



Redakční otázky k tématu

ŠKODLIVÉ KÓDY A URL FILTERING

odborného on-line magazínu ICT SECURITY – www.ictsecurity.cz

Braňte se účinně proti aktuálním hrozbám zvenčí

Petr Herman, IT Security Consultant, COMGUARD a.s.

1) Jak účinné jsou dnešní filtry obsahu? Jak tuto účinnost měřit nebo jakým typům měření v laboratořích důvěřovat?

Účinnost námi nabízených řešení využívající databázi McAfee Smartfilter se pohybuje okolo 80% s false positives v rozmezí 0.1%.

Vhodným nastavením je však možné účinnost zvýšit a umožnit následné automatické dokategorizování na základě např. klíčových slov v parametrech URL, detekcí vložených URL atd. Součástí každého filtru obsahu by mělo být napojení na globalní reputační systém, díky kterému můžeme filtrovat webové stránky nejenom na základě kategorií, ale též na základě úrovně aktuální hrozby, kterým tato stránka může být (phishing, šíření malware, spam). Při výběru vhodného URL filtru musíme vycházet především z velikosti URL databáze výrobce, množství senzorů a dat, který výrobce denně zpracovává a především jeho pozici na trhu bezpečnostních technologií.

2) Které škodlivé kódy (umístění, typ, účely...) dnes představují největší nebezpečí?

Aktuální a z dlouhodobého hlediska největší hrozbu budou představovat Botnety, které je, díky své univerzálnosti, možné využít snad ke všem hrozbám dneška, ať již se jedná o šíření spamu, malware, tak provádění DDoS útoků, případně zcizení dat nebo identity.

Vhodným řešením tohoto problému z hlediska bezpečnostní politiky firmy může být restriktivní nastavení internetového firewallu s instalací specializovaných web proxy serverů umožňující detekci nejenom malware aplikací, ale též i tzv. PUP (potentially unwanted program) na klientských PC s možností automatické blokáce těchto stanic.

3) Jak se před škodlivými kódy a nebezpečím z webu co nejúčinněji chránit?

Aktuálně nejúčinnější ochranou webového provozu jsou specializované proxy brány, jako je např. zařízení McAfee Web Gateway, obsahující antivirovou-antimalware ochranu a umožňující filtraci/kontrolohu HTML objektů, které mohou být využity pro šíření malwaru. Jedná se především o různé potenciálně nebezpečné Web 2.0 komponenty, jako jsou Java aplety, ActiveX prvky atd. Pro šíření malware aplikací je ve velké míře využíván šifrovaný HTTPS protokol, proto při výběru vhodné bezpečnostní proxy je nutné zaměřit pozornost i na funkce dešifrace HTTPS provozu a práci s SSL certifikáty.



4) Nakolik se na URL filtering dá spolehnout a nakolik jej kombinovat s jinými (jakými?) technologiemi?

Z pohledu bezpečnosti je URL filtering pouze doplňková služba, kterou je nutné doplnit dalšími bezpečnostními technologiemi, jako je např. reputační kontrola.

5) Jak vytvořit co nejlepší proaktivní zed' novým (= neznámým) škodlivým kódům?

Aplikací vícestupňové kontroly, kdy již často nestačí využívat antiviry více výrobců, ale je nutné využívat specializované antimalware enginy s funkcemi jako je proaktivní skenování umožňující detekci chování tzv. mobilního kódu. Velkým problémem dnešních antivirů je též časová prodleva mezi hrozbou, vytvořením virové signatury a aktualizací virové databáze na zákaznických systémech. Proto se stále více začínají prosazovat antivirové systémy, umožňující detekci hrozby v reálném čase a využívající online virovou databázi výrobce. Vhodným příkladem nasazení této technologie může být systém McAfee Artemis.