

## Dziesięć przypadków utraty danych wrażliwych w ciągu ostatniego roku

### Skuteczna strategia ochrony zgodnie z normą ISO 27001



Dziesięć przypadków utraty danych na przestrzeni ostatniego roku w różnych krajach świata daje do myślenia. „Przypadki takie jak kradzież danych z tajnych archiwów wojskowych, firm farmaceutycznych lub spółki prowadzącej portal pośrednictwa pracy pokazują narastającą potrzebę opracowania właściwej strategii skutecznej ochrony informacji” tłumaczy w ostatnim komunikacie prasowym dyrektor generalny CIS-Cert Erich Scheiber. „Licznym przypadkom utraty danych można było w znacznym stopniu zapobiec”, dodaje.

### Rekordowy rok 2007

W roku 2007 osiągnięty został niechlubny światowy rekord: grupa ekspertów ds. bezpieczeństwa z "attrition.org" szacuje, że skradzionych zostało ponad 167 milionów danych osobowych, trzy razy więcej niż rok wcześniej. "Większe firmy są dobrze wyposażone technicznie. Zbyt mało uwagi poświęca się natomiast czynnikowi ludzkiemu", mówi Stefan Poschinger, administrator bezpieczeństwa informacji w Austriackim Federalnym Centrum Obliczeniowym BRZ.

### Czynnik ludzki i jego konsekwencje

Problem na świecie jest znaczący. W badaniu 194 przedstawicieli kierownictwa amerykańskich przedsiębiorstw, przeprowadzonym przez Computer Security Institute wynika, że w 2007 r. straty w wyniku kradzieży sprzętu zawierającego dane chronione, nadużyć, a nawet sabotaży dotyczących ujawnienia danych, wyniosły 66,9 mln dolarów. Najnowszy raport austriackiej Izby

Handlowej pt. „IT sprawą kierownictwa” mówi, że utraty danych doświadczyło 20,5 procent z 300 respondentów, a szkody z tego tytułu wyniosły od 100.000 do 500.000 euro.

### Nowy aspekt problemu

"Kradzież danych tworzy nowy aspekt problemu: zniszczenia mają charakter informacyjny, a nie fizyczny", mówi inż. Gernot Schmieda, ekspert w zakresie dowodów cyfrowych. Poprzednie metody zarządzania atrybutami plików pozwalały na "czytanie, zapisywanie i uruchamianie, ale nie były w stanie zapobiec kopiowaniu. Rozwiązanie musi przynieść zmianę w kierunku zapobiegania wyciekom danych".

### Bezpieczeństwo od A do Z: ISO 27001

"Odpowiedniego poziomu bezpieczeństwa w przedsiębiorstwie nie da się osiągnąć przez rozwiązania częściowe – luki w zabezpieczeniach grożą potencjalnymi atakami," mówi dr Elisabeth Stiller-Erdprieser z Siemens IT Solutions and Services. Nawet wiele lat po certyfikacji ISO 27001 firma jest zmuszona do ciągłego usprawniania procedur bezpieczeństwa wynikających z kolejno nabywanych doświadczeń ze współpracy z klientami. Siemens zaleca "wszechstronne bezpieczeństwo" w oparciu o normę ISO – poczynając od analizy ryzyka w kontekście funkcjonowania firmy w celu poprawy jej działań.

### Cykl życia informacji

"System Zarządzania Bezpieczeństwem Informacji zgodnie z normą ISO 27001 wymaga zidentyfikowania słabych stron i zagrożeń, ich oceny oraz zmniejszenia do akceptowalnego poziomu", wyjaśnia Stefan Poschinger. W ten sposób chroniony jest cały "cykl życia informacji" od jej powstania, przez użytkowanie, archiwizację, aż do zniszczenia.

### Zasada 16 oczu

Jednym z najważniejszych zabezpieczeń wynikających z ISO 27001 jest klasyfikacja informacji na: publiczne, poufne, tajne lub ściśle tajne. "Różnią się w zależności od poziomu - od

zasady 4 oczu, przydatnej w sytuacjach krytycznych dla bezpieczeństwa informacji do zasady 16 oczu ", tłumaczy Poschinger. Technicznie rzecz biorąc, można ograniczyć dostęp poprzez szyfrowanie i rozdzielanie klucza pomiędzy kilka osób. Dane są wtedy dostępne dla dwóch lub więcej uprawnionych osób . Systemy dostępu mogą być zaprogramowane w podobny sposób.

### **Urządzenia mobilne i media**

CRM w telefonach komórkowych, urządzenia do przechowywania danych, laptopy z wynikami badań coraz bardziej popularna praca na odległość to według ISO 27001 argumenty do wykorzystywania technologii szyfrowania i kontroli. Device Control umożliwia zdefiniowanie polityki lokalnego systemu interfejsów i urządzeń zewnętrznych. Application Control może być dozwolone jedynie w celu zainstalowania programów. Dzięki pełnemu szyfrowaniu dysku twardego dane chronione są przed nieautoryzowanym dostępem nawet w przypadku utraty urządzenia.

### **Włącz zarządzanie i monitorowanie w czasie rzeczywistym**

Ukierunkowanie na ciągłą ocenę protokołów i logowania ma zasadnicze znaczenie dla zrozumienia regularnego przepływu informacji. Inż. Gernot Schmieda podkreśla: "Tylko wiedza o standardowej eksploatacji pozwala na dostrzeżenie rozbieżności. Główne aspekty zintegrowanego zarządzania to gromadzenie, korelacja, konsolidacja, analiza i ostrzeżenie".

### **Zarządzania ryzykiem**

Dla zarządzania najistotniejsza jest świadomość zasady: dostępność do informacji zależy od pełnionej przez pracownika funkcji. Informacje powinny być sklasyfikowane, zbyt wiele środków ochrony danych utrudnia działanie, zbyt mało zwiększa ryzyko ich wycieku. "Dlatego, ISO 27001 zaleca wykonanie analizy ryzyka w celu podjęcia skutecznych środków służących do jego oceny w rozsądnym zakresie ", mówi szef CIS-Cert, Erich

Scheiber. "Celem jest zapewnienie opłacalnego ekonomicznie bezpieczeństwa na najwyższym poziomie."

### **Z mediów 2007-2008: dziesięć przypadków utraty danych wrażliwych w ciągu ośmiu miesięcy.**

#### **Marzec 2008**

Znany brytyjski nadawca poinformował 5000 osób, że ich dane osobowe oraz informacje dotyczące wynagrodzeń zostały skradzione z sieci korporacyjnej.

#### **Luty 2008**

Złodzieje ukradli dane 4,2 mln numerów kart kredytowych z systemu sieci supermarketów Hannaford Brothers w New England, USA.

#### **Luty 2008**

Dla konserwatywnych polityków nielegalnie skopiowano dane byłych pracowników wojskowych.

#### **Styczeń 2008**

Skradziono laptopa brytyjskiemu oficerowi. Wraz z nim zniknęło 600.000 danych osobowych dotyczących wojskowych różnego szczebla.

#### **Styczeń 2008**

W 2007 utracono 100.000 rekordów z numerami id i osobistymi historiami medycznymi z kilku brytyjskich ośrodków zdrowia.

#### **Grudzień 2007**

Skradziono poufne dane trzech milionów brytyjskich kandydatów na prawo jazdy. Odpowiedzialna okazała się prywatna firma ze Stanów Zjednoczonych.

#### **Październik 2007**

Luka w znanym portalu aukcyjnym eBay umożliwiła oszustom podszywanie się podużytkowników portalu i składanie fałszywych ofert.

### **Październik 2007**

Skradziony został laptop zawierający niezaszyfrowane dane 800 000 kandydatów do pracy w sieci odzieżowej Gap.

### **Wrzesień 2007**

Były pracownik międzynarodowej firmy farmaceutycznej Pfizer ukradł informacje dotyczące 34.000 współpracowników, w tym numery kont i kart kredytowych.

### **Sierpień 2007**

Za pomocą trojana wyłudzone od firmy headhunterskiej dane dostępne do portalu pośrednictwa pracy monster.com i skradziono dane 1,6 miliona osób poszukujących pracy.

### **Największa w kradzież danych historii.**

Według doniesień Wall Street Journal największy w historii rabunek bazy danych miał miejsce w firmie TJX. Rozpoczął się 2006 r. w samochodzie przy użyciu tzw. lustra parabolicznego. Wyposażeni w antenę satelitarną, laptopa i oprogramowanie dekodujące transmisję strumieniową złodzieje uzyskali dostęp do systemu centralnego. Skradziono numery co najmniej 45 mln kart płatniczych oraz szczegółowe dane tysięcy klientów.