Základy ochrany citlivých dat

„Americké ministerstvo energetiky nařídilo přerušení utajovaných operací v řadě jaderných zařízení. Rozhodnutí je důsledkem zjištění možného úniku informací z Národní jaderné laboratoře v Los Alamos. Při inventuře bylo zjištěno, že chybějí dva počítačové disky s utajovanými materiály."

„Zloděj ukradl počítač z kanceláře místopředsedy Senátu Přemysla Sobotky. Přišel však o veškerou databázi za dobu šesti let, kdy je senátorem. Šlo o adresář, různé kontakty, publikované články a další texty."

„Senátor Luděk Sefzig přišel o počítač s důležitými daty, která se dají snadno zneužít. Neznámý zloděj se vloupal do jeho rokycanské kanceláře a odnesl si stolní počítač i monitor. Jeho kancelář za necelé čtyři roky, co je senátorem, vykradli už potřetí."

[Ze zpráv tiskových agentur, kráceno.]

Tři ilustrativní příklady z poslední doby názorně ilustrují jednu věc, kterou všichni tušíme, ale více či méně je ignorujeme: v oblasti informačních technologií jsou tím nejcennějším elektronická data. Věnujeme jejich ochraně odpovídající pozornost?

Výše uvedené příběhy ze života nám dávají jasnou odpověď: Nikoliv! Dávná pravda říká, že cenu něčeho poznáme zpravidla až v okamžiku, kdy o to přijdeme. Přitom existují jednoduchá opatření, která nám mohou pomoci ztrátě elektronických dat zabránit. Stačí si jen jejich cenu uvědomit – a jednat.

V případě fyzického zcizení nosičů s daty (k čemuž došlo ve třech uvedených případech) stojíme před dvěma úkoly. Jednak je to zajistit, aby se data nedostala do nepovolaných rukou, jednak aby byla i po incidentu k dispozici (náklady finanční i časové na jejich obnovu bývají značné).

Aby byla data stále k dispozici je nutné pravidelné zálohování a následné pečování o tyto zálohy (zálohování na druhý pevný disk postrádá v případě krádeže počítače smysl). Přesné postupy a zodpovědnost za zálohování by měla zvláště ve středních a větších organizacích, institucích, firmách a úřadech řešit bezpečnostní politika.

Jak už bylo uvedeno výše, neméně důležitým úkolem je zajistit, aby elektronická data neskončila u nepovolané osoby. K tomu existuje velmi jednoduchý prostředek, který se jmenuje „šifrování". Byť toto slůvko stále ještě mnoha lidem zní velmi cizokrajně a evokuje v nich nejrůznější exotické představy (špionážní thrillery apod.), ve skutečnosti jde o velmi rozšířenou techniku ochrany dat. A na svém významu nabývá čím dál více, protože spolehlivě chrání nejen v případě ztráty hardware, ale také při soustavných hackerských útocích, jimž je každý počítač připojený do sítě prakticky nepřetržitě vystaven.

Šifrování je proces, při němž jsou data převáděna z otevřené (běžně čitelné) podoby pomocí šifrovacího klíče a/nebo hesla do podoby, která je nepoužitelná. Jejich opětovná dostupnost je vázaná právě na dispozici šifrovacího klíče a/nebo znalost hesla – bez těchto atributů se potencionální útočník dostane pouze k nesmyslné a nepoužitelné změti dat, z nichž není schopen vyzískat žádnou informaci.

Samotný proces šifrování přitom není nikterak obtížný nebo běžnému smrtelníkovi nedostupný, protože ho provádí specializované počítačové programy. Práce s nimi je přitom stejně jednoduchá jako práce s jakýmkoliv jiným softwarem (nejčastěji bývají šifrovací nástroje přirovnávány k archivačním programům, protože plní prakticky stejnou roli – až na to, že při šifrování může data zpětně získat pouze osoba oprávněná). Pokud si chcete šifrování jednoduše vyzkoušet na vlastní kůži, můžete si z internetu stáhnout např. freewarový nástroj TrustPortr Encryption Lite.

TOMÁŠ PŘIBYL, AEC
www.aec.cz