



Zabezpečení malých a středních společností

Jaroslav Mareček

Může zvyšování úrovně zabezpečení jít ruku v ruce se snižováním nákladů? Naštěstí ano. Rozumní výrobci umí nabídnout řešení, která zprostředkovávají sofistikované technologie vyvinuté pro ty největší nadnárodní organizace o několika tisících uživatelů i malým a středním firmám, viděno optikou našeho regionu. Respektují přitom i hledisko nákladové, a to nejen z pohledu vynaložených finančních prostředků po dobu životnosti zařízení, ale také z hlediska lidských zdrojů, kam můžeme započítat jak čas administrátorů, tak také nároky na uživatele samotné. Následující řádky jsou věnovány popisu zabezpečení, které respektuje požadavky na ochranu stále narůstajících a cennějších informačních aktiv i racionalizaci a efektivitu z pohledu vynaložených zdrojů.

Přestože 99 procent organizací nebude bezpečnost stavět na zelené louce, je dobré čas od času inventarizovat, co vlastně z pohledu elektronických-informačních aktiv máme, co z toho a proti čemu chceme chránit a na jaké úrovni. Z takové rizikové analýzy se může snadno stát projekt obřích rozměrů, nicméně nelze než doporučit střízlivý přístup, který bude rezonovat s flexibilitou menších subjektů. Vycházejme z toho, že v tuto chvíli firma nepotřebuje certifikovaný ISMS (integrováný systém řízení bezpečnosti) dle ISO 27001 a že veškeré IT v rámci organizace je spravováno několika málo administrátory, nebo dokonce administrátorem outsourcovaným. Jakmile proběhne analýza rizik, kterou může reprezentovat kvalifikovaná úvaha zainteresovaných osob, máme solidní základ k tomu, abychom k budování bezpečnosti přistupovali efektivně. Výsledkem analýzy by totiž nemělo být pouhé odhalení hrozeb, ale zejména finanční vyčíslení možných dopadů, což vede ke snadnější orientaci a porozumění

výsledkům ze strany majitele/jednatele či ředitele. Jasně z takové analýzy vyplývá, kolik stojí ztráta, nedostupnost či narušení integrity daného informačního aktiva (ocení ztráty databáze ERP, nedostupnosti e-shopu atp.). Odtud je už jen jeden krok k tomu, abychom věděli, jaké investice do bezpečnosti IT jsou skutečně potřebné a zároveň adekvátní (analogie s klasickým pojištěním není náhodná).

Obvykle se nevyhneme investicím do zabezpečení uživatelů a jejich pracovních stanic ani do ochrany sítě jako takové. Z pohledu síťové bezpečnosti je klíčovým bodem ochrana vstupu do sítě. Na této pozici jsme byli zvyklí vidat linuxová open source řešení nebo bezpečnost integrovanou na modemu či routeru. Doba se změnila a s ní i hrozby, které jsou mnohem sofistikovanější. Většina útoků je vedena na aplikační úrovni a jsou vyvíjeny tak, aby na sebe pokud možno vůbec neupozorňovaly. Rovněž správa linuxu jako firewallu je čím dál náročnější, a tak je dnes efektivnější poohlédnout se po komerčním

řešení, které toho bude „dělat spoustu za nás“ a v neposlední řadě bude vždy rychleji reagovat na nové typy útoků a hrozeb.

Stále nejnásazovanějším konceptem v prostředí malých a středních organizací je UTM, čili konsolidace všech relevantních bezpečnostních nástrojů na jedné hardwarové platformě se zabezpečeným operačním systémem. Obvykle obsahuje firewall, anti-virus, antispam, IPS, URL filtraci, řízení šířky pásma a VPN bránu pro přístup mobilních uživatelů do LAN, nejlépe na bázi SSL VPN pro maximální komfort uživatelů. Pokud budeme dbát na skutečnou efektivitu a návratnost investice, je vhodné vybírat z řešení, která v sobě mají kromě výše uvedených funkcí integrován i nástroj pro reportování a analýzu provozu v reálném čase, což šetří administrátorům spoustu času při zvládání incidentů. Rovněž zajímavou vlastností vedoucí k úsporám je řízení provozu na základě identity uživatelů, kdy na základě synchronizace s adresářovou strukturou (například MS AD nebo vytvořenou na zařízení) řídíme přístup uživatelů dle jejich jmen či skupin (a nikoliv jen dle IP) ke službám internetu. Uživatel je transparentně autentizován proti UTM a dle jeho identity je mu přidělena politika pro užívání internetu (obr. 1). Příkladem takového řešení je bezpečnostní brána (UTM) Cyberoam.

Mnoho organizací bude upřednostňovat nejen pořízení efektivních nástrojů, ale také ochranu a využití stávajících investic. Pokud například v síti již nějaký firewall funguje, může být z hlediska pokrytí aktuálních hrozeb šířících se zejména přes web a e-mail vhodné dokoupení specializované brány filtrující právě tyto druhy provozu.

Produktem šitým na míru menším organizacím v řádu desítek až stovek uživatelů je integrovaná McAfee Web a Email Security Appliance. Toto bezpečnostní zařízení je zaměřeno na likvidaci všech druhů škodlivých kódů (malwaru), a to od klasických virů přes trojany, dialery, adwary, spywary až po rootkity. Dalším funkčním modulem je URL filtrace McAfee Smartfilter, která staví na propracované kategorizované databázi webových stránek a zároveň na globálním reputačním systému TrustedSource.org. Díky URL filtraci je možné řešit nejen problémy s neproduktivním využíváním internetu uživateli, ale lze jej využít k zamezení plýtvání šířkou pásma připojení, a co je nejdůležitější, jako preventivní nástroj infiltrace škodlivých kódů, které se samovolně infiltují do sítě při návštěvě infikovaných webů. Zařízení by nebylo komplexní bez kvalitního antispamového řešení, jelikož spam je evergreenem mezi internetovými hrozbami.

McAfee Web a Email Security Appliance je zajímavá nejen z pohledu uceleného souboru bezpečnostních nástrojů, ale také z pohledu efektivity a návratnosti investice. Přední světový výrobce u tohoto řešení vsadil

především na nízkou cenu a maximální usnadnění nasazení a správy. Zařízení nevyžaduje změnu konfigurace sítě díky bridge módu a existuje i v softwarové verzi pro VMware prostředí. Z hlediska konfigurace politik a nastavení klade minimální nároky na administraci (zapoj, nastav a zapomeň), což je navíc podpořeno karanténou přístupnou přímo uživatelům.

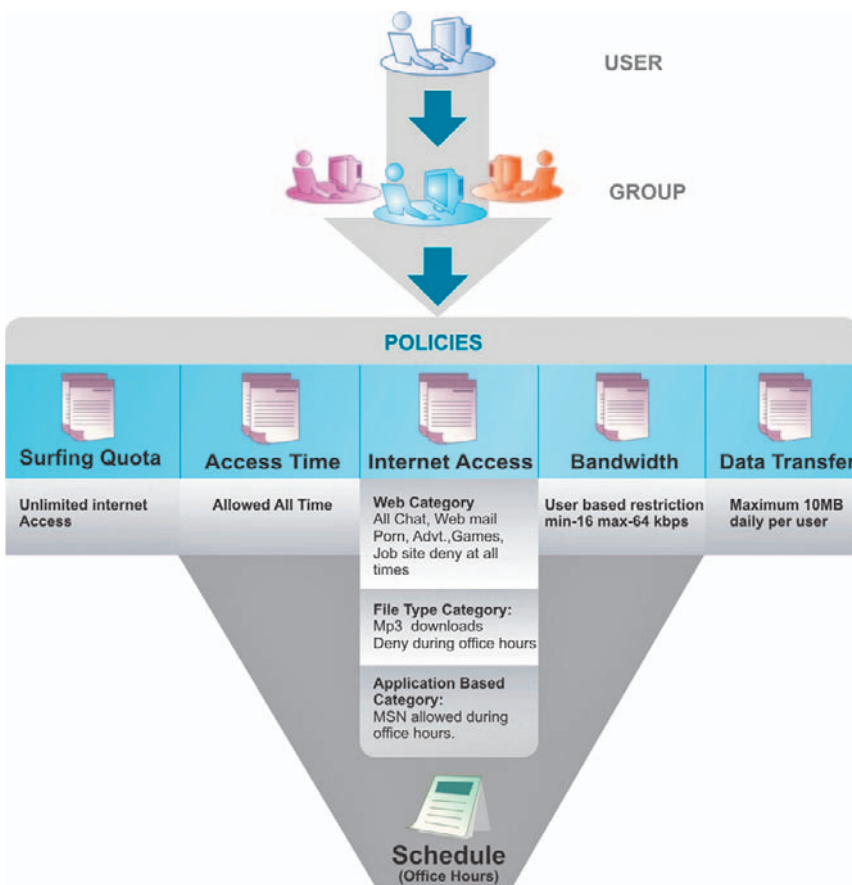
Samotnou kapitolou je centrální management systém McAfee ePolicy Orchestrator (ePo), který je vyvíjen jako univerzální nástroj pro správu všech McAfee produktů. Slouží nejenom jako prodloužená ruka administrátora při nasazení a konfiguraci výkonných systémů, ale také jako nástroj vynucení centrálních bezpečnostních politik a monitorovací nástroj v jednom. Navíc dokáže hlídat připojování systémů do sítě a odhalit tak nelegitimní připojení cizích notebooků apod. Firmy, kde je funkce IT administrátorů outsourcována, ocení nabídku SaaS (Security as a Service). McAfee nabízí poskytnutí serverů vzdálené správy jako službu dostupnou přes webové rozhraní. Hlavním přínosem, mimo to, že malá organizace nemusí instalovat centrální správu, je i možnost pro outsourcovaného správce

přistoupit k webovému rozhraní odkudkoliv. Nemusí tak kvůli řešení problému cestovat do firmy a může pružněji reagovat.

McAfee ePolicy Orchestrator je velmi dobře uplatnitelný také při ochraně uživatelských stanic, kde řídí komplexní soubor produktů pod názvem McAfee Total Protection for Endpoint. Tento ucelený systém nové generace potřebný zejména pro mobilní uživatele s notebooky kombinuje několik stupňů detekce narušení, od rozpoznání známých útoků na základě automaticky aktualizovaných signatur přes pravidla chování pro detekci neznámých útoků (včetně DoS útoků, anomálií provozu a zero-day attack ochrany), s možnostmi desktop firewallů. Doplnit lze dále o šifrování celých disků, souborů a adresářů nebo šifrované USB tokeny (McAfee Encrypted USB) centrálně spravované přes ePo.

Chápeme-li investice do pořízení a provozu bezpečnostních systémů jako jistou analogii k pojištění rizik spojených se ztrátou, nedostupností a narušením integrity aktiv, a to zejména informací, nesmíme přitom zapomenout na uživatele. Ten pravděpodobně nikdy nepřestane být tím největším rizikem, ať už se jedná o neúmyslné chyby při zadávání dat do systému, či záměr vynést citlivá data mimo hranice společnosti. Eliminace těchto rizik je oříškem pro velké korporace a instituce, jelikož jsou technologicky i finančně poměrně náročná. Nic ale nebrání firmě jakékoli velikosti posílat e-maily obsahující důvěrné informace šifrované, chránit projektové dokumenty uložené na sdílených úložištích tak, aby byly čitelné pouze legitimním uživatelům, a mít zašifrovaný notebook pro případ krádeže či ztráty. Pokud hledáte produkt, který tyto problémy umí řešit efektivně z jednoho místa, je možné doporučit systém od společnosti PGP.

Obr. 1: Řízení přístupu uživatelů k internetu na základě jejich identity



Autor působí jako product specialist ve společnosti Comguard.