

Centrální správa bezpečnostních produktů

ROBERT ŠEFR

Bezpečnostní produkty jsou ideálním příkladem nutnosti nasazení centrální správy. Tradičně jsou nasazeny napříč celou organizací, na různých strojích a pro odlišné skupiny uživatelů. Kvalitní centrální správa musí sledovat celý životní cyklus klientské aplikace – od nasazení, přes úpravu politik a instalace aktualizací až po případné odebrání aplikace.

Většinou není třeba udržovat duplicitní databázi strojů a uživatelů, která je již spravována existující adresářovou službou. Každá centrální správa ale vyžaduje školení administrátorů, liší se v technickém zpracování, používá jiné postupy pro instalaci a vynucování politik nebo vyžaduje vlastní databázový stroj pro ukládání dat. Větší počet produktů a jejich centrálních správ tak dospěje do stadia, kdy je nejjednodušší mít jednotnou centrální správu, která zaštití všechny ostatní.

Cestu jednotné centrální správy pro všechny produkty vyznává společnost McAfee produktem ePolicy Orchestrator (ePO), jenž se instaluje jako serverová aplikace na Windows Server a vyžaduje pro svou práci MS SQL Server (2005 nebo 2008, lze nainstalovat i na Express Edition). Využitím služeb Windows Cluster Service lze instalovat ePO na více serverů pro zvýšení dostupnosti a rozložení zátěže. Propojení se službou LDAP umožňuje synchronizovat stroje pro správu (včetně dělení do organizačních jednotek), podporuje autentizaci administrátorů ePO vůči LDAP. Přístup k ePO je přes webové rozhraní, které je založeno na Ajaxu a uživatelské rozhraní tedy zahrnuje i funkce jako drag-and-drop nebo interaktivní formuláře.

Prvním krokem pro správu stroje je instalace McAfee agenta, což je miniaturní program, který se stará o komunikaci s ePO, instalaci softwaru, aktualizace, vynucování politik a odesílání událostí. Instalace agenta na koncové stroje přímo pomocí ePO lze za předpokladu, že má administrátor dostatečná oprávnění v Active Directory. Jakmile je agent na stanici nainstalovaný, je stroj ve správě ePO a následující přidávání nebo

odebrání softwaru již probíhá přes něj (tedy přes oprávnění v ePO a ne v Active Directory). Spravované stroje jsou ukládány do stromové struktury. Na jednotlivé větve lze aplikovat odlišné politiky, instalovat na ně odlišný software a přiřazovat různé správce. Tímto způsobem se dají odělit např. servery a klientské počítače nebo jednotlivé pobočky a oddělení.

ePo je aktuálně ve verzi 4.5 a právě od verze 4.0 je uživatelské rozhraní čistě webové, dříve správa probíhala pomocí klientské aplikace. Verze 4.5 nemění logiku správy, ale nabízí několik nových funkcí a podporu dalších protokolů. Nově je k dispozici tzv. Agent Handler, který může suplovat funkce ePO pro vybrané agenty. Pomocí jednoho Agent Handleru tak můžete obsluhovat pobočku nebo celé oddělení, aniž by všechny stanice musely nezávisle na sobě přistupovat přímo do ePO. Agent Handler jim zprostředkovává aktualizace dat a politik výměnou za souhrn událostí, které se staly od poslední komunikace.

Jednou z dalších novinek je úprava komunikace mezi agentem a serverem, která je od verze 4.5 šifrována pomocí TLS a již je plně podporován i protokol IPv6. V možnostech centrální správy jsou dvě nové sekce – Automatic Responses a Policy Assignment Rules. Automatic Responses spouští předdefinované akce, pokud nastanou podmínky definované logickým výrokem. Pro definici logického výroku je k dispozici množství proměnných a událostí, se kterými ePO pracuje. Jako následná akce může být zvolena některá z naplánovaných úloh, vytvoření

tiketů, zaslání e-mailu nebo SNMP trapu. Policy Assignment Rules provazují politiky se skupinami a uživateli z Active Directory. To lze využít např. při filtrování webového obsahu (např. zakázat vybrané skupině sociální sítě) nebo šifrování dat (např. zpřístupnit vedení šifrovací klíče ke strategickým dokumentům).

Které bezpečnostní nástroje McAfee se pomocí ePO dají spravovat? Samozřejmě je antivirus VirusScan Enterprise a firewall s integrovaným IPS – Host Intrusion Prevention System. Další nástroje jsou zaměřeny na ochranu dat – Host Data Loss Prevention monitoruje pohyb citlivých dat po společnosti a hlídá odchozí vektory. Endpoint Encryption šifruje transparentně buď celé oddíly disku, nebo jednotlivé soubory a složky. Spravovat lze i šifrované USB disky (flash nebo klasické) Encrypted USB. Další sada produktů se soustředí na integritu dat, konfigurací



a spuštěných aplikací za pomoci tří produktů z oblasti Risk & Compliance. Integrity Monitor a Change Control se soustředí na audit a autorizaci při změně dat (na souborovém systému nebo v databázích) a konfigurací. Application Control uzamkne softwarové vybavení stroje a blokuje neautorizované procesy. Efektivně tak blokuje nežádoucí software, aniž by se musel zabývat signaturami jako např. antivír.

ePolicy Orchestrator je koncipován jako centrální bod správy bezpečnostního softwaru McAfee a díky jeho návrhu je možné jej využívat ve společnostech nejrůznějších velikostí a struktury. Stromová struktura zařízení a na ní navázané delegování oprávnění dalším administrátorům, dělení politik, distribuce bezpečnostního softwaru a vytváření reportů umožňuje vytvořit prostředí virtuální správy, které odpovídá reálné struktuře a procesům ve společnosti.

Mgr. Robert Šefr je IT Security konzultant společnosti COMGUARD