

# RSA Data Loss Prevention

ochrana citlivých informací v úložištích, v síti i na stanicích

- „Komerční pojišťovna musí podle rozhodnutí Nejvyššího správního soudu zaplatit pokutu tři milióny korun za únik informací o klientech, kterou ji vyměřil Úřad pro ochranu osobních údajů...“
- „Jeden z pracovníků společnosti Panasonic z Borských Polí získal databázi zaměstnanců, která obsahovala jména, rodná čísla, adresy, a také výdělky jednotlivých zaměstnanců. Databázi poslal Plzeňskému deníku...“
- „Česká pojišťovna vyšetřuje podezření, že informace o svých klientech skončily v brněnském bazaru s počítačovou technikou...“



Úniky citlivých dat jsou dnes podle mnoha studií (např. Trend Micro) druhým nejpalčivějším problémem a hrozbou pro firmy i státní instituce. Jedná se dokonce o větší hrozbu, než kterou je spam, spyware, phishing a Trojské koně. Přesto má jen necelá polovina firem a institucí pravidla, která by je, alespoň teoreticky, měla před únikem citlivých dat ochránit. Nicméně jak se v Čechách často říká, pravidla jsou od toho, aby se obcházel. A tak to také mnoho zaměstnanců, ať už vědomě či nevědomě, činí. Citlivá data pak putují volně po elektronickém světě a jejich původním majitelům způsobují nemalé problémy – viz citáty v perexu.

Z logiky věci je zřejmé, že nastavením firemních pravidel pro práci s citlivými informacemi jejich úniky nezastavíme. Pravidla sa-

ma o sobě pouze sdělují, jakým způsobem se má s daty nakládat, ale nejsou schopna zajistit jejich dodržování. K tomu tedy potřebujeme něco víc – správnou technologii. Takovou technologii, která dokáže rychle analyzovat dokument, s maximální přesností určit úroveň jeho citlivosti a následně zajistit, aby s ním uživatel zacházel pouze v rámci vymezených pravidel.

Abychom však byli schopni zamezit únikům citlivých dat, musíme si nejdříve velmi dobře pohlídat, kde všude máme taková data uložena. Jedním z nejrozšířenějších mýtů v IT je totiž představa, že firmy vědí, kde mají uloženy citlivé dokumenty. Samozřejmě, že to firmy nevědí, ony si jen myslí, že to vědí. Jaké je pak zděšení bezpečnostních a IT ředitelů, když zjistí, že seznamy jejich zákazníků s osobními údaji či popis připravovaného

produktového balíčku se jen tak „válí“ na firmním FTP serveru s anonymním přihlášením, na noteboocích, v soukromých e-mailových schránkách zaměstnanců na Gmailu, nebo na CD-R či USB discích.

Ještě před tím, než jsme schopni lokalizovat všechny naše citlivé dokumenty, musíme si definovat, co to z pohledu dané firmy či instituce vlastně citlivý dokument je. Pro někoho jsou to seznamy čísel kreditních karet, pro jiného výrobní proces či lékařské zprávy. Každá firma a instituce tak má mnoho typů dokumentů, které se z pohledu jejího podnikání či zaměření musí považovat za citlivé a chránit je.

Společnost RSA se od svého založení věnuje informační bezpečnosti. Je známa svými produkty pro řízení přístupu, pro šifrování dat, pro analýzu bezpečnostních událostí v IS, a dnes již také svým řešením pro zamezení úniku informací. Toto řešení se nazývá RSA Data Loss Prevention Suite (RSA DLP) a na velmi profesionální úrovni řeší právě výše popsany problém.

RSA DLP Suite je, jak už plyne z názvu, integrovanou sadu produktů nabízejících proaktivní přístup k ochraně citlivých dokumentů na třech základních vrstvách – v datovém centru (disková pole, databáze, file-shares, atd.), v síťovém provozu (zasílání na web

přes http či FTP protokoly, odesílání e-mailem, atd.) a v neposlední řadě na koncových stanicích (kopírování, tisk, vypalování na CD, atd.) Tato funkčnost je zajištěna třemi moduly – RSA DLP Datacenter, RSA DLP Network a RSA DLP Endpoint. Pro správu politik, tedy toho, jak systém pozná citlivý dokument a jak se s ním smí zacházet, je v sadě ještě modul RSA DLP Enterprise Manager.

Proces implementace řešení DLP je takový, že se v první fázi vytvoří pravidla zabezpečení informací a pomocí velmi přesných vyhledávacích a klasifikačních technologií se identifikují citlivá data přímo tam, kde jsou fyzicky uložena. Jakmile jsou data identifikována, moduly RSA DLP zajistí jejich ochranu, opět v závislosti na definovaných politikách. Propracovaný systém procesů, notifikací, auditu a reportingu pak umožňuje rychlou identifikaci pokusu o porušení bezpečnostních pravidel a politik, které jsou základní příčinou úniku dat mimo firmu. Mechanismy v rámci sady RSA DLP jsou dostatečně flexibilní pro zajištění konkrétních potřeb různých oddělení a jejich pohledů na citlivé dokumenty.

U DLP systémů jsou obecně nejdůležitějšími vlastnostmi rychlost a přesnost analýzy dokumentů. Nikdo nebude chtít čekat týdny, než mu systém bude schopen analyzovat

několik terabajtů dat, stejně jako nikdo nebude chtít, aby byl každý druhý nevinný e-mail zachycen jen proto, že obsahuje číslo kreditní karty odesílatele. A toto jsou přesně důvody, proč zákazníci při výběru produktů pro ochranu citlivých dat stále více sázejí na řešení společnosti RSA Data Loss Prevention Suite. Toto řešení je také dnes jako jediné integrováno s řešením Microsoft Active Directory Rights Management Services (MS AD RMS). To v kombinaci s RSA DLP plně automatizuje procesy řízení přístupu k dokumentům podle jejich citlivosti.

Více informací naleznete na [www.rsa.com](http://www.rsa.com)