

Eliminace bezpečnostních rizik webového provozu ve společnosti Skanska

Strmý nárůst popularity webu přináší nárůst velkého množství a „kvality“ hrozeb spojených s protokolem HTTP/HTTPS (malware). Je nutné čelit sofistikovaným útokům kombinujícím různé strategie pro cílené získávání citlivých dat, často skrytých v HTTP či „nekontrolovatelném“ HTTPS provozu. McAfee Web Gateway (Webwasher®) posiluje v jednom zařízení „bojeschopnost“ antivirových a webových filtrů integrací zabezpečené cache (i pro DNS), napojení na systém globální inteligence a dešifrací HTTPS protokolu. Navíc díky proaktivnímu skenování tzv. „mobilního kódu“ s rozšiřujícím Anti-Malware enginem zdvojuje ochranu proti zákeřným kódům a filtruje tak provoz dvěma nezávislými systémy najednou.

Stavební skupiny se snaží vytvořit příjemné prostředí pro bydlení, práci a cestování. Odvádí poctivou práci ve vysoké kvalitě při dodržování standardů bezpečnosti práce a s ohledem na šetrné chování k životnímu prostředí. Zachování si dobrého jména je pro ně zcela zásadní a proto nakupují osvědčená řešení. Samozřejmostí je i oblast IT bezpečnosti chránící firemní síť proti nejrůznějším rizikům, únikům firemních dat a informací.

Výchozí situace

Společnost byla nucena řešit situaci z pohledu eliminace možných bezpečnostních rizik internetového provozu. V rámci shrnutí možných rizik se soustředila na následující položky.

- **Viry, malware a hackerské útoky.** Tvůrci virů a jiných škodlivých kódů (spyware, adware, Web 2.0, exploits, active x prvky, crosssite scripting) využívají jako prostředek pro infiltraci do vnitřní sítě nejčastěji IM (Instant Messaging) komunikaci. Aplikace typu IM jsou vyvíjeny tak, aby si byly vždy schopny najít cestu (otevřený port) pro svoji činnost. Mají schopnost skenovat všechny přístupné porty a díky tomu otevírají přístup pro hackerské útoky na vnitřní síť.

- **Nekontrolovatelnost zdrojových kódů aplikací.** Pro správce sítě není možné zjistit skutečný obsah provozu u aplikací, jako je např. Skype a tudíž garantovat bezpečnost takového provozu.

- **Kapacita šířky pásma.** Ekonomickým problémem je „plýtvání“ internetovou konektivitou, jelikož zejména stahování

různých typů dat, jako jsou např. mediální soubory MP3, video, filmy, internetová rádia a jiná streamovaná media, neefektivně zatěžují kapacitu připojení.

- **Šifrovaný provoz.** Objevila se i nutnost řešit kontrolu HTTPS provozu, protože sofistikované útoky zvenčí kombinují různé strategie pro cílené získávání citlivých dat, často skrytých v obecně akceptovaném HTTP nebo právě v „nekontrolovatelném“ HTTPS provozu.

- **Nekontrolovatelný přístup a nelegální obsah.** Díky nelegitímnímu chování uživatelů, kteří stahují prostřednictvím P2P sítí nelegální software, dochází ke střetu s platnými právními normami.

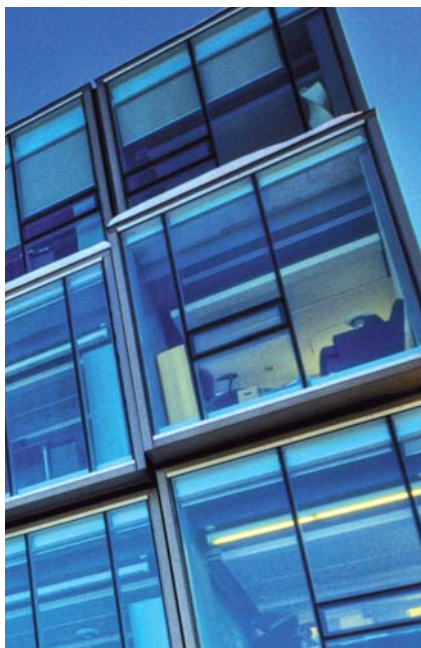
Společnost řešila i problém nekontrolovatelného přístupu do internetu jednotlivých zaměstnanců, jako jsou prohlížení webových stránek s mimo pracovní aktivitou, stahování dat k nepracovním účelům nebo eticky problematický obsah (erotika/sex, nelegální software).

Řešení a hlavní přínosy nasazení McAfee Network Security

Řešení McAfee Network Security zahrnuje celou řadu bezpečnostních produktů zaměřených na ochranu perimetru sítě, poštovního a webového provozu. Pro eliminaci výše uvedených internetových rizik byl doporučen produkt McAfee Web Gateway.

McAfee Web Gateway (Webwasher®)

- **Dokonalá ochrana informačních aktiv.** Ucelené portfolio preventivních



Specifikace zákazníka

Skupina Skanska v České a Slovenské republice je jednou ze 13 obchodních jednotek celosvětové skupiny Skanska, čtvrtého největšího stavebního a developerského koncernu se sídlem ve Švédském království.

Základním předmětem podnikání skupiny je stavební činnost, zejména dopravní, občanské, bytové, inženýrské a průmyslové stavby, dále development a Facility Management.

Počet uživatelů v síti: 2800

COMGUARD

communication security

Společnost COMGUARD a.s. je nadnárodní společností zaměřenou na value-added distribuci produktů bezpečnosti IT. K jejím hlavním partnerům patří společnosti McAfee (vč. akvizované Secure Computing), LogRhythm, Infoblox, Elitecore-Cyberoam, ActivIdentity, Breach Security, PGP a další. Společnost působí na trzích střední a východní Evropy, zejména v České republice, na Slovensku a na Ukrajině. Poskytuje řešení a služby pro segment SMB, velké komerční společnosti a státní organizace. Společnost je vlastněna jejím managementem.

www.comguard.cz

i reaktivních nástrojů proti veškerým formám nebezpečného a nechtěného obsahu webového provozu generovaného uživateli.

- **Rychlá návratnost investice.** Okamžitý růst produktivity zaměstnanců díky omezení nepracovního využití internetu, méně bezpečnostních incidentů v síti, úspora nákladů za internetovou konektivitu.

Klíčové charakteristiky

- **Úspěšnost kontroly 99 %.** Díky více než 99% úspěšnosti kontroly protokolu HTTP, HTTPS a FTP je Web Gateway řešením No. 1 v boji proti nebezpečným kódům. Využívá unikátní kombinaci lokálních analýz s globální inteligencí „McAfee's Global Threat Intelligence“.

- **Globální inteligence.** Proaktivní detekce s napojením na systém globálních reputací založené na technologii TrustedSource™, využívá znalosti chování subjektů na internetu, identifikuje podezřelé a nelegitimní chování entit (např. IP adres, URL, domén, atd.). Blokuje spojení bez využití vlastního výpočetního výkonu lokálního zařízení!

- **Web & DNS Cache** proaktivní kontrola a testy reputace objektů před doručením uživatelům, nižší nároky na kapacitu disku, odpadá časté čištění cache.

- **URL Filtrace s technologií Smart-Filter.** Denně aktualizovaná databáze 35 mil. stránek v 90 kategoriích dokáže ochránit uživatele před nebezpečnými webovými stránkami. Jde o preventivní nástroj v boji proti malware s nástrojem personálního řízení. Dochází ke zvýšení produktivity zaměstnanců, zamezení stahování nelegálních dat a zvýšení efektivity využívání internetové konektivity.

- **Kontrola šifrovaného provozu.** Umožňuje dočasné dešifrování odchozího i příchozího HTTP a HTTPS provozu, následnou kontrolu obsahu včetně SSL certifikátů a následné zpětné zašifrování, čímž brání vzniku „tunelů“ (např. free mail via HTTPS), kterými lze infiltrovat malware do jinak zabezpečené sítě a zachovat tak důvěrnost dat.

- **HSM Card** (Hardware Security Module) doplnění pro SSL Scanner. Provádí fyzickou ochranu šifrovacích klíčů a certifikátů, čímž naplňuje požadavky bezpečnostních norem a standardů. Je k dispozici pro všechny hardwarové modely McAfee Web Gateway.

- **Správa a přehledné reporty.** Díky nástroji Web Reporter je umožněno správcům sítě volitelné a jednoduché nastavení politik uživatelů s přehlednými reporty.

Konkrétní modely, nasazené technologie a implementace

- ▶ Na základě analýzy webového provozu zákazník zvolil Web Gateway Appliance model WG 5000. Analýza webového provozu zohledňovala konkrétní požadavky, jako např. předpokládané HTTPS hity/sec (plus peak – krátkodobé maximum), předpokládaný objem přenesených dat (den/měsíc), předpokládanou šířku pásma do internetu (s výhledem na min. 3 roky), předpokládaný počet uživatelů (s výhledem na 3 roky) a nasazení PROXY včetně DNS a Secure Cache. Celková implementace, která zahrnovala i analýzu průběžného provozu, trvala 1 měsíc. Prvotní instalace včetně přípravy trvala 18 hodin.

CÍLE ŘEŠENÍ

- ▶ Pokryly se současné i budoucí hrozby díky implementaci unikátního webového bezpečnostního zařízení McAfee Web Gateway (Webwasher) s technologií WEB PROXY&CACHE a inspekci HTTPS provozu, díky čemuž může firma účinně eliminovat hrozby Webu 2.0 a účinně řídit a kontrolovat obsah internetové komunikace. Firma může využít přídatného HSM (Hardware Security Module) jako bezpečné úložiště certifikátů pro SSL provoz.
- ▶ Splnil se požadavek na vyšší výkon a efektivitu, včetně případné škálovatelnosti a rozšiřitelnosti řešení.
- ▶ Řešení respektuje požadavky z hlediska funkčnosti a výkonu s ohledem na rozvoj infrastruktury společnosti a s výhledem min. na 3 roky.