

➔ Bywa, że dane stają się kartą przetargową, którą warto „wkupić się” u nowego pracodawcy. Często dowodzi to tego, że firmy nie mają kontroli nad własnymi danymi

Statystyki są bezlitosne

W wielu firmach panuje przekonanie, że dane powierzone w outsourcing są mniej bezpieczne, niż te pozostające pod opieką własnego zespołu. Tymczasem naprawdę jest dokładnie odwrotnie.

Arnold Nowak – Członkowie organizacji uważają, że skoro dla outsourcingera są jedynym z wielu klientów, nie wiadomo, czy będzie on wystarczająco dobrze chronił dane, czy będzie potrafił o nie zadbać, wreszcie czy będzie obchodził się z nimi z należytą starannością. Menedżerom firm często wydaje się, że kontrolują sytuację tylko wtedy, gdy dane są przechowywane wewnątrz organizacji.

Brutalna rzeczywistość
Prawda jest jednak brutalna. Firmy wcale nie mają kontroli nad własnymi danymi. Statystyki są bezlitosne, większość danych wycieka z wnętrza firmy poprzez jej włas-

nych pracowników. Powody przekazywania danych na zewnątrz są różne. Pamiętajmy, że pieniądze nie są jedyną motywacją pracowników, czasem jest to frustracja, złość na pracodawcę. Bywa, że dane stają się kartą przetargową, którą warto „wkupić się” u nowego pracodawcy. Czasem jest to też zwykła niewiedza i podatność na manipulację. Pracownicy organizacji nie dość, że wiedzą jakie dane są najistotniejsze, to jeszcze – znając system zabezpieczeń – wiedzą jak je niepostrzeżenie wyprowadzić.

Ścisłe tajne/chronione

W przypadku firmy outsourcingowej jest inaczej. Istnieje tu znacznie mniejsze prawdopodobieństwo takiego zdarze-

nia. Zewnętrzni pracownicy obsługujący systemy nie mają dostępu do interpretacji danych, nie są oni zorientowani, które dane są ważne, newralgiczne. Najczęściej obsługują fragment systemu np. bazy danych i widzą tylko parametry informatyczne systemu bez możliwości wglądu w procesy biznesowe klienta. Poza tym dobry outsourcinger, dbając o swoją wiarygodność i zaufanie klientów, ma znacznie ostrzejsze procedury ochrony i zapobiegania utracie danych. Inwestuje w złożone, najnowsze i najdroższe systemy zabezpieczeń. Musi to robić, bo za każdy „wyciek” może słono zapłacić – pieniędzmi bądź w ostateczności swoim istnieniem na rynku.

*Autor jest prezesem zarządu
Intelligence*