



Autor: Katarína Rusnáková

Pátek, 24 Duben 2009 08:43

Na redakční otázky odpovídá Mgr. Marian Lysák, Senior Security Consultant, COMGUARD a.s.

1) Jak se nejlépe zajistit před útoky z webu?

Útoky z webu, tedy na klienty, kteří přistupují na webové aplikace, představují jedno z horkých míst, kde se aktivně bojuje několika způsoby ochrany. První linii představují antivirové programy na jednotlivých stanicích, které odchytily známé viry, červy a spyware podle signatur uveřejněných daným výrobcem. Další v pořadí je personální firewall, který může zabraňovat např. odchozí nebo příchozí síťové komunikaci zákeřného kódu. Zajímavou funkcionalitou, která teprve čeká na svoji větší popularizaci, je blokáce spouštění nechtěných aplikací a zejména pak omezování komunikace mezi aplikacemi samotnými.

Když opustíme zabezpečení klientského systému, pak do webové bezpečnosti další výraznou měrou zasahují aplikační firewally a také specializované zařízení webové filtrace. Moudré aplikační firewally umí zkontrolovat http provoz tak, aby klient a server hráli podle daných pravidel. Mezi funkcionality obrany patří regulace a přepisování hlaviček, vyřezávání aktivního obsahu určitého typu, kontrola provozu antivirovým softwarem. Uživatelé může být i úplně zakázán přístup na webovou aplikaci s daným obsahem dle URL filtrační databáze s kategoriemi. Mezi další prvky ochrany, které jsou obsaženy na robustních aplikačních firewallech, je i kontrola IPS/IDS na základě signatur.

Tam, kde firewallům dochází dech, přichází na scénu specializovaná řešení webové filtrace. Možnosti kontroly robustních aplikačních firewallů zvládnou jedním dechem. Přidávají však další prvky dosud nevídané. Jedním z nich je kontrola spustitelného kódu interpretovaných jazyků nebo dokonce i programů v binárním kódu. Daný analytický stroj provede analýzu spustitelného kódu, vyhledává funkce různého zaměření, např. funkce, které by mohly zapisovat na disk, otevírat socket apod. Jednotlivý nežádoucí kód lze pak ze stránky vyříznout a klientu pak poskytnout "ošetřený" výstup. U přeloženého binárního kódu se pak stroj pokouší detekovat smysl posloupnosti instrukcí. Dle toho pak provádí vyhodnocení zranitelnosti s přidělenou pravděpodobnostní mírou.

Do popředí zájmu se dostává i kombinace několika antivirových strojů. Říká se, že antivir od jednoho výrobce samotný nestačí a je potřeba kombinace signatur od více výrobců. I na tuto možnost tvůrci specializovaných řešení mysleli. U některých lze kombinovat až tři antivirové stroje naráz. Další zajímavou funkcionalitou může být tzv. "data leakage protection", pomocí něj se analyzují známé dokumenty kancelářského softwaru na určité citlivé řetězce. Citlivé dokumenty pak nemohou odejít přes tuto kontrolu ven z firmy.

2) Jak nejlépe zajistit svůj web před útoky?

Bezpečnost webových aplikací je velice komplexní téma. Existuje několik vrstev zabezpečení webových serverů. Jedním z nich je zabezpečení samotné webové aplikace. Je mnoho útoků specializujících se na webové aplikace. Např. XSS, SQL injection, útoky založené na chybné autentizaci a řízení sezení, CSRF, špatné ošetření chybového výstupu atd. Některé robustní aplikační firewally a IPS/IDS řešení se s tímto snaží trochu vyrovnat. Aplikační firewally kladou důrazem na striktní dodržování protokolu HTTP, umí antivirovou kontrolu, omezování hlaviček a příkazů v HTTP. Tím narážejí na svoje hranice a danou úlohu se snaží pak opět vyřešit specializované firewally jen pro webové aplikace. Tyto webové firewally se snaží porozumět nejenom definovanému protokolu a obsahu na základě signatur, ale i chování samotné aplikace. V tom je jejich opravdová síla. Při nasazení do provozu je nutný určitý čas na usazení řešení a odladění false-positives/negatives. Webové firewally také nabízejí pomocnou ruku aplikacím v oblasti zabezpečení kreditních karet. V této oblasti se snaží vyhovět požadavkům stanovených PCI (Payment Card Industry). Dalšími možnostmi se zabývá odpověď na další otázku.

3) Jak zjistit, že je webová aplikace bezpečná?

Existuje mnoho nástrojů, které pomohou při řešení bezpečnosti webových aplikací. Rozlišujme v tomto ohledu mezi bezpečností operačního systému, kde daná aplikace běží, bezpečností samotného webového serveru a

aplikací nutných k běhu (např. databázového systému). V neposlední řadě stojí bezpečnost samotné webové aplikace.

Bezpečnost operačního systému zahrnuje pravidelné sledování nových bezpečnostních hrozeb, následně aplikaci příslušných záplat na daný systém. To samé se týká bezpečnosti programů nad kterými běží samotná webová aplikace. Nesmíme zapomenout na méně používané metody tzv. hardened operačních systémů, které především izolují aplikace mezi sebou. Výrazně se uplatňuje princip co nejmenších práv (principle of least privilege) a omezení nebo rozmělnění moci superuživatelé. Jedná se zejména o projekty RSBAC (Rule Set Based Access Control) nebo DTPE (Domain and Type Enforcement). Tyto technologie, založené na matematických modelech, jsou známé již několik let, ale pořád stojí spíše na prahu reálného používání. I když v některých komerčních řešení se již používají delší dobu.

Na samotnou webovou aplikaci lze provést semi-automatizované testy zranitelnosti, které mohou objevit bezpečnostní chyby, které pak vývojový tým musí opravit. Opravdu mravenčí práci pak představuje analýza zdrojového kódu samotné aplikace, která znamená opravdu podrobné nalezení možných rizik uvnitř samotného programu.

Pomocí těchto několika bodů pak můžeme směřovat k bezpečnější webové aplikaci.

4) Jsou z hlediska webové bezpečnosti lepší řešení běžná - multifunkční nebo proprietární?

To je spíše otázka filosofická. Otevřené řešení přináší možnost kontroly kódu na případné zranitelnosti, komunita kolem projektu sleduje jiný cíl než firmy, které se tím zabývají komerčně. Soustředění je zejména na funkční vlastnosti než na estetické. Komerční řešení dbá i na estetickou stránku a také na použitelnost. Nesmíme zapomenout, že komerční řešení přináší ušetření časových prostředků zaměstnanců spravující a monitorující jednotlivé řešení. Běžně je poskytována záruka na hardware, technická podpora přímo od výrobce, aktualizace na několik měsíců dopředu. Kterým směrem se firma ubere závisí na její velikosti, hodnoty ohrožených aktiv a také výše dostupných prostředků pro řešení tohoto problému.

[Antiviry](#) | [Bezpečnostní management](#) | [Firewall](#) | [Management citlivých dat](#) | [Operační systémy](#) | [Webfiltering](#)