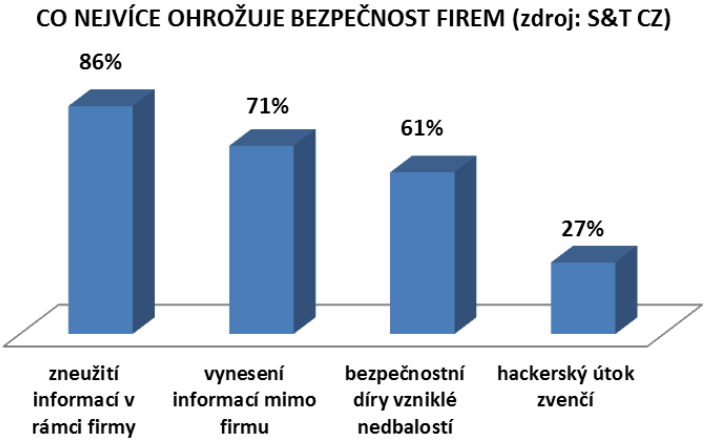
TISKOVÁ ZPRÁVA

Intriky zaměstnanců snižují konkurenceschopnost firem

Výkonnost a bezpečnost tuzemských firem ohrožují intriky zaměstnanců – 40 procent z nich poškodí zaměstnavatele či nadřízeného kvůli osobnímu prospěchu. Pravděpodobnost útoku zevnitř je třikrát vyšší než zvenčí. Firmy proto nasazují speciální bezpečnostní systémy, které je před neloajálními zaměstnanci chrání.

PRAHA, 14. prosince 2011 – Podle analýzy technologické společnosti **S&T CZ** nejvíce ohrožuje bezpečnost a konkurenceschopnost tuzemských firem **intrikaření zaměstnanců**. „Interní pletichy, tedy snaha získat nekalým způsobem nějakou výhodu uvnitř firmy, patří mezi nejrozšířenější bezpečnostní rizika. V závěsu je vynášení strategických informací mimo firmu, například podrobnosti o nabídkách klíčových tendrů," říká **Petr Hněvkovský**, bezpečnostní expert společnosti S&T CZ.

Z analýzy klíčových bezpečnostních hrozeb společnosti S&T CZ vyplývá, že **interní zneužívání dat představuje větší bezpečnostní riziko (86 %) než zneužití dat zvenčí**, například útok hackerů (27 %), viz graf. „K intrikaření dochází v každé firmě. Vynést tajnou informaci mimo firmu a ještě ji zpeněžit je rizikové a náročné, to si běžný zaměstnanec netroufne. U interního zneužití je to ale jinak: upevnit svou pozici uvnitř firmy chce každý, s rostoucí nezaměstnaností budou interní pletichy narůstat," varuje Petr Hněvkovský.



JAKÉ INFORMACE SE NEJVÍCE KRADOU:

- rozvojové plány
- informace o platech a odměnách
- další klíčové informace k upevnění vlivu uvnitř firmy
- nabídky v rámci tendrů

Firemní know-how proto stále častěji ochraňují sofistikované bezpečnostní systémy, které umějí upozornit na potenciální rizikové chování uživatelů. „Zaznamenáváme meziročně zhruba 30procentní nárůst prodejů. Tyto systémy monitorují a vyhodnocují všechny události, které by mohly mít vliv na bezpečnost firmy – od pohybu osob po přístup k citlivým datům a využívání různorodých informačních zdrojů," vysvětluje Petr Hněvkovský. Lze tak snadno zjistit aktivity jednotlivých uživatelů a včas vyhodnotit nestandardní situace.

40 procent Čechů poruší pravidla kvůli osobnímu prospěchu

Zneužití citlivých informací nejvíce **hrozí firmám s více než 50 zaměstnanci**, kde již existuje značné konkurenční prostředí. „V malých firmách je relativně snadné zajistit, aby se k citlivým informacím dostaly jen autorizované osoby. Případně o sobě a firmě vědí téměř vše, takže není co tajit," popisuje běžnou praxi Petr Hněvkovský.

Jakmile ale začne vznikat soutěživé prostředí, situace se rázem změní: „Češi jsou poměrně soutěživí a ambiciózní, bohužel až **40 procent z nich bez skrupulí poruší pravidla hry**, pokud jim to přinese osobní výhodu. Může za to přijetí neetických forem chování v české populaci jako zcela běžné součásti života," vysvětluje psycholog Jiří Šimonek. Vyplývá to z testování 84 tisíc zaměstnanců během posledních pěti let, které provedla společnost DAP Services.

Nejvíce se intrikáni zajímají o klíčové informace, které jim umožní upevnit vliv uvnitř firmy. „Výše platů a odměn kolegů, rozvojové a strategické plány či vlastní nabídky nebo dohody s externími dodavateli," vyjmenovává Petr Hněvkovský. To potvrzují i soudní znalci v oblasti informačních technologií: „Setkáváme se často s nulovým zabezpečením interních dat. V případě jejich zneužití se pak velmi těžko hledá viník, a i pokud se najde, bez pádných důkazů nelze takového pracovníka kvůli zneužití interních informací propustit," říká soudní znalec Ivan Janoušek ze znaleckého ústavu **Apogeo Esteem**.

Firmy podceňují nepřítele uvnitř firmy

Za špatnou bezpečnostní situaci uvnitř firem může i fakt, že se manažeři často zaměřují na zmiňovaná vnější bezpečnostní rizika, třeba útok hackerů. Vnitřní bezpečnostní hrozby naopak bagatelizují. „Přitom pravděpodobnost útoku zevnitř je **třikrát vyšší** než zvenčí. Přesto se investice firem týkají hlavně vnějších rizik," varuje bezpečnostní expert Petr Hněvkovský.

RIZIKEM JSOU „CHODBOVÉ ŘEČI"

- Bezpečnostním rizikem jsou i „chodbové řeči" a hlavně pauzy na kouření. V těchto neformálních situacích se překvapivě snadno stírá subordinace a jiné formální bariéry.

- V těchto kolektivech se často probírají velmi důvěrné informace, které by v kanceláři málokdo řekl nahlas. Případně slouží ke sdílení velmi citlivých informací, například jak obcházet nová nařízení nebo bezpečnostní opatření.

Podle psychologů se tak děje i kvůli tomu, že si manažeři neradi připouštějí zrádce ve vlastním týmu: „Je to přirozené, stejně jako každý rodič vidí vlastní děti v lepším světle než okolí. O to více je třeba být na pozoru, protože intriky mohou rozložit celý pracovní tým," vysvětluje psycholog Jiří Šimonek.

Neloajalita vůči zaměstnavateli představuje historický problém, který přetrvává v české společnosti z let komunistického režimu. „V duchu rčení, kdo nekrade, okrádá svou rodinu' český zaměstnanec spíše hledá osobní prospěch. Prosperita firmy či týmu je pro něj až druhořadá. V Asii tomu je naopak, zaměstnanci jsou mnohem loajálnější a na úspěchu firmy jim záleží," vysvětluje psycholog Jiří Šimonek ze společnosti DAP Services.

Intrikaření snižuje výkonnost firmy

Pletichy uvnitř firem představují velké riziko pro jejich další rozvoj. Pokud vliv získávají intrikáni namísto opravdu schopných zaměstnanců, konkurenceschopnost společnosti rapidně klesá. „Vliv pak mají lidé, kteří mají nízkou morálku a nezastaví se prakticky před ničím. Naopak ti schopnější a loajálnější mohou být rychle vyšachováni ze hry," vysvětluje Jiří Šimonek.

Dalším rizikem je obyčejná lidská závist. „Do bezpečnosti může firma investovat miliony, ale pokud se někdo dozví, že jeho plat je menší než kolegův, může získat touhu si přivydělat jinak či kolegu poškodit. Morálně si to obhájí tak, že si stejně bere jen to, o co ho firma připravuje," vysvětluje chování zaměstnanců v praxi soudní znalec Ivan Janoušek.

Lékem proti pletichám je nejen dobré zabezpečení interních dat, ale i vypracování systému kompetencí. „Přehnané restrikce vedou k tomu, že se lidé bezpečnostní pravidla snaží obcházet. Klíčem je tedy jasně určit, kdo k jakým informacím může a za jakých bezpečnostních podmínek. Samotné technologie jsou důležitým podpůrným prostředkem, ale nikoli spásou," uzavírá Petr Hněvkovský, bezpečnostní expert společnosti S&T CZ.

Více informací poskytnou:

Radovan Suk, mediální zástupce S&T CZ, tel.: (+420) 731 444 043, radovan.suk@mediakom.cz
Otta Matoušek, marketingový ředitel S&T CZ, otta.matousek@snt-world.com, http://www.sntcz.cz/

O společnosti S&T CZ

Společnost S&T CZ je jedním z největších systémových integrátorů v České republice. Firma je součástí nadnárodní skupiny S&T AG, předního evropského dodavatele IT řešení a služeb, zastoupeného vedle Rakouska v 18 dalších zemích střední a východní Evropy. S&T AG čítá přibližně 2000 zaměstnanců.

S&T CZ v Česku disponuje týmem 210 odborníků a má pobočky v osmi městech: v Praze, Brně, Liberci, Plzni, Českých Budějovicích, Pardubicích, Olomouci a Ostravě. Do tuzemské skupiny S&T rovněž patří dodavatel lékařské techniky S&T Plus. Centrála nadnárodní skupiny S&T AG sídlí v Rakousku, s akciemi společnosti se od roku 2003 obchoduje na Vídeňské burze.

S&T CZ navrhuje, dodává a provozuje informační systémy a poskytuje řešení a služby v oblasti informačních technologií. Zaměřuje se zejména na výrobní podniky a utility, finanční instituce, obchodní organizace a veřejnou správu. K dlouhodobým klíčovým zákazníkům společnosti patří například Škoda Auto, Komerční banka, Česká spořitelna, Citibank, RWE, PwC, MPSV ČR, MMR ČR a další.

http://www.sntcz.cz/