Jak bezpečný je váš PC?

Předem varovaný znamená **DŮKLADNĚ OZBROJENÝ**: nástroje z našeho DVD zkontrolují váš systém od A až do Z a odstraní mezery ve Windows, aplikacích, browseru i hardwaru.

MARKUS HERMANNSDORFER

Rozhodně existují lepší věci ke čtení, než je pravidelná měsíční zpráva o bezpečnostních hrozbách: stále více nových hrozeb z webu, prohnanější škůdci a jako bonus malwarové stavebnice, pomocí nichž dokáže škůdce vytvořit i začátečník. Během roku 2008 již bezpečnostní společnost Sophos napočítala 11 milionů typů malwaru. Každých pět sekund objeví experti nově infikované webové stránky, které chtějí do počítače surfaře propašovat škodlivý kód. Tato fakta jsou nepříjemná především ve spojení s následující otázkou: Jak dobře je můj počítač chráněn před novými hrozbami?

Bezpečnostní nástroje, které vám nabízíme na DVD, tuto kontrolu ulehčují a zároveň kompletně zabezpečí váš systém. Zmiňované nástroje odhalí každou bezpečnostní mezeru, zobrazí místo, kde je nutno provést akci, případně ochrání ty počítačové oblasti, které jsou ve skutečném ohrožení. Protože v některých případech již nejsou virové scannery a firewall dostačující, zahrnuje náš ochranný balíček také detektory rootkitů, nástroje na kontrolu updatů, ochranu prohlížeče a další pomocníky...

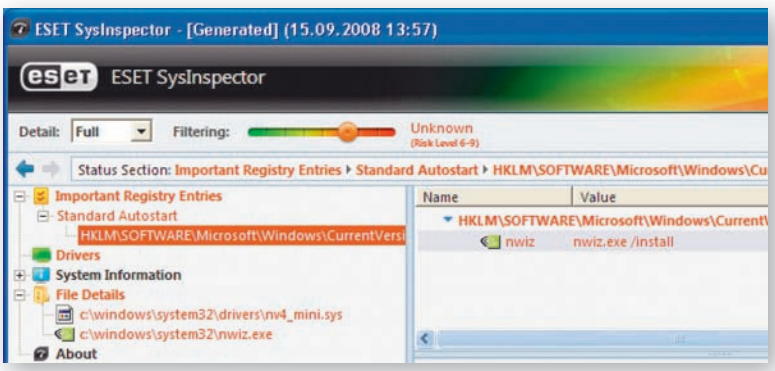
Samozřejmě že existují i komerční bezpečnostní balíky, které spojují zmiňované ochranné nástroje do jednotného rozhraní. Ty však mají v porovnání s našimi nástroji i dvě nevýhody: částečně zpomalují systém a především stojí nezanedbatelné peníze.

Windows: Čtyři kontroly, žádné viry

Nástroj: Eset Sysinspector

Bude-li napaden operační systém, všechna další opatření jsou zbytečná. Z toho důvodu by celková kontrola měla začít právě u Windows. Nástroj Eset Sysinspector z našeho DVD zkontroluje čtyři z nejčastěji zasažených míst v XP a ve Vistě a informuje vás o existujících bezpečnostních rizicích ve vygenerovaném log souboru. Nástroj nepotřebuje žádnou instalaci a může být spuštěn i z USB.

Po spuštění nástroj analyzuje tato čtyři kritická místa: registry, spuštěné procesy, automaticky spouštěné programy a položky v sekci „Místa v síti“.



Poplach: Položky označené červenou barvou mohou obsahovat malware.

NAJDETE NA CHIP DVD

Dokonalá komplexní ochrana

Antivir PE ► oblíbený bezplatný antivirový skener

a-squared Hijack Free ► pomocník při hledání malwaru

avast 4 Home ► bezplatný antivirový nástroj

Avert Stinger ► rychlá pomoc proti virovým útokům

Avira AntiRootkit Tool ► specializový nástroj proti rootkitům

BTF Sniffer ► odstraňuje stopy po internetovém surfování

Eset Sysinspector ► kontroluje rizikové zóny v XP a Windows Vista

Gmer ► nástroj na hledání a odstraňování rootkitů

LauschAngriff ► monitoruje disky a soubory

NoScript ► chrání uživatele Firefoxu před nebezpečnými skripty

Outpost Firewall Pro ► pokročilá kontrola síťového provozu

PC-Antiklau ► pomoc proti krádežím notebooků

PC Security Test 2008 ► simulátor útoků hackerů

Radix Antirootkit ► odhalení skrytého malwaru a rootkitů

Secunia PSI ► kontrola zranitelností u aplikací

Spyware Terminator ► odstraňuje špiónský software

Sunbelt Personal Firewall ► blokuje nejen hackery

ThreatFire ► rozpoznání škůdců na základě chování

TrueCrypt ► šifrování celého disku

UpdateStar ► zajištění updatů nainstalovaných programů

► **NA DVD:** Programy k tomuto článku najdete na DVD pod indexem **SECURITY**.

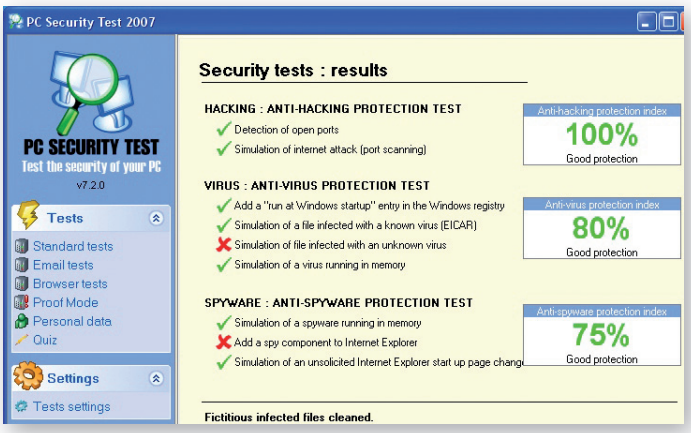
V dalším kroku nastavte posuvník „Filtering“ na úroveň „Risky (Risk Level 7-9)“. Červeně označené soubory či položky si poté poznamenejte.

Důvod: Sysinspector nedokáže škůdce eliminovat. Nechtěných hostů se musíte zbavit manuálně. Dříve než tak ale učiníte, ověřte si na **www.runscanner.net**, zda má nalezený soubor opravdu co dělat s malwarem. Na našem testovacím PC Sysinspector červeně označil i ovladač grafické karty nVidia...

Alarm: Simuluje útoky

Nástroj: PC Security Test 2008

Pokud jste našli a odstranili škůdce, musíte také zjistit, jak se mohl dostat na váš disk. S tím vám pomůže PC Security Test 2008. Ten simuluje různé útoky na počítač a poukazuje na potenciální kritická místa. Abyste počítač otestovali, klikněte po instalaci a spuštění nástroje na nabídku »Standard checks | Start«. Pokud se po spuštění testu v počítači „hlásí o slovo“ firewall a virové scannery, je to dobrý signál. V tom případě nástroje zaregistrovaly simulovaného „hackera“ i virové útoky. Jestliže bezpečností programy nereagují, pak buď nejsou aktualizované, nebo virus může vystupovat jako systémový soubor. Po skončení bezpečnostního testu program zobrazí odhalené bezpečnostní mezery a nabídne tipy, jak je eliminovat.



Nadprůměrný výsledek: Na našem testovacím počítači nebylo nutné příliš mnoho bezpečnostních zásahů...

INFO

Ověřte si zabezpečení svého počítače

Náš seznam vám pomůže při kontrole jednotlivých komponent.

ZABEZPEČENÍ WINDOWS:

- ☐ aktivujte automatické updaty;
- ☐ nainstalujte kvalitní firewall, antivir a antispyware;
- ☐ proveďte update všech bezpečnostních nástrojů.

ZABEZPEČENÍ APLIKACÍ:

- ☐ vždy používejte nejnovější verze;
- ☐ aktivujte systém automatických updatů – pokud je k dispozici;
- ☐ pokud automatické updaty chybí, použijte aplikaci UpdateStar;
- ☐ používejte alternativy k nejpoužívanějším programům – bývají bezpečnější;
- ☐ nepoužívejte beta verze;
- ☐ pokud už beta verze používat musíte, nahraďte je co nejdříve finální verzí.

ZABEZPEČENÍ PROHLÍŽEČE:

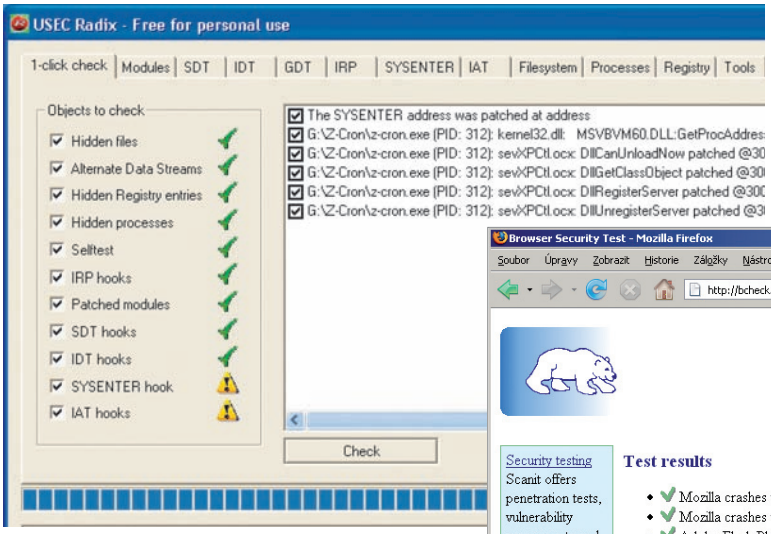
- ☐ pro surfování použijte účet s omezenými právy;
- ☐ využívejte spíše alternativní browsery – například Operu;
- ☐ zakažte používání Javy a JavaScriptu;
- ☐ aktivujte ochranu proti phishingu, blokování vyskakovacích oken a další ochranné funkce.

OCHRANA E-MAILU:

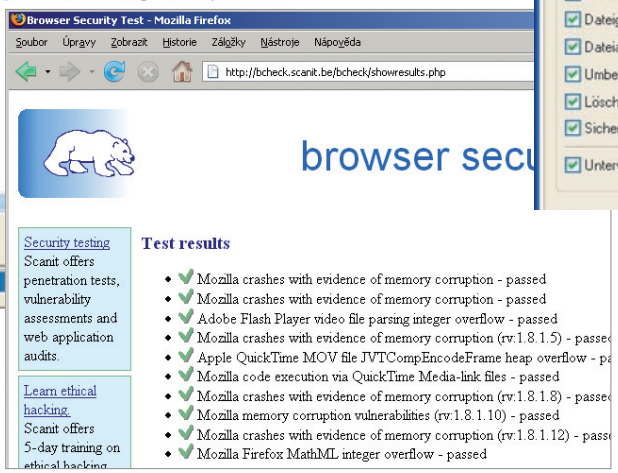
- ☐ používejte bezpečnější e-mailové klienty (jako je například Mozilla Thunderbird);
- ☐ zakažte funkci automatického náhledu;
- ☐ zrušte automatické otvírání příloh;
- ☐ nainstalujte si „před“ poštovní program kvalitní spamový filtr (například Spamihilator);
- ☐ neotvírejte maily od neznámých uživatelů.

NEDEJTE ŠANCI HARDWAROVÝM HACKERŮM:

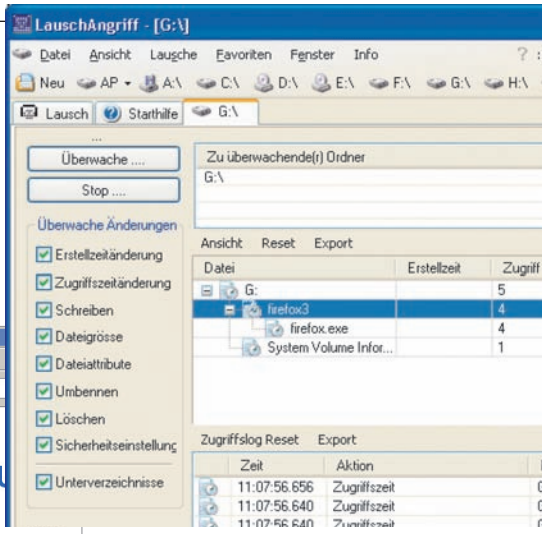
- ☐ nepoužívejte při běžné práci neomezená administrátorská práva;
- ☐ chraňte BIOS heslem;
- ☐ zakažte v BIOS nabootování počítače z DVD, USB nebo síťových disků;
- ☐ nainstalujte si nástroj PC-Antiklau;
- ☐ zašifrujte si systémový disk;
- ☐ monitorujte disky pomocí aplikace typu Devicelock.



Vyhledání rootkitů: Radix scanner odhalí a smaže maskované viry a v případě nutnosti i opraví poškozené soubory.



Vše je OK: Náš prohlížeč odolal útoku deseti různých exploitů. U Internet Exploreru byl výsledek horší...



Plná kontrola: Nástroj Lausch-Angriff vás zvukovým signálem upozorní, když se malware pokouší modifikovat soubory na disku nebo měnit přístupová práva ke složkám.

Rootkity: Nalézání maskovaných virů

Nástroj: Radix Antirootkit

Škůdci jsou stále důmyslnější. Jsou dobře maskovaní, a tak se vyhýbají jak klasickým virovým scannerům, tak i nástrojům proti malwaru. Obvyklým trikem je využití tzv. skrytých ADS data streamů. Proti tomuto typu malwaru dokáže pomoci pouze specializovaný scanner rootkitů, který odstraní škůdce a opraví zmanipulované drivery, systémové soubory nebo procesy. A jak na to?

Spusťte z USB Radix Antirootkit tak, aby se nástroji nedostala do cesty systémová ochrana souborů (ideálně tedy po nabootování alternativního systému). Poté aktivujte všechny možnosti v kartě „1-click check“. Nejdůležitější varovná zpráva se objeví před kontrolou registrů. Pokud zde rootkit něco změnil, scanner se to pokusí opravit, což ale ve výjimečných případech může skončit i selháním systému. Jestliže však tuto opravu odmítnete, rootkit vám v systému zůstane. Po dokončení všech testů zobrazí program soubory a položky, které byly rootkity upraveny a programem opraveny.

Programy: Eliminace všech děr

Nástroje: UpdateStar, Secunia PSI

Jako potenciální zdroj hrozeb mohou „sloužit“ nejenom Windows, ale i nainstalované aplikace. Hackeři totiž dokáží na váš počítač zaútočit pomocí exploitů – programů, které využívají bezpečnostních mezer v aplikacích. Jediným řešením je eliminace děr pomocí nejnovějších aktualizací.

Většina důležitých programů (jako jsou například virové scannery) má integrovánu automatickou aktualizační funkci – musíte pouze zkontrolovat, zda je zapnuta. Všechny další aplikace mohou být aktualizovány pomocí nástrojů UpdateStar či Secunia PSI (oba na DVD). První z nich rozezná více aplikací, ten druhý se specializuje především na bezpečnostní aktualizace. Výběr nástroje by měl záviset na nainstalovaných programech. Čím více jich používáte, tím podrobnější by měly být „znalosti“ specializovaného softwaru. Z hlediska principu je činnost obou nástrojů identická: po instalaci a spuštění nástroj zkontroluje, které aplikace se na disku nacházejí a zda jsou aktualizované. Pokud nejsou, stáhne nástroj z internetu aktualizace, které eliminují existující „netěsnosti“ a případně chyby.

Prošel váš browser testem?

Browser: Crash Test

Nástroj: Bcheck-webová stránka

Nejběžnějším cílem hackerů je obvykle prohlížeč. I pro tento případ platí „finta s exploity“, zmíněná v minulém tipu. Útoky na počítač však mohou být v tomto případě vedeny i přes modifikované webové stránky, které vyvolají například „přetečení bufferu“. Na adrese **http://bcheck.scanit.be/bcheck** si můžete zkontrolovat, zda je váš prohlížeč schopen takovému útoku odolat. Jak na to?

Otevřete webovou stránku, která okamžitě rozpozná váš prohlížeč a operační systém (i tato informace je pro hackera důležitá). Poté zvolte možnost „Only test for bugs specific to my type of browser“ a pomocí „Start the test“ vystavte browser útoku, který může eventuálně způsobit i jeho pád. Náš Firefox browser byl potrápen deseti různými testy; v případě Internet Exploreru jich bylo osm. Bude-li vše v pořádku, obdržíte po testu potvrzovací zprávu. Pokud se prohlížeč zhroutí, otevřete stránku ještě jednou a dozvíte se, kde byl problém...

Browser: Zabezpečení IE & Co.

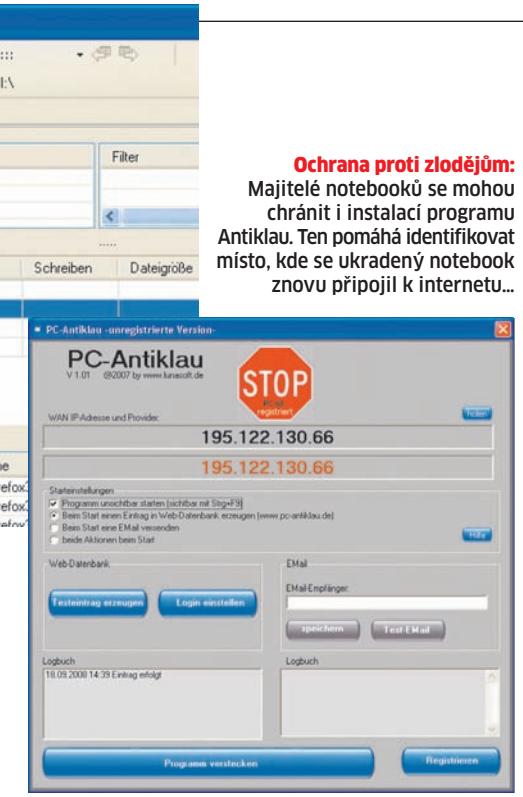
Nástroj: podle prohlížeče

Jestliže prohlížeč v předchozím testu neuspěl, je nejvyšší čas díry eliminovat.

Problém: Neexistuje univerzální rada, jak dokonale zabezpečit libovolný prohlížeč. Úroveň zabezpečení záleží na vašich surfovacích návycích. Pokud je vrcholem vašeho surfování návštěva serveru Idnes.cz, klidně nechte browser v původním stavu. Hledáteli na ruských serverech cracky, lze doporučit co nejdůkladnější zabezpečení. Záleží i na typu obsahu stránek – pokud rádi navštěvujete „fotogalerie“ jako Flickr, sotva můžete zablokovat zobrazování obrázků, i kdyby eventuálně obsahovaly škodlivé kódy.

Doporučujeme následující strategii:

1) POUŽIJTE OMEZENÉ KONTO: Zřiďte si konto s omezenými právy: klikněte na »Start | Control Panel | User Accounts«. Toto konto pak používejte jen pro surfování. Jestliže pak na váš disk pronikne škůdce, nebude schopen se zde usadit, protože nebude mít požadovaná práva.



Ochrana proti zlodějům: Majitelé notebooků se mohou chránit i instalací programu Antiklau. Ten pomáhá identifikovat místo, kde se ukradený notebook znovu připojil k internetu...

2) ZABLOKUJTE SKRIPTOVACÍ JAZYKY: Dávejte si pozor na ActiveX, Javu a JavaScript, protože většina škůdců je programována v těchto jazycích. Tyto jazyky můžete obvykle deaktivovat v bezpečnostním nastavení prohlížeče. Ve Firefoxu například přes »Nástroje | Možnosti | Obsah« a v Internet Exploreru přes »Tools | Internet Options | Advanced". V Opeře zvolte „Tools | Preferences | Advanced | Content«.

Pro spolehlivé stránky, které používají skripty, pak nastavte výjimku – tu by měly například dostat téměř všechny internetové virové scannery. Všechny prohlížeče nabízejí tlačítko typu „Výjimky...", pomocí něhož můžete specifikovat adresu stránky, která může se skripty bez problémů pracovat.

3) MONITORUJTE DISK: V době, kdy surfujete, by vždy měl běžet na pozadí virový scanner. Navíc si z našeho DVD můžete nainstalovat nástroj LauschAngriff, který je k vystopování škůdců ideální. Po spuštění totiž průběžně monitoruje všechny soubory a složky a spustí alarm, jakmile malware změní přístupová práva či atributy souboru. Ale pozor! Tuto činnost občas dělají i samotná Windows, a to včetně změn v souborech. Nepropadejte tedy panice, pokud se objeví hlášení o poplachu – nejprve vždy zkontrolujte, zda byl opravdu spuštěn kvůli malwaru.

Hardware: Blokování a kódování

Nástroje: Devicelock, TrueCrypt, PC-Antiklau

Vložení nakaženého USB flash disku nezabere více než pár sekund. Pokud je tedy vaše PC umístěno ve volně dostupné místnosti, musíte ho také ochránit před „fyzickým přístupem". Mezi nejčastěji napadaná místa v počítači patří BIOS a disk, USB porty a firewire...

Doporučujeme následující ochranná opatření:

BIOS: Zde si obvykle můžete určit dvě hesla – „User Password", které se vyžaduje při bootování počítače, a „Supervisor Password", které zamezuje samotnému neautorizovanému přístupu k nastavení BIOS. Ale pozor! Jakmile tato hesla zapomenete, jediným řešením je vymazání obsahu BIOS odstraněním CMOS baterie.

Další ochranné řešení: V bootovací konfiguraci BIOS povolte pouze spuštění disku. To zabrání nabootování pomocí CD s Linuxem a aplikací typu Ophcrack, které dokáží odhalit heslo Windows za pár minut.

DISK: V BIOS jste už zakázali bootování počítače z USB či DVD disku. Abyste ochránili běžící PC, potřebujete nástroj, který monitoruje disk. Pro tuto práci je nejlepší komerční Devicelock. Demoverzi najdete na **www.devicelock.com/de/dl**.

Pokud nechcete utrácet peníze, můžete harddisk zašifrovat pomocí nástroje TrueCrypt. Najdete ho na DVD. Na webu na adrese **http://blog.evologiq.com/11-Verschluesseln-mit-truecrypt.html** najdete ilustrovanou instruktáž (krok za krokem) pro anglickou verzi TrueCryptu. O něco méně podrobný, ale zato český návod najdete na adrese **http://leyer.profitux.cz/blog/true-crypt-navod/**.

PC KRÁDEŽE: V podstatě jsou to především notebooky, které se rychle ztrácejí z bytů a pracovišť. Zloděj pak může v klidu doma počítač hacknout, přestože jste aplikovali veškerá dosud zmíněná ochranná opatření. Proti tomu vám však pomůže nástroj PC-Antiklau z našeho DVD. Při instalaci nástroje specifikujte jméno uživatele a heslo. Obojí se uloží na serveru výrobce Antiklau na **www.pc-antiklau.de**. Je-li vám počítač ukraden, přihlaste se na Antiklau server. Pokud zloděj alespoň jednou navázal internetové spojení, najdete zde jasnou informaci, jako je lokální IP adresa PC a poskytovatele, prostřednictvím které lze pachatele chytit do pasti. Tato data předáte policii a ta zloděje rychle chytí. Za tento nástroj zaplatíte pouze jednoduchý registrační poplatek 5 eur, což je každopádně levnější než ztráta vyplývající z důsledku krádeže...

AUTOR@CHIP.CZ