

## Aké chyby najčastejšie spôsobujú stratu dát

*Štúdia Cisco poukazuje na rozdiely v správaní ľudí v závislosti od krajiny a kultúry, ktoré vedú k úniku podnikových informácií*

Bratislava, 22. októbra 2008

Rizikové správanie sa zamestnancov, ktoré podnikom spôsobuje únik dát, nie je univerzálne, líši sa podľa krajiny a kultúry. Organizácie by preto mali prispôbovať plán riadenia rizík v oblasti prevencie lokálnym podmienkam tak, aby dosahovali globálne kritériá bezpečnosti. Vyplýva to zo štúdie spoločnosti Cisco, ktorá skúmala rizikové prvky v správaní zamestnancov. Štúdia, ktorá sa opiera o prieskum na vzorke viac ako 2000 zamestnancov a IT pracovníkov v desiatich krajinách, identifikovala najčastejšie chyby vedúce k úniku podnikových dát.

### Zamestnanie a životný štýl

Autorom štúdie je spoločnosť InsightExpress, ktorá sa špecializuje na prieskumy trhu v USA. Dalo ju vypracovať Cisco s cieľom preskúmať dosah bezpečnostných problémov na firmy v čase, kedy sa mení životný štýl a pracovné prostredie. Namiesto centralizovaných sídiel s kancelárskymi miestami sa čoraz viac presadzujú modely práce na diaľku, stiera sa deliaca línia medzi pracovným a súkromným životom.

Podniky to nútia meniť prevádzkové procesy a životný štýl zamestnancov. Jedným z hlavných faktorov, ktorý k tejto zmene prispieva, je nástup zariadení a aplikácií pre spoluprácu, ktoré sa používajú na oba účely – vrátane mobilných telefónov, laptopov, aplikácií pre Web 2.0, videa a iných sociálnych médií.

Na štúdiu sa zúčastnili pracovníci z rôznych odvetví a typov firiem z USA, Veľkej Británie, Francúzska, Nemecka, Talianska, Japonska, Číny, Indie, Austrálie a Brazílie. Autori štúdie si vybrali tieto štáty preto, že reprezentujú rôzne spoločenské a obchodné kultúry, ktoré zahŕňajú vyspelé i rozvíjajúce sa ekonomiky s rôznou mierou využívania internetu.

„Tento výskum sme nerobili preto, aby sme predpovedali katastrofické scenáre,“ uviedol John N. Stewart, riaditeľ Cisco pre bezpečnosť. „Firmy každej veľkosti a zamestnanci vo všetkých profesiách musia chápať, ako ich správanie ovplyvňuje bezpečnostné riziká. Ak to pochopia, budú schopní vytvárať lokalizované programy, ktoré im umožnia lepšie tieto riziká kontrolovať. Ich bezpečnostné praktiky budú jednoducho efektívnejšie.“

### Desať najčastejších chýb

#### 1. Zmena bezpečnostných nastavení na počítačoch

Každý piaty zamestnanec zmenil bezpečnostné nastavenia na pracovnom zariadení, aby získal prístup k neautorizovaným webovým stránkam. Najčastejšie sa tento problém objavuje v Číne a Indii.

#### 2. Používanie neautorizovaných aplikácií

Sedem z desiatich IT profesionálov konštatovalo, že používanie neautorizovaných aplikácií a webových stránok (ako sú napríklad zakázané sociálne médiá, softvér na sťahovanie hudby alebo elektronické obchody) viedlo v každej druhej spoločnosti k úniku dát. Tento názor sa najčastejšie vyskytoval v USA (74 %) a Indii (79 %).

#### 3. Neautorizovaný prístup k sieti a zariadeniam

Dvaja z piatich IT profesionálov v poslednom roku riešili situáciu, keď mal zamestnanec prístup do nepovolených častí siete alebo zariadenia. Najčastejší výskyt bol v Číne, kde tento problém zaznamenali dve tretiny respondentov. Až 14 percent opýtaných sa s týmto problémom stretáva každý mesiac.

#### 4. Zdieľanie citlivých podnikových informácií

Až 24 percent zamestnancov sa priznalo, že hovorili o citlivých informáciách s osobami, ako sú priatelia, rodinní príslušníci alebo dokonca s úplne neznámymi ľuďmi. Pri otázke, prečo to urobili, zaznievali odpovede ako: „Potreboval som si na niekom vyskúšať, ako bude reagovať na moju

myšlienku“, „Chcel som sa uvoľniť“ alebo „Nevidel som na tom nič zlé.“

#### 5. Zdieľanie podnikových zariadení

Podnikové dáta nemusia byť vždy v správnych rukách. Takmer polovica zamestnancov (44 %) zdieľa pracovné zariadenia s osobami aj mimo firmy, a to bez akéhokoľvek dohľadu.

#### 6. Stieranie hranice medzi pracovnými a osobnými zariadeniami

Takmer dve tretiny zamestnancov pripustili, že používajú pracovný počítač na osobné účely. K najčastejším aktivitám patrí sťahovanie hudby, nakupovanie, bankové operácie, blogovanie a komunikácia v chatových skupinách. Až polovica zamestnancov používa osobný e-mail na komunikáciu so zákazníkmi a kolegami, avšak len 40 percent malo takýto postup schválený.

#### 7. Nechránené zariadenia

Minimálne jeden z troch zamestnancov bežne odchádza od svojho pracovného stola bez toho, aby sa odhlásil z počítača alebo ho zamkol. Títo pracovníci majú zároveň tendenciu nechávať svoje laptopy cez noc na pracovnom stole, niekedy dokonca bez odhlásenia sa, čo predstavuje potenciálne riziko krádeže a neoprávneného prístupu k podnikovým dátam.

#### 8. Ukladanie prihlasovacích mien a hesiel

Každý piaty zamestnanec si ukladá svoje prihlasovacie mená a heslá do počítača alebo si ich zapisuje na papier a necháva na stole, v nezamknutých odkladacích priestoroch či prilepené na počítačoch. V niektorých krajinách ako Čína (28 %) zamestnanci uviedli, že si odkladajú prihlasovacie mená a heslá k osobným finančným účtom do svojich pracovných zariadení, čo ohrozuje ich identitu a financie.

#### 9. Strata prenosných úložných zariadení

Až 22 percent zamestnancov nosí firemné dáta na podnikových úložných zariadeniach mimo spoločnosť, čím sa vystavujú riziku ich straty alebo krádeže. Najviac sa tento neduh prejavuje v Číne (41 %).

#### 10. Možnosť vstupu do priestorov bez dozoru

Asi 22 percent zamestnancov v Nemecku umožňuje návštevam pohybovať sa po priestoroch spoločnosti bez dozoru. Celosvetový priemer potom dosahuje 13 percent. Približne 18 percent organizácií umožňuje neznámym osobám dostať sa do podnikových priestorov v sprievode zamestnancov.

### Odporúčané postupy

J. N. Stewart v tejto súvislosti uviedol, že závery štúdie by mali firmám pomôcť štrukturovať vzdelávanie zamestnancov na regionálnej úrovni a formulovať plány riadenia rizika v globálnom meradle. Medzi odporúčané zásady, ktoré môžu zabrániť únikom dát, zaradil:

- Majte prehľad o tom, ako a kde sú ukladané dáta, ako sa k nim pristupuje a ako sa používajú
- Správajte sa k podnikovým dátam ako k vlastným a chráňte ich tak, ako chránite svoje peniaze
- Inštitucionalizujte štandardy bezpečného správania
- Zamestnanci sa nesmú báť nahlasovať incidenty, aby IT útvary mohli rýchlejšie riešiť problémy
- Myslite globálne, ale prispôbujte programy lokálnym podmienkam
- Ochrana dát si vyžaduje tímovú prácu v rámci celej spoločnosti, nie je to len úloha pre IT

### O Cisco Systems

Cisco (NASDAQ: CSCO) je svetový líder v oblasti sietí, ktorý mení spôsob, akým ľudia nadväzujú kontakty, komunikujú a spolupracujú. Informácie o spoločnosti Cisco je možné získať na <http://www.cisco.com>. Aktuálne informácie nájdete na <http://newsroom.cisco.com>.