

Počítačovní zločinci

přestávají mít zájem o soukromá data,

zaměřují se na duševní vlastnictví firem

Pavel Hanko



Zatímco v několika posledních letech se hlavním terčem útoků počítačových zločinců stávaly citlivé informace soukromých osob, jako jsou data k bankovním účtům či údaje ke kreditním kartám, v současnosti se jejich zájem přesouvá do podnikové sféry. Předmětem jejich zájmu se stává duševní vlastnictví firem, především nejznámějších celosvětově působících korporací. V ohrožení jsou ale i menší či středně velké firmy, které by neměly usnout na vavřínech.

Podle celosvětové studie McAfee a Science Applications International Corporation „Underground Economies: Intellectual Capital and Sensitive Corporate Data Now the Latest Cybercrime Currency“ (Podsvětí ekonomiky: Duševní vlastnictví a citlivá firemní data se staly hlavním platidlem počítačových podvodníků) se podvodníci stále více zaměřují na obchodní tajemství, marketingové plány, výsledky výzkumu a vývoje nebo na zdrojové kódy softwaru. Takovým útokem byla například nedávná Operace Aurora, kdy se v rámci cíleného útoku hackeři pokusili ukrást intelektuální vlastnictví Google a dalších třiceti firem.

Duševní vlastnictví se stává napadnutelným v souvislosti se současným trendem konvergence podnikání a informačních technologií. Obchodní tajemství a citlivá data se nacházejí v databázích, které jsou často sdílené přes e-mail a internet. Intelektuální majetek společností přitom bývá velmi často nedostatečně chráněn a stává se tak snadnou kořistí kybernetického podsvětí. Protože se dají tyto údaje snadno zpeněžit, stávají

se v podstatě novým platidlem počítačového podsvětí.

Zločincům pomohla i krize

Nedostatečná péče o bezpečnost důvěrných firemních informací souvisí mimo jiné s nedávnou ekonomickou krizí, která firemní sektor přinutila hledat úspory právě v oblasti ukládání dat. Podniky tak například přehodnotily rizika spojená s ukládáním dat v zahraničí. Zatímco před dvěma lety plánovala zvýšit množství ukládaných dat v levnějších zahraničních destinacích pětina firem, nyní je to podle McAfee zhruba třetina organizací. Na vyspělých trzích v USA, Velké Británii, Číně a Japonsku vynakládají velké firmy na IT v průměru více než jeden milion dolarů denně, výdaje těchto firem na zabezpečení citlivých informací v zahraničí se pak pohybují okolo více než jednoho milionu dolarů týdně.

Které země tedy jsou z hlediska ukládání dat bezpečné? Nadnárodní firmy nejvíce věří úložištím ve Velké Británii, Německu a USA.

Tomu ale odpovídá i cena, kterou správci prostoru za ukládání informací požadují. Na opačném konci žebříčku důvěryhodnosti se pak nachází Čína, Rusko a Pákistán.

Firmy hodnocení bezpečnosti dat podceňují

Velké podniky včetně firem s celosvětovou působností se mnohdy nedostatečně věnují hodnocení a řízení rizik souvisejících se skladováním dat. Více než čtvrtina organizací posuzuje rizika hrozící jejich datům pouze dvakrát do roka, nebo ještě méně často. K ochraně svých dat podniky nejčastěji používají antivirové programy, firewally a systémy IDS/IPS. K těmto nástrojům se uchylují čtyři firmy z pěti. Pokud již k útoku



došlo, ven z firmy se informace o incidentu ve většině případů nedostane. O všech narušeních bezpečnosti dat informují jen zhruba tři firmy z deseti, naopak šest organizací z deseti si vybírá, jaké incidenty oznámí a jaké ne. Podniky zároveň hledají země, kde existuje mírnější legislativa z hlediska povinnosti informovat o únicích dat. Osm z deseti organizací, které uchovávají svá citlivá data v zahraničí, volí svou politiku podle povinnosti oznamovat narušení dat svým zákazníkům.

Nová zařízení, nové hrozby

Vedle sdílení dat na internetu se velkým problémem stává stále větší počet koncových zařízení, která zaměstnanci firem používají. Podniky stále častěji využívají chytré mobilní telefony nebo tablety, jako je iPad, iPhone a telefony se systémem Android. Zabezpečení mobilních zařízení v rámci firemní IT infrastruktury je i nadále bolavým místem většiny organizací a jako problém ho vnímá 62 procent podniků. Dalším slabým místem je využívání sociálních sítí z pracovních počítačů a dalších zařízení.

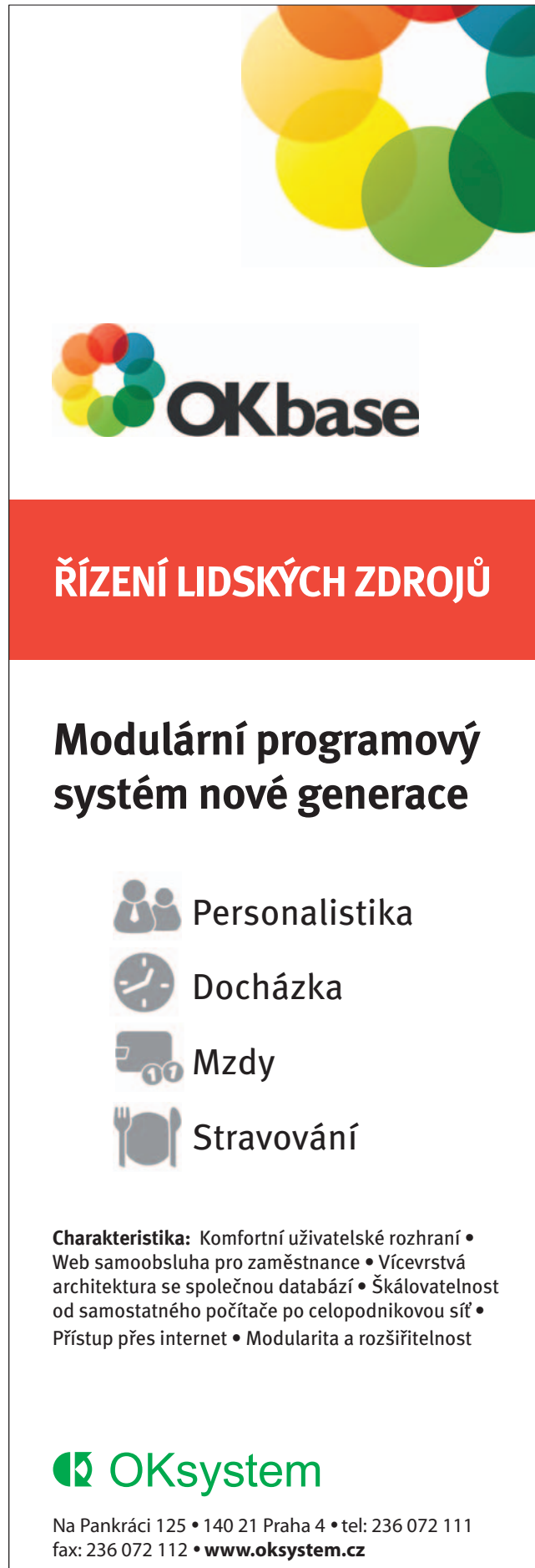
Krádeže duševního vlastnictví se stávají novým fenoménem, se kterým se korporátní sféra bude muset vyrovnat a účinně mu čelit. Podniky si budou muset uvědomit, jaká data na síti ukládají a jak je mají chráněna. Na druhé straně krádeže firemních dat vyžadují vyšší míru sofistikovanosti i od kybernetických podvodníků, než tomu bylo v případě krádeží identity či údajů ke kreditním kartám.

Jak na problematiku ochrany dat

Tyto problémy řeší systémy DLP (data loss prevention). Na rozdíl od jednoúčelových nástrojů zabezpečení (antivirus, firewall, aplikace blokuji škodlivé weby, ...) nabízejí kontrolu nad daty po celé období jejich životního cyklu. Monitorují data bez ohledu na to, kde se právě nacházejí, tj. i když jsou zrovna uložena například na notebooku mimo firemní síť. Lze v nich snadno nastavit, jaké operace lze s daty provádět, a jaké jsou naopak zakázány (příkladem takových operací může být třeba prohlížení souboru, jeho kopírování na USB flash disky, tisk, odesílání e-mailem, ...), firemní politiku práce s daty centrálně řídit a její dodržování také vynutit. Samozřejmostí je řízení přístupu k datům a přiřazení práv jednotlivým uživatelům. Na DLP lze navázat standardní podnikové procesy i další bezpečnostní technologie, například šifrování dat, řízení rizik (risk and compliance, risk management) nebo DRM (digital rights management – tyto systémy zdaleka neslouží jen jako ochrana proti kopírování hudby či filmů!). Systémy DLP reportují pokusy o narušení dat a jejich výstupy mohou sloužit také pro účely auditu, kdy dokazují soulad s firemními i dalšími předpisy. S jejich pomocí lze bezpečnostním incidentům proaktivně předcházet, a když už k nim přece jen dojde, lze na ně rychle a adekvátně zareagovat. ■

Autor působí jako territory channel manager společnosti McAfee.

Inzerce



ŘÍZENÍ LIDSKÝCH ZDROJŮ

Modulární programový systém nové generace

- Personalistika
- Docházka
- Mzdy
- Stravování

Charakteristika: Komfortní uživatelské rozhraní • Web samoobsluha pro zaměstnance • Vícevrstvá architektura se společnou databází • Škálovatelnost od samostatného počítače po celopodnikovou síť • Přístup přes internet • Modularita a rozšiřitelnost

OKsystem

Na Pankráci 125 • 140 21 Praha 4 • tel: 236 072 111
fax: 236 072 112 • www.oksystem.cz