Perfektní firewall

Samozřejmě, bezpečnost především. Ale musí nás firewall tolik stresovat? Odpověď zní jasně: Ne. Stačí jej jednou správně nastavit, a trápení je konec. *Valentin Pletzer, autor@chip.cz*

V tomto článku najdete

Je to k zoufání. Ať je v počítači nainstalována kterákoli z „bezpečnostních souprav“, sotva aktivujete firewall, okamžitě máte po náladě. Najednou vám přestanou přicházet e-maily nebo je internetové spojení šíleně pomalé. Prozradíme vám, proč tomu tak je a jak tyto i jiné problémy s firewallem můžete vyřešit. Stále však zůstává kardinální otázka, kterou si klade mnoho uživatelů: Když firewall přináší tolik potíží, má cenu jej vůbec instalovat?

Kontroverzní diskuse:
Proč má smysl osobní firewall

Jako na kolovrátku se na nejrůznějších fórech stále omílá názor, že personální firewall je zbytečný. S odůvodněním, že „kdo chce, vždycky dokáže firewall na PC přelstít“.

Tvrzení o neúčinnosti osobního (či chcete-li personálního nebo desktopového) firewallu není úplně falešné – ale také ne úplně pravdivé. Chytří hackeři samozřejmě dokážou osobní firewall ošálit. Jedním z jejich oblíbených triků je zneužití zdánlivě neškodného programu, například webového prohlížeče, k rozesílání dat z vetřeleckého malwaru. Aby totiž mohl kontrolovat odchozí spojení, vede si firewall seznam bezpečných programů a procesů. Pokud se malware „namaskuje“ za jeden z těchto programů, svá data pak kolem firewallu snadno propašuje. Mnohé firewally tyto triky znají a částečně jim mohou zabránit. Ovšem jen do doby, než si hackeři vymyslí zase něco nového...

Z toho však neplyne, že firewall, který běží pod Windows, by byl automaticky neu- →

Najdete na ChipDVD **Process Explorer** freeware ■ **TOR** freeware ■ **Shutdown Windows‘ Servers** freeware

→ žitečný. Realita je taková, že internetová mafie vždy sáhne po tom ovoci, které visí nejníže. To znamená, že kdo si firewall nenainstaluje a neučiní ani jiná bezpečnostní opatření, bude se u ní těšit mimořádné oblibě. Převážná část na internetu nalezeného spywaru a trojských koní se totiž vůbec nenamáhá s nějakým překonáváním firewallů – přinejmenším na tak dlouho, dokud bude dostatek jiných obětí. Takže: personální firewall vás ochrání před hromadnými útoky z internetu, nikoli však před cíleným napadením jedním hackerem.

Zrušení firewallové blokády: Jak reaktivovat poštovní program

Zpočátku všechno fungovalo skvěle: nainstalovali jste si nějakou „Security Suite" a Outlook spolehlivě zpracovával maily jako dřív. Najednou však přestává fungovat jejich odesílání.

S největší pravděpodobností dodatečně došlo ke změně konfigurace firewallu. Příčinu potíží vám pomohou odhalit tři jednoduché testy.

Krok 1: Nejprve zkontrolujte, zda je blokován jenom poštovní program, nebo zda bylo přerušeno veškeré spojení. Otevřete tedy internetový prohlížeč a v něm webmailovou stránku svého e-mailového účtu. Pokud se stránka otevře a podaří se přihlášení, jste o kousek dál: přesvědčili jste se, že vaše připojení je funkční, a že na vině tudíž není server.

Krok 2: V případě, že jste první krok nemohli provést, poněvadž své maily ze serveru stahujete pomocí POP3 nebo IMAP, poslouží vám ke kontrole i libovolná jiná domovská stránka. Když se otevře, je zatím vše v pořádku. Pokud ne, přejděte na nastavení svého firewallu a vyhledejte tam položku popsanou zpravidla jako „Blokovat všechna příchozí spojení" nebo podobně. Firewall ve Windows toto nastavení nabízí na záložce „Obecné". Zrušte tam zaškrtnutí a pak spojení znovu přezkoušejte pomocí browseru.

Krok 3: Jestliže funguje internetové spojení i e-mailový účet, připadá v úvahu jiné nevhodné nastavení. Zkontrolujte, zda váš poštovní program není buď blokován, nebo prostě jen není uvolněn pro síťový provoz. Ve firewallu Windows toto nastavení objevíte pod nabídkou „Výjimky". V případě pochybností vymažte všechny položky, které se týkají poštovního programu, a znovu se pokuste odeslat zprávu. Osobní firewall by se nyní měl dotázat, zda přístup dovolíte – poté odpovězte kladně.

Uvolnění brzdy: Jak zabránit trhavému streamování videa

Se svou „bezpečnostní soupravou" jste docela spokojeni. Jste chráněni a přitom ještě vše funguje. Jenom streamování videa je trhavé, a to i přesto, že máte čtyřmegabitové DSL.

V každé bezpečnostní soupravě jsou dvě komponenty, které mohou připadat v úvahu jako brzdy. První z nich je antivirový program. Přechodně jej proto vypněte a vyzkoušejte, zda to mělo nějaký vliv na přenos videa. Nezapomeňte však po této zkoušce virový skener opět aktivovat!

Druhou komponentu, firewall, byste neměli takto jednoduše vypínat. Ke zkoušce proto použijte firewall Windows. Ten sice není zvláště vytříbený, poskytuje však dostatečnou ochranu a přitom streamování zaručeně nezpomaluje.

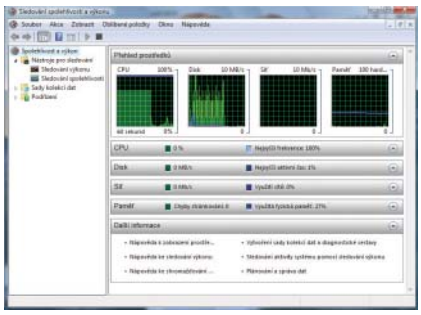
Trápení s programy: Jak najít a uvolnit správné porty

Chcete-li se vyhnout pozdějším zádrhelům, je vhodné uvolnit hned ze začátku příslušné porty. K tomu ovšem potřebujete vědět, který program které porty používá, nebo alespoň jak to lze zjistit.

Na internetu kolují seznamy, v nichž je uvedeno, který protokol používá zvolený port. Mnozí však nevědí, že zde jsou míněny serverové porty. Tak například webový server (HTTP) je identifikován číslem portu 80, FTP portem 21 a SSH portem 22. To je však důležité jenom pro administrátory; tato čísla totiž udávají, které porty musí být otevřeny na straně webového serveru.

Pro domácí počítač jsou tyto porty zajímavé nejvýše pro regulaci odchozích spojení. Tato nastavení však zpravidla převezme sám firewall, jakmile program, a tedy i spojení odstartujete.

Pokud by se přesto vyskytl nějaký problém, pomůže vám osvědčený nástroj „Process Explorer", který si můžete stáh-



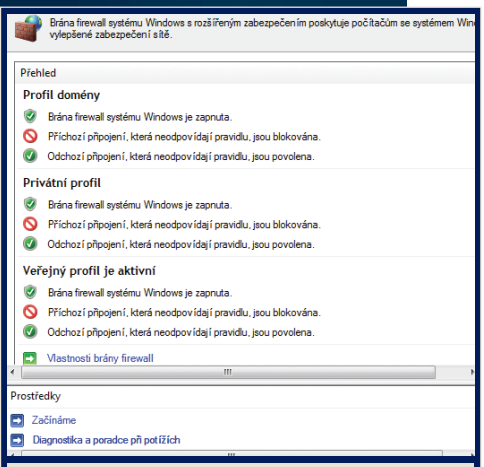
CPU NA HRANICI: Při streamování se vytížení procesoru rychle vyšplhá na 100 % – může za to firewall.

Jak se obejít bez firewallu

Počínaje Service Packem 2 pro XP obsahuje každá nová verze Windows také firewall. Pojďme se podívat, co software od Microsoftu dokáže.

Windows XP

Teprve když červ Blaster 2003 vyvolal mezi počítači s Windows opravdový masakr, Microsoft pochopil, že je třeba něco udělat také pro bezpečnost operačního systému. Bohužel však toho firewall v XP příliš mnoho neumí. Nedaří se totiž ani tak jednoduché záležitosti, jako je kontrola odchozích spojení. Naštěstí však program chrání alespoň před útoky červů. Přinejmenším to pomůže překonat krátké období bez ochrany, než si nainstalujete opravdový firewall a aktualizace Windows.



V ÚKRYTU: Zajímavé ochranné funkce Visty najdete v části „Windows Firewall s rozšířenou bezpečností".

Windows Vista

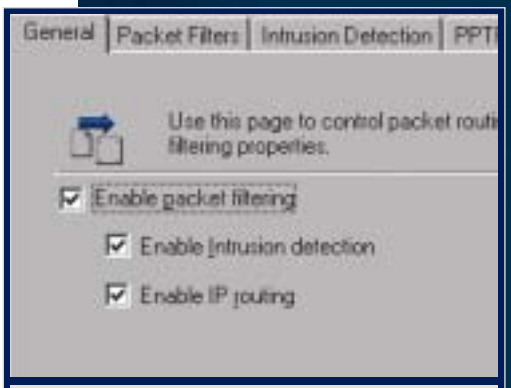
Pro Vistu vyvinul Microsoft poprvé „Out-Bound Firewall", který umožňuje kontrolovat i odchozí spojení. Poněvadž však mnoho nezkušených uživatelů s touto funkcí a s programy jako RealPlayer mělo ve fázi beta testů potíže, byla tato vymoženost bez okolků deaktivována. Pokročilé funkce však můžete z „propadliště dějin" opět vyzvednout: do vyhledávacího pole v nabídce Start napište „Windows Firewall s rozšířenou bezpečností", načež se před vámi otevře detailní nastavovací menu. Tak bezpečný a komfortní jako jeho komerční příbuzní ovšem firewall ve Vistě není. Chybějí mu smysluplná přednastavení, jednoduchá menu i pomoc asistentů, a nejspíš je nepřinese ani první Service Pack.

Jak se obejít bez firewallu

Desktopový firewall je důležitou součástí každé bezpečnostní soupravy. Avšak software, který nepřetržitě běží na pozadí, stojí výpočetní výkon i paměť. Chcete-li se této zátěže zbavit, řiďte se následujícími pokyny.

Správná konfigurace routeru

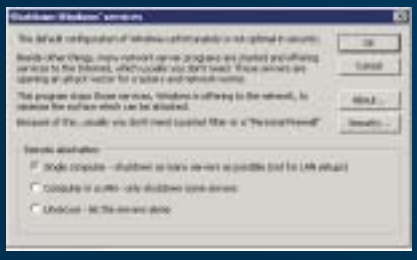
Je-li vaše domácí síť napojena na internet přes router, hned si můžete trochu oddychnout. Červi jako Blaster vám nemohou ublížit. Při pokusu o spojení s vaším počítačem zůstane takový škůdce „viset" v routeru – pokud jste ovšem nezapnuli „Port-Forwarding" a neumožnili tak proniknutí nebezpečných požadavků do počítače. U většiny směrovačů je však tato volba standardně vypnuta. Pozor! Pakety se zfalšovanou adresou odesílatele přesto dosáhnou svého cíle, pokud hacker zná vaši interní IP adresu. Aby k tomu nedošlo, musíte svůj směrovač nakonfigurovat tak, aby odfiltroval ty pakety, které přicházejí zvenčí (ze strany DSL) a jako adresu odesílatele mají privátní IP adresu. Síťové IP z privátního adresového prostoru mají hodnoty 192.168.0.0/16, 10.0.0.0/8, 172.16.0.0/12 a 127.0.0.0/8.



FILTROVÁNÍ PAKETŮ: **IP pakety se zfalšovanou adresou odesílatele bude váš směrovač při správném nastavení rovnou zahazovat.**

Vypnutí zbytečných síťových služeb

Windows spouštějí mnoho síťových služeb, které mají administrátorům umožnit správu počítačů na dálku. Patří k nim služby jako DCOM, přes kterou také proniká červ Blaster. V privátní síti či dokonce na samostatném počítači se můžete bez obav těchto služeb vzdát. Velmi pohodlně tak můžete učinit pomocí nástroje „Shutdown Windows' Servers" (na Chip DVD nebo na **www.dingens.org**). Vše, co k tomu potřebujete znát, je konfigurace vaší sítě: máte-li jen jeden počítač a žádný směrovač, zvolte Single Computer. Pokud je počítač, na němž provádíte nastavení, za routerem, vyberte možnost Computer in a LAN. Akci potvrďte kliknutím na OK a program pro vás všechny nepotřebné služby Windows vypne.



Instalace antivirového programu

Bez nějakého virového skeneru se neobejdete. Sice také užírá výkon, ale ochrání vás před nebezpečími, s nimiž žádný firewall bojovat neumí. K nim patří například e-mailoví červi, spyware, adware a rootkity.

Pravidelné aktualizace

Service Pack 2 je pro Windows XP naprosto povinný. Napravuje totiž již známé slabiny operačního systému, které jiná bezpečnostní opatření neřeší vždy optimálně. Doporučujeme – pokud ovšem máte rychlé napojení na internet – aktivovat si automatické aktualizace Windows. Pak na to nemusíte neustále myslet a pídit se po updatech. Máte-li spojení trochu pomalejší, měli byste aktualizace nahrávat manuálně. Při bezpečnostních aktualizacích však nemyslete jenom na Windows: také ostatní programy a především přídavné moduly mohou mít bezpečnostní mezery. Taková mezera například ve Flashplayeru je přinejmenším stejně nebezpečná jako skulina v XP, jakmile zavítáte na flashovou webovou stránku.

Používání alternativního softwaru

Na častých stížnostech proti „monokultuře" Microsoftu je určitě i zrnko pravdy. Kdyby totiž většina uživatelů nepoužívala stejný software, hned by spousta vetřelců neměla šanci. Většinou totiž využívají stejnou bezpečnostní díru. Proto doporučujeme: Namísto Outlook Expressu vyzkoušejte Mozilla Thunderbird a místo Internet Exploreru prohlížeče Firefox a Opera. Také tyto alternativní programy najdete na Chip DVD.

nout ze stránky *www.microsoft.com/technet/sysinternals/Security/ProcessExplorer.mspx*. Spusťte Process Explorer a v seznamu vyhledejte svůj program. Na něj klikněte pravým tlačítkem myši, zvolte *Properties* a pak otevřete záložku TCP/IP. Tam se mimo jiné dozvíte, které porty se daný program pokouší otevírat. Ty pak ve svém firewallu uvolněte.

Pomalé stahování: Řešení konfliktů při sdílení souborů

Ať jde o BitTorrent, nebo o EMule – je-li desktopový firewall aktivní, stahování ze sítě P2P silně pokulhává. Samozřejmě byste rádi věděli, proč tomu tak je.

V zásadě platí, že firewally a filesharing se spolu špatně snášejí. A vyřešit tento problém úplně ani není možné. Správné nastavení portů však u mnoha firewallů dělá téměř zázraky. Důležité jsou tyto UDP porty:

EMule	4711
BitTorrent	6881, resp. 25819
Kazaa	1214
Overnet/EDonkey	4662

Pokud uvolnění odpovídajících portů úspěch nepřinese, mohlo by se jednat o záležitost vašeho směrovače – aktivujte pro něj proto „Port-Forwarding". A máte ještě jednu možnost: upustit od firewallové ochrany. V tom případě však doporučujeme využít pro sdílení starý PC a na něm neskladovat žádná důležitá data.

Privátní sítě: Sdílení souborů vzdor firewallu

Pro rychlou výměnu souborů mezi dvěma počítači v síti je sdílení souborů ve Windows ideální metodou. Avšak do tohoto procesu se neustále vměšuje firewall. Zajímá vás proto, jak aktivovat sdílení souborů, a přesto se nevzdat ochrany firewallem.

Obecně platí, že čím více portů na firewallu otevřete, tím hůře bude váš PC chráněn. Zvláště se to týká sdílení souborů a tiskáren pod Windows. Právě tady totiž hackeři v minulosti nacházeli a také zneužívali spoustu slabých míst. Používáte-li tedy notebook, měli byste ve veřejných „hotspotech" otevřené porty zase zavřít. Moderní firewally už rozpoznají síť automaticky a odpovídajícím způsobem se nakonfigurují. Jiné programy, jako třeba firewall XP, je zapotřebí pokaždé přizpůsobit manuálně. →

→ Většina dnešních firewallů už nabízí funkci, která pro sdílení souborů a tiskáren zařídí veškerá nastavení. Ve firewallu Windows se jmenuje prostě „Sdílení souborů a tiskáren“ a najdete ji v menu „Výjimky“.

U starších firewallů, které nejsou příliš dobře přizpůsobeny pro Windows, musíte potřebné volby nastavit sami. Chcete-li aktivovat sdílení souborů a tiskáren, povolte příchozí datový provoz pro TCP porty 139 a 445 a pro UDP porty 137 a 138. Kromě toho musíte dovolit požadavek na odezvu v protokolu ICMP, aby ostatní počítače mohly do vašeho posílat příkaz „ping“.

Stealth mode: Na webu nepozorovaně

Chtěli byste surfovat po internetu, aniž by si vás při tom mohli povšimnout hackeři. Právě to slibuje „neviditelný režim“ (stealth mode), který nabízejí mnohé firewally.

Tato funkce opravdu dokáže váš počítat ukrýt před nežádoucími zvědavci. Jestliže se útočník pokusí příkazem „ping“ zjistit, zda je pod nějakou IP adresou skutečně připojen PC, dostane nesprávnou odpověď.

Jakmile ovšem otevřete nějakou webovou stránku nebo „chatujete“, pak je vaše IP adresa pro váš protějšek samozřejmě „viditelná“, neboť bez výměny IP adres protokol TCP/IP nemůže fungovat. Vaši přítomnost však prozradí i prosté prohledání portů.

Chcete-li surfovat skutečně anonymně, potřebujete k tomu nějakého prostředníka neboli „proxy“. Svá data pak předáváte jemu a teprve on je pak posílá k příslušnému cíli. Vaši IP adresu tedy zná jenom proxy. Velmi sofistikovaný systém, umožňující každému uživateli zatajit IP adresu, nabízí anonymizační nástroj TOR. Stáhnout si jej můžete z adresy **http://tor.eff.org**, jeho podrobný popis jsme přinesli v Chipu 4/2007.

Profesionální know-how: Co znamenají časté zprávy od Svchost

Tajuplná varovná hlášení firewallu dokáží otrávit i počítačové experty. Zajímá vás proto, jak těmto zprávám rozumět a co se za nimi skrývá.

Jedno z nejnesrozumitelnějších hlášení se vztahuje k procesu „svchost.exe“ (Service Host). Pod něj spadá několik služeb Windows, které jsou prováděny za pomoci různých DLL souborů. Tyto služby jsou potřebné například pro automatický update, rozpoznání USB zařízení nebo také pro tiskové funkce. Kdykoli systém potřebuje některou z těchto služeb, Windows spouštějí Svchost. Každá služba však vyvolává vlastní hlášku firewallu, což celou věc hodně komplikuje.

Chcete-li zjistit, zda se skutečně jedná o legitimní spojení, podívejte se nejprve na cestu k souboru a na vzdálenou adresu, s níž se služba pokouší spojit.

Soubor „svchost.exe“ musí být umístěn ve složce *C:\Windows\System32*. Důležité je zkontrolovat také přesný zápis názvu. Mnoho trojských koní se totiž pokouší schovat za podobně vypadajícím názvem, jako třeba „svhost.exe“, „svchosts.exe“ nebo „sychost.exe“.

Chcete-li vědět úplně přesně, které subprocesy a s nimi svázané služby Windows váš program vyvolává, spusťte freewarový „Process Explorer“, který lze stáhnout z webových stránek Microsoftu. Nástroj vám pak všechny běžící procesy vypíše. Vyberte proces „svchost.exe“. V detailním okně pak najdete všechny soubory, adresáře a položky systémového registru, které jsou s ním spojeny.

Po kliknutí na *Properties* se dozvíte další podrobnosti. Mezi nimi je také IP adresa a port, s nímž se program spojuje. Obvykle se „svchost.exe“ spojuje jen s lokálními adresami jako „127.0.0.1“ nebo „192.168...“. U všech jiných adres je třeba mít se na pozoru.

Předsunutá stráž: Nakolik chrání firewall v routeru

Snad u každého routeru je možné nastavit volbu „Firewall“. Dokáže však tato funkce držet krok s desktopovým firewallem?

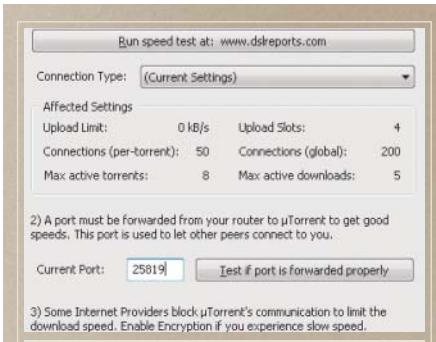
Stručná odpověď zní: Ne. Personální firewall může odchozí pakety přiřadit konkrétním programům a tak daleko přesněji zkontrolovat, zda byla dodržena určitá pravidla. Samozřejmě však firewall směrovače žádné škody nenadělá. Pokud jej aktivujete, měli byste ovšem v případě výskytu problémů se spojením překontrolovat také jeho nastavení.

Zdvojená ochrana: Jak správně zkombinovat dva firewally

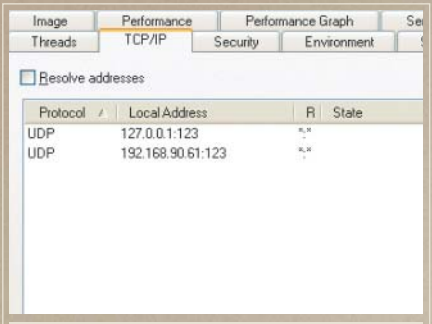
Mnozí výrobci zlepšují rozpoznávání virů použitím dvou virových skenerů. Chtěli byste podobně ochránit svou síť – nasazením dvou firewallů.

Provozovat dva firewally v jednom počítači s Windows nelze. Ve většině případů se jeden z nich vůbec nespustí. A pokud ano, blokují se oba programy navzájem, čímž práci na PC zcela znemožní.

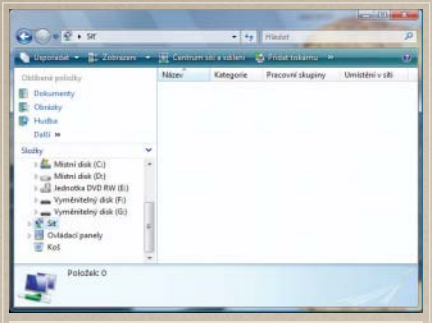
Dva firewally však můžete použít, pokud je nainstalujete do různých počítačů. Jeden z nich bude váš pracovní PC s obvyklým osobním firewallem, druhý bude fungovat jako směrovač a ochrání rozhraní mezi vaší sítí a internetem. Takové řešení se často používá pod Linuxem a předpokládá dobré znalosti TCP/IP. Dobrý opensourcový firewall najdete například na *www.m0n0.ch/wall* („0“ jsou nuly). Náklady se vám však vyplatí jen v případě, že chcete chránit opravdu důležitá data. Pro běžný provoz zcela postačí jeden z firewallů, které jsme testovali v předchozím článku. *Valentin Pletzer*



BITTORENT: Jsou-li v osobním firewallu uvolněny správné porty, bude se dařit i filesharing.



VOLBA PORTŮ: Nástroj „Process Explorer“ vám ihned ukáže, na které porty je váš program napojen.



SDÍLENÍ SOUBORŮ: Firewall blokuje přístup, v přehledu sítě už se žádný počítač nezobrazuje.