



# Systemy DLP se stávají nezbytností pro ochranu duševního vlastnictví firem

Pavel Hanko

Jedním z výrazných trendů posledních let je přechod od izolovaných bezpečnostních produktů ke komplexním řešením. Příčiny tohoto jevu jsou vcelku zřejmé, na jednu stranu rovněž tak často komplexní povaha dnešních hrozeb, na druhé straně pak snaha ušetřit – především náklady na správu mnoha různých IT systémů používaných paralelně vedle sebe. Jeden z moderních přístupů k ucelenému zajištění bezpečnosti IT se označuje jako DLP (data loss prevention, prevence ztráty/úniku dat). Nejde však jen o to, že DLP řeší zabezpečení komplexně, ale i o zásadnější změnu celého přístupu: důraz na celý životní cyklus dat.

## Trocha historie

První viry a další škodlivé kódy mohly data nanejvýš smazat nebo modifikovat. Počítače, které nebyly propojené, nebo byly propojené pouze v rámci firemní sítě, únik dat víceméně neohrožoval. Průmyslová špionáž samozřejmě existovala už tehdy (a i dávno před samotnými počítači), bylo ji však třeba realizovat jinak. Bezpečnost IT zajišťovala především antivirová ochrana.

V době internetu se situace změnila. Hlavními nástroji ochrany zůstaly antiviry, přidal se však firewall, který chránil ne už jednotlivé počítače, ale rozhraní mezi

vnitřní sítí a internetem. I u obousměrných firewallů se ale předpokládalo, že jejich hlavním úkolem je bránit útočníkům v průniku do vnitřní sítě, ne naopak blokovat přenos informací ven.

Tyto nástroje samozřejmě neztratily svůj význam, jenže (a pochopitelně) odpovídaly technologiím své doby. Postupně se začalo ukazovat, že to, co je třeba chránit, nejsou ani tak počítače nebo sítě, ale informace.

## Role duševního bohatství

Data představují hlavní aktivum řady firem, ať už jde o databáze zákazníků,

marketingové plány, finanční výsledky, technické dokumentace výrobní linky, specifikace produktů nebo zdrojové kódy softwaru. V některých případech si ani samotné firmy nejsou přesně vědomy, jaké informace (respektive jejich důvěrnost) jsou základem jejich úspěchu. Zdaleka se nemusí jednat o „velká“ tajemství typu receptury na Coca Colu. U většiny firem již dnes jejich nehmotná aktiva výrazně převažují cenu „fyzického“ majetku.

Současní počítačové podvodníci fungují především pro peníze. Nic moc jim nepřinese, pokud do firemní sítě vpašují destruktivní malware (jistěže i takové ekonomické modely kriminálních skupin mohou existovat, třeba spojené s následným vydíráním, „aby se to už neopakovalo“, nebo taková akce může být i motivována politickým hacktivismem, jehož cílem je prostě nějakou instituci poškodit bez nároku na finanční prospěch původců útoku). Nepotřebují citlivé soubory smazat, ale zmocnit se jich a dále je na černém trhu prodávat dalším subjektům. Totéž platí i z pohledu serverů a služeb: útok DDoS, který vyřadí z provozu firemní server, je jistě nepřijemný, ale

sám o sobě útočníkům k ničemu, pokud se současně nedostanou k citlivým informacím. Hlavním plátdlem internetového podzemí jsou dnes spíše firemní data než třeba čísla platebních karet nebo hesla k účtům Facebooku, i když i zde bychom měli být ve střehu.

Z druhé strany pak přibývá úniků dat, které způsobují samotní legitimní uživatelé v rámci firmy, ať už nedopatřením, nebo úmyslně. Za mnohými krádežemi dat stojí insideri (lze spekulovat, zda na tomto vzestupu neměla nějaký podíl ekonomická krize), jenže do hry vstupují i další technologické trendy. Data se různě sdílí, masově se rozšířila externí paměťová média a disky, uživatelé často pracují nikoliv na desktopech, ale na noteboocích, které si nosí domů. Přibývají smartphony, tablety a další podobná zařízení. Lidé se z domova mnohdy připojují do firemní sítě nezabezpečeným způsobem, k vyřizování pracovních záležitostí používají webové e-maily, své soukromé smartphony používají k práci s podnikovými daty a naopak firemní notebooky s nimi sdílejí jejich rodinní příslušníci. Rozhraní mezi firmou a vnějším světem je celá řada – existuje mnoho druhů koncových bodů.

### Osobní data vs. duševní vlastnictví

Hlavním cílem útočníků už nejsou osobní data uživatelů, ale duševní bohatství firem. Pokud firmě uniknou čísla platebních karet klientů, je to ostuda – výsledkem bude negativní publicita a nutnost složitě dodržet legislativní požadavky, které tyto případy ošetřují. Firmy se proto pochopitelně snaží incidentům tohoto typu předcházet. Důležité je ale uvědomit si, že pro útočníky dnes má větší cenu duševní vlastnictví firmy, které je mnohdy chráněno naopak nedostatečně.

Zdroj: McAfee Underground Economy Report 2011

### Přesná definice povolených činností

Tento chaos je přirozeně zvládnutelný řadou způsobů, a to i když pomíneme maximální restriktce (jež naopak snižují produktivitu práce). Existují nástroje, které se přímo specializují na ochranu koncových bodů.

Je však důležité uvědomit si, že hlavní cenu dnes nemá zařízení, ale informace. Při ztrátě nebo krádeži firemních notebooků a smartphonů škody často mnohonásobně převyšují cenu samotného zařízení. Chránit je proto třeba hlavně data, bez ohledu na to, zda jsou právě v počítači, na médiu USB, někdo si

je tiskne, preposílá je domů e-mailem, přistupuje k nim bez patřičných oprávnění nebo se snaží tato oprávnění „povyšit“.

Ochrana má v ideálním případě podobu jednoduché rovnice: data plus uživatel rovná se povolená činnost. Data přitom nemusejí být jen soubory ve vlastním slova smyslu, ale třeba i položky v databázi nebo archivy e-mailů. Uživatel zase není nutně jeden konkrétní člověk, ale celá skupina, navíc i jediný člověk může pracovat s různými oprávněními (identity, role, ...), třeba podle toho, zda zrovna sedí v zaměstnání, nebo je na cestách.

Řešení DLP odpovídá právě na tyto požadavky. Slovo „prevence“ ve zkratce je důležité, protože mnohem nákladnější je řešit bezpečnostní incidenty než jim předcházet. Podobný proaktivní přístup ovšem deklarují i jiná řešení zabezpečení, u DLP je naopak klíčový důraz na ochranu informací. Systém DLP se neomezuje pouze na řízení přístupu, ale právě na množinu povolených činností – to, že někdo smí přečíst určitý dokument, například ještě neznamená, že ho může také poslat e-mailem nebo tisknout. Specifikace může být velmi podrobná, soubor lze třeba poslat firemním e-mailem, ale ne už webovým.

Firmy na celém světě jsou dnes vystaveny velkému množství pokročilých a cílených útoků typu APT (advanced persistent threat). Podle studie 2011 Threat Predictions společnosti McAfee jsou právě útoky APT jedním z trendů letošního roku. Tyto akce bývají dlouhodobé, nezaměřují se jen na nějaký konkrétní malware nebo softwarovou zranitelnost. Záplatování systémů a aplikací ani aktualizovaný antivir zde proto nepředstavují záruku bezpečí. Když k tomu připočteme, že útoky ATP bývají často spojeny i s akcemi insiderů nebo sociálním inženýrstvím, vychází jako prakticky jediná obrana proti nim právě řízení přístupu k informacím a kontrola nad tím, co se s nimi děje.

### DLP není izolovaný nástroj

Systémy DLP lze různě kombinovat s dalšími nástroji pro ochranu dat či duševního vlastnictví: například DRM (digital rights management – zdaleka přitom nejde jen o nástroje ztěžující kopírování hudby či filmů), ERM (enterprise rights management) a IRM (information rights management). Vymezení těchto kategorií je pochopitelné do značné míry věci každého dodavatele a svou funkcí se tyto systémy mnohdy podstatně překrývají.

V zásadě platí, že zatímco DLP slouží především pro ochranu informace směrem ven, před únikem z koncových bodů, ostatní

nástroje se snaží nad ní mít nějakou kontrolu i mimo samotné prostředí firmy (dokument, byť už se třeba nachází v partnerské firmě, například nepůjde dále preposílat, tisknout apod.). Všechny tyto nástroje mají ale společně sloužit ke vzájemnému přiřazení informací a uživatelů, z něhož vyplyne skupina dále povolených operací. Pokud software zjistí, že se uživatel pokouší o nějakou neoprávněnou činnost, operaci přeruší. Dále může upozornit například uživatele nebo správce a vytvořit příslušný záznam v auditovacím nebo log souboru (soubor protokolu). Obecně platí, že systémy DLP reportují pokusy o narušení dat, a jejich výstupy mohou proto sloužit také pro účely auditu, kdy dokazují soulad s firemními i dalšími předpisy.

A samozřejmě – DLP bývá propojeno i s dalšími systémy, ať už čistě technologickými (šifrování/správa klíčů) nebo zaměřenými na obchodní aspekty (řízení rizik – risk and compliance, risk management, správa politik, ...).

Z kauzy WikiLeaks bychom rozhodně neměli získat dojem, že cílem zlodějí dat bývají výhradně armády, vlády nebo největší společnosti. Zloděje dat a další kybernetické podvodníky vysloveně lákají malé a střední společnosti, a to právě z důvodu, že mnohdy nemají dostatečně propracované vlastní zabezpečení. Počítačové kriminálníci je vnímají jako snadnější oběti. Právě malé a střední firmy by měly rozhodně uvažovat, zda, respektive jak do své bezpečnostní strategie začlenit systémy DLP.

### Jak vybírat

V zásadě lze doporučit, aby firma, která se rozhodne pro implementaci DLP, sáhla po osvědčeném dodavateli, s jehož produkty má již nějakou zkušenost. Samotná implementace dnes již není zdaleka tak složitá jako v minulosti, takže o nasazení DLP má smysl uvažovat i v rámci menších firem. Ty navíc mohou využívat nabídky systémů poskytovaných formou služby. Důležité je, aby dodavatel dokázal zajistit, že:

- před implementací je možné zásady DLP nějak otestovat, a nemuset pak bezpečnostní politiky nasazovat metodou pokusu a omylu,
- implementace nenaruší běžný provoz firmy,
- po dokončení implementace budou systémy DLP „průhledné“ z hlediska dalších firemních systémů, ať už jde o CRM, ERP nebo ekonomický software. ■