Počítač jako pevnost

Bezpečnost malé domácí sítě nemá cenu podceňovat

PATRIK MALINA

O tom, že problematika zabezpečení domácích počítačů či malých domácích sítí, jež disponují připojením k internetu, je věcí více než aktuální, jsme v PC WORLDu již psali nejednou. Události posledního půlroku jasně dokládají, že dříve jen libůstka opravdových fandů PC či koníček excentrických specialistů se proměňuje v téměř existenční nutnost: bez ohledu na vaše uživatelské znalosti bezpečnostních či síťových technologií tak nadále rostou nároky na aktivní obranu proti sílícím hrozbám. Stejně jako v každé jiné nelítostné džungli zde platí, že není nezúčastněných či neutrálních stran: buďto budete při využívání i těch nejpomalejších internetových linek nanejvýš obezřetní a učiníte alespoň základní kroky pro svou obranu, nebo budete riskovat, že bloumající internetoví dravci a vetřelci snadno zavětří kořist v podobě vašeho pevného disku a operačního systému.

Předchozí řádky ve vás možná vyvolaly pocit, že nezbytnou nutností je náročná investice či nadprůměrně vysoká znalost potřebných technologií. V následujících odstavcích bychom rádi tyto obavy rozptýlili. V první řadě je potřeba si uvědomit nejdůležitější zásadu: nemusím mít nejlépe zabezpečenou síť či počítač v celém internetu. Ale mé zabezpečení musí být alespoň o stupínek lepší, než u většiny ostatních. Útočník si pak při zevrubném průzkumu vybere snadnější kořist a obětí se stane počítač uživatele, jenž situaci podcenil či ignoroval. Ale to vy přeci nebudete!

V následujících odstavcích totiž naleznete několik typických situací a postupů, jež vám pomohou krok za krokem zabezpečit váš domácí počítač či malou síť, jež nedisponuje speciálními servery či náročnými hardwarovými ochrannými prvky. Ukážeme si, že i s nasazením minimálních investic a přiměřeného úsilí lze značně zvýšit laťku bezpečnosti stávajících operačních systémů, a posunout tak vaše stroje do řad nesnadných potenciálních obětí. Námi popsané scénáře zohledňují různé typy internetových připojení a jim odpovídajících konfigurací a představují jedny z nejběžnějších modelů, jež se v běžných, počítačem vybavených domácnostech či firmičkách vyskytují. Pokud je pro vás síťová a bezpečnostní problematika koníčkem a jste pokročilejšími znalci, berte prosím naše ukázky a návody jako základní a výchozí materiál, na němž lze dále stavět. Důležité je pochopitelně zvládnout principy, jež lze nadále rozvíjet.

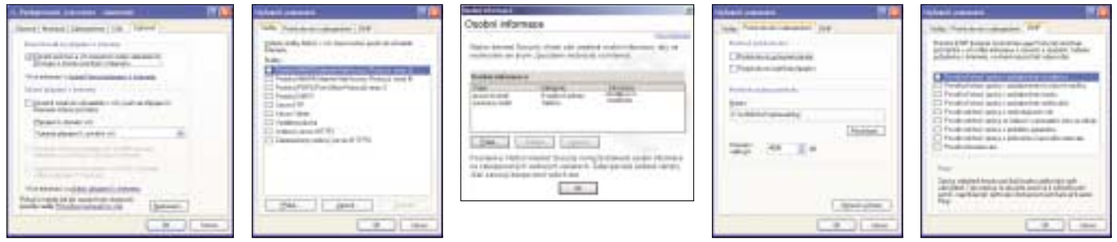
Situace, jež jsou v následujících odstavcích zařazeny a popsány, jsme rozdělili dle způsobu, jímž je využívána internetová přípojka. Naleznete zde model nejjednodušší, kterým je dnes určitě jediný počítač s tradiční vytáčenou linkou a „klasickým" analogovým modemem, složitější situaci s jediným počítačem pro pokročilejší uživatele, a samozřejmě komplikovanější řešení, při nichž dochází ke sdílení internetové linky vícero počítači v malé síti. Při realizaci různých zapojení vřele doporučujeme postupovat dle chápání předkládané látky – nejste-li si u komplikovanější síťové architektury zcela jisti, co vlastně spouštíte, raději se poraďte se zkušenějším uživatelem či si alespoň přečtěte článek znovu, neboť jak jsme již uvedli, potenciální útočníci se falešným sentimentem a shovívavostí v žádném případě nezdržují.

Na závěr úvodního pojednání bychom rádi zařadili jedno důležité upozornění. Námi poskytnuté návody nemohou, podobně jako žádné jinde uveřejněné postupy či rady, zaručit stoprocentní bezpečnost vašeho počítače a sítě! Nespoléhejte jen na popsané konfigurace, neboť nic není absolutní, což v oblasti počítačové bezpečnosti platí trojnásob! Snažte se i nadále vstřebávat informace a novinky, a především pečlivě sledujte, jak se váš operační systém chová. V případě nejistoty nelitujte námahy a čas od času si sežeňte znalého uživatele, jenž vám poradí či konfiguraci třeba zkontroluje. A je-li vaší filozofií to, že domácí počítač je pracovní nástroj a bezpečnost vás nezajímá, odborník by k vám měl jistě najít cestu.

Scénář č. 1

Struktura zapojení: jediný počítač připojený k internetu
Typ internetové linky: vytáčená (dial-up) linka
Vybavení: jen OS Windows XP
Cenové nároky: jen licence na OS
Nároky na znalosti uživatele: nízké

Ne náhodou stojí na prvním místě tento v podstatě nejjednodušší postup a návod, jak zabezpečit internetové připojení. Jednou z největších výhod je, že budeme při konfiguraci využívat pouze komponentu operačního systému, a nebude potřeba instalovat žádný dodatečný software či hardware.



Ihned na počátku je potřeba zdůraznit některá zásadní fakta. To, že se jedná o konfiguračně poměrně nenáročnou záležitost, neznamená, že by šlo o řešení primitivní, neřku-li nefunkční. Komponenta, o níž bude řeč, je poměrně zdařilá a velmi dobře dokáže odvést svou práci. A vzápětí dodáváme veledůležité upozornění: tato metoda ochrany je minimálním nezbytným postupem, jejž nejen můžete, ale nejlépe musíte nastavit pro to, aby váš počítač byl chráněn! Opět se nenechte zmást faktem, že jde „pouze" o součást Windows XP. Rozdíl mezi nechráněným počítačem a strojem, jehož zabezpečení si vzápětí ukážeme, je propastný!

Klíčovou funkcionalitu, o níž bude řeč, zajišťuje komponenta Internet Connection Firewall *(ICF, Brána Firewall pro připojení k internetu)*, jež chrání síťová připojení. Je důležité si uvědomit, že tato vymoženost je dostupná pouze uživatelům Windows XP (a případně Windows 2003 Serveru, jehož použití ovšem doma nepředpokládáme), a pokud pracujete se starší variantou Windows, budete nuceni zvolit některé z následujících řešení. ICF je k dispozici jednotlivě pro každé síťové rozhraní, jež operační systém používá, a to jak v případě nainstalovaných síťových karet (což doma nemusí být typické), tak především v případě telefonických připojení k internetu. Umístění této funkce přímo na jednotlivých síťových rozhraních má pochopitelně svou logiku: zabezpečení tak „sedí" přímo u „vstupních dveří" do vašeho počítače a provoz je striktně kontrolován co nejdříve.

V souvislosti s dříve popsanou koncepcí naleznete konfiguraci ICF ve složce či pod *Ovládacím panelem Síťová připojení*. Zde je potřeba vybrat odpovídající síťové rozhraní, jež chceme chránit – tedy v našem případě telefonické připojení k internetu – a přejít pomocí stisku pravého tlačítka myši na volbu *Vlastnosti*. Potřebné ovládání najdete na kartě *Upřesnit*.

Pomocí jediného zaškrtávacího pole v horní části karty dosáhnete zapnutí ICF. Je důležité si uvědomit dopad tohoto kroku na funkcionalitu systému a síťové komunikace: veškerý tok dat bude od této chvíle pomocí vestavěného firewallu důsledně kontrolován. Požadavky aplikací, jež budou zasílány z vašeho počítače přes síťové rozhraní směrem „ven", tedy třeba do internetu, budou propouštěny, a co je velmi důležité, systém si také počká na případné odpovědi a propustí je dovnitř. Tento postup (říkáme, že firewall je stavový) je naprosto nezbytný, neboť typická internetová komunikace probíhá právě způsobem požadavek-příslušná odpověď, na což bere ICF ohled, takže se nemusíte bát, že užitečný a vámi požadovaný provoz by ustal. Na druhou stranu, veškeré požadavky, jež budou vzneseny ze strany internetu směrem na váš počítač, budou v dosud popsané konfiguraci zahozeny a váš stroj bude zvenčí nedostupný. Pokud jste běžnými uživateli základních internetových služeb (WWW, elektronická pošta), je pro vás toto nastavení dostačující.

Mohou však nastat situace, kdy popsaný postup „vše ven, nic dovnitř" nebude vyhovovat. Jednou z typických možností je využití funkce *Vzdálená plocha*, kdy budete chtít odněkud ze sítě vzdáleně ovládat svůj počítač. Protože spojení je iniciováno zvenčí, ICF vše zablokuje, a proto je potřeba nastavení zjemnit. Poslouží nám tlačítko *Nastavení* na dolním okraji karty *Upřesnit*, a následně karta *Služby* v otevřeném dialogovém okně.

Naleznete zde seznam nejtypičtějších služeb, jež můžete opět jediným zaškrtnutím zpřístupnit pro uživatele přistupující z internetu na váš počítač. Krom již zmíněné *Vzdálené plochy* jsou zde např. volby pro webový server či poštovní server. Protože zde uvedený skromný seznam zdaleka nezahrnuje všechny běžně používané protokoly, je někdy potřeba využít tlačítko *Přidat* a protokol pro danou službu ručně specifikovat. Tento postup je žádoucí např. u některých chatovacích aplikací (ICQ apod.), ale typicky též u nástrojů na sdílení digitálního obsahu, jako je třeba Direct Connect. Zde je namístě upozornit, že takového otevření „vstupních dveří" může mít vážné následky, a proto buďte opatrní.

V otevřeném dialogu nám ICF nabízí ještě dvě karty pro upřesnění nastavení. Protokolování zabezpečení slouží k nastavení, zdali se provoz firewallu bude podrobně zaznamenávat do seznamu událostí (logu), a karta ICMP umožňuje povolit zasílání zpráv tohoto pomocného diagnostického protokolu.

Pokud netušíte, co ICMP je, nic nepovolujte – jen pro vaši informaci, slouží např. k zasílání zpráv pomocí příkazu PING, a v případě chybného nastavení umožňuje realizovat útoky, jež váš operační systém mohou přinejmenším shodit a restartovat.

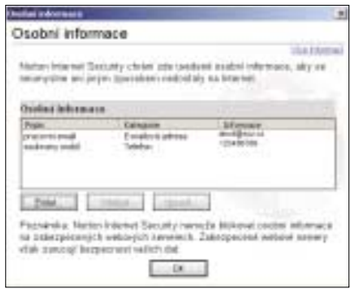
Několika málo výše uvedenými kroky jsme udělali nezbytné minimum pro naši síťovou bezpečnost, jež představuje slušný kompromis mezi náročností na obsluhu a mírou zabezpečení. Pochopitelně buďte obezřetní, neboť ICF neřeší zdaleka vše, jak se dozvíte dále.

Tip na závěr scénáře: pozorně sledujte vývoj změn operačního systému Windows XP. Společnost Microsoft připravuje v rámci chystaného aktualizačního balíku Service Pack 2 poměrně zásadní změny a vylepšení, jež funkci Internet Connection Firewallu nadále rozšíří.

Scénář č. 2

Struktura zapojení: jediný počítač připojený k internetu
Typ internetové linky: vytáčená (dial-up) linka, ADSL či kabelový rozvod
Vybavení: OS Windows a personální firewall
Cenové nároky: od 0 Kč po cca 3 000 Kč
Nároky na znalosti uživatele: nízké až střední

Ačkoliv výše popsaný postup s využitím ICF nabízí základní míru zabezpečení, jeho možnosti mohou být brzy vyčerpány. Typickým případem je situace, kdy nedisponujete operačním systémem



Typická konfigurace osobního firewallu

Použitý software:
Kerio Personal Firewall 4.0.10
Využití: všestranný, univerzální osobní firewall
Náklady: základní verze zdarma, plná verze cca 1 300 Kč

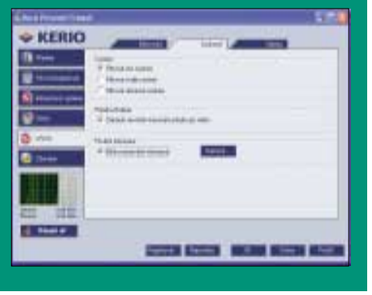
Nastavení osobního firewallu, jež v tomto článku podrobněji zmíníme, je aktivně využíváno pro běžné pracovní i testovací účely. Jsou v něm zahrnuta typická nastavení, jež zajistí normální použitelnost internetu při domácí práci. Nezapomeňte, že internetová přípojka je vždy označena jako nedůvěryhodná zóna! Přehled nezahrnuje všechny parametry, snažili jsme se spíše upozornit na funkčně nejdůležitější prvky.

Dialog: Síťová bezpečnost – Předdefinované

Zde jsme ponechali nastavení blízké výchozí podobě. Mezi nejdůležitější patří *povolení Domain Name System* (DNS), což zajišťuje překlad jmen počítačů v internetu, dále *Ping out* (diagnostika vzdálených počítačů) a *Dynamic Host Configuration Protocol* (DHCP) pro získání IP adresy, např. od vašeho ADSL modemu či přímo internetového poskytovatele.

Dialog: Síťová bezpečnost – Aplikace

V této části jsme zajistili průchod bez zbytečného dotazování především pro aplikace MS Internet Explorer *(Odchozí povolit)*, dále pro Outlook Express *(Odchozí povolit)*, ICQ *(Odchozí povolit)* či pro klienta pro updatování antivirové aplikace *(Odchozí povolit pro Symantec)*. Z dalších aplikací se hodí propustit FTP klienta (třeba *Total Commander*) a obzvláště opatrní musíte být na službu Sdílení souborů a tiskáren v sítích Microsoftu *(Microsoft File and Print Sharing)*, u níž směrem do nedůvěryhodné sítě vyžadujte vždy alespoň dotazování. Z dalších aplikací je dobré povolit provoz např. Windows Media Playeru či obdobným nástrojům pro sledování internetových rádií či videopřenosů.



Dialog: Útoky – Obecné

V tomto dialogu doporučujeme zakázat alespoň útoky s vysokou a střední prioritou. Pokud hodláte po útoku blíže zkoumat jeho průběh, zapněte si volbu *Zaznamenat*.

Dialog: WWW – Soukromí

Na tomto místě rozhodně věnujte pozornost spodní volbě *Blokovat privátní informace*. Pomocí tlačítka *Nastavit* vstoupíte do dialogu, kde postupně naplníte seznam položkami s vašimi privátními daty, o jejichž vyzrazení nestojíte. Ačkoliv to vyžaduje jistou námahu, nepodceňujte tento krok a dejte si projednou tu práci tuto funkci uvést v život.

Windows XP, ale jinou, starší verzí. Další vážnou okolností, jež nabádá k využití dodatečných prostředků, je poměrně hrubý postup vestavěného firewallu: povolení přístupu do internetu a prohlížení webových stránek samo o sobě může znamenat velmi vážné riziko, neboť nebezpečí číhá např. při stahování souborů či odesílání dat pomocí různých formulářů a dotazníků.

Chcete-li posílit svou ochranu a zároveň výrazně rozšířit možnosti konfigurace při kontrole síťového provozu v obou směrech, nastal pravý čas pro nasazení některého z řešení, jež bývají často zjednodušeně nazývána jako osobní (personal) firewall. Jedná se o program (či kolekci programů), jenž je instalován běžnou cestou do prostředí Windows a následně nabízí řadu funkcí. Zde je chvíle pro důležité upozornění: budete-li využívat jakýkoliv nástroj tohoto druhu, vypněte před jeho zprovozněním funkci ICF (viz výše), neboť by mohlo docházet k nežádoucím konfliktům.

Velmi dobrým příkladem tohoto typu aplikace je *Norton Internet Security* – na ni narazíte v tomto čísle rovněž v rubrice Software, a to v podobě recenze. Balík je určen speciálně domácím uživatelům a nabízí širokou škálu ochranných mechanismů, často na poměrně luxusní úrovni. Především je důležité pochopit, že takovýto program hlídá komunikaci velmi jemně: můžete nejen říci, že povolíte prohlížení WWW stránek či zasílání e-mailů, ale také jasně říkáte, které aplikace to budou dělat, čímž striktně kontrolujete i odchozí provoz. Krom více než plnohodnotné náhrady funkce ICF jsou zde k nalezení další možnosti, jako třeba *Detekce narušení*, jež dovoluje rychle započít obranu proti pokusům o útok z internetu, a velmi zásadní je dále *Ochrana osobních údajů*, zabraňující nechtěnému odeslání privátních a citlivých informací do sítě (např. PIN kreditních karet, různá hesla, soukromá telefonní čísla apod.). Velmi praktická je v současné době též ochrana proti nevyžádané poště (antispam) či třeba blokování otravných reklamních oken v prohlížečích webových stránek.

Nastavení Norton Internet Security (a dalších podobných aplikací) probíhá v několika fázích. Po instalaci je potřeba aplikaci říci, které nástroje pro přístup do internetu hodláte používat a co jim povolíte, a následně při běžném využívání toto dále zpřesňovat. Pro běžný provoz doporučujeme propustit alespoň prohlížeč (např. MS Internet Explorer či Operu) na portech TCP 80 a 443, dále poštovní program (např. Eudora či Outlook Express) na portech TCP 25, 110 a 143 a samotný operační systém Windows na portu UDP 53 (pro překlad jmen pomocí DNS). V případě dalších funkcí, jako je třeba ochrana osobních údajů, je samozřejmě potřeba provádět další konfiguraci v podobě „nakrmení" aplikace citlivými informacemi, jež chceme chránit – na tento fakt nikdy nezapomínejte, neboť jinak nemůže ochrana plnohodnotně pracovat!

Na základě shodných principů a s velmi obdobným ovládáním pracují i produkty dalších výrobců. Často je spojuje jedna význačná vlastnost: základní funkce, jež jsou srovnatelné s ICF ve Windows XP, jsou nabízeny zdarma (např. u Zone Alarmu či Kerio Personal Firewallu), a rozšířené a dodatečné vymoženosti, jako kontrola soukromí či detekce narušení, jsou zpoplatňovány. Z toho, co jsme popsali, je zřejmé, že aplikace typu osobní firewall je zásadním posílením bezpečnosti a významným rozšířením funkcionality. Z těchto důvodů vřele doporučujeme se s některým z nich blíže seznámit a zprovoznit jej alespoň v bezplatné verzi, ve formě základního firewallu. Ačkoliv nastavení většiny těchto nástrojů již vyžaduje jakési minimální znalosti, investovaný čas se vyplatí.

Tip na závěr scénáře: pokud vládnete alespoň základy anglického jazyka, velmi pěkné aktuální srovnání osobních firewallů naleznete na stránce *www.securityfocus.com/infocus/1750*.

Scénář č. 3

Struktura zapojení: malá síť s hardwarově sdíleným připojením k internetu
Typ internetové linky: ADSL či kabelový rozvod
Vybavení: OS Windows a hardwarový modem/router/firewall
Cenové nároky: od cca 2 000 po cca 7 000 Kč
Nároky na znalosti uživatele: střední až vysoké

V případě, že vaše síťové prostředí je tvořeno hned několika počítači, jež sdílejí rychlejší internetovou přípojku, je potřeba vyřešit jak bezpečnost celé sítě jako takové, tak zabezpečení jednotlivých počítačů. Ochranu je možno definovat na několika úrovních v závislosti na konkrétní konfiguraci, takže si popíšeme různé možnosti.

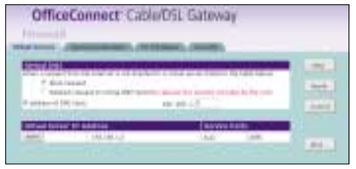
Jedna z variant může zahrnovat internetové přístupové zařízení, jež nedisponuje žádnými či téměř žádnými možnostmi zabezpečení, jako je tomu např. u ADSL modemu Alcatel Speed Touch Home (dodáván v loňském roce se základní variantou ADSL) či u řady kabelových modemů. Následné rozbočení sítě a poskytnutí přístupu vícero počítačům může být realizováno podobně jako v naší experimentální síti třeba hardwarovým integrovaným zařízením, jako je poměrně jednoduchá 3COM OfficeConnect Cable/DSL Gateway 3C857 – zahrnuje v sobě jak přepínač (pro 4 PC), tak základní firewall, a dokáže zajistit první úroveň ochrany na centrálním přístupu k internetu.

Zabudované mechanismy lze považovat za mírně pokročilé: uživatel může buďto příchozí komunikaci zcela zakázat, což je výchozí varianta, nebo využít speciálně definovaných pravidel k propuštění požadovaných typů provozu do své vnitřní sítě (typicky ICQ, zasílání pošty, Vzdálená plocha atd.). Zásadní výhodou je, že takto vložený hardwarový prvek dokáže většinu nežádoucí komunikace, přicházející z internetu, odrazit již v jakési „předsunuté pozici", a samotné počítače jsou tak chráněny od první vlny nebezpečného provozu.

Druhým stupněm zabezpečení, jenž řeší komplikovanější nároky, je posléze opět osobní firewall. Je nutno mít na mysli, že ačkoliv internetová přípojka je chráněna již hardwarovým předstupněm, musíte na tuto síť stále pohlížet z hlediska operačního systému či personálního firewallu jako na potenciálně nebezpečnou, tedy na veřejnou (public). V našem testovacím prostředí využíváme na PC řešení Kerio Personal Firewall, a internetovou přípojku jsme v příslušném ovládacím rozhraní označili jako nedůvěryhodnou (kvůli prázdnému zaškrtávacímu poli). Veškerá přístupová oprávnění je nutno do této sítě nastavit stejně, jako by byla přímou internetovou linkou – jen díky této důslednosti získáte výhodu dvojí obrany, neboť pokud by útočník prolomil hardwarový firewall, stále mu bude stát v cestě další ochrana.

Jiná varianta, jež se od předchozí odlišuje jen mírně, v sobě zahrnuje rovněž dvojstupňovou ochranu. Prvním, předsunutým prvkem je zde opět hardwarové zařízení, ovšem tentokrát v integrovaném provedení odlišného charakteru – základem je vlastní ADSL modem, a s ním je spojena dále funkce přepínače (opět např. 4 porty), routeru a především kýženého firewallu. Jedním z vhodných modelů, jejž jsme vyzkoušeli, je např. Lucent CellPipe DSL Modem 22A-FX, nabízený řadou poskytovatelů internetového připojení ke službě ADSL. Součástí tohoto zařízení je poměrně zdařilý základní firewall, jenž dokáže ochránit první linii vaší sítě a opět odstínit počítače od většiny nežádoucí příchozí komunikace. Podobně jako v předchozí variantě, i zde samozřejmě budeme nadále spoléhat na druhou úroveň ochrany, jíž jsou osobní firewally na všech PC v malé síti.

Konfigurace, na niž jsme se zaměřili v tomto scénáři, již představuje z hlediska malé, domácí sítě velmi solidní bezpečnostní hradbu. Hardwarová část by měla zajistit, že bude odražen i soustředěný útok na vaši síť, jehož intenzita by mohla ohrozit stabilitu OS či softwarového firewallu, a ochranná aplikace naopak umožní jemnější nastavení a důslednější kontrolu. Je však nutno počítat s určitou investicí do samotného hardwaru a také se připravit na konfiguraci, jež nemusí být úplně primitivní. Odměnou za vynaložené úsilí je pak velmi bezpečné a odolné připojení. 4 0007/FEL ❑



Zapamatujte si...

V první řadě je potřeba si uvědomit nejdůležitější zásadu: nemusím mít nejlépe zabezpečenou síť či počítač v celém internetu. Ale mé zabezpečení musí být alespoň o stupínek lepší, než u většiny ostatních.