Lsti, fígle a triky pro domácí firewally

Ochrana počítače před útoky z internetu je dnes aktuální téma. Nepochybujeme, že ani vy nechcete zůstat pozadu a přemýšlíte, jak svůj počítač zabezpečit. Pokusíme se vám tento úkol usnadnit a poskytnout několik tipů. Zjistíte, na co se zaměřit, který firewall potřebujete a jak jej optimálně nakonfigurovat.

Sada tipů a triků pro správné nastavení a používání firewallu (CD)

DAVID ČEPIČKA, HERMANN APFELBÖCK, CHRISTIAN LÖBERING A DAVID WOLSKI

Zapnout a mít jistotu. Tak nějak by měl fungovat každý správný firewall. Při jeho konfiguraci a každodenním používání se však často objevuje řada nečekaných problémů. Firewally například vydávají hlášení, která s vaší prací zdánlivě vůbec nesouvisejí. A přesto firewall hlásí stále nové pokusy o přístup z internetu a do internetu.

Abyste ochránili svůj počítač skutečně dokonale, objasníme vám v tomto článku nejnovější způsoby přístupu programů k internetu a z internetu a také vám prozradíme, jak na tyto metody váš firewall připravit. Přečtete si řadu užitečných tipů pro použití Zone Alarmu, dále se budeme věnovat firewallu zabudovanému ve Windows XP SP 2 a probereme i nasazení v současné době cenově výhodných hardwarových firewallů.

Útoky na počítače

Z hlediska počtu útoků na počítače uplynulý rok ukázal jednoznačný trend: množství útoků se neustále zvyšuje. Kupříkladu firma *Sophos*, která se zabývá vývojem antivirových programů, zaznamenala za rok 2004 asi o 50 procent více nových virů, než tomu bylo v roce 2003. I počet útoků hackerů v loňském roce vzrostl a nic nenasvědčuje tomu, že by se tato situace měla nějak zásadně změnit. Útoky na počítače se dnes vedou třemi způsoby: pomocí škodlivých kódů, hackingem a phishingem. Cílem útoků se bohužel stále více stávají i počítače běžných uživatelů.

1. Škodlivý kód: jak napadnout počítač tímto způsobem

Většina útoků na váš počítač probíhá přes různé nebezpečné programy jako červy či trojské koně. Hackeři, kteří takové programy píší, jsou velmi dobře obeznámeni s bezpečnostními trhlinami ve Windows i v jiných často používaných programech a šikovně těchto slabých míst využívají.

Jako jeden příklad za všechny lze uvést červ Bizex. Ten nainstaluje do napadeného počítače keylogger (utilitu, která zaznamenává do souboru všechny aktivity uživatele – stisknuté klávesy, otevřená okna, spuštěné programy, otevřené složky, obsah schránky, systémové události apod.), jenž zaznamenává stisky kláves a další události, pokud se pohybujete po internetových stránkách některých bank. Rozšiřuje se pomocí instant messengeru **ICQ** (tento jinak velmi zdařilý zdarma dostupný komunikační nástroj vám nabízíme ve verzi 5.03 Lite Edition určené pro Windows 98/ME, 2000 a XP NA NAŠEM CD, popřípadě jej můžete získat na internetové stránce **www.icq.com**, ICQ_SETUP.EXE, 4,07 MB). Ve zprávě se objevuje odkaz, který ukazuje na zvukové schéma pro ICQ. Klepnutím na tento odkaz se však stáhne ještě další programek, jenž využívá slabiny Internet Exploreru a tímto způsobem do systému „propašuje" již zmiňovaný keylogger. Nakonec rozešle tento odkaz na všechny kontakty uvedené v adresáři ICQ. Podrobnější informace o červu Bizex mohou zájemci získat kupříkladu v encyklopedii virů na internetové stránce **www.viruslist.com**.

Další škodlivé kódy se rozšiřují tak, že nemusíte vůbec na nic klepat. Klasickými příklady jsou červi Blaster a Sasser, které se opět množí díky chybě v zabezpečení Windows. Ačkoliv byla pro toto slabé místo už před delší dobou vydána záplata, jsou tito červi stále ještě značně rozšířeni.

Prodejci antivirových a jiných programů pro zabezpečení počítače často rádi předvádějí následující test: připojí počítač, který není nijak chráněný a na němž jsou Windows XP bez jakýchkoliv záplat, k internetu a předpoví, že bude trvat přibližně jednu minutu, než se do systému dostane první virus. A věřte nebo ne, většinou mají pravdu. Jenom někdy to trvá pět až deset minut, než se v systému bez záplat, firewallu a antiviru objeví první nákaza.

Útočníci hromadným útokem škodlivého softwaru na počítač většinou sledují dva cíle. Za prvé chtějí z počítače získat citlivá data, jako jsou údaje pro přístup k bankovnímu účtu nebo licenční klíče k různým programům, nebo chtějí počítač jednoduše ovládnout. To se jim může podařit kupříkladu pomocí tzv. *bots* (botů – zkratka od slova *robots*). Infikovaný počítač pak přihlásí k nějakému centrálnímu serveru na internetu a čekají na příkazy. Několik set nebo tisíc počítačů napadených boty pak vytvářejí tzv. *botnet* (slovo je odvozeno od slov *robots* a *network*). Autor pak takovou síť využívá například pro útoky typu DoS (viz dále), cílené na internetové stránky. Botnet lze také pronajmout spammerům, kteří přes něj hromadně posílají množství reklamních e-mailů.

2. Phishing: krádež dat pomocí stále rafinovanějších triků

Jako *phishing* je označován způsob, jak prostřednictvím falešných e-mailů či internetových stránek získat uživatelova citlivá data. Zloději používají při phishingu stále rafinovanější metody. Například posílají e-maily, které se tváří, jako kdyby pocházely přímo od vaší banky a přitom lákají uživatele na falešné internetové stránky, do nichž mají zadat svoje údaje.

Možná vás napadne, že pokud na takový trik někdo naletí, je to jeho problém, Pak pravděpodobně ještě neznáte všechny způsoby, jak na vás phishing může zaútočit. Například odkaz, který otevře internetovou stránku vaší banky a přitom zobrazí malé pop-up okno, které vás vyzve k zadání vašich citlivých dat. Stránka banky je skutečně pravá, pop-up okno sice také vypadá věrohodně, jedná se však o podvod (viz obrázek).

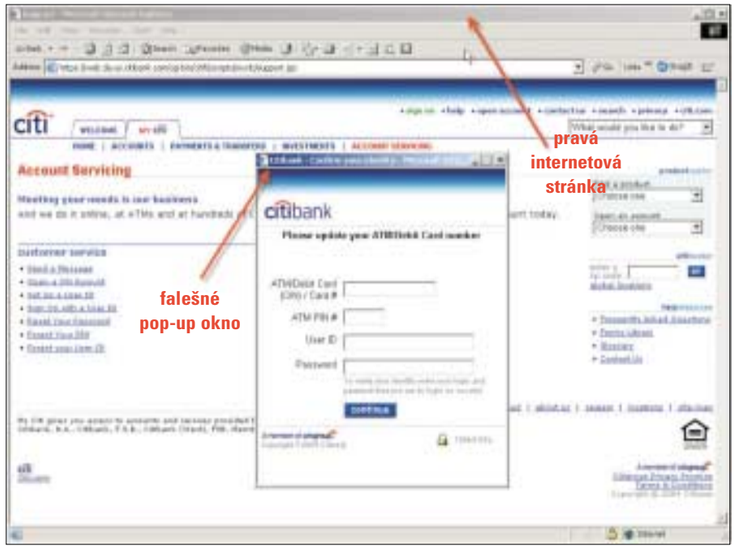
Proto platí: spouštějte internetové stránky bank a podobných institucí, kam zadáváte nějaké osobní údaje, vždy pouze zadáním skutečné adresy do adresního řádku prohlížeče. Nikdy neotevírejte tyto stránky klepnutím na internetový odkaz v e-mailech. Sbírku triků využívaných při phishingu můžete nalézt i na internetu na adrese **www.antiphishing.org**.

3. Hacking: útoky na počítače domácích uživatelů

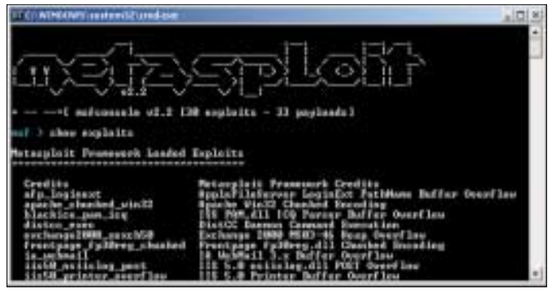
Pokud jste připojeni k internetu, pak firewall často hlásí pokusy o proniknutí do systému. Přesto jen málokdy za těmito útoky stojí hacker s černou kapucí, který se snaží vloupat do vašeho počítače. Daleko častěji se jedná o varovná hlášení způsobená červy, tedy nějakým druhem škodlivého softwaru, který se dokáže sám šířit a dokáže sám vyhledat v internetu zranitelné počítače.

V některých případech však přece jen stojí za útoky na počítač člověk. Často jsou to tzv. *Script-Kiddies* – to jsou lidé, kteří na internetu pomocí skenerů portů náhodně vyhledávají otevřené porty. Pakliže takový naleznou, použijí další druh utilit. Většinou se jedná o nástroje vyvíjené pro potřeby síťových administrátorů. K nejúčinnějším patří v současnosti program **Metasploit**. Tuto zdarma dostupnou utilitu naleznete NA NAŠEM CD, popřípadě na internetu na adrese **www.metasploit.com** (FRAMEWORK-2.3.EXE, 17,1 MB). Zajímavá je tím, že obsahuje nástroje, které využívají aktuální bezpečnostní trhliny ve Windows, Unixu a v systémech Apple. Uživatel na profesionální úrovni tak může ve své vlastní síti diagnostikovat její slabá místa.

Velmi málo odolné vůči hackerům jsou také sítě WLAN. Bezdrátové sítě jsou totiž až na výjimky špatně zabezpečovány. Proto představují takřka ideální výzvu, pozvánku k bezplatnému a anonymnímu surfování.



▲ **Perfektně utajeno: po klepnutí na odkaz v podvodném e-mailu se sice otevře pravá internetová stránka vaší banky, ale do popředí vyskočí falešné pop-up okno, které s bankou nemá nic společného. Jediným jeho smyslem je zjistit vaše přihlašovací údaje.**



◀ **Utilita pro analýzu: program Metasploit určený pro správce sítí rozpozná trhliny v zabezpečení různých operačních systémů a pak je využívá.**

Utility pro útoky na sítě WLAN se dají najít na internetu, například programy **Airsnort** či **WEP-Crack**. Tyto v angličtině komunikující programy dokáží prolomit šifrování WEP, které používají právě sítě WLAN. Snadno si tedy můžete sami udělat obrázek o tom, v jakém bezpečí asi vaše data jsou.

Administrátorům sítí je určena i utilita **Ettercap 0.7.2**, kterou vám nabízíme i NA NAŠEM CD jako soubor ettercap-NG-0.7.2.tar.gz (1,06 MB). Dostupný je též na internetu na adrese **ettercap.sourceforge.net**. Pomocí tohoto freewaru zjistíte, nakolik je náchylná vaše WLAN síť pro útoky typu „*Man in the Middle*“. Program se totiž postaví do cesty mezi váš počítač s rozhraním WLAN a Access Point a analyzuje možná slabá místa.

Upozornění: Výše zmiňované utility používejte pouze pro testování bezpečnosti vašeho systému nebo vaší počítačové sítě!

Softwarové firewally

Softwarové firewally vám prokáží při odrážení útoků z internetu dobré služby. Pokud je firewall správně nakonfigurovaný, blokuje všechna nevyžádaná data a neoprávněné požadavky na přístup do vašeho počítače. Tím jej chrání před červy rozšířenými na internetu a stejně tak poskytuje ochranu před útoky hackerů. Tímto způsobem lze do jisté míry ochránit i počítač, na němž nejsou nainstalovány všechny bezpečnostní záplaty. Ale i softwarové firewally mají své chyby. V následujícím textu vám prozradíme, jak je používat a kde jsou jejich slabiny.

4. Výhody softwarových firewallů: co dokáží tyto programy v praxi

V současnosti neexistuje žádný důvod, proč byste neměli mít na svém počítači nainstalovaný firewall – vždyť se jedná o slušné programy pro ochranu vašeho počítače a navíc jsou v řadě případů k dispozici zdarma. Jako typický případ lze uvést **Zone Alarm 5.5.062.011**, který je ve základní verzi pro soukromé použití dostupný zdarma. Naleznete jej NA NAŠEM CD jako soubor ZLSSETUP_55_062_011.EXE o velikosti 6,36 MB, popřípadě jej můžete stáhnout z internetové stránky **www.zonelabs.com**.

Jako alternativu k Zone Alarmu vám nabízíme **McAfee Personal Firewall Plus**, který si můžete jako 30denní zkušební verzi zdarma po registraci stáhnout na internetové stránce **us.mcafee.com**.

Uživatelé, kteří se spokojí s nejjednodušší variantou, určitě přivítají firewall obsažený ve standardní instalaci Windows XP s nainstalovaným Service Packem 2.

Většina softwarových firewallů se vyznačuje jednoduchou konfigurací. Obvykle pracují s filtrem, který má zabudovaný seznam aplikací a uživateli vždy ohlásí, pokud se bude pokoušet o přístup nějaká aplikace, která v seznamu není a která nemá definovaná žádná pravidla o přístupu k internetu. Tímto způsobem je pak uživatel informován o všem, co se na jeho počítači odehrává.

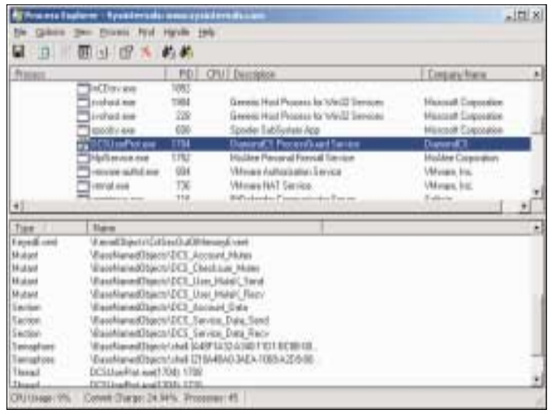
5. Slabiny softwarových firewallů: popis několika jejich nevýhod

Softwarové firewally jsou napadnutelné. Stačí jeden škodlivý kód, jenž se do počítače dostane kupříkladu prostřednictvím elektronické pošty. Ten může firewall jednoduše vypnout nebo vyřadit z provozu a poté může na počítači řádit dle libosti. Proto je nutné ke každému firewallu pořídit ještě některý z antivirových programů, například pro soukromé použití zdarma dostupný **Antivir PersonalEdition Classic 6.30**. Najdete jej i NA NAŠEM CD, a to jako soubor AVWINSFX.EXE o velikosti 6,03 MB, popřípadě na internetové adrese **www.free-av.com**.

Na druhou stranu každý program má své silné a slabé stránky. Z hlediska bezpečnosti systému jsou nejnebezpečnější ty aplikace, které se připojují k internetu. Tato skutečnost se samozřejmě týká i firewallu, jelikož se jedná o klasický program kombinovaný s on-line aplikací. Mohlo by se tedy na první pohled zdát, že instalací firewallu naopak počítač učiníme zranitelnějším. Ale i přes tyto slabiny je instalace firewallu prakticky nezbytná. Daleko bezpečnější je však z tohoto pohledu surfování kontrolované hardwarovým firewallem.

Seznam utilit pro větší bezpečnost systémů

Program	Kategorie	Cena	Operační systém	Internetová adresa, název a velikost souboru
Antivir Personal Edition Classic 6.30	antivirový program	pro soukromé použití zdarma	Windows 95/98/ME, NT4, 2000, XP	NA NAŠEM CD nebo na **www.free-av.com** (AVWINSFX.EXE, 6,03 MB)
Airsnort 0.2.7e	dešifrování klíče používaného pro šifrování přenosu v sítích WLAN	zdarma	Windows 98/ME, NT4, 2000, XP	**airsnort.shmoo.com** (204 KB)
Ettercap 0.7.2	analýza síťového provozu	zdarma	Windows 2000, XP	NA NAŠEM CD nebo na **ettercap.sourceforge.net** (ettercap-NG-0.7.2.tar.gz, 1,06 MB)
Fli4l 2.0.8	router	zdarma	Windows 95, 98/ME, NT4, 2000, XP, Linux	NA NAŠEM CD nebo na **www.fli4l.de/english/e_download.htm** (FLI4L.ZIP, 6,75 MB)
ICQ 5	instant messenger	zdarma	Windows 98/ME, NT4, 2000, XP	NA NAŠEM CD nebo na **www.icq.com** (ICQ_SETUP.EXE, 4,07 MB)
Metasploit 2.3	analýza síťového provozu	zdarma	Windows 98/ME, NT4, 2000 a XP	NA NAŠEM CD nebo na **www.metasploit.com** (FRAMEWORK-2.3.EXE, 17,1 MB)
Norton Personal Firewall 2005	firewall	2 040 Kč	Windows 98/ME, 2000, XP	**www.symantec.cz**
WEP-Crack 0.1.0	dešifrování klíče používaného pro šifrování přenosu v sítích WLAN	zdarma	Linux	**wepcrack.sourceforge.net** (7 KB)
Zone Alarm 5.5.062.011	firewall	pro soukromé použití zdarma	Windows 98/ME, 2000, XP	NA NAŠEM CD nebo na internetové adrese **www.zonelabs.com** (ZLSSETUP_55_062_011.EXE, 6,36 MB)



◀ **Napadnutelný: mnoho aplikací pro ochranu systému je možné ukončit už pomocí jednoduchého Správce úloh. Toho samozřejmě viry a červi s oblibou využívají.**

Konfigurace firewallu

Softwarový firewall vás bude chránit pouze tehdy, pokud jej správně nakonfigurujete. V této části najdete informace o základních principech, které je třeba při konfiguraci firewallu dodržet.

6. Izolace počítače od okolí: trénujte svůj firewall

Pokud používáte svůj počítač především k surfování a práci s elektronickou poštou, není správná konfigurace firewallu nic složitého. Při standardním nastavení pracuje firewall v režimu učení. Pokud se libovolný program pokusí o přístup k internetu, pak firewall nejprve tento pokus zablokuje a následně se zeptá, zda dovolíte aplikaci přístup k internetu.

U většiny firewallů pak máte na výběr ze dvou odpovědí – zamítnout nebo povolit. V závislosti na konkrétním firewallu je vaše rozhodnutí zpravidla buď okamžitě uloženo, popřípadě platí pouze do doby, než počítač znovu pustíte. V tomto případě pak existuje ještě další možnost, která vám umožní vytvořit vlastní pravidlo.

Cílem je vytrénovat váš firewall tak, aby směly do internetu přistupovat pouze vámi používané internetové aplikace. Ve většině případů je taková konfigurace poměrně jednoduchá, neboť jednotlivá hlášení k různým utilitám bezprostředně souvisí s vaší prací na počítači. Spustíte-li například program ICQ, položí vám firewall dotaz, zda smí aplikaci ICQ.EXE povolit přístup k internetu. Souvislost mezi akcí a vydaným hlášením je v tomto případě jednoznačná.

7. Pozor: viry se maskují jako názvy systémových programů

Obtížnější je situace, kdy souvislost zmíněná v poslední větě minulého tipu zas až tak jasná není. To může být případ systémových komponent Windows. Některé se pokouší připojit k internetu už po startu Windows, čímž okamžitě vyvolají hlášení firewallu. Nejčastějším kandidátem přitom bezesporu je aplikace SVCHOST.EXE. Některé firewally tento program nazývají také *Generic Host Process for Win32 Service*. Jedná se o systémovou komponentu, kterou využívají služby Windows.

Některé firewally, jako například **Norton Personal Firewall 2005**, tuto komponentu automaticky důkladně prověří a pokud se skutečně jedná o modul systému Windows, pak ji nechají projít do internetu, aniž by vydávaly nějaké hlášení.

Pokud firewall zobrazí upozornění k modulu SVCHOST.EXE, je třeba zvýšit pozornost na nejvyšší míru. Řada virů se totiž skrývá právě pod podobně znějícími názvy jako SVCHOST.EXE se znakem „**0**“ místo „**O**“ nebo SVCHOSTS.EXE s nadbytečným písmenem „**s**“ v názvu, popřípadě jako soubor SVCHOST32.EXE. Programátoři virů, trojských koní a spywaru tento trik používají velmi často. Své výtvory také často nazývají například WINSYNC.EXE či MSIWIN84.EXE, a to proto, aby uživatelům vsugerovali, že se jedná o systémové komponenty.

Pokud si budete chtít ověřit, zda nějaká aplikace náhodou není riziková nebo přímo nebezpečná, pak vám může pomoci internetová stránka **www.reger24.de/prozesse**. Tam je uveden seznam více než 500 programů, které navazují přístup k internetu, a jejich stručný popis (v angličtině).

8. Neprůhledná a zvláštní hlášení firewallu

Často se stává, že hlášení, která firewall vydá, nemůže uživatel nikam zařadit – kupříkladu neví, proč daný program vůbec na internet potřebuje. Pokud například zkopírujete text z internetové stránky do dokumentu ve Wordu, potřebuje najednou Word přístup k internetu, i když je jasné, že všechna data jsou již ve schránce Windows. Nebo například poslouchátе hudbu ve formátu MP3 a váš program pro přehrávání potřebuje přístup k internetu.

V takových případech se nejprve přesvědčte, zda odpovídající EXE soubor v hlášení firewallu skutečně odpovídá nějaké vám známé aplikaci. Nechte si u firewallu zjistit úplnou cestu ke spouštěcímu souboru a zkontrolujte, zda cesta uváděná firewallem je totožná s cestou k dané aplikaci. Kupříkladu soubor WINWORD.EXE se při standardní instalaci nachází ve složce *C:\Program Files\Microsoft Office*. Pokud firewall ohlásí, že se tento soubor nachází ve složce *C:\Windows*, je to přinejmenším podezřelé.

Obecně vzato: i když obě zadání cest souhlasí, můžete napoprvé přijmout konzervativnější řešení a přístup k internetu zakázat. Pokud i poté všechno funguje jak má, pak si jenom musíte zapamatovat, že jste programu zablokovali přístup na internet. Jestliže byste někdy příště chtěli tomuto programu přístup k internetu povolit, pak je nutné příslušná pravidla v nastavení firewallu upravit ručně.

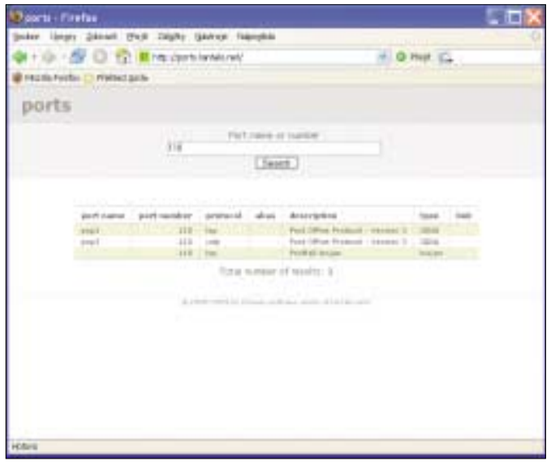
Vysvětlení: v našem příkladě Word při kopírování textu z internetové stránky potřebuje získat přístup k internetu, neboť potřebuje přenést i způsob formátování textu. Program pro přehrávání hudby se zase snaží získat informace o přehrávaném CD nebo o MP3 souboru.

▲ **Zone Alarm: typické dialogové okno firewallu s varováním oznamujícím pokus o připojení k internetu.**

9. Těžký případ: konfigurace firewallu ve výjimečných situacích

U on-line aplikací určitého typu režim „učení“ u některých firewallů selhává. I když je program na seznamu aplikací, jimž je přístup do internetu povolen, komunikace stejně nefunguje. To se často stává u aplikací pro IP telefonii a pro videokonference, někdy je to problém u her a u programů typu ICQ. U těchto aplikací je nutné zabezpečit nepřetržitý tok dat. Proto se data neposílají pouze přes jeden port, nýbrž se ke stejnému účelu využívají porty dva nebo více. Na těchto ostatních však doposud žádná komunikace daného programu neprobíhala. Firewally v takových případech zasáhnou a takovou komunikaci jednoduše odmítnou.

Řešení problému závisí na konkrétním firewallu. Zone Alarm například disponuje nastave-



Informace o portech: který program používá daný port? Tuto informaci získáte v databázi, která se nachází na internetové stránce ports.tantalo.net. Na ní najdete, které porty využívají obvyklé aplikace a které viry a trojské koně.

ním *Server*. Program s tímto oprávněním může přijímat data bez předchozího vyslání požadavku.

U ostatních firewallů – mimochodem i u firewallu ve Windows XP – musíte vytvořit nové pravidlo, které povolí posílání dat i přes jiný port. Jeho číslo zjistíte zpravidla z nápovědy k danému programu, popřípadě na internetových stránkách podpory výrobce programu. Velmi rozsáhlý seznam portů naleznete na internetové stránce **www.iana.org/assignments/port-numbers**. Další databáze portů s asi 7 000 záznamy je na stránce **ports.tantalo.net**. Informace v obou seznamech se vzájemně výtečně doplňují.

Upozornění: Otevírejte porty pouze tehdy, pokud je to nezbytné. Obecně platí, že otevřený port představuje bezpečnostní riziko, pokud program, který jej využívá, obsahuje trhlinu v zabezpečení, jež se dá zneužít. Proto firewall s příliš velkým počtem výjimek nemusí znamenat zvýšení úrovně zabezpečení.

Zone Alarm

Zdarma dostupný **Zone Alarm 5.5.062.011,** který naleznete NA NAŠEM CD a o němž jsme se již zmiňovali, velmi úspěšně odráží útoky vedené na váš počítač z internetu a kromě toho disponuje velmi slušnou ochranou sebe sama. Kromě toho vám aplikace ohlásí všechny programy, které chtějí získat přístup k internetu a poskytuje přehledný protokol o všech aktivitách probíhajících v počítačové síti.

10. Kontrola: automatické vytvoření pravidel, případně jejich ruční úprava

Jakmile nějaká aplikace chce získat přístup k internetu, zeptá se vás Zone Alarm, zda jí to dovolíte. Úplnou cestu ke spouštěcímu souboru aplikace však bohužel neposkytuje. Dozvíte se ji až tehdy, když pro ni Zone Alarm vytvoří pravidlo. V případě pochybností byste rozhodně měli pokus o přístup k internetu zablokovat a poté zkontrolovat cestu v rozhraní firewallu klepnutím na položku *Program Control* a dále na záložku *Programs*. Na tomto místě firewall uchovává seznam všech aplikací, jež se pokoušely získat přístup k internetu. Pokud chcete nějaké aplikaci přístup k internetu povolit, klepněte levým tlačítkem myši do sloupečku *Access*. Na výběr máte možnosti *Allow* (*Povolit*), *Block* (*Zablokovat*) a *Ask* (*Dotázat se*). Pokud zvolíte poslední možnost, bude se vás ptát firewall pokaždé, když se bude daný program pokoušet připojit k internetu. Klepnutím pravým tlačítkem pak máte možnost aplikaci ze seznamu odebrat nebo naopak přidat jinou.

Zone Alarm většinou spolehlivě rozpozná, pokud se nějaký program chová jako aplikace typu *Server*, upozorní na tuto skutečnost uživatele a požádá ho o souhlas. Pokud by bylo ještě později nutné pro aplikaci tohoto typu vytvořené pravidlo upravit, stačí klepnout v Zone Alarmu v seznamu aplikací do sloupce *Server*.

11. Tipy pro Zone Alarm: individuální nastavení firewallu

Vedle pravidel nabízí Zone Alarm i další možnosti nastavení. Například můžete vypnout zobrazování nadbytečných varování (menu *Alerts & Logs*) nebo můžete optimalizovat konfiguraci pro místní síť. Tato optimalizace se provádí prostřednictvím menu *Firewall* na záložce *Zones*, pokud klepnete pravým tlačítkem a z kontextového menu vyberete položku *Add/IP Range*. Zde můžete zadat rozsah IP adres, který je určen pro počítače v síti. Jako popis (*Description*) uveďte název vaší sítě nebo třeba jen výraz *LAN*.

Firewall ve Windows XP

Před útoky z internetu váš počítač poměrně spolehlivě ochrání i firewall integrovaný ve Windows XP s nainstalovaným Service Packem 2. Ten, kdo hledá utilitu, která jej bude jen minimálně zatěžovat dotazy, bude s tímto programem od Microsoftu určitě spokojen.

Ovšem i tato aplikace má svoje stinné stránky. Existují škodlivé programy, které dokáží tento firewall obejít. Ochrana před útoky tedy není na příliš vysoké úrovni. V souboru protokolu se sice ukládají záznamy o internetovém provozu, ovšem bez jmen aplikací. Tento firewall rovněž neposkytuje možnost filtrování aplikací. O programech, které chtějí přístup k internetu, firewall informuje pouze tehdy, pokud je pro ně nutno otevřít port a pokud chtějí fungovat jako server. Ale ani toto vždy neplatí. Ovšem ten, kdo chce i přes tyto slabiny uvedený firewall používat, najde na následujících řádcích několik užitečných tipů.

12. Konfigurace: zapnutí firewallu a vytváření pravidel

Po instalaci Service Packu 2 je firewall ve Windows XP standardně aktivován. Jeho konfigurace se provádí v Ovládacích panelech poklepáním na ikonu *Brána firewall systému Windows*.

Pro volbu *Zapnuto (doporučeno)* je zde k dispozici upřesňující položka *Nepovolovat výjimky*. Ta se týká aplikací uvedených na záložce *Výjimky*. Programy, které se na zmíněné záložce vyskytují, smějí vystupovat v pozici *Server*, tzn. že firewall propouští z internetu do počítače i ta data, která nebyla operačním systémem vyžádána. Pakliže umístíte zatržítko před položku *Nepovolovat výjimky*, smějí popisované aplikace data do internetu zasílat a na vyžádání data přijímat. Vypnuta je tedy pouze možnost fungovat jako *Server*. Pokud pouze surfujete po internetu a přijímáte či odesíláte elektronickou poštu, můžete tuto volbu bez obav deaktivovat.

Firewall ve Windows XP: tento nástroj je součástí Windows XP s nainstalovaným Service Packem 2 a jeho nespornou výhodou je, že vás jen málokdy bude obtěžovat nějakým hlášením.

Pravidla: dříve než smí libovolný program otevřít port pro komunikaci, požádá firewall v XP uživatele o povolení. Na základě jeho odpovědi pak vytvoří příslušné pravidlo.

Výše popisovaný seznam aplikací se vytváří na základě hlášení firewallu. Pokud spustíte například program pro IP telefonii, který pracuje jako *Server*, zeptá se vás firewall, zda ho chcete přidat k seznamu aplikací, které smějí v rámci internetu komunikovat.

Popisovaná operace se však ne vždy podaří – důsledkem je pak chybná funkce aplikace. Pak je třeba vytvořit pravidlo manuálně. Přesuňte se proto na záložku *Výjimky* a stiskem tlačítka *Přidat program* vložte odkaz na daný program do seznamu. Pokud aplikace stále nefunguje korektně, je potřeba na stejné záložce uvolnit port, a to pomocí tlačítka *Přidat port*.

Je pravda, že na většině počítačů pracuje firewall integrovaný ve Windows XP bez problémů. Pokud byste se přesto rozhodli používat jiný firewall, měli byste ten integrovaný ve Windows XP vypnout. V opačném případě by se mohly vzájemně rušit.

Upozornění: Microsoft přiznal, že jeho firewall má v oblasti uvolňování portů značné slabiny a na téma *Výjimky* připravil speciální návody, které naleznete na internetové stránce **support.microsoft.com/default.aspx?scid=kb;cs;842242**.

Hardwarové firewally

Jako hardwarový firewall můžete nakonfigurovat samostatný počítač s operačním systémem **Linux** nebo **Free BSD**, další možností je koupě samostatného zařízení, na němž běží nějaká na kapacitu nenáročná verze Linuxu. Na následujících řádcích naleznete tipy pro konfiguraci hardwarového firewalu, a to jak na bázi samostatného počítače s operačním systémem Linux, tak na bázi samostatného zařízení. Všechny tipy jsou určeny především pro uživatele připojující se k internetu přes ADSL.

13. Výhody hardwarového firewallu aneb co všechno ještě zvládnou vysloužilé počítače

Hardwarové firewally poskytují zabezpečení proti napadení počítače či ochranu místní sítě opravdu na vysoké úrovni. Na rozdíl od softwarových firewallů jsou zřídka ohrožovány útoky z internetu, využívajícími bezpečnostních trhlin v softwaru. Navíc lze jedním zařízením chránit několik počítačů současně, což u velkých sítí značně usnadňuje nároky na jejich konfiguraci. Další výhodou je fakt, že fungují nezávisle na operačním systému nainstalovaném na jednotlivých počítačích v síti.

14. Nevýhody hardwarových firewallů: na co je třeba dávat pozor

Hardwarové firewally na špičkové úrovni jsou poměrně nákladnou záležitostí. Cena typů vhodných pro nasazení v malých sítích začíná sice někde kolem 12 000 Kč, při vyšších nárocích však stoupá strmě vzhůru až k 150 000 Kč a více – to je případ firewallů pro středně velké podniky. Pokud uživatelé chtějí více než surfovat a pracovat s programem pro elektronickou poštou, je správné nastavení hardwarového firewallu poměrně náročné. Navíc stačí jedna chyba při konfiguraci a buď se nelze k internetu připojit vůbec, nebo je síť před útoky z internetu zcela nechráněná.

15. Hardwarový firewall jako samostatný počítač

Jak již bylo zmíněno, jako hardwarový firewall může fungovat prakticky jakýkoliv starší počítač vybavený síťovou kartou. Toto řešení je z ekonomického hlediska velmi zajímavé, neboť kromě starého počítače, který nemusí mít ani pevný disk, potřebujete pouze zdarma dostupný software **Fli4l**, který se pohodlně vejde na disketu. Program **Fli4l** představuje distribuci minilinuxu s funkcí routeru a je vybudován na modulárním principu, což znamená, že jako základní funkci nabízí všem počítačům v síti pouze připojení k internetu a další funkce se dodávají ve formě přídavných modulů – například se jedná o modul firewallu či forwarderu portů, tj. utility, jež umožňuje navenek otevírat požadované porty. A právě takové moduly se dají v případě potřeby do systému začlenit. I způsob připojení k internetu se konfiguruje v příslušných modulech – existují moduly pro připojení přes modem, ISDN či DSL. Vhodný modul jednoduše přidáte k základnímu programu. Podrobnější informace o těchto modulech a seznam podporovaného hardwaru naleznete na internetové adrese **www.fli4l.de/english/e_download.htm**. Podrobný návod pro konfiguraci programu pak najdete na stejném serveru na adrese **www.fli4l.de/english/e_howtos.htm**.

V následujícím popisu se omezíme pouze na zásadní kroky:

1. Pro zprovoznění základní funkce programu potřebujete balíček **fli4l-2.0.8** a podle způsobu připojení buď balíček **isdn**, nebo **dsl**. Ve Windows budete mít pro snazší konfiguraci k dispo-

Pět tipů pro bezpečnější bezdrátovou síť

Připravili jsme pro vás pět tipů, které by měly informovat o tom, jak nastavit bezdrátovou síť tak, aby ji nikdo nepovolaný nemohl zneužít. Ochrana vašeho systému však bude úplná pouze tehdy, pokud budete zachovávat všechna naše doporučení.

1. Změňte výchozí nastavení

Ze všeho nejdříve byste rozhodně měli změnit standardně nastavené přístupové heslo. To totiž není pro nikoho žádným tajemstvím, neboť je uvedeno v příručce k WLAN routeru a ta se dá zdarma stáhnout na internetu.

2. Omezení MAC adres

Přístup k Access Pointu byste měli povolit pouze vašim počítačům. To se dá zařídit omezením přístupu jen na ty síťové karty, které jsou ve vašich počítačích. Do nastavení Access Pointu tedy zadejte MAC adresu síťové karty každého vašeho počítače. Ta je totiž jednoznačným identifikátorem počítače a zjistíte ji nejsnáze pomocí utility **Ipconfig**, která pracuje na příkazovém řádku a dá se spustit, pokud v nabídce *Start/Spustit* zapíšete do políčka *Otevřít* příkaz *CMD*. Otevře se program *Příkazový řádek* a do něj stačí posléze zadat příkaz *ipconfig*.

3. Povolte šifrování

Dalším pravidlem, které zajistí ve vaší bezdrátové síti bezpečnou komunikaci, je povolení šifrování. Sice platí, že při použití standardní metody šifrování *WEP* (*Wired Equivalent Privacy*) postačí šikovnějšímu hackerovi jen asi 20 minut záznamu šifrovaného bezdrátového síťového provozu, aby toto šifrování pomocí freewarového programu prolomil, nicméně šifrování alespoň odradí vaše méně zkušené sousedy od pokusů napadnout vaši síť. Daleko lepší ochranu v tomto směru nabízí nová technologie *WPA* (*Wi-Fi Protected Access*). Pokud váš Access Point a vaše počítače uvedený protokol podporují, pak byste rozhodně měli zvolit tento způsob šifrování.

4. Správné umístění Access Pointu

Nedávejte Access Point na okno, nýbrž někam doprostřed domu či místnosti. Za prvé tím zabráníte možnosti, aby někdo na ulici rozpoznal váš Access Point, jednak zvětšíte jeho dosah ve vašem domě či bytu. Nesprávné umístění Access Pointu bezpochyby činí vaši síť náchylnější k útoku hackerů. Nehledě na to, že hackerovi stačí přijet a zaparkovat před vaším domem, spustit notebook, dát si kávu a pak může ve vaší síti bez obav řádit podle libosti.

5. Zadávejte nesmyslné názvy

Do Access Pointu se mimo jiné zadává i tzv. *SSID* (*Server Set Identifier*), tedy jakýsi popis, jímž bude vaše síť charakterizována. Rozhodně byste se měli vyhnout možnosti vysílání SSID přes Access Point. Vzhledem k tomu, že klienti připojení k síti stejně toto SSID posílají společně s ostatními daty, může být přesto zkušenějšími hackery odhaleno. Proto naše rada zní – používejte pro charakteristiku vaší WLAN nějaké nesmyslné jméno. Jedině tak nebude mít hacker možnost dozvědět se, s kým má tu čest. Pokud jako SSID zadáte výraz typu Domácí síť, předvídá hacker snadnou kořist, neboť tento výraz v něm vyvolá představu špatně zabezpečené soukromé sítě. Zadáte-li nějaký atraktivní název, pak už jen ten samotný může v hackerovi vyvolat touhu síť prolomit.

zici program **Fliwiz NG**. Nejsou potřeba žádné znalosti Linuxu. Ostatně celý program s balíčky **dsl** a **isdn** včetně konfiguračního programu FLIWIZNG.EXE naleznete NA NAŠEM CD jako soubor FLI4L.ZIP o velikosti 6,75 MB, nebo na internetové adrese **www.fli4l.de/english/e_download.htm**, kde si můžete stáhnout balíčky další.

2. Pomocí libovolného dekomprimačního programu rozbalte všechny archivy TAR.GZ včetně podsložek do složky **fli4l-2.0.8**. Nezapomeňte například při použití Winzipu deaktivovat volbu *TAR file smart CR/LF conversion*.

3. Spusťte poklepáním soubor FLIWIZNG.EXE. Na uvítací obrazovce klepněte na tlačítko *Öffnen*. Tím se nahraje výchozí konfigurační soubor. Poté stiskněte tlačítko *Hosts*. Nyní zadejte počet počítačů v síti a rozsah IP adres. Nezapomeňte k celkovému počtu počítačů připočítat i router.

4. Nejjednodušší je konfigurace pro připojení přes DSL. Tady stačí zadat pouze uživatelské jméno a heslo.

5. Pro připojení přes ISDN je zadáno připojení přes MSN, které je pro nás nezajímavé. Proto zvolíme poněkud komplikovanější cestu, protože se budeme připojovat přes svého poskytovatele. Klepněte proto na tlačítko *Circuit*. Tam nastavené hodnoty změníte tím, že v poli *Circuit Variablen* označíte hodnotu a pak pod položkou *Wert* zadáte její novou hodnotu. Začněte parametrem ISDN_CIRC_1_NAME a jako hodnotu mu přiřaďte název vašeho poskytovatele. Do parametru ISDN_CIRC_1_NAME zadejte uživatelské jméno a do ISDN_CIRC_1_PASS heslo. Do parametru ISDN_CIRC_1_DIALOUT vepište číslo, které se má vytočit. Další parametry raději neměňte.

Tím je konfigurace routeru na disketě hotová. Nyní můžete disketu vložit do onoho starého počítače a zkusit z diskety nabootovat. Ostatní počítače musíte ještě nakonfigurovat tak, aby se jejich IP adresy nacházely ve stejné oblasti jako router. Jako bránu zadejte na každém počítači IP adresu routeru. Od této chvíle je z internetu přímo dostupný pouze router, ostatní počítače s Windows včetně všech portů a služeb jsou skryty.

16. Kombinovaná zařízení: hardwarový firewall, DSL modem, router a WLAN

Pro nenáročného uživatele pracujícího na jednom počítači nebo v malé počítačové síti představují zajímavé řešení kombinovaná zařízení obsahující hardwarový firewall společně s DSL modemem, routerem a případně s WLAN. Proto se budou naše tipy pro používání a nákup hardwarových firewallů se budou věnovat právě takovým zařízením.

Obsluha: I zkušení uživatelé vstoupí při konfiguraci firewallu na dosud neprozkoumané pole. Čeká na ně totiž celá řada výzev – vždyť ne každý tuší, co se skrývá za zkratkami NAT, SSID, DHCP či SPI. Dobrý průvodce konfigurací a podrobná příručka jsou v tomto případě k nezaplacení. Proto určitě doporučujeme před koupí zařízení vyhledat na internetových stránkách výrobce odpovídající manuál. Jedině tak si budete moci být jisti, že návod k použití je pro vás skutečně srozumitelný.

Funkce: V kombinovaných zařízeních je většinou integrovaný i router. S jeho pomocí se dá propojit několik počítačů do počítačové sítě a tyto počítače připojit k internetu. Router je vybaven funkcí *Network Address Translation* (*NAT*). Už samotná existence této služby účinně chrání před masivními útoky z internetu. Její princip je následující: IP adresu, která se vám přiděluje při připojení k internetu u vašeho poskytovatele, obdrží router, nikoliv váš počítač. Router přidělí interní IP adresy připojeným počítačům a požadavky z internetu pak rozděluje těm počítačům, které si je vyžádaly. Pokud se někdo pokusí o útok na takto chráněný počítač nebo síť, bude se jednat o pakety dat, které nebyly nikým vyžádány – router tedy pro ně nenajde žádného příjemce a tyto pakety zahodí. Pokud se například červ Sasser dostane na IP adresu routeru, pokusí se využít bezpečnostní trhliny týkající se přístupu přes port 445. Vzhledem k tomu, že na routeru neběží Windows, je i v tomto případě útok odražen. Navíc router, popřípadě firewall rozpozná, že se jedná o nelegitimní požadavek a odmítne jej.

NAT bohužel nechrání před útoky typu *Denial of Service* (*DoS*), při nichž útočník hromadným

◀ Fliwiz NG: tato konfigurační utilita vám umožní pohodlné nastavení hardwarového routeru, provozovaného na počítači prostřednictvím programu Fli4l.

zasíláním legitimních dat přinutí router k tomu, aby postupně vždy čekal na následující pakety. Tím se router tak zahltí, že brzy už neprojde nic. Pakliže chcete být chráněni i před útoky tohoto druhu, mělo by mít vaše zařízení firewall s funkcí *Stateful Packet Inspection* (*SPI*). Ta nejen zkoumá, zda mají pakety legitimního odesílatele a příjemce, nýbrž testuje i to, jak často určité pakety přicházejí. Jakmile jejich počet překročí nastavenou kritickou hodnotu, přestane router další pakety přijímat.

Další funkcí, kterou by měl firewall v kombinovaném zařízení ovládat, je možnost uvolňovat libovolné porty. Tato možnost se většinou nachází mezi pokročilými funkcemi. Na tomto místě pak můžete stanovit, že v souvislosti s končící komunikací na určitém portu se otevře jeden nebo více vstupních portů, které daná aplikace potřebuje současně využívat.

Tato funkce je dobře využitelná kupříkladu při videotelefonii. Kontrolní data jsou zde vysílána přes port 5060, vlastní obsah je ale očekáván na portech 16384 a 16403. Vzhledem k tomu, že na těchto portech doposud žádná komunikace neprobíhala, router by všechna data na těchto portech automaticky zahazoval. Prostřednictvím úprav v „pokročilých nastaveních" zajistíte, že i takové aplikace budou bez problémů fungovat.

Podrobnosti: Vedle těchto základních funkcí je pro uživatele se dvěma či více počítači zajímavá i přítomnost USB zásuvky na kombinovaném zařízení. Ta se dá využít například pro připojení USB tiskárny nebo externího pevného disku, na nějž pak mohou přistupovat všechny počítače v síti.

WLAN: Mnohá z nabízených kombinovaných zařízení nabízejí možnost bezdrátového připojení (*Wireless LAN*). V tomto případě si všímejte toho, aby poskytovala novější a lepší šifrovací technologii *WPA* (*Wi-Fi Protected Access*). Podrobnosti naleznete v rámečku **Pět tipů pro bezpečnější bezdrátovou síť**.

17. Kontrola: kombinace hardwarového a softwarového firewallu

Ten, kdo využívá hardwarový firewall, nic nezkazí, pokud na počítač nainstaluje i softwarový firewall. Hardwarovým řešením získáte velmi dobrou ochranu před útoky z internetu, softwarový firewall vás zase bude informovat o všech aplikacích, které se chtějí připojit k internetu. Takže budete chráněni a zároveň informováni. Důrazně kombinaci hardwarového a softwarového firewallu doporučujeme při používání WLAN, neboť bezdrátová síť je velmi snadno napadnutelná. 5 0315/OK ❑