



CIBULE NEBO IT?

Jak šetřit v IT s novým imunitním systémem?

Zdánlivě nesourodý nadpis tohoto článku nám ukazuje, jak si mohou být významově blízké i velmi vzdálené oblasti jako zemědělství a informatika. Nemohu si pomoci, ale když se podívám na odborný článek s obrázkem operačního systému nebo schéma nějakého procesu, vidím cibuli...

Záleží na interpretaci daného autora, zda-li jednotlivé slupky využije k popisu technického řešení, nebo nějaké bohubilbě činnosti. Nicméně, tento lehký start měl pouze navodit stav širšího vnímání souvislostí a pokusit se vás úvodem zbavit profesních klapků na očích, které často rádi (někdy i zarputile) nosíme. Jsem zaměstnanec společnosti, která se řadu let zabývá bezpečností informačních technologií, a setkávám se při své práci s opravdu pestrou paletou názorů na bezpečnost. Výjimkou nejsou ani zcela protichůdné postoje: „Bezpečnost je jen marketingová bublina komerčních společností, aby vytáhly co nejvíce peněz z klientů“, nebo „Nikdy nemůžeme být dobře ochráněni, nejlépe je všechno zakázat!“.

Pokud si však klapky z očí sejmeme, reálně vidíme, že hrozba existuje, a také chápeme, že informatika by nám měla co nejlépe sloužit, a nikoliv nás při práci

Poslední statistiky ukazují že 80 až 96 % e-mailové komunikace je spam či jiný závadný provoz

omezovat a brzdit. A každý, kdo už si někdy koupil „levný výrobek“, ví, kolik času, peněz i starostí levná věc stojí. Pojďme se tedy podívat, jaké úspory může, pro IT a celou organizaci, přinést nový komplexní imunitní systém McAfee spojující Network Security a System Security.

Kritická místa ochrany

Jaké existuje tedy řešení? Jako dobrý začátek se mi jeví použití selského rozumu, přečíst si pár odborných článků, navštívit několik

konferencí a po krátké době byste měli být schopni pochopit tato fakta:

- » existuje „nějaký“ perimetr, tedy hranice spojující naši síť s okolním světem;
- » existují jisté „oblasti/zóny“ v naší síti, které vyžadují shodná pravidla pro umístění zařízení (aplikační a databázové servery, datová skladiště, stanice, přístupy uživatelů, administrátorů či externích subjektů...);
- » existují aplikace, které jsou v rámci společnosti používány;

» existují lidé, kteří jsou uživateli uvedených technologií, a lidé, kteří jsou jejich správci;

» existují investiční možnosti na pořízení, ale také na provoz těchto technologií.

Když prostý firewall nestačí

Začneme u perimetru. Nejčastější provoz je webový (http, https), e-mailový (smtp) a následuje celá řada dalších provozů, například VPN, VoIP, videokonference, ftp, vzdálené servisní přístupy třetích stran apod.

Většina společností již využívá na perimetru firewall, který je samozřejmě dobré mít, protože filtruje provoz z neznáma, ale také kontroluje provoz od našich partnerů či zaměstnanců na cestách. Méně známé jsou ovšem výhody řešení zvaných „proxy firewall“, někdy též aplikační proxy firewall (např. McAfee Enterprise Firewall / Sidewinder). Taková zařízení poskytují vláknovou technologii s možností definování bezpečnostních zón přímo, a to vše s podporou virtualizace.

Každá definovaná proxy může obsahovat stovky pravidel a zajistit, že neexistuje žádné přímé spojení z nedůvěryhodných segmentů (zejména internetu) do důvěryhodných. Na důvěryhodné totiž vždy komunikuje vlastní proxy firewall poté, co provede hloubkovou kontrolu.

Implementace těchto řešení potom dokáže ušetřit potřebu dalších proxy či bezpečnostních segmentů mimo hlavní perimetr, a poskytuje nejvyšší míru bezpečnosti za přijatelných cenových podmínek. Místo desítek specifických řešení (specializovaných firewallů či jiných oddělovačů, NAC a IPS) stačí společnosti jen jedno komplexní,

s jednou správou a centrální definicí bezpečnostních politik. Navíc takto zabezpečený firewall umožňuje i provoz serverových služeb kritických pro infrastrukturu jako DNS a NTP. Šetříme tedy nejen na hardwarových komponentách, ale i jejich správě a získáváme i potřebnou jistotu bezpečnosti.

Webový provoz pod palcem

Další řešení, které by na perimetru nemělo chybět, je kontrola webového provozu, a to nejen příchozího, ale i odchozího. V rámci imunitního systému nabízí McAfee WebGateway /WebWasher/, která nejenom odfiltruje závadný provoz s kontrolou budoucích rizik (antimalware), ale navíc kontroly provede i uvnitř šifrovaného provozu.

Dokážeme tak eliminovat slepá místa tradičních nástrojů, použít rentgen https provozu a odhalit jak snahu o vpašování nežádoucích kódů, tak například snahu o únik informací nebo tzv. „volání domů“ již instalovaného spywaru. Navíc řešení poskytuje firmám nástroj pro řízení přístupu uživatelů k internetu, snadno provázatelný s Active Directory.

Vítaným doplněním může být caching vyvinutý pro dynamicky generovaný web 2.0. Jedná se o velmi koncentrovanou léčbu a prevenci, čímž i zde dochází k úsporám. Opět tedy namísto samostatných řešení

v podobě proxy, URL filtrace s pravidly přístupu, antiviru, webové cache či DLP (ochrany před únikem informací), máme jedno a navíc propojené na systém globálních reputací TrustedSource, nový fenomén bezpečnosti vycházející z cloud computingu.

Poštovní provoz, jedna z nejvíce kritických služeb pro většinu organizací, a jeho zabezpečení na perimetru bývá stále více vzpomínanou potřebou. Poslední statistiky ukazují že 80 až 96 % e-mailové komunikace je spam nebo jiný závadný provoz (phishing), hromadí se cílené útoky na nepřítel zabezpečené externí smtp servery apod. Opět se podíváme na koncentrovanou léčbu pomocí McAfee Email Gateway /IronMail/, která nejen zkontroluje každý mail, ať přichází, nebo odchozí včetně obrázkových,

Nárůst malwaru za několik let dle údajů McAfee.



a detekuje velmi přesně spam, ale poradí si i s pokusy o únik informací (DLP analýza jako fingerprinting, adaptive lexical analysis a clustering) a zejména obsahuje IPS pro ochranu mail serverů v DMZ nebo vnitřní síti. V rámci své komplexnosti realizuje také ochranu firemních web mail portálů (OWA, LNWA) a nabízí šifrovací modul (TLS,S/MIME, Open PGP).

Umělá inteligence

Popsaná řešení jsou sama o sobě velmi silnou ochranou. A pokud je propojíme pomocí umělé inteligence založené na sofistikovaném reputačním systému? Jednou takovou technologií spojující gateway řešení McAfee je TrustedSource (www.trustedsource.org). Aktivací této inteligence ušetříme až 2/3 kapacity výkonu našich bezpečnostních bran a navíc odfiltruje až 70 % veškerého nežádoucího provozu (ověřeno praxí). Další „vychytávkou“ této technologie je tzv. GEO-LOCATION, tedy reputace podle geologického umístění zařízení žádajícího o spojení s naší sítí.

Dovolu mi dnešní první díl o umělé inteligence uzavřít a vybidnout vás ke kontrole reputace právě vaší organizace na uvedeném portálu. Příště se podíváme na naše uživatele a odloupneme další slupku z naší ochranné cibule s pomocí řešení McAfee. □

Muzeum v knize

Repliky středověkých mincí, bankovek a státovek



Poznejte historii na vlastní oči.