W dużych przedsiębiorstwach i korporacjach częsta wymiana sprzętu IT to standard, z którym wiąże się szereg niebezpieczeństw - przede wszystkim ryzyko udostępnienia poufnych danych osobom trzecim. Użycie polecenia delete nie usuwa skutecznie informacji zapisanych na dyskach twardych, a ich wydostanie się poza firmę niesie za sobą nie tylko poważne konsekwencje finansowe i prawne, ale przede wszystkim godzi w jej dobre imię.

W ostatnich latach sposób prowadzenia biznesu został silnie zdeterminowany przez nieustanny rozwój technologii informatycznych. Zmuszają one do częstej wymiany sprzętu IT oraz nośników danych, przede wszystkim dysków twardych. Pojawia się zatem konieczność weryfikacji przydatności zapisanych informacji, a co za tym idzie usunięcia nieaktualnych lub niepotrzebnych, w dużej mierze klasyfikowanych jako poufne.

Wielu pracowników firm i instytucji wciąż nie jest świadomych, że skasowanie pliku nie jest równoznaczne z usunięciem z dysku. System operacyjny likwiduje jedynie informację o lokalizacji, natomiast fizycznie plik dalej istnieje. Dane można odzyskać po sformatowaniu dysku twardego z poziomu BIOS-u, podobnie jak w przypadku fizycznego zniszczenia - z odpowiednią wiedzą nie będzie żadnego problemu, aby odczytać informacje nawet z fragmentów nośnika.

Gdy nadchodzi czas wymiany starych komputerów, często zostają one sprzedane lub wyrzucone wraz z dyskami twardymi (HDD), które nadal zawierają istotne i poufne informacje. W przypadku dużych firm i korporacji, szczególnie w miejscach zaufania publicznego, jak banki czy instytucje finansowe, to działanie absolutnie niedopuszczalne!

Skasować raz, a dobrze

Istnieją dwie skuteczne metody usuwania danych z dysków twardych. Pierwsza opiera się na wykorzystaniu specjalistycznego oprogramowania, które poprzez wielokrotne nadpisanie danych według specjalnego algorytmu uniemożliwia odczytanie informacji. Dysk można ponownie wykorzystać, jednak cały proces jest powolny, a koszt wysoki.

Druga metoda bazuje na demagnetyzacji polegającej na trwałym usunięciu danych przy pomocy specjalistycznych urządzeń – tzw. demagnetyzerów. - Można je zastosować zarówno w przypadku sprawnych, jak i uszkodzonych dysków twardych HDD czy taśm magnetycznych - mówi Katarzyna Stempień z T&T Trading, generalnego dostawcy demagnetyzerów na polskim rynku. Nośniki są poddawane działaniu silnego impulsu magnetycznego, który niszczy wszystkie zapisy w warstwie magnetycznej - dane zostają bezpowrotnie utracone. Zaletą demagnetyzacji jest przede wszystkim bezpieczeństwo procesu i krótki czas jego trwania. W przypadku np. demagnetyzera Intimus 9000 bezpowrotne skasowanie zawartości dysku zajmuje jedynie 10 sekund.

W przeciwieństwie do demagnetyzacji, która uniemożliwia dalsze korzystanie z dysku, na rynku dostępne są również rozwiązania pozwalające na oczyszczenie nośnika i jego ponowne użycie. - Jako przykład można wymienić Intimus Hammer, który opierając się na metodzie secure erase, trwale usuwa dane (z prędkością 4 GB na minutę), jednocześnie nie niszcząc dysku - dodaje Katarzyna Stempień.

Konsekwencje wycieku danych

Wyciek danych z firm czy instytucji niesie ze sobą poważne konsekwencje prawne, finansowe i przede wszystkim negatywnie wpływa na wizerunek. Zgodnie z art. 51 ustawy o ochronie danych osobowych, administratorzy danych, którzy udostępniają lub umożliwiają dostęp do nich osobom nieupoważnionym podlegają grzywnie, karze ograniczenia wolności lub pozbawienia wolności do lat 2. Wymiar kary zmniejsza się do roku w przypadku, gdy było to działanie nieumyślne.

Znaczne osłabienie marki i reputacji firmy, utrata klientów spowodowana obniżeniem zaufania czy zanik przewagi konkurencyjnej i wiążący się z tym spadek wartości firmy to tylko część z wizerunkowych skutków wycieku danych. Wysokie koszty związane z informowaniem otoczenia o sytuacji i eliminowaniem negatywnych konsekwencji, kary nałożone przez organy kontroli oraz straty finansowe w wyniku procesów sądowych mogą determinować dalsze funkcjonowanie firmy.

Ataki, wycieki, kradzieże mogą dotknąć każdego...

O tym, że wyciek danych może spotkać nawet największe, wydawałoby się najbardziej zabezpieczone korporacje świadczą przykłady z życia wzięte. Z problemem wciąż boryka się koncern Sony, który po raz kolejny padł ofiarą działań hakerów. Na początku czerwca 2011 r. z serwisu SonyPictures.com wykradziono informacje (adresy e-mail, hasła, adresy domowe, daty urodzenia i inne) powiązane z ponad milionem kont klientów Sony. Grupa LulzSec odpowiedzialna za włamanie weszła także w posiadanie danych administratorów serwera oraz 3,5 mln kuponów muzycznych. Dodatkowo opublikowano plany sieci wewnętrznej Sony zawierające lokalizację i listę wykorzystywanych urządzeń sieciowych wraz z wersją oprogramowania i administratorem. Udostępniono również kod źródłowy prywatnej sieci developerów.

Nie tak dawno temu, bo w kwietniu br. wykradziono także 78 mln rekordów z sieci PSN, a na początku maja kolejne kilkadziesiąt milionów z serwerów Sony należących do sieci SOE, które zawierały informacje, takie jak: imię i nazwisko, adres, loginy i hash hasła. Dodatkowo w niepowołane ręce dostało się ponad 12 tys. numerów kart kredytowych/debetowych wraz z datą ważności. Według agencji Reuters kurs akcji Sony spadł o 5%, a koszty zaistniałej sytuacji szacuje się na ponad 1,5 mld dolarów.

Poufne informacje na śmietniku

Głośne historie o udostępnieniu poufnych danych klientów banków, firm ubezpieczeniowych, operatorów telefonii komórkowej czy dużych przedsiębiorstw świadczą o braku odpowiedniego zabezpieczenia lub wykorzystywaniu nieskutecznych metod niszczenia istotnych informacji.

Ostatnio umorzono postępowanie w sprawie wycieku danych kilkuset klientów mBanku w Łodzi. 18 kartek formatu A4 z informacjami zawierającymi m.in. nazwy firm, ich adresy, dane personalne i adresowe właścicieli, numery NIP, REGON, PESEL, a nawet numery rachunków bankowych z bieżącym stanem i posiadanym limitem zostały znalezione przez przechodnia w śmietniku na terenie kompleksu biurowego. Nikt nie został pociągnięty do odpowiedzialności, ponieważ nie ustalono, kto zawinił.

Jak podsumowuje Piotr Trawa z firmy Printcom, dystrybutora demagnetyzerów, osoby sprawujące pieczę nad ochroną poufnych danych powinny być świadome zagrożeń wynikających nie tylko z niewłaściwego doboru lub wykorzystania zabezpieczeń, ale także nieodpowiedniego sposobu usunięcia niepotrzebnych danych. Warto zwrócić się o pomoc do eksperta i zainwestować w odpowiedni sprzęt, który przy użyciu skutecznych i sprawdzonych metod trwale skasuje informacje zapisane na dysku, a tym samym ochroni firmę przed negatywnymi skutkami wycieku danych.

Źródło: www.demagnetyzery.pl