



Strefa druku



IT w małej i średniej firmie



Smartfony



Tablety



Notebooki

rozwiń

Niebezpieczeństwa związane z zaniechaniem utylizacji dysków

Niebezpieczne pozostałości

Opis eksperymentu, który pokazał jak niebezpieczne jest odsprzedawanie dysków twardych bez skutecznego zamazania na nich danych

AUTOR: szymon piłat, kamil kulesza

DODANO: 01.09.2006

TAGI: bezpieczeństwo danych, dyski twarde, utrata danych, utylizacja

LICZBA WYSWIETLEŃ: 130

Pliki komputerowe są dziś tym, czym kiedyś były dokumenty papierowe, teczki, archiwa itd. Kiedyś sensacją wzbudzało odnalezienie tajnych akt, dziś natomiast równie wielkie emocje wywołuje wyciek poufnych danych elektronicznych. Najbardziej znane przykłady to dyski z Ministerstwa Spraw Zagranicznych, które odkupił Jerzy Urban, lub pliki z komputera Aleksandry Jakubowskiej, które stały się ważnym materiałem dowodowym w głośnej sprawie.

Problem jest istotny nie tylko dla polityków, gdyż komputery i Internet wykorzystuje się do przechowywania i przesyłania informacji związanych z operacjami bankowymi, działalnością firm, stanem majątku oraz prywatnymi sprawami z życia osobistego. Zachowanie ich poufności jest sprawą wysokiej wagi, bo stanowi



tak o bezpieczeństwie państwa, jak i firm czy zwykłych ludzi.

Karty płatnicze na śmietniku

Postanowiliśmy sprawdzić, czy użytkownicy komputerów dbają o własne dane z dysków, które zamierzają sprzedać, oraz co można znaleźć na nośnikach dostępnych na rynku wtórnym. Zbadaliśmy, czy i jak przeciętny użytkownik komputera usuwa pliki przed sprzedażą "twardziela". W ramach projektu badawczego przeprowadzonego w Instytucie Podstawowych Problemów Techniki Polskiej Akademii Nauk przeprowadziliśmy eksperymenty obejmujące różne aspekty ochrony informacji. Koncentrowaliśmy się na sprawdzeniu, jakie dane można znaleźć na używanych dyskach twardych.

Podobny eksperyment przeprowadzili przed trzema laty w USA Simson L. Garfinkel i Abhi Shelat z Massachusetts Institute of Technology. W ciągu dwóch lat zebrali oni 158 dysków twardych. Dyski kupowali w sklepach z używanym sprzętem komputerowym firm, które wyprzedawały towar, oraz na aukcjach internetowych (eBay). Na dyskach znaleźli m.in. ponad 5000 numerów kart kredytowych (jeden z napędów pochodził z... bankomatu). Prawie wszystkie nośniki zawierały jakieś informacje, a jedynie mały ich odsetek był prawidłowo oczyszczony z danych w taki sposób, że nie udało się niczego odzyskać (9% dysków, czyli 12



sztuk). Dotyczył on jednak realiów amerykańskich. Postanowiliśmy przekonać się, na ile tamte rezultaty pozostają aktualne w naszym kraju.

Dlaczego kasowanie plików jest nieskuteczne?

Kasowanie plików poprzez przesuwanie ich do systemowego Kosza pozostawia dane w zasadzie nietknięte. Technicznie rzecz biorąc, kasowanie to niewielka modyfikacja w tablicy alokacji plików. Podobnie przedstawia się sprawa z formatowaniem. Każdy program przeznaczony do odzyskiwania sformatowanych danych potrafi je całkowicie odtworzyć. Dopiero zastosowanie specjalnej aplikacji skutecznie usuwa pliki.

Publikacji wyników grupy z MIT towarzyszył duży rozgłos. Sprawdziliśmy więc, czy ówczesna wrzawa wokół uzyskanych w USA wyników wpłynęła w znaczący sposób na zachowanie użytkowników komputerów w Polsce, czyli czy sytuacja u nas jest równie katastrofalna.

Myśleć jak przestępca

W trakcie przygotowań do eksperymentu staraliśmy się zdobyć jak najwięcej używanych dysków twardych. Następnie odzyskiwaliśmy z nich dane, sprawdzaliśmy, czy zdobyte pliki są poufne oraz czy mogą stanowić niebezpieczeństwo w razie dostania się w niepowołane ręce. Nasze działania miały jednocześnie być symulacją postępowania potencjalnego napastnika, jednak wszystkie odzyskane i przeanalizowane dane nie były wykorzystywane do żadnych celów poza naukowymi. Każdy dysk, który był później odsprzedawany na aukcjach, został przez nas zabezpieczony programami do kasowania danych, tak aby nikt nie był w stanie odtworzyć oryginalnych informacji.

Jednym z założeń eksperymentu była kwota, którą przeznaczaliśmy na projekt. Budżet ograniczyliśmy do około 1500 zł, przyjęliśmy bowiem założenie, że potencjalny przestępca dysponuje skromnymi środkami.

Użyty przez nas sprzęt jest ogólnodostępny i względnie tani, a zastosowane oprogramowanie do pobrania z Internetu. Użyty przez nas metodę mógłby zastosować każdy, kto ma podstawową wiedzę informatyczną, także osoby, których podstawową motywacją działań jest zysk, osiągnięty nawet metodami niezgodnymi z prawem, jak np. oszustwa i wyłudzenia.

200 zdobytych dysków

Zakładaliśmy, że część użytkowników komputerów będzie przezorna i skasuje pliki lub sformatuje dyski, dlatego nasz eksperyment zaczęliśmy od wyboru oprogramowania, które miało odzyskiwać informacje. Przeprowadziliśmy trwające ponad tydzień testy tego rodzaju software'u. Spośród ogólnodostępnych aplikacji wyłoniliśmy trzy najlepsze naszym zdaniem programy, które odzyskują dane utracone na skutek kasowania, formatowania lub uszkodzenia systemu plików.

Badane dyski twarde były głównie kupowane na aukcjach internetowych, choć udało się uzyskać też sporą liczbę napędów od różnych ofiarodawców. Po przebadaniu nośniki były z powrotem wystawiane na aukcjach, ponieważ zasoby finansowe, jakimi dysponowaliśmy, były niewielkie. W sumie, dysponując kwotą 1500 zł, udało się nam pozyskać ponad 200 dysków!

Kluczowym elementem działań był sam proces odzyskiwania danych ze zdobytych nośników. Po podłączeniu badanego dysku najpierw kopiowano zapisane na nim dane (jeśli takowe były). Następnie, korzystając z oprogramowania do odzyskiwania danych, odtwarzano pliki, które przechowywano na dysku przed jego formatowaniem. Wszystkie zdobyte informacje gromadzono na wyodrębnionym komputerze, wyposażonym w dyski twarde o dużych pojemnościach.

Odtworzona biografia

Oto informacje o pewnej osobie, utworzone na podstawie danych odzyskanych z dysku kupionego na aukcji internetowej. Dane pozwalające na identyfikację tej osoby zostały zmienione.

Anna mieszka na Żoliborzu. Ma 25 lat, jest bardzo pogodną i ładną dziewczyną o rudych włosach. Ukończyła filologię ukraińską na UW. Zajmuje się redakcją i korektą tekstów. Do tej pory pracowała w kilku wydawnictwach, obecnie stara się o pracę w kolejnym (niestety, w CV, które wysłała e-mailem popełniła literówkę). Jedną z jej pasji są sporty ekstremalne, szczególnie bungee jumping i spadochroniarstwo. Jej zainteresowania to również literatura i historia współczesna. Ma konto w banku Inteligo, często odwiedza portal wizaz.pl poświęcony kosmetykom. Lubi zwierzęta, ma gekona, którego uwielbia. Często udziela się na forum hodowców gekonów. Na dysku przechowywała również wiele zdjęć (niektórych z nich na pewno nie pokazałaby znajomym), olbrzymie archiwum e-maili, kompletne dane adresowe i osobowe (swoje oraz rodziny, chłopaka i innych osób). Anna sprzedała swój dwugigabajtowy dysk, gdy zmieniała komputer.

Źródło pochodzenia dysku: Allegro.pl



©Copyright 1993-2013 Burda Communications Sp. z o.o.