

jednotnou správu, která nám má naši bezpečnostní politiku snadno nasadit a vynutit. U správy se musí do hledáčku také dostat možnost stanovení rolí a oprávnění v celém systému a mimo jiné zajištění nepopiratelnosti jednotlivých kroků. S tímto hlediskem musíme hledat systém s detailním reportingem, který dá kompletní přehled o všech důležitých událostech jak vlastního systému, tak uživatelských akcí. Z praktického důvodu je výhodou, když správa je prováděna pomocí webového rozhraní.

Kvalitní bezpečnostní řešení by mělo podporovat velké množství autentizačních zařízení (tokeny, SmartCards), pochopitelně s pravidelnou aktualizací a přidáváním nových. Klíče jsou na těchto zařízeních uloženy výrazně bezpečněji než při pouhém uložení na disk a zašifrování heslem. Zabezpečení by mělo být provázáno s operačním systémem, tak aby při zašifrování celého disku uživatel zadával heslo pouze při pre-boot autentizaci, o přihlášení do Windows se již může postarat samotné bezpečnostní řešení. Podobně při práci se šifrováním složek a e-mailů by mělo být možné klíče cachovat na stanovenou dobu, aby se uživatel nemusel autentizovat při každé operaci. Šifrování souborů a složek (i na sdílených úložištích) je pro organizace velmi důležité, lze sice definovat přístupová práva, ale ta nejsou zdaleka dokonalá. K datům se mohou dostat administrátoři, práva mohou být špatně nastavena, nahrána do špatného úložiště atd. Se zašifrovanými daty k takovým situacím dojít nemůže.

Při šifrování e-mailové komunikace existuje řada problémů – zejména distribuce důvěryhodných veřejných klíčů. Je zcela jasné, že aby bylo řešení úspěšné, musí být maximálně transparentní pro uživatele, ale ne na úkor bezpečnosti. Kromě manuálního přidání klíče by tak měly být k dispozici i další způsoby – například získání z bezpečnostního serveru na doméně adresáta nebo z centrálního bezpečnostního serveru. Samozřejmě by měla být centrální správa zařízení, politik, uživatelů, klíčů a logů. Nároky šifrování pro jednotlivce jsou velmi odlišné od nároků šifrování pro organizaci. Organizace chce ochránit svá data, ale zároveň nad nimi nesmí ztratit kontrolu, a to ani v případě, že zaměstnanec nechce nebo nemůže spolupracovat na jejich dešifrování nebo při poruše hardwaru. Možným řešením je vytvoření tzv. additional decryption key, který může být použit k dešifrování dat (dat zašifrovaných po jeho vytvoření).

Je už na zvážení každého z vás, které řešení finálně vyberete. Pokud se podíváme na dostupné možnosti na trhu, jednoznačně podle našeho názoru vyniká řešení společnosti PGP Corporation, které zahrnuje všechny uvedené možnosti, a může tak být vzorem. Zajímejte se o podporu výrobce a nezapomeňte na kompatibilitu se standardy, a tím možnost komunikace s partnery.

Michal Mezera, Senior Security Consultant, COMGUARD.

10 0233/luc ■

INZERCE





Snižte své provozní náklady cíleným řízením údržby strojů a zařízení

QAD Řízení údržby vám poskytne komfortní sledování a řízení nákladů v oblastech údržby, náhradních dílů a řízení projektů.

Výrobní společnosti na svých strojích:

- zvýší produktivitu
- sníží čas odstávek
- sníží počet oprav a nákupů
- využijí lépe času servisního týmu
- prodlouží životnost zařízení



QAD
Our Passion. Your Advantage.

Informujte se, jak snížit své provozní náklady na marketing@minerva-is.cz nebo na tel. 386 351 870.