Ontrack Investigations

zagrożenia IT dla organizacji i przedsiębiorstw

Jarosław Kubica

Referat został opracowany na podstawie danych korporacji **KrollOntrack** oraz firmy **Ontrack odzyskiwanie danych** będącej wyłącznym dostawcą technologii Ontrack w Polsce i Europie Środkowo-Wschodniej.

Spis treści

W ciągu ostatnich kilku lat dyski twarde (i inne nośniki danych) stały się pierwszoplanowymi bohaterami kilku bardzo znanych spraw. Krótko wspominając dane z komputera Minister Jakubowskiej w sprawie Rywina; 12 dysków, które z magazynów MSZ trafiło do redakcji „NIE"; notebook Prezesa Wirtualnej Polski (www.wp.pl), który został zdeponowany u osoby zaufania publicznego.

Dane i informacja stanowią dziś nie tylko o jakości spraw karnych, mogą zostać wykorzystane również przez organizacje jak i zwykłych użytkowników w celu dochodzenia własnych praw. Niestety biorąc pod uwagę tylko wymienione poprzednio 3 sprawy okazuje się, że nie do końca wiemy w Polsce jak posługiwać się komputerem, jak postępować z danymi niejawnymi, czy jak zabezpieczyć dowody występujące w formie elektronicznej.

1 Pojęcie Computer Forensics

Computer Forensics (dostarczanie elektronicznych środków dowodowych) obejmuje poszukiwanie dowodów nadużyć i przestępstw dokonanych z użyciem komputera lub innego urządzenia elektronicznego. Computer Forensic jest często związany z odtworzeniem zdarzeń w czasie, poszukiwaniem danych skasowanych czy wyszukiwaniem informacji niedostępnych dla typowego użytkownika, czy administratora systemu.
Produktem końcowym Computer Forensics są dane przygotowane w taki sposób, aby stanowiły materiał dowodowy w prowadzonych dochodzeniach.

Podobnie jak w przypadku dowodów występujących w formie tradycyjnej (odciski palców czy dokumenty w formie papierowej) odnalezienie i przygotowanie w odpowiedniej formie dowodów elektronicznych obarczone jest ryzykiem ich zniszczenia, np. zatarcia lub takiej ingerencji w dane, która uniemożliwi przedstawienie danych jako wiarygodnego dowodu w prowadzonym procesie sądowym. Dokonując niewłaściwych czynności w trakcie zabezpieczania danych na nośniku można doprowadzić do ich zniszczenia, równie łatwo jak można zatrzeć ślady odcisków palców.
Należy zdawać sobie sprawę, że każde włącznie komputera pozostawia swój ślad w danych, a więc zmienia zawartość nośnika. Każde otwarcie pliku, czy uruchomienie aplikacji powoduje zmiany informacji przechowywanej na nośniku.

Najczęstsze przypadki wykorzystania Computer Forensics

Jak wynika z danych KrollOntrack istnieje kilka typowych kategorii przypadków, w których wykorzystywane są działania mające na celu dostarczenie dowodów przestępstw popełnionych z użyciem komputera. Należą do nich przypadki oszustwa, fałszerstwa

komputerowego, niszczenia danych lub szpiegostwa przemysłowego, włamania do systemu, jak również sabotażu komputerowego oraz cała gama przestępstw związanych z pornografią i molestowaniem seksualnym.
Najczęstsze przypadki jakie trafiają do polskiego laboratorium związane były z celowym niszczeniem danych np. przez zwolnionego pracownika. Kolejne przypadki dotyczyły fałszowania dokumentów (np. zaświadczeń o chorobach do WKU, prawa jazdy, dowodów osobistych), wzorów pieczęci urzędowych. Do laboratorium Ontrack trafiła również sprawa związana z popełnieniem zabójstwa. Specjaliści Ontrack odtworzyli i analizowali zapis z kamer przemysłowych monitorujących jedną z ulic w Łodzi.

2 Proces Computer Forensics

Proces CF to zbiór następujących po sobie czynności, których wykonanie gwarantuje dostarczenie organom ścigania, a także osobom prowadzącym dochodzenie, danych o pełnej wartości dowodowej. Na proces Computer Forensics składają się: zbieranie informacji, odtwarzanie i odzyskiwanie danych oraz ich analiza. Wynikiem działania jest raport ekspertów.
Rozpoczęcie procesu CF poprzedzone jest dokładnym zapoznaniem się specjalistów ze sprawą. Klient musi przekazać ekspertom możliwie dużo informacji o prowadzonym postępowaniu tak aby możliwe było podjęcie decyzji jakie nośniki mogą zawierać istotne informacje.

2.1 Zbieranie informacji

Podstawową zasadą na etapie zbierania informacji jest zabezpieczenie oryginalnych nośników jak typowych dowodów. Następnie wykonuje się co najmniej dwie kopie danych. Kopie powstają bez uruchomienia systemu operacyjnego urządzenia, na którym mogą znajdować się potencjalne dowody. Procedura taka spowodowana jest faktem, iż w momencie uruchomienia systemu operacyjnego oryginalnego urządzenia zmienia się dotychczasowa zawartość danych znajdujących się na nośniku (dysku, pamięci itp.).
Zabezpieczanie danych, jako dowodów, dotyczy zarówno komputerów osobistych, przenośnych jak i serwerów plików (poczty), baz danych oraz wszystkich kopii bezpieczeństwa.
W zależności od typu postępowania zabezpiecza się także dane z urządzeń przenośnych PDA, płyt CD/ DVD i wszelkich pamięci przenośnych.

Po przygotowaniu dwóch kopii zapasowych otrzymanego nośnika specjaliści Computer Forensics zabezpieczają jedną z nich w sposób identyczny do tego w jaki zabezpieczony został oryginalny nośnik.
Wszelkie prace są prowadzone na drugiej kopii. Każda operacja podjęta przez specjalistów CF musi być szczegółowo udokumentowana, a każde udostępnienie nośnika lub informacji musi być zarejestrowane.

Suma kontrolna

Każde kopiowanie danych musi być zabezpieczone wyliczeniem sumy kontrolnej. Można na jej podstawie określić czy opisywana przez nią struktura była modyfikowana. Proces ten polega na powtórnym wyliczeniu sumy kontrolnej. Jeżeli zgadza się z pierwotną wartością, oznacza to, że mamy do czynienia z oryginalną wersją cyfrowego zapisu.
W czasie tego procesu stosuje się specjalne urządzenia uniemożliwiające jakikolwiek zapis na oryginalny nośnik.

Najczęstsze nośniki dowodów elektronicznych

Najpopularniejszymi nośnikami dowodów elektronicznych trafiającymi do firmy KrollOntrack w analizowanym okresie były dyski twarde komputerów osobistych (61,5%), serwery (20 % - w tym serwery pocztowe 7% oraz pozostałe serwery - np. zapisujące dane z kamer monitorujących ulice - 13%), płyty CD (8,5%), notatniki elektroniczne (3%), pamięci przenośne (2,5%), telefony (2,5%), dyskietki (2%). Większość serwerów trafia do ekspertyzy wraz z kopiami bezpieczeństwa.
Każdy z nośników musi zostać zabezpieczony w sposób odpowiedni do jego indywidualnych właściwości np. w przypadku dysków twardych odbywa się to za pomocą wygenerowanej podczas kopiowania sumy kontrolnej.
Niezależnie jednak od sposobu zbierania informacji, zasady zabezpieczania dowodów wymagają ochrony oryginalnego nośnika oraz wykonania pełnej kopii danych bez żadnej ingerencji w oryginał. Dodatkowo konieczne jest zastosowanie metod gwarantujących identyczność danych (np. przez wykonanie wspomnianej wcześniej sumy kontrolnej). Jakikolwiek błąd na tym etapie pracy może skutkować nie tylko utratą krytycznych danych, ale również odrzuceniem dowodów przez sąd.

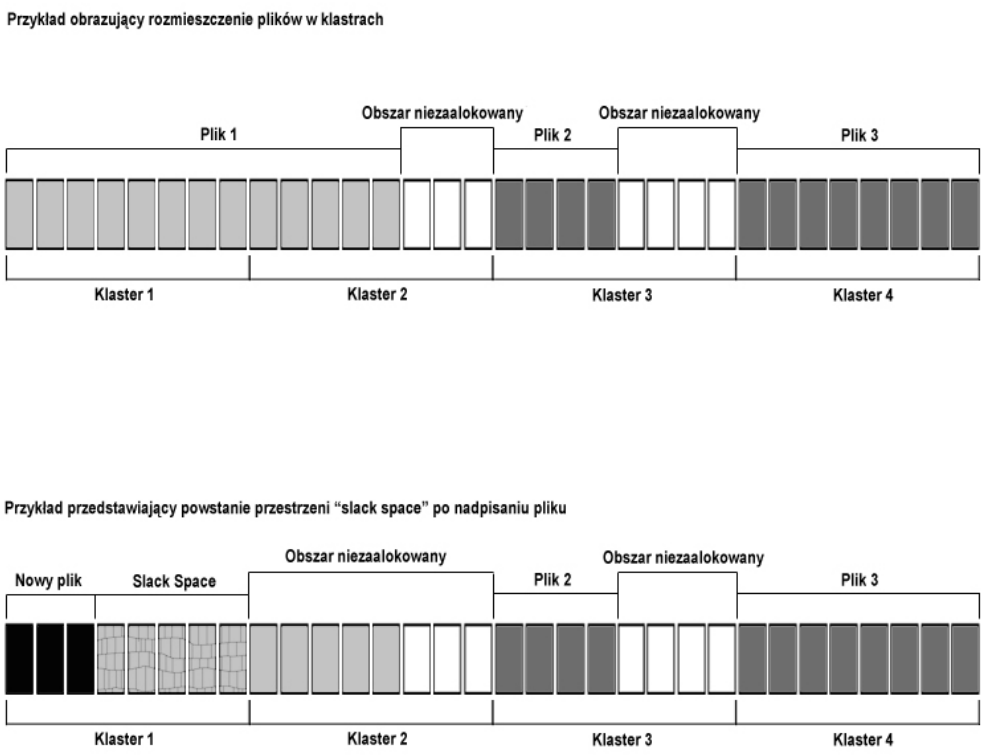
W szczególnych przypadkach, kiedy dane zostają zabezpieczane w wielu lokalizacjach – specjaliści Computer Forensics zwracają szczególną uwagę na synchronizację czasową. W ten sposób udaje się uniknąć manipulowania danymi mogącymi posłużyć jako dowód w prowadzonym dochodzeniu.

2.2 Odtwarzanie i odzyskiwanie danych

Dane pobrane z nośników zawierają najczęściej ogromną ilość informacji, z których część z punktu widzenia prowadzonego dochodzenia jest nieprzydatna. Wyłowienie interesujących danych jest często szukaniem igły w stogu siana. Przed przystąpieniem do analizy należy sobie zadać fundamentalne pytanie – czego szukamy.
Sytuację dodatkowo może skomplikować fakt, że nośnik zawiera dużą ilość danych niewidocznych dla użytkownika, a dostępnych dopiero w procesie odtwarzania danych (np. skasowanych, ukrytych lub zaszyfrowanych). Dzieje się tak często w momencie gdy oprócz celowo skasowanych danych nastąpiło uszkodzenie logiczne bądź fizyczne nośnika. W takiej sytuacji nim specjaliści Computer Forensics przejdą do analizy danych znajdujących się na nośniku muszą najpierw odzyskać utracone wcześniej informacje. Specjaliści w procesie odtwarzania danych docierają również do tzw. „slack space" – sektorów i klastrów resztkowych, które mogą być nieocenionym zbiorem informacji dla prowadzących śledztwa czy dochodzenia, szczególnie w przypadkach, w których nastąpiło nadpisanie danych dowodowych czyli zapisanie na nie nowych informacji.

Slack space

Najmniejszą jednostką informacji, którą operuje system plików jest klaster danych. Najczęściej po usunięciu pliku dane nie są kasowane – a jedynie zajmowane przez nie klastry (sektory) są zaznaczane jako wolne. W czasie normalnej eksploatacji komputera wolne klastry są nadpisywane nową informacją. Każdy nadpisujący plik zawiera określoną ilość klastrów danych. Ostatni klaster zawiera przypadkową ilość danych (jeżeli dane nie zostały dobrane w specyficzny sposób). Statystycznie każdy nowy plik pozostawia niewykorzystaną połowę ostatniego klastra (czyli około 2KB danych). 2KB może zawierać 2048 znaków zawartych w pliku txt, (czyli ponad 1 stronę tekstu) które mogą przesądzić o winie lub uniewinnieniu podejrzanych przeciw którym gromadzone są materiały dowodowe.



Rys. 2 Mechanizm powstawania „slack space".

Szczególnym przypadkiem odtwarzania danych może być odzyskiwanie danych z fizycznie uszkodzonego nośnika. Średnia światowa skuteczność odzyskiwania danych w profesjonalnym laboratorium wynosi 76%. Składają się na nią również najcięższe przypadki, w których nośniki zostały celowo zniszczone fizycznie, spalone czy zalane wodą. W większości tego typu przypadków dane nie są tracone bezpowrotnie.

2.3 Analiza

Kolejnym krokiem po odtworzeniu danych w procesie Computer Forensics jest ich analiza. Typowe poszukiwanie danych polega na dostosowaniu wszystkich zebranych danych do formatu pozwalającego użytkownikowi na łatwy dostęp do informacji (odszyfrowanie, pominięcie nietypowych aplikacji, ujednolicenie formatu). Praca specjalisty CF na etapie analizy danych polega na odpowiedzi na kluczowe pytania (kto, co i kiedy) oraz na odtworzeniu kolejności krytycznych zdarzeń.

Najczęstsze rodzaje danych analizowanych w procesie Computer Forensics

Dostarczając dowodów przestępczości elektronicznej specjaliści CF najczęściej operują na następujących kategoriach danych:

- dane pocztowe – najczęstsza kategoria danych, które stanowią materiały dowodowe w procesie Computer Forensics. W ich przypadku zabezpieczenie dowodów polega prócz zabezpieczenia plików pocztowych na konkretnym komputerze, również zabezpieczeniu dostępu do serwerów poczty elektronicznej,
- dane bieżące - np. dokumenty pakietu Office,
- dane odtworzone i odzyskane – skasowane lub uszkodzone wcześniej przez użytkownika,
- dane zaszyfrowane przez właściciela i udostępnione po złamaniu zabezpieczeń.
- dane zawarte w logach systemowych i metadanych – analiza powłamaniowa

Na tym etapie prac przydatne są narzędzia ułatwiające konwersję danych. Aplikacje takie pozwalają między innymi na bardzo wygodne wyszukiwanie informacji, zaznaczanie i komentowanie odnalezionych danych oraz przygotowywanie szczegółowych raportów z przeprowadzonych prac.
Najpopularniejsze narzędzia (aplikacje) stosowane w procesie CF opisane zostały w punkcie 3 niniejszego raportu.

Elementy procesu analizy danych

Proces analizy danych obejmuje:

- odtwarzanie istotnych zdarzeń z uwzględnieniem ich chronologii (wizyty na stronach internetowych, komunikacja pocztą elektroniczną, zmiany dokumentów, kasowanie danych, szczegóły penetracji systemu itp.),
- poszukiwanie dokumentów zawierające słowa kluczowe związane ze sprawą, a wskazywane najczęściej przez organa śledcze,
- poszukiwanie kopii istotnych dokumentów oraz ich wcześniejszych wersji,
- sprawdzanie istnienia na nośniku i zaistnienia operacji z wykorzystaniem programów kasujących dane,
- analizę autentyczności danych oraz znaczników czasowych.

2.4 Raport

Wynikiem pracy specjalistów Computer Forensics jest szczegółowy raport zawierający informacje o odnalezionych danych istotnych dla prowadzonej sprawy. Elementem raportu powinno być także osadzenie w czasie kluczowych zdarzeń.

Jako, że treść raportu musi być ściśle skorelowana ze sprawą konieczna jest bliska współpraca specjalistów w laboratorium z osobami prowadzącymi sprawę.
Elementem współpracy laboratorium Computer Forensics i klienta jest także przedstawianie wyników prac w sądzie. Specjaliści CF przywołani przez prokuratora i sądy dla wydania opinii prezentują materiał dowodowy jako tzw. biegli ad-hoc . Pomimo faktu, że nie wszystkie sprawy trafiają na wokandę, wszystkie czynności w ramach procesu Computer Forensics muszą być prowadzone w taki sposób, aby wartość dowodowa zgromadzonego materiału była niepodważalna. Na świecie tylko około 20% spraw prowadzonych przez specjalistów CF ma finał w sądzie. Często potrzebne są jedynie np. dowody winy pracownika pozwalające pracodawcy na uszczelnienie systemu dostępu do informacji.

Jak wspomniano wcześniej jedną z najczęściej analizowanych kategorii danych w procesie Computer Forensics są pliki poczty elektronicznej. Wydaje się, że ta kategoria danych nie ustąpi z pierwszego miejsca w ciągu najbliższych lat. Już dziś szacuje się, że tylko w Stanach Zjednoczonych przeciętny pracownik używający poczty elektronicznej otrzymuje i wysyła łącznie między 60 a 200 wiadomości pocztowych dziennie. The International Data Corporation ocenia, że globalnie tylko w ciągu jednego dnia ogólna liczba przesyłanych informacji poczty elektronicznej to 36 miliardów dokumentów elektronicznych.

Przesyłane drogą elektroniczną informacje (dane) od komputera nadawcy, przez jego serwer pocztowy trafiają do sieci skąd wędrują do serwera pocztowego odbiorcy kończąc swą podróż w komputerze adresata.

Na każdym z powyższych etapów istnieje możliwość wykorzystania tych danych w procesie dowodowym zmierzającym do wykrycia „przecieku" informacji, czy to poprzez odtworzenie treści podejrzanej wiadomości, czasu jej, wysłania czy też innych jej cech.

Korporacyjne serwery pocztowe przechowują wiadomości wszystkich pracowników, którzy korzystają z poczty elektronicznej. Zgodnie z wymogami Disaster Recovery Plans sporządzane i przechowywane są kopie zapasowe zasobów gromadzonych na serwerach firmowych. Często specjaliści CF stają przed koniecznością analizy wielu milionów informacji pocztowych niejednokrotnie pochodzących z różnych serwerów (ich kopii bezpieczeństwa).

3 Uwarunkowania prawne Computer Forensics

Właściwe przepisy prawne

Przestępstwa przeciwko ochronie informacji uwzględniające przestępczość komputerową regulują w Polsce Artykuły 267 – 269 oraz Artykuł 287 Kodeksu Karnego.

Art. 267. § 1. Kto bez uprawnienia uzyskuje informację dla niego nie przeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym.

§ 3. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1 lub 2 ujawnia innej osobie.

§ 4. ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

Art. 268. § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na komputerowym nośniku informacji, sprawca podlega karze pozbawienia wolności do lat 3.

§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 4. ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

Art. 269. § 1. Kto, na komputerowym nośniku informacji, niszczy, uszkadza, usuwa lub zmienia zapis o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub administracji samorządowej albo zakłóca lub uniemożliwia automatyczne gromadzenie lub przekazywanie takich informacji, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.
§ 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając nośnik informacji lub niszcząc albo uszkadzając urządzenie służące automatycznemu przetwarzaniu, gromadzeniu lub przesyłaniu informacji.

Art. 287. § 1. Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przesyłanie informacji lub zmienia, usuwa albo wprowadza nowy zapis na komputerowym nośniku informacji, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
§ 2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
§ 3. Jeżeli oszustwo popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego.

Zdaniem prawnika

Jednym z najczęstszych przypadków wykorzystania Computer Forensics jest naruszenie zasad obowiązującej umowy o pracę często przyjmujące postać sabotażu lub celowego usunięcia danych.

Katarzyna Strażecka, Strażeccy i Wspólnicy: „Wymazanie danych z elektronicznego nośnika informacji np. twardego dysku komputera należącego do pracodawcy wyczerpuje znamiona przestępstwa z art. 287 par. 1 kodeksu karnego - tzw. oszustwa komputerowego. Przestępstwo to zagrożone jest karą pozbawienia wolności od 3 miesięcy do 5 lat. W wypadku mniejszej wagi sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
W świetle regulacji kodeksu pracy wymazanie lub kradzież danych może stanowić podstawę do rozwiązania umowy o pracę przez pracodawcę bez wypowiedzenia w trybie art. 52 par. 1 pkt. 1 kodeksu pracy, albowiem takie zachowanie stanowi ciężkie naruszenie obowiązków pracowniczych.

Zgodnie z art. 114 kodeksu pracy pracownik, który wskutek niewykonania lub nienależytego wykonania obowiązków pracowniczych ze swej winy wyrządził pracodawcy szkodę, ponosi odpowiedzialność materialną. Pracownik ponosi odpowiedzialność za szkodę w granicach rzeczywistej straty poniesionej przez pracodawcę i tylko za normalne działania lub zaniechania, z którego szkoda wynikła. Odszkodowanie ustala się w wysokości wyrządzonej szkody, jednakże co do zasady nie może ono przewyższać kwoty trzymiesięcznego wynagrodzenia pracownika w chwili wyrządzenia szkody. Zgodnie z art. 122 kodeksu pracy jeżeli szkoda wyrządzona przez pracownika została umyślnie, pracownik jest zobowiązany do jej naprawienia w pełnej wysokości.

Ponadto art. 11 ustawy o zwalczaniu nieuczciwej konkurencji (Dz.U. 197 poz.1661 z 2002 r.) określa, iż czynem nieuczciwej konkurencji jest przekazanie, ujawnienie lub wykorzystanie cudzych informacji stanowiących tajemnicę przedsiębiorstwa. Art. 11 ustawy stosuje się również do osób, które świadczyły pracę na podstawie stosunku pracy lub innego stosunku prawnego - przez okres trzech lat od jego ustania, chyba że umowa stanowi inaczej albo ustał stan tajemnicy.

Art. 23 wyżej wymienionej ustawy stanowi, iż "kto, wbrew ciążącemu na nim obowiązkowi w stosunku do przedsiębiorcy, ujawnia innej osobie lub wykorzystuje we własnej działalności gospodarczej informacje stanowiące tajemnicę przedsiębiorstwa, jeżeli wyrządza to poważną szkodę przedsiębiorcy podlega karze grzywny, karze ograniczenia wolności albo pozbawienia wolności do lat 2".

4 Computer Forensics na świecie

W 2001 roku Amerykańskie Stowarzyszenie Zarządzania (The American Management Association) przeprowadziło badania, z których wynikało, że 100 spośród 1000 firm, które znalazły się w rankingu magazynu Fortune musiało przedstawić w sądzie elektroniczne materiały dowodowe w sprawach dotyczących nie zachowania warunków umowy o pracę.

Branża Computer Forensics na świecie

Firma *KrollOntrack* - największa firma Computer Forensics na świecie, w 2003 roku rozwiązała tylko w USA ponad 500 spraw Computer Forensics. Jej największym klientem było FBI. Firma działa w kilkunastu krajach na całym świecie w tym w Polsce – jej przedstawicielem jest *Ontrack odzyskiwanie danych*. Polski przedstawiciel światowego potentata współpracuje w zakresie CF m.in. z *Departamentem Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego i Policją*.

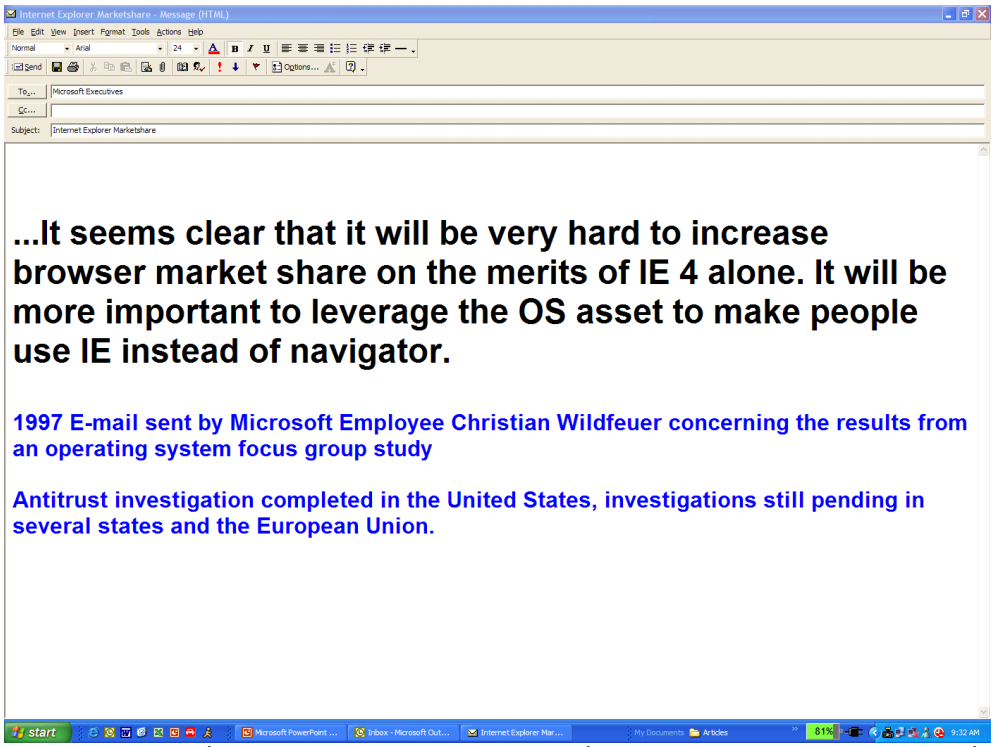
Do światowych liderów branży CF obok *KrollOntrack*, który dzięki globalnemu zasięgowi usług jest największą firmą w branży CF, należą *Computer Forensics Inc*, największe firmy konsultingowe (*KPMG, PriceWaterhouse Coopers, Deloitte&Touche, Ernst&Young*) specjalizujące się w tzw. Forensic Accounting oraz *Data Recovery Services Inc*.
Drugą grupę firm w branży CF stanowią producenci oprogramowania. Największymi z nich są *Guidance Software* – producent EnCase (firma od 2003 wprowadziła usługi CF), *Access Data* – producent narzędzia FTK oraz firma *NIST*.

Największym rynkiem usług Computer Forensics są obecnie Stany Zjednoczone.

Przykłady zastosowania Computer Forensics

a. Microsoft – Netscape

Wiadomość pocztowa odnaleziona przez specjalistów Computer Forensics była dowodem w śledztwie prowadzonym przeciw monopolistycznym praktykom Microsoft Corporation w 1997 roku. 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.



Rys. 2 Koronny dowód na to, że włączenie przeglądarki w środowisko systemu operacyjnego było świadomą decyzją w walce z konkurentem.

b. Wybory prezydenckie w USA w 2000 roku

Podczas wyborów prezydenckich w Stanach Zjednoczonych w 2000 roku konsorcjum utworzone przez największe amerykańskie media zleciło firmie KrollOntrack weryfikację wyników wyborów na Florydzie (USA).

Specjaliści KrollOntrack stworzyli kopie czterech twardych dysków znajdujących się w biurze Katherine Harris - ówczesnego Sekretarza Stanu na Florydzie. Istniało podejrzenie, że Republikanie użyli komputerów rządowych do prowadzenia kampanii wyborczej.
Przeanalizowano dostępne i odzyskane dane pod kontem 91 słów kluczowych. Firma KrollOntrack po około 20 godzinach dostarczyła konsorcjum kompletny raport z działań Computer Forensics.

c. „bomba zegarowa" sprawa prowadzona przez FBI i Prokuratora Federalnego USA

Sprawa wytoczona została pracownikowi dużej korporacji w Stanach Zjednoczonych. Pracownik został oskarżony o umyślne spowodowanie utraty strategicznych danych korporacji co spowodowało znaczne straty firmy, a w efekcie zwolnienie 100 pracowników.
Po analizie wszystkich danych znajdujących się na serwerach pocztowych oraz koncie pocztowym podejrzanego pracownika specjaliści KrollOntrack dostarczyli dowodów winy.
Okazało się, że pracownik, jeszcze przed zwolnieniem opracował program komputerowy, który niszczył dane elektroniczne. Program umieścił na serwerze firmowym. Okazało się, że narzędzie działało na zasadzie bomby zegarowej. „Bombę" aktywował nieświadomie jeden z pracowników logując się po określonym czasie na serwerze firmowym. Specjaliści wykazali winę zwolnionego pracownika obalając główny argument obrony, jakoby dane firmowe zostały skasowane przypadkowo. Wykazali dodatkowo, że na prywatnym komputerze oskarżonego znajdowały się dane identyczne z tymi, które posłużyły do stworzenia groźnego programu. Pracownicy KrollOntrack przedstawili materiał dowodowy w sądzie.

5 Computer Forensics w Polsce

Według danych Komendy Głównej Policji, wykrywalność przestępstw komputerowych sięga w Polsce ponad 70%. Pamiętajmy jednak, że zdecydowana większość działań Computer Forensics odbywa się na poziomie B2B i B2C i dzięki ugodom ostatecznie nie trafia na wokandę ani do prokuratury.

Świadomość usług Computer Forensics w Polsce praktycznie nie istnieje. Pozwala to przypuszczać, że rok rocznie z powodu niskiej świadomości dostępności usług CF poszkodowanych zostaje wiele firm, instytucji i osób prywatnych.

Case studies

W ciągu ostatnich dwóch lat w Polsce pojawiło się kilka głośnych spraw dotyczących Computer Forensics, które szczególnie zwróciły uwagę opinii publicznej.

a. Dysk twardy Minister Jakubowskiej

Wiadomość pocztowa wysłana przez Minister Jakubowską, która została odzyskana ze sformatowanego dysku twardego pozwoliła na ustalenie przebiegu wydarzeń w jednym z wątków afery korupcyjnej.
Biorąc pod uwagę, że większość opublikowanych danych pochodziła z poczty elektronicznej dziwi fakt, że nie zabezpieczono kopii serwera pocztowego Ministerstwa. Pomimo stosowania danych komputera osobistego – poczta jest również przechowywana w innych miejscach.

b. Dyski wykradzione z Ministerstwa Spraw Zagranicznych

Brak zabezpieczenia zużytych nośników i monitorowania dostępności do nich mógł doprowadzić do pogorszenia stosunków międzynarodowych.

c. Sprawa komputera przenośnego prezesa Wirtualnej Polski

Sprawa Wirtualnej Polski – jednego z największych portali w kraju jest przykładem straty jaką poniosła jedna ze stron spowodowanej brakiem świadomości istnienia usług CF 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.

BŁĄD:

Komputer, zawierający dane, które miały stanowić materiał dowodowy w sprawie, zdeponowano u notariusza. Niczym 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 MBM 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.
***