

Rozhovor: Kompetenční centrum Comguardu a McAfee má firmám otevřít oči



Zdroj: ChannelWorld, autor Jan Mazal, foto ChannelWorld | 04.10.11

S Janem Dymáčkem ze společnosti Comguard, Pavlem Hankem a Jonem Parksem z McAfee jsme hovořili o příležitostech, které otevírá nové kompetenční centrum.

Distributor s přidanou hodnotou, společnost **Comguard**, otevřel společně s hlavním partnerem, společností **McAfee**, vlastní kompetenční centrum. Jeho cílem je informování zákazníků o nových bezpečnostních rizicích a dalším vývoji a pomoc jim na ně reagovat novými bezpečnostními technologiemi. V kompetenčním centru je možné nasimulovat reálný provoz určitého prostředí a tím otestovat funkčnost navrhovaného řešení ještě před jeho implementací v praxi.

Základem síťové infrastruktury jsou technologie Cisco, aplikační vrstva je založena na produktech společnosti Microsoft a virtualizační prostředí zajišťuje VMware.

Jak mohou vaši partneři využívat nového kompetenčního centra a jak výhody jim přináší?

Jan Dymáček: Dneska mají IT profesionálové problém přesvědčit management organizace, že jsou skutečně pod bezpečnostním rizikem. Je obtížné vedení vysvětlit, že riziko reálně existuje i v České republice a na Slovensku. V kompetenčním centru dokážeme srozumitelným způsobem organizacím předvést různé hrozby a především řešení, které jim dokáží čelit na základě šestnácti různých scénářů. Pokud mají vybrány konkrétní nástroje pro zabezpečení, umožníme jim vyzkoušet a otestovat, zda jsou skutečně účinné proti konkrétním hrozbám.

Jaká je hlavní role Comguardu v novém kompetenčním centru?

Pavel Hanko: Comguard ze svého postavení pomáhá nejen zviditelnit riziko a ochranu, ale také jít o krok dál. Management si někdy hrozby skutečně uvědomuje, ale vlivem různých legislativních předpisů či politik může mít svázané ruce a nedokáže s tím tak nic dělat. Vizualizace celého problému může přispět ke konečné implementaci řešení.

Jak mohou partneři přistupovat do centra?

Jan Dymáček: Partneři nás mohou v Brně buď navštívit tzv. on-site, tedy přijdou osobně, nebo si přivedou zákazníka. Případně, pokud to řešení technologicky umožňuje, se k nám lze připojit vzdáleně přes SSL zabezpečené VPN.

Kdy je tedy pro partnera/zákazníka zajímavější zvolit vzdálený přístup a videokonference?

Jan Dymáček: Záleží na způsobu formulace požadavku. Pokud bude jednoznačný a dokážeme se na něj plně připravit, není problém jej předvést vzdáleně. Zákazník nebo partner tak nemusí trávit hodiny času na cestě. Samozřejmě, pokud budou chtít hledat řešení ochrany s námi na místě, je lepší přijít a konzultovat to naživo.

Pavel Hanko: Osobně bych být zákazníkem či partnerem preferoval osobní kontakt kvůli bližší možnosti interakce. Pokud má zákazník skutečně získat „dojem zabezpečení“, cesta do Brna se vyplatí. Z Prahy ani Bratislavy to není daleko.

Podle čeho bylo vybráno oněch 16 případových studií?





Jan Dymáček: Vycházeli jsme z praxe a předchozích zkušeností se zákazníky. Rozdělili jsme je také podle vertikálních trhů – finanční sektor, zdravotnictví, vláda a výrobní podniky, takže se najdou příklady v podstatě pro každého.

V jedné z případových studií jsem si všiml přístupu zabezpečení koncových bodů z cloudu. Znamená to tedy, že pokud jsem offline, není koncový bod chráněn?

Jon Parkes: Pokud zákazník využívá zabezpečení z cloudu, je k dispozici několik modulů. V cloudu může být provozována pouze „intelligence“, přičemž moduly lze stáhnout do koncového zařízení. Když je klient on-

line, chráníme jej v reálném čase, při odpojení se pro ochranu používají informace uložené v cache paměti. I v případě, že klient využívá kompletní ochranu z cloudu, má na koncovém bodu nainstalován základní software, který jej v základní míře chrání, ne však pochopitelně na úrovni plné kapacity.

V rámci centra jsou k dispozici i místnosti pro individuální konzultace a přednáškové a výukové místnosti. Poskytujete školení a semináře bezplatně?

Jan Dymáček: Ano, jak pro partnery, tak pro klienty. Cílem není na školení vydělávat, ale poskytovat službu a přidanou hodnotu zákazníkovi.

Mohou partneři v kompetenčním centru testovat také řešení poskládané z produktů různých výrobců?

Jan Dymáček: Hlavním záměrem je umožnit partnerům testovat funkčnost řešení s produkty třetích stran, nikoliv však bezpečnostními. Umožňujeme jim například zjistit, zda skener zranitelností funguje s aktuální verzí databáze a jestli ji to při skenování neshodí. Kompetenční centrum nabízí ucelenou platformu bezpečnostního řešení a při předvádění jejich účinnosti lze samozřejmě omezit funkčnost na jednotlivé moduly (antispam s antivirem nebo včetně pokročilých metod s analýzou obsahu). Naši odborníci však nemohou být specializovaní na všechny bezpečnostní produkty dostupné na trhu.

Jon Parkes: Naše zákazníky i partnery zajímá fungující řešení zabezpečení a je tedy nevyhnutelné, že budou používat „multi-vendor“ a „multi-product“ řešení. Ačkoliv McAfee nabízí kompletní portfolio, zastáváme pragmatický přístup. Záleží na volbě zákazníka.

Dlouhodobými trendy jsou mobilita a vestavěné systémy, jaká je budoucnost partnerů v těchto oblastech?

Jon Parkes: Systém pro management chipsetů Intel dnes mohou partneři spravovat z McAfee UPM a brzy také uvedeme produkt, který jej dokáže i zabezpečit. Wind River, jeden z největších dodavatelů operačních systémů pro vestavěné systémy, se prostřednictvím Intelu stal i naším partnerem. Nyní spolupracujeme na zabezpečení jejich softwaru. Vestavěné systémy budeme moci dodávat s bezpečnostním softwarem, který zároveň umožní k těmto zařízením vzdáleně přistupovat a konfigurovat je z pohledu zabezpečení.

Myslím si, že klíčovou oblastí pro partnery budou služby s přidanou hodnotou, správa těchto zařízení a konzultace. S naší pomocí se dokáží posunout ze správy 10 000 počítačů na 100 000 zařízení, ať už mobilních či desktopových.



Pokud se na stejnou věc podívám optikou volume resellerů? Jaké možnosti pro ně otevírá technologie Deep Save (zabezpečení pod úrovní OS, pozn. red.)?

Jon Parkes: Produkty založené na technologii DeepSave se chystáme představit v říjnu na konferenci v Las Vegas. Určitě budou dostupné pro naše prodejní partnery. Jedná se o add-on k našemu řešení pro ochranu koncových bodů, který otevírá obrovskou příležitost pro volume resellery.

O aktuálních trendech, kterými jsou cloud computing a mobilita, a o nebezpečí hrozeb podobných operaci Temná krysa, se dočtete v další části rozhovoru s **Jonem Parkesem** na [sesterském webu CIO BusinessWorld](#).

Jon Parkes, viceprezident presales, je v McAfee zodpovědný za veškeré technicko-obchodní operace a návrhy řešení pro zákazníky EMEA regionu. Pomáhá zákazníkům postavit a realizovat řešení splňující jejich konkrétní bezpečnostní a obchodní potřeby a optimalizovat náklady na zabezpečení s ohledem na vývoj bezpečnostních

hrozeb. Jon Parkes se pohybuje na poli softwarové konzultační činnosti, zejména pro velké firmy, již 20 let. Během své dlouholeté kariéry pracoval na vedoucích pozicích a spolupracoval se zákazníky z některých největších světových firem v mnoha průmyslových odvětvích včetně telekomunikací, finančních služeb či vládních organizacích, a to jak v oblasti EMEA, tak I Asie či Tichomoří.

Jan Dymáček, výkonný ředitel společnosti Comguard. Buduje silný tým expertů, komunikační kanály s výrobcí bezpečnostních řešení a sestavuje komplexní výběr bezpečnostních řešení vhodných jak pro státní správu, tak velké společnosti nebo SMB trh. Jeho významnou rolí je i realizace nových projektů, jako je Kompetenční centrum pro ICT bezpečnostní řešení nebo plánování obchodních strategií či jednání s obchodními partnery. Dříve pracoval u nadnárodní společnosti KPNQwest a v managementu společnosti SkyNet, kde působil jako ředitel divize Bezpečnosti.

Pavel Hanko, channel account manager ve společnosti McAfee – má na starost distribuční strukturu, partnerský kanál a podporu koncových zákazníků v České republice i na Slovensku. Dříve působil ve společnosti Panduit, kde řídil obchodní týmy a partnerský kanál na pozici area manažera pro ČR, SR, Polsko a Maďarsko.
