BEZPIECZEŃSTWO 2013 nr 4 (XIII)
TEORIA I PRAKTYKA

Przemysław Gwizd*

Analiza danych w informatyce śledczej

Pojęcie informatyki śledczej

Informatyka śledcza (*computer forensics*) to gałąź informatyki specjalizująca się w poszukiwaniu, zabezpieczaniu oraz przekazywaniu elektronicznych dowodów przestępstwa. Informatyka śledcza na ogół stara się niejako „cofnąć czas" w badanym urządzeniu, np. komputerze, poprzez odtworzenie zdarzeń, które miały miejsce w przeszłości, wyszukiwanie danych, które zostały skasowane, albo też znalezienie informacji zwykle z jakichś powodów niedostępnych dla użytkownika. Bardzo ważnym elementem informatyki śledczej jest odpowiednie zabezpieczenie śladów elektronicznych. Dane elektroniczne posiadają wartość dowodową tylko wtedy, gdy są identyczne, zgodne z oryginałem, co za tym idzie – nie są zmienione. Analiza danych pozyskanych z elektronicznych materiałów dowodowych jest procesem niezmiernie żmudnym ze względu na ilość danych, jakie możemy zebrać i na konieczność odseparowania danych istotnych od tych niemających znaczenia dla dalszego postępowania. Dowody elektroniczne podobnie jak tradycyjne dowody mogą ulec zniszczeniu, zatarciu czy modyfikacji poprzez wykonanie niewłaściwych czynności przy ich zabezpieczaniu lub obróbce. Nie wolno zapomnieć, że każde włączenie komputera pozostawia ślad, nawet otwarcie programu komputerowego również zmienia dane w nim przechowane. Należy podkreślić, że aby uzyskane przez informatyka śledczego dane w przypadku potwierdzenia podejrzenia popełnienia przestępstwa mogły posłużyć jako materiał dowodowy organom ścigania lub zostać przedstawione w sądzie, wszelkie czynności muszą być prowadzone zgodnie z obowiązującymi procedurami dopuszczalności materiałów dowodowych określonymi w prawie karnym procesowym. W szczególności materiał dowodowy musi być pozyskany zgodnie z prawem, musi być poddany odpowiedniemu badaniu, oczywiście z użyciem kopii, a nie oryginału, zgodnie z dokumentacją przedstawiającą wszelkie fazy postępowania z materiałem dowodowym,

* Mgr inż., Wydział Prawa i Administracji Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego.

tak aby nie można było przedstawić zarzutu manipulacji czy zmian w materiale, co podważałoby autentyfikację dowodu. Wszelkie prace muszą być wykonywane z zastosowaniem legalnych, licencjonowanych oprogramowań, ponieważ zarzut dotyczący legalności oprogramowania pozbawia wiarygodności osobę badającego i, co najważniejsze, dowodu elektronicznego. Celem informatyki śledczej jest zgromadzenie i analiza danych ze wszelkiego rodzaju urządzeń elektronicznych, które odpowiednio zabezpieczone w momencie pozyskania mogą stać się wiarygodnymi dowodami potwierdzającymi lub obalającymi podejrzenia nadużyć bądź przestępstw. Proces informatyki śledczej tradycyjnie możemy podzielić na cztery etapy: zbieranie informacji; odtwarzanie i odzyskiwanie danych; analiza; końcowy raport ekspertów. Szczegółowe omówienie poszczególnych etapów procesu informatyki śledczej zostaną przedstawione poniżej.

Computer Forensic w praktyce (przykłady zastosowania)

Elektroniczny materiał dowodowy ze względu na swą specyfikę polegającą na podatności na manipulacje wymaga właściwego obchodzenia się z nim, eksperci ze Stowarzyszenia Instytutu Informatyki Śledczej za kluczowy dla wiarygodności dowodów uważają etap zabezpieczenia nośników cyfrowych. Według ekspertów, nie ma precyzyjnych wytycznych, jak poprawnie je zabezpieczyć, dlatego stowarzyszenie opublikowało na swojej stronie internetowej zestaw najlepszych praktyk w tym zakresie, zostały one wybrane na podstawie doświadczeń polskich i zachodnich specjalistów. Według szefa instytutu Przemysława Krejza podstawą działania powinna być zasada: widzę wszystko i nie zmieniam nic. Niewiele osób jednak zna te praktyki, co powoduje błędy przy zabezpieczeniu i kompromitację zebranego materiału dowodowego.

Zasady naczelne informatyki śledczej według Stowarzyszenia Instytutu Informatyki Śledczej (na podstawie danych ze strony www.siis.org.pl)

1. Specjalistą/biegłym z zakresu informatyki śledczej powinna być osoba posiadająca stosowną wiedzę i doświadczenie.
2. Szczególnej wiedzy i doświadczenia wymagają działania podejmowane na oryginalnym materiale dowodowym.
3. Specjalista/biegły powinien przeprowadzać swoją ekspertyzę z wykorzystaniem rozwiązań technicznych uniemożliwiających modyfikację analizowanych danych.
4. Jeśli to tylko możliwe, wszelkie czynności biegły powinien przeprowadzać na odpowiednio wykonanych kopiach nośników, chyba że nie zachodzi taka potrzeba.
5. Zabezpieczenie danych z nośników dowodowych powinno odbywać się w sposób umożliwiający weryfikację ich integralności, w szczególności zaś z zastosowaniem sumy kontrolnej.
6. Czynności związane z zabezpieczeniem oraz analizą dowodów elektronicznych powinny być należycie dokumentowane w celu umożliwienia późniejszej weryfikacji dokonanych czynności.
7. Specjalista/biegły powinien potrafić wykazać, co działo się z powierzonym mu materiałem od momentu wejścia w jego posiadanie do momentu przekazania organom ścigania.

8. Szczególnej uwagi podczas zabezpieczania i analizy materiału dowodowego wymaga weryfikacja zgodności czasu wskazywanego przez urządzenie z czasem rzeczywistym.
9. W trakcie zabezpieczania dowodów należy przyjąć zasadę zabezpieczania od najbardziej ulotnych dowodów do najmniej ulotnych.
10. Czynności specjalisty/biegłego z zakresu informatyki śledczej w sposób szczególny wymagają zachowania tajemnicy zawodowej oraz przestrzegania przepisów o ochronie prywatności.
11. Specjalista/biegły dokonuje analizy tylko w zakresie zleconym mu przez organy ścigania lub wymiaru sprawiedliwości. Widząc konieczność rozszerzenia zakresu opinii, biegły może poinformować o tym organ zlecający opinię.
12. Specjalista/biegły powinien sformułować swoją opinię w sposób klarowny i w języku możliwie zrozumiałym dla organów procesowych ze wskazaniem użytych metod i narzędzi wraz z ich wersją.

Zasady opracował Arkadiusz Lach, UMK Toruń.

Informatyka śledcza jest orężem, którym dysponują organy ścigania i przedsiębiorcy w walce z nieuczciwą konkurencją, przestępcami wykorzystującymi brak dostatecznej wiedzy społeczeństwa na temat zabezpieczenia danych elektronicznych i sądzącymi, iż mogą bezkarnie wykorzystywać informacje zdobyte w sposób nielegalny. Dlatego też istnieją firmy, takie jak KrollOntrack, Mediarecovery oferujące cały zestaw usług służących Computer Forensics: od zbierania informacji, poprzez analizę danych, aż do raportu końcowego. Specjaliści z firmy Mediarecovery w przypadku poważnych podejrzeń np. przekrętów finansowych wynoszenia sekretów produkcyjnych bardzo często pracują w siedzibie firmy często nocą, a o takiej akcji wie na ogół tylko szef firmy, by wyeliminować możliwości zaalarmowania podejrzanych. Przedstawię poniżej studium przypadków wykorzystania informatyki śledczej przez największą na świecie firmę w branży Computer Forensics KrollOntrack jej klientem było FBI, posiada oddział w Polsce, który współpracuje z Departamentem Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego i Policją.

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.

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 kątem 91 słów kluczowych. Firma KrollOntrack po około 20 godzinach dostarczyła konsorcjum kompletny raport z działań Computer Forensics.

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. 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.

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 rokrocznie z powodu niskiej świadomości dostępności usług CF poszkodowanych zostaje wiele firm, instytucji i osób prywatnych[1].

W jednej z dużych firm IT kierownictwo zaczęło zauważać częste przypadki zwalniania się najlepszych przedstawicieli handlowych. Po przeprowadzeniu analizy informacji zawartych na firmowych komputerach udało się ustalić, że jeden z pracowników administracji firmy przekazywał wyniki finansowe, jakie uzyskiwali najlepsi handlowcy konkurencji. W odpowiedzi konkurencja prowadziła rozmowy w celu zwerbowania najlepszych do siebie.

Firma branży spożywczej przegrywa kolejne przetargi w różnych częściach kraju, zawsze z tym samym konkurentem. Różnica w cenach ofert jest niewielka. Kierownictwo firmy zaczyna podejrzewać przeciek. Analiza zabezpieczonych twardych dysków prowadzona była przez informatyków śledczych Mediarecovery m.in. za pomocą wyszukiwania słów kluczowych przez platformę EnCase. Ręczne przejrzenie dziesiątków tysięcy plików zapisanych na jednym tylko komputerowym dysku zajęłoby lata, wymagałoby armii ludzi, a większość informacji byłaby i tak nieczytelna bez odpowiednich narzędzi. Użycie EnCase pozwoliło stwierdzić, że wskazane słowa kluczowe występują między innymi w plikach HTML.

Nielojalny pracownik wykazał dużo sprytu. Przekazywał informacje o kwotach ofert przetargowych za pomocą popularnej gry online „OGame". Jest w niej opcja wysyłania wiadomości do innych graczy i to właśnie w ten sposób wyciekały z firmy informacje. Proces autentyfikacji i dokumentacji znalezionych dowodów nie byłby możliwy bez użycia narzędzi informatyki śledczej.

W firmie z branży ogrodniczej „wykradziono" całą bazę klientów. Przekazano ją prawdopodobnie konkurencyjnemu przedsiębiorstwu o podobnej nazwie. Specjalistom

[1] Powyższe przykłady zostały przygotowane na podstawie materiałów *Ontrack Investigations: zagrożenia IT dla organizacji i przedsiębiorstw* autorstwa Jarosława Kubicy.

Mediarecovery postawiono zadanie odnalezienia winnego w sposób niealarmujący pracowników. O sprawie wiedział jedynie szef. Po tygodniu udało się ustalić, na jakim stanowisku roboczym doszło do przegrania na płytę CD całej bazy klientów. Stwierdzono również, który użytkownik był zalogowany w trakcie tego wydarzenia.

W firmie branży informatycznej doszło do „wycieku danych". Przeprowadzono analizę firmowej sieci komputerowej z wykorzystaniem narzędzi informatyki śledczej. Poza ścisłym kierownictwem nikt nie wiedział o przeprowadzanej kontroli. Specjaliści ustalili, że dane wyciekały z komputera Prezesa. Kopiowano je na zewnętrzny nośnik. Stwierdzono, że informacje kopiowano poza standardowymi godzinami pracy w firmie. Kontrola w systemie HR pozwoliła wytypować osobę, której przyjścia i wyjścia do pracy w 100% pokrywały się z godzinami, w których dochodziło do wycieku. Zręcznym hackerem okazała się sprzątaczka.

Oprócz metody „na sprzątaczkę" popularna jest również metoda kradzieży danych „na ochroniarza". Z takim przypadkiem miał do czynienia w 2008 roku Urząd Miasta w Siemianowicach Śląskich. Ochroniarz podczas nocnej zmiany wyniósł komputer z wydziału komunikacji i więcej się nie pojawił. Szczęśliwie komputery urzędników obsługujących petentów to były jedynie końcówki robocze, a wszystkie dane kierowców przechowywane były w dobrze strzeżonej serwerowni.

W kilku firmach z różnych branż wykonywane przez księgowość przelewy nie trafiały na konta kontrahentów. Informatycy śledczy stwierdzili włamanie do systemu. Sprytni hakerzy zmieniali dane dotyczące adresata przelewu po zatwierdzeniu płatności przez księgową, zanim polecenie transakcji wychodziło do banku[2].

Zbigniew Engel informuje, że do analiz śledczych jego firma używa specjalistycznego sprzętu oraz oprogramowania. Podstawowym narzędziem informatyka śledczego jest broker uniemożliwiający ingerencje w dany nośnik, np. Tableu TK35es. Najczęściej wykorzystywany przez policję i informatyków śledczych jest program do analiz śledczych – EnCase Forensic.

Pozyskiwanie i zabezpieczanie dowodów elektronicznych

Dowód elektroniczny (*electronic evidence*) jest pojęciem dość szerokim, ponieważ zawiera w sobie dowody zapisane w formie elektronicznej związanej z komputerem oraz zapisy dokonywane przy użyciu innych urządzeń, np. kamer użytkowych, telefonów komórkowych, mogą to być zapisy analogowe bądź – co jest dziś bardziej rozpowszechnione – cyfrowe. W kryminalistyce można spotkać się z pojęciem elektronicznych śladów przestępstwa, które są dowodami elektronicznymi odwołującymi się do pojęcia śladów kryminalistycznych. Dowody elektroniczne należą do kategorii dowodów elektronicznych rzeczowych, ponieważ są nierozerwalnie związane z nośnikiem informacji, na którym są zapisane. Są też dowodami zmysłowymi albo

[2] Powyższe przykłady zostały przygotowane na podstawie wywiadu Przemysława Muszyńskiego ze Zbigniewem Engelem z dnia 31 sierpnia 2010 roku.

pojęciowymi, ponieważ dopiero ich odczytanie przez nasze zmysły wydobywa z nich cechy niezbędne do właściwej interpretacji dowodów lub odczyt informacji. Przy dowodach elektronicznych ze względu na łatwość kopiowania występuje poważny problem z odróżnieniem kopii od oryginału (potrzebne są dodatkowe zabezpieczenia). Z drugiej strony ta łatwość powielania chroni materiał dowodowy przed zniszczeniem (podczas pracy nad dowodami pracuje się na kopii). Występuje tu jeszcze jeden aspekt ze względu na gromadzenie materiału w wielu kopiach czasem przetrzymywanych w różnych miejscach, więc trudno je zniszczyć definitywnie. Ślady elektroniczne pojedynczej działalności można znaleźć w wielu miejscach równocześnie (komputer, serwer, kamera), co ułatwia ich właściwą autentyfikację. Ważna tutaj wydaje się myśl T. Hanauska, że każdy dowód zawiera treści informacyjne, lecz nie każda informacja ma znaczenie dowodowe.

Istnieją następujące rodzaje dowodów elektronicznych:

- dokumenty zdigitalizowane, np. zeskanowane księgi rachunkowe, księgi wieczyste, polecenia zapłaty;
- dane pochodzące z sesji IRC (Internet Relay Chat) zwane czatem;
- dane pochodzące z sesji ICQ (I Seek You) w Polsce najbardziej popularną wersją jest Gadu-Gadu, Tlen;
- pliki rejestrowe, w których system czasowo zapisuje informacje dotyczące uruchamianych programów. Pliki te są w formacie tekstowym, co ułatwia analizę systemu komputerowego;
- dane bilingowe zawierające numer stacji abonenta, jego adres, numery, z którymi uzyskał połączenie, datę oraz czas połączeń;
- zapisy urządzeń rejestrujących transakcje płatnicze (wypłaty z bankomatów, czynności płatnicze przez internet, sieci bankowe (SWIFT, ELIXIR), zakupy za pomocą kart kredytowych;
- wiadomości e-mail uzyskane podczas transmisji wiadomości;
- zapisy urządzeń kontrolujących dostęp do pomieszczeń – identyfikacja osób może polegać w tym przypadku – na wprowadzeniu odpowiedniego hasła, wykorzystaniu karty magnetycznej oraz wykorzystaniu metod biometrycznych (analiza linii papilarnych, głosu);
- dowody zawierające zapisy dźwięku, zapisy rozmów telefonicznych, automatycznych sekretarek, poczty głosowej, nagrania jakiejś osoby;
- animacje i symulacje komputerowe wykorzystywane na szeroką skalę w krajach anglosaskich mają zastosowane przy badaniu strzałów z broni palnej, wypadków drogowych;
- zapisy kamer użytkowych CCTV.

Od momentu zabezpieczenia dowodu elektronicznego każdy do niego dostęp musi być ewidencjonowany poprzez szczegółowe podanie: daty, danych personalnych osoby mającej kontakt z dowodem, określenia, jakie działania zostały wykonane i ich powód, z podaniem opisu sprzętu, jaki został użyty. Dowód elektroniczny musi być odpowiednio chroniony w pomieszczeniu z zabezpieczonym dostępem osób niepowołanych. Najczęstszym dowodem jest dysk twardy komputera oraz inne urządzenia, z których możemy odczytać dane. Najważniejszą zasadą przy pozyskiwaniu i odzyskiwaniu danych elektronicznych jest odpowiednie zabezpieczenie nośników, z których chcemy

odzyskać dane elektroniczne, jest to podstawa, od której zaczynamy odzyskiwanie danych. Taka czynność musi być przeprowadzona przed uruchomieniem systemu operacyjnego na komputerze analizowanym, gdyż uruchomienie takie może spowodować zmianę dotychczasowej zawartości danych, dla wyeliminowania możliwości zmiany stosuje się specjalne oprogramowanie oraz szczególną procedurę, która dokumentuje każde działanie z nośnikiem. Każda czynność, np. kopiowanie, musi być opatrzona w sumę kontrolną. Suma kontrolna to ta liczba uzyskana w wyniku wykonywania operacji matematycznych na przesyłanych danych. Suma taka pozwala na sprawdzenie, czy dana informacja została zmodyfikowana, jeżeli suma jest inna, oznacza to, że informacja jest zmieniona, jeżeli taka sama, to mamy pewność, że nie zostały zmodyfikowane dane na badanym sprzęcie. W zależności od konkretnego przypadku zabezpiecza się również dane na urządzeniach przenośnych typu CD/DVD oraz wszelkich pamięciach przenośnych. Sprawę komplikuje również to, że nośnik analizowany zawiera również dane niewidoczne dla użytkownika, a dostęp do nich jest na etapie analizy dysku przez eksperta. Dzieje się tak, gdy kasujemy na komputerze jakieś dane, np. muzykę, film czy dokument tekstowy. Jeżeli dany sektor w pamięci komputera nie zostanie zapisany przez inną informację, czyli nie zostanie zajęty przez inne dane to takie odtworzenie jest możliwe za pomocą specjalistycznych programów typu PC inspektor smart recovery 4.5: jest to program do odzyskiwania zdjęć z nośników danych. Pozyskane dane elektroniczne zawierają najczęściej ogromną ilość informacji. Ważne jest więc wyłonienie tych, które będą przydatne do dalszej analizy. Najważniejsze w wyłonieniu z tak dużej grupy informacji tych najbardziej potrzebnych jest zadanie sobie pytania, czego szukamy. W procesie odzyskiwania danych specjaliści docierają do sektorów i klastrów resztkowych, które czasami stają się bardzo ważnym źródłem informacji. Szczególnie gdy dana została nadpisana, czyli w miejscu jednej danej została wpisana inna dana. Klaster danych to najmniejsza jednostka informacji, należy zauważyć, że po skasowaniu dane nie są automatycznie kasowane, a jedynie klaster zostaje oznaczony jako wolny, gotowy do zapisu, więc komputer takie wolne klastry zapisuje nowymi informacjami i wtedy stare informacje uprzednio skasowane zostają utracone. Mogą tutaj występować dwa rodzaje przypadków. Pierwszy: gdy nowa informacja zajmuje więcej miejsca niż informacja stara, wówczas można zapełnić wszystkie klastry poprzedniej wiadomości i wówczas cała stara wiadomość została utracona. Drugi przypadek, kiedy nadpisany plik zawiera mniejszą ilość danych, niż poprzedni, czyli nadpisana informacja nie zajmuje całego klastra, wówczas można odczytać część starej informacji, która została wcześniej pozornie skasowana. Dane pobrane z nośników zawierają sporą ilość informacji. Możemy je podzielić na dane ulotne i nieulotne. Dane ulotne (*volatile data*) są to dane przede wszystkim zawarte w pamięci ulotnej RAM, czyli po wyłączeniu komputera informacje te zostają utracone. Dane nieulotne (*non-volatile data*) są to wszystkie dane zapisane przez system na dysku twardym komputera w różnych plikach. Nas najbardziej interesują oczywiście pliki poczty, dokumenty oraz kosz. Dane elektroniczne można teoretycznie pozyskać z każdego urządzenia elektronicznego. Są to kolejno: palmtop, komputer, aparat cyfrowy, telefon komórkowy, karty pamięci, serwery poczty, ogólnie każde urządzenie, które korzysta w swojej pracy z zapisywania danych w formie elektronicznej i ma możliwość połączenia się z internetem. Rozpatrując dowody elektroniczne, należy zdawać

sobie sprawę z ich specyfiki, np. możliwości przejęcia czyjejś tożsamości, ponieważ nie jest weryfikowana osoba, a jedynie wiedza umożliwiająca dostanie się do systemu komputerowego wiedzą tą może być np. hasło. Z tego powodu panuje pogląd, że samo zalogowanie do systemu nie jest identyfikacją osoby, przecież możliwe jest również obejście zabezpieczania. Kolejnym problemem jest również zakładanie kont mailowych na osoby z innymi danymi osobowymi oraz całkiem fikcyjne (*fake account).* Również problematycznie przedstawia się sprawa z IP komputera jego ustalenie nie wskazuje osoby korzystającej z komputera w określonym czasie i miejscu, a jedynie numer karty sieciowej ustalonej w jednostce roboczej. Jeszcze więcej trudności sprawiają:

- adresy dynamiczne IP komputerów;
- serwery Proxy;
- serwery anonimizujące.

Serwer Proxy jest to serwer, który pośredniczy pomiędzy komputerem użytkownika a internetem. Na tym serwerze przechowywane są kopie plików, które użytkownik ściąga z internetu, np. strony internetowe i inne dane ułatwiające kolejne logowanie na tych stronach.

Serwery anonimuzujące pośredniczą w przekazywaniu informacji między nadawcą a odbiorcą, usuwając jednocześnie dane, które pozwalają na identyfikacje nadawcy poza tekstem wiadomości. Możliwe jest podszywanie się pod inny komputer np. przez przejęcie adresu IP komputera, co jest wykonalne, kiedy zna się adres IP komputera, pod którego użytkownika chcemy się podszyć, oraz adres MAC (*media access control addresses*, numer identyfikacji karty sieciowej, nadawany przez producenta tej karty i ją indywidualizujący). Dla ustalenia właściwego stanu faktycznego bardzo korzystne jest łączenie dowodów elektronicznych pochodzących z różnych źródeł, którymi są czytnik kart dostępu, kamery umieszczone w newralgicznych punktach obiektu oraz indywidualne hasła. Główną zasadą przy zbieraniu informacji jest zabezpieczanie oryginalnych nośników w stanie nienaruszonym tak jak zwyczajnych dowodów. Następnie wykonuje się zwykle dwie kopie (na jednej będziemy pracować), drugą zabezpieczamy jak oryginał, kopie muszą powstać bez uruchomienia systemu operacyjnego danego urządzenia, mogą się tam bowiem znajdować dowody, które przy uruchomieniu mogłyby zostać zmodyfikowane i przez to straciłyby wartość dowodową. Powyższa procedura zabezpieczenia dotyczy: komputerów, serwerów plików, baz danych, kopii bezpieczeństwa, danych z urządzeń przenośnych, płyt CD/DVD, pamięci przenośnych, zapisu monitoringu, notatników elektronicznych, telefonów, palmtopów. Każdy z wymienionych nośników wymaga odpowiedniego dla siebie zabezpieczenia, przykładowo dla dysków twardych będzie to wyliczenie sumy kontrolnej. Suma kontrolna urządzenia służy do określenia, czy dany materiał został zmodyfikowany, czy też jest oryginalnym nośnikiem. Każde kopiowanie bowiem musi być zabezpieczone poprzez wyliczenie sumy kontrolnej, powtórne jej wyliczenie i porównanie z pierwotną wartością, jeśli się zgadza, to daje nam pewność, że mamy do czynienia z oryginalną wersją. Ogromną zaletą sumy kontrolnej jest fakt, że można ją wyliczyć w dowolnym momencie i tym samym wykazać, że dowód nie został zmodyfikowany.

Analiza danych w informatyce śledczej

Dzięki procesowi analizy śledczej uzyskujemy:

- chronologiczne odtworzenie działań użytkownika, czyli poczta elektroniczna, zmiany w dokumentach, odwiedzane strony internetowe;
- znalezienie poprzednich kopii najistotniejszych dokumentów;
- sprawdzenie, czy były wykorzystywane programy kasujące dane;
- autentyfikacja wykrytych danych.

Analiza śledcza powinna odpowiedzieć na pytania dotyczące wszelkich działań z dowodem elektronicznym, kto wykonywał operacje, w jakim zakresie, kiedy zostały zapisane, czyli pozwala na chronologiczne odtworzenie zdarzeń. Po zgromadzeniu danych możemy przystąpić do ich analizy. Jej metody będą uzależnione od typu danych: w przypadku analizy danych sieciowych ważne jest sprawdzenie danych między komputerem badanym a kopią danych na serwerach świadczących usługi sieciowe. Jeśli sprawdzamy dane sieciowe, to przy przeglądaniu logów usług sieciowych musimy zwrócić uwagę na nazwę użytkownika, datę oraz rodzaj zasobów, z których korzystał, należy przejrzeć też logi zapory ogniowej, serwerów proxy, zdalnego sterowania oraz wykrywanie włamań. Analizując dane na komputerze, należy wyselekcjonować informacje, które mogą być użyteczne, czyli wszystko, co mogło być związane z działaniem, podlega kontroli, więc należy przejrzeć uruchomione aplikacje wraz z ich połączeniami sieciowymi. Jeśli chodzi o dane zawarte na nośnikach pozyskanych wcześniej i zawierające pliki związane ze sprawą, zadanie to będzie żmudną pracą, zwłaszcza jeśli chodzi o ogrom plików zawartych na dyskach twardych. Jak już wspomniano, pracujemy na kopii w celu ochrony oryginalnego dowodu. Sprawdzamy, czy nie występują podejrzanie zaszyfrowane dane, przeszukujemy rejestr systemowy, aby znaleźć procesy, jakie zostały uruchomione podczas startu, jakie aplikacje zainstalowano oraz sprawdzamy, kto logował się do domeny. Po przeszukaniu plików pod względem ich związku z badaną sprawą analizujemy ich metadane. Ostatnim zadaniem jest wykorzystanie przeglądarek plików do sprawdzenia ich zawartości. Procedura szukania danych na komputerze osobistym uzależniona jest od systemu operacyjnego zainstalowanego na komputerze, jednak dla naszej pracy skoncentrujemy się na najbardziej popularnym systemie Windows, gdzie w dalszej części rozdziału przedstawię najpopularniejsze miejsca, gdzie można znaleźć ślady działalności użytkownika. Analiza zabezpieczonych i przygotowanych do badania danych jest to zadanie niezmiernie czasochłonne i wymagające dużego doświadczenia. Jeżeli chodzi o analizę danych w komputerze, to należy ją rozpocząć od sprawdzenia podstawowych plików:

- domyślny folder systemowy (ang. System Folder) jest to plik, w którym jest zainstalowany system Windows;
- profil użytkownika (ang. User Profile Folder) jest to folder, w którym przechowywane są informacje na temat użytkownika dla wartości analizy jest to jedno z ważniejszych miejsc, gdzie możemy zdobyć informacje o użytkowniku, jego ustawieniach i powstaniu dokumentów oraz ściąganych plików internetowych;
- pulpit (ang. Desktop), w początkowej fazie folder ten jest mały i tworzony jest podczas procesu powstawania profilu użytkownika;
- moje dokumenty (ang. My Documents), katalog przeznaczony na pliki tworzone przez danego użytkownika może zawierać podkatalogi pt.: Moja muzyka, Moje obrazy;

- temp (ang. Temporary) folder plików tymczasowych, są w nim np. przetrzymywane kopie otwartych dokumentów. Jest on wykorzystywany chwilowo do rozpakowania plików instalacyjnych, więc można tu znaleźć ślady po zainstalowanych aplikacjach;
- ulubione (ang. Favorites Folder) znajdziemy tutaj łącza do stron internetowych, które zostały zapisane przez danego użytkownika;
- ciasteczka (ang. Cookies Folder) folder, który zawiera pliki tekstowe. Plik ten kontroluje i monitoruje użytkowników, np. poprzez zapamiętywanie hasło i login do witryn internetowych;
- Katalog Historia (ang. History Folder) folder ten zawiera historie przeglądanych witryn;
- Tymczasowe pliki internetowe (ang. Temporary Internet Files) są tutaj kopie plików związane z odwiedzonymi stronami;
- Plik hibernacji (ang. Hibernation Files) wykorzystywany do usypiania komputera bez zamykania go. Hibernacja polega na tym, że cała pamięć RAM na czas uśpienia zostaje zrzucana do pliku. Wybudzenie to przywrócenie pamięci RAM z pliku. Dla analizy śledczej może to być cenne źródło informacji;
- Poczta elektroniczna, pliki te należą do najczęściej analizowanych danych. Z komputera nadawcy przez serwer pocztowy informacje trafiają do sieci, a następnie do serwera pocztowego odbiorcy. Na każdym z przedstawionych etapów istnieje możliwość odtworzenia danych z treści bądź czasu wiadomości. Niektóre korporacje przechowują kopie wiadomości wysłanych przez pracowników na serwerach firmowych;
- Steganografia to technika ukrywania informacji w plikach graficznych lub dźwiękowych, zaletą tej techniki jest możliwość przesyłania informacji oficjalnymi kanałami bez możliwości kontroli;
- Rootkity (ang. Rootkits), groźne programy z obcym kodem źródłowym, co może powodować zastępowanie plików oryginalnych bibliotek systemu, przez co są niewykrywalne przez większość programów antywirusowych;
- Kosz (ang. Recycle Bin) jest to folder, w którym umieszczone są usunięte przez użytkownika pliki, jest nieocenionym źródłem informacji.

Analiza danych i Data Mining

W dzisiejszym świecie analiza danych zdobywa coraz większą popularność jako narzędzie do sprawnego poruszania się po ogromnej ilości danych. Analiza danych oraz jej matematyczne modele są wykorzystywane praktycznie w każdej dziedzinie życia. Należy pamiętać, że wszędzie, gdzie istnieje dużo danych, które stanowią pewien ograniczony zbiór, możemy korzystać z matematycznych analiz, co ułatwia analizę zbioru danych. Należy zaznaczyć, że obecnie do szukania danych w zbiorach stosowane są dwa podejścia tradycyjne: eksploracja danych, czyli (EDA), oraz Data Mining.

W metodzie EDA badamy praktyczne zastosowania danych w odróżnieniu od metody Data Minig, gdzie badamy zależności między poszczególnymi danymi. Różnica również polega na sposobie analizowania danych i ich przeznaczeniu. Nacisk w tej metodzie jest postawiony na wynik naszego postępowania. Można powiedzieć, że

przy opracowaniu dobrej metody odpowiedzi, czyli takiej, która najbardziej nas satysfakcjonuje, można przy tym podejściu darować sobie wzajemne oddziaływanie między danymi, a skoncentrować się na wyniku i jego użyteczności. Mechanizm ten wykorzystany jest również w sieciach neuronowych, gdzie nie są analizowane współzależności pomiędzy zmiennymi. W metodzie (EDA) możemy zarówno zrobić bardzo zaawansowane wielowymiarowe zbiory danych, w których można zastosować np. analizę czynnikową lub skale wielowymiarowe, analizę kanoniczną, szeregi czasowe, analizę skupień, jak i mniej zawansowane badanie, które obejmuje rozkład zmiennych lub przeszukiwanie macierzy, szukając wartości, które odbiegają od ustalonych.

Natomiast Data Mining to proces badania dużych zasobów danych pozwalający różnym danym przyporządkować różne ważności dla konkretnego pytania, dla jakiego poszukujemy odpowiedzi w zbiorze zadań. Weryfikacja danych dla procesu badania dużych zasobów danych jest niezmiernie ważna, gdyż jeżeli działamy na danych zbieranych automatycznie często przez systemy, które dodatkowo pełnią funkcje archiwizującą dane, możemy spotkać się z przekłamaniami rzędu „minus lub znaczek" przy danej liczbowej dopisany do wartości liczbowej. Możemy również zredukować dane, czyli wyeliminować dane nieistotne; do tego celu stosujemy techniki statystyczne. Dlatego też należy pamiętać o tych błędach systemów, aby dobrze dobrać dane do analizy. Weryfikacja powoduje, że uzyskujemy właściwe wyniki, czyli poprawne i takie, które możemy wykorzystać w późniejszej pracy. Proces ten składa się z trzech etapów. Pierwszy to wstępne przeszukania, drugi: budowa modelu, trzeci: zastosowanie modelu. Przeszukanie danych obejmuje przekształcanie danych podzbiorów, rekordów oraz kolumn i pól wyboru, ogólnie mówiąc cech danych. Zaczynamy od etapu przeszukania, czyli przygotowujemy dane, czyścimy i przekształcamy je tak, aby odrzucić dane, które dla danego pytania nie są istotne, a pracować jedynie na danych istotnych. Sposób szukania danych w zbiorze zależy od zapytania, jakie wcześniej zadaliśmy dla danego zbioru danych, sposób szukania jest uzależniony również od pytania, na które chcemy odpowiedzieć. Możemy przeszukiwać zbiór różnymi technikami graficznymi i statystycznymi, jednak każda metoda powinna nas prowadzić do kolejnej fazy Data Mining, czyli do budowania modelu i oceny jego przydatności. Dane w zbiorach możemy również dzięki tej metodzie przedstawiać w sposób graficzny. Jest to korzystne ze względu na identyfikacje relacji między danymi lub identyfikacje danych, które są na pograniczu zbioru. Przedstawienie takie jest zdecydowanie lepszą metodą bardziej przemawiającą do analityka, który może łatwiej zaobserwować te zależności między danymi. W metodzie naszej występuje również technika wyróżniania, czyli wybieramy na wykresie pewną wcześniej określoną liczbę punktów i określamy cechy między naszymi wybranymi punktami lub traktujemy je jako grupę i określamy cechy pomiędzy nimi a wybranym przez nas układem odniesienia. Technika ta ma zastosowanie dla badania, np. ludzie mieszkający w mieście a ludzie mieszkający na wsi. Dla tych dwóch punktów możemy określić, jak wygląda zależność dla różnych zmiennych w wybranym zakresie zmiennych dla naszego przypadku możemy zadać pytanie, ilu ludzi przeszło z punktu A do punktu B, jaka jest migracja w którą stronę, jak dana grupa ludzi wybiera lokale, które kupuje lub wynajmuje, Okazuje się, że dzięki analizie tych danych można zaplanować budowę nowego osiedla, które będzie cieszyć się większą popularnością niż pozostałe. W tej fazie badania zbiorów tworzymy różne modele, po czym wybierany jest najlepszy z nich, czyli taki, który da

najbardziej prawdziwą odpowiedź układu na zadany zbiór danych (próbę danych), często do weryfikacji modelu stosowane (ang. *competitive evaluation of models*) są sposoby porównania różnych modeli i wyboru najodpowiedniejszego dla danego pytania. Kolejną fazą stosowania Data Mining jest podstawienie do znanego już wcześniej wybranego algorytmu, czyli modelu przeszukiwania danych, nowych danych, które właśnie badamy, a ich wynik będzie wnioskiem.

Metoda (Bootsrap Aggregating) zaproponowana przez Breimana polega na wielości przewidywań wniosków uzyskanych z wielu modeli tego samego typu dla różnych zbiorów oraz wielu modeli różnego typu dla jednego zbioru danych, metoda ta pomaga poprawić modele, ich dokładność, zastosowanie tej metody również organiczna wariancje poszczególnych danych w zbiorze. Przy modelowaniu zmiennych ilościowych ta metoda powoduje uśrednianie (*averaging*), a w przypadku zmiennych jakościowych powoduje głosowanie (*voting*).

Metoda (*boosting*). Metoda ta jest bardziej skomplikowana niż przedstawiona wyżej, ale jej struktura jest podobna, w praktyce często ta metoda jest wykorzystywana do rozpoznania tekstu. Metoda ta polega na zbudowaniu wielu modeli i wyznaczeniu odpowiedniej wagi dla każdej danej. Pierwszy model posiada równe wagi, później zmieniamy je, wyznaczamy błąd wersji próbnej, który jest uzależniony od zastosowanego modelu. Wyznaczamy te dane, które mają największe błędy dla tego badania i stosujemy dla nich inne wagi, procedurę powtarzamy, aż osiągniemy zadowalające wyniki. Końcowym etapem stosowania tej metody jest analiza wyników, do których podchodzimy bardzo nieufnie, gdyż należy je poddać np. krzyżowej ocenie, która odpowie na pytanie, jak pewny wynik otrzymaliśmy i może dać odpowiedź, jaki model najlepiej zastosować do dalszej analizy danych.

Sieci neuronowe klasyfikowane są jako techniki analityczne wzorowane na funkcji uczenia, podobnie jak działa mózg, co za tym idzie, takie sieci neuronowe są zdolne do przewidywania na podstawie wcześniej dostarczonych danych, ten proces nazywamy w tym przypadku uczeniem sieci neuronowej. Sieci budowane są etapami: pierwszy polega na zbudowaniu określonej liczby warstw, która posiada pewną liczbę neuronów. Ta struktura jest uzależniona od zjawiska, które chcemy badać. Ten proces nie jest łatwy, bo na początku mamy więcej pytań niż odpowiedzi, ale pojawiły się już programy sztucznej inteligencji, co w znaczny sposób ułatwia dobór odpowiedniej struktury sieci do zjawiska, które chcemy za jej pomocą badać. Gdy już zbudujemy sieć, musimy ją „nauczyć", czyli przepuścić przez nią przypadki, które są podobne do naszego oraz dla pewnych brzegowych danych będą mieć takie same wartości, jakie my chcemy mieć dla naszych. Różne dane przyporządkowują im różne wartości, więc proces uczenia polega na dopasowaniu do konkretnych zależności między danymi odpowiedniej wagi. Możemy sprawdzić efekt naszej pracy poprzez doprowadzenie zbioru danych do naszej sieci i zadanie jej jakiegoś pytania, na które znamy odpowiedź, niezwiązanego z naszym pierwotnym problemem, a mającym za zadanie sprawdzić działanie sieci. Sieć tak zbudowaną można w przybliżeniu określić jako model. Jednak nie jest to ujęcie tradycyjne, ponieważ takie wymaga opisu zależności za pomocą wzorów matematycznych. Sieci neuronowe zatem traktujemy przy analizie jako pudełko, do którego coś wkładamy, a wyjmujemy coś zupełnie innego. Jeżeli wyciągamy z pudełka to, co nam odpowiada, to sieć jest dobra i możemy włożyć naszą niewiadomą, jeżeli z pudełka wyciągamy niezadawalające dane, to zmieniamy

sieć czyli model i zabawa zaczyna się do początku. Sieci te mogą być wykorzystywane do przeszukiwania zbiorów, aby znaleźć te zmienne, które zostały zadane. Zaletą sieci jest ich wszechstronność, gdyż mogą one aproksymować jakąkolwiek ciągłą funkcję, w związku z tym nie stawiamy hipotez badanego modelu. Wadą jest fakt, iż dane wyjściowe mają ścisłą korelację z danymi wejściowymi.

Typologia nadużyć komputerowych według Petera Grabosky'ego

W związku z informatyzacją życia i postępem technologicznym wciąż pojawiają się nowe przestępstwa popełniane z użyciem komputera, dlatego też organy ścigania ciągle unowocześniają metody ich wykrywania. Każdy człowiek powinien zdawać sobie sprawę z zagrożeń, jakie niesie za sobą informatyzacja życia, która obok szeregu ułatwień przynosi również wiele nowych rodzajów przestępstw. Aby się ich wystrzegać, należy być świadomym, dlatego też istotna jest typologia nadużyć komputerowych (za: Peter Grabosky) przedstawiona poniżej:

Haking, czyli uzyskiwanie nieautoryzowanego dostępu do komputera, może to być np. dostęp do wielu komputerów lub włamanie do komputera i utrudnienie, a nawet uniemożliwienie korzystania z systemu. Jednym z pierwszych i najbardziej znanym hakerem jest Kevin Mitnick uważany za bohatera, który obecnie zajmuje się bezpieczeństwem informacji firmy konsultingowej i jest autorem wielu książek.
Spam, czyli niechciane wiadomości poczty elektronicznej, często przekazywane w dużych ilościach.
Phishing, czyli rodzaj spamu zawierającego odsyłacze do stron internetowych, mogą one służyć do wyłudzenia danych osobowych, haseł do kont, numerów kart kredytowych, Kliknięcie w taki link może prowadzić do zainfekowania komputera przez wirus. W wiadomości e-mail pochodzącej od rzekomo legalnej organizacji z linkiem do jej strony internetowej ofiara jest proszona o zalogowanie się i podanie ważnych informacji, np. numeru karty kredytowej, PIN.

Rodzaje złośliwych oprogramowań

- Wirus to program komputerowy, który może rozprzestrzeniać się z komputera do komputera oraz zmieniać inne programy bez zgody użytkownika.
- Robaki to programy podobne od wirusów, ale działają tylko przez sieć; często rozprzestrzeniają się przez pocztę.
- Wabitty – program mnożący plik aż do zapełnienia dysku.
- Trojany – program podszywa się pod nazwę funkcjonującego programu w komputerze, przez co nie jest zauważony przez użytkownika i potrafi zmienić częściowo działanie komputera.
- Spoofing – celowe przeinaczanie nazwy nadawcy i adresu informacji, aby okazać, że wiadomość pochodzi od kogoś innego
- Steganografia jest procesem ukrywania jednego obiektu w innym, np. pornograficzne zdjęcie dziecka ukryte w niewinnie wyglądającym obrazku z wakacji. Jest

wykorzystywana również przez terrorystów, np. działaczy Hamasu na Bliskim Wschodzie (często ukrywane są w ten sposób takie dane jak mapa czy instrukcja obsługi materiałów niebezpiecznych).
- Spyware jest to technika pozwalająca na monitorowanie czyjegoś komputera, np. program o nazwie „Loverspy" był ukryty w kartkach okolicznościowych i instalował się na komputerze, gdy adresat otworzył kartkę, dzięki czemu nadawca przejmował kontrolę nad komputerem.
- Kradzież usług jest to nielegalne nabywanie usług (telefon, internet) poprzez uzyskanie nielegalnego dostępu do centrali telefonicznej lub dostawcy usług internetowych.
- Fałszywe zamawianie towarów – korzystając z kradzionej karty kredytowej lub stosując inne umiejętności, łatwo jest zamówić online produkt, który zostanie dostarczony na tymczasowy adres, i uciec z towarem.
- Manipulacja cenami akcji – internet radykalnie zwiększył zdolność do rozprzestrzeniania się fałszywych pogłosek o wartości akcji będących przedmiotem obrotu na giełdzie.
- Oszpecanie witryny wraz z pojawieniem się Word Wide Web stało się popularną rozrywką hakerów. W 1996 roku szwedzkiej grupie hakerów udało się zmienić nazwę Centralnej Agencji Wywiadowczej.
- Kradzież danych. Jest mnóstwo rodzajów danych, które są atrakcyjne dla złodzieja: tajemnice handlowe, niejawne informacje wojskowe.

Rodzaje ataków przestępczych

Ataki przestępców chcących uzyskać korzyści materialne za pomocą sprzętu elektronicznego mogą przybrać cztery formy:
1) ataki na sprzęt i środowisko systemów wsparcia (Hardware),
2) ataki na oprogramowanie (Software),
3) ataki na media,
4) ataki na ludzi.

Ad 1. Bardzo często pojawiają się różne usterki sieci komputerowej, awarie serwera mogące świadczyć o tego rodzaju atakach. Należy wówczas sprawdzić dowody świadczące o uszkodzeniach fizycznych na PC, serwerach, urządzeniach peryferyjnych, liniach przesyłowych, liniach telekomunikacyjnych, światłowodach. Należy sprawdzić, czy uszkodzenie nie ma związku z czynnikami środowiskowymi, takimi jak zasilanie, wilgotność czy zmiana temperatury. Po znalezieniu uszkodzeń należy ustalić, czy powstały one w wyniku działań przypadkowych czy celowych. Wszelkie umyślne szkody spowodowane wandalizmem, sabotażem czy kradzieżą mogą być próbą ukrycia innego poważniejszego przestępstwa. W przypadku włamania właściwe zabezpieczanie dowodów fizycznych będzie polegało w szczególności na zwróceniu uwagi na: odciski butów, odciski palców, stłuczone szkło.

Ad 2. Drobne zmiany w kodzie mogą powodować poważne zmiany w oprogramowaniu, sprawcą może być haker lub pracownik biurowy (przykładowo sprzedawca, który ma wypłacaną prowizję od sprzedaży, wyliczaną na podstawie mnożnika premii

od 0,0005 wystarczy, że zmieni tę daną na 0,005 i jego dochody wzrastają dziesięciokrotnie).

Ad 3. Wszelkie media, począwszy od dyskietek poprzez taśmy magnetyczne oraz napędy ZIP, CD, DVD, dyski itd. Wszystkie te formy przechowywania informacji charakteryzują się niskim bezpieczeństwem ze względu na łatwość przenoszenia i kopiowania.

Ad 4. Bardzo ważnym elementem bezpieczeństwa w firmach są pracownicy i zaufanie do nich, które niestety w wielu przypadkach może zostać podważone z kilku powodów: chciwość, rodzina i problemy finansowe, sprawy polityczne, szantaż lub presja zewnętrzna. Często zdarza się, że przyzwoity człowiek znajduje się w pułapce, np. analityk systemów spotyka atrakcyjną kobietę, nawiązuję romans, po jakimś czasie okazuje się, że jej brat ma poważne długi hazardowe, dlatego ona prosi analityka o pomoc i udostępnienie bazy danych klientów do kopiowania, pracownik łamie zaufanie i ulega prośbie, nie zdając sobie sprawy z tego, że ta sytuacja została wcześniej ukartowana. Inny przykład: pracownik działu kryminalnego Policji dowiaduje się, że jego brat, który jest zawodowym kierowcą, prowadził samochód pod wpływem alkoholu (brat ma rodzinę na utrzymaniu), więc pomaga mu, usuwając elektroniczne dowody przestępstwa.

Inżynieria społeczna

Sporo teoretyków bezpieczeństwa komputerowego uważa, że szereg technicznych środków zaradczych dla zapewnienia bezpieczeństwa jest niewystarczający. Faktycznie mimo całego aparatu firewalls, haseł, urządzeń wykrywających włamania nadal najsłabszym ogniwem pozostaje człowiek. Jak stwierdził Kevin Mitnick w *The Art of Deception* (Wiley Publishing, 2002), uzyskał dostęp do większości systemów dzięki rozmowie z ludźmi, a nie dzięki nadzwyczajnej technice, cechą natury ludzkiej jest to, że ludzie chcą być pomocni, a inni mogą to wykorzystywać. Książki Mitnicka o inżynierii społecznej, sztuce przeprowadzenia rozmowy tak, aby udało się uzyskać identyfikatory, hasła lub poufne pliki powinny być lekturą menadżerów i badaczy przestępczości komputerowej. Jest kilka podstawowych scenariuszy dotyczących inżynierii społecznej:

1) ktoś wcześniej nie znany przedstawia się jako człowiek pracownika przez telefon i mówi, że jest w trudnym położeniu i pilnie potrzebuje jakiejś informacji;
2) rozmówca telefoniczny informuje, że jest ze zdalnej lokalizacji firmy i potrzebuje ważnych informacji natychmiast;
3) ktoś kontaktuje się przez telefon i twierdzi, że jest np. autoryzowanym sprzedawcą, a osoba, z którą się zwykle kontaktuje, jest poza biurem, zaś on potrzebuje pilnie jakiejś informacji;
4) rozmówca twierdzi, że jest z zarządu firmy i próbuje uzyskać informacje na poziomie pracownika.

Wspólnym elementem tych oszustw jest pilna potrzeba informacji w nagłych przypadkach i plan obejścia zwyczajowej procedury w firmie. W badaniu pracownika, który mógł nieumyślnie ujawnić ważne informacje, wymagany jest duży stopień

empatii badacza w celu pokonania wstydu i strachu pracownika. W wywiadzie należy ustalić datę i godzinę połączenia lub e-maila oraz sprawdzić, czy jest kopia dokumentu, jaką wiedzę na temat firmy posiadał rozmówca i czego dowiedział się podczas rozmowy.

Literatura

Mendell R., *Investigating computer crime in the 21ST Century*, Charles c Thomas Publisher LTD 2006.

Franklin C.J., *The Investigator`s guide to computer crime*, Charles c Thomas Publisher LTD 2006.

Bryant R., *Digital Crime*, John Wiley & Sons Ltd England 2008.

Grabosky P., *Electronic Crime*, Person Education 2007.

Marshall A., *Digital Forensics*, John Wiley & Sons Ltd England 2008.

Lach A., *Dowody elektroniczne w procesie karnym*, Wydawnictwo „Dom Organizatora, Toruń 2004.

Ernst & Young V Międzynarodowy Kongres Audytu Kontroli Wewnętrznej oraz Procedur Zwalczania Oszust i Korupcji, Kraków, 21 kwietnia 2006, http://webapp01.ey.com.pl/EYP/WEB/eycom_ download.nsf/resources/Informatyka_sledcza_TD_pl.pdf/$FILE/Informatyka_sledcza_TD_pl.pdf; dostęp: 10.10.2011.

Kubica J., *Ontrack Investigations zagroiżenia IT dla organizacji i przedsiębiorstw*, http://data.proidea.org.pl/confidence/1edycja/materialy/prezentacje/jaroslaw_kubica.pdf, dostęp: 12.12.2011.

Kim są informatycy śledczy?, wywiad ze Zbigniewem Engielem i Przemysławem Muszyńskim, 31 sierpnia 2010, dostęp: 12.12.2011. http://vbeta.pl/2010/08/31/kim-sa-informatycy-sledczy-rozmowa-ze-zbigniewem-engielem; Stat Soft Elektronic Statistics Texbook, http://www.data-mining.pl/textbook/stathome_stat.html?http%3A%2F%2Fwww.d ata-mining.pl%2Ftextbook%2Fstdatmin.html, dostęp: 12.12.2011.

Ustawa z dnia 6 kwietnia 1990 o Policji.

Ustawa z dnia 6 czerwca 1997 r., *Kodeks postępowania karnego*, Dz.U. z dnia 4 sierpnia 1997.

Ustawa z dnia 6 czerwca 1997 r., *Kodeks karny*, Dz.U. z dnia 2 sierpnia.