Nejen dobré vzpomínky mají na letošní jaro někteří uživatelé osobních počítačů, ale i administrátoři počítačových sítí. Již ke konci zimy se v mnoha PC usídlil první výrazný tzv. e-mailový virus Happy 99, brzy na to jej následovala sexuální Mellisa. Krátké období klidu rychle vystřídal výbuch viru CIH, označovaného též jako Černobyl. A konečně blížící se léto přineslo zatím poslední zemětřesení ve formě raketově šířícího se červa Worm.ExploreZip, zákeřně ničícího všechny dokumenty.

Komplexní ochrana od Symantecu

Všichni postižení, kteří se nedobrovolně setkali s výše uvedenými viry, popřípadě i jinými a dosud neměli žádnou antivirovou ochranu, jistě začali o nějaké uvažovat. Antivirových programů a firem zabývajících se touto problematikou je v současné době mnoho a zdaleka se mezi nimi neztratí ani české produkty. S rozmachem sítí, internetu a elektronické komunikace nestačí pouze antivirová ochrana jednotlivých pracovních stanic, nýbrž jsou nutná také kompletní antivirová řešení implementovaná do firemních sítí či intranetů.

Do čela společností zabývajících se těmito technologiemi se v posledních letech dostala firma **Symantec**, dříve známá především svými různorodými utilitami, obzvlášť produktem Norton Utilities, který v posledním vydání má též integrovánu základní verzi antivirového programu.

Kompletní antivirové řešení od Symantecu spočívá v produktu nazvaném *Norton AntiVirus Solution*. Ten přináší nástroje na celkovou ochranu sítí od pracovních stanic až po servery a gatewaye. Samozřejmostí u produktů Symantecu je jednoduchá správa a co nejvíce automatická aktualizace produktu včetně virových databází.

Celý produkt dodávaný na jednom disku CD-ROM je rozčleněn do čtyř kategorií. První nese označení *Desktop Solutions* a zahrnuje program Norton Antivirus pro operační systémy DOS, Windows 3.1, Windows 95/98, Windows NT Workstation, Mac OS a OS/2. Jedná se o klasické antivirové programy, jež při zavádění operačního systému zkontrolují startovací oblasti pevného disku, prověří obsah operační paměti a spustí rezidentní část programu, která pak ochraňuje systém po celou dobu práce. V pravidelných intervalech, uživatelem nastavených při instalaci, překontroluje všechny soubory na pevných discích. Novinkou poslední dodávané verze je automatická ochrana proti nebezpečným appletům ActiveX a Java.

Druhou kategorii logicky tvoří ochrana serverů, označená jako *Server Solutions*. Zde nabízí Symantec antivirovou ochranu pro systémy Windows NT Server, Novell Netware, Lotus Notes a Microsoft Exchange. Ochrana systémů Windows NT Server a Netware je obdobná jako v předchozí kategorii. Doplněna je o lepší podporu pro specifické serverové prvky. Speciální ochrana je u groupwarových aplikací Lotus Notes a Microsoft Exchange, kde antivirový program umožňuje

procházet e-mailové schránky jednotlivých uživatelů a prověřovat soubory připojené ke zprávám. Kontrola může být zapnuta neustále anebo v pravidelných intervalech, například každou noc.

Další kategorie zahrnuje ochranu na vstupu do vaší sítě a nese název *Gateway Solutions*. Ta zahrnuje *Norton AntiVirus for Internet Email Gateways* a *Norton AntiVirus for Firewalls*. Tyto aplikace zajišťují primární antivirovou kontrolu před vstupem jakýchkoliv dat do vaší sítě. Úzce spolupracují s implementovanými přenosovými protokoly a kompletní detekci provádějí v reálném čase. Samozřejmě umějí prověřovat i odchozí data, abyste své zákazníky “neobohatili” o nějaké to virové překvapení.

Poslední kategorií je *Administration*. Již z názvu vyplývá, že se jedná o nástroje určené ke správě a celkové organizaci antivirové ochrany v počítačové síti. Zahrnuje programy *Norton System Center*, *Norton AntiVirus Network Manager*, *Norton AntiVirus Plus for Tivoli Enterprise* a *Norton AntiVirus Plus for Tivoli IT Director*. Norton System Center využívá Microsoft Management Console a zajišťuje správu a údržbu antivirového systému. Obsahuje nástroj *Extension* k řízení aplikací Norton AntiVirus na jednotlivých lokálních stanicích. Při detekci viru, popř. nějaké nestandardní situaci takovou událost zaznamená speciální *Event Manager*, který administrátora upozorní e-mailem či jinou přednastavenou službou i v jeho nepřítomnosti. Norton AntiVirus Network Manager je pak duální nástroj k Norton System Centeru. Využívá se, potřebujete-li řídit Norton AntiVirus na lokálních počítačích pouze pomocí login scriptů při startech systémů.

Pomocí výše uvedených nástrojů lze spravovat i vzdáleně připojené stanice, poněvadž CD-ROM Norton AntiVirus Solution obsahuje i aplikaci *pcAnywhere* od firmy Symantec, určenou pro komunikaci se stanicemi či sítěmi připojenými přes internet anebo pomocí modemů.

Norton AntiVirus Plus for Tivoli Enterprise a Norton AntiVirus Plus for Tivoli IT Director zajišťují integraci správy systému Norton AntiVirus do řídicích nástrojů těchto systémů, speciálně do Tivoli Management Environment 10. Tyto dvě aplikace jsou začleněny v celém balíku Norton AntiVirus Solution kvůli úzké spolupráci Symantecu a IBM na poli antivirových technologií.

Obecně Norton AntiVirus používá k detekci virů několik metod. Standardní je porovnávání s vlastní virovou databází, dále se používá dnes hojně využívaná heuristická analýza, jež umí rozpoznat i nové viry, a v neposlední řadě speciální techniky k detekci virů, které vyvinula a patentovala společnost IBM. Při nalezení viru v nějakém souboru jej můžete vyléčit, pokud se jedná o vir již analyzovaný, anebo můžete použít speciální nástroj nazvaný *Quarantine* (karanténa), který uloží infikovaný soubor do schránky do té doby, než jej budete schopni opravit, a tím ochrání systém před dalším napadením a šířením viru.

Pokud máte to “štěstí” a usídlil se u vás nový vir či máte problémy s odstraněním nějakého viru, můžete pomocí průvodce poslat izolovaný soubor do výzkumného střediska Symantec AntiVirus Research Center (SARC), kde odborníci provedou podrobnou analýzu a pošlou vám zpět řešení.

Na závěr asi to nejlepší – tím je služba *LiveUpdate*, integrovaná v celém balíku Norton AntiVirus Solution. Ta zajišťuje on-line aktualizaci všech programových součástí celého produktu a samozřejmě aktualizaci virové databáze. Pokud jste připojeni přes internet, proběhne automatické stažení nových součástí ze serveru společnosti Symantec a potom automatická instalace na vašem PC. Pokud využíváte nějaké síťové řešení, budete mít na svém serveru nainstalován *LiveUpdate Administrator*, který zajistí automatické stažení nových komponent; ty uloží ve vašem intranetu a pak je ve spolupráci s Norton System Centerem nebo s Norton AntiVirus Network Managerem distribuuje na lokální stanice.

Pokud na internet připojeni nejste, ale vlastníte modem, lze se připojit přímo k některým serverům Symantecu po světě a provést aktualizaci stejným způsobem. Poslední možností je zasílat aktualizace na disketě, ale to už je za určitý poplatek.

Co říci úplným závěrem? Společnost Symantec svým balíkem aplikací Norton AntiVirus Solution připravila opravdu kompletní antivirovou ochranu pro firemní sítě. Norton AntiVirus patří jistě mezi nejlepší produkty na trhu. Kvalitu umocňuje ještě rychlá a jednoduchá aktualizace produktu. To Symantec ostatně potvrdil při výskytu viru Worm.ExploreZip – řešení na jeho odstranění totiž našel jako první.

Miroslav Koukola