

# Chraňte se před hackery

## Jakou službu vám udělá osobní firewall?

Když se jednoho dne připojíte k Internetu, musíte se rozhodnout, zdali a jak budete chránit data uložená na vašem počítači před zraky nezvaných či zvědavých návštěvníků. Musíte si zvyknout na to, že řada aplikací, které na svém počítači používáte, komunikuje s Internetem, aniž by vám o tom podávaly nějakou zprávu. Aby se tak dělo jen s vaším souhlasem, vznikl typ aplikací s názvem osobní firewall - anglicky personal firewall nebo desktop firewall. Pojďme se blíže podívat na nejnovější z nich – Tiny Personal Firewall od Tiny Software.

Z hlediska přenosu dat stojí personal firewall mezi Internetem a vaším počítačem. Ačkoli hovoříme zatím pouze o Internetu, stejnou službu vám personal firewall udělá i v lokální síti LAN. Ochrání osobní počítač tak, aby nikdo nepovolaný nemohl proniknout dovnitř a zároveň aby nikdo nemohl odeslat data z počítače ven.

Personal firewall dohlíží na veškerou síťovou aktivitu počítače a umožňuje komunikovat jen programům, které prohlásíte za důvěryhodné. Při každém pokusu o neautorizovaný přenos dat vyvolá firewall poplach.

## Poslání personal firewallu

Váš počítač komunikuje oběma směry – proud dat míří z Internetu do vašeho počítače a jiný proud dat směřuje z vašeho počítače ven. Internet je mimořádně plodným pro vznik a šíření nejrůznějších typů zákeřných aplikací jako jsou trojské koně, viry či špehové. Zejména trojské koně – programy, které předstírají, že jsou přátelskou aplikací – mají na svědomí únik dat.

Je samozřejmě důležité provádět antivirovou kontrolu počítače, která přítomnost většiny nepřátelských aplikací odhalí. V průběhu vašeho internetového života se přesto může stát, že nějaký trojský kůň se do vašeho počítače dostane, třeba jako příloha emailu od dobrého známého nebo nerozvážným downloadem z webových stránek. Personal firewall je proto nezbytným doplňkem každého počítače, pokud to s ochranou vašich dat myslíte skutečně vážně.

Smyslem personal firewallu ale je, aby v případě, kdy už se nějakým způsobem některá zákeřná aplikace dostane do počítače, odhalil okamžitě její pokus o navázání komunikace a zabránil jí ve spojení s mateřským serverem na Internetu. Antivirové programy tedy odhalují přítomnost, kdežto personal firewally činnost nepřátelských aplikací.

## Jak program pracuje?

Tiny Personal Firewall je po instalaci nastaven tak, že nezná žádnou aplikaci provozovanou na daném počítači. Proto je uživatel v okamžiku, kdy se některá aplikace poprvé přihlásí s požadavkem na komunikaci po Internetu, dotázán, zda-li má aplikaci a její komunikaci považovat za důvěryhodnou, zapsat si ji do tabulky oprávněných aplikací a povolit její provoz. Jako první se o povolení obvykle přihlašují nejběžnější programy typu prohlížeč a poštovní klient (Internet Explorer, Netscape Navigator, Eudora, Outlook Express).

Zde musí být uživatel maximálně obezřetný, protože může povolit aplikaci, která se tváří jako Outlook Express a přitom jde o trojského koně s falešným názvem.

### **Zabezpečení pomocí šifrovaných podpisů**

Předstírání falešného jména je oblíbenou technikou trojských koňů. Tomuto problému čelí Tiny Personal Firewall vytvářením tabulky oprávněných aplikací a přidělených rozsahů portů. Každá oprávněná aplikace získává po vaší předchozí autorizaci vlastní zašifrovaný podpis, který personal firewallu předkládá s každým svým požadavkem na povolení přenosu dat. Pokud tento podpis souhlasí se záznamy personal firewallu, komunikace je umožněna.

### **Bezpečné sdílení adresářů**

Řekněme, když máte ve svém počítači adresář, který potřebujete sdílet, nicméně jen s vybranými uživateli v rámci lokální sítě nebo Internetu. Windows umožňují sdílení adresáře chráněné přístupovým jménem a heslem. Potřebujete-li ale zpřístupnit přístup k těmto adresářům pouze na konkrétní IP adresu lokální sítě nebo Internetu, Windows vám nepomohou. V tomto případě můžete výhodně využít Tiny Personal Firewallu, který umí omezit přístup k Vašemu počítači jen z jedné nebo z několika vybraných IP adres. Pak budou moci k Vašemu počítači přistupovat přes lokální síť například jen kolegové z kanceláře, nikoli však lidé z jiných oddělení. Pohled na nastavení bezpečnostní politiky vašeho Tiny Personal Firewallu můžete také obrátit a konkrétním IP adresám přístup k počítači zakázat.

### **Rozhodování firewallu aneb stavová inspekce**

TCP/IP je jediným způsobem komunikace v rozsáhlých sítích jako je Internet a je běžnou formou komunikace v lokálních sítích. IP protokol zodpovídá za identifikaci každého paketu, proto ke každému přidává takzvanou hlavičku. V ní jsou informace o typu protokolu, cílové a zdrojové adrese a řada dalších. Firewall vyhodnocuje, zda se informace z hlavičky paketu shodují s jeho předpoklady a s bezpečnostními pravidly. Při svém rozhodování bere firewall v úvahu i informace o portech, které si jednotlivé aplikace otevírají a jimiž komunikují se světem. Firewall dokáže zajistit, aby tyto aplikace a služby neumožnily nežádoucím návštěvníkům proniknout dovnitř vašeho počítače skrz jimi otevřený port. Schopnost prověřovat informace a fundovaně rozhodnout, zda-li paket propustit dovnitř nebo zahodit, se jmenuje stavová inspekce.

### **První kroky po nainstalování**

Tiny Personal Firewall je určen pro Windows 95/98/NT/ME/2000. Program po nainstalování zabere na harddisku příjmných 517 kB. Instalace trvá jen několik sekund a vyžádá si jeden restart.

Tiny Personal Firewall má zabudovány tři typy bezpečnostní politiky a při prvním spuštění budete požádáni o výběr jedné z nich. Implicitně je TPFW nastaven na střední úroveň zabezpečení. To znamená, že veškerá komunikace je zablokována, ale firewall sleduje činnost vašich aplikací a automaticky vyvolá dialog s nabídkou nastavení filtrovacího pravidla pro povolení síťové aktivity. Nastavení filtrovacího pravidla můžete později libovolně změnit.

Protože některé aplikace využívají pro svoji komunikaci celou plejádu portů, můžete si usnadnit práci a říci Tiny Personal Firewallu, že daná aplikace může využívat všechny porty, které potřebuje. Vždy ale máte možnost ručně povolovat každý port zvlášť.

Mějte na paměti, že čím více portů otevřete, tím zranitelnější váš počítač bude. V tomto případě ani tak nezáleží na renomé autora programu – připomeňme si nedávno

objevenou závažnou bezpečnostní díru v programu Outlook a Outlook Express. Personal firewall je jen pomůckou, která vám má pomoci ochránit váš počítač, ale určitá obezřetnost je vždy na místě.

Jistě dobrou zprávou je, že Tiny Personal Firewall prochází trvalým vývojem. Bez zajímavosti není ani fakt, že tento produkt je jednou z klíčových komponent systému centrální správy zabezpečení počítačů (CMDS), který Tiny Software v současné době vyvíjí pro U.S. AirForce.

----- finito -----