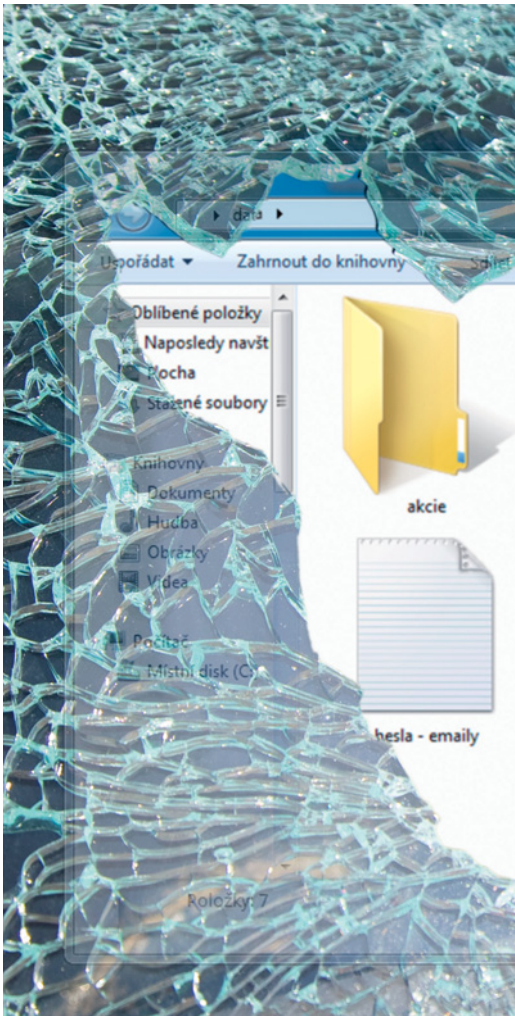
Mezi vámi a hackery

Taktika hackerů se rok od roku mění – útoky přicházejí z e-mailu, z falešných antivirů nebo z obyčejných nakažených souborů. Ať už proti těmto metodám bojujete jakkoliv, **KVALITNÍ FIREWALL** vám pomůže vždy.

PETR KRATOCHVÍL



Softwarový firewall sice patří k základní výzbroji opatrnějšího nebo zkušenějšího uživatele, jeho výběr ale nepatří k nejjednodušším činnostem. Pojďme se podívat, podle jakých vlastností a funkcí lze vybrat optimální firewall.

Kdy ano, kdy ne

Celá řada uživatelů se při diskusi o zabezpečení počítače „ohání“ tím, že ve Windows už firewall integrovaný je – a že uživatelům stačí. Je tomu opravdu tak? V oblasti zabezpečení platí obecné pravidlo: Čím větší nároky na bezpečnost, tím kvalitnější by měl být firewall. Na běžné domácí surfování stačí firewall ve Windows, pokud je však počítač využíván pro práci, nebo dokonce pro finanční záležitosti (internet banking, správa spoření, nakupování), rozhodně se vyplatí investovat do kvalitního firewallu. Pokud jste připojeni k internetu přes router (např Wi-Fi nebo ADSL), rozhodně nezapomeňte zapnout hardwarový firewall, který najdete v naprosté většině produktů. Ten může pomoci „odfiltrovat“ část rizik a usnadnit práci svému softwarovému příbuznému. Chcete-li i přes naše upozornění vsadit na firewall ve Windows, alespoň si prostudujte jeho potenciální slabiny (viz rámeček).

Jak vybírat

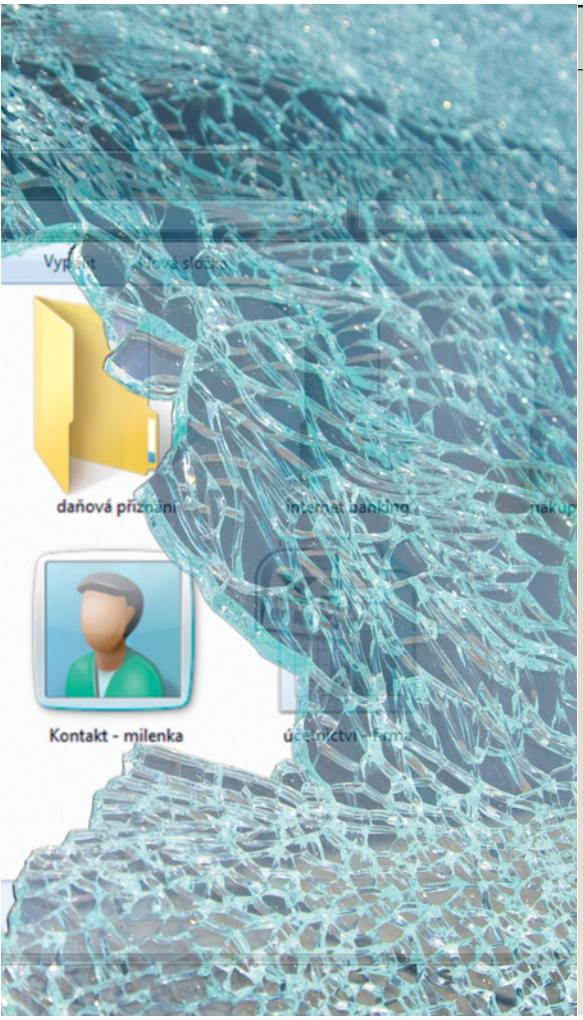
Volba firewallu sice nepatří k podobně kontroverzním tématům jako volba operačního systému nebo výběr mobilního telefonu, přesto se diskusní fóra hemží útoky. Každý z desítky bezplatných firewallů má své skalní příznivce, kteří ho jsou ochotni hájit do poslední kapky krve. Hledat rozumné doporučení na internetu je tak zbytečné. Jak tedy vybrat ideální firewall? Jedním z hlavních kritérií je pochopitelně bezpečnost. I v sebelepším produktu se najdou chyby, a pokud jejich zazáplatování trvá příliš dlouho (nebo je chyb podezřele hodně), dejte rychle ruce pryč. Důležité informace o zranitelnostech najdete na **www.secunia.com** nebo **www.securityfocus.com**. Zde se vyplatí podívat se i na „příbuzné“ produkty, které naznačují „aktivitu“ firmy.

Poněkud paradoxně úspěšná může být sázka na méně známý a rozšířený firewall – hackeři se totiž specializují na nejrozšířenější produkty, u kterých se jim vrátí investice do hledání zranitelností.

Dalším kritériem výběru by měly být schopnosti. Základem je filtrování provozu, a to jak pomocí jednoduchého nastavení pravidel, tak i včetně učícího se režimu. Samozřejmostí je filtrování provozu „ven“, jako obrana proti malwaru, který pronikne do počítače. Požadavky na jednoduché ovládání a nízké systémové nároky pak závisí na potřebách konkrétního uživatele. Existuje ale ještě jeden parametr, který vám o úrovni firewallu leccos napoví – frekvence vydávání updatů nebo nových verzí. Jestliže narazíte na nástroj, který je už rok k dispozici ve stejné verzi, rychle dejte ruce pryč. Je velmi pravděpodobné, že řešení potenciálních problémů nebude nejrychlejší...

Čtyři kandidáti

Protože nabídka firewallů je více než bohatá, využili jsme při výběru těch nejlepších nástrojů malého pomocníka. Tím je světoznámý projekt Davida Matouška, který s několika dalšími lidmi začal testovat firewally, přičemž výsledky testu najdete na **www.matousec.com**. Nejprve je ale nutné podotknout, že nejde o klasické testy firewallů – tedy zkoušení rychlosti propustnosti nebo kvality filtrování paketů. Jde spíše o testy, které prověřují firewally z hlediska „zabezpečení počítače“ a širokého spektra dodatečných funkcí. Mezi zkouškami je například pokus vyřadit firewall pomocí zastavení jeho procesu, detekce „falešného“ procesu nebo pokus o nahrání infikovaných DLL knihoven. Test se skládá z deseti úrovní, které postupují od nejjednodušší k nejobtížnější, a ve finálních výsledcích najdete kromě procentuálního ohodnocení také úroveň, na kterou se firewall v testech dostal. My se zaměříme na první čtyři (bezplatné) nástroje, které dosáhly hodnocení alespoň 90 % a v testech dosáhly úrovně 10. Výsledky testů najdete na adrese **www.matousec.com/projects/proactive-security-challenge/results.php**. Našimi kandidáty na nejlepší firewall jsou tedy Comodo Internet Security, PC Tools Firewall Plus, Outpost Firewall Free a Online Armor Personal Firewal.



INFO

Firewally ve Windows

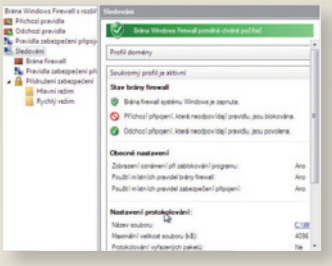
Celá řada uživatelů se snahám o hledání kvalitního firewallu usmívá s vědomím, že oni už jeden firewall ve Windows mají. To může být ale nepříjemný omyl. Pojďme se podívat, jak jsou na tom jednotlivé verze Windows.

Ve Windows XP najdete jednoduchý firewall, který přibližně odpovídá úrovni základních bezplatných nástrojů z doby uvedení XP na trh. Dalo by se říci, že nenáročným uživatelům by skutečně mohl stačit, jenže je tu jedno velké „ale“. Tento firewall totiž bohužel nefiltruje odchozí pakety – pokud se vám usadí v počítači škodlivý software, nemůžete ho jeho pomocí odhalit.

Firewall ve Windows Vista je na tom podstatně lépe. Nabízí filtrování příchozí i odchozí komunikace, umožňuje vytváření jednoduchých pravidel, a pokud ho doplníte o kvalitní antivir a antispyware (pozor – nikoliv o podprůměrný Windows Defender!), lze považovat Vistu za slušně zabezpečenou. Zkušenější uživatelé ale i zde narazí na jeden nepříjemný problém. U příchozí komunikace firewall blokuje vše přesně podle pravidel, u odchozí komunikace je filtrování (a blokování) poněkud obtížnější. Navíc implicitní nastavení firewallu je takové, že „odchozí připojení, která neodpovídají pravidlu, jsou povolena“.

Pokud chcete i přes výše uvedené informace používat integrovaný firewall Windows, doporučujeme ho zkombinovat s hardwarovým řešením. HW firewall například ve Wi-Fi nebo ADSL routeru je i se softwarovým firewallem Windows dostatečným bezpečnostním řešením.

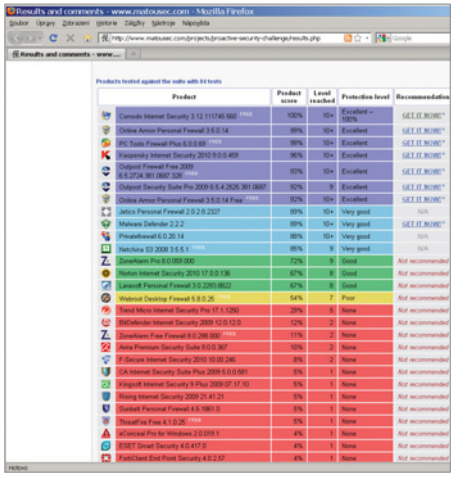
TIP: Základní firewall ve Windows Vista toho opravdu moc neumí. Pokud hledáte pokročilejší nástroj s rozsáhlejší nabídkou funkcí, musíte hledat jinde. V sekci »Ovládací panely | Systém a údržba | Nástroje pro správu | Brána firewall systému Windows s vyspělým zabezpečením« najdete firewall s rozsáhlejšími možnostmi…



Pro náročné: Pokročilejší verze firewallu ve Vistě toho umí poměrně dost.

Kdo s koho

V oblasti zranitelností jsou na tom všechny produkty překvapivě dobře – jak u vítěze testu, firewallu Comodo, tak i druhého nástroje od PC Tools se v poslední době žádný problém neobjevil – na drobnosti lze narazit jen u příbuzných produktů (Comodo Antivirus a PC Tools Spyware Doctor), kde byla nalezena jediná zranitelnost. Podobně je na tom i produkt Outpost Security Suite, který také neobsahuje žádnou zranitelnost. Jediného „černého petra“ má Online Armor Personal Firewall, který obsahuje (zazáplatovanou) zranitelnost. Z hlediska schopností mezi testovanými aplikacemi příliš velké rozdíly nebyly: funkce navíc nabídl Comodo Internet Security a širší ochranu lze očekávat i od nástroje Outpost Firewall Free. U Firewallu Comodo se nám také líbil režim Defense+, který podstatně zlepšuje obranné schopnosti. Obecně lze ale říci, že všechny programy zvládly to, co od nich běžný uživatel očekává.



Nejlepší: Náročné testy na webu matousec.com ukazují překvapivé slabiny některých známých nástrojů.

Z hlediska přehlednosti a jednoduchosti ovládání u nás zvítězil Outpost těsně před nástrojem Comodo, nicméně problémy s prací v libovolném z nástrojů by neměl mít ani méně zkušený uživatel.

TIP: Pokud patříte mezi náruživé hráče World of Warcraft nebo jiné on-line hry, před prvním spuštěním zvolte režim „Training mode“, který automaticky nastaví příslušná pravidla. Ušetříte si spoustu času na přepínání se do režimu firewallu. Po ukončení hry se ale opět vraťte do původního režimu (např. Train with Safe Mode). Na základě všech zmiňovaných kritérií lze tedy jednoznačně doporučit především vítěze testu, firewall Comodo Internet Security, který nabídne jak špičkovou bezpečnost, tak i přehledné ovládání.

Jak firewall nastavit

Konfigurace firewallu obvykle probíhá v několika krocích – jako první je nutné určit, zda připojení, které aktuálně využíváte, je „bezpečné“ (například do firemní sítě), nebo rizikové (přímo do internetu). Poté je buď možné zvolit úroveň zabezpečení (obvykle tři úrovně, podle kterých se volí přísnost filtrování), nebo se rovnou pustit do „výuky“ firewallu. Během ní musíte určit, které aplikace mohou komunikovat „s internetem“, a které nesmí. Při povolování je nutné vědět, zda odpovídá jméno aplikace: pokud se například při spuštění Internet Exploreru snaží komunikovat aplikace „Wintool.exe“, budete mít asi problém. Druhým důležitým faktorem je port, který aplikace ke komunikaci používá. S tím vám pomůže stránka **www.chebucto.ns.ca/~rakerman/port-table**.html, kde najdete seznam nejpoužívanějších portů spolu s aplikacemi, které je používají.

PETR.KRATOCHVIL@CHIP.CZ