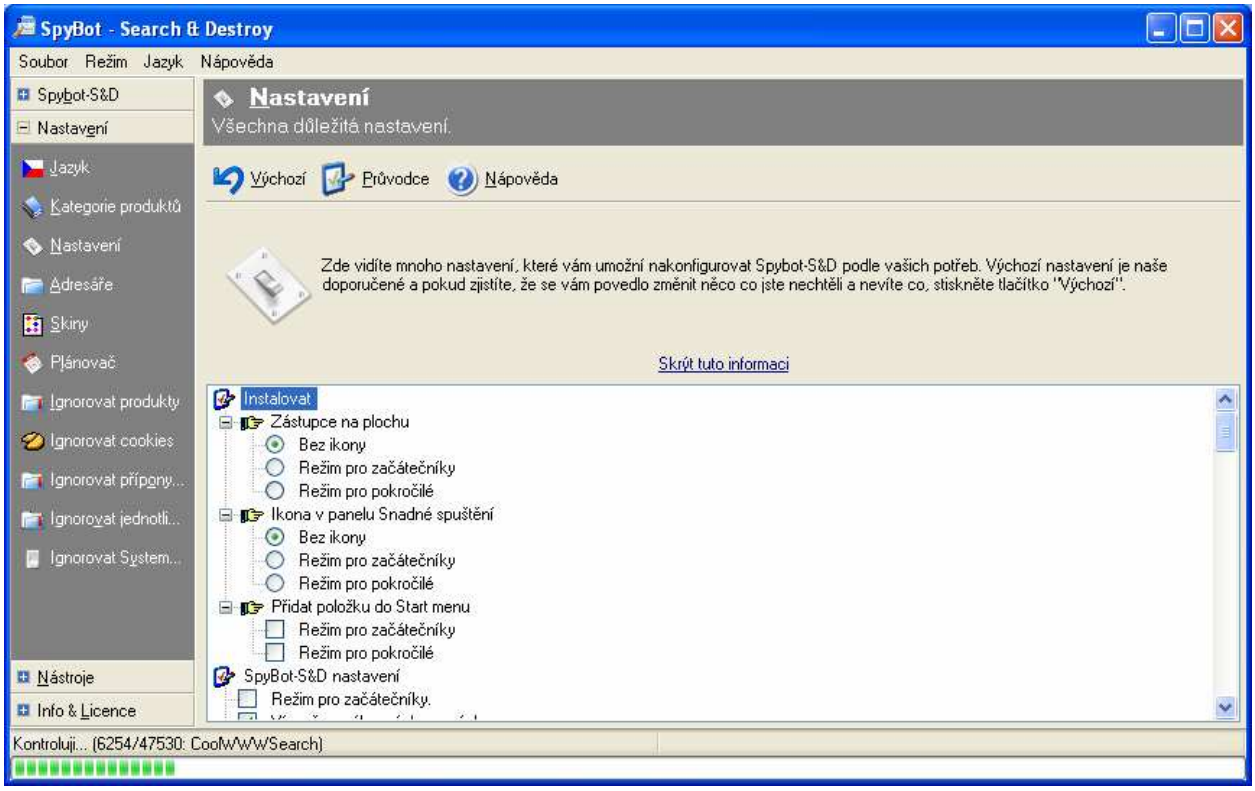
=nedoporučeno žádnému uživateli, který pracuje s hodnotnými daty

2.5 Antispyware

Software antispyware bývá většinou integrován již spolu s některými AV programy, či se nachází v komplexním balíčku služeb (internet security). Pokud sestavujeme zabezpečení počítače dle řešení I. je vhodné mít i tento druh zabezpečovacího software. Aktuální informace lze najít na odkazech [12], [13].

2.5.1 SpyBot – Search & Destroy

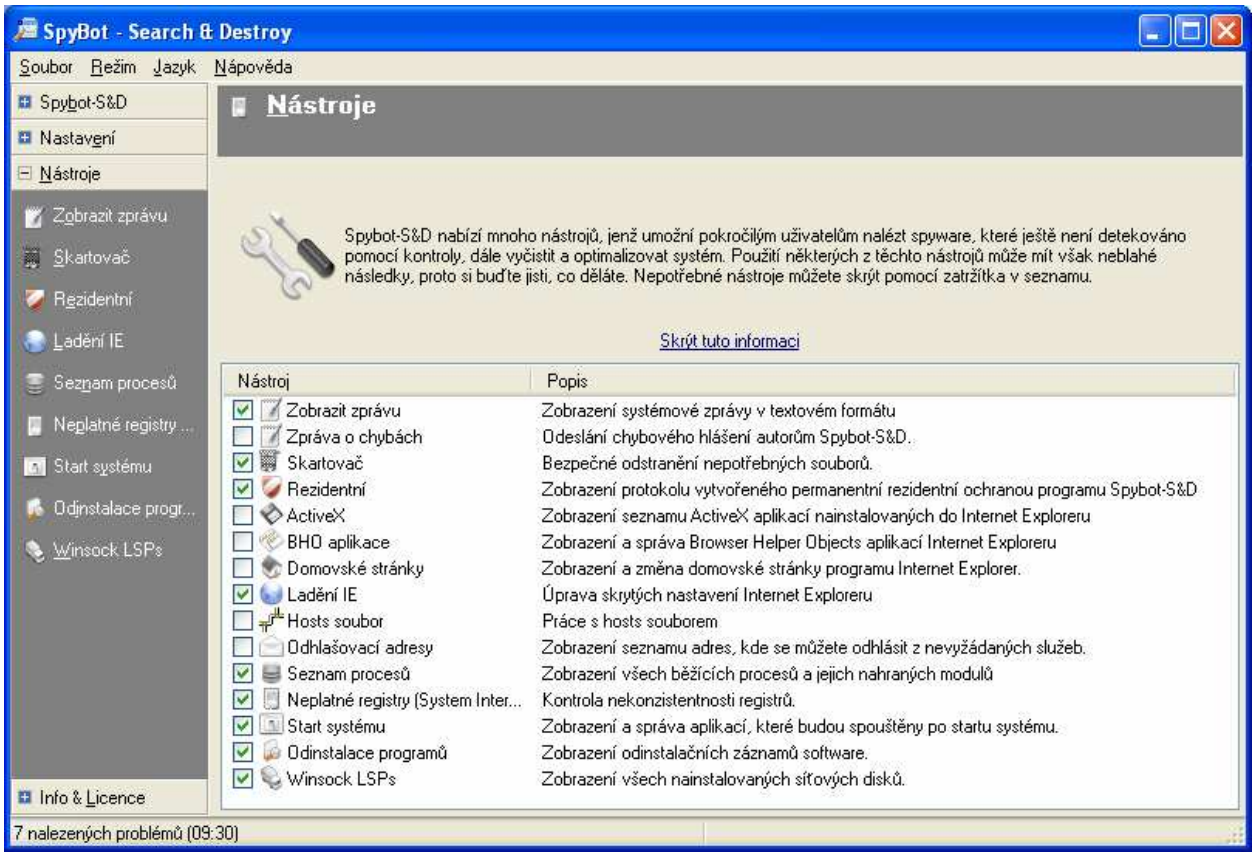
Jde o nejlepší produkt v našem kraji. Navíc je zdarma a není vůbec omezován. Autoři tohoto software očekávají pouze dobrovolné příspěvky od solidárních uživatelů. Test lze spustit v záložce **Spybot – S&D** a tím tak zkontrolovat problémy na daném počítači, viz [4]. Test zachycuje nejrůznější podezřelé jevy (změny v registrech, cookies atd.) Program v **režim**u **Pro pokročilé** nabízí mnoho možností nastavení a nástrojů.



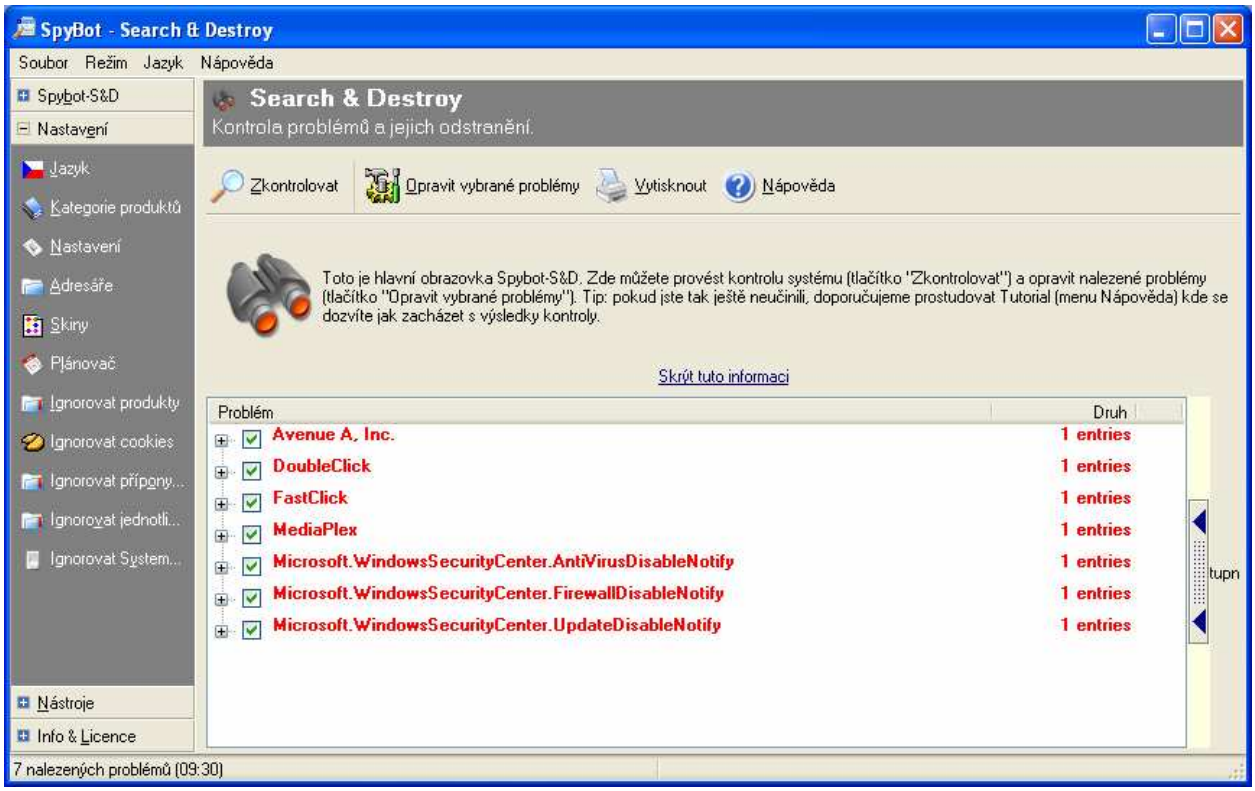
Obr. 2.11: nabídka **Nastavení** u SpyBot - SD (dole na obr. je rozběhnutý test)

V nabídce **Nastavení** lze konfigurovat základní funkce SpyBot. Dále můžeme nastavit až sedmi stupňovou prioritu kontroly. Také lze nastavovat různé automatizace (např. startu programu či startu systému) a aktualizace (například obnovení databáze konfiguračních souborů) a další nastavení týkající se chování programu (viz obr. 2.11).

Další pestrou nabídkou jsou **Nástroje**, kde uživatel může nastavit velmi mnoho funkcí, které jsou zobrazeny na obr. 2.12. Mezi tyto funkce patří Skartovač, rezidentní ochrana (proti škodlivým downloadům), ladění (nastavení skrytých funkcí Internet Explorer), procesy(zobrazí všechny procesy probíhající na PC a jejich nahrané moduly), neplatné registry (monitoruje změny v registrech) a nakonec běžné funkce, které nabízí i Windows XP a sice vypínání nepotřebných programů a procesů po startu systému a odinstalace programů.



Obr. 2.12: nabídka nástroje (dole je vidět dokončení testu)



Obr. 2.13: dokončení testu a jeho možnosti (program našel cookies a registry)

3 Vlastní návrh zabezpečení střední počítačové sítě

V této části je komplexně rozebráno zabezpečení firmy o střední velikosti. Návrh bude obsahovat široký rozsah prostředků a zařízení, které jsou dnes síťovým návrhářům, IT manažerům či bezpečnostním technikům k dispozici. Komponenty jako systém IDS, senzory IDS, kvalitní hraniční směrovač s integrovaným paketovým firewallem, proxy firewall, bezpečnostní servery pro webové služby, zařízení VPN či systémy IPS nejsou dnes levnou záležitostí. V praxi je obvykle takovýto návrh omezen finančním rozpočtem určený firmou. V následujících částích je uveden celkový koncept schématu zabezpečení firemní sítě a jejich jednotlivé komponenty budou rozebrány a uvedeny jejich nejlepší vlastnosti, které by se měli plně využít. Ke každé komponentě bude uveden soupis doporučení a tipů, které vychází jak z nejnovějších trendů tak z osvědčených a ujatých pravidel a funkcí. Dále budou popsány funkce a doporučení co se týče bezpečnostní politiky, jako jsou například režimy přístupu, technologie autorizace, authentizace a účtování (AAA) a některá doporučení o přidělování hesel. V návrhu nebudou chybět ani prostředky pro monitorování a dohled a jejich funkce a doporučení. Nakonec budou rozebrány havarijní stavy a možná protiopatření.

Postup návrhu zabezpečení počítačové sítě

1. Návrh struktury:
- návrh typů bezpečnostních komponentů s ohledem na infrastrukturu sítě
- výběr základních bezpečnostních komponentů (firewally, VPN karty, směrovače) dle velikosti sítě (hustota provozu, počet spojení TCP/UDP, počet VPN ve firmě)
- určení počtu rozhranní(zón) a určení jejich důvěrnosti

2. Konfigurace komponentů:
- povolení a zakazování typu služeb a jejich směru provozu skrz bezpečnostní komponenty (hraniční směrovač, firewall)
- nastavení specifických služeb firewallu (překlad adres NAT/PAT, relační časovače a inspekční pravidla)
- konfigurace jiných síťových prvků (access pointy u WLAN, brány VPN)

3. Nastavení a určení bezpečnostní politiky ve firmě:
- rozdělení sítě na bezpečnostní segmenty
- určení přístupových práv (autorizace)
- přidělení správných hesel (authetizace)
- kontrola dodržovaní pravidel, zavedení účtování (accounting)

4. Monitorování bezpečné činnosti sítě:
- využití systémů odhalování průniků do sítě (IDS)
- použití návnad (honeypots) k odhalení postupů útoků
- monitorování činnosti na aktivních síťových prvcích zprávami Syslog
- kontrola pravidelným testováním zranitelných míst

5. Obranné zajištění proti případným chybám a výpadkům v síti
- mít v záloze důležité náhradní komponenty (směrovače, hraniční směrovač)
- zálohovat důležité konfigurační nastavení a data
- sekundární firewall ihned přebere činnost při poruše primárního firewallu

3.1 Návrh struktury zabezpečení

Jelikož tento návrh není finančně omezen bude kladen důraz na co nejlepší bezpečnost firemní sítě s využití síťových aktivních prvků a minimalizovat zatížení AV softwarem na jednotlivých stanicí v síti, který je rozebírán v kapitole 2. Na obr. 3.1 je naznačena obecná struktura návrhu, která využívá hraniční směrovač, jako vnější paketový firewall. V případě poruchy směrovače je vhodné mít jeden náhradní k dispozici. Dále provoz směřuje do stavového proxy firewallu, který zabezpečuje většinu bezpečnostních opatření. Protože tvoří úzké hrdlo v síti je třeba se pojistit záložním (sekundárním) firewallem, nejlépe totožným zařízením, které má stejné nastavení jako aktivní (primární) firewall a který pak neprodleně přebírá všechny povinnosti za nefunkční zařízení.

Mezi firewallem a hraničním směrovačem je umístěno zařízení IPS, které ve svých modulech prověřuje síťový provoz a zpětnou konfigurací aktivně ovládá chování směrovače či firewallu. Při výskytu podezřelých jevů a útoků, které jsou odhaleny na základě signatur v IPS, jsou pak tyto útoky včas blokovány v firewallu. V případech pokud firewall nepodporuje sítě VPN je třeba umístit bránu VPN paralelně s firewallem, která zajišťuje bezpečné šifrované spojení skrz nedůvěrné prostředí vnější sítě.

Do demilitarizované zóny umístíme všechny servery, které budou poskytovat služby veřejnosti, kde běžnou činnost v této zóně bude hlídat systém IDS a návnada (honeypot). Bezdrátovou síť WLAN přivedeme do firewallu, jako další zónu a přenos do vnitřní sítě bude zabezpečen šifrováním dat branou VPN. Celý provoz pak sleduje systém IDS, který má za úkol odhalit případné útoky a anomálie na trase wlan – firewall.

Rozhrání vnitřní sítě (inside) je připojeno k firewallu a případně k bráně VPN a je na trase pojištěno systémem IPS, který rovněž aktivně prověřuje provoz na různých vrstvách, zejména na aplikační, a zpětně řídí činnost firewallu, který případné útočné a nežádoucí pakety (výskyt virů, spamů, spyware atd.) odhalí a blokuje či spojení celé zruší.

Do posledního oddělení managementu sítě bude z firewallu povolen pouze příjem výstražných, autentizačních, autorizačních, učetních a informativních zpráv s celé sítě. Zde je systém IDS, který by na základě těchto zpráv měl upozorňovat na problémy v síti.

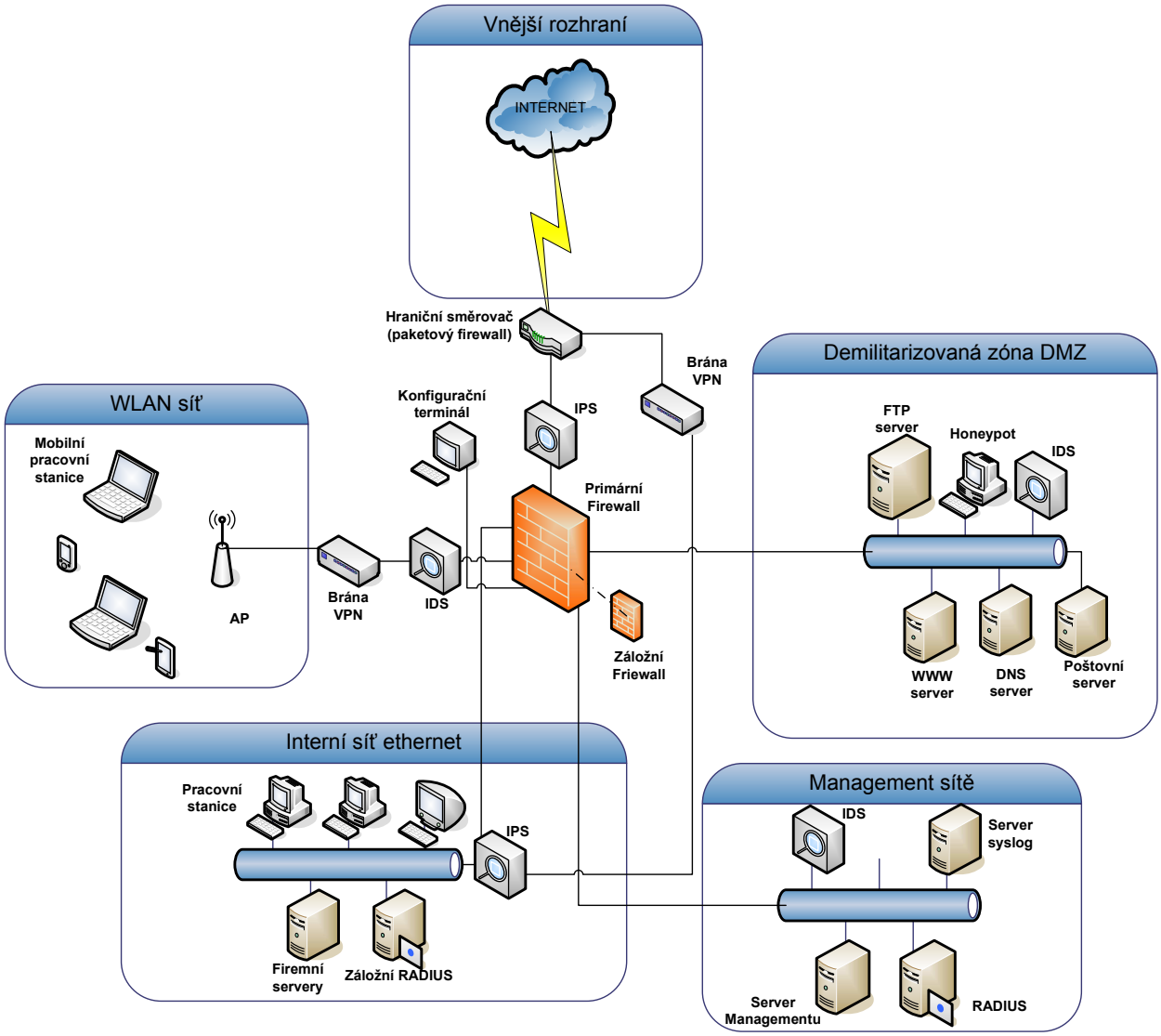
Tato struktura návrhu zabezpečení sítě se může realizovat různými komponenty, které se liší výrobcem, výkonností, cenou, podporou a servisem výrobců. U firewallu je navíc možnost dvou realizací a to softwarová a hardwarová.

Softwarový firewall versus hardwarový firewall

Softwarové firewally jsou obvykle levnější, dokonce existují i verze open source (bezplatné), nebo se u nich platí licence na počet připojených uživatelů či stanic v síti. Tyto firewally běží obvykle na opevněném hostiteli, který by měl obsahovat pouze zabezpečený a zaplátovaný operační systém a na něm by měla běžet pouze jedna aplikace, tedy softwarový firewall. U tohoto hostitele jsou vysoké nároky na hardware, který musí stihnout obsloužit veškerý síťový provoz. Proto nejsou vhodné u velkých sítí. Další nevýhoda spočívá přímo v operačním systému, který hostí aplikaci a může být slabým místem pro útoky. Nejbezpečnějším systémem ale bývá vhodně nakonfigurovaná distribuce unix.

Hardwarové firewally přináší velkou výhodu, která spočívá ve vlastním hardwarovém zařízení, které je přizpůsobeno na míru pro vlastní nesený software. Tento software je navíc přímo zaměřen na bezpečnost a zřídka se na něm najdou bezpečnostní chyby (i když k nim bohužel dochází). Samotný hardware je pak jako aktivní síťový prvek dimenzován na velké výpočetní výkony a dokáže obsloužit provoz i velkých sítí. Tyto firewally obvykle podporují několik fyzických rozhraní (běžně 3 zóny, dražší modely více) a několik virtuálních, stejně

jako softwarové firewally. Mezi nevýhody naopak patří velmi vysoká cena a drahý servis. Více informací o typech a druzích firewallů viz [8].

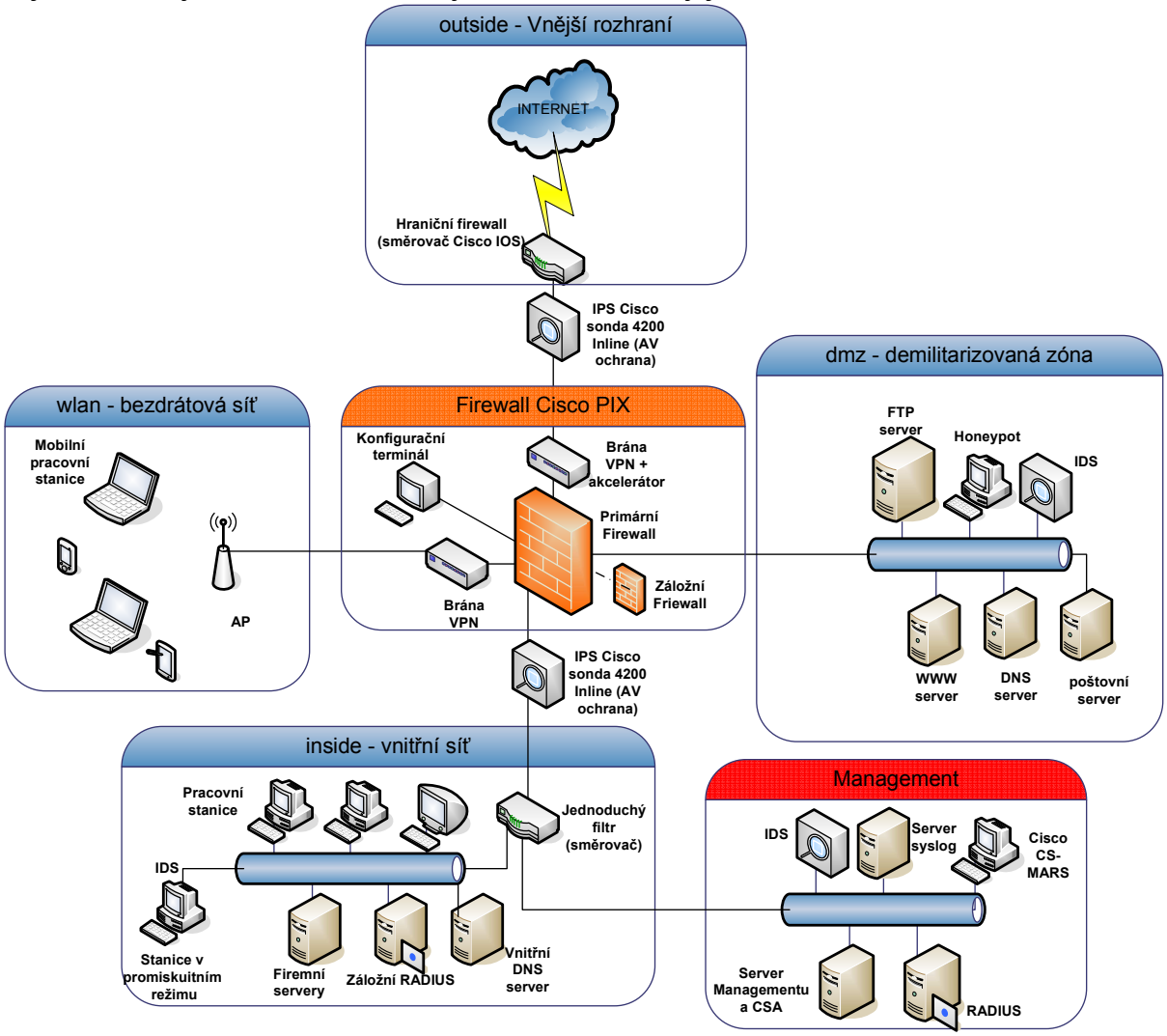


Obr. 3.1: obecná celková struktura zabezpečení sítě

Struktura zabezpečení sítě komponenty Cisco

Nejznámější a nejdostupnější komponenty jsou od firmy Cisco. Cisco má dlouhou tradici v oblasti síťové komunikace a její bezpečnosti a nabízí širokou nabídku bezpečnostních aktivních prvků a přidruženého bezpečnostního softwaru. Dále poskytuje širokou podporu a servis. Rovněž konfigurační příručky a jiné literatury o výrobcích Cisco jsou velmi rozšířené a dostupné v češtině narozdíl od jiných výrobců. Návrhář se pak může předem rozhodnout, zda-li mu popisované výrobky, které potřebuje implementovat do podnikové sítě, budou vyhovovat či nikoliv. Rovněž tím, že jsou takto dostupné příručky a literatura k různým Cisco zařízením se může předem naučit a porozumět správné konfiguraci zařízení a takto zkvalitnit a urychlit celou implementaci. Toto je velká výhoda vůči menším výrobcům, u kterých tak uživatel kolikrát neví co očekávat. U velkých firem jako např. Cisco je naopak nevýhodou větší cena za značku a za poskytovanou podporu zákazníků. Na obr. 3.2 je návrh struktury řešený pomocí komponent Cisco. Jelikož je celá struktura realizovaná výrobky Cisco, nevyskytuje se pak žádný problém s kompatibilitou. Naopak pak taková

homogenní bezpečnostní struktura přináší výhody v celkovém monitorování sítě. Jiné typy struktur jsou uvedeny v [9]. Podstatná nevýhoda této struktury je finanční náročnost.



Obr. 3.2: celková struktura zabezpečení sítě s pomocí komponentů Cisco

3.1.1 Hraniční firewall (směrovač)

Na hranicích podnikové sítě s vnějším digitálním světem (internetem) se nachází úzké hrdlo, které řídí příchozí a odchozí provoz. Většinou se jedná o směrovač, který rozhoduje který paket pošle skrz a který zahodí. V podstatě se jedná o paketový filtr (firewall). Můžeme tedy tento směrovač jako paketový firewall vhodně nakonfigurovat a tím zajistit první obranou linii naší firemní sítě. Je však zapotřebí pamatovat na jeho původní funkci a příliš směrovač nezatěžovat různými filtrovacími funkcemi. Mohlo by lehce dojít k přetížení a vytváření front, jelikož skrz něj prochází veškerá komunikace firemní sítě s okolním světem a jejími pobočkami či vzdálenými klienty. Často se stane, že je tato brána do internetu, tedy směrovač, umístěná u poskytovatele internetových služeb (ISP), který sám provádí konfiguraci a údržbu nad zařízením a k firemní síti je vyvedena ethernetová linka (optický kabel). V těchto případech již nemůžeme důvěřovat tomuto cizímu zařízení a na první linii se tak posune síťový firewall. Je možné se dohodnout s poskytovatelem na určité spolupráci na nastavení a konfiguraci směrovače, ačkoli hlavní slovo bude mít poskytovatel, který raději nebude zatěžovat výkonnost směrovače, popřípadě se za daný přístup ke konfiguraci

směrovače bude platit. Tak i tak je výhodné přenést některé bezpečnostní funkce již na směrovač, který tak odlehčí část práce síťovému firewallu a tím dojde k rozložení zátěže na těchto dvou úzkých hrdlech v síti. V případě vlastního směrovače je třeba mít v záloze další náhradní, který bude v záloze při poškození aktivního směrovače.

Množina funkcí hraničního firewallu a jeho konfigurace

- Filtrování paketů (povolovat a blokovat pakety na základě vymezení rozsahů IP adres ACL-access lists).

- V případě výpadku hlavního a sekundárního firewallu zajištění překladu adres funkcí NAT (Network Address translation) a přetížení portů PAT (Port address translation), čímž se ukryje celá vnitřní topologie sítě za použitou jednu veřejnou adresu (u PAT) či rozsah veřejných adres (statický či dynamický NAT).

- Blokovat nepovolené typy směrovaní (hrozí přepsání směrovací tabulky).

- Řídit tok zpráv ICMP (blokovat příchozí typy jako –host unreachable), povolit příchozí echo request a host unreachable jen na servery v DMZ, povolit odchozí echo reply, time exceeded (překročení časového limitu), packet-too-big, unreachables a komunikace ukončena. Dále zakázat přenosy na všesměrové adresy(directed-broadcast) a přesměrování (redirects).

- Blokovat zprávy SNMP směřující do sítě, které prozrazují info o managementu sítě (nastavit blokování portů 161 a 162, na kterých SNMP funguje, a pak další příbuzné porty tcp a udp 199, 391 a 1993).

- U kvalitnějších směrovačů Cisco používat funkci NBAR (pracuje s hlubší analýzou přenosu, rozezná u HTTP typy MIME –audio/video, adresy URL, rozezná statické a dynamické porty). Díky NBAR lze například zaručit pro kvalitu služeb QoS potřebnou šířkou pásma, což je vhodné pro důležité firemní video konference.

- Nepoužívat zbytečné a nevyužité funkce jako například small service, NTP(Network time protocol) či Finger (poskytuje info o přihlášených uživatelích).

- Zablokovat všechny nechtěné možnosti konfigurace směrovače (Telnet, FTP), používat šifrovaný SSH, používat autentizaci pomocí RADIUS.

3.1.2 Síťový firewall

Tento prvek v síti je jednou z nejpodstatnější součástí v zabezpečení podnikové sítě. Moderní firewally jsou velmi výkonné a slučují několik inspekčních pravidel, které se uplatní nad úzkým hrdlem síťového provozu, někdy jsou označovány jako aplikační stavové. Provádějí aplikační inspekci, překlad adres, podporují VPN, IPS, autentizaci uživatelů, dynamické směrování, zálohování, atd. Takový komplexní firewall bude v síťové bezpečnosti nejdražší komponentou. Nabízí se ovšem i řešení s více firewally v síti které fungují v sérii či paralelně. Tyto řešení navyšují propustnost úzkého hrdla v síti, které firewall svojí polohou vytváří. Možnosti jsou jako vždy omezeny finančními prostředky. Drahé zařízení jako Cisco ASA (Adaptive Security Appliance) v sobě sdružují funkce stavového aplikačního firewallu, systému IPS, koncentrátoru VPN a antivirového modulu. Chrání tak síť od linkové po

aplikační vrstvu. Moduly Cisco FWSM (firewall service module) se instalují do výkonných síťových přepínačů a tvoří v nich přídavné moduly, které mají vlastnosti aplikačně stavových firewallů. Vhodné pro struktury, kde hraniční směrovač plní i funkci síťového firewallu.

Výhody(+) a nevýhody(-) aplikačně-stavových firewallů

+ díky technologii NAT jsou skryty všechny vnitřní IP adresy terminálů a vnitřních serverů
+ skrytá je celá topologie sítě
+ zaměřují se na výkonnost, která je vyvážena poměrem inspekce prověření a rychlosti dat
+ podpora autentizace, autorizace a účtování AAA, generování zpráv syslog
+ odolnost proti falšování IP adres
+ jednotná režie více typů systémů (paketový firewall+server proxy + IDS +VPN)

- obvykle neposkytují kompletní prověřování aplikací (AV software, anti SPAM)
- pomalejší než paketové filtry
- úzké hrdlo v síti, mohou se tvořit fronty a zahazovat pakety
- finančně dražší systémy
- firewally bez podpory VPN mají problémy s tunelujícími protokoly IPSec a SSL díky NAT

Typy softwarových firewallů

Mezi vyhledávané softwarové firewally patří tzv. projekty open source, které levněji poskytují ochranu počítačovým sítím. Mezi tyto firewally patří například IPCop či M0n0wall.

IPCop je linuxovou distribucí spustitelná na IBM kompatibilním PC, dostupný z [15]. Je vyvíjen celosvětovou komunitou a kromě samotných verzí jsou volně dostupné i addony, což jsou neoficiální doplňky, které rozšiřují funkce firewallu. Další výhodou je rozsáhlé fórum všech uživatelů, kteří si navzájem poskytují tipy a cenné rady (v ang.j.). IPCop podporuje až 4 rozhraní (red-outside, green-inside, orange-dmz a blue-wlan), čímž vyhovuje navrhnuté struktuře. Pro správnou komunikaci se musí mezi jednotlivými síťovými kartami (každá představuje jedno rozhraní) nakonfigurovat tzv. Pinholes.

IPCop kromě blokování paketů dle pravidel obsahuje několik užitečných funkcí:

- DHCP server
- proxy server (squid), filtr URL, pokročilé filtrování (addon AdvProxy)
- IDS (snort)
- lokální dns server (DNSmasq)
- SSH
- VPN
- NTP (klient a server časové synchronizace)
- traffic shaping (omezení provozu)
- zakázání odpovědí na ping
- NAT
- logování a dohled nad provozem (addon IpTraf, addon Logsend)
- mail proxy and filtr spam (addon POPFile)
- kontrola integrity souborů (addon TripWire)

M0n0wall je postaven na kostře FreeBSD, webovém serveru, PHP a dalších utilitách. Jeho konfigurace je uložena ve formátu XML. M0n0wall podobně jako IPCop poskytuje množinu základních bezpečnostních funkcí, které mají komerční firewally. Rovněž podporuje čtyři rozhraní a navíc podporuje i virtuální sítě LAN (VLAN). Jeho přednostní je graficky přehledné webově orientované konfigurační menu zabezpečené SSL. Více na [17].

Typy hardwarových firewallů

Pro různé velikosti sítí je dnes široká nabídka firewallů. Pro střední firemní sítě existují firewally, které již sdružují více funkcí jako jsou VPN, IDS atd. Základním parametrem je počet portů tedy rozhraní a jejich druh síťové karty (Ethernet, Gigabit ethernet). Kromě požadavků na bezpečnostní mechanismy (NAT, PAT, stateful inspection, DoS, AAA) se požaduje od těchto zařízení i vysoká propustnost, jelikož tvoří úzké hrdlo v síti, kde tedy veškerý odchozí a příchozí provoz prochází skrz firewall. Kromě propustnosti dat (šifrovaných a nešifrovaných) se nahlíží i na počet současně udržovaných spojení TCP/UDP. Dražší systémy mají zabudovanou kartu akcelerátor VPN s maximálním současným počtem uživatelů VPN a jejich stupně zabezpečení (DES, 3DES, AES). Dalšími obvyklými součástmi jsou Antivirové programy, Antispamy, filtry URL a různé moduly na aplikační vrstvě.

Vzhledem k velkému rozmachu bezpečnosti sítě se na trhu objevuje spoustu výrobců. Mezi nejznámější výrobce patří Cisco (řady PIX a ASA), D-link, Juniper, Secure Computing, 3com, IBM, SonicWALL, Elron. V následujícím přehledu tab. I jsou ukázky základních funkcí některých modelů, které jsou vhodné pro střední firmy i včetně ceny, která je jen přibližná k době tvorby tohoto přehledu a nemusí být aktuální.

Tab. I: přehled hardwarových firewallů

Firma	**typ**	**max.počet rozhraní /typ rozhraní**	**základní bezpečnostní funkce**	**max.počet spojení TCP,UDP /počet spojení VPN**	**propustnost (nešifrované a šifrované data)**	**přibližná cena**
Cisco	PIX 515E	6 / FastEth	Stateful inspection, DoS, AAA, NAT/PAT	130000 / 2000	188Mb/s, 140Mb/s (3DES) AES	110000kč
Cisco	PIX 525	8 /FastEth nebo GigaEth	Stateful inspection, DoS, AAA, NAT/PAT	280000 / 2000	330Mb/s, 155Mb/s (3DES) AES	185000kč
Cisco	ASA 5510	3 / FastEth	Stateful inspection, DoS, AAA, NAT/PAT,IPS MalwareP,AV,	32000 / 50IPSec 50Web VPN	300Mb/s, 170Mb/s (3DES) AES	100000kč
D-link	DFL -2500	8 /GigaEth	PPPoE, IDS NAT/PAT, ZoneDefense, ALG	1000000 / 2500	600Mb/s, 300Mb/s (3DES)AES	110000kč
D-link	DFL -1600	6 /GigaEth	PPPoE,IDS,NAT/PAT, ZoneDefense, ALG	400000 / 1200	320Mb/s, 120Mb/s (3DES) AES	56000kč
Juniper	SSG550	4 / GigaEth	Stateful firewall, IPS, Antivirus, Anti-Spam a Web Filtering	128000 / 1000	1Gb/s, 500Mb/s VPN,IPS	170000kč
Juniper	SSG520	4 / GigaEth	Stateful firewall, IPS, Antivirus, Anti-Spam a Web Filtering	64000 / 500	600Mb/s, 300Mb/s VPN,IPS	105000kč
Secure Computing	Sidewinder 210D	4 / Eth	Stateful proxy firewall,IPS, Antivirus, Anti-Spam a Web Filtering	x / 200	180 Mbps	124000kč
SnapGear	SG720	2 / Eth + 2x4 Switch Eth	Stateful proxy firewall,IPS, Antivirus, Anti-Spam a Web Filtering	x / 1000 (IPsec) 140 (PPTP)	300Mbps, 45Mbps AES, 12Mbps PPTP RC4	86000kč

Základní doporučení ke konfiguraci firewallu Cisco typu PIX

- Nastavení důvěrnosti spravovaných segmentů, nebo-li rozhranní, viz tab. II. Každému takovému segmentu, který vstupuje do firewallu, přiřazujeme úroveň zabezpečení v intervalu od 0 do 100 (respektive 1 až 99, 0 a 100 jsou implicitně přiřazeny). Firewall tak rozezná díky koeficientům úroveň zabezpečení či důvěrnosti, od které se odvozuje inspekční logika. K danému návrhu tedy potřebujeme, aby firewall podporoval minimálně 4 segmenty. Z modelů firewallů cisco PIX jsou tedy vhodné produkty 515E, 525 a 535 určeny pro střední a velké sítě. Produkty s označením –UR-BUN mají navíc neomezenou softwarovou licenci, které například u 515E rozšiřují na šest portů (rozhraní), viz [18].

Tab. II: úroveň zabezpečení zón

hardware id	Název rozhraní (zóny)	úroveň zabezpečení	popis
ethernet0	outside	0	nedůvěryhodná vnější síť (internet)
ethernet2	dmz	50	demilitarizovaná zóna
ethernet3	wlan	60	síť bezdrátové místní sítě
ethernet1	inside	100	důvěryhodná vnitřní síť

- Nastavíme přenosovou rychlost jednotlivých připojených rozhraní.

- Přiřadíme IP adresy jednotlivým rozhraním.

- Zajistíme překlad lokálních adres na globální adresy funkcí NAT (Network Address Translation), která ukrývá lokální reálné adresy vnitřní sítě před uživateli vnější sítě. Umožňuje přiřazovat IP adresy velkému rozsahu hostitelů uvnitř podnikové sítě (přesné intervaly alokace adres jsou k dispozici v dokumentu RFC 1918) Dále uvedeme interval či fond globálních adres, které budou veřejně známé.

- U převodu na jednu globální IP adresu se využívá převod na více portů PAT (port address translation). Vhodné pro firmy s nízkým počtem veřejných IP adres, který se brzy při silném provozu vyčerpá (počet aktivních lokálních IP adres převýší počet veřejných ve fondu global). PAT nepodporuje některé multimediální aplikace, proto se používá jako poslední možnost při silném provozu v síti a dokáže obsloužit až 64000 hostitelských lokálních adres. Je vhodná pro služby HTTP, DNS, FTP, elektronickou poštou, atd.

- Globalní adresa PAT nesmí být v intervalu globálních adres podporující NAT.

- Povolovat zahájení komunikace z důvěryhodného prostředí do nedůvěryhodného pro známé služby (http, ftp, dns, smtp) a dynamicky povolovat odpovědi.

- Staticky povolit zahájení komunikace pro definované služby využívající VPN (vzdálené pracovní stanice, partnerské sítě). Vytvoření přístupových odchozích a příchozích seznamů ACL na základě portů a IP adres.

- Povolit průchod z vnějšího prostředí do demilitarizované zóny pro služby DNS, SMTP, FTP a HTTP. Povolit výjimky komunikace TCP/UDP na zadané IP adresy WWW,DNS a FTP serverů na použitých portech.

- Nastavit stavovou inspekci pro používané služby (ftp, http, smtp, rsh, sqlnet, atd.) skrz firewall tj. převádět adresy dle NAT či PAT i v datové zátěži paketů, pro každou relaci dynamicky vytvářet volný průchod (conn table) pro odpovědi, který se po rozpadnutí či vypršení časovače odstraní.

- Vyhradit interval používaných portů u multimediálních služeb (rtsp, h323, ..) pro stavovou inspekci.

- Více o konfiguraci, příkazech a syntaxí v příručkách firewallů Cisco, či v použitých literaturách [6] a [7].

Několik dalších tipů pro konfiguraci Cisco PIX firewallu

- Vzhledem k útokům na službu DNS (záplavy požadavků DNS) snížit implicitní časovač UDP ze 2 minut na poloviční hodnotu, případně na nižší.
- Nepovolovat fragmentaci paketů v komunikaci, případně zapnout stráž fragmentačních útoků příkazem **sysopt security fragguard.**
- Nastavit maximální počet spojení a limit rozpracovaných spojení na hodnoty zjištěné z běžného provozu, které chrání proti záplavám paketů syn, které vedou k DoS.
- V případě přídavné karty VPN nastavit přístupové seznamy (access control list) a parametry pro šifrování IPSec, takto povolíme a zabezpečíme provoz z internetu

3.1.3 Nastavení provozu skrz firewall pro rozhraní v síti

Rozdělení sítě na několik bezpečnostních zón nebo-li rozhraní je základem každého návrhu zabezpečení počítačové sítě. Tedy pokud se nejedná o velmi malé sítě, nebo sítě, které nejsou připojeny k vnějšímu světu, tedy internetu. V návrhu jsou celkem čtyři rozhraní (outside, inside, dmz, wlan).

Outside

- Strana poskytovatele internetových služeb IPS označována jako vnější síť.
- Zóna je nedůvěryhodná.
- Na firewallech Cisco má nejnižší bezpečnostní koeficient (0-100) implicitně nastaven na 0.
- Na firewallu se povolují jen používané odchozí služby (http,dns,ftp,smtp,atd.)
- Z vnější sítě povolíme díky rozšířeného přístupového seznamu ACL jen sítě VPN

Dmz

- Strana poskytující informace a služby veřejnosti (servery DNS, Webové servery, poštovní servery a FTP servery) se nazývá demilitarizovaná zóna.
- Střední důvěryhodnost.
- Na firewallu Cisco definujeme koeficient volně s intervalu (1-99).

- Na firewallu pak povolíme příchod do demilitarizované zóny jen pro používané služby a zakážeme navazování spojení do zóny outside, kromě odesílání elektronické pošty (což zabrání zneužití DNS serveru jako „zombie“ při DDoS).

Wlan

- Bezdrátová sít WLAN, je potřeba pro tuto síť zavést taky samostatnou bezpečnostní zónu.
- Střední důvěryhodnost.
- Na firewallu Cisco definujeme koeficient v intervalu (1-99), ale v rozmezí (dmz < wlan < inside).
- Pracovním stanicím v rozhraní wlan bude umožněno díky firewallu navazovat odchozí spojení směrem do outside pro povolené služby a aplikace (http, https, ftp, sftp, dns) podobně jako u zóny inside a do dmz pro výběr el.pošty.
- Pro přístup do sítě inside se vytvoří na firewallu seznamy ACL, které povolují navázání spojení jen známým zařízením na základě zdrojových a cílových IP adres a portů. Navíc tyto přenosy jako VPN budou chráněny šifrováním IPSec.

Inside

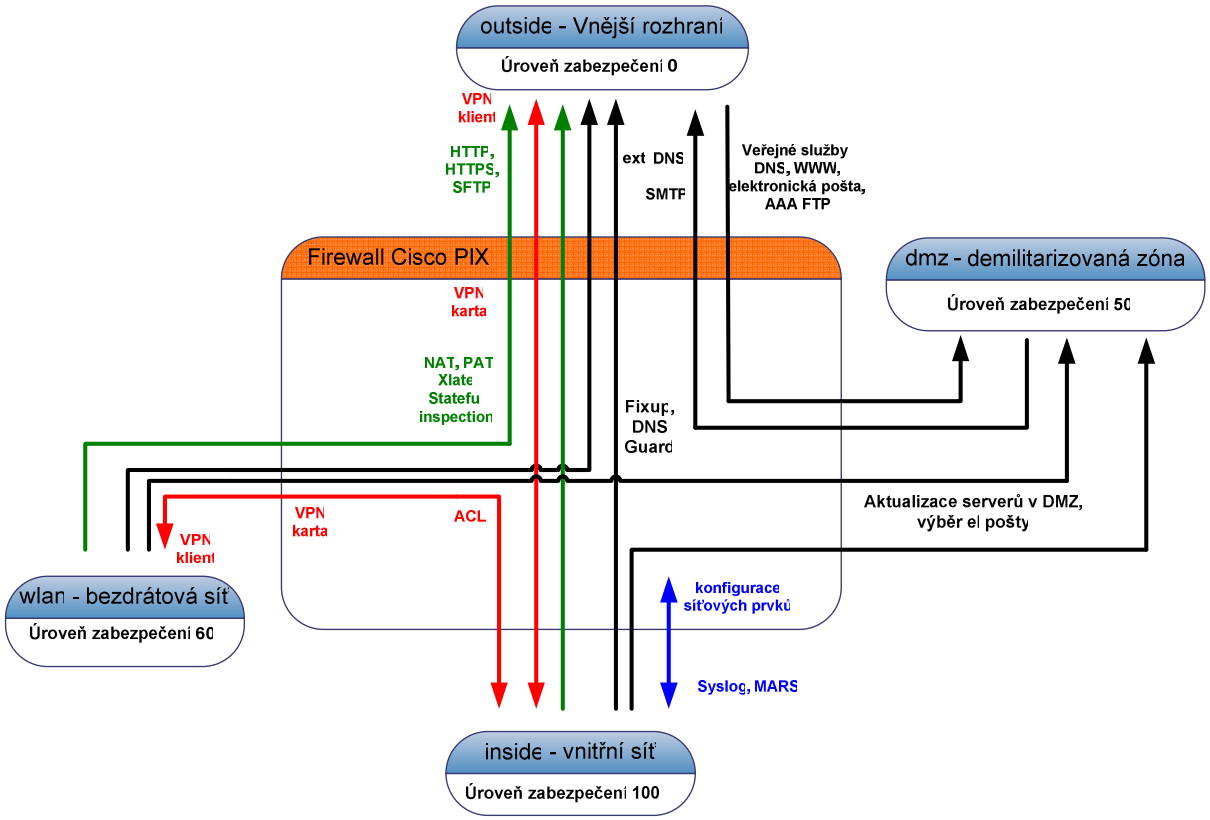
- Zóna inside je vnitřní podniková síť.
- Zóna je důvěryhodná.
- Na firewallech Cisco má nejvyšší bezpečnostní koeficient 100.
- Veškeré inicializované příchozí spojení do této zóny je zakázáno až na výjimky nastavené v access control listu ACL. Výjimky mohou být vzdálené firemní pobočky, podnikový partneři či pracovní stanice v rozhraních wlan a outside zabezpečené šifrováným přenosem VPN.
- z vnitřní sítě (inside) do outside budou povoleny běžné služby jako http, https, ftp, sftp, přičemž firewall každý pokus o nové spojení či relaci ukládá do dynamických zárodečných tabulek (embryonic), provede NAT a po úspěšném spojení (established) ukládá relaci do tabulky spojení (conn table), které pak zpřístupňují tok paketů přenosu TCP v obou směrech v definované udržované relaci.
- U nespojového UDP protokolu, který provozuje zejména DNS, je povolen provoz směrem ven a čekání na odpověď je ve firewallu implicitně nastaveno na 2 minuty. Odpověď musí přijít v daném časovém limitu a navíc musí obsahovat příslušnou zdrojovou a cílovou adresu, pro které byl požadavek DNS inicializován. Funkce DNS Guard po přijetí první odpovědi DNS nečeká na vypršení časovače a spojení rovnou ukončuje, tedy zahazuje i jiné odpovědi, které mohou být padělané útočníky.
- Navazování spojení aplikací jako SMTP, H323, RTSP budou poté podléhat inspekcím pomocí funkce **fixup**, která specifikuje použité porty.
- Do rozhraní inside tak budou mít pevně povolený přístup pouze vzdálené stanice VPN na základě přístupových listů ACL (kterým se vytvoří výjimky v provozu).
- Do rozhraní inside je také povolený přístup zpráv syslog vyhrazený pomocí ACL aktivních síťových zařízení (směrovače, firewally, IPS, IDS), které zprávy umí generovat.

Celkový přehled základních pravidel o inicializaci je zobrazen v tabulce III, kterou navíc vykresluje obrázek (obr. 3.3). Pravidla, která nejsou povolena jsou implicitně zakázána. V případě použití jiných protokolů, které by podnik využíval (zejména některé multimediální), se musí dodatečně povolit průchod ve správném směru mezi správnými

rozhraní. Pro některé multimediální protokoly je navíc potřeba zpřístupnit některé množiny portů. Ale čím víc je povoleno služeb a portů, tím míň je počítačová síť bezpečná.

Tab III: Základní pravidla rozhodování o inicializaci provozu .

Příchozí zóna	Odchozí zóna	Zdroj	Cíl	Služba	Akce
outside	dmz	jakýkoliv	www server	http, https	povolit
outside	dmz	jakýkoliv	poštovní server	smtp	povolit
outside	dmz	jakýkoliv	dns server	dns	povolit
outside	dmz	AAA	ftp server	ftp	povolit
dmz	outside	poštovní server	jakýkoliv	smtp	povolit
inside	dmz	firemní server	www server	ssh	povolit
inside,wlan	dmz	pracovní stanice	poštovní server	ssh	povolit
inside	dmz	firemní server	ftp server	ssh	povolit
inside,wlan	outside	pracovní stanice	jakýkoliv	http, https, ftp (AAA)	povolit
inside,wlan	outside	pracovní stanice	externí server DNS	dns	povolit
jakákoliv	inside	firewall,IPS,IDS	server syslog	syslog	povolit
inside	jakákoliv	server managementu	firewall, IPS, IDS	ssh	povolit, zaznamenat
wlan / inside	inside / wlan	pracovní stanice	pracovní stanice	VPN	povolit ACL
inside / outside	outside / inside	(vzdálená) pracovní stanice	(vzdálená) pracovní stanice	VPN	povolit ACL
jakákoliv	jakákoliv	established -conn table (response)	established -conn table (request)	jakákoliv	inspekce Xlate, povolit
jakákoliv	jakákoliv	jakákoliv	jakákoliv	jakákoliv	zamítnout, zaznamenat



Obr. 3.3: Křižovatka povolení navázání (inicializace) provozu ve firewallu PIX.

Access control list ACL

Zkratka ACL (access control list) označuje řízení přístupu na základě určitých pravidel. Jde tedy o seznam pravidel, které filtrují pakety na základě určitých parametrů. Tímto se zvyšuje nejen bezpečnost provozu v síti, ale i její propustnost. Každý seznam ACL se stahuje k základním parametrům rozhraní(eth0,eth1,atd.), směr(dovnitř,ven) a protokol (http, ftp, ssh, atd.). Seznamů můžeme vytvořit hned několik, který bude specifikovat pravidla pro dané určité rozhraní, směr a protokol. Seznam ACL může být základní nebo rozšířený.

Základní seznam ACL filtruje pakety na základě čísla seznamu ACL (ten identifikuje rozhraní, směr a protokol), splnění podmínek (permit/deny), zdrojové adresy (IP adresa stanice nebo sítě, která paket vyslala) a případně relevantní zdrojové masky (může být i any nebo 0.0.0.0). Pakety přídavným příznakem log můžeme zaznamenávat.

Rozšířený seznam ACL kromě filtračních parametrů základního seznamu umí navíc filtrovat pakety na základě cílové adresy (IP adresa stanice nebo sítě, které paket přijme), protokolu (tcp nebo udp) a cílové masky, cílového a zdrojového portu (název operátora např. http, ftp nebo číslo či rozsah např. 1234-1244) a dále dle příznaku established (spojení navázáno).

Vytvořené seznamy ACL ve směrovačích a firewallech je možné případně doplňovat o nové pravidla a záznamy, které se zapisují nakonec seznamu pravidel. Takto se staticky přidávají například nové vzdálené pobočky, stanice či stanice sítě WLAN. Rovněž se dají i odebírat již povolené pravidla či mazat celé seznamy.

3.1.4 Bezdrátový přístup WLAN

Dnešní podnikové sítě mají implementovány bezdrátové sítě WLAN (Wireless LAN). Mezi nesporné výhody patří mobilita pracovních stanic realizována zpravidla notebooky. Sítě wlan sebou nesou jistá rizika, která mohou být pro podnikovou síť nebezpečná.

Rizika WLAN

- Na AP (access point) se může teoreticky připojit kdokoliv, po prolomení bezpečnostních autentizace.
- Útok man-in-middle, který se například realizuje falešným AP a má za úkol získat MAC adresy legitimních klientů sítě, podrobněji v [5].
- Útoky DoS, realizovány například jako jamming (rušení přenosového kanálu), záplavy rámců, atd.
- Nezašifrovaný síťový provoz může být vystaven odposlechu.

Vzhledem k možným nebezpečím je vhodné tuto síť považovat za středně důvěryhodnou a přivést ji do sítě podobně jako demilitarizovanou zónu DMZ, ale s vyšším koeficientem důvěrnosti. Základem je vždy šifrovat provoz (pomocí VPN).

Dále také je vhodné tuto síť monitorovat, ke zjišťovaní falešných přístupových bodů. Například využitím přenosových skenerů, které naleznou všechny AP v dosahu a porovnáním výsledků s vlastním zmapovaným seznamem autorizovaných AP. Často se stane, že se zachytí signál z AP například sousední firmy, pak se stačí pouze ubezpečit, že se jedná o tzv. přátelský AP, který má sloužit jen sousedům zrovna jako naše AP pro naše potřeby. Toto také souvisí s prevencí, proti nechtěnému přidružení našich uživatelů k cizí sousedské WLAN. Čímž by tak mohlo docházet k úniku firemních informací, podrobněji v [10].

Dále je vhodné použití AP se směrovými anténami, stínění či pomocných reflektorů, tak aby signál neopouštěl prostory firmy, na které by se již neměl útočník se svým vybavením

fyzicky dostat. V neposlední řadě je řádná identifikace přítomných klientů. Monitorování anomálií. Záznamy a sledování uživatelských připojení. Například monitorovaní připojení klienta v neobvyklý čas (po pracovní době).

Tipy zabezpečení WLAN

- Vhodná infrastruktura – vymezení dosahu signálu sítě pouze na požadované a fyzicky zabezpečené okolí v areálu firmy, zabraňuje odposlechu a zachycení signálu útočníkem.

- Nastavit implicitního jména sítě SSID na co nejméně nápadné (softwarový generátor hesel) a pravidelně toto jméno obměňovat, nevysílat rámec Beacon s SSID. Tímto opatřením pak útočník musí hádat i SSID.

- Použít bezpečný přenos dat pomocí VPN. Při nepoužití VPN, zavést v síti WLAN nejlepší dostupný bezpečnostní mechanismus tj. WPA2/802.11i (vylepšené šifrování AES), popřípadě WPA podporující autentizaci, šifrování a integritu dat (dynamické klíče TKIP). Pokud dostupná zařízení v síti nepodporují výše zmíněné mechanismy, tak zavést alespoň vylepšený WEP (802.1x) o autentizaci a management klíčů díky autentizačnímu serveru RADIUS. V nejhorším možném případě zapnout WEP a nastavit na 128 bitový klíč (nejsilnější možný) a autentizaci nastavit na open, což je vhodné proti zachycení výměn výzev.

- Provádět vzájemnou autentizaci na bázi digitálních certifikátů EAP-TTLS nebo PEAP, jak uživatele, tak i přístupového bodu, za pomocí serveru RADIUS. Nastavit časový limit komunikační relace v závislosti na podnikové intenzitě přenosu dat.

- Nepovolovat sdílení důležitých souborů, adresářů a aplikací, které by v případném průniku do wlan sítě mohli být k dispozici útočníkům.

- Filtrovat MAC adresy pomocí speciálních seznamů ACL (pokusit se vymezit seznam použitých síťových adaptérů v podniku) je vhodné při odhalení IP adres útočníkem, filtrace IP adres, omezení DHCP, statické adresování.

- Zavedení authentizace klientů na základě vnitropodnikových identifikátorů, chrání především před odcizení a zneužití fyzického zařízení, které bylo používané v síti např. notebooku. Využívat jednu z několika metod authentizací typu EAP. Nejbezpečnější se jeví EAP-TLS či PEAP.

- Oddělení od podnikové sítě firewallem, použití brány VPN pro zvýšení ochranné vrstvy přenášených dat do bezpečné vnitřní podnikové sítě a podpora na AP VLAN (Virtual LAN) kvůli škálovatelnosti přístupů k síťovým prostředkům.

3.1.5 Zabezpečení vzdálených entit pomocí VPN

U středních podnikových sítí se vyskytují také vzdálené pobočky, obchodní partneři (stálý dodavatelé či odběratelé), domácí kanceláře a mobilní pracovníci v terénu. U všech zmíněných entit je obvykle požadovaný přístup do podnikové sítě pro zvýšení produktivity podniku. Jak situaci řešit, aby byl výsledek nejlevnější a nejbezpečnější, nám umožňuje VPN

(Virtual Private Network), viz obr. 3.4. Řešení jako pronajmutí pevných linek nebo okruhy frame relay do vzdálených pracovišť jsou dnes již zcela zavrhnutá především z důvodu vysoké ceny, která navíc roste se vzdáleností.

VPN naopak umožňuje spolehlivé a bezpečné připojení přes internet, který se hradí jen místním poskytovatelům služeb internetu, či telekomunikační společnostem na obou stranách přenosu. Navíc se může VPN snadno a mnohem levněji rozšiřovat až do určitého limitu kapacity VPN na hardwarovém vybavení v síti (firewall, směrovač, brána nebo-li koncentrátor VPN) implementované v síti. VPN běží na vrstvách aplikační (SSH), transportní (SSL), síťové (IPSec) a pro linkovou se používají protokoly PPTP a L2TP. Tyto protokoly byli vytvořeny vzhledem k agresivnímu prostředí internetu, na kterém se vyskytují potencionální útočníci, kteří mají metody pro odposlouchávání nezašifrovaných dat či falšovaní paketů. Tyto metody jsou podrobněji probírány v [5].

IPSec

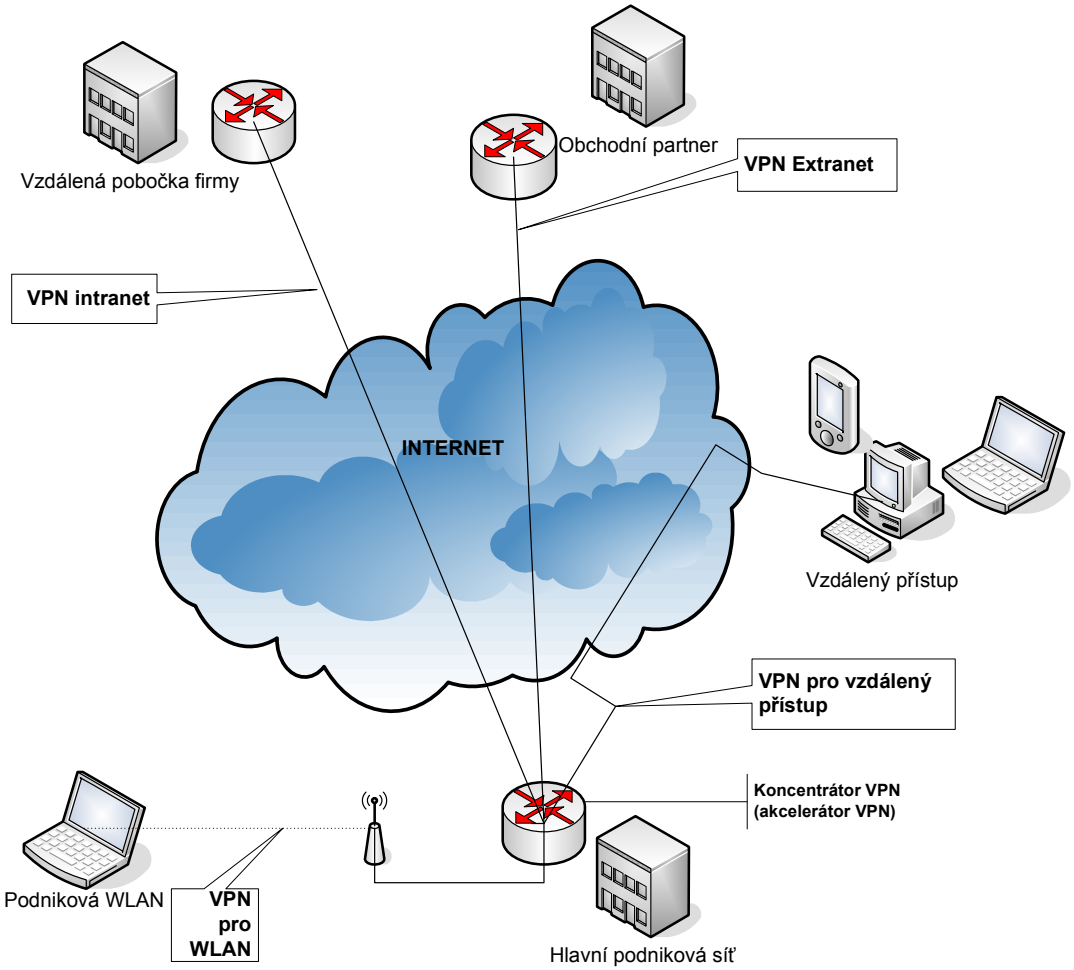
Virtuální privátní síť pomocí šifrovaní IPSec, tak vytváří ochranou obálku dat, které jsou přenášené přes nedůvěryhodnou síť internetu. VPN se rovněž použije i při přenosu ve WLAN síti, kde se mohou data snadno odposlouchávat. Proces, který zapouzdřuje jeden typ paketu do jiného, se nazývá tunelování. U IPSec máme možnost použít dva módy spojení. Jde o transportní a tunelující mód. Transportní mód se používá ve spojení s protokolem L2TP a šifruje pouze data, ale ne původní hlavičku IP, čímž se stává méně bezpečným vůči tunelujícímu módu, který šifruje, jak data, tak i hlavičku přenášeného IP. Protokol IPSec pracuje na síťové vrstvě a ve VPN nám zajišťuje:

-šifrování dat a informací TCP/IP
-integritu dat
-autentizaci
-ochranu proti opakování relace

IPSec spolupracuje s protokoly ISAKMP, ESP a AH. ISAKMP (Internet Association nad Key Management Protocol) se stará o fázi dohody spojení a o výměnu klíčů, nastavuje tzv. bezpečnostní asociaci SA (Security Association). Podporuje protokol IKE (Internet Key Exchange), který zajistí dohodu klíčů, autentizaci partnerů, správu klíčů a jejich výměnu. Po úspěšné autentizaci a dohodnutí partnerů na typu šifrování se použijí protokoly ESP nebo AH (po případě obojí), které přenášená data chrání proti opakovaní relace přidáním sekvenčního čísla do každého paketu a zajišťují jejich důvěrnost šifrováním pomocí algoritmů DES, 3DES či IDEA. V případě VPN procházející internetem je vhodnější využívat protokol ESP, který v tunelujícím režimu spolehlivě spolupracuje s mechanismem NAT. Případná kombinace ESP a AH je sice o něco bezpečnější, ale také finančně náročná, díky konfliktům s mechanismem NAT. Jelikož frewally Cisco (PIX, ASA) podporují IPsec, nemají problémy s NAT.

OpenVPN

Open source SSL VPN, nebo-li OpenVPN je novodobou náhradou za IPSec. Je vyvinut internetovou komunitou (open source). Vytváří zabezpečené šifrované spojení pomocí kryptografických knihoven a protokolů SSL/TLS v jednom balíčku. OpenVPN narozdíl od IPSec, který je až příliš komplexní, není tak náročný na implementaci v síti a funguje na bázi tunelů či klient - server. U firem a komerčních společností se musí platit licence za komerční verzi. Více o OpenVPN viz [14].



Obr. 3.4: možnosti bezpečného připojení VPN

Zabezpečení pomocí VPN

- Provést řádné plánování o počtu VPN relací v celé síti a pořídit vybavení s dostatečným počtem VPN i pro případné budoucí rozšiřovaní.

- Provést přípravy na protokol IPSec či OpenVPN na všech použitých zařízení v síti dle jednotlivých manuálů pro zařízení.

- Provést počáteční výměnu sdílených klíčů s partnery a segmenty v síti, nepoužívat stejné klíče pro více partnerů. Případně využít certifikační autoritu CA či DNSSec, která přiděluje unikátní digitální podpisy. Díky lepší škálovatelnosti je CA vhodné pro větší počet partnerů VPN.

- Provést dohody o jednotlivých parametrech o šifrování, hash, autentizace a doby života u asociací SA s ohledem na parametry jednotlivých zařízení a partnerů.

- Vytvořit na firewallu a směrovači rozšířené přístupové seznamy (ACL), které povolí navázaní spojení vzdáleným stanicím do vnitřní sítě.

- Transformace IPSec (vytvoření transformačních množin bezpečnostních protokolů – v internetovém prostředí použít ESP), dohoda na tunelujícím režimu.

- Vytvořit šifrovací mapy (nadefinovat který provoz bude procházet ochranou IPSec, určit vzdálené partnery, na jednotlivé provozy nadefinovat transformační množiny, upřesnění SA jako např. dobu života, druh zavádění(manuální/výměna IKE), atd. dle možností příslušného zařízení).

- Stejným způsobem nastavit záložní (alternativní) brány VPN zvláště u důležitých partnerů.

- Testovaní funkčnosti VPN a kontrola celkové konfigurace IPSec.

3.1.6 Zařízení IDS a IPS

Zařízení IDS (intrusion detection system) má v síti za úkol monitorovat a analyzovat podezřelé chování a nejrůznější anomálie. Sondy či moduly IDS ověřují kopie datového síťového provozu, který je zpracován paralelně a detekují možné hrozby. Zařízení jako směrovače a firewally, které mají vnitřní moduly IDS mohou ověřovat i přímo provoz (sériově). Při detekci určité hrozby, buď předavají varovaní správci, který podnikne případné protiopatření, nebo u sofistikovanějších zařízení se IDS pokusí řešit problém samostatně, které již jsou definovány jako zařízení IPS(intrusion protection system, někdy se objeví i slovo prevention).

Systémy IDS se rozhodují na základě signatur. Tyto signatury mohou korespondovat s běžnými známými útoky, které systém již zná, či může vyvozovat nové typy na základě odchýlení od běžného síťového provozu či určité anomálie. Výrobci mají profesionální povinnost poskytovat signatury o nových útocích svým klientům.

Existují i obecné signatury, které často budou vyvolávat falešné poplachy, ale někdy také zareagují na skutečnou hrozbu. Je tedy otázka jak nastavit prahy citlivosti, které vhodně kombinují skutečné hrozby od těch falešných. Při použití více senzorů v síti na jednotlivé hlídané segmenty, lze nastavit senzory na odlišné prahy citlivosti dle specifických chování v daném segmentu, které pak generují různé počty výstrah. Výhoda je také rychlejší nalezení problému či průniku.

Několik možných alternativ zařízení IDS od různých výrobců: Cisco NIDS 3.x, 4.x, Network IDS module 3.x, 4.x, Enterasys Dragon NIDS 6.x ISS RealSecure Network Sensor 6.5, 7.0, Snort NIDS 2.x, McAfee Intrushield NIDS 1.x, NetScreen IDP 2.x, OS 4.x, 5.x, Symantec MANHUNT

implementace IDS do firemní sítě

- Použít více senzorů. Umístit hlavně senzory před a za síťový firewall i paketový filtr, poté také do jednotlivých segmentů v síti (DMZ, interní sít, WLAN, management).

- Senzory vyladit dle specifik typického provozu v každém segmentu (omezit nadměrné výstrahy).

- Možnost použití více senzorů v přetíženém segmentu je žádoucí kvůli rozdělení hlídaného provozu.

- Externí senzor, tedy za hraničním filtrem, omezit na vyhledávání útoků DoS.

- Kontrolu šifrovaných přenosů VPN zajistíme umístění senzoru přímo za zařízení VPN brány (Firewall, VPN koncentrátor, Směrovač podporující VPN, atd.).

- Implementace IPS ve firewallu jako jsou zejména zařízení Cisco ASA a FWSM, či některé typy PIX (501-535) dává velkou časovou výhodu a blokuje útoky (zahazuje pakety) dřív než se dokáží realizovat, potlačují tak delší zpětnou vazbu u senzorů mimo firewall (provádí reset relace TCP, nebo překonfigurují příslušné síťové zařízení).

- Senzory mimo firewall usnadňují lokaci problémů (počet senzorů je otázka finančních prostředků, sledovat alespoň rizikové lokace DMZ, WLAN a management).

- Kombinace se softwarovými IDS na hostitelích se bezpečnost jen vyztuží.

- Vyladění závažnosti útoků (omezení množin signatur) vzhledem k zátěži provozu a hodnotám dat a zařízení v určitých segmentech.

- Schopnost rozhodnutí zda-li může útok ohrozit prvky v segmentu (útoky na neexistující zařízení nebo na nepoužívaný operační systém nebudou výstrahou, ale jen logovány) přináší technologie Cisco Threat Response, tímto se sníží falešné poplachy.

3.2 Nastavení bezpečnostní politiky

Již od počátku vzniku firmy či jisté organizace bývají sepsány pravidla a zásady pro chod firmy, které se týkají rozdělení správních úkolů, povinností a omezení či vyhrazení přístupů. V dobách kdy ve firmách nebyly implementovány počítače, se tyto omezení týkali především fyzického omezení přístupu.

V dnešních dobách, kdy se téměř všechny data, objednávky, technologické postupy, evidence a jiné užitečné údaje zpracovávají prostřednictvím výpočetní techniky a distribuce se zprostředkovává počítačovou sítí a internetem, roste nebezpečí nepovoleného a nežádoucího přístupu k citlivým informacím. Proto se nestačí bránit pouze díky aktivních síťových prvků a zabezpečených VPN, které zabraňují nepovolenému přístupu hlavně z vnějšího světa, ale je také zapotřebí chránit cenné a důležité informace i vůči vnitřním nepovolaným uživatelům.

Základem je rozdělení působnosti a udělování práv různým skupinám uvnitř podniku. Přidělování hesel a přístupových práv, se vymezí povolené pracovní prostředky pro každého uživatele ve firmě.

Dále je třeba vymezit seznam pravidel zákazů a povolení, které se budou stahovat na zaměstnance podniku a na jejich pracovní zařazení do firemních oddělení. Případné přestupky a porušení pravidel, které se dají zjistit prostřednictvím monitorování sítě, bude řešeno dle sepsaných sankcí. Níže je uvedeno několik zásad pro práci s heslem, autentizační a autorizační funkce pro síťové prostředky a režimy přístupu.

3.2.1 Režimy přístupu

V každé firmě existuje jistá stromovitá struktura postavení a zařazení pracovníků a daných oddělení. Ve firmě se tedy nachází různé skupiny, které vyžadují různé síťové služby.

Např. vedoucí výrobních provozů vyžadují přístup do různých databází, které se týkají nových objednávek, stavů potřebného výrobního materiálu a technologických dat. Naopak např. oddělení zpracování objednávek a prodeje požaduje přístup navíc k webovému serveru, díky kterému si zákaznici objednávají požadované zboží či služby. Management, pak např. vyžaduje přístup k celkovému auditu chodu dané firmy (všechny používané servery), pro efektivní plánování a sledování hospodaření podniku. Je tedy vidět, že každé oddělení vyžaduje určitý rozsah prostředků, které není předmětné více rozebírat v tomto návrhu. Základní přehled obecným oprávnění přístupu k síti je naznačena v tab. IV, kde jsou pouze doporučené parametry a v praxi se mohou lišit. Firemní oddělení rozdělujeme buďto pomocí fyzického rozdělení sítě díky jednoduchému směrovači nebo vytvoření virtuálních sítí VLAN, které vytvoříme např. v inteligentním směrovači (Cisco Catalyst).

Při více softwarů (Windows, Unix, MacOS) na jednotlivých terminálech v síti je vhodným síťovým softwarem Novell NetWare, který nabízí vzdálený přístup(WWW, Novell client, nativní přístup či sftp) na základě přístupových jmen/hesel a vyhrazených oprávnění k jednotlivým serverům ve stromové databázi NDS/e-directory. V dané struktuře lze pak nastavit určitou hierarchičnost, která povoluje daným skupinám prostředky (sdílené datové servery, tiskárny a jiné síťové zařízení) pomocí zařazení do daných kontejnerů a koncových objektů (listů). Novell eDirectory má tyto výhody hierarchičnost, distribuce, globálnost a multiplatformost. V dnešní dobách se používání Novellu snižuje. Mezi častější síťové operační systémy patří Windows (NT, 2003, 2008) či Unixové distribuce a odnože.

Tab. IV: Třídy pracovního oprávnění přístupu k síti na základě subjektivního doporučení

režim přístupu	**přístup k prostředkům**	**požadavek na složitost hesla/cyklus změny**		**sankce za porušení pravidel či zneužití proti firmě (praktická ukázka)**
řadoví pracovníci	omezený na používané aplikace, přístup k používaným síťovým zařízení(tisk,fax,VoIP)	nižší / 1 x za rok		nízké (nižší pokuty)
vedoucí a pověření pracovníci	omezený na používané aplikace, přístup k používaným síťovým zařízení(tisk,fax,VoIP) a k příslušným firemním datovým serverům	střední / 2 - 4 x za rok		střední (vyšší pokuty)
administrátor skupiny	přístup a konfigurace neomezený v dané skupině na všechny používané aplikace, datové servery, zařízení, nástroje a diagnostické programy, omezený v síti	vyšší / 4 - 6 x za rok		vyšší (degradace, vysoké pokuty)
hlavní administrátor (popř. skupina hlavních administrátorů)	neomezený ve všech skupinách a v celé síti, konfigurace aktivních síťových prvků, správa hesel, AAA a serverů SYSLOG	vyšší / 12 - 24 x za rok		nejvyšší (vyhazov)

3.2.2 Autentizace, autorizace a účtování technologie AAA

Proces autentizace stanovuje totožnost uživatele a ověřuje platnost zadaných informací (uživatelského id + uživatelské heslo). Při správnosti zadaných autentizačních parametrů přidělí autentizační server určitý rozsah oprávnění, tedy provede se autorizace. Při využívání určitého rozsahu operací a práci v systému se uživatelova činnost monitoruje, nebo-li účtuje (accounting). Technologie AAA je tedy zkratkou Authentication, Authorization and Accounting.

Moderní firewally tuto službu poskytují svým uživatelům a tato funkce nechybí ani ve firewallech cisco PIX či ASA. Základní přístup k PIX firewallu je založen na ip adresách a příslušných portech. Klient pošle požadavek přístupu k určité službě do firewallu PIX, který tvoří bránu mezi klientem a cílovou službou a který si zpětně vyžádá(dle typu služby) zaslání uživatelského id a hesla. Jakmile přijme PIX firewall vyžádané parametry, tak je posílá serveru AAA, kde se parametry porovnají a následně při správnosti hesla a id potvrdí. Na serveru AAA můžeme konfigurovat jednotlivé režimy přístupu pomocí softwaru CSACS (cisco secure access control server) a tím tak například povolit uživatelům vnitřní sítě, dle různých skupin, přístup na HTTP, FTP atd. Firewall cisco PIX podporuje průřezovou proxy autentizaci, která po ověření platného id a hesla uživatele na serveru AAA v databázi RADIUS či TACACS+, udržuje stav o toku relace mezi klientem a serverem služby.

Konfigurace mechanismů authetizace Cisco PIX firewallu

- Definovat skupiny kontrolních serverů AAA či server AAA.
- Vhodný výběr serverového protokolu.
- Zadat klíč na co nejsilnější hodnotu tj.127 alfanumerických znaků, tento klíč pak musí být shodný jak u klienta tak na severu TACACS+. Při nezadání klíče by komunikace byla nešifrovaná.
- Ve stejné síti můžeme povolit jen jeden typ protokolu a to buď RADIUS nebo TACACS+.
- Vytvořit záložní skupiny pro definované skupiny AAA a tyto zálohy umístit na jiné IP adresy serverů.
- Definovat služby pro dané skupiny, upřesnit pravidla a vytvořit výjimky.
- Nastavit časovače, pro dobu nečinnosti a pro dobu opakování autentizace. Dobu nečinnosti se doporučuje určit na několik desítek minut, např. na 20 minut. Časovač pro vyžádání opakování autentizace musíme nastavit na delší dobu např. na 3 hodiny.

Konfigurace mechanismů autorizace Cisco PIX firewallu

- Nadefinovat jaké služby budou pro dané skupiny zpřístupněny.
- Neuvedené služby jsou totiž často implicitně povoleny, je potřeba některé služby výjimečně zakázat, aby měli k nim přístup pouze oprávnění uživatelé.

Konfigurace mechanismů účtování Cisco PIX firewallu

- Aktivním účtováním sledovat přístup na důležité služby nebo na služby s cennými daty.
- Zaznamenávat délku připojení uživatele, množství přijatých a odeslaných dat.
- Sledovat určité skupiny a služby a prohlížet účetní záznamy je možné spuštěním volby **Reports and Activity** v navigační liště v **CSACS**.

3.2.3 Bezpečnostní šifrování, práce s hesly

Jakákoliv data, která jsou pro podnik cenná by se měla při svém přenosu šifrovat, zejména pak při přenosu nedůvěřivým prostředím (internet, WLAN, dmz). K tomuto můžeme využít zabezpečené virtuální privátní sítě VPN bezpečným IPSec (viz 3.1.5) nebo pomocí SSL či SSH. SSH nebo-li secure shell je bezpečné zašifrované spojení (přenos souborů a jednotlivých aplikací) ke vzdálenému shellu (příkazovém interpretu).

Standardní SSH je silně šifrované spojení od klienta ke vzdálenému serveru. Mezi nejznámější bezplatné softwarové klienty patří PuTTy a OpenSSH. Na straně firmy je třeba potom zajistit server SSH, např. na mnoha unixových systémech je již ssh démon implicitně nainstalován. Dále by se tyto servery měli pravidelně aktualizovat a doplňovat nejnovější záplaty, jelikož jsou oblíbenými cíli pro mnoho útočníků.

Nejčastější šifrovací metodou je však SSL, která je webově orientovaná. V internetových prohlížečích se označuje malým zámkem ve stavových lištách. Data protokolu HTTP (port 80), které jsou šifrovány pomocí SSL se označují HTTPS a běží nad TCP portem 443. SSL dále šifruje i protokoly SMTP, NNTP, LDAP, IMAP, POP3 nad TLS/SSL a také obsahují přídavné S např. POP3S. Klienty SSL jsou internetové prohlížeče či běžné různí poštovní klienti.

U SSL serverů je zapotřebí zavést digitální certifikáty tj. vygenerovat dle hesla dvojici veřejných klíčů a u libovolné spolehlivé certifikační autority CA nechat podepsat žádost, která veřejný klíč obsahuje. Certifikační autorita (v ČR Česká pošta, ICA) na základě podpůrných informací ověří platnost žadatele a poté digitálně podepíše veřejný klíč a tím vygeneruje digitální certifikát. Digitálně podepsaný veřejný klíč (digitální certifikát) zašle zpět administrátorovi, který ho poté nainstaluje na server SSL.

Navázání provozu SSL (SSL handshake) pak probíhá na principu asymetrické šifry pomocí veřejného a soukromého klíče:

1. Klient→Server -požadavek o spojení SSL +info(verze SSL, nastavení šifrovaní, atd.)
2. Server→Klient -info(verze SSL, nastavení šifrovaní, atd.) + dig.certifikát serveru
3. Klient -díky certifikátu, který obsahuje veřejný klíč, ověří autentičnost serveru
4. Klient -vygeneruje základ šifrovacího klíče, kterým se bude šifrovat následná relace
5. Klient→Server -odešle základ šifrovacího klíče zašifrovaný veřejným klíčem serveru
6. Server -svým soukromým klíčem rozšifruje základ šifrovacího klíče
7. Klient a Server -ze základu vygenerují hlavní šifrovací klíč
8. Klient ↔ Server -vzájemné potvrzení hlavního šifrovacího klíče
9. Klient ↔ Server -šifrované spojení (konec handshake SSL)

Doporučení SSH

- používat novější SSH2 (bezpečnější než SSH)
- nastavit počet neúspěšných pokusů přihlášení v jedné relaci na 3
- umísťovat SSH server do DMZ a zavést tak dvojí autentizaci, příkladem je bezpečný přenos souborů serveru SFTP
- při použití tunelů SSH se vyhýbat vnoření tunelů do sebe, které pak díky složitosti výpočtů zpomalují komunikaci
- používat souborový manager WinSCP, který pracuje v režimu SFTP a SCP

Doporučení SSL

- u použití certifikátů pro vnější prostředí(internet) je třeba využít známou a spolehlivou certifikační autoritu CA
- u použití certifikátů pro vnitřní prostředí(firemní síť, wlan) je možné využít vlastní certifikační autoritu CA
- pro citlivé údaje použít minimálně 128 bitovou šifru (nutné je také upozorňovat uživatele na danou silnou šifru z hlediska kompatibility)
- podporovat SSL 3.0 a TLS 1.0
- při použití tunelů SSL se vyhýbat vnoření tunelů do sebe, které pak díky složitosti výpočtů zpomalují komunikaci
- implementace SSL u klientů POP a IMAP nemusí být implicitně povolena a v případě použití SSL pro bezpečnou poštu je třeba tuto službu zapnout
- u webových stránek podniku omezit šifrování dat na důvěryhodné informace (objednávky, finanční transakce, registrace atd.), naopak není třeba šifrovat data jako nabídku zboží, informace o službách atd. (pro útočníky tyto data nemají žádnou cenu)

Kryptografie na síťové vrstvě

Jak již bylo zmíněno, šifrování nad nedůvěryhodnou sítí je pro cenné data přímo povinností. Při zvyšování délky šifrovacího klíče rostou také výpočetní nároky a tudíž se snižuje šířka přenosového pásma. Je tedy nutné nalézt vhodný kompromis bezpečnosti a výkonu.

Vzhledem k dnešním rizikům prolomení šifrování dat pomocí hrubé síly, je vhodné data, které mají dlouhodobě cenný charakter, šifrovat pokud možno co nejbezpečněji. U dat, které jsou cenné jen dočasně např. vyřízení objednávek, aktuální úkoly, atd. je vhodné použít algoritmy s menšími klíči, čímž se podstatně zvýší rychlost přenosu. U sítí VPN je proto vhodné používat hardwarové akcelerátory s podporou kryptografických algoritmů VPN pro zvýšení rychlosti, které jsou rychlejší než obecné procesory. Některé nejznámější algoritmy spolu s velikostí jejich klíče jsou shrnuty v tab. V.

Tab. V: Přehled velikosti klíčů pro algoritmy se symetrickým klíčem

algoritmus	velikost klíče
RC4	40 bitů
FWZ-1	48 bitů
DES	40 nebo 56 bitů
3DES	168 bitů
AES	násobky 32 bitů: 128, 192 nebo 256 bitů
Twofish	128 bitů

Práce s hesly

Jednoduchá hesla nebývají pro útočníky již žádným problémem. Existuje spoustu programů, které lámou hesla na základě slovníkových databází, či těch složitějších na základě permutačních metod. Hesla obecně tvoří poslední obranou linii pro útočníky při průniku na různé účty či aplikace.

Ohledně stanovování hesel má firma obecně dvě základní řešení. Buďto bude svým zaměstnancům hesla generovat, přiřazovat a měnit v určitých časových intervalech. Nebo se

vypracují standarty pro vytváření hesel a pravidla, která budou kontrolovány. První možnost je přísnější, bezpečnější, ale neoblíbená a pro zaměstnance značně nepohodlná. Druhá možnost je pro zaměstnance přívětivější, ale je potřeba zajistit dohled nad volbami bezpečných hesel, vyžadovaných dle standardů. V obou případech je třeba poučit pracovníky, aby hesla nikomu neprozrazovala (ani nadřízeným či vysoce postaveným funkcím firmy, protože útočníci pomocí sociálního inženýrství se často vydávají za např. ředitele a žádají hesla po telefonu) a nezapisovala je (zvláště na email, papír, elektronicky např. word atd.). Vhodné je určit směrnice pro přidělování hesel na základě paměťové ztráty.

Uživatelské jméno je rovněž v mnoha případech bráno jako heslo. Útočník musí tedy pro průnik k účtu uhodnout i uživatelské jméno. To spolu s heslem tvoří dvojí ochranu a podstatně ztěžuje útoky hrubou silou. Avšak pamatovat si dvě tajná hesla je pro řadového zaměstnance často velkým problémem. Obecně je proto vhodné přidělovat uživatelské jména jako stálé identifikační čísla uvnitř firmy, které jsou pro externího útočníka neznámé, i přes zachycené jméno zaměstnance např. prostřednictvím vizitek. Uživatelské účty se takto i lepší zařazují z hlediska číselné povahy id zaměstnance. V tab. VI jsou uvedeny přibližné rozsahy a parametry hesel.

Poslední zásada, která navíc zvyšuje bezpečnost, je počet povolených špatných přihlašovacích údajů po sobě. Každý se občas splete a proto je vhodné nastavit vhodnou rezervu. Při celkovém počtu možných kombinací uživatelského jména a hesla je minimální pravděpodobnost, že by kombinace byla uhádnuta (slovníkovým útokem, permutační metodou) např. v prvních pěti či deseti povolených pokusech. Je třeba také ošetřit následné zablokování účtu na určitý časový interval např. na 2 hodiny, aby se útočník po neúspěšných pokusech nepokoušel hádat další kombinace ihned po zahájení nové relace.

Tab. VI: Doporučení nastavení a typů hesel a id na základě přístupu

režim přístupu	**požadavek na složitost hesla/cyklus změny**	**přístupové jméno**	**rozsah a typ hesla**	**pozn.**
řadoví pracovníci	nižší / 1 - 2 x za rok	známé firemní id číslo pracovníka	min. 5 – 10 alfanumerických znaků	u terminálů připojených k internetu heslo min. 8 alfanum.znaků
vedoucí a pověření pracovníci	střední / 2 - 4 x za rok	známé firemní id číslo pracovníka	min. 10 alfanumerických znaků	vedoucí s přístupem k firemním serverům by měli měnit častěji heslo
administrátor skupiny	vyšší / 4 - 6 x za rok	utajované firemní id číslo	min. 10 ASCII znaků(tj. použití znaků typu !@#$%^&*{}:”Aa4ř>?)	dodržování složitosti hesel zajišťují velké postihy
hlavní administrátor (popř. skupina hlavních administrátorů)	vyšší / 6 - 12 x za rok	utajované firemní id číslo	min. 10 ASCII znaků(tj. použití znaků typu !@#$%^&*{}:”Aa4ř>?)	dodržování složitosti hesel zajišťují velké postihy

3.3 Monitorování bezpečnosti sítě

Monitorování sítě je účelným prostředkem jak vyhledávat zranitelná místa, odhalovat pokusy o útoky hackerů, či přímo jejich strategie. K tomuto zavedeme do sítě nástroje jako systémy IDS, které mohou být realizovány hardwarově prostřednictvím sond, které naslouchají síťovému provozu. Softwarové IDS jsou často součástí AV softwaru. Existují i samostatné produkty, které fungují podobně jako síťové analyzátory a reagují na nepřirozené jevy odchylující se od normálního provozu, tak i na známé projevy útoků popsány signaturami.

Monitorování pomocí IDS ve více segmentech určuje rychleji ohniska vyskytnutých problémů či útoků. Nástroje pro odhalení strategií útoku na sítě odhalují tzv. návnady (honeypots). Což jsou stanice, které umožní snadnější přístup pro útok, ale neobsahují důležité či postradatelné data. Sledovat stav sítě se také vyplatí i s různých diagnostických důvodů. Můžeme tak například odhalit tvoření front paketů v úzkém hrdlu v síti, které tvoří firewall či hraniční směrovač. Dále máme možnost odhalit porušení bezpečnostních pravidel vnitřní sítě. Sledování sítě můžeme realizovat prostřednictvím zachycených výstrah, které se shromažďují na serverech syslog. Jednou za čas by se také měli provádět kontroly a testování, které odhalují slabosti v síti a nechtěné pozměněné konfigurace na hostitelích, které se za provozu mohou přihodit.

Jestliže chceme pohodlně a komplexně sledovat síť a vyhodnotit její zranitelná místa, je vhodné použít výkonný a účinný nástroj **Cisco Security Monitoring, Analysis and Response System** (**MARS**). Toto zařízení přináší hlavně:

- inteligentní sběr informací, jejich zpracování v reálném čase, ukládání do databáze a komprimaci.
- kontextovou korelaci (technologie ContextCorrelation™), která zajišťuje detekce anomálií s pomocí Netflow, korelaci událostí podle chování a definovaných pravidel(možnost uživatelské editace).
- vizualizace topologie sítě a topologie útoku, účinné potlačení útoku
- spolehlivou analýzu útoku, technologie SureVector™ pro zobrazení útoku
- blokování útoku aktivní konfigurací prvků síťové infrastruktury (funkce AutoMitigate™), výhodou je podpora konfigurovaných zařízení i od jiných výrobců než Cisco (Generic, Symantec, Nokia, Checkpoint Firewall-1, atd.)
- analýza útoku v reálném čase
- vytváření přehledných výkazů o incidentu (normalizované, uživatelsky definované)
- vysoký výkon a kapacita zařízení, rychlé nasazení technologie a široká podpora zařízení (heterogenní sítě)

Mezi nevýhody rozhodně patří finanční náročnost a možná nekompatibilita s některými staršími síťovými prvky či softwarem.

3.3.1 Softwarové systémy detekce vniknutí IDS a návnady (honeypots)

IDS mohou být realizovány hardwarově či softwarově. O hardwarových sondách, které jsou částí struktury sítě, buďto jako modul ve firewallu, či síťový prvek, více v části 3.1.6. Softwarové systémy detekce vniknutí IDS mohou být levnější alternativou. Softwarové IDS pracují podobně jako hardwarové, také na bázi signatur, ze kterých poté usuzují pokusy o útoky. Rozdíly je však v odposlechu dat, kdy hardwarové pracují buďto jako součást kvalitního firewallu (IPS) nebo na bázi sond, které odebírají veškerý zkopírovaný provoz pomocí zrcadlení portů na směrovačích.

Softwarové IDS jsou také umístěny na jednotlivých hostitelích. Sofistikovanější softwarový IDS, který je umístěn na pracovní stanici, může také dohlížet nad celým segmentem sítě. Je zapotřebí nastavit síťovou kartu do promiskuitního režimu, tzn. že síťovou kartou prochází veškerý provoz v daném segmentu ethernetu. Takto poté IDS může zachytávat veškerý provoz a upozorňovat na závadné pakety a případné útoky rekonstrukcí síťové relace. Tyto IDS, které nejsou propojeny se směrovači či firewally nedokáží sice ukončovat relace (TCP reset) nebo zamítat detekovaný škodlivý provoz přednastavením pravidel ve filtrech, ale mohou upozorňovat na dané problémy odesíláním zpráv do serveru syslog, popřípadě na mobil či email dohlížejících pracovníků, kteří na základě vyhodnocení závažnosti provedou opravy v aktivních síťových prvcích. Mezi doporučené produkty IDS patří Snort! dostupný z webových stránek www.snort.org a pro systémy Windows je vyvinut software IDScenter, který je grafickou nástavbou Snort!, který je napsán jako open source, čili pracuje v systémech unix, linux.

Honeypots (návnady)

Tyto prvky v síťové bezpečnosti, které jsou jistým druhem systémů detekce průniku IDS, můžeme realizovat různými způsoby. Nejzákladnější návnady jsou například terminály, které jsou umístěny např. demilitarizované zóně a čekají na podezřelou aktivitu.

Tyto terminály musíme naaranžovat takovým způsobem, aby se zdáli útočník důvěryhodné a aby pro ně měli naoko cenné informace. Ve skutečnosti je samozřejmě vybavíme falešnými informacemi. Aby byla návnada efektivní je potřeba do ní povolit veškerý příchozí provoz na firewallu. Základní návnady v podstatě by měli zaznamenávat jakékoliv skenovaní portů, tyto výsledky budou mít povolený průchod ven do odděleného a opevněného serveru syslog, aby v případě ovládnutí návnady nedostal útočník výchozí bod pro další průnik do sítě. Rozšířené návnady dokáží emulovat nějaký typ služby či množinu služeb, například falešný emailový server pro POP3 atd. obecně se ale doporučuje povolit z návnady do internetu služby FTP, DNS a ICMP. Nástrojem může být například program Specter.

Dalšími druhy návnad nemusí být přímo pracovní stanice, ale i cenné informace kdekoli na systému. Administrátor může například vytvořit falešný administrátorský účet, který má práva specifické pouze na bezcenné aplikace a prostředí dat. Tento účet bude poté monitorovat, čímž zpravidla odhalí průnik z vnitřního prostředí. Útočníkům může ještě předhazovat různé falešné hesla a protože se skenují všechny špatné přihlášení, odhalí tak že někdo má konkrétní zájem se dostat na jeho účet.

3.3.2 Sběr výstražných zpráv pomocí funkce Syslog

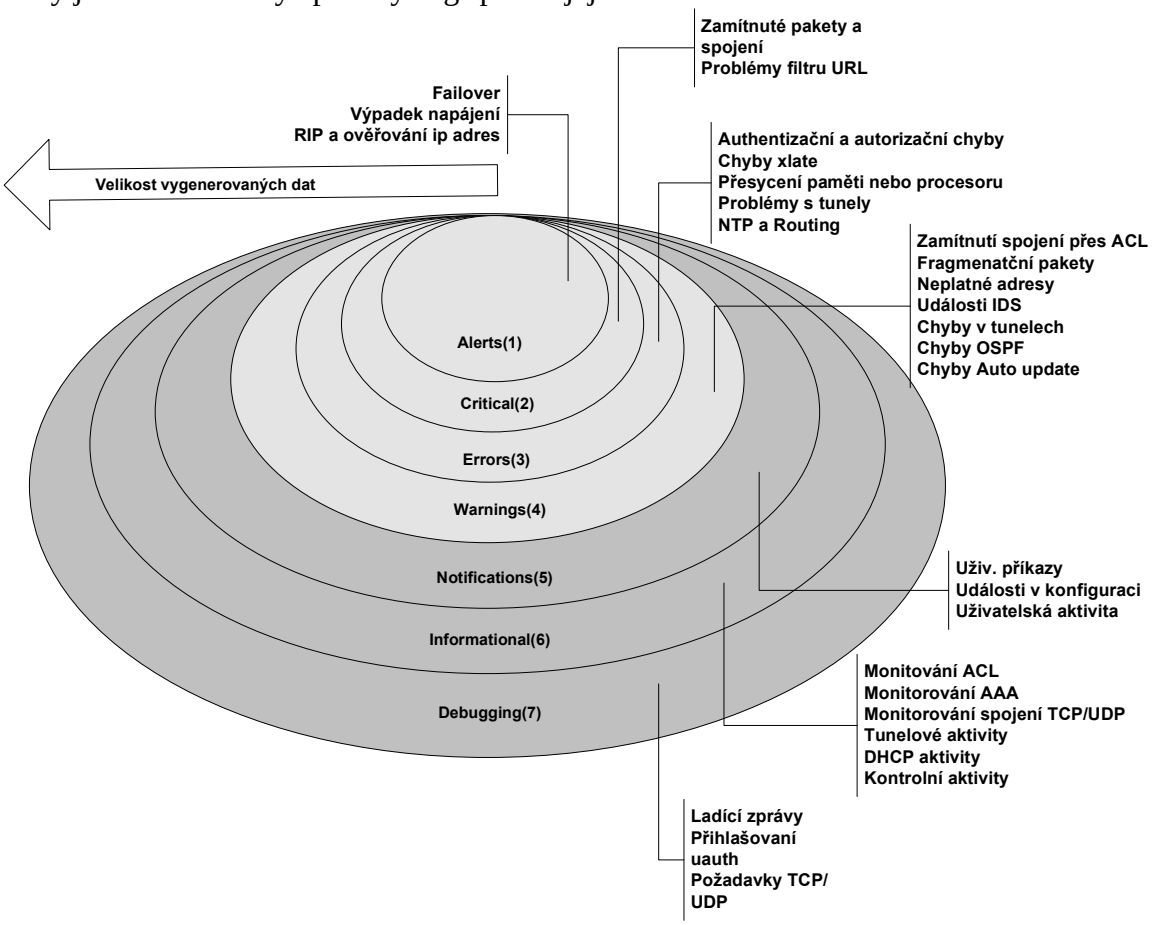
Funkce syslog zajišťuje sběr všech výstrah generovaní firewally, které se ukládají na zaznamenávací server umístěný nejlépe v oddělení správy sítě. Díky zprávám syslog máme přehled celkové činnosti síťového provozu, který protéká firewally. Zprávy uchované v serveru syslog slouží také jako důkazní materiál různých přestupků v lokální bezpečnostní politice.

Je potřeba však nastavit tuto funkci na určitou citlivost, tak aby se neukládala nepodstatná data a falešné výstrahy, které zbytečně zabírají místo na serveru. Server syslog také podporuje Kerio Personal Firewall v placené verzi, který je implementován na všech hostitelích. Je třeba jen nastavit IP adresu serveru syslog a port pro komunikaci. Použití více serverů pro jednotlivé oddělení (WLAN, management, interní sít) usnadní celkový dohled.

Firewally cisco (PIX, ASA) a hraniční směrovače cisco IOS rovněž podporují funkci zpráv pro server syslog. Jelikož hardwarovými firewally prochází veškerý provoz budou zde

vygenerované data nejobjemnější. Vhodné je použít servery z velkou kapacitou a na firewallech nastavit generování podstatnějších výstrah, jako například útoky DDoS, DoS, skenování portů atd.

Nastavení ip adresy serveru syslog u firewallu cisco PIX provedeme zadáním **logging host** inside ip-adresa. Příkazem **logging on** službu aktivujeme a příkazem **logging timestamps** aktivujeme přiřazení časového razítka dle vnitřních hodin na firewallu. Firewall cisco PIX generuje deset úrovní záznamu. Vzhledem k objemnosti provozu se doporučuje zapnout pouze závažné sdělení tj. nastavit **logging 3** a zachytávat tak zprávy typu o nepoužitelnosti systému (emergencies), výstražné zprávy (alert), kritické zprávy (critical) a chybové zprávy (errors). V případě dostatečných prostředků aktivovat **logging 4** a sledovat navíc varovné zprávy (warnings). Nicméně sledovat oznamovací, informativní a ladící zprávy je víceméně zbytečnou zátěží a doporučuje se jen ve výjimečných situacích (např. při provádění kontrol a testovaní bezpečnosti sítě v plánovaných období). Na obrázku 3.5 jsou vykresleny jednotlivé vrstvy zpráv syslog spolu s jejich obsahem.



Obr. 3.5: diagram zpráv syslog

3.3.3 Kontrola a testování bezpečnosti sítě

Vzhledem k vývoji technologií je kontrola a testování sítě nezbytnou rutinou. Testování sítě by mělo prověřit a odhalit slabá místa v podnikové síti. Průběžné kontroly by se pravidelně měli provádět nad celkovou integritou sítě až po jednotlivé hostitele v síti.

Mezi základní prvky patří nastavení pravidelných automatických antivirových testů a monitorování jejich výsledků. Dalším základním prvkem je občasná důkladnější revize v datech serverů syslog, před kterou je vhodné se seznámit s novými trendy síťových útoků, bezpečnostních narušení a novými škodlivými kódy, které bývají zveřejňovány na odborných

webech například www.cert.org a www.sans.org. Tyto kontroly by se měly provádět v určitých cyklech a také při implementaci nových síťových prvků, stanic či nového softwaru. Jako použité nástroje a pomůcky se doporučuje program Nessus (www.nessus.org), který odhaluje zranitelná místa na základě prověření určitého místa vzdálené sítě. Je třeba, ale specifikovat určitý port, komponentu či službu, která má být prověřena. Podobnými programy jsou ISS internet scanner (www.iss.net) a také retina (www.eeye.com), které jsou však komerční, avšak uživatelsky příjemné na ovládání.

Pro provádění komplexnějších kontrol, například se zásahy do konfigurací úzkých hrdel, jako jsou hraniční směrovače či firewally, u kterých se počítá s částečnými výpadky provozu sítě se doporučuje počkat na vhodnou dobu, ve které je síťový provoz co nejmenší, např. noční provoz.

Nicméně pro kompletní provedení auditu bezpečnosti se doporučuje využít externí profesionální firmu, která se danými věcmi denně zabývá. Tyto firmy vytváří posudky o bezpečnosti sítě a navrhují bezpečnostní protiopatření vůči nedostatkům, které se časem v síti vyskytnou.

3.4 Obranné opatření

Je nutné se připravit na situaci, při které dojde k výpadku činnosti firewallu. Jelikož firewall tvoří logickou křižovatku mezi rozhraními vnitřním, vnějším, dmz a wlan, je potřeba zajistit náhradní alternativu, tedy sekundární firewall, který převezme úkoly po výpadku primárního firewallu. Rovněž je nutné mít v záloze hraniční směrovač a zálohovaná konfigurační data. Výpadky systému IDS či IPS sice oslabí bezpečnost, ale nemají dopady na celkovou funkci sítě.

3.4.1 Havarijní stav (Failover)

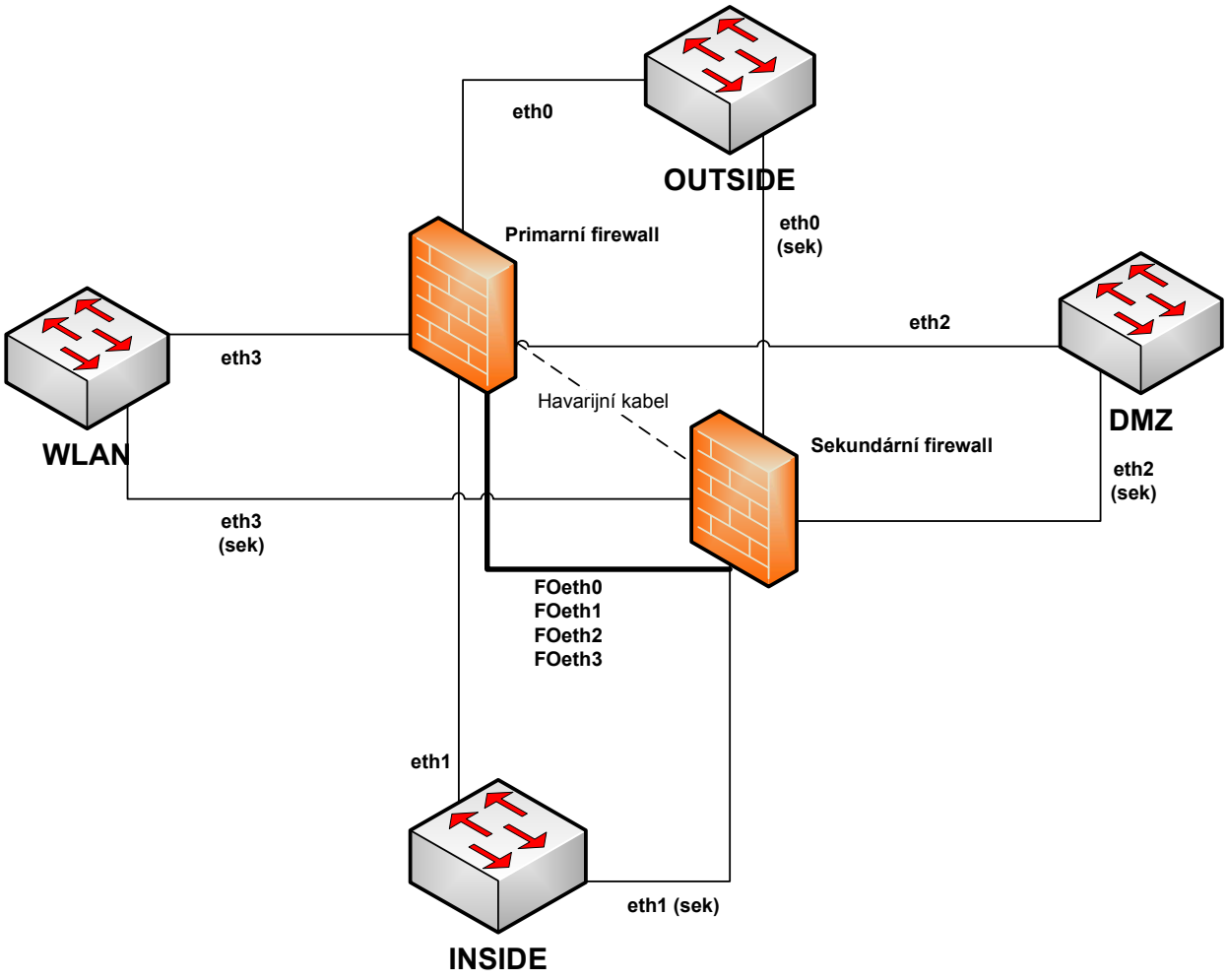
Při výpadku činnosti primárního firewallu přebírá veškerý provoz sekundární firewall. Funkce, která počítá s automatizovaným přebráním činnosti u firewallů cisco PIX, se nazývá failover. Mezi primárním a sekundárním firewallem se nachází kabel, po kterém probíhá základní spolehlivá komunikace mezi firewally. Mezi firewally se pravidelně posílají zprávy hello (keepalive, „jsem naživu“), adresy MAC, informace o stavu(aktivní/pohotovostní), stavy síťové linky a pravidelná synchronizace aktivního nastavení nebo-li replikace aktivní konfigurace.

Zprávy replikace aktivní konfigurace se posílají pouze u naprosto stejných typů firewallů se stejným softwarem. K výměně zpráv dojde při první konfiguraci a dále při konfiguraci za pochodu na aktivním firewallu se změny přenášejí zrovna i na sekundární, viz obr. 3.6. Je nutné u konfigurace za běhu systému zapisovat i na energeticky nezávislou paměť flash, která uchová aktuální konfiguraci i v případě energetické poruchy.

K dotazovacím zprávám dochází v intervalu 15 sekund a monitoruje se aktivita sítě, stav komunikace po kabelu havarijního převzetí a stav síťového napájení. Kontaktní pakety hello mají zasílací interval 3 až 15 sekund a změna implicitní doby se provede příkazem **failover poll** sekundy. Jestliže pohotovostní jednotka neposílá aktivnímu firewallu pakety prohlásí se za neprovozní. Pokud dojde k výpadku aktivní jednotky tzn. pohotovostní firewall neobdrží paket hello po třech po sobě jdoucích kontrolách, potom sekundární pohotovostní firewall přebere kontrolu a aktivní firewall je prohlášen za nečinný. Aby nedošlo ke konfliktu dvou funkčních zařízení, dochází ještě před přebráním kontroly k testům (Test stavu síťové karty, test síťové aktivity, test protokolu ARP a test PING). Kabel detekuje zapojení a přítomnost síťového napětí, proto při výpadku kabelu, firewall ještě nepřebírá provoz.

Doporučení ke konfiguraci havarijního převzetí

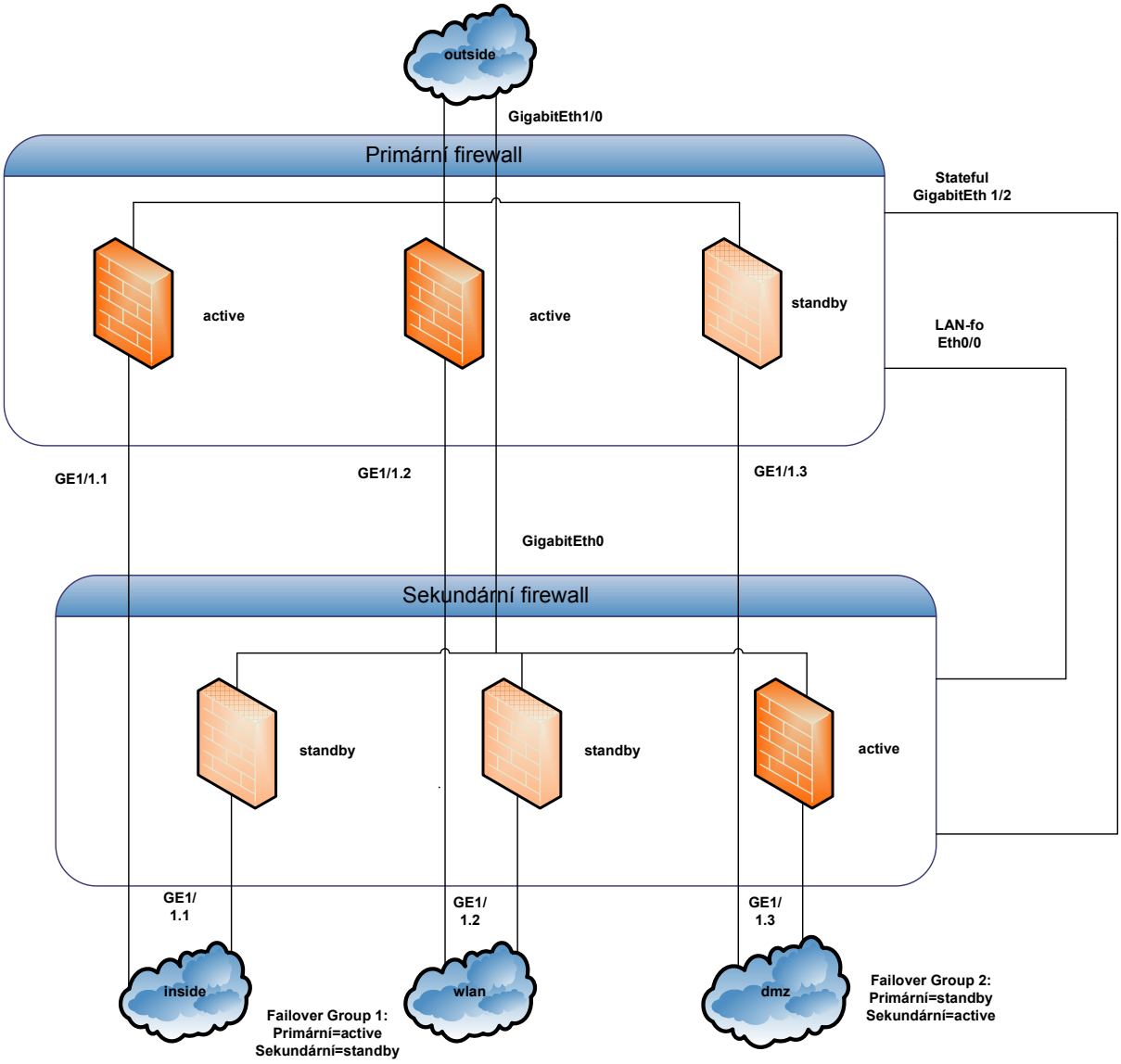
- Správně nastavit IP adresy aktivního a záložního firewallu např. pro vnitřní respektive (vnější) rozhraní primární IP adresa 10.0.0.1 (192.168.0.1), sekundární IP adresa 10.0.0.2 (192.168.0.2).
- Zkrátit dobu intervalu hello asi na 3 až 5 sekund, pokud je primární a sekundární firewall připojen k přepínači pracující na 2 vrstvě (který používá protocol SPT-spanning tree protocol), kde se očekávající interval zdvojnásobuje.
- Při častém zahlcování sítě je vhodné nastavovat dobu intervalu na vyšší dobu čili na 10 až 15 sekund, aby nedocházelo k falešným přebíráním provozu.
- Po opravě primární jednotky je nutné ručně přepnout aktivitu zpět na primární firewall příkazem **failover active** a nebo na sekundární jednotce **no failover active**.
- Pro stavové převzetí služeb, které uchovává otevřené relace TCP a síťový provoz je třeba spojit oba firewally kříženým kabelem kategorie 5, nebo rozbočovačem a přímými kabely cat 5, čímž se nadefinuje nové rozhraní rescue FOeth0, FOeth1, FOeth2, FOeth3.
- U návrhu s dražším firewallem ASA je výhodou zapojení active-active, kde se podílí na činnosti i záložní firewall (obr. 3.7).



Obr. 3.6: failover active-standby nastaven pro všechny 4 rozhraní

U firewallů PIX se podporovalo spojení active-standby (aktivní-záložní), ale u novějších firewallů cisco ASA (7.0 a více) a FWSM 3.1 se začala zavádět nová technologie

active-active, která umožňuje rozdělovat zátěž provozu mezi primární a sekundární firewall, viz obr. 3.7. Například hustější provoz do demilitarizované zóny je vhodné přenechat inspekcím provádějící se na sekundárním firewallu. Takto se jednotlivé kontexty rozdělí na primární a sekundární firewally pomocí příkazu **failover group 1**_nebo_**2**, kde se v případě havárie jednoho z firewallů přenese zbylá působnost na činný firewall. Tímto se tak potlačuje zdánlivá nečinnost sekundární jednotky. V anglických literaturách je rozdělení zátěže provozu příznačně označováno jako Load Balancing. Tuto funkci kromě některých modelů Cisco ASA a FWSM, taky podporují i jiné špičkové firewally, například SnapGear SG720, Sidewinter 210D nebo Juniper SSG 550, atd.



Obr. 3.7: failover active-active nastaven pro 4 rozhraní

4 Závěr

Jestliže chceme efektivně bojovat proti počítačovým virům, je třeba důkladně prozkoumat jejich možnosti škození a způsoby infiltrace a infekce, které jsou popsány v kapitole 1. Na základě těchto poznatků lze potom vytvářet účinná protiopatření a bezpečnostní software. V dnešní době se viry a jiné škodlivé kódy snaží nejčastěji o následující tři věci:

-zničit nebo znehodnotit data hostitele
-krást cenné informace s typickým úmyslem obohatit útočníka
-podsouvat hostiteli nevyžádanou reklamu

Na základě těchto poznatků vyplynou dva základní typy řešení bezpečnosti uživatelského počítače proti Malware, viz kapitola 2. Tyto řešení se vztahují k nejběžnějšímu operačnímu systému (Windows 2003/XP/Vista). Typ řešení I. je velmi variabilní a tím pádem se snažíme o co nejkompaktnější složení, co se týče poměru kvality a ceny. Je ale jisté, že v rozdílných sférách důležitosti dat a fungujícího systému, bude i poměr kvality a ceny, také logicky rozdílný.

Kromě základní konfigurace a nastavení bezpečnostního softwaru by měl administrátor sledovat vývoj nového potenciálního nebezpečí, které se šíří globální sítí internet. V důsledku toho by měl obstarávat nejnovější bezpečnostní záplaty od daných výrobců operačních systémů, antivirových programů a jiného softwaru a provádět pravidelné aktualizace.

V případě proniknutí škodlivého kódu do systému by měl mít v záloze určitý postup a sadu nástrojů, jak daný problém vyřešit. Tento postup by se pak skládal ze základních kroků:

-převzít zpět kontrolu nad systémem (ukončení činnosti viru)
-odstranění viru ze systému (proces léčení)
-zabezpečení daného zranitelného místa

Tyto kroky se řeší více způsoby a pro každý škodlivý kód rozdílně.

Ve firmách a organizacích, které ke své činnosti potřebují počítačovou síť, je nutné se bránit proti Malware již na hranicích sítě. Škodlivý kód, tedy moderní počítačový virus či neoprávněný přístup útočníka (crackera) nesmí dostat šanci k průniku do systému. Proto se do sítí implementují bezpečnostní mechanismy a zařízení, které pracují od linkové a síťové (proti průnikům) až po aplikační vrstvu (proti virům, spamům, spyware). Další pravidla, která zabraňují a omezují přístup k službám a prostředkům různým pracovním skupinám, chrání vnitřní informace a rovněž také zabraňují šíření virů a škodlivé činnosti v síti.

Konkrétní navrhované zabezpečení počítačové sítě pro střední firmu vychází z komponentů Cisco a opírá se o hlavní hardwarový firewall typu PIX. Dalším důležitým bezpečnostním prvkem ve struktuře je hraniční směrovač Cisco IOS, který má funkci paketového filtru. Díky základní filtraci paketů urychluje i činnost síťového firewallu PIX, který provádí zbylé inspekce. K hlavnímu firewallu je připojen i sekundární firewall PIX, který při poruše okamžitě přebere činnost v síti. Sondy IDS či IPS mají v síti dohled a vhodně reagují v případě rozpoznaného útoku. Tyto zařízení jsou také vybaveny antivir, antispam a antispyware moduly, které zpětnovazebně zabraňují vniku Malware a průnikům do sítě. Na citlivých místech v síti jsou rozmístěny návnady k odhalování pokusů o útok. Při práci se vzdálenými entitami (obchodní partneři, vzdálené pracovní stanice, pobočky atd.) jsou zavedeny virtuální privátní sítě VPN, které díky šifrovaní a autentizaci zabezpečují provoz přes nedůvěryhodný internet a WLAN, které jsou náchylné na cizí odposlech. Celkovou síťovou bezpečnost zvyšuje vymezení přístupu a práv pro jednotlivé účastníky v síti a dohled na používaní správných a těžce odhalitelných hesel. Důležité je také monitorování, nebo-li pravidelný dohled nad činností v síti a provádění testů a kontrol k určení zranitelných míst.

Seznam literatury

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

[2] Kerstin, Eisenkolb; Mehmet, Gökhan; Helge, Weickardt. Bezpečnost Windows 2000/XP Praha : Computer Press, 2003, 501 s. : ISBN: 80-7226-789-2.

[3] Szor, Peter. Počítačové viry - analýza útoku a obrana. Brno : Zoner Press, 2006, 608 s. : ISBN: 80-86815-04-8.

[4] Kocman, Rostislav; Lohniský, Jakub. Jak se bránit virům, spamu, dialerům a spyware. Brno : CP Books, 2005, 148 s. : ISBN: 80-251-0793-0.

[5] Scambray, Joel; McClure, Stuart; Kuntz, George. Hacking bez tajemství. Brno : Computer Press, 2002, 625 s. : ISBN: 80-7226-644-6.

[6] Chapman Jr., David W.; Fox, Andy. Zabezpečení sítí pomocí Cisco PIX Firewall. Brno : Computer Press, 2004, 337 s. : ISBN: 80-7226-963-1.

[7] Hucaby, David. Cisco ASA, PIX, and FWSM firewall handbook. Indianapolis : Cisco Press, 2008. xxv, 869 s.: ISBN: 978-1-58705-457-0.

[8] Strebe, Matthew; Perkins, Charles. Firewally a proxy-servery : Praktický průvodce. Brno : Computer Press, 2003, 450 s. : ISBN: 80-7226-983-6.

[9] Northcutt, Stephen; Zeltser, Lenny; Winters, Scott; Ritchey, Ronald W.; Kent Frederic, Karen. Bezpečnost sítí : Velká kniha. Brno : CP Books, 2005, 589 s. : ISBN: 80-251-0697-7.

[10] Pužmanová, Rita. Bezpečnost bezdrátové komunikace : Jak zabezpečit Wi-Fi, Bluetooth,GPRS či 3G. Brno : CP Books, 2005, 179 s. : ISBN: 80-251-0791-4.

[11] *Www.viry.cz* [online]. c1998-2007 [cit. 2007-09-06]. Dostupný z WWW: <http://www.viry.cz/go.php>.

[12] *Www.spammer.cz* [online]. c1998-2007 [cit. 2007-09-14]. Dostupný z WWW: <http://www.spammer.cz/go.php>.

[13] *Www.spyware.cz* [online]. c1998-2007 [cit. 2007-09-13]. Dostupný z WWW: <http://www.spyware.cz/go.php>.

[14] *Www.openvpn.net* [online]. 2008 [cit. 2008-04-21]. Dostupný z WWW: <http://openvpn.net/index.php>.

[15] *Www.ipcop.org* [online]. 2008 [cit. 2008-04-21]. Dostupný z WWW: <http://www.ipcop.org/>.

[16] Recenze a testy. *Prevence* [online]. 2006 [cit. 2006-04-27]. Dostupný z WWW: <http://www.viry.cz/go.php?p=viry&t=listrecenze>.

[17] *Http://m0n0.ch/wall/* [online]. 2003-2008 [cit. 2008-04-22]. Dostupný z WWW: <http://m0n0.ch/wall/>.

[18] *Http://www.cisco.com/en/US/products/hw/vpndevc/index.html* [online]. 1992-2008 [cit. 2008-04-22]. Dostupný z WWW: <http://www.cisco.com/en/US/products/hw/vpndevc/index.html>.