Glosa

Pocit sucha a bezpečí

Jistě to znáte, valí se to ze všech stran. „Přidali jsme do našeho antiviru funkci osobního firewallu.“ „Uvedli jsme novou bránu integrující funkci firewallu, IDS, antiviru a filtrování obsahu.“ „Nabízíme kompletní bezpečnostní řešení“. Zdá se, že konec specializovaných zařízení pro určitou úlohu se neodvratně blíží. Všechno se zjednoduší a zlevní, odpadnou problémy s kompatibilitou zařízení mezi sebou, zjednoduší se administrace a instalace. Často slýcháme tyto argumenty. Ale je tomu skutečně tak? Jsou všechny vlastnosti zakoupeného zařízení zákazníkem skutečně využité? Nemělo by vzdělávání zákazníků v oblasti IT být nadřazeno touze prodat a to cokoliv?

Pro příklady nemusíme chodit daleko, ale abych nikoho neurazil, konkrétní zúčastněné vynechám. V jedné brněnské organizaci čítající cca 50 počítačů, říkejme jí třeba Moderní firma, řídí a omezuje provoz unifikovaná bezpečnostní brána integrující firewall, antivirus a filtrování nežádoucího obsahu. Na všech pravidelně aktualizovaných počítačích můžeme samozřejmě najít poslední verzi antiviru renomovaného světového výrobce. Celá firemní síť je předpisově strukturovaná, najdeme zde důsledně oddělenou privátní LAN od sítě určené návštěvníkům a demilitarizované zóny.

A protože je Moderní firma opravdu moderní, rozhodli se pro audit provozu datové sítě. K nikoliv mému překvapení stačilo spustit monitoring provozu na síti a klientská stanice rozesílající přes 100 spamů za minutu vedla žebříček pomyslné hitparády. Na počítači se pak našel dobře schovaný škodlivý program „svcnost“ nápadně podobný systémové součásti „svchost“. Po jeho odstranění bylo po spamech, ale to už jsou nepodstatné podrobnosti. Už méně nepodstatná je nemožnost odesílat e-maily z celé firemní sítě v důsledku zařazení organizace na blacklist, které reálně hrozilo. A tak se ptám, nechybí konceptu Unified Threat Management něco? A kolik takových počítačů máte ve vaší síti vy?

Pavel Minařík - *Chief Technology Officer ve společnosti AdvaICT*
pavel.minarik@advaict.com | *08.11.10*