FIREWALLY: Labutí píseň?

Dříve oblíbené firewally nyní zůstávají ve stínu nejnovějších antivirů a specializovaných nástrojů na boj proti malwaru. Má tedy smysl je instalovat?

PETR KRATOCHVÍL

Den co den se v počítačových médiích dozvídáte o nových programech určených pro boj proti malwaru. Oblíbené jsou především antivirové nástroje s propojením do cloudu, specializovaní pomocníci pro detekci rootkitů nebo slabin systému, případně skenery odkazů a ochránci při surfování. Na slovo firewall však již téměř nenarazíte. Znamená to, že tyto programy už nemají z hlediska bezpečnosti význam?

Jak pracuje malware

Způsobů, jak se malware dokáže dostat do počítače, je celá řada. Stále oblíbené je ukrývání škodlivých kódů do hacknutých programů nebo do cracků, případně do pirátských generátorů klíčů pro software a hry. Jakmile uživatel takový software spustí, malware deaktivuje bezpečnostní software a z webu si stáhne další komponenty.

Mezi stále častější metody infiltrace patří také drive by download. Při tomto útoku je škodlivý kód integrován útočníkem do webové stránky nebo HTML e-mailu. Do počítače se pak stáhne v okamžiku, kdy si uživatel stránku zobrazí v prohlížeči nebo si otevře e-mail. Škodlivým kódem je obvykle jednoduchý JavaScript, který nejprve pouze detekuje software běžící na počítači surfaře (například verzi operačního systému, prohlížeče včetně doplňků a také verzi Flashe a především Javy). Poté ve své databázi zjistí, zda existuje pro zjištěný software zranitelnost, a v kladném případě si ji z hackerského serveru stáhne a použije. Nakonec je na počítač uživatele nahrán malware, který už dělá to, co hackeři potřebují.

Všimněte si, že první krok útoku je ve své podstatě neškodný – teprve poté, co škodlivý kód začne komunikovat se serverem hackerů (případně si stáhne další komponenty malwaru), začne být hrozba skutečně nebezpečná. A právě zde je úkol pro firewall – zablokovat komunikaci škodlivého kódu a tak zabránit jeho aktivaci. Na první pohled se tedy zdá, že firewall by teoreticky mohl nahradit antivir.

Firewall proti malwaru

Výše uvedené tvrzení podporuje i bezpečnostní studie, ve které nezávislý australský bezpečnostní výzkumník Craig Wright zjistil, že nainstalovaný firewall drasticky snižuje pravděpodobnost infikování počítače. V rámci svého testování použil 640 virtuálních počítačů, na kterých nebylo kromě operačního systému nic nainstalováno – žádný další software třetích stran ani antivir. Bez firewallu nezůstal během testování žádný z počítačů nenakažený déle než pět dní (jeden dokonce pouhých pět sekund). Po aktivaci firewallu se doba, po kterou zůstaly počítače bez infekce, protáhla minimálně na 108 dní. V rámci své studie Wright dokázal, že i obyčejný firewall integrovaný ve Windows může malwaru ztížit práci. Kvalitní firewall může dobu bez infekce prodloužit prakticky do nekonečna – je jen na uživateli, jak schopnosti firewallu využije. Zde totiž leží základní slabina těchto praktických nástrojů: až teprve ve spojení se schopnostmi zkušeného uživatele vytvoří firewall pro malware neprostupnou bariéru.

Komunikace v cizím jazyce?

Když se před přibližně patnácti lety začaly psát dějiny akčních počítačových hrozeb a i běžní uživatelé začali masivně využívat bezpečnostní programy, stal se firewall noční můrou. Bohužel nikoliv hackerů, ale především méně zkušených surfařů. Ti najednou měli komunikovat s programem používajícím cizí pojmy, jako port, subnet nebo IP adresa. Navíc po nich chtěl odpovědi na otázky, kterým ani nerozuměli, natož aby se dokázali správně rozhodnout.

Ano, první firewally skutečně fungovaly pouze v režimu dotazů, kdy byl při každém připojení uživatel vyzván, aby určil, zda je či není legální. Zde stačilo jedno chybné rozhodnutí, a uživatel nevědomky vytvořil pro hackery bezplatnou dálnici do svého počítače. Další generace firewallů už nabídla i komfortní režim, v rámci kterého nástroj rozpoznal nainstalované bezpečné programy (internetový prohlížeč, messenger nebo FTP klient) a dokázal pro ně připravit vhodná komunikační pravidla.

Ani v nejnovějších firewallech však není uživatel zbaven práva (a povinnosti) rozhodnout, zda danou komunikaci povolit či zakázat. Moderní firewally si ale s okolním softwarem rozumí natolik, že je podobná zpráva spíše výjimkou, a i proto vyžaduje plnou pozornost uživatele. Obvykle totiž znamená potenciální bezpečnostní riziko.

Palubní firewall nestačí?

Na základě výše uvedených informací je tedy otázkou, zda by vám nestačil jen firewall integrovaný v operačním systému. Pravda je, že Windows od verze Vista disponují poměrně kvalitním firewallem, ale s minimální uživatelskou přívětivostí. Je také nutné vzít v úvahu, že sofistikovanější malware obvykle dokáže integrovaný firewall vypnout, zatímco méně známý program třetí strany nikoliv. Jaký ale zvolit?

Hned v úvodu je nutné říci, že neexistuje žádné objektivní hledisko, podle kterého by se dalo říci, že je jeden firewall lepší a druhý horší. Otázka volby tedy zůstává čistě na uživateli, jeho požadavcích a potřebách. Někdo může preferovat komfortní nástroj s minimem nastavování, zkušenější uživatel zase ocení rozsáhlé možnosti konfigurace a ten, kdo se pohybuje v rizikovějších oblastech, bude chtít i kvalitní antivir. Naštěstí je nabídka (i bezplatných) firewallů natolik rozsáhlá, že si v ní vybere i ten nejnáročnější uživatel.

PETR.KRATOCHVIL@CHIP.CZ

NA CHIP DVD

Připravili jsme pro vás ty nejoblíbenější firewally – tři nástroje, mezi kterými si vybere každý.

ZoneAlarm Free
Jeden z nejstarších a nejznámějších bezpečnostních nástrojů prošel dlouhým vývojem. I bezplatná verze nabízí kontrolu webů, ochranu před sledováním nebo kontrolu stahovaných dat. Ve srovnání s placenou verzí jí chybí podpora a rodičovská kontrola. Na webu výrobce (**www.zonealarm.com**) si náročnější uživatelé mohou stáhnout verzi ZoneAlarm Free Antivirus + Firewall 2013, která k firewallu zdarma přidává i antivir. Na rozdíl od placené verze u ní ale dochází k aktualizaci signatur jen jednou za 24 hodin.

Comodo Firewall
Jeden z nejlepších moderních firewallů, který v celé řadě testů zazářil i nad placenou konkurencí. Mimo jiné nabízí i automatický sandbox, který nedůvěryhodné programy umístí do chráněné zóny, ve které nemohou počítač ohrozit. Podobně jako moderní bezpečnostní nástroje renomovaných firem využívá Comodo Firewall pro svou práci cloud – a to nejen pro prověření důvěryhodných programů a souborů, ale i pro detekci zero day útoků na základě chování softwaru. Vzhledem k uživatelsky přívětivému rozhraní a celé řadě průvodců ho lze doporučit i méně zkušeným uživatelům.

Outpost Firewall FREE
Tento nástroj patří mezi programy staré školy a lze ho doporučit všem, kdo si zvykli na starší firewally a jejich způsoby ovládání. Ani Outpost však nepostrádá moderní technologie, jako je ochrana před zero day hrozbami nebo integrovaný herní režim, při kterém firewall uživatele neruší. Technologie jsou ale zabaleny v poněkud starším kabátu a ani nabídka funkcí nepatří k nejširším. Nástroj od firmy Agnitum dává svým uživatelům najevo, že bezplatná verze je jen ochutnávkou a zájemci o lepší bezpečnost by měli dát přednost verzi Security Suite Pro za 50 dolarů.

POHLED DO BUDOUCNOSTI

Stejně jako hackeři nebo vývojáři antivirových nástrojů nespí ani autoři firewallů. Firewally příští generace, jak je začala nazývat firma Palo Alto Networks, která se jejich vývojem zabývá, by ale měly umět mnohem více, než si uživatel dokáže představit. Jejich hlavním místem nasazení budou převážně firmy – domácí uživatel bude pravděpodobně i nadále preferovat jednodušší bezplatné produkty nebo firewally integrované do bezpečnostních balíků. Co tyto profesionální nástroje, které u nás nabízí například firma Fortinet, nabídnou?

Identifikaci aplikace, nikoliv portu, na kterém je provozována. Základem pro bezpečnostní politiku bude identifikace aplikace, respektive komunikačního protokolu, který využívá, případně použité šifrování nebo podobná charakteristika. Nebude chybět možnost tvorby vlastních signatur pro aplikační detekci.

Identifikaci uživatele jménem, nikoliv jen podle IP adresy. Využití informací o zaměstnanci firmy pro zjednodušenou tvorbu bezpečnostních politik a pro forenzní dohledání bez ohledu na to, kde se uživatel nachází.

Blokování hrozeb v reálném čase. Samozřejmostí je ochrana sítě před zranitelnostmi, malwarem, vysoce riskantními URL adresami a velkým množstvím hrozeb ze souborů nebo obsahu.

Zjednodušení správy bezpečnostních politik. Bezpečné a jednoduché použití grafického nástroje pro editaci bezpečnostních politik. Samozřejmostí jsou jednoduché principy fungování, např. možnost rozdělení jednotlivých rozhraní do bezpečnostních zón a použití těchto zón pro tvorbu pravidel.

JAK OVLÁDAT firewall

Práce s firewallem není nic obtížného – jen je třeba znát několik základních pravidel. Budete-li se jich držet, nemůže vás nic překvapit. Jako příklad pro náš praktický návod jsme použili firewall Comodo, principy práce jsou však stejné i u konkurenčních produktů.

1 DŘÍVE NEŽ SE PUSTÍTE DO SAMOTNÉ INSTALACE, nabídne vám Comodo tři možnosti. Pokud vám hodně záleží na soukromí, nechte políčka prázdná. V opačném případě druhou volbou nic nezkazíte a třetí uděláte dobrou věc.

2 PRVNÍM DŮLEŽITÝM ROZHODNUTÍM po nainstalování firewallu je volba umístění počítače. Tato volba je klíčová pro chování firewallu a v případě notebooku ji uvidíte častěji. U domácího počítače, který svou polohu nemění, můžete přidat zatržítko u položky »Příště již nedetekovat nové sítě«.

3 POTÉ, CO SE NA OBRAZOVCE OBJEVÍ STAVOVÉ OKNO FIREWALLU, klikněte na něj pravým tlačítkem a v nabídce »Miniaplikace« aktivujte všechny nabízené položky.

4 DVOJITÝM KLIKNUTÍM pak otevřete okno firewallu a kliknutím na »Aktualizace« stáhněte nejnovější updaty. Jen tak budete mít jistotu, že program váš počítač ochrání.

5 PO POKUSU NĚKTERÉHO Z PROGRAMŮ O SPOJENÍ S INTERNETEM se na obrazovce objeví zpráva. Pokud si nejste jisti, zda jde o korektní žádost, klikněte na jméno souboru vpravo od položky »Aplikace«. Objeví se informace o souboru, který pokus o spojení aktivoval. V našem případě jde očividně o komponentu tiskárny, takže lze komunikaci povolit.

6 V NĚKTERÝCH PŘÍPADECH však situace zcela jasná nebude. Buď nebude jasné, která aplikace spojení aktivovala (u příslušné položky bude například popisek „systém“), nebo si nebudete jisti, zda je chování známé aplikace korektní (například připojování textového editoru k internetu). V tomto případě jednoduše spojení zakažte a uvidíte, zda se tento zákaz projeví na chování aplikace. Pokud se objeví chybové hlášení nebo nebude něco fungovat, spojení povolte.

7 JEDINOU VÝTKU U FIREWALLU COMODO máme k jeho odinstalaci. Při ní se totiž ze systému neodstraní komponenty Comodo Dragon a Comodo Buddy, které se při instalaci drze nahrály do systému.