



Redakční otázky k tématu

BEZPEČNOST PRO SMB

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

Nadpis článku:

ICT technologie jako nástroj pomáhající vytvářet zisk

Autor odpovědí:

Jaroslav Mareček, Product Manager, COMGUARD a.s.

1) Firmy z oblasti SMB pocítují tlak na cenu ICT řešení nebo jeho části ještě intenzivněji než ostatní. Jak co nejlépe vyvážit poměr cena-výkon?

Dle mého názoru by nemělo být prioritou hledat nejlepší řešení z pohledu cena / výkon. Důležité je v první řadě brát ICT technologie jako službu podporující hlavní činnosti tvořící společnosti zisk. Pak je pohled na to, co firma potřebuje a kolik může investovat, daleko jednodušší.

2) Myslíte si, že rozvoj firmy jde ruku v ruce s rozvojem datové infrastruktury? Je vůbec rozvoj SMB firmy možný bez rozvoje ICT infrastruktury? V čem se tohoto pohledu zabezpečení v SMB liší od ostatních segmentů?

Na první otázku lze obecně odpovědět ano, na druhou ne. Samozřejmě mohou být výjimky s ohledem na obor podnikání. S návazností na odpověď výše mám za to, že se liší v objemu a struktuře informačních aktiv (data, infrastruktura, ...), které jsou hodny nějaké ochrany. Každý si je schopen spočítat výhodnost havarijního pojištění u svého auta. Analogicky lze uvažovat i o investicích do bezpečnosti, které mají de facto povahu pojištění či zajištění dostupnosti, důvěrnosti a integrity poskytovaných služeb.

3) Dá se bezpečnost u SMB zvládnout „svépomocí“, nebo je lepší spolehnout na outsourcing?

Pokud organizace disponuje šikovným administrátorem se zájmem o bezpečnost IT, pak asi ano, protože existují produkty, které jsou zaměřeny na maximální komplexnost bezpečnostních funkcí, jednoduchost správy a v neposlední řadě efektivitu z pohledu vynakládání prostředků vč. času administrátora (např. UTM Cyberoam). Obecně lze ale spíše doporučit služby specializovaných IT firem.

4) Dá se říct, že cloud computing řešení je pro SMB velmi vhodný. Lze toto tvrzení paušalizovat? Jaké výhody a nevýhody cloud computing pro segment SMB přináší?

Výhodný v řadě případů může být. Jisté je, že jeho využití bude narůstat. Čím více je organizace zvyklá na outsourcing, tím je rozhodování pro cloud snazší.



Problémem může být potřeba zachovat a využít stávající investice, ale v jistých případech také např. právní otázky v případě umístění serverů poskytovatele mimo EU. Strach ze svěřením dat je ve většině případů irelevantní, navíc není problém data šifrovat.

5) Které produkty či služby Vaše společnost zaměřuje na segment SMB? (včetně balíčků, slev, věrnostních programů apod.)

Z portfolia produktů a služeb distributorské společnosti COMGUARD a.s. bych na prvním místě jmenoval výrobce McAfee a Cyberoam.

- McAfee Endpoint Protection – „antivirové“ balíčky pro ochranu stanic a serverů v LAN

(<http://www.comguard.cz/produkty/mcafee-endpoint-sec/mcafee-total-protection-for-endpoint/>),

- McAfee SaaS – hostované bezpečnostní služby (cloud computing) pro ochranu webu, emailu i koncových stanic a serverů

(<http://www.comguard.cz/produkty/mcafee-web-email-sec/mcafee-email-web-security-ews/>),

- McAfee Email & Web Security Appliance – nákladově efektivní bezpečnostní bránu dostupnou i v softwarové verzi pro VMware

(<http://www.comguard.cz/produkty/mcafee-saas-hosting/>),

- UTM Cyberoam – komplexní bezpečnostní bránu pro organizace od cca 5 uživatelů zahrnující Firewall, VPN, SSL VPN, Bandwidth Management, Multiple ISP, Load Balancing & Failover, Reporting Module, Antivirus, Antispam, Web & Application Filter, IPS, ...

(<http://www.cyberoam.cz>)