

Aplikační ochrany na firewallu v roce 2010

Zpočátku se bezpečnost řešila na velmi nízké úrovni, hlavně rozšířením funkcí switchů a routerů. Cílem bylo oddělit svou vlastní síť od internetu povolením příslušných portů pro žádoucí provoz (HTTP, SMTP, FTP, Telnet aj.). Jak ale zabezpečit síť v roce 2010?

Dříve než si odpovíme, je nutné si znovu připomenout jednoduchou, ale o to důležitější věc. Skutečným cílem není mít zabezpečenou síť, ta je „pouze“ prostředím pro existenci dat, tj. cenných informačních aktiv. Samotné informace jsou pak shromažďovány v aplikacích, databázích či datových skladech, přičemž cesta k jejich zneužití vede přes odchytní provozu, kompromitaci aplikací, frontendů nebo databází. Jejich ochrana tedy začíná zabezpečením perimetru sítě, a to s maximálním důrazem na aplikační úroveň.

Dobrý firewall byl, je a bude základem

Když se řekne zabezpečení perimetru sítě, asi všem nejdříve vytane na mysli firewall. Jeho evoluce v posledních letech je odrazem vývoje potřeb zabezpečení sítě, a tak dnes firewall není pouhým „vrátným“, ale sofistikovaným systémem s řadou integrovaných ochranných (UTM), které jsou zaměřeny na komplexní ochranu na aplikační, tedy dle známého OSI modelu nejvyšší (7.) úrovni. Přístup většiny výrobců se více či méně podobá, mám na mysli technologii založenou primárně na paketové filtraci. Nicméně existuje i jiný přístup, který vsadil od začátku na systém aplikačních proxy bran, tedy nekompromisní bezpečnosti na aplikační úrovni.

(Např. McAfee Firewall Enterprise, mnohým známý pod dřívějším názvem Sidewinder.)

Jedním ze základních pilířů firewallů tohoto druhu jsou obousměrné aplikační brány oddělující jednotlivé segmenty sítě (Internet, LAN, DMZ, atd.). Obvykle se jedná o desítky specializovaných inteligentních proxy kontrolujících komunikaci řady aplikací a často užívaných protokolů (web, email, VoIP, SQL, atd.). Provoz je filtrován od 3. (síťové) po 7. (aplikační) vrstvu OSI modelu. Nevytváří se zde žádné přímé spojení mezi interní a externí sítí, takže se útočník nikdy nedoví, co je za firewallem. V praxi se jedná téměř o ekvivalent fyzického oddělení sítě.

Proxy funguje jako prostředník mezi klientem a cílovým počítačem nebo serverem, překládá klientské požadavky a vůči cílovému počítači vystupuje sám jako klient. Na straně interní sítě vystupuje jako server, který přijímá požadavek (a ucelený jej na aplikační úrovni překontroluje). Poté, již v roli klienta, zahajuje komunikaci se skutečným serverem. Aplikační proxy umožňuje nejen ochranu IP zásobníků chráněných zařízení, ale i jemnější řízení datového provozu, a to díky možnosti zadávat aplikačně specifická pravidla, jako je filtrace příkazů v aktivním kódu apod.

Nelze než kladně přijmout na firewallu možnost dešifrace (a po uplatnění kontrol opětovného zašifrování) HTTPS, SSH, SCP a SFTP spojení. Tím se eliminuje jedna z nejsnadnějších cest pro útočníky, kterou představuje zneužití šifrovaných protokolů pro obcházení bezpečnostních kontrol.

Bez sofistikované kontroly narušení (IPS modulu) se dnes neobejde žádný skutečně použitelný firewall. Zde je třeba se zaměřit na dvě hlavní oblasti. Tou první je kvalita, kvantita a frekvence aktualizace signatur, kterou má firewall k dispozici. Tou druhou je možnost optimalizace uplatňování IPS kontrol, čili uplatňování pouze relevantních kontrol na daný provoz a možnost vytvářet specifické nastavení i pro jednotlivá pravidla. Výsledkem by měla být maximální bezpečnost při minimálním zpomalení provozu.

Důvěřuj, ale prověřuj

Důvěra je jedním ze stěžejních aspektů zabezpečení komunikace na aplikační úrovni. V době, kdy nastupuje cloud computing, je důvěryhodnost druhé strany spojení jedním z kritických ukazatelů. Jak má ale firewall zjistit, komu má důvěřovat a komu ne? Ke slovu se hlásí moderní reputační systémy typu www.trustedsource.org které dokážou vyhodnocovat reputaci dynamicky v čase.

10 0058/tj ■



Jaroslav Mareček
Autor pracuje ve společnosti Comguard jako Product Specialist.

Jaroslav Mareček