Za Windows zdravější

Bezpečnostní ofenziva společnosti Microsoft (CD)

PATRIK MALINA

Mnohým z nás by se chtělo říci: „Kdo zaseje vítr, sklízí bouři!“ Ano, produkty společnosti Microsoft jsou především kvůli dříve liknavému přístupu tohoto softwarového gigantu dnes a denně lákavým cílem různých záškodníků a nekalých živlů. Platforma Windows se však zároveň v podstatě mimochodem stala nejlepším terčem už jen díky tomu, že je nejrozšířenější. A ještě k tomu zběsilý nástup nevyžádaných e-mailů… Microsoft se snaží o obranu a výsledky jsou vidět.

Jako uživatelé pracovních stanic s operačním systémem Windows jste si možná dlouho říkali, že „ty řeči“ o důsledném zabezpečení se vás netýkají, neboť je to přece věc administrátorů velkých sítí. Bezprostřední internetová realita však jako už mnohokrát předčila všechna očekávání a nevídaný nárůst šíření špionážního softwaru, červů, nevyžádaných e-mailů a všemožné další havěti dává jasně pocítit, že ignorování problému je cesta do počítačových pekel. Výrobce operačního systému Windows své uživatele přece jen nenechal v úplném zatracení, a proto jsme pro vás připravili malý přehled stávajících i zcela nových nástrojů a postupů, jež vám mohou pomoci v orientaci i praktické aplikaci ochrany.

Záplaty a MBSA

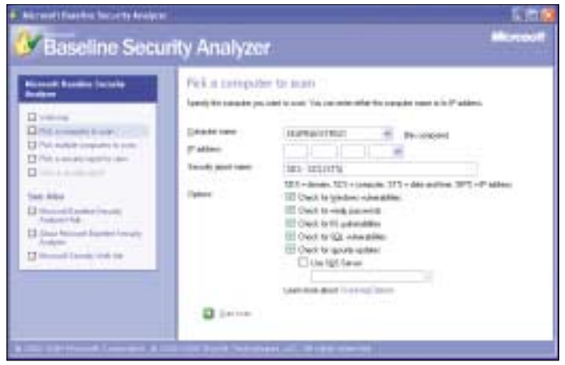
Přestože někteří počítačoví „odborníci“ ve vašem bezprostředním okolí možná stále tvrdí pravý opak nebo význam pravidelného updatování Windows bagatelizují, praktické zkušenosti jasně naznačují, že ignorování bezpečnostních záplat může být cesta k rychlému konci vašich Windows a hlavně spolehlivý způsob, jak přijít o data či o řadu citlivých informací. Jako dostatečný argument nemohou dnes tváří v tvář hrozícím nebezpečím obstát téměř žádné námitky: pokud je váš domácí počítač přímo připojen k internetu (vytáčené připojení, ADSL přes USB modem, ISDN atd.), je cesta škodlivého kódu přes objevenou díru do nezabezpečeného stroje často velmi snadná.

Udržování Windows v čerstvém stavu, v souladu s posledními uvolněnými záplatami, nemusí být nijak obtížné. Klient služby Windows Update je běžně k dispozici jak ve Windows XP, tak ve Windows 2000 a dovoluje vybrat konfiguraci, jež vám bude vyhovovat. Nejste limitování ani absencí trvalého připojení k internetu: kontrolu aktuálnosti záplat lze provádět kdykoliv na požádání až linku připojíte, prověření lze též provádět bez momentálně dostupné síťové konektivity.

Velmi dobrým pomocníkem může v takovéto situaci být aplikace **Microsoft Baseline Security Analyzer**. Nejedná se o program nový – ke stažení zdarma je k dispozici již delší dobu, ale nedávno byla uvedena jeho prozatím poslední verze 1.2.1, jež mimo jiné podporuje kontrolu nainstalovaného kancelářského balíku MS Office v několika verzích. Jedná se o naprosto klíčovou vlastnost, neboť nejen známé díry v samotném systému, ale také slabiny v aplikačním softwaru MS Office často vedly ke vzniku závažných bezpečnostních trhlin. Kromě toho MBSA testuje také řadu parametrů Windows, jež můžete za účelem zlepšení ochrany nastavit lépe, takže zdaleka nejde jen o kontrolu chybějících záplat.

Program MBSA je z hlediska ovládání poměrně jednoduchý, neboť kromě možnosti spouštění v režimu příkazové řádky samozřejmě nabízí též plnohodnotné grafické rozhraní. Jeho instalaci najdete buď přímo na stránkách výrobce *www.microsoft.com/technet/security/tools/mbsahome.mspx*, nebo NA NAŠEM CD. Pokud máte starší Windows 2000 Professional, můžete ještě narazit na chybějící podporu standardu XML, takže příslušný balíček rovněž najdete NA NAŠEM CD. Poslední podmínkou pro běh MBSA je dostatečně aktuální verze MS Internet Exploreru. Přestože samotná aplikace není vybavena českým rozhraním, práce s ní není nijak obtížná.

◀ **Nástroj pro základní analýzu zabezpečení Windows pracuje jak s jednotlivými počítači, tak dokáže v rámci jediné akce zkontrolovat celou síť.**



◀ **Základní sken zahrnuje nejen kompletní prověření instalovaných oprav a záplat pro Windows, ale též prozkoumání některých serverových služeb jako jsou IIS či SQL Server.**

◀ **Při ručním zpracování výstupů kontroly je uživateli k dispozici přehledné grafické rozhraní s užitečnými odkazy na detailní informace o nalezených problémech.**

Při spuštění vám na první obrazovce bude nabídnuto, zda chcete kontrolovat jeden či více počítačů najednou. V případě, že nástroj nepoužíváte poprvé, budete si také moci prohlédnout výsledky dřívějších bezpečnostních skenů. Následující obrazovka již slouží k výběru cílového počítače a dalšímu nastavení: chcete-li kontrolovat stroj, na němž je MBSA spuštěn, bude jméno lokálního počítače automaticky vybráno a nemusíte v tomto ohledu zadávat žádné další informace. Urychlení celé operace lze dosáhnout pomocí voleb (*Options*), kde díky zrušení zatržítek u některých služeb (třeba SQL server) dosáhnete vynechání testů, jež na vašem počítači nemají význam. Pokud si nejste jisti, zda databázi nepoužíváte (byť v podobě „kapesní“ varianty MSDE), raději test proveďte. Po následném spuštění se pokusí program kontaktovat stránky výrobce a stáhnout si aktualizovanou sbírku vydaných oprav, aby sken byl aktuální: právě tuto fázi lze nahradit dodáním již předem staženého souboru, test pak může pokračovat bez internetové konektivity.

Po několika vteřinách až málo desítkách vteřin získáte přehled o zabezpečení Windows v podobě grafického seznamu. V záhlaví dokumentu jsou vypsána základní data o provedené kontrole a pak již následují výpisy nalezených parametrů. Výsledky jsou rozděleny do několika sekcí – zvlášť je testován systém, některé služby (SQL, IIS) a třeba balík MS Office. Dobře si všimněte, že na každé řádce jsou u provedené kontroly odkazy, kde najdete, co bylo přesně *kontrolováno (What was scanned)*, detailní výsledky (*Result details*) a hlavně jak problém odstranit a napravit momentální stav (*How to correct this*). Výsledky všech testů jsou ukládány a mohou být kdykoliv dodatečně prohlédnuty.

Výše jsme zmínili, že MBSA lze použít i mimo dosah internetu – důležité kontrolní soubory s přehledem aktuálních záplat lze totiž stáhnout i jinde (v práci, ve škole…) a posléze je do off-line varianty dokopírovat. Za tímto účelem nainstalujte MBSA na alespoň jeden počítač, jenž si může sáhnout na internet, a posléze proveďte alespoň jeden sken, díky němuž dojde ke stažení aktuálních nastavení. Poté vstupte do adresáře *C:\Program Files\Microsoft Baseline Security Analyzer* a okopírujte si soubor s příponou .cab (třeba *mssecure_1033.cab)* a *mssecure.xml*, jež posléze umístěte na odpojeném počítači do stejného adresáře (případné starší verze přepište). Přestože MBSA při dalším spuštění ohlásí nemožnost připojení, provede korektní sken s po-

◀ Přestože nástroj AntiSpyware je vlastně teprve v rané vývojové verzi, nabízí kolekci zajímavých funkcí a pracuje až překvapivě spolehlivě.

▲ Po instalaci provedete základní nastavení prostřednictvím jasného a přehledného průvodce, jenž nastaví automatické updaty či spustí prvotní kontrolu.

užitím aktuálního nastavení v dodaných souborech. Pouze mu to bude trvat o trochu déle, neboť se nějakou chvíli bude pokoušet o připojení.

Microsoft AntiSpyware

Další frontou, na níž se vede již několik let urputný boj, je špionážní software a jeho různé varianty, jež narušují činnost vašeho systému nejen prostým zdržováním, ale také snahou přesměrovávat komunikaci či odesílat citlivé informace do internetu. Pokud využíváte personální firewall, může být váš stroj slušně chráněn, ale přesto je dobré po přítomnosti parazitů účinně čas od času pátrat a fyzicky je likvidovat. V této oblasti je již dlouho k dispozici řada specializovaných programů, avšak Microsoft se rozhodl i v této oblasti udeřit a nasadil do boje prozatím testovací verzi nástroje **Microsoft AntiSpyware**.

V danou chvíli aktuální beta-verzi programu najdete na stránkách výrobce *www.microsoft.com/athome/security/spyware/software/default.mspx*, kde je také k dispozici řada zajímavých informací. Stažení softwaru je doprovázeno prozatím dobrovolnou kontrolou legálnosti Windows, a proto instalaci nenajdete NA NAŠEM CD. Pro úspěšnou instalaci a spuštění potřebujete operační systém od Windows 2000 výše a MS Internet Explorer alespoň ve verzi 6.0.

Funkcionalita nového nástroje je založena na úspěšném starším vývojovém úsilí společnosti GIANT Company Software, jež byla před koncem loňského roku Microsoftem zakoupena – AntiSpyware je tedy narychlo převlečený program právě tohoto výrobce, o čemž se otevřeně můžete dočíst na stránkách *www.spynet.com*, kam Microsoft začíná koncentrovat své úsilí v boji proti spywaru obecně.

Program pracuje v zásadě na podobném principu jako třeba antiviry: právě prostřednictvím stránek SpyNet pravidelně aktualizuje svou databázi odhalených a identifikovaných špionážních kódů a lokální počítač průběžně monitoruje či na požádání prozkoumá, zda něco podezřelého nemáte „pod kapotou“. Již první seznámení s programem vás přesvědčí především o schůdném a dobře srozumitelném ovládání. Po úspěšném provedení instalace budete vyzváni „asistentem“ k úvodnímu nastavení důležitých parametrů, takže si okamžitě zvolíte, zda chcete databázi hrozeb automaticky aktualizovat (třeba dvě hodiny po půlnoci), zda se má spustit ochrana v reálném čase pro průběžné sledování špionážních „příznaků“ a zda bude ihned po startu zběžně zkontrolován celý počítač. Parametry lze samozřejmě i v budoucnu měnit.

Pro běžnou práci nabízí program několik možností. Na požádání můžete provádět tzv. inteligentní rychlý sken, jenž projde určitá vybraná místa a po několika málo minutách zahlásí případná podezření. Mnohem důkladnější je tzv. plný sken systému, do nějž jsou zahrnuty všechny důležité složky a soubory, včetně vámi speciálně označených disků či adresářů – zde však očekávejte práci na půl hodinky až hodinku. Mnohem výhodnější je samozřejmě takový důkladný průzkum naplánovat na noční hodiny pomocí funkce *Schedule*, jež nabízí buď každodenní opakování nebo volbu dnů v týdnu. Námi zvolený pravidelný sken probíhá na značně „zaneřáděném“ počítači s Windows XP a více než 150 000 soubory kolem hodiny.

Ochrana v reálném čase je realizována pomocí tří tzv. agentů, jež sledují specifické parametry ohrožení: internetoví strážci bdí nad pokusy změnit parametry internetového nastavení, systémoví agenti hlídají bezpečnostní parametry souborového systému a Windows a aplikační strážci dohlíží nad záludnými snahami stahovat či instalovat nežádoucí ActiveX prvky pro internetový prohlížeč, jejichž nebezpečnost je často velmi vysoká. Poměrně užitečné jsou i rozšiřující pokročilé nástroje (*Advanced Tools*). Najdete mezi nimi třeba *System Explorers*, s jejichž pomocí vstoupíte do konfigurace řady nastavení Windows, k nimž se běžně takto hezky nedostanete (automatické spuštění, nainstalované ActiveX prvky). Dále je zde *Browser Hijack Restore*, jenž vrací konfiguraci MS Internet Exploreru do stavu před případným útokem, a poměrně nekompromisní *Tracks Eraser*, jenž po vás smaže dočasné soubory v prohlížeči, historii a také pozůstatky po práci jiných aplikací jako WinZip, chatovací nástroje atd. Funkci všech komponent lze podrobně konfigurovat.

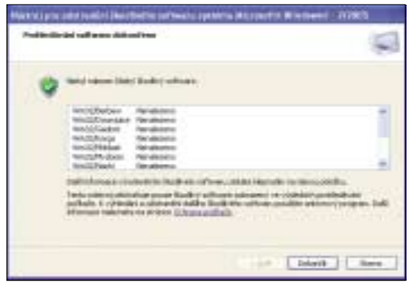
Na závěr dodejme, že při úspěšném nalezení záškodnického softwaru používá program tzv. karanténu, tedy bezpečné úložiště, kde můžete nalezené podezřelé soubory sami osobně prověřit a případně nelítostně odstranit, stejně jako osvobodit, pokud obvinění bylo neoprávněné a rozeznali jste v izolovaných objektech užitečné a důvěrně známé nástroje.

Mezi pokročilejší nástroje patří též jakýsi „Zametač stop“, díky němuž můžete z operačního systému odstranit třeba pozůstatky po internetovém brouzdání.

Program je ke stažení zdarma, a proto doporučujeme s jeho vyzkoušením neváhat.

Malicious Software Removal Tool

Přestože o automatických updatech jsme zde již hovořili, ještě jednou se k této službě vrátíme. Nedávno totiž začal Microsoft mimo jiné tímto způsobem opakovaně dodávat nový jednorázový nástroj s výše uvedeným názvem. Pokud jste mírně zběhlí angličtináři, asi jste správně vytušili, že se jedná o aplikaci na rychlé a přímočaré použití, jež se podobá běžným programkům antivirových firem. Jejím úkolem je velmi rychlým skenováním odhalit přesně určenou množinu škodlivých programů či nebezpečného kódu, o nichž získala aktuální informace při posledním stahování. Podrobnosti o tomto nástroji v českém jazyce najdete v článku databáze znalostí Microsoftu pod označením KB 890830 (na adrese *support.microsoft.com/?kbid=890830*), kde se můžete dočíst velké množství zajímavých informací a také zde najdete seznam nebezpečného softwaru, po němž aplikace pátrá. Nástroj samotný můžete stáhnout zdarma právě zde, nebo jej najdete NA NAŠEM CD v aktuální verzi s českou lokalizací.



▲ Dopadne-li jednorázová kontrola operačního systému dobře a „známé firmy“ v podobě červů a trojských koní nejsou nalezeny, obdržíte takovouto zprávu.

Činnost této utilitky je velmi přímočará: jejím spuštěním a potvrzením licenčního ujednání spustíte akci, jež buď vyústí v prohlášení, že nic podezřelého nebylo nalezeno, nebo odhalený a rozpoznaný nebezpečný software bez milosti zlikviduje. Pokud si nějakého červa třeba z experimentálních důvodů hýčkáte, dejte si pozor, neboť byste o něj takto mohli snadno přijít. Na závěr podá program hlášení a zobrazí přehled, jak pátrání či likvidace dopadly.

Nejzajímavější na tomto řešení je fakt, že bude každý měsíc aktualizováno a tím se budou jeho možnosti vylepšovat. Momentální podoba a seznam hledaných škodlivých programů najdete, pokud Microsoft dodrží slovo, vždy na stejném místě v uvedeném článku databáze znalostí. Pokud používáte službu Windows Update, bude se nástroj stahovat a po odsouhlasení též spouštět každý měsíc znovu.

Přestože možnosti nastavení této aplikace jsou fakticky nulové, jedná se o velmi vhodný doplněk ostatních bezpečnostních řešení. Jednou měsíčně dojde k důkladné kontrole, která ničemu neuškodí a dodá vám jistotu, že se do vašeho PC žádný červík nedopatřením nezatoulal.

Outlook a spam

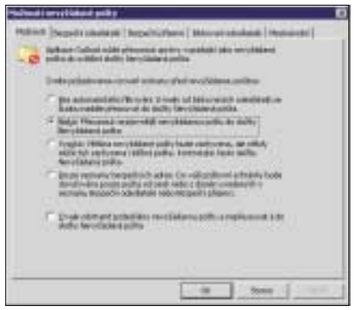
Poslední službu, na níž se v tomto článku podíváme, je filtr pro odstraňování nežádoucí pošty v aplikaci MS Outlook z balíku MS Office System 2003. Problémy se spamováním (obesíláním uživatelů nevyžádanými zprávami, typicky reklamního charakteru) nesmírně narostly a Microsoft není zdaleka jediný, kdo na to ve svém softwaru reaguje.

Program Outlook 2003 obsahuje speciální komponentu s názvem Nevyžádaná pošta (Junk mail), jež zajišťuje dvojí funkci. V první řadě dokáže podle vámi zadaných pravidel jednoznačně říci, jaké zprávy jsou nežádoucí a podle nastavené přísnosti je buď odklidit do příslušné složky nebo přímo nekompromisně zlikvidovat. Protože jen stěží můžete dopředu odhadnout, odkud přijde nová záplava spamu, je zde druhá funkce – inteligentní filtr, jehož úkolem je na základě obsahu zprávy provést klasifikaci a případně jej označit jako spam a provést následné kroky.

Pokud chcete službu přizpůsobit, přejděte do menu *Nástroje – Možnosti* a pomocí tlačítka *Nevyžádaná pošta* obdržíte potřebné rozhraní. K dispozici jsou zde záložky, na nichž můžete sestavit seznam naprosto důvěryhodných osob či doménových jmen, jimž má váš poštovní klient důvěřovat, a naopak, můžete sem zařadit jednoznačně identifikované „rozesílače“ nežádoucího obsahu, jenž bude následně bez milosti filtrován. Velmi důležité nastavení najdete na první kartě *Možnosti*. Pomocí jednotlivých voleb zde definujete úroveň zabezpečení, s níž bude filtr automaticky pracovat při rozpoznávání neznámých, potenciálně nežádoucích e-mailů. Škála má čtyři úrovně, od benevolentního blokování pouze vyjmenovaných záškodníků po nejtvrdší metodu, kdy naopak projdou jen zprávy od přesně vyjmenovaných důvěryhodných osob. Zvolíte-li tvrdší postup, pak po nějakou dobu či raději trvale pravidelně kontrolujte složku Nevyžádaná pošta, kam se odchycený spam odkládá, abyste náhodou nezahodili i korektní poštovní zprávy. S volbou, jež na téže kartě dovoluje nastavit okamžitou likvidaci rozpoznaného spamu, nakládejte velmi obezřetně. Protože techniky spamerů se rychle rozvíjejí, firma Microsoft čas od času připraví v rámci updatu balíku Office i novou verzi filtru, takže sledujte aktuální dění.

Protože tato funkce pracuje velmi hezky a poměrně účinně, nezbývá než dodat jediné: škoda, že není součástí programu MS Outlook Express. Uživatelé bez „velkého“ Outlooku mají smůlu a musí sáhnout po poštovním programu od jiného výrobce, jenž tuto funkci nabízí: žhavým kandidátem je třeba Thunderbird z projektu Mozilla.org.

▲ Funkce pro filtrování nevyžádané pošty (junk mail) je v aplikaci Outlook 2003 již přímo zabudovanou součástí.



▲ Základní úrovně ochrany proti spamu jsou čtyři a zahrnují rozmezí od eliminace pouze jednoznačně pojmenovaných „spamerů“ po totální likvidaci všeho, co explicitně neoznačíte jako povolené.

▲ Nejjednodušší cesta, jak zamezit záplavám z již známých adres, je jejich přesné vyjmenování v seznamu blokovaných odesílatelů.

5 0149/OK ❑