

PROXY HRÁZ

Komerční úvěrová pojišťovna EGAP (dále jen KUPEG) poskytuje komerční úvěrové pojištění a je jedničkou na českém trhu dlouhodobě držící 40% podíl na trhu s úvěrovým pojištěním. Na tomto trhu začala působit již v roce 1992, tehdy jako součást společnosti Exportní garanční a pojišťovací společnost (dále jen EGAP).

V případě výběru vhodného firewallu pro KUPEG byla jednoznačně rozhodujícím kritériem úroveň a kvalita technického řešení, podpory a v neposlední řadě zajištění nezbytného servisu. Důležitým požadavkem byla jednoduchá a přehledná obsluha, filozofie typu „zakázáno je vše, co nepovolíme“ a variabilita řešení. Po zvážení všech variant řešení bylo vybráno řešení Secure Firewall Sidewinder od společnosti Secure Computing, firewall pracující na principu aplikačních proxy bran.

Při srovnávání konkurenčních produktů nás zaujala mimo jiné technologie aplikačních proxy ochrany, zabezpečený Secure OS s patentovanou technologií TypeEnforcement, díky které firewall za 15 let své existence nevyžadoval bezpečnostní patchování, a zabezpečené split servery pro SMTP a DNS integrované přímo na firewallu. V oblasti aplikačních proxy firewallů je Sidewinder špičkou a implementace těchto typů obran nepřinesla žádné nežádoucí komplikace pro dostupnost služeb. Naopak umožnila jednoznačně splnit princip zajištění důvěryhodnosti, protože aplikační proxy firewallu (přes 40 proxy) a split servery vždy terminují provoz z nedůvěryhodných segmentů na externí proxy a důvěryhodná proxy (interní) firewallu pak navazuje nové spojení na servery v DMZ a LAN, aniž by však byla dotčena dostupnost.

KUPEG používá uvedené technické zařízení od svého založení v roce 2005. Můžeme použít i zkušenosti z mateřské společnosti EGAP s provozováním stejného typu zařízení (již od roku 1999). V roce 2007 KUPEG pořídila druhé zařízení Sidewinder pro nově budovanou záložní lokalitu. Velkou výhodou se ukázala možnost klonování konfigurace, fyzická zastupitelnost a hlavně možnost správy obou zařízení z jediné konzole.

Komerční a úvěrová pojišťovna EGAP pravidelně prochází penetračními testy použitých technologií včetně revize používaných pravidel a politik. Ty jí pomáhají udržovat po-

žadovanou míru bezpečí a přinášejí i nezbytné připomínky a poznatky ke stávající bezpečnostní politice. Navíc se zde projevuje další faktor: zcela nezávislý pohled na bezpečnostní pravidla společnosti. Je mylné se domnívat, že samotný, byť sebelepší firewall zajistí patřičnou míru bezpečí. Vždy se jedná o soubor pravidel, politik, nastavení, monitorování, patch managementu, testování, vyhodnocení a mnoho jiných činností, které se musejí pravidelně opakovat. Pokud si však dovoluji z výsledků penetračních testů vyčlenit pasáže týkající se fyzického zařízení, vždy se jednalo o potvrzení vysokých kvalitativních parametrů UTM firewallu Sidewinder.

Za zmínku stojí administrativní rozhraní, které bylo několikrát upraveno a které je v poslední verzi uživatelsky přívětivější, přitom ale zůstává zachována i možnost plnohodnotné správy z command line. Z vlastní zkušenosti si troufám tvrdit, že uživatelé starších verzí nenarazí na žádný problém s administrací zařízení po přechodu na vyšší verze.

Pro zajištění provozu využívá KUPEG konzultační a školicí služby od distributora, jímž je společnost Comguard. Po celou dobu jsou společnosti Comguard poskytovány jak profesionální služby technického charakteru, tak kvalitní konzultační činnost v oblasti bezpečnostních řešení. Oceňujeme spolehlivost a rychlost při řešení svých požadavků i adekvátní reakci při řešení problémových stavů a dialog.

Firewall jsme postupně rozšířili o následující moduly: IPS engine, SecurityReporter, Anti-Virus & Anti-Spyware, Anti-Spam & Anti-Fraud a SmartFilter. Uvedené moduly jsou integrované do administrativní konzoly Sidewinderu, SecurityReporter jako externí re-

portovací nástroj zpracovávající logy z desítek i stovek zařízení a SmartFilter mají svoji administrativní konzolu.

IPS engine rozšiřuje Sidewinder o detekci nežádoucího provozu, přičemž IPS signatury jsou automaticky aktualizovány a umožňují rozšířit přímo jednotlivá firewallová pravidla o tento druh kontroly. Vzniká tak možnost přesně specifikovat kritéria provozu dle cílových serverů a aplikací, a virtuálně tak nasadit desítky IPS sond.

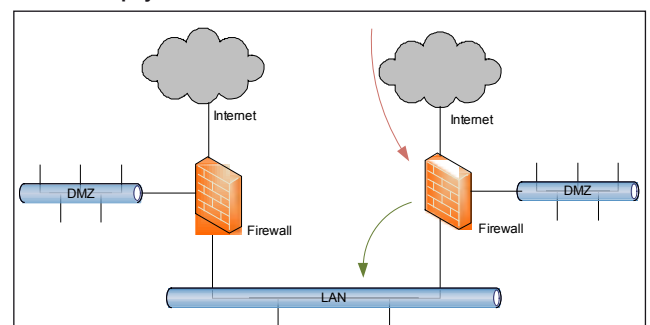
Anti-Virus & Anti-Spyware je plně integrovan do Sidewinder UTM appliance a v našem pojetí se jedná o první „hráz“ a obranu proti nechtěnému obsahu. Umožňuje nám kontrolovat http, ftp a smtp provoz vedoucí do naší sítě.

Anti-Spam & Anti-Fraud je plně integrovan do Sidewinder appliance s propojením na systém globálních reputací TrustedSource.org a stejně jako u antivirového řešení se v našem pojetí jedná o první kontrolní úroveň. Jako zajímavost poslouží údaje ze SecurityReporteru o počtu zachycených spamů. Můžeme zde uvést číslo ukazující na více než 120 tisíc zachycených spamů za měsíc.

SmartFilter je řešením, které nám umožňuje zachycovat a případně omezovat uživatelskou činnost na internetu. Pomocí předdefinovaných nebo vlastních pravidel můžeme vynucovat firemní politiku a v případě potřeby monitorovat aktivitu zaměstnance. Již jen povědomí o používání monitorovacích systémů dokáže napravit ty „nejzřehavější“ hlavy a zaměstnavatelé se investice v této oblasti vrátí přinejmenším v podobě vyšší efektivity práce.

Díky bezpečnostnímu řešení od společ-

Schéma zapojení KUPEG



ností Secure Computing se nám podařilo vybudovat robustní, dobře spravovatelné a variabilní řešení, které plně vyhovuje nárokům společnosti KUPEG v oblasti řízení přístupu a ochrany dat. Řešení pomocí appliance Sidewinderu je velice dobře udržovatelné a rozšiřovatelné. Plně pokrývá stávající hrozby a je velice otevřené k řešení hrozeb budoucích.

Ing. Radek Pohnán, KUPEG,
pohnan@kupeg.cz