

Jon Parkes z McAfee: Temná krysa byla jen špičkou ledovce

Zdroj: businessworld, **Rady & názory**, autor redakce, foto businessworld | 04.10.11

Při příležitosti otevření kompetenčního centra společností Comguard jsme měli možnost hovořit s Jonem Parkesem z McAfee.



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.

CIO BusinessWorld: V souvislosti s rostoucí úlohou cloud computingu se hovoří o tom, že bude stále více docházet k přesunu bezpečnostního softwaru z koncových zařízení do prostředí "výpočetního mraku". Dokážete popsat, jaké vývojové fáze nás čekají v průběhu tohoto přesunu? Jak podle vás bude vypadat "koncový" stav tohoto procesu?



Jon Parkes: Nevím, jestli dokáže někdo skutečně předpovědět, jak bude tento vývoj pokračovat. Co však víme, je, že tato změna probíhá velmi rychle. Svět zažívá obrovský nárůst využití různých zařízení a všechny mohou přistupovat ke službám v cloudu. Mnoho podniků do cloudu nevstoupí, dokud si nebudou jisté, že existuje bezpečný způsob, jak k těmto datům přistupovat. Využití cloudu je nevyhnutelné a poroste stále rychleji, velké společnosti do něj budou však vstupovat pomaleji v závislosti na nabytých důvěře. Proto také vyvíjíme vlastní autentizační technologie, protože si uvědomujeme, že tohle je krok, jak otevřít cestu podnikům do výpočetního mraku.

Mnoho spotřebitelů dnes využívá služby v cloudu a poskytovatelé těchto služeb dodávají určitou úroveň zabezpečení. Problémem je však transparentnost, nikdo přesně neví, na kolik je cloudová služba, kterou zrovna využívá, bezpečná. V některých zemích zákon poskytovatelům ukládá povinnost jednou ročně projít bezpečnostním auditem, jenže to je v konečném důsledku jako letět v letadle s jedním křídlem. V McAfee máme program zvaný Cloud Secure, prostřednictvím kterého poskytujeme scamming scanning poskytovatelů cloudových služeb a webových stránek na denní bázi. Pokud testem projdou, získávají certifikaci.

CIO BusinessWorld: Dalším z velkých trendů dneška je mobilita, kde si dominantní postavení buduje operační systém Android, který svou oblibu z velké části vybudoval na volnosti pro tvůrce aplikací i jejich "konzumenty". Ten je však zároveň nechvalně proslulý tím, že se v důsledku oné volnosti do jeho app-store dostává i software, který v sobě obsahuje škodlivé kódy. Kdy přijde "ten správný" okamžik, kdy se tvůrcům virů začne vyplácet psát škodlivé kódy pro tuto platformu jako na běžícím pásu, podobně jako se tomu stalo u PC (Windows)? Jaké to může mít důsledky na celou platformu?

Jon Parkes: Je důležité si uvědomit, že tento stav právě nastává, ne sice ve stejném objemu jako u Windows, ale i tak množství malwaru pro Android roste neuvěřitelně rychle. Proto McAfee poskytuje antivirus také pro tuto mobilní platformu. Vyvážení otevřenosti platformy a schopnosti zabezpečení zařízení je velkou výzvou. K mobilitě přistupujeme jako k jedné ze strategických oblastí a rozvíjíme v ní naše portfolio ruku v ruce s Intelem. Aktuálně se na trhu pohybuje kolem miliardy aktivních mobilních zařízení, v roce 2018 jich bude 50 miliard. Nelze však

zapomínat ani na diskrétní zařízení jako jsou chytré televizory, ale i automobily a všechny další zařízení využívající vestavěné systémy.

CIO BusinessWorld: Nedávné odhalení operace "Temná krysa" přineslo překvapující závěry o tom, kolik organizací může být dlouhodobě sledováno skupinou kyberzločinců, aniž by o tom cokoliv tušily. Jedná se podle vás o odкрытие pomyslné špičky ledovce a podobně rozsáhlé akce jsou tak spíše vzácností nebo jsou počítačové sítě již dokonale pod nadvládou kyberzločinců, o níž máme pouze mlhavé tušení?

Jon Parkes: Pravdivá je skutečně první druhá verze – odhalili jsme pouze nepatrný kousíček obrovského problému. Celosvětový nárůst malwaru je neuvěřitelný, přičemž 60 % z těchto hrozeb je zcela nových. Podstatně hrozivější statistikou pro korporace jsou však APT (advanced persistence threats) jako právě operace „Temná krysa“. Někdo se na vás zaměří a využívá celou řadu cest od sociálního inženýrství až po různé přímé IT útoky, aby se dostal do vaší organizace. Jste tedy sledovaní, špehovaní a lidé, kteří pronikli do vaší organizace, dlouhodobě přidávají další backdoory, sbírají informace, a vyčkávají na strategický okamžik, kdy se dostanou k vysoce důležitým materiálům, které mohou zpeněžit.

Temná krysa byla pouze tenoučkým kouskem toho, co jsme dokázali odhalit, po celém světě bude celá řada dalších instancí, o kterých vůbec společnosti nevědí.

Další pokračování tohoto rozhovoru vedl Jan Mazal ze sesterského serveru ChannelWorld:

<http://channelworld.cz/clanky/rozhovor-kompetencni-centrum-comguardu-a-mcafee-ma-firmam-otevrit-oci-4943>

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.
