Únik informací – nikoli hackeři, ale zaměstnanci

Author: SF / pb | Published: 02.12.2011

Z auditů několika set firem, které během posledních tří let realizoval již zmíněný ústav APOGEO Esteem, vyplývá, že úniky dat a informací nejčastěji způsobují zaměstnanci svojí nedbalostí (50 %), ztrátou datových nosičů (13 %) či krádeží (12 %). Teprve pak následují útoky hackerů (14 %). Mezi nejčastější nedbalostní důvody úniku či ztráty dat patří nedostatečné proškolení zaměstnanců či chybějící dokumentace, neaktualizované informační systémy a nesprávně nastavená přístupová oprávnění.

Třetina firem má problémy

„Paradoxem je, že čím více se firmy snaží chránit svá data zejména proti útokům zvenčí, tím větší hrozbu představují interní bezpečnostní rizika. Například citlivá účetní data lze snadno získat předstíranou rutinní kontrolou počítače v účetním oddělení," varuje Ivan Janoušek. Úniky citlivých informací mohou vést k poškození dobrého jména firmy, ztrátě konkurenčních výhod, ztrátě zákazníků či vést k sankcím za nedodržování uzavřených dohod. Podle odhadů expertů APOGEO Esteem se jen v loňském roce potýkalo s únikem citlivých informací přes 28 % českých firem.

Pravděpodobnost cílené krádeže firemních dat roste s citlivostí uchovávaných informací. Firmy, disponující velmi choulostivými daty, čelí v průměru šestinásobnému riziku jejich úniku než ty, které informace klasifikované jako „tajné" neuchovávají. „Nejčastěji se tento problém týká firem v bankovnictví a ve vyspělých technologických odvětvích, například v leteckém průmyslu, ve zbrojařství, v elektrotechnickém průmyslu nebo v poradenství," vyjmenovává Janoušek.

Bez ohledu na obor jsou nejžádanějšími a nejcennějšími daty informace, které se dají rychle zpeněžit nebo využít v konkurenčním boji. Největší hrozbu představují zaměstnanci, kteří hodlají z firmy odejít či jsou ve výpovědní lhůtě. Přitom ve finančním vyjádření je interní krádež dat desetkrát nákladnější, namísto statisíců jsou v sázce řádově miliony korun.

Bezpečnostní mýty

Experti v této souvislosti varují před „bezpečnostními mýty", kterým manažeři hlavně středních a menších společností často podléhají. „Jedním z nich je přesvědčení, že na ochranu dat stačí sofistikované bezpečnostní systémy. Ty jsou sice důležité, ale je třeba vyloučit i řadu interních slabin a dát je do

kontextu s pracovněprávní agendou firmy. Jedině tak je možné únikům zamezit, případně vymáhat úhradu škod způsobených porušením bezpečnostních pravidel," doporučuje J. Binder z APOGEO Esteem.

Zabránit neodpovědnému chování zaměstnanců, a tím i úniku, ztrátě či zneužití citlivých dat lze pouze zavedením pravidel, jejichž dodržování je nekompromisně vymáháno. „I ta nejlepší bezpečnostní pravidla jsou k ničemu, pokud zaměstnanec nechá ležet své heslo u počítače nebo si z domova přinese zavirované soubory na výměnném disku. Podle našich zkušeností například jen 23 % podniků aktivně kontroluje připojení výměnných médií," vyjmenovaná Ivan Janoušek.

Opačným extrémem je až příliš přísná kontrola zaměstnanců. Pokud má styl „velkého bratra", řadu lidí demotivuje a může být i v rozporu se zákony na ochranu osobních údajů. Typickým příkladem jsou nezákonný monitoring zaměstnanců, například prostřednictvím kamerových systémů. Ivan Janoušek k tomu dodává: „Firmy by proto měly svá bezpečnostní opatření sladit i s pracovněprávní agendou firmy, normami na ochranu informací a platnou legislativou."

Datová centra: kam s nimi?

S problematikou úniku citlivých informací z interních databází a počítačových systémů souvisí i rizika jejich „skladování". Narůstání objemů uschovávaných dat zákonitě vedlo ke vzniku datových center, koncentrace pro podnik významných informací na jednom místě zase ovšem zvyšuje rizika ztráty. Datová střediska – v případě velkých firem často dislokovaná v zahraničí – zajišťují chod kriticky důležitých IT systémů a jakýkoli jejich výpadek může způsobit milionové ztráty z titulu ušlých tržeb nebo i ohrozit samu existenci podniku.

Studii na téma rizik datových středisek nedávno zveřejnily společnosti Cushman & Wakefield a hurleypalmerflatt (poradenská společnost, specializující se na projektování systémů, jež mají kritickou důležitost pro podnikání firem, jako např. datová střediska, obchodní sály a centra řízení provozu). Studie Index rizik datových středisek (Data Centre Risk Index) vyhodnocuje rizika, jimž datová střediska čelí v dnešní globální době. Autoři přitom brali v potaz řadu faktorů, k nimž patří zejména náklady na energie, přenosová kapacita, podnikatelské prostředí, daně, kvalita pracovní síly, politická stabilita, četnost přírodních katastrof apod.

Na prvním místě takto sestaveného žebříčku se umístily USA, kde je riziko pro umístění datového střediska nejnižší zejména díky nízkým nákladům na energie a příznivému podnikatelskému prostředí. Na druhém místě následuje Kanada a na třetím Německo. V žebříčku dvaceti zemí, které jsou pro umístění datových center nejméně rizikové, se z evropských zemí umístily ještě Británie, Švédsko, Francie, Nizozemsko, Španělsko, Rusko, Polsko a Irsko. Česko „nezabodovalo".

Význam ochrany dat a počítačových sítí vůbec dokazují i údaje právě včera publikovaného materiálu poradenské společnosti PwC „Celosvětový průzkum hospodářské kriminality". Ten počítačovou kriminalitu označuje za relativně nový trend – v České republice zaujímá svou četností, respektive podílem na hospodářských trestných činech již čtvrtou pozici (13 %) za účetními podvody a korupcí (shodně 21 %). Tuzemské firmy si stále více uvědomují reálné nebezpečí, které přichází z virtuálního světa – téměř třetina dotázaných vnímá za uplynulý rok nárůst počítačové kriminality. Více než polovina (56 %) českých respondentů však zároveň uvedla, že jejich organizace nesleduje používání sociálních sítí, nebo si toho nejsou vědomi. „Toto číslo je poměrně překvapivé, neboť tyto stránky mohou představovat velké bezpečnostní riziko, pokud je zaměstnanec zneužije. Přestože sociální sítě jako Facebook či LinkedIn nemusí samy o sobě představovat skutečného původce počítačové kriminality, mohou sloužit jako velmi cenný zdroj pro počítačový zločin typu sociálního inženýrství a následné efektivní útoky, např. phishing," varuje Filip Volavka, odborník na počítačovou kriminalitu ze společnosti PwC Česká republika.

Foto: Armin Hanisch

02.12.2011 08:05, SF / pb