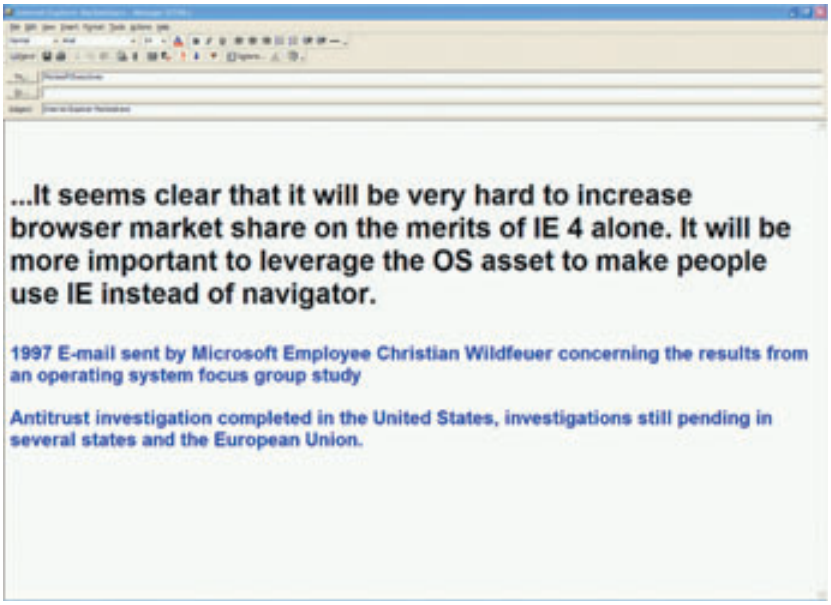
Fot. Victorpr/Dreamstime

Paweł Odor*

Elektroniczni detektywi i wirtualni przestępcy

W 1997 roku do komputera usiadł Christian Wildfeuer. Treść wiadomości e-mail, którą po chwili zredagował i wysłał do swojego przełożonego, miała przysporzyć największemu producentowi oprogramowania na świecie wielu problemów. Brzmiała następująco:



Specjaliści Computer Forensics to wysokiej klasy eksperci, którzy korzystając z najnowszych osiągnięć technologicznych i zaawansowanej wiedzy w zakresie odzyskiwania danych dostarczają elektroniczne środki dowodowe.

Jej adresatem okazał się Bill Gates. Ta wiadomość pocztowa była dowodem w śledztwie prowadzonym przeciw monopolistycznym praktykom Microsoft Corporation w 1997 r. Odtworzona wiadomość pocztowa była dowodem na to, że włączenie przeglądarki Internet Explorer do systemu operacyjnego Windows było świadomą decyzją zarządu Microsoft Corporation mającą na celu zdobycie przewagi rynkowej nad konkurencyjnym produktem firmy Netscape.

Załączenie do akt sprawy powyższej wiadomości jako dowodu nie byłoby możliwe, gdyby nie dziedzina o tajemniczej nazwie – Computer Forensics.

Elektroniczni detektywi

Elektroniczni detektywi, czyli specjaliści Computer Forensics to wysokiej klasy eksperci, którzy korzystając z najnowszych osiągnięć technologicznych i zaawansowanej wiedzy w zakresie odzyskiwania danych dostarczają elektroniczne środki dowodowe tzn. dane w wersji elektronicznej zabezpieczone w taki sposób, aby były wiarygodne dla sądu.

Patrząc na odsetek dokumentów tworzonych wyłącznie w formie elektronicznej (70 proc.), z których 90 proc. nigdy nie jest drukowana, widzimy, że nie branie pod uwagę dowodów elektronicznych mogłoby spowodować, że wiele możliwych do rozwiązania spraw sądowych nigdy nie znalazłoby swojego końca.

Detektyw komputerowy znad Wisły

Powinniśmy raczej powiedzieć – znad Rawy, rzeki przepływającej przez Katowice. Właśnie w tym mieście działają elektroniczni detektywi Ontrack – firmy, która jest największym na świecie dostawcą usług CF, zarówno na całym świecie, jak i w tej części Europy, również w Polsce. Zapleczem technologicznym dla specjalistów Computer Forensics Ontracka jest opisane w poprzednim numerze „e-Faktów" katowickie laboratorium odzyskiwania danych Ontrack.

Polscy detektywi, dzięki współpracy z innymi oddziałami korporacji rozwiązują najcięższe przypadki związane z przestępczością komputerową. Jako jedyna firma w Europie pracują również transgranicznie – rozwiązują w jednym czasie przypadki przestępstw elektronicznych mające miejsce w różnych krajach jednocześnie.

Przykładem takiej sprawy może być przypadek koncernu francuskiego. W kwietniu 2005 r. eksperci działu Ontrack Electronic Investigations w Polsce otrzymali zlecenie tzw. akwizycji danych polegającej na skopiowaniu informacji elektronicznych w taki sposób, aby nie straciły one wartości dowodowej (a więc z zachowaniem tzw. sumy kontrolnej, której niezmieniona wartość gwarantuje brak ingerencji w zawartość zabezpieczanych plików elektronicznych). Identyczną operację przeprowadzili w tym samym czasie specjaliści Ontracka w Niemczech i Francji. Zleceniodawcą był zarząd francuskiej firmy farmaceutycznej.

Powodem do zatrudnienia „elektronicznych detektywów" było podejrzenie o malwersacje finansowe zarządu polskiego oddziału firmy, którego członkowie otworzyli firmę pośredniczącą w zakupach dla koncernu oferując towary po cenach nierynkowych i powodując w ten sposób powstanie wymiernych strat dla firmy.

Operacja zebrania materiałów dowodowych przeprowadzana w każdym z trzech krajów tej samej nocy odbyła się w obecności prawnika, notariusza i służby ochrony mienia. „Elektroniczni detektywi" Ontracka skopiowali dane z każdego komputera w firmie oraz z urządzeń służących do archiwizacji danych firmowych. Każde z miejsc pracy zostało sfotografowane.

Dane z Niemiec i Polski trafiły następnie do Francji. Podobnie jak dane z siedziby głównej koncernu, zostały poddane analizie. Wynikało z niej, że przypuszczenie działania na szkodę koncernu przez zarząd polskiego oddziału firmy jest prawdziwe.

Po sprawdzeniu wyników analizy zarząd francuskiego koncernu zdecydował się na zmianę całego personelu polskiego oddziału (zarządu i pracowników). Nie wiadomo, czy członkom zarządu wytoczono procesy.

Przestępczość elektroniczna w Polsce

Molestowanie seksualne w Internecie, pedofilia, celowe usuwanie danych przez zwalnianych pracowników oraz sabotaż to najczęściej popełniane przestępstwa komputerowe. Oficjalnie w Polsce rocznie zgłaszanych jest blisko 1000 przestępstw komputerowych, nieoficjalnie może być ich wielokrotnie więcej. Większość z tych spraw stanowią proste z technicznego punktu widzenia przypadki np. łamania praw autorskich producentów oprogramowania. Najtrudniejszych i największych spraw, które dotyczą zwykle dużych korporacji, największych spraw kryminalistycznych czy ważnych zdarzeń z punktu widzenia bezpieczeństwa narodowego, jest znacznie mniej. Eksperci Ontracka oceniają, że nie więcej niż 30–40 rocznie. Te, które zostają zlecane elektronicznym detektywom trafiają do katowickiego laboratorium odzyskiwania danych Ontracka.

Metody ich wykrywania są u nas już dobrze znane i dostępne. Jednak większość zainteresowanych, często również informatyków, nie jest tego świadoma. Dowodem na to może być głośny swego czasu spór pomiędzy założycielami serwisu internetowego Wirtualna Polska a jego głównym udziałowcem – Telekomunikacją Polską SA. Spór rozwiązano na koszt założycieli, którzy otrzymali ogromne odszkodowanie po kilku latach batalii sądowej. Prawdopodobnie sprawa mogła być zakończona dużo wcześniej, gdyby skorzystano wtedy z usług elektronicznych detektywów. Sprawa Wirtualnej Polski – jednego z największych portali w kraju, jest przykładem straty, jaką poniosła jedna ze stron, spowodowanej brakiem świadomości istnienia usług dostarczania elektronicznych środków dowodowych w Polsce.

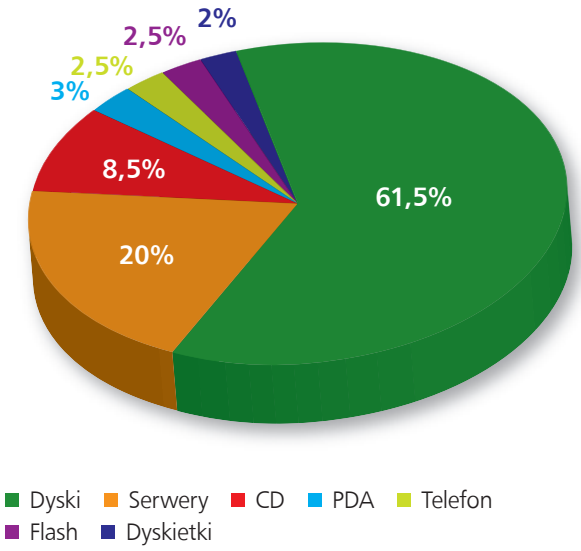
Większościowy udziałowiec portalu wp.pl zawarł porozumienie z posiadaczami udziałów stanowiącymi mniejszość, w którym zobowiązał się do odkupienia reszty udziałów po określonym czasie. Cena wykupienia udziałów miała zależeć bezpośrednio od ilości użytkowników portalu.

Po upływie terminu, w którym miało nastąpić odkupienie udziałów okazało się, że mniejszościowy pakiet udziałów był droższy niż łączna kapitalizacja dwóch najbardziej konkurencyjnych portali.

Większościowy udziałowiec wycofał się z podjętego zobowiązania. Podjęte zostały działania prowadzące do pogorszenia kondycji finansowej portalu, a w konsekwencji do doprowadzenia portalu do upadłości.

Mniejszościowi udziałowcy zdecydowali się na zweryfikowanie zawartości komputera przenośnego jednego z managerów.
Popełniono jednak błąd. Komputer zawierający dane, które miały stanowić materiał dowodowy w sprawie, zdeponowano u notariusza. Zanim to jednak nastąpiło osoby te otwarły pliki, w których znajdowały się strategiczne dla sprawy informacje – materiały mające świadczyć o próbie doprowadzenia portalu do upadłości. Niestety, otwierając dokument zmieniono jego atrybuty włącznie z datą utworzenia, pozbawiając dokument wartości dowodowej.
W przypadku zlecenia takich działań firmie Ontrack, specjaliści zabezpieczyliby nośnik, wykonaliby kopię jego zawartości bez uruchamiania plików oraz umożliwiliby osobom prowadzącym dochodzenie wgląd do zawartości plików. W ten sposób wartość dowodowa zgromadzonego materiału zostałaby zachowana. Finał sprawy opisał w październiku 2005 Forbes.

Gdzie są te dowody?



Najwięcej przestępstw komputerowych popełniają zwalniani pracownicy. Zwykle kasują dane firmowe lub przekazują je konkurencji. Najwięcej dowodów można znaleźć w korespondencji elektronicznej.
Większość, bo aż 61,5 proc. dowodów elektronicznych zapisywana jest na dyskach twardych komputerów. Drugie w kolejności są serwery (20 proc.) zawierające zarówno archiwa przesyłanych przez pracowników wiadomości e-mail, jak i te, na których znajdują się np. zapisy z kamer monitorujących ulice. W dalszej kolejności nośnikami elektronicznych dowodów popełnionych przestępstw są płyty CD, pamięci przenośne i pamięci telefonów komórkowych. Statystycznie najmniej dowodów przestępczości elektronicznej znajduje się na wycofywanych już z użycia tradycyjnych dyskietkach.
Często dowody w formie elektronicznej są tak przekonywujące, że strony sporu nie decydują się na wejście na drogę sądową, rozwiązując sprawy polubownie. Niezależnie jednak od dalszych losów sprawy specjaliści Computer Forensics muszą postępować zgodnie z procesem umożliwiającym dostarczenie danych elektronicznych w takiej formie, która gwarantuje, że dane nie zostały zmienione i są autentyczne.

Proces Computer Forensics

Jednym z najważniejszych etapów procesu CF są konsultacje prowadzone przez elektronicznych detektywów przed przystąpieniem do właściwych działań Computer Forensics.
Podczas konsultacji specjaliści CF muszą precyzyjnie ustalić czego i w jakim kontekście szukają. Nie jest bowiem możliwa precyzyjna analiza całej zawartości zasobów np. średniego przedsiębiorstwa bez ściśle określonych kryteriów wyszukiwania.
Po konsultacjach następuje zbieranie danych, a więc kompletowanie informacji z różnych nośników danych, na których mogą się znajdować – począwszy od komputera, poprzez serwer firmowy a skończywszy np. na telefonie komórkowym osoby biorącej udział w sprawie. Eksperci Ontracka wykonują zawsze dwie kopie danych. Wszystkie prace i analizy przeprowadzane są na drugiej kopii. Wykonaniu kopii towarzyszy zawsze wykonanie image nośników oraz ustalenie sum kontrolnych.
Kolejnym etapem jest przeszukiwanie danych pod kątem zadanych kryteriów. Często zanim dojdzie do przeszukiwania danych należy je odkodować, a jeszcze częściej odzyskać. Jedną z najpopularniejszych metod zacierania śladów przez przestępcę komputerowego jest bowiem umyślne kasowanie danych.
Wyniki analizy i przeszukiwania danych zawarte zostają w specjalistycznym raporcie, wykorzystywanym następnie w sądzie lub w negocjacjach dotyczących ugodowego sposobu rozwiązania sprawy.
Jednak właściciele firm czy indywidualni użytkownicy komputerów nie muszą się martwić. Ogrom prac opisanych powyżej spoczywa zawsze na elektronicznych detektywach. Mogą pomóc w najtrudniejszych chwilach. Wystarczy tylko … o nich wiedzieć.

* Paweł Odor jest głównym specjalistą odzyskiwania danych i Computer Forensics firmy Ontrack Odzyskiwanie Danych