Paweł Odor*

Leć do Afryki, Twoje dane już tam są...

Fot. Kuzma

W sierpniu portale internetowe na całym świecie obiegła wiadomość, że w jednym z afrykańskich krajów można kupić za kilkanaście dolarów wszystkie dane dotyczące przysłowiowego Pana Smitha, klienta szanowanego banku w Wielkiej Brytanii. To nie żart, a brak procedur kasowania danych. Jak widać, problem niekoniecznie musi dotyczyć małych firm czy indywidualnych użytkowników komputerów. A czy Twoje dane, Drogi Czytelniku, będziesz mógł odkupić od handlarza używanymi komputerami, będąc na wakacjach, np. w Egipcie?

Taki scenariusz nie jest wykluczony. Wszędzie tam, gdzie zarządza się danymi osobowymi istnieje taka możliwość. Dotyczy to przede wszystkim instytucji zaufania publicznego, takich jak banki czy firmy ubezpieczeniowe, oraz urzędów. Obowiązek usuwania danych reguluje ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 roku, w której czytamy:

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

1) likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
2) przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie.

Źródłem problemów nie jest wbrew pozorom brak dostępu do zaawansowanych technologii, a niewiedza dotycząca elementarnych zasad kasowania danych.

Otrzymanie przez pracownika lub urzędnika nowego komputera i brak procedur kasowania danych to niemal gwarancja, że nasze dane mogą wydostać się na zewnątrz.

Problem, w większym lub mniejszym stopniu, dotyczy niemal wszystkich rodzajów organizacji i instytucji. Jednym z najbardziej banalnych i jednocześnie niebezpiecznych dla nas wszystkich sposobów wycieku istotnych danych, jest nieumiejętność ich kasowania oraz, niestety, bezmyślność.

Dostałem nowy komputer!

Otrzymanie przez pracownika lub urzędnika nowego komputera i brak procedur kasowania danych to niemal gwarancja, że nasze dane mogą wydostać się na zewnątrz. Co dzieje się ze starym komputerem? Są dwie możliwości. Nasza maszyna przechodzi w ręce kolegi lub koleżanki lub też zostaje sprzedana do komisu, ewentualnie oddana na złomowisko.
W przypadku pozbycia się komputera z firmy, najczęściej stosowanym sposobem usunięcia danych (oczywiście nieskutecznym), jest formatowanie. Po tej operacji wszystkie dane są dostępne dla amatora odzyskiwania danych, który może skorzystać z dobrego i ogólnodostępnego programu odzyskiwania danych, jak np. EasyRecovery.

Dowiedli tego kilka lat temu studenci Massachusetts Institute of Technology, jednej z najlepszych uczelni technicznych na świecie, a także w tym roku polscy informatycy, przeprowadzając doświadczenie polegające na zebraniu starych komputerów ze złomowiska (w pierwszym przypadku) lub zakupie używanych nośników w Internecie (drugi przypadek).
W obu przypadkach okazało się, że dane firm, które pozbyły się starych komputerów, były tam, gdzie być nie powinny lub starano się je usunąć w tak nieporadny sposób, że odzyskanie danych, z kilkuset nośników w każdym z doświadczeń, zajęło kilkanaście dni żmudnej, ale efektywnej pracy – zaznaczmy – nieprofesjonalistów!

Jak więc skutecznie kasować dane?

Istnieją dwie metody bezpowrotnego kasowania danych – programowa i sprzętowa. Pierwsza wykorzystuje aplikacje dedykowane do bezpowrotnego usuwania danych. Warto dodać, że przy obecnych gęstościach zapisu danych, wystarczy jednokrotny pełny cykl nadpisania informacji, aby nie było możliwe ich odtworzenie. Tę właściwość wykorzystuje wiele programów służących

Algorytm	Treść algorytmu	Uwagi
Instrukcja o Ochronie Informacji Departamentu Obrony USA (NISPO) DoD 5220,22-M,1995r.	Ilość cykli zapisu- 3 Cykl 1- zapis dowolnego kodu Cykl 2- zapis inwertowanego kodu Cykl 3- zapis przypadkowych kodów	NISPO zabrania wykorzystywania tego algorytmu do niszczenia danych o zaznaczeniu „ściśle tajne" Alternatywa- rozmagnesowanie, fizyczne niszczenie
Standard VISR,1999r. Niemcy	Ilość cykli zapisu- 3 Cykl 1-zapis ciągu zer Cykl 2-zapis ciągu jedynek Cykl 3-zapis kodu naprzemiennie z zerami i jedynkami	
GOST P50739-95r. Rosja	Dla klasy ochrony danych 1..3 Ilość cykli zapisu- 2 Cykl 1- zapis ciągu zer Cykl 2- zapis kodów przypadkowych Dla klasy ochrony 4..6 Jeden cykl zapisu ciągu zer	
Algorytm Bruce'a Schneiera	Ilość cykli zapisu – 7 Cykl 1- zapis ciągu jedynek Cykl 2- zapis ciągu zer Cykli 3..7– zapis przypadkowych kodów	
Algorytm Petera Gutmana	Ilość cykli- 35 Cykle 1..4- zapis dowolnego kodu Cykle 5..6- zapis kodów 55h, AAh Cykle 7..9- zapis kodów 92h,49h,24h Cykle 10..25- zapis kolejnych kodów od 00,11h,22h, itd. do FFh Cykle 26..28- jak w 7..9 Cykle 29..31- zapis kodu 6Dh, B6h Cykle 32..35- jak w 1..4	

kasowaniu danych, choć te najbardziej profesjonalne, np. DataEraser, nadpisują dane wielokrotnie.
Choć programowe kasowanie danych jest pewną i bezpieczną metodą, istnieją pewne sytuacje, w których nie można go wykorzystać.
Takie sytuacje mogą dotyczyć np. uszkodzonych nośników danych. O ile uszkodzenie nośnika powoduje niemożność bezpośredniego skorzystania z danych na nim zgromadzonych, o tyle nie można wykluczyć, że osoby nieuprawnione doprowadzą do naprawy nośnika i uzyskają dostęp do danych.

Inna grupa przypadków, kiedy programowe kasowanie danych nie jest metodą gwarantującą absolutne bezpieczeństwo, dotyczy zaawansowanych technologicznie nośników, które są zdolne do tzw. remapowania sektorów dysku, które zawiodły. Dane z sektorów, które zostały (przez elektronikę sterującą nośnika) uznane za uszkodzone, nie mogą zostać usunięte w sposób programowy. Jednak dysponując zaawansowaną techniką laboratoryjną, można uzyskać do nich dostęp, a co za tym idzie, również dostęp do danych tam zapisanych.

Do zastosowania innych metod, niż programowe kasowanie danych, czasami skłaniają również bardziej prozaiczne przyczyny. Jeśli mamy do czynienia z dużą ilością nośników, a jednocześnie czas, którym dysponujemy, jest ograniczony, należy rozważyć metody szybsze od programowego nadpisywania danych.
Jedną z takich metod jest demagnetyzacja (ang. *degaussing*) nośników magnetycznych polegająca na poddaniu nośnika działaniu silnego impulsu magnetycznego, który niszczy bezpowrotnie wszelkie zapisy dokonane w warstwie magnetycznej nośnika. W przypadku dysków twardych, ta metoda usuwa również dane niezbędne do prawidłowej pracy dysku, co powoduje, że po demagnetyzacji nośnik nie nadaje się do dalszego użytku.

Kasowanie dla zaawansowanych

Istnieją trzy poziomy programowego kasowania danych. Zostały opracowane w zgodności z normami dotyczącymi bezpowrotnego usuwania danych. Profesjonalne aplikacje, jak np. Ontrack DataEraser, spełniają uwarunkowania, które zostały określone w jednym z najbardziej restrykcyjnych dokumentów tego typu – Instrukcji o Ochronie Informacji Departamentu Obrony USA.

Początkowy poziom (poziom 0)

Najprostsza, najszybsza i często stosowana forma niszczenia informacji, polegająca na niszczeniu część danych przy pomocy formatowania lub skasowania zawartości, ewentualnie usunięcia informacji o partycjach.
W tym przypadku, dane na dysku nie są niszczone, tylko utrudnia się do nich dostęp – można go jednak odzyskać za pomocą specjalnego oprogramowania, dokonującego analizy sektorów dysku (Norton DiskEdit, WinHex).

Poziom 1

Na tym poziomie dokonuje się zapisu ciągu zer albo jedynek do sektorów danych. Przy tym niszczy się nie tylko obszar ładowania, ale również i dane.
Wykorzystanie tej metody praktycznie uniemożliwia odzyskanie danych poza profesjonalnym laboratorium. Teoretycznie odtworzenie danych jest jednak stale możliwe.

Poziom 1+

Poziom 1+ wymusza zastosowanie kilku cykli zapisu ponownego. Użycie tej metody praktycznie eliminuje możliwość odzyskania danych. Tabela z poprzedniej strony opisuje rodzaje stosowanych algorytmów programowego kasowania i ich treść.
W przypadku metod sprzętowych, możliwych jest sześć sposobów usuwania danych. Oprócz opisanego powyżej oddziaływania polem magnetycznym, stosowane są również metody mechaniczne – polegające na rozdrobnieniu nośnika i termiczne, w których nośnik nagrzewany jest do temperatury topnienia podstawy lub do temperatury punktu Curie, w której usunięte zostają dane z nośnika magnetycznego.
Jedną z najbardziej widowiskowych metod sprzętowych usuwania danych jest metoda pirotechniczna, polegająca na zniszczeniu nośnika wybuchem. Pozostałe to metoda chemiczna, w której do kasowania danych używa się środowisk agresywnych chemicznie, i radioaktywna – technika oddziaływania na nośnik promieniami jonizującymi.
Ze względu na trudności techniczne, związane z wykorzystaniem niektórych metod sprzętowych usuwania danych, jedną z najpopularniejszych technik pozostaje namagnesowanie nośnika danych.

* Paweł Odor jest głównym specjalistą firmy Ontrack Odzyskiwanie Danych w Polsce