Barometr nebezpečí

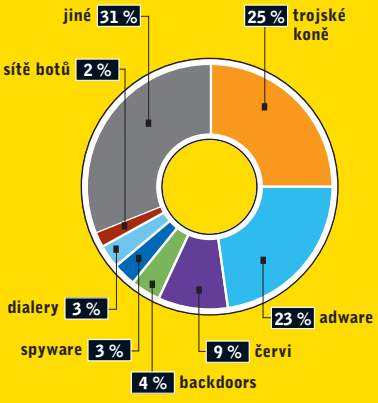
Se začátkem roku opět narůstají spamové a phishingové aktivity. Velkých vln červů se však není třeba obávat.

Hrozby roku 2008

1. Malware k olympiádě v Pekingu
2. Útoky na Mac OS, iPhone
3. Spam v blozích a fórech
4. Hacking sociálních sítí
5. Více infikovaných webových stránek
6. Portály jako cíl hackerů
7. Polymorfní javaskripty
8. Zašifrovaný malware
9. Phishing přes VoIP, Voice Spam

Nebezpečí nákazy narůstá. Letos se na mušce ocitly přístroje od Applu a Web 2.0.

Malwarové útoky



Na konci roku 2007 napadaly pécéčka převážně trojské koně a adware. Červů ubylo.

Odhalení: ZeuS – otec všech trojských koní

Je to vyděrač, lupič a špion v jednom. Tedy perfektní nástroj pro malwarovou scénu, něco jako univerzální trojský kůň. Jmenuje se ZeuS, ale pod tímto názvem je znám teprve krátkou dobu. Vypátraly jej výzkumy antivirových specialistů firmy Kaspersky.

Byl objeven jako gpcode.ai, trojský kůň, který v napadených počítačích zašifruje soubory a uvolní je až po zaplacení výkupného. Že se toho za „šifrovacím trojanem" skrývá ještě více, toho si experti povšimli na základě drobného detailu: gpcode.ai označuje svou přítomnost v operační paměti záznamem „_SYSTEM_64AD0625_". Tento řetězec se totiž vyskytuje v podezřele mnoha současných malwarových programech.

Univerzální kód: Malwarový program pro tisíc virů

V gpcode.ai tak výzkumníci odhalili jakýsi univerzální záškodnický kód, který může být nasazen pro nejrůznější účely. Kód je obsažen například v trojském koni Bancos.aam, který odcizuje přístupová data k bankovním účtům. Najdeme jej v červu Zhelatin, který se šíří prostřednictvím příloh elektronické pošty. A vyskytuje se celkem ve stovkách virů. Teprve analýza činnosti všech těchto škůdců nám osvětlí původ jména ZeuS: trojský kůň se do počítače nainstaluje jako ntos.exe a z webu pak zavede soubory zeus.exe a zupa.exe. Poté se přihlásí k síti botů (botnet).

ZÁKEŘNOST: Trojský kůň ZeuS nepozorovaně připojí nebezpečný odkaz ke každému příspěvku do internetového fóra, který uživatel vytvoří.

Výroba zombie: ZeuS začlení napadené PC do sítě botů

Agresivní špehovací úkol přebírá zeus.exe, zatímco zupa.exe je klient, který komunikuje s botnetovou centrálou a dostává od ní pokyny. Jedna z největších takto vzniklých sítí zahrnovala podle firmy Kaspersky přes 100 000 zotročených počítačů, než byla odhalena. Takové botnety jsou také výnosným obchodním artiklem, prodávaným často za hodně vysoké částky.

Že se ZeuS mezi autory virů etabloval jako komerční nástroj, tomu se vzhledem k jeho mnoha funkcím nelze divit. Program nejen krade přístupová data, certifikáty a hesla. Umí také odvést uživatele na phishingové stránky nebo doplnit do webových stránek infikovaná vstupní pole.

Jeho odhalení by však také mohlo znamenat jeho konec. Vývojář nástroje na jednom fóru prohlásil: „ZeuS už nebude dále prodáván, avšak podpora pro staré zákazníky je dosud k dispozici. Mnoho úspěchů všem."

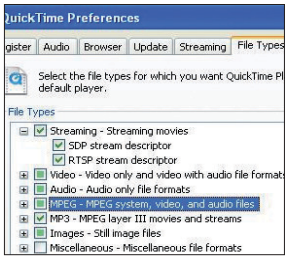
APPLE QUICKTIME 7.3

Mezery bez konce

Již v minulém Chipu jsme poukazovali na bezpečnostní mezery v novém QuickTimu 7.3. Toto téma musíme bohužel znovu otevřít, neboť Apple zřejmě stále ještě nemá problémy se svým mediálním přehrávačem pod kontrolou.

Nejnovější scénář: útočníci mohou v QuickTimu vyvolat přetečení bufferu. Stačí jim k tomu pouze zmanipulovat hlavičku streamu, který je vyslán protokolem RealTime Streaming Protokoll (RTSP). Na základě vzniklého „buffer overflow" lze pak do napadeného počítače propašovat libovolný kód. Postiženi jsou i uživatelé iTunes, neboť při jeho instalaci se zároveň nahrává QuickTime.

A je tu i vážný případ: na jedné pornografické webové stránce byl odhalen zmanipulovaný stream, který do počítače zavádí trojského koně. Mezitím tvůrci SecondLife varují před reprodukcí v portálu začleněných videosekvencí, neboť ty jsou také v QuickTimu přehrávají automaticky.



Opravu dosud Apple nedal k dispozici, proto je třeba zasáhnout vlastnoručně: v nastavení QuickTimu jednoduše dočasně vypněte RTSP streaming (viz obrázek).

Info: www.apple.com

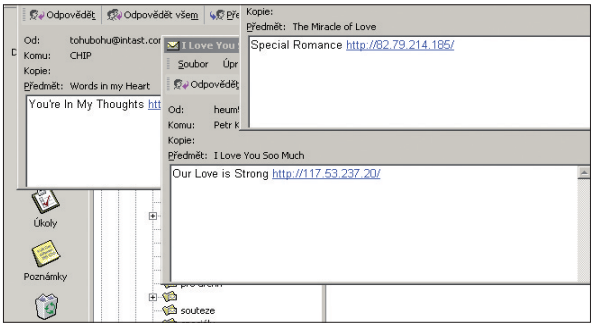
ÚTOK VIRŮ

Nebezpečný Valentýn

Virové laboratoře softwarové společnosti Eset zachytily už na konci ledna tisíce nových vzorků škodlivého červa z rodiny Nuwar. Tvůrci uvedeného červa změnili jeho kód tak, že se navenek již vůbec nepodobá předešlým variantám. S blížícím se příchodem svátku sv. Valentýna již autoři Nuwarů, pravděpodobně v rámci příprav na další z vhodných událostí pro podvody pomocí sociálního inženýrství, nasazují novou verzi, tentokrát s valentýnskou tematikou. Příkladem mohou být první e-mailové valentýnské pozdravy s textem předmětu či těla jako například „Sending you my love" nebo grafická úprava webové stránky, na které je umístěn kód červa se jménem with_love.exe s obrázkem růžového srdce.

Díky detekční schopnosti technologie ThreatSense, která tvoří jádro bezpečnostních produktů Eset, červa zachytává slovenský softwarový dům již od začátku jeho šíření pod názvem Win32/Nuwar. Velká většina významných konkurenčních antivirových produktů má zatím s jeho detekcí problémy. Po spuštění kódu červa Nuwar se infikovaný počítač stane členem botnetu, což je síť klientů (botů) ovládaných na dálku jejich správcem. Botnety jsou zneužívány k masovému rozesílání nevyžádané elektronické pošty a útokům typu DDoS.

Info: www.eset.cz



VALENTÝN: **Zázrak lásky, naše láska je silná a ty jsi má touha – virové vyznání...**

MALWAROVÝ ŽEBŘÍČEK

Top 10 malware, leden 2008

Společnost BitDefender zveřejnila žebříček Top 10 malware. Tomuto žebříčku vévodí škodlivé kódy využívající zranitelnosti grafického renderovacího jádra operačního systému Microsoft Windows. Zranitelnost popisuje bulletin společnosti Microsoft MS06-001 a byla odstraněna aktualizací SP2.

„Tato situace je pravděpodobně způsobena existencí velkého počtu neaktualizovaných verzí operačního systému Windows, většinou nelegálních. Uživatelé je neaktualizují, aby se vyhnuli nutnosti aktivace", komentuje tento fakt ředitel antivirového výzkumu společnosti BitDefender Sorin Dudea.

Top 10 malware		
1.	Exploit.Win32.WMF-PFV	9,6
2.	Win32.Netsky.P@mm	4,4
3.	Win32.Worm.Sohanat.AJ	4,0
4.	Trojan.Dropper.RNY	2,9
5.	Win32.NetSky.D@mm	1,4
6.	Win32.Netsky.AA@mm	1,25
7.	Trojan.Kobcka.CG	1,19
8.	Win32.Nyxem.E@mm	1,1
9.	I-Worm/Mytob	1,0
10.	Trojan.Pandex.AC	0,9
11.	Ostatní	72,26

Zdroj: BitDefender

Druhým nejrozšířenějším malwarem byl Netsky.P, který tak dokazuje neuvěřitelnou schopnost přežití tohoto viru. Pravda však je, že už se vyskytuje méně často než ve svých „nejlepších" dnech (4,35 % ve srovnání s více než 30 % v prvních měsících po vypuštění). Další verze stejného viru obsadily také nižší příčky žebříku.

NOVÉ ZASTOUPENÍ FIRMY

Trend Micro v České republice

Společnost Trend Micro Incorporated začátkem roku 2008 otevřela v Praze pobočku pro Českou a Slovenskou republiku. Otevření kanceláře vychází ze záměrů firmy decentralizovat řízení regionu CEE – centrální východní Evropy a přenést je z Mnichova do jednotlivých zemí regionu s cílem lépe uspokojit lokální potřeby svých zákazníků. Globální strategií firmy je posunout činnost Trend Micro od vývoje a prodeje bezpečnostních produktů a řešení k poskytování služeb v této oblasti.

Nová bezpečnostní rizika

VLC MEDIA PLAYER
Samotný přehrávač slabá místa nemá, na vině je jeho ActiveX prvek (axvlc.dll) pro Internet Explorer. Kvůli nedbalé kontrole předaných parametrů může malware do počítače propašovat a spustit škodlivý kód. Bezpečnostní mezeru uzavře aktualizace na verzi 0.8.6d.
Info: **www.videolan.org**

OPENOFFICE
Databanka HSQLDB integrovaná v OpenOffice vykazuje bezpečnostní mezeru. Ta útočníkům umožňuje prostřednictvím zmanipulovaného dokumentu spouštět na napadeném počítači libovolný kód v Javě. Mezeru odstraňuje update na verzi 2.3.1.
Info: **www.openoffice.org**

INTERNET EXPLORER
Automatické hledání proxy v prohlížeči se dá jistým trikem převést z LAN na internet. Útočníci tak mohou prostřednictvím simulované proxy sledovat provoz na síti. Řešení je snadné. V IE pomocí Nástroje | Možnosti Internetu | Připojení | Nastavení místní sítě deaktivujte „Automatické hledání".
Info: **www.microsoft.com**

WIRESHARK
I snad nejznámější program pro analýzu provozu na síti má svou slabinu: při analýze preparovaných MP3 souborů se program zhroutí. Řešení: Dokud nebude k dispozici opravená verze, může pomoci jenom vypnutí analytického modulu. Info: **www.wireshark.org**

WORDPRESS WASSUP PLUGIN
Byla nalezena zranitelnost ve WassUp Pluginu pro WordPress **(http://secunia.com/advisories/28702/)**, která může být zneužita k SQL injection útokům. Vstup posílaný „to_date" parametru v souboru spy.php není potřebně ošetřen před použitím v SQL frontách, se kterými pak může útočník manipulovat nastrčením vlastního kódu. Úspěšný útok mu pak dovoluje získat uživatelská jména a záznamy hesel. Problém byl vyřešen ve verzi 1.4.3a.
Info: **zprávy.actinet.cz**

SUN JAVA RUNTIME
Zranitelnost v JRE XML kódu může umožnit přístup k určitým URL nebo vyvolat Denial of Service i přes nastavení vlastnosti „external general entities" na FALSE. K využití této zranitelnosti je zapotřebí, aby XML data se zákeřným obsahem zpracovala důvěryhodná aplikace. Neprojeví se při zpracování nedůvěryhodným appletem nebo Java Web Start aplikací. Tato zranitelnost se nevyskytuje v JDK nebo JRE 6 update 4 nebo pozdějších verzích. Původní oznámení včetně posledních verzí JDK a JRE najdete na webu výrobce **(http://sunsolve.sun.com)**.
Info: **zprávy.actinet.cz**

SQLITEMANAGER
Program SQLiteManager 1.2 obsahuje chybu **(viz http://secunia.com/advisories/28642/)** ve zpracování uživatelem zadaných parametrů, která může vést k zobrazení citlivých informací ze souborů systému. Oprava ještě nebyla zveřejněna.
Info: **zprávy.actinet.cz**

NĚKOLIK CHYB V IBM AIX
Společnost IBM oznámila několik chyb v IBM AIX. Chyby mohou vést ke zvýšení práv lokálně přihlášeného uživatele, k neoprávněné manipulaci s daty nebo ke zpřístupnění citlivých informací. Více informací včetně oprav naleznete na stránkách výrobce **(www14.software.ibm.com)**.
Info: **zprávy.actinet.cz**

CHYBA V HP-UX ARPA
Společnost HP oznámila zranitelnost v HP-UX ARPA Transport, která může vést k Denial of Service (DoS). Zranitelnost je způsobena blíže nespecifikovanou chybou při běžícím ARPA transportu. Více informací včetně opravných patchů naleznete přímo v prohlášení společnosti **(http://h20000.www2.hp.com)**.
Info: **zprávy.actinet.cz**

BEZPEČNOST PRO WINDOWS

Service pack pro Windows Vista

Microsoft oznámil uvolnění prvního servisního balíčku (SP1) pro Windows Vista do výroby (RTM). Během několika týdnů bude současným uživatelům tohoto operačního systému nabídnut nejprve ke stažení na internetových stránkách společnosti Microsoft a následně bude dostupný prostřednictvím služby Windows Update. Připravený servisní balíček především zvýší bezpečnost, výkon, spolehlivost a kompatibilitu systému Windows Vista. Servisní balíček pro české verze Windows Vista bude dostupný v polovině dubna a prostřednictvím služby Windows Update v polovině května. Servisní balíček obsahuje kromě zcela nových dodatků také všechny předešlé aktualizace. Jeho instalace přinese zákazníkům nejen zvýšení výkonu, ale i zlepšení klíčových vlastností samotného operačního systému. Uživatelům notebooků s Windows Vista například umožní delší dobu používání notebooku na baterie. Novinkou je i větší integrace Windows Live služeb a zvýšení podpory konektivity počítače s dalšími zařízeními, včetně mobilních telefonů a smartphonů. Významného kroku bylo dosaženo i v přípravách Windows Serveru 2008. Tento nový serverový operační systém společnosti Microsoft je již plně připraven na uvedení na trh a jeho finální verze byla uvolněna do výroby (RTM). Během jeho přípravy byl proveden historicky největší počet testů, a to jak ze strany Microsoftu, tak i ze strany partnerů a vývojářské komunity. Díky tomu by měl Windows Server 2008 přinést zákazníkům nejen pokrok v oblasti bezpečnosti a výkonu, ale i v oblasti rozšiřitelnosti a spolehlivosti. Při společném nasazení systémů Windows Vista a Windows Server 2008 získají firemní zákazníci tři hlavní výhody. V první řadě dojde díky dostupnosti komplexních nástrojů k zjednodušení a zlepšení správy firemní IT infrastruktury. To s sebou přinese snížení nákladů a zefektivnění všech prováděných operací. Do třetice uživatelé a správci uvítají jednodušší nasazení systémů a lepší využití zdrojů.

Komentář redakce:
Service Pack (SP) pro Windows Vista je pro celou řadu uživatelů důležitým mezníkem v použitelnosti. Je to pozitivní zpráva především pro uživatele notebooků. Tento SP by měl vyřešit námi několikrát zmiňované problémy, přičemž prodloužení výdrže na baterie je už jen příjemný bonus. A Windows Server 2008? Po téměř pěti letech opět nový serverový systém – jsme zvědavi, co nového přinese. Pouze doufáme, že novinky nebudou stejně rozporuplné jako u původních Windows Vista.

ZÁLOHOVÁNÍ DAT

Acronis Recovery pro MS SQL Server

Společnost Acronis ohlásila nový software pro zálohování a obnovu, který je určen speciálně pro databáze včetně MS SQL Serveru, Oracle a MS Exchange. Jeho pomocí mohou správci IT a databází (DBA) snadno a bezpečně zálohovat své databáze a obnovovat je k okamžiku závady, a to včetně tabulek, logů a všech ostatních součástí. Software obsahuje správní konzolu řízenou průvodci a funkci umožňující vytváření záložních archivů, které jsou až o 90 procent menší než původní databáze. Umožňuje také zálohování na FTP server bez jakýchkoliv mezikroků, díky čemuž zajišťuje rychlý a spolehlivý způsob přesunu záloh mimo lokalitu.

„Právě v tomto týdnu byly zveřejněny zprávy o tisících SQL databází, které byly napadeny hijack skriptem, který napadal osobní počítače," řekl Walter Scott, výkonný ředitel společnosti Acronis. „Viry nenapadají jen osobní počítače, útočí také na servery, na nichž běží Microsoft SQL Server. Když má malý nebo střední podnik aktuální zálohu databáze, může mu to ušetřit desítky hodin času, který by byl potřeba pro přebudování poškozené nebo infikované databáze.

„Správci databází potřebují vědět, že jejich zálohy jsou dostatečně bezpečné na to, aby splnily zákonné požadavky, a přitom musí být efektivní z hlediska využitého místa, snadno spravovatelné a rychle obnovitelné," řekl Scott. „Naše řada produktů pro obnovu databází po haváriích nabízí vlastnosti a funkce, které konkrétně požadují správci IT a DBA zodpovědní za udržování různých databází v rámci svých datacenter."

Nová bezpečnostní rizika

SKYPE

Skype obsahuje chybu v zobrazování „Web content Zones". Zákeřně upraveným kódem pak může vzdálený útočník v aplikaci spouštět libovolný kód. Více informací naleznete na webu výrobce **(http://skype.com/security/skype-sb-2008-001.html)** v původním oznámení.
Info: **zprávy.actinet.cz**

APACHE HTTP SERVER

Nebezpečná chyba „mod_status" byla objevena v Apache Serveru 2.2.6 a starších. Tato zranitelnost dovoluje vzdáleným útočníkům provést na serveru Cross-Site Scripting útok. Více informací o chybě najdete na adrese **http://httpd.apache.org/security/vulnerabilities_22.html**. Zranitelnost byla spolu s jinými opravena v nové verzi 2.2.8.
Info: **zprávy.actinet.cz**

THUNDERBIRD A SEAMONKEY

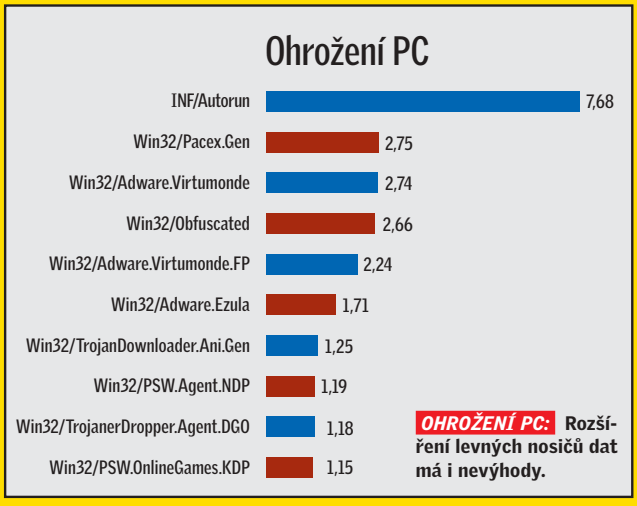
V aplikacích Mozilla Thunderbird **(http://secunia.com/advisories/28808/)** a SeaMonkey **(http://secunia.com/advisories/28815/)** bylo nalezeno několik zranitelností. V obou případech mohou mít zranitelnosti za následek vyzrazení citlivých informací o uživateli, obcházení určitých bezpečnostních opatření, vedení spoofing útoků a případně také kompromitaci uživatelského systému. Zranitelnosti se vyskytují v Mozille Thunderbird do verze 2.0.0.12 a v SeaMonkey až do verze 1.1.8. V dalších verzích softwaru budou chyby podle vyjádření výrobce opraveny. Odkazy na popis jednotlivých zranitelností na stránkách výrobce najdete na výše jmenovaném serveru Secunia.
Info: **zprávy.actinet.cz**

STATISTIKY ESET THREATSENSE.NET

Roste počet útoků s cílem ukrást hesla

Podle statistik zjištěných pomocí systému Eset ThreatSense.Net v posledních týdnech výrazně vzrostlo šíření trojských koní vykrádajících hesla a jiné citlivé údaje z počítače uživatele. Již několik měsíců zaznamenává zmiňovaný systém i zvýšený počet šíření nejrůznějších druhů adwaru, tedy škodlivých programů pro doručování nebo zobrazování nevyžádané reklamy.

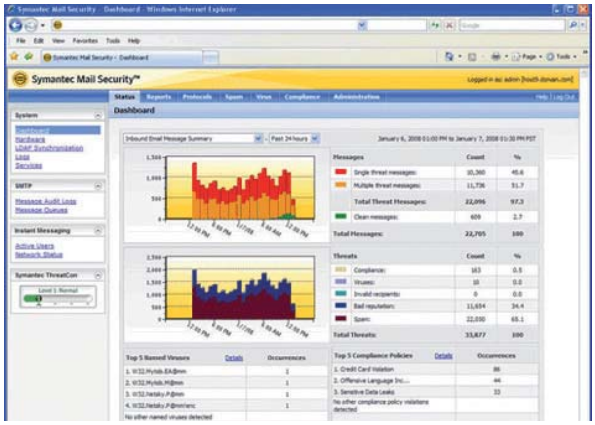
V lednu 2008 vyhodnotil statistický systém Eset ThreatSense.Net jako globálně nejvíce rozšířenou hrozbu infiltraci INF/Autorun (7,68% podíl na všech šířených hrozbách). Je to směs škodlivých kódů využívajících soubor autorun.inf s informací o spuštění programu poté, co uživatel vloží do počítače přenosné médium (nejčastěji USB nosič). K šíření tohoto typu infiltrace velmi pomáhá zvyšující se počet nejrůznějších USB úložných zařízení, jejichž cena v posledních měsících výrazně klesá. Druhé místo v lednovém žebříčku globálních hrozeb patří Win32/Pacex.Gen (2,75 %). Win32/Pacex.Gen slouží jako platforma pro distribuci různých druhů infiltrací využívajících charakteristicky zašifrovaný obal a používá se především u trojských koní, které vykrádají hesla z počítače uživatele. Na předních příčkách se dlouhodobě drží rozšířený adware Win32/Adware.Virtumonde (2,74 %), kterému v lednu patřilo třetí místo. Adware slouží k doručování nevyžádané reklamy. Eset ThreatSense.Net v lednu zaznamenal mírný pokles šíření trojanů pod názvem Win32/Obfuscated.A1 (2,66 %). V tomto případě jde o soubor downloaderů a infiltrací. Specifická varianta viru z rodiny Virtumonde, kterou Eset detekuje jako Win32/Adware.Virtumonde.FP, se z prosincové druhé desítky dostala až na lednové páté místo. Je charakteristická otevíráním množství oken obsahujících rozmanité kategorie nevyžádané reklamy, převážně v angličtině. V prvním měsíci roku 2008 v Česku počítače nejvíce napadal Win32/Stration.ABD, který se šíří hlavně pomocí instant messengerů (ICQ, MSN atp.) nebo elektronické pošty a slouží k rozšiřování spamu.



OHROŽENÍ PC: Rozšíření levných nosičů dat má i nevýhody.

SYMANTEC MAIL SECURITY 8300

Virtualizace ochrany zasílání zpráv



SYMANTEC MAIL SECURITY: Důležité údaje lze přehledně kontrolovat v reálném čase

Nová verze Virtual Edition zařízení Symantec Mail Security 8300 umožňuje uživatelům okamžitě zvýšit nebo snížit kapacitu antivirové ochrany a ochrany před nevyžádanou poštou

Společnost Symantec představila produkt Symantec Mail Security 8300 Series Virtual Edition, virtuální verzi zařízení pro zabezpečení systémů zasílání zpráv. Tento program, který pracuje v prostředí VMware Server a ESX, pomáhá snížit náklady a šetří čas tím, že dává uživatelům možnost okamžitě přizpůsobit kapacitu filtrování nevyžádané pošty a virů bez nutnosti rozšiřovat nebo konfigurovat fyzickou infrastrukturu. „Objem nevyžádané pošty se den ze dne mění, ale celkově je na vzestupu. Zpráva January 2008 State of Spam společnosti Symantec ukázala, že objem nevyžádané pošty dosáhl na konci roku 2007 nových výšin a nevyžádaná pošta tvořila 75 % všech zaslaných e-mailů," řekl Art Gilliland, Vice President of Product Management ve společnosti Symantec.

Centralizovaná řídicí konzola této virtuální verze zařízení umožňuje uživatelům okamžitě zvýšit nebo snížit kapacitu prověřování zpráv na všech stávajících serverech a ve všech stávajících zařízeních.

Virtuální zařízení navíc zvyšuje efektivitu infrastruktury zasílání zpráv tím, že prověřuje a odebírá nevyžádané zprávy ze sítě a poštovních serverů. Symantec Mail Security Virtual Edition nabízí také rychlejší nastavení a instalaci, takže testování a zkoušení řešení před jeho zavedením do produkčního e-mailového prostředí je snazší než kdykoli dříve. Úplnou verzi Virtual Edition je možné během několika minut stáhnout, odemknout licenčním kódem a zavést do virtualizačního prostředí. Všechna řešení Symantec Mail Security 8300 podporuje globální zpravodajská síť společnosti Symantec, která řešení aktualizuje tak, aby zjišťovala nejnovější nevyžádanou poštu a bezpečnostní hrozby. Tato špičková síť sestává z více než 150 milionů antivirových senzorů, dvou milionů nástražných e-mailových adres, 40 000 senzorů v systémech detekce narušení a bránách firewall a 4 300 sledovaných a spravovaných systémů zabezpečení na celém světě. Virtuální zařízení Symantec Mail Security Virtual Edition je možno zakoupit s roční nebo víceletou licencí a jeho cena je dána počtem uživatelů e-mailu.

CHECK POINT ENDPOINT SECURITY

Agent pro komplexní ochranu koncových bodů

Společnost Check Point Software Technologies představila Check Point Endpoint Security, řešení pro komplexní ochranu koncových bodů. Software v sobě kombinuje špičkový firewall, řízení přístupu k síti (NAC), kontrolu aplikací, antivirus, antispyware, zabezpečení dat a chráněný vzdálený přístup. Využití jediného, centrálně řízeného agenta, jediné administrační konzole a centrální instalace i aktualizace znatelně snižuje náklady společností vynakládané na zabezpečení IT.

Check Point Endpoint Security vznikl spojením předních technologií a zahrnuje v sobě nejrozšířenější podnikový firewall a antimalware založený na bázi řešení ZoneAlarm, dále zabezpečení dat v podání technologie Pointsec, aktuálně používané na více než 14 milionech osobních počítačů, a nejprodávanější řešení pro vzdálený přístup VPN. Další součástí řešení je technologie SmartDefense Program Advisor. Pomocí ní mohou správci na základě dynamické databáze účinně kontrolovat, které programy „běží" na firemních počítačích, a zabraňovat tak v aktivitě škodlivého softwaru. Všechny tyto funkce v kombinaci s řešením pro centrální správu představují zcela novou generaci komplexní ochrany koncových bodů, nabízené dnes pouze společností Check Point.

Vlastnosti jednotlivých komponent Check Point Endpoint Security:

- Firewall/NAC/Program Control – u koncových bodů obousměrně chrání síťový provoz, neumožní jim připojení do firemní sítě, pokud nejsou zabezpečené, a účinně vynucuje bezpečnostní pravidla týkající se toho, jaké aplikace smí běžet na daném počítači.
- Antivirus/Antispyware – odhalí a odstraní viry, spyware a jiné malwarové hrozby. Díky kombinaci signatur, analýzy podezřelého chování a pokročilé heuristické analýzy disponuje vysokými detekčními schopnostmi. Software je navíc každou hodinu aktualizován pomocí služby SmartDefense.
- Ochrana dat – díky pokročilému šifrování dat na discích a vyměnitelných mediích, kontrole přístupu a kontrole portů chrání data obsažená v přenosných počítačích, stolních PC i na přenosných mediích.
- Vzdálený přístup – šifrování a ověřování přenášených dat po celou dobu, kdy je koncový bod vzdáleně připojen, chrání koncový bod i firemní síť.

ENDPOINT SECURITY: **Nejen integrovaný firewall a antivirus...**