Zabarikádujte se!

NAJDETE NA NAŠEM CD

MARTIN IGNJATEVIČ

FIREWALLY BEZ TAJEMSTVÍ

V tomto článku se zaměříme na téma, které je poměrně zajímavé – tentokrát bude řeč o firewallech. Někteří z vás jistě tuší, co tento termín znamená, mnozí máte zcela jistě jasnou představu, co firewall je a k čemu slouží, a někteří z vás slyší možná tento výraz poprvé. Podíváme se tedy na téma firewallů podrobněji. Vysvětlíme si, co to vlastně firewall je, k čemu slouží, kdy je vhodné jej používat, jak jej používat a ukážeme si některé produkty, které lze prakticky využít.

Označení firewall pochází ze stavebnictví. Jde o protipožární přepážku, která je odolná proti ohni. Můžete se s ní setkat například u automobilů, kde chrání prostor mezi řidičem a motorem, nebo v budovách, kde má za úkol bránit rozšíření požáru do okolních místností. A takový je v podstatě i princip firewallů v souvislosti s výpočetní technikou. Jde o jakousi přepážku či zábranu, jejímž úkolem je chránit. Chránit lze mnoho věcí, ať již jde o samostatný počítač, připojený modemem nebo o velkou podnikovou síť. Podle toho, co chceme chránit, musíme vybrat i typ firewallu a určit přesnou strategii a taktiku. Naplánování strategie a taktiky je jednou z nejdůležitějších činností při stavbě firewallu. Pravděpodobně zabere i nejvíce práce a času.

Pokud plánujete používat firewall, musíte si položit několik základních otázek. První a nejdůležitější otázkou je, co vlastně chcete chránit. Pokud chcete nainstalovat firewall na svém domácím počítači, který je připojen k síti modemem, budete postupovat zcela jinak než v případě, kdy budete chtít ochránit firewallem svou podnikovou síť. Druhá zásadní otázka se týká výběru operačního systému. Asi by nebylo příliš vhodné používat jako firewall pro podnikovou síť počítač s operačním systémem Windows 98 s nainstalovaným Zone Alarmem (o tomto produktu za chvíli), a na druhou stranu nemá cenu přecházet na operační systém FreeBSD na své pracovní stanici jen z důvodu(!) její ochrany firewallem. Nyní se tedy zaměřme na případ, kdy chcete firewallem ochránit menší podnikovou nebo domácí síť. Poté se podíváme na situaci, kdy budete chtít ochránit svůj počítač. Tématem, jak zabezpečit velkou síť, se zabývat nebudeme, protože je to činnost velmi náročná a většina běžných uživatelů se k ní nedostane. Pro případ, že uvažujete o zabezpečení větší sítě, doporučuji prostudovat odbornou literaturu a vše konzultovat s odborníky.

ZABEZPEČUJEME SÍŤ

Rozhodli jste se tedy zabezpečit svou menší podnikovou nebo domácí síť. První co musíte zvážit je, jaký máte hardware a kolik chcete do firewallu investovat. Pokud provozujete nějaký veřejnosti určený server, například poštovní nebo webový, musíte zvážit, zda umístíte tyto servery na počítač, který bude zároveň sloužit jako firewall, nebo je dáte na samostatný stroj a firewall umístíte „před“, případně ještě „za“ tyto servery. Toto druhé řešení je bezpečnější z několika důvodů, ale zároveň i finančně nákladnější. Prvé řešení, tedy pokud se rozhodnete umístit nějaké servery společně na firewall, je finančně méně nákladné, ale nese i svá rizika. Tato rizika lze však vhodnou strategií výrazně eliminovat. Výběr záleží čistě na vás, ale musíte vzít v potaz, že pokud se rozhodnete umístit nějaké služby na firewall, budete muset posílit hardware, na kterém to vše poběží. Samotný systém s firewallem nebude mít takové nároky jako systém s ještě nainstalovaným poštovním či webovým serverem. V žádném případě se neodporučuje umisťovat na tento systém data či aplikace, které slouží uživatelům vnitřní sítě, a které nemají být přístupné veřejnosti.

Nyní před vámi stojí otázka volby operačního systému. Pokud máte dostatek finančních prostředků a nadprůměrně silný hardware, můžete uvažovat o produktech vytvořených pro operační systémy firmy Microsoft. Pokud se vám nechce investovat desítky tisíc jak do softwaru, tak do hardwaru, můžete s klidem uvažovat o unixovém systému. Unixové systémy mají několik výhod. Nejvýraznější je jejich cena. Například operační systémy Linux, FreeBSD či OpenBSD lze pořídit zcela zdarma a jejich výkon si v ničem nezadá s výkonem komerčních produktů, a v mnohém je dokonce výrazně předčí. Nezanedbatelnou stránkou věci jsou i nároky na hardware, které nejsou tak vysoké jako u grafických operačních systémů (samozřejmě záleží na instalaci a konfiguraci).

TYPY FIREWALLŮ

Chceme-li se bavit o firewallech, musíme si říci, jaké vlastně typy firewallů máme. Základní dělení podle toho, jak firewall pracuje, je dělení na paketové filtry a aplikační servery. Typickým příkladem paketového filtru je firewall zabudovaný do jádra většiny unixových systémů. Většina operačních systémů Windows, s výjimkou Windows XP a 2000, nemá tento druh firewallu implementován. A i tato implementace zdaleka nedosahuje kvalit unixových filtrů. Představitelem aplikačních serverů je například unixový proxy server Squid nebo WinProxy pro operační systémy Windows. Základní odlišnost obou typů je v tom, jak pracují. Zatímco paketový filtr jednoduše blokuje, zakazuje nebo směruje pakety podle daných pravidel bez analýzy obsahu, aplikační server se snaží obsah analyzovat a podle výsledků analýzy i rozhodovat. Může tedy například analyzovat obsah přenášených webových stránek a blokovat Javascripty. Není výjimkou, že síť chrání oba druhy těchto firewallů. Mělo by ale platit, že směrem do vnitřní sítě by měl být paketový filtr na prvním místě a až za ním by měl být umístěný aplikační server, a to z několika důvodů. Jedním z nich je snížení zátěže aplikačního serveru, jenž zpracovává jen data, která chceme, aby byla zpracovávána. Nemusí se tak zabývat pakety, které nechceme vůbec pustit do naší sítě. Toto obstarává paketový filtr umístěný před aplikačním serverem.

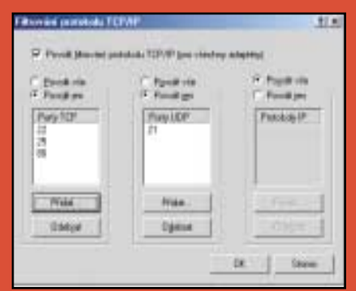
POLITIKA FIREWALLU

Ať již se rozhodnete pro jakýkoliv typ firewallu s jakoukoliv topologií, musíte zvolit vhodnou politiku pro firewall. Máte dvě možnosti. Za prvé jde o takzvaný implicitní zákaz. Princip této politiky spočívá v zakázání všech služeb a protokolů a povolení pouze těch, které chceme. Druhým typem politiky je implicitní povolení. Princip, jak již jistě tušíte, spočívá v zakázání jen definovaných služeb a protokolů a povolení všech ostatních. Každá z těchto politik má svá plus i svá mínus. Povolovací politika je jednodušší na správu a konfiguraci, na druhou stranu nechává útočníkovi více příležitostí k útoku. Druhá metoda je o něco bezpečnější, protože máte výhodu v tom, že víte, kde můžete útočníka čekat. Pozor ale na různá opomenutí, a to u obou druhů politik. Jakmile přehlédnete nějakou službu nebo protokol, které byste měl zabezpečit, a neprovedete to, je vám celá bezpečnostní politika k ničemu.

STRATEGIE

Jak již jsme v úvodu řekli, je naplánování vhodné strategie jednou z nejdůležitějších činností při stavbě firewallu. Při jejím plánování musíme myslet a brát ohled na spoustu různých věcí. Je dobré si síť nakreslit, vypsat všechny služby, které provozujeme, a pečlivě zvážit, jak budeme chtít síť chránit. Je třeba si uvědomit, že funkce firewallu nespočívá v pouhém zabránění pravidel pro jednotlivé protokoly a porty opravdu snadné.

Nevýhodou je, že nemůžete definovat pravidla „za letu“, ale až v době, kdy zjistíte, že vám něco nefunguje. Rovněž nemůžete pravidla definovat pro jednotlivé aplikace, ale jen pro protokoly, a to pouze TCP a UDP. V tomto má ohromnou výhodu jiný produkt, a sice Kerio Personal Firewall.



Firewall jako součást systémů Windows 2000 a XP

Jedná se o jednoduchý paketový filtr, který se výkonem a robustností nemůže měřit s unixovými systémy, ale běžným uživatelům na jejich pracovních stanicích může poskytnout dostatečný komfort při zabezpečování jejich počítače, a to zejména těm, kteří nechtějí stále „něco instalovat, když je to součástí Windows“.

Pokud chcete definovat nějaká vlastní pravidla, otevřete si *Ovládací panely – Síťová a telefonická připojení* a zvolte připojení, přes které se připojujete, například tedy *Připojení k místní síti* či *Telefonické připojení*. Zvolte *Vlastnosti* a vyberte protokol *TCP/IP* a opět klikněte na *Vlastnosti*. V následujícím okně zvolte položku *Upřesnit* a přejděte na záložku *Možnosti*. Zde *zvolte Filtrování protokolu TCP/IP* a opět klikněte na *Vlastnosti*.

Nyní si trochu odpočiňte od neustálého klikání, a poté se můžete pustit do nastavování filtrovacích pravidel. Jak vidíte na obrázku, je defi-

ní přístupu útočníka do sítě. Jeho smysl je mnohem hlubší. Jde například i o ochranu dat, která by mohla být zneužita zevnitř sítě, nebo o rozložení zátěže jednotlivých počítačů. Musíte vzít v potaz také topologii sítě, její technické podmínky jako je rychlost, operační systémy v síti, fyzické umístění počítačů a kabelů a běžnou zátěž sítě. Pokud budete brát ohled na všechny tyto věci, přispějete tím k vytvoření velmi kvalitního a bezproblémového firewallu.

PAKETOVÝ FILTR IMPLEMENTOVANÝ V JÁDŘE OPERAČNÍHO SYSTÉMU LINUX

Nyní se podíváme na to, jak řeší filtrování paketů jádro operačního systému Linux. Linux je dnes už poměrně rozšířeným operačním systémem, který se nachází nejen na spoustě serverů, ale dnes už i na velkém množství pracovních stanic, proto bude jistě zajímavé se na tento systém a jeho řešení daného problému podívat podrobněji. Pokud chceme pochopit smysl a funkce paketového filtru zabudovaného do jádra systému, musíme se na chvíli vrátit do historie a podívat se na to, jak vývoj tohoto filtru probíhal.

OD IPFWADM PŘES IPCHAINS K IPTABLES

Dnes již historická linuxová jádra řady 1.0 v sobě měla implementován BSD firewall ipfw. Tak tomu bylo i u jader 2.0, kde však byla implementace BSD firewallu mnohem propracovanější. Základním nástrojem pro konfiguraci firewallu je nástroj ipfwadm. V jádrech řady 2.2 už byl nasazen nástroj ipchains, vytvořený Paulem Russelem a Michaelem Neulingem. Tento nástroj je už poměrně robustním prostředkem sloužícím k ochraně sítě či počítače a na mnohých systémech se s ním můžeme setkat ještě dnes. Program oproti původním ipfwadm obsahuje velké množství pravidel, která mohou při vhodném použití výrazně zvýšit výkon firewallu. Postupem času však vývojáři dospěli k názoru, že práce firewallu by měla být výrazně zjednodušena, a že současná implementace nepracuje dostatečně efektivně. Zjednodušením by se výrazně zvýšila bezpečnost, ale i výkon systému. Proto byla zahájena práce na implementaci zvané netfilter. Ta se snaží být co nejjednodušším a zároveň robustním řešením filtrovacích pravidel. Implementuje v sobě NAT *(Network Address Resolution)* a IP maškarádu, které dříve nebyly přímou součástí firewallu. Tím se celý mechanismus zjednodušil a zároveň tak stoupl i výkon. Nástroj pro správu implementace netfilter se jmenuje iptables a je součástí jader verze 2.4. Proto se doporučuje přejít na tyto verze jádra. Přechod z předešlých verzí není vůbec obtížný, neboť byla zachována zpětná kompatibilita filtrovacích pravidel. Existují dokonce nástroje, které filtrovací pravidla určená pro ipchains konvertují do formátu pro iptables. Nyní již k tomu, co linuxový firewall dokáže.

S linuxovým firewallem dokážeme při správném použití skutečné divy. Umožňuje nejen například IP maškarádu, která nám poslouží v případě, kdy je naší síti přidělena jen jedna veřejná IP adresa, ale umožňuje nám bezpečně kontrolovat veškerá příchozí a odchozí data. Je důležité firewall správně nastavit. Ke konfiguraci můžete použít příkazový řádek, ale pokud nejste zrovna jeho fandou, existují desítky grafických a automatických nástrojů, které vám konfiguraci firewallu maximálně usnadní. Pomocí tohoto firewallu můžete přesně definovat, jak bude s kterými pakety zacházeno. Zda-li budou přijmuty, odmítnuty, přeposlány nebo zahozeny. Rovněž můžete velmi podrobně definovat IP adresy, případně jejich třídy, zdrojové a cílové porty, protokoly atd. Možností je k dispozici opravdu hodně. Záleží jen na vás, jaký si konfigurační nástroj vyberete a jak se s ním naučíte zacházet, i když je třeba znovu podotknout, že mnohem důležitější je naplánování vhodné strategie než aplikace samotných pravidel. O všech spojeních lze navíc vést podrobné záznamy. Tuto možnost oceníte nejen v ostrém provozu jako výborný analyzátor toho, co se na vaší síti děje, ale i jako skvělou možnost testování firewallu při jeho stavbě. Nejste-li si jistí, které služby, protokoly a porty vaši uživatelé potřebují (což by se vám ale stát nemělo), zakažte veškerý provoz z a do vaší sítě a všechny pokusy o připojení zaznamenávejte. Poté můžete celkem přesně stanovit, co je potřeba a co naopak nikoliv.

Zone alarm

Zone alarm je dalším osobním firewallem určeným pro pracovní stanice. Jeho možnosti jsou širší než možnosti firewallu, jenž je dodáván spolu s operačními systémy Windows 2000 a XP, ale nedosahuje kvalit Kerio Personal Firewallu. Uvádíme zde obrázek, který by měl přiblížit, jak tento firewall pracuje.

WINDOWS A FIREWALLY

Pokud nechcete z nejrůznějších důvodů používat unixové systémy, například máte-li spoustu zbytečných finančních prostředků, můžete použít operační systémy firmy Microsoft. O operačních systémech řady 9x nemá asi ani cenu v souvislosti s ochranou sítě uvažovat. Zbývají nám tedy operační systémy Windows 2000 a XP. Oba tyto produkty existují i ve své serverové verzi, ale ta oproti standardní verzi pro pracovní stanice nepřináší v souvislosti s firewally nic nového. Osobně nedoporučuji používat vestavěný firewall z těchto systémů, neboť zdaleka nedosahuje výkonu a možností například linuxového netfilteru. Navíc při velkém vytížení mají tyto systémy problémy s výkonem. Doporučuji tedy sáhnout po produktech třetích stran. Těch existují stovky, možná tisíce a je jen na vás najít si ten, který vám bude vyhovovat. Já osobně bych volil unixovou variantu, kdy je řešení „all in one“, navíc zdarma. To se týká jak paketových filtrů, tak aplikačních serverů. Těch je zdarma k dispozici také velké množství. Zkuste někdy zabloudit na stránky *sourceforge.net* a zadejte hledat výraz proxy. Jistě budete příjemně překvapeni.

FIREWALL NA DOMÁCÍM POČÍTAČI

Mnoho z vás se jistě připojuje k internetu z domova. Někteří po kabelu, někteří přes mikrovlny, další přes satelit a většina zřejmě přes modem. Ptáte se, jestli má cenu instalovat na svém počítači firewall? Ano, má. Pamatujte na to, že pro ochranu svých dat nikdy nemůžete udělat dost a stále je co zlepšovat. Většina uživatelů používá systémy Windows. Ti, kteří používají na svém domácím počítači systém Linux či jiný unixový systém, mohou k ochraně použít firewall implementovaný v jádře (viz výše). Pokud jste uživatelem produktů Windows, budete nuceni sáhnout po výrobcích třetích stran, i když firewall obsažený v základní instalaci systémů Windows 2000 a XP se dá při domácím použití celkem vhodně použít.

ZÁVĚREM

Na závěr lze konstatovat, že firewall je mocným pomocníkem při budování bezpečnostní politiky a účinným nástrojem k ochraně sítě či počítače. Použití firewallu však vyžaduje porozumění síťové komunikaci a bezpečnosti dat jako celku. 3 0065/FEL ❑

Kerio Personal Firewall

Podle výsledků mnoha testů a recenzí různých odborných serverů jde o jeden z nejlepších firewallů určených pro pracovní stanice uživatelů. Dobrou zprávou je, že produkt je pro domácí použití k dispozici zdarma. Mnozí z vás si jej jistě pamatují ještě pod starým označením Tiny Personal Firewall. Poslední verze instalačního souboru, zhruba o velikosti 2 MB, je ke stažení na stránkách firmy Kerio *(www.kerio.com)*. Tato firma se zabývá vývojem síťových aplikací a v komerční sféře jsou její produkty velmi úspěšné. Prohlédnutí stránek o jejích produktech jistě stojí při troše volného času za to. S Kerio Personal Firewallem se můžete pravidelně setkávat též na PC WORLD CD-ROMu. Jelikož je tento produkt tolik oblíbený a úspěšný, podíváme se na něj podrobněji a popíšeme si některé jeho funkce. Po přečtení následujících několika řádků by měl být každý z vás schopen nainstalovat vlastní firewall a definovat si na něm příslušná pravidla. Začneme tedy instalací. Instalace je standardní a nepůsobí žádné vážné problémy. Po jejím dokončení bude třeba systém restartovat, aby došlo k natažení a spuštění potřebných modulů. Ve vašem trayi se poté objeví nová ikona ve tvaru štítu. Pokud na ikonu dvakrát poklepete, otevře se vám okno, kde je zobrazen stav všech připojení. Pokud si přejete program nastavit, což je po instalaci celkem pravděpodobné, otevřete si administrační část firewallu a to buď klasicky přes nabídku *Start*, nebo klikněte pravým tlačítkem na ikonu v trayi a zvolte *Administration*. Měli byste vidět okno podobné tomu na obrázku.

První záložku zatím necháme být a povíme se něco o těch dalších. Na záložce *Authentication* lze nastavit přístupové heslo k administrační nebo statistické částí firewallu. To je užitečné zejména v případě víceuživatelského počítače, kdy si správce toho počítače přeje zablokovat určité adresy. Na kartě *Miscellaneous* si můžete zvolit další vlastnosti, jako je například rozlišování DNS *jmen (DNS name resolving)*, automatická aktualizace programu nebo automatické spouštění po startu Windows. Nyní se ale vraťme k první kartě, ze které se nastavuje to nejdůležitější, a sice pravidla firewallu. Na této kartě si můžete pomocí posuvníku zvolit výchozí úroveň zabezpečení. Na výběr máte ze tří možností. Úroveň Permit Unknown znamená, že pokud firewall narazí na nějaký požadavek na spojení, který není definován v pravidlech, implicitně jej povolí. Toto není příliš šťastné řešení, pokud předem nevíte, co budete chtít omezit. Druhá úroveň Ask Me First je výchozí a zároveň také nespolehlivější. Při tomto nastavení se vás firewall pokaždé zeptá, pokud narazí na neznámý požadavek na připojení. O tomto dotazu si povíme za okamžik. Třetí, nejvíce bezpečnou úrovní je Deny Unknown. Při aktivované této úrovni zabezpečení počítač odmítá jakékoliv požadavky na spojení, které nezná. Na tuto úroveň byste si měli rovněž dát pozor, neboť vám po její aktivaci nemusí spousta věcí fungovat. Dejme tedy tomu, že jsme zvolili úroveň Ask Me First. Uložíme tedy tuto úroveň a pokusíme se otevřít nějakou síťovou aplikaci, například Outlook Express. Pokud jste již v tu chvíli připojeni k síti, zobrazí se vám okno s informační hláškou, která oznamuje, že aplikace Outlook Express se snaží odeslat nějaká data. Na vás je rozhodnout se, zda to povolíte, nebo ne. Pokud nepatříte k zarytým odpůrcům tohoto e-mailového klienta, kliknete pravděpodobně na tlačítko *Permit* (Povolit), a ne na *Deny* (Zakázat). Můžete si ale vybrat i další možnosti a svou volbu blíže specifikovat.

Pokud zatrhnete tlačítko *Create appropriate filter rule...*, nebude se vás už firewall v budoucnu ptát, zda chcete povolit této aplikaci přístup. Můžete rovněž kliknout na tlačítko *Customize rule* a pravidla dále specifikovat.

Jak vidíte na obrázku můžete například specifikovat lokální port, vzdálenou adresu nebo vzdálený port. Pokud tedy například chcete povolit uživatelům prohlížení jen vlastní firemní stránky, nastavte u pravidel Internet Exploreru jen adresu vašeho serveru.

SPECIFIKACE DALŠÍCH PRAVIDEL

Než nastavíte všechna pravidla, která si přejete, bude vám to jistě chvíli trvat a ze začátku vám to možná nebude připadat jako jednoduché řešení. Věřte ale tomu, že jakmile jednou daná pravidla nastavíte, bude vám firewall dobře sloužit k vaší plné spokojenosti. Musíte ale vzít zároveň v potaz, že jakmile jednou nějakou aplikaci povolíte na firewallu, ztrácíte nad ní kontrolu. Aplikace pak může bez vašeho vědomí odesílat data, která si nepřejete. Proto vždy dobře zvažte, které aplikaci přístup povolujete. Neznámým aplikacím, o nichž si nejste jisti, co chtějí odeslat, přístup raději zakažte.