MAGAZYN

NR 25 / MARZEC 2015

www.magazyn.mediarecovery.pl

INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

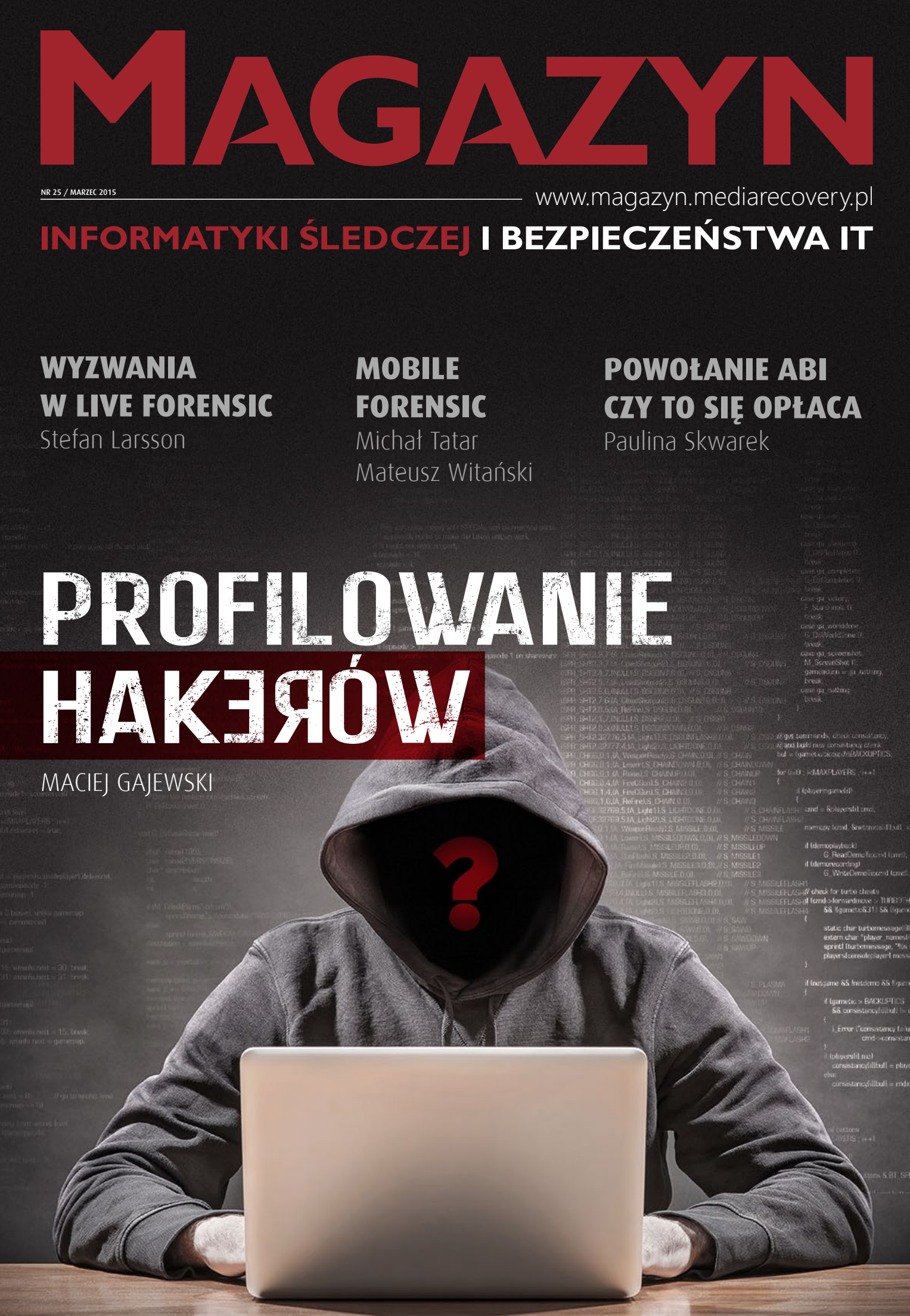
WYZWANIA W LIVE FORENSIC
Stefan Larsson

MOBILE FORENSIC
Michał Tatar
Mateusz Witański

POWOŁANIE ABI CZY TO SIĘ OPŁACA
Paulina Skwarek

PROFILOWANIE HAKERÓW

MACIEJ GAJEWSKI



Od redakcji

Przywykliśmy już do tego, że wszelkie ataki hakerskie rozpatrujemy pod kątem metod, narzędzi czy podatności wykorzystanych przez hakerów. Prasa specjalistyczna, portale tematyczne rozpisują się na ten temat szeroko i stosunkowo często. Bardzo rzadko (i nie w języku polskim) można spotkać opracowania dotyczące profilowania hakerów. Dlatego też niezwykle cieszymy się, że to na naszych łamach pojawia się tekst dotyczący tej właśnie tematyki. Artykuł Macieja Gajewskiego, jest jedynie wstępem do zagadnienia, jednak czyta się go z przyjemnością, a wciąga jak rasowa powieść kryminalna. Będziemy namawiać Autora do kontynuacji.

Profilowanie hakerów to nie jedyny temat w bieżącym numerze Magazynu. Zamieszczamy również artykuł „Wyzwania live forensic", który skupia się na konieczność i nieodzowności stosowania w analizach śledczych zarówno narzędzi, jak i możliwości wynikających z zabezpieczania danych z pracujących sieci i systemów. Ciekawym połączeniem praktyki i teorii, jest wspólny tekst Michała Tatara i Mateusza Witańskiego o alternatywnych metodach odczytywania danych z punktu widzenia biegłego. Tekst ten udowadnia, że w zakresie mobile forensics nie powiedziano jeszcze ostatniego słowa. Budujący dla nas jest fakt, że potwierdzają to polscy specjaliści. Adwokat Paulina Skwarek, specjalizująca się m.in. w ochronie danych osobowych rozważa co jest bardziej efektywne dla firm i instytucji: powołanie Administratora Bezpieczeństwa Informacji czy pozostawienie wszystkiego po staremu? Jak w większości przypadków każdy z wyborów ma swoje plusy i minusy.

Miłej lektury!

P.s.
Drodzy Czytelnicy, przypominamy, że jesteśmy otwarci na Wasze głosy, uwagi i opinie. Jeśli chcecie nam coś przekazać najlepiej zrobić to za pośrednictwem adresu e-mail: magazyn@mediarecovery.pl.

Profilowanie hakerów

Maciej Gajewski

Poniższy tekst jest wynikiem zainteresowania autora zjawiskiem hakera i hakingiem ze szczególnym zwróceniem uwagi na szerokie tło kulturowe i wynikłą z tego próbą zastanowienia się, czy można zastosować wiedzę o tego typu zjawiskach praktycznie, czyli np. w działaniach związanych z zapewnieniem bezpieczeństwa informacji. Nie myślę tu tylko o analizie ryzyka, ale o innych mechanizmach.

Chciałbym od razu zastrzec z uwagi na wielkość tego tekstu, że jest on tylko próbką zasygnalizowania tematyki bardzo mało obecnej w polskiej rzeczywistości, co należy ze smutkiem skonstatować. Osoby zainteresowanie tematyką zapraszam do kontaktu mailowego.

Podejrzewam, że wszyscy czytelnicy Magazynu zetknęli się z profilowaniem oglądając amerykańskie filmy i literaturę. W powszechnej świadomości od 1991 roku – pojawienia się na ekranach „Milczenia owiec" - obecne są mity genialnego zabójcy: doktora Hannibala Lectera i równie sprawnego genialnego policjanta – profilera – Agenta specjalnego FBI, Jacka Crawforda, postaci zbudowanej niczym składanka z prawdziwych amerykańskich tuzów profilowania.

Od tego czasu analizując produkty kultury popularnej możemy znaleźć wiele postaci i bohaterów wzorowanych na powyższych archetypach.

W popularnej powieści Zygmunta Miłoszewskiego „Gniew" występuje ktoś w rodzaju profilera i przez młodego prokuratora Falka traktowany jest jako hochsztapler. Czy naprawdę można tak łatwo odrzucić tego rodzaju działania?

Trochę historii

Literatura opisując historyczny rozwój metod, które współcześnie określa się mianem profilowania, koncentruje się na słynnych przypadkach, w których organy ścigania korzystały z pomocy psychologów i psychiatrów. Pierwszym takim przykładem jest opis nieznanego sprawcy przestępstwa na podstawie sekcji zwłok, a dotyczy sprawy „Kuby Rozpruwacza".

Inny ciekawy przykład to zamówienie w 1943 roku przez agendę amerykańskiego wywiadu (poprzednika CIA) ekspertyzy typologicznej Adolfa Hitlera. Miał on stworzyć profil osobowościowy Hitlera oraz przekazać sugestie dotyczące ewentualnej reakcji przywódcy Niemiec na porażki. Co ważne – Walter Langer - autor opracowania oparł się na analizie przemówień i publikacji Hitlera.

Historycznie biorąc pierwszym przypadkiem wykorzystania profilu osobowościowego przez policję była sprawa tzw. Mad Bomber'a, który w latach 1940-1956 podłożył w Nowym Yorku ponad 50 ładunków wybuchowych. Mimo posiadania bogatego materiału dowodowego - nawet listów wysyłanych przez sprawcę do prasy – policja

nie była w stanie wskazać sprawcy. Dopiero na podstawie profilu stworzonego przez Jamesa Brussela i jego strategii sprawcę udało się schwytać. Profilerowi udało się nawet przewidzieć szczegóły ubioru sprawcy w chwili zatrzymania.

Efektywność prac Jamesa Brussela zainteresowała Howarda Tetena, pioniera badań behawioralnych w Akademii FBI. To właśnie Teten częściowo opierając się na doświadczeniach Brussela, uzupełniając je o naukowe podstawy kryminalistyczne, analizę medyczną i ocenę psychologiczo-psychiatryczną zachowań przestępczych rozpoczął cykl szkoleń zwanych „kryminologią praktyczną". W 1972 współtworzył Wydział Badań Behawioralnych FBI (obecnie Wydział Wsparcia Dochodzeniowego). Uważny czytelnik zapyta z pewnością jaki związek z badaniami nad hakingiem mają osoby tworzące modele zachowań morderców, podpalaczy i innych dewiantów - patrz Hitler? Po pierwsze oddziedziczona nazwa profilowania, może nawet trochę myląca, i rozbudzająca niepotrzebne nadzieje. O ile bowiem w przypadku sprawców przestępstw seryjnych można mówić o sukcesach profilowania, to w przypadku hakingu stworzony profil pozwala stworzyć zespół cech osobowościowych, czyli inaczej mówiąc skłonności, upodobań wskazujących, że taka osoba może ewentualnie stanowić bazę, podbudowę do stania się hakerem. Nie jest wcale pewne, ze się takim stanie, ale istnieje duże prawdopodobieństwo.

Otwartym pozostaje pytanie, jak zmierzyć tego rodzaju skłonności? I czy można to zrobić?

Po drugie stosowane metody badawcze. Badania prowadzi się zarówno na pozostawionych przez cyberprzestępców śladach: np. ślady pozostawione w skompromitowanych systemach, rodzaje wpisów, wykorzystywane języki i stopień ich znajomości. Jak i ich własnych wytworach, czyli opublikowanych manifestach, wypowiedziach na forach, wpisach na zhakowanych stronach, wykorzystywanych nazwach własnych itp.

Podobnie jak w przypadku klasycznego profilowania analizuje się pamiętniki hakerów, przeprowadza i rejestruje przeprowadzone rozmowy i wywiady. Wielu specjalistów twierdzi, że w przypadku hakingu stworzenie takiego modelu jest niemożliwe, gdyż każdy przypadek jest indywidualny, ale próby badań się pojawiają i jest ich coraz więcej. Niestety osobiście nie znam polskich badań w tym zakresie. Omawiając zagadnienie profilowania hakerów należy zacząć od wydanej już w 1997 roku pracy Nicolas Chantler Profile of a Computer Hacker. Sześć lat później - po raz pierwszy na rynku polskim -w 2003 roku J.Mrugalski w ABC ochrony komputera przed atakami hakera opisał kilka cech szczególnych hakera: wiek (15-30 lat), zainteresowania (informatyka, elektronika, telekomunikacja), wykształcenie (wyższe), praca (nie pracuje, a jeśli ma pracę, to w branży informatycznej). W tym czasie nikt o tym nie pisał.

Od 2005 roku prace związane z cyberprzestępczością rozpoczął UNICRI – instytut badawczy ONZ, gdzie do prowadzenia zajęć ze studentami na tematy związane z hakingiem i przestępczością komputerową zaangażowany został Raoul Chiesa, były włoski haker. Współpraca jego z kryminolog dr Strefanią Ducci zaowocowała zainicjowaniem projektu HPP Hackers Profiling Project. Jest to największy na świecie projekt badawczy dotyczący hakingu.

W 2008 roku pojawiła się publikacja autorstwa Raoula Chiesy i Stefanii Ducci Profiling hackers. The Science of Criminal Profiling as applied to the world of hacking.

Projekt HPP jest w dalszym ciągu kontynuowany i rozwijany przez UNICRI, gdzie opiekuje się nim między innymi kryminolog Francesa Bosco. Zarówno Raoul Chiesa jak i Francesa Bosco gościli w Polsce na konferencjach związanych z IT security i ich prezentacje są szeroko dostępne w internecie.

Uważny czytelnik zapyta z pewnością jaki związek z badaniami nad hakingiem mają osoby tworzące modele zachowań morderców, podpalaczy i innych dewiantów - patrz Hitler?

Innymi projektami, które zwracają uwagę na zagadnienie motywu sprawcy, a w skład zespołu wchodzą psycholodzy, są projekty związane z różnymi honeypotami. Największy z tych projektów i działający od 1999 roku to the Honeynet Project. Od 2000 roku z projektem związany jest psycholog dr Max Kilger. Zainteresowani tematyką czytelnicy mogą sięgnąć na początek do: Trace-back. A concept for Tracing and Profiling Malicious Computer Attackers.

Osobnym, ale wykorzystującym podobne metody badawcze, w pewnym sensie bazujące na profilowaniu, zagadnieniem jest problem insider'ów.

Autor jest specjalistą w zakresie ochrony informacji w sektorze publicznym z 15 letnim doświadczeniem. W wolnym czasie realizuje się jako niezależny badacz „ciemnej strony" cyberkultury i pasjonat security awareness.

MOBILE FORENSICS

alternatywne metody, odczytywanie danych i ich odpowiednia analiza okiem biegłego

Michał Tatar, Mateusz Witański

Przestrzeń ‘mobilna’ zajmuje w życiu prawie każdego Polaka coraz ważniejsze miejsce. Bez względu na wiek, wszyscy ludzie począwszy od dzieci, a skończywszy na seniorach używają urządzeń mobilnych na różne sposoby, w zależności od swoich preferencji, hobby czy biznesu. Głównie sytuacja odnosi się do telefonów komórkowych, ale na rodzimym rynku nie możemy zapominać o wszechobecnych tabletach. Aby wyobrazić sobie skalę wystarczy podać informacje za Głównym Urzędem Statystycznym, który zakomunikował, iż na koniec III kwartału 2014 roku w Polsce działało 57.250.300 aktywnych kart SIM. Naturalnie oprócz kart polskich operatorów w naszym kraju działa mnóstwo aktywnych kart SIM pochodzących głównie z Wysp Brytyjskich czy Europy Środkowo-Wschodniej. W związku z powyższym możemy założyć, że skala ilości urządzeń obsługujących karty SIM będzie podobna. Oczywiście urządzenia mobilne obsługujące karty SIM to nie tylko telefony czy wspomniane tablety. To również modemy telefonii bezprzewodowej, nawigacje satelitarne czy systemy sieciowe.

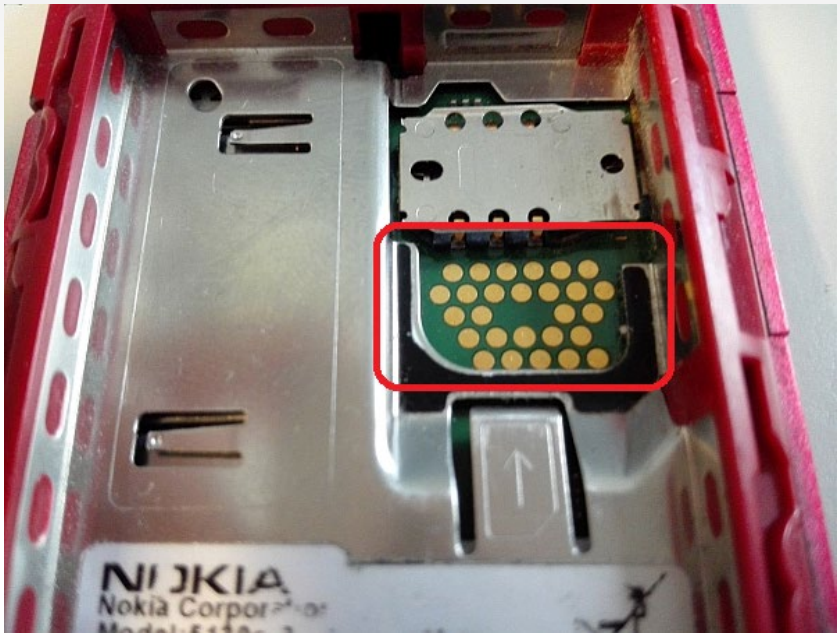
W przypadku używania słów mobile forensics zawsze należy wziąć pod uwagę wszystkie podręczne urządzenia, które każdy może schować do kieszeni i przechowywać na nim dane. Na rynku jest kilka wartych uwagi komercyjnych narzędzi służących do zabezpieczeń urządzeń mobilnych jednak w wielu przypadkach nawet te najlepsze rozwiązania zawodzą. Dzieje się tak głównie w sytuacjach, gdy urządzenie mobilne jest uszkodzone (np. po zalaniu wodą), zabezpieczone (np. hasłem dostępu), bądź gdy nie ma możliwości nawiązania komunikacji pomiędzy nim, a komputerem (np. urządzenia nie wyposażone w żaden interfejs kablowy/radiowy). Czy wówczas jesteśmy skazani na porażkę w takich sprawach?

Odpowiedź brzmi jak się zapewne wszyscy domyślają – nie. Dzięki alternatywnym metodom ekstrakcji danych je-

steśmy w stanie stoczyć walkę z takim urządzeniem i w większości wypadków to my, jako specjaliści mobile forensics wychodzimy z niej zwycięsko.

Jednym z ciekawszych rozwiązań jakie warto zaprezentować czytelnikom jest interfejs JTAG będący liderem alternatywnej metody odczytu i opisać pokrótce proces pozyskiwania danych. Na początek warto przytoczyć kilka słów o samym JTAG. Joint Test Action Group to nazwa standardu IEEE 1149.1 definiującego protokół używany do testowania połączeń na płytkach drukowanych, stosowany także do uruchamiania, programowania układów i systemów mikroprocesorowych. Prościej mówiąc, interfejs JTAG umożliwia zarówno programowanie procesorów, jak i debugowanie zawartego w nich kodu, a także połączeń elektrycznych mikrokontrolera z resztą układu, w tym z pamięcią FLASH. Widzimy więc, że możliwości tego interfejsu są duże. Przewagą odczytu pamięci FLASH przez interfejs JTAG jest fakt, iż odbywa się on sektorowo bit po bicie. Oznacza to, że otrzymujemy nic innego jak odczyt fizyczny takiej pamięci co jest niezwykle istotne przy próbie odzyskiwania skasowanych danych. Interfejsy JTAG znajdujemy w większości urządzeń elektronicznych, niekiedy bardziej odsłonięte, niekiedy ukryte. Co ciekawe nawet wiele bardzo starych urządzeń mobilnych posiada to złącze.

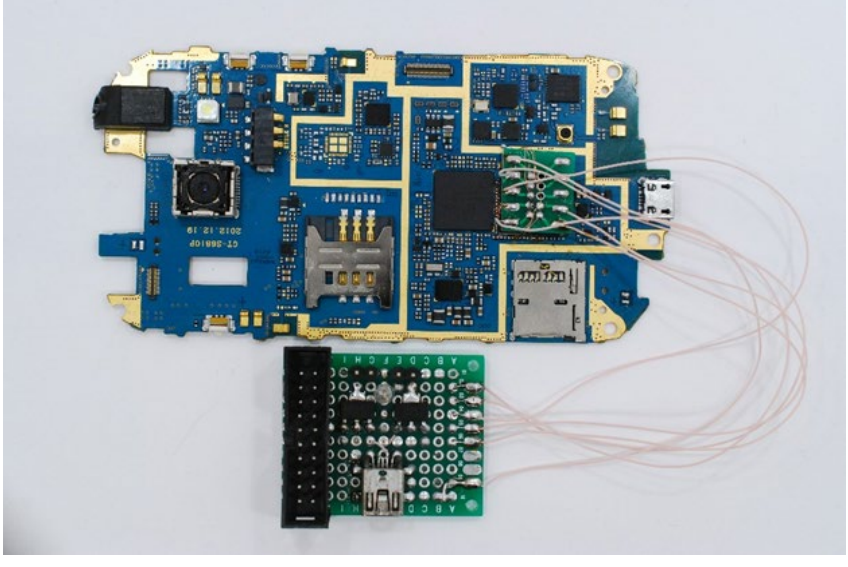
Sam odczyt polega na właściwym podłączeniu interfejsu JTAG z urządzeniem.



Rys. 1 – Przykładowe złącze JTAG.

W świecie mobile forensics najczęściej wykorzystuje się tzw. BOXy serwisowe, których główną funkcją jest zaawansowany dostęp do wykonywania napraw software`owych telefonów, ściąganie blokad SIM-Lock, flash`owanie niewłączającego się telefonu, odbudowę certyfikatów. Prócz tych i wielu innych funkcji niektóre z nich oferują wykonywanie tzw. MEMORY DUMP czyli zrzut fizyczny pamięci FLASH.

Aby poprawnie połączyć się z interfejsem JTAG musimy znać sekwencje połączeń sygnałów serwisowych (RX/TX/D+/D-/GND), a następnie wykonać połączenie pomiędzy płytą główną telefonu, a BOXem serwisowym. Dla osób nie mających nic wspólnego z elektroniką cała sytuacja może wydawać się skomplikowana i skutecznie zniechęcić do tego typu działań. Nie należy się poddawać, gdyż z pomocą przychodzą adaptery JTAG, które są ogólnodostępne. Nie wymagają one od użytkownika znajomości rozkładu sygnałów oraz umiejętności lutowniczych. Adaptery przystosowane są pod konkretne urządzenie mobilne i ich zastosowanie na ogół sprowadza się do gotowego połączenia z płytą główną.



Rys. 2 – JTAG – Połączenie kablowe.

Po poprawnym podłączeniu się do odpowiedniego BOXa serwisowego, w programie obsługującym to urządzenie wybieramy opcję odczytu pamięci FLASH i czekamy, aż plik zostanie zapisany w komputerze. Niestety proces odczytu pamięci przez interfejs JTAG jest bardzo wolny i cała operacja może potrwać nawet kilkadziesiąt godzin.

Gdy odczyt wykona się poprawnie możliwa jest jego analiza. Plik odczytu fizycznego możemy zaimportować do komercyjnego narzędzia mobile forensics (np. XRY) i oczekiwać na dane gotowe do interpretacji przez biegłego.

Współczesne urządzenia mobilne to zminiaturyzowane komputery przenośne. Są tak traktowane przez producentów, jak i przez użytkowników. Tylko od pojemności pamięci wewnętrznej Flash

oraz obsługiwanych kart zewnętrznych zależy, jak blisko danemu urządzeniu do komputera i ile ciekawych danych możemy na nim znaleźć. Telefon komórkowy w dzisiejszych czasach powie nam, jaki tryb życia prowadzimy, jak bardzo jesteśmy aktywni i jak bardzo jesteśmy społeczni. Biegły z zakresu psychologii na podstawie możliwych do uzyskania z telefonu danych, przygotuje profil psychologiczny użytkownika. Biegły z zakresu teleinformatyki wyodrębni pełną informację, kiedy, gdzie, jak i w jakim celu telefon został użyty. Każdy zapyta, jak to możliwe, żeby telefon tak bardzo zdradzał, co i kiedy robimy. Przecież nie w każdym momencie z niego korzystamy, nie zawsze wykonujemy połączenia czy piszemy sms-y.

Niewiele osób zdaje sobie sprawę, jakie dane rejestruje telefon także bez naszej wiedzy. Można stwierdzić, że pozwalamy telefonowi na bardzo wiele, nie zawsze zastanawiając się nad konsekwencjami. Zaczniemy od najbardziej oczywistych rzeczy, czyli wszystkie połączenia, zarówno wychodzące, jak i przychodzące, odebrane i nieodebrane. Do tego komunikacja poprzez SMS i MMS. Trzeba pamiętać, że wszystkie dane kontaktowe są zapisywane w pamięci telefonu. Nie jest to jednak wszystko. Coraz częściej komunikujemy się poprzez komunikatory (np. Skype), a telefon potrafi zapamiętać wszystkie rozmowy wykonane z każdego loginu, przy pomocy którego zalogowano się do usługi. Jako że smartfon jest praktycznie przenośnym komputerem, instalujemy na nim różne aplikacje, a urządzenie rejestruje, z jakiej korzystamy i jak często.

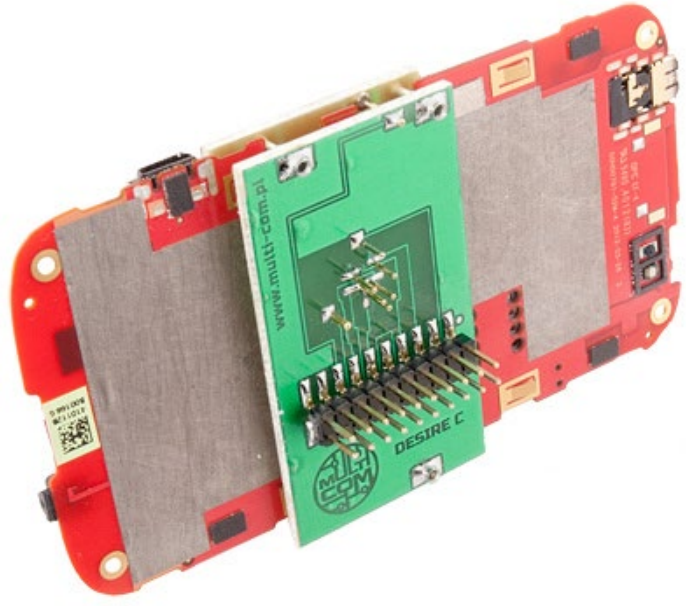
Wiele aplikacji do prawidłowego działania potrzebuje dwóch elementów – informacji o lokalizacji i dostępu do internetu. A żeby było szybciej i często taniej, zezwalamy naszemu urządzeniu mobilnemu wyszukiwać sieć WiFi i logować się do niej. A każda aplikacja, dla własnego bezpieczeństwa i wygody, zapisuje swoją historię. Do tego dochodzą kalendarz, przeglądarka internetowa, skrzynki mailowe, zdjęcia i filmy, dokumenty i ... rejestracja wszystkich znaków, jakie wprowadzamy z klawiatury.

Dużo tego. Jednak wielu czytelników stwierdzi, że „mnie to nie dotyczy, bo kasuję niepotrzebne dane, często czyszczę historię". Niech więc każda z tych osób spojrzy na swój telefon i sprawdzi, ile ma wolnego miejsca w pamięci urządzenia. 1 GB, 2 BG, może więcej? W uproszczeniu, tyle ma danych, które po odczycie pamięci będą zaznaczone jako „deleted items". Te dane są niewidoczne dla użytkownika telefonu, nie są one jednak niewidoczne dla biegłego z zakresu informatyki śledczej, który dokona odczytu binarnego takiej pamięci.

Specjalista z zakresu mobile forensico-trzymuje telefon w celu wyodrębnienia informacji znajdujących się na nim, a nie jakiego rodzaju aplikacje są na nim zainstalowane. Na podstawie całego szeregu danych, biegły musi wskazać dowody w określonej sprawie - zarówno obciążające, jak i uniewinniające. Pierwszym krokiem w analizie telefonu powinna być analiza sposobu korzystania z telefonu.

Na taką analizę składać się będzie kilka elementów: jak często i jak długo dana osoba rozmawia przez telefon, czy wysyła wiadomości SMS/MMS. Ważne będzie również, jak dana osoba korzysta z internetu (przeglądarka internetowa i poczta e-mail), czy loguje się do każdej napotkanej sieci WiFi, czy tylko do kilku, jak często i jak długo korzysta z tych sieci, czy korzysta z pakietu danych oferowanego przez operatora. Trzecim istotnym elementem będzie stwierdzenie, z jakich aplikacji użytkownik telefonu korzysta, jak często to robi, czy jest jakiś określony, przybliżony czas korzystania z aplikacji. No i czy aplikacje mają zezwolenie na korzystanie z lokalizacji, czy też nie.

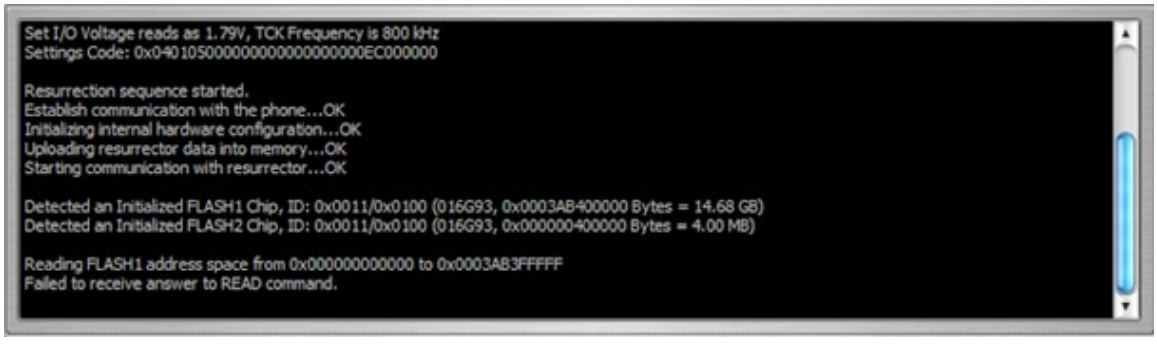
Na podstawie wskazanych wyżej danych powstaje profil użytkownika urządzenia mobilnego. Niech będzie to osoba, która częściej dzwoni niż korzysta z SMS/MMS, zazwyczaj nie odbiera telefonu, tylko oddzwania, większość rozmów prowadzi z osobami z książki telefonicznej, ma zainstalowanych kilka aplikacji, z których korzysta w miarę często i regularnie (np. codziennie ok. godz. 7.00 sprawdza aktualną temperaturę w aplikacji Thermometer, zawsze między 9.00 a 10.00, korzysta z aplikacji mobilnych trzech banków itd.), zezwala każdej aplikacji na korzystanie z danych lokalizacyjnych, korzysta z czterech stałych sieci WiFi, poza tym z usług operatorskich, nieregularnie korzysta z przeglądarki internetowej, prawie zawsze podczas podróży ma włączoną nawigację, mimo że pokonuje tą samą trasę regularnie.



Rys. 3 – JTAG – Połączenie przez adapter.

Tak przygotowany opis pozwoli nam na stwierdzenie, czy na podstawie danych zawartych w telefonie rozwikłamy problem, jaki przed nami postawiono. Jeżeli będziemy chcieli stwierdzić, czy dana osoba była w jakimś miejscu nie korzystając przy tym z telefonu, to tych informacji nie znajdziemy w tym urządzeniu. Taki użytkownik musiałby bowiem skorzystać z telefonu w jakikolwiek sposób, żeby pojawił się jakiś ślad. Z kolei jeżeli będziemy chcieli sprawdzić alibi danej osoby to ustalimy czy użytkownik będąc w domu był zalogowany do swojej sieci WiF. Natomiast w przypaku użytkownika, który korzysta z telefonu w zupełnie inny sposób, np. cały czas jest zalogowany do aplikacji Facebooka, dużo łatwiej będzie sprawdzić, gdzie był w danym momencie.

Najlepiej zabezpieczone, urządzenia mobilne nie są tajemnicą dla biegłych zajmujących się informatyką śledczą. Specjalista przy pomocy zaawansowanego oprogramowania i rozwiązań oraz najwyższych kompetencji jest w stanie odzyskać dane z urządzeń przenośnych jak i dokonać ich interpretacji. Dlatego warto zastanowić się nad tym, w jaki sposób korzystamy z urządzenia mobilnego oraz jakie ślady w nim pozostawiamy. Na zakończenie pamietajmy, że dane zlokalizowane na urządzeniach mobilnych można odzyskać. Pozostaje to jedynie kwestią czasu.



Rys. 4 – Odczyt pamięci za pomocą interfejsu JTAG.

View Name	Number of Items	Deleted Items
Contacts	1590	608
Calls	528	28
Calendar / Calendar Events	144	
Messages / SMS	2259	70
Messages / MMS	171	71
Messages / Chat	15495	38
Device / Network Information	58	21
Device / Event Log	4916	10
Locations / History	767	1
Locations / Bookmarks	2	
Web / History	4491	3160
Web / Bookmarks	8	
Web / Searches	44	1
Web / Cookies	14232	12187
Files / Pictures	3046	38
Files / Videos	18	
Files / Audio	87	
Files / Documents	549	
Files / Archives	324	2
Files / Databases	533	
Files / Unrecognized	16463	12791
Device / Keyboard Cache	4	

Rys. 5 – Dane zaimportowane przez narzędzie XRY.

Michał Tatar

Autor jest specjalistą w zakresie analizy urządzeń mobilnych (Mobile Forensics) w Laboratorium Informatyki Śledczej Mediarecovery. Zajmuje się również implementacją rozwiązań mobilnych zarówno w sektorze prywatnym jak i publicznym (m.in. Mobile Device Management). Trener w ramach Akademii Informatyki Śledczej.

Mateusz Witański

Dyrektor Zarządzający w Buszman & Witański Consulting Group, biegły sądowy w zakresie analizy danych transmisyjnych, specjalista w zakresie projektów teleinformatycznych, analityk i praktyk zarządzania.

Wyzwania w Live Forensic

Stefan Larsson

Live Forensic, jest obszarem informatyki śledczej, który zawsze był owiany tajemnicą... Właściwie, ową tajemniczość wytworzył brak wiedzy i niepewność.

Live Forensic nigdy nie było ważniejsze, niż w dzisiejszych czasach. Nasze domy, miejsca pracy, a także całe nasze życie codzienne, wypełnione są urządzeniami, które pozwalają na nieprzerwane, ciągłe połączenie z Internetem, który dla wielu ludzi stanowi kamień węgielny nowoczesnego społeczeństwa. To złożone środowisko nakłada na nas, jako na śledczych, a zwłaszcza specjalistów informatyki śledczej, wymagania większe, niż kiedykolwiek wcześniej. Laptopy, tablety, telefony komórkowe tworzą ogromną ilość możliwości połączenia mobilnego. Jednocześnie coraz bardziej przejmują rolę, wcześniej przypisaną „tradycyjnemu", domowemu urządzeniu gospodarującemu dane, czyli komputerowi. Odbija się to na zmniejszającym się, kruszącym rynku PC, ponieważ ludzie zaczynają porzucać komputery stacjonarne. Tak samo jak urządzenia mobilne wypierają komputery stacjonarne, połączenie za pomocą stałego łącza jest wypierane przez rozwiązania bezprzewodowe. Punkty WiFi są dostępne w kawiarniach, restauracjach i innych miejscach przestrzeni publicznej. Możliwość łączenia się za pomocą WiFi nigdy nie była tak wielka.

Stajemy się coraz bardziej mobilni, niemal zawsze połączeni z internetem, a przy tym polegamy na coraz to mniejszych urządzeniach, by wykonać naszą pracę, a także by pomagały w naszym życiu codziennym, gospodarowaniu czasu wolnego i kontaktach społecznych. Potrzeba ochrony naszych informacji stale wzrasta. Przechowujemy prywatne dane na urządzeniu, które jest zawsze przy nas i zapisuje więcej, na nasz temat, niż byśmy chcieli. Przez to jesteśmy coraz bardziej narażeni na próby kradzieży informacji. Wymagania dotyczące ochrony danych były brane pod uwagę przez przemysł, przez co szyfrowanie ich jest obecnie łatwiejsze, niż było dotychczas. To, co było zarezerwowane dla osób posiadających duże umiejętności w sferze IT, w dniu dzisiejszym jest możliwe poprzez kilka naciśnięć klawiszy, dla osoby, która nie posiada choćby małej wiedzy w tej materii. Obecny sposób szyfrowania jest niezauważalny, jest wbudowaną cechą integralną, dostępną także dla użytkowników, którzy nigdy nie wpisywali trudnych haseł, czy kluczy sprzętowych. Wraz ze zwiększoną mobilnością i bezpiecznym sposobem magazynowania danych, wzrasta także pojemność dostępnej przestrzeni, a ogrom jej wzrostu jest trudny do przewidzenia. Małe, przenośne urządzenia mogą obecnie przechowywać porównywalną ilość danych, którą w nieodległej przeszłości posiadały duże serwerownie. Nasza sieć domowa staje się coraz bardziej rozwinięta, a już w jej obrębie urządzenia mogą się komunikować ze sobą.

To, co było zarezerwowane dla osób posiadających duże umiejętności w sferze IT, w dniu dzisiejszym jest możliwe poprzez kilka naciśnięć klawiszy, dla osoby, która nie posiada choćby małej wiedzy w tej materii.

Rozwój sam w sobie jest zjawiskiem pozytywnym, zwłaszcza patrząc przez pryzmat wygody. Nasze życia, zarówno te prywatne, jak i profesjonalne, nie są już powiązane. Informacje osobiste są na ogół chronione przed kradzieżą. Przynajmniej można tak powiedzieć o informacjach, które sami przechowujemy, a mamy możliwość przechowywania ogromnej ilości danych. Tak, to jest pozytywne zjawisko, a rozwój stale się dokonuje. Plamą na obrazie jasnej przyszłości, jest fakt, że także przestępcy mogą się cieszyć swobodą, a ochrona, dostarcza im świetne narzędzia do kontynuowania ich procederu.

Oznacza to, że specjaliści informatyki śledczej, których zadaniem jest zabezpieczanie, analizowanie urządzeń przenoszących dane, które należą do podejrzanych osób, mają przed sobą ogromne wyzwania. To, co kiedyś można było rzadko spotkać na swojej drodze, dla dzisiejszych specjalistów informatyki śledczej stało się właściwie codziennością. Czym jest zatem Live Forensic? Można pokusić się o tradycyjną definicję, mówiącą o zabezpieczaniu informacji z systemu, który jest „live", np. pracuje. Znaczyło to, że system był badany poprzez różne narzędzia, często w celu zebrania

danych, które były „live" w systemie. Na to mogły się składać wszelakie niezapisane dokumenty, trwające czaty, czy też przeglądanie stron internetowych. To, jakie narzędzia specjalista informatyki śledczej wykorzystywał, było jego osobistym wyborem, opartym na badaniach i doświadczeniu. Ilość narzędzi zależała od poziomu kompetencji specjalisty informatyki śledczej, a ich liczba wzrastała wraz z rozwojem środowisk IT. Zwiększona mobilność postawiła nowe wyzwania specjalistom informatyki śledczej, zmieniając to, co znaczy Live Forensic. Oznacza to, że koncepcja zawiera obecnie także informacje, które są przesyłane bezprzewodowo, informacje o urządzeniach oraz na temat ich interaktywnej komunikacji. Live Forensic nie może już być czymś, co będzie robione w wolnej chwili. Musi być integralną częścią procesu informatyki śledczej, które są warte swej nazwy. Ryzyko tego, że przechwycone dane nie będą mogły być zanalizowane ze względu na zaszyfrowanie, jest dzisiaj największe w dziejach. Ze względu na to systemy muszą być badane „live", zanim zostaną poddane dalszej analizie. Ponieważ alternatywą jest potrzeba otwarcia zaszyfrowanego dysku twardego, która często jest krokiem daremnym. Live Forensic już dłużej nie może być procesem na wyłączność dla specjalistów informatyki śledczej mających wysokie umiejętności, ponieważ musi być dokonywany przez wszystkich, którzy wchodzą w kontakt ze środowiskami IT. Duża część specjalistów informatyki śledczej traci swój cenny czas na podróżowaniu na i z miejsca zbrodni, zamiast aktywnie dokonywać analizy dowodów przestępstwa. Środowiska IT można znaleźć wszędzie, w domach, miejscach pracy, a także w przestrzeni publicznej. Poleganie na małej, ograniczonej liczebnie grupie specjalistów informatyki śledczej, by tylko oni zajmowali się zebranymi informacjami, przeszukiwaniem domów, oraz innymi procesami, które mają potencjalny związek z IT jest fizycznie niemożliwe. Ze względu na zwiększającą się liczbę dochodzeń, specjaliści informatyki śledczej będą zmuszeni do wcielenia się w rolę konsultancką, skupioną na analizie, natomiast w kwestii zbierania materiałów będą potrzebowali wsparcia innego personelu. Tak jak dzisiejsi oficerowie policji są często zmuszeni do zbierania odcisków palców i dowodów DNA, zbieranie materiałów w Live Forensic będzie musiało być przeprowadzone w podobny sposób. Luka znajduje się pomiędzy kompetencjami i narzędziami. The Information Collection Tool (ICT) jest narzędziem, które przeobraża kilka różnych metod zbierania w małe, przenośne i proste narzędzie. Prostota oraz mobilność to filary, na których opiera się ICT. Prostota pozwala osobie nie będącej specjalistą informatyki śledczej, aby po krótkim treningu, dokonywać złożonych procesów zbierania danych. Informacje te są zapisywane w zaszyfrowanych plikach, które później przekazane do analizy specjalistów informatyki śledczej.

ICT może również zbierać informacje ze środowisk WiFi, a także Ethernet'u, które w innym przypadku byłyby utracone. ICT zezwala na dostęp do komputerów poprzez metodę obchodzenie blokady ekranu. To daje specjaliście zbierającemu informacje możliwość zabezpieczenia danych, które byłyby ukryte za szyfrowaniem przy wyłączeniu. ICT tworzy także ważne, często niezauważane połączenie między komputerem śledczym, a monitoringiem. Wzrost mobilności tworzy świetną okazję na dokonanie monitoringu technicznego, w którym podejrzani oraz dane, które transmitują dają śledczym nowe możliwości powstrzymywania zbrodni. Nadszedł czas, by dać Live Forensic uwagę, na którą zasługują poprzez rozwiązywanie przestępstw. Nadszedł czas, by uświadomić sobie, że informatyka śledcza to coś więcej, niż tylko dublowanie twardych dysków, czy pendrive'ów. Informatyka śledcza jako dziedzina, także powinna zostać usankcjonowana, a specjaliści w tej dziedzinie, muszą być gotowi na to, by zebrane informacje przekazać, między innymi oficerom Policji, oficerom zajmującym się monitoringiem, technikom kryminalnym, a samemu skupić się na wzrastającej liczbie skomplikowanych analiz. Aby zmaksymalizować skuteczność, oficer, który pojawi się na miejscu zbrodni jako pierwszy, powinien być wyposażony w sprzęt niezbędny do zebrania informacji.

Stefan Larsson
Autor jest założycielem firmy Swedish Forensic Technologies (Swedfor), zajmującej się produkcją rozwiązań (Information Collection Tool - ICT) wykorzystywanych przez organy ścigania do gromadzenia cyfrowego materiału dowodowego.

Powołanie ABI, czy to się opłaca?
Nowelizacja ustawy o ochronie danych osobowych

Paulina Skwarek

Z początkiem stycznia tego roku, nastąpiła jedna z największych dotychczas zmian w prawie ochrony danych osobowych. Była to długo oczekiwana nowelizacja, która w znacznej mierze skupiła się na uregulowaniu statusu Administratorów Bezpieczeństwa Informacji. Na mocy nowych przepisów, administratorzy danych powinni dokonać wyboru, czy będą dbali o bezpieczeństwo danych osobowych samodzielnie, czy też za pomocą wykwalifikowanego podmiotu jakim jest Administrator Bezpieczeństwa Informacji.

Na mocy nowych przepisów, administratorzy danych powinni dokonać wyboru, czy będą dbali o bezpieczeństwo danych osobowych samodzielnie, czy też za pomocą wykwalifikowanego podmiotu jakim jest Administrator Bezpieczeństwa Informacji.

Korzyści z powołania ABI

Na pierwszy rzut oka, szczególnie dla tych przedsiębiorców, którzy dotychczas nie przywiązywali szczególnej wagi do ochrony danych osobowych, powoływanie ABI wydaje się zbędnym kosztem. Warto jednak rozważyć, czy w dłuższej perspektywie poniesiony koszt nie przyniesie wymiernych korzyści.

Analiza znowelizowanych przepisów pozwala na wskazanie dwóch podstawowych zalet związanych z powołaniem ABI. Pierwszą jest niewątpliwie uproszczona procedura kontroli, drugą uproszczona procedura rejestracji zbiorów danych osobowych.
Uproszczona procedura kontroli polega na tym, że Generalny Inspektor Ochrony Danych Osobowych w firmie, w której powołano ABI, będzie mógł zaniechać przeprowadzania zewnętrznej kontroli. Nie oznacza to jednak, że kontrola w ogóle nie będzie się odbywać. Będzie miała miejsce, ale na innych zasadach.

W firmie, w której powołano ABI, GIODO będzie mógł przeprowadzać, zamiast kontroli wykonywanej przez własnych inspektorów (jak to miało miejsce do grudnia 2014), tzw. kontrolę wewnętrzną. Kontrola wewnętrzna to nic innego jak sprawdzenie przez ABI, na wniosek GIODO, czy dane osobowe w firmie przetwarzane są zgodnie z prawem. Taka kontrola wydaje się sprzyjać przedsiębiorcom. Nie będą kontrolowani przez zewnętrzne podmioty, lecz przez własnego pracownika, który przedstawi GIODO sprawozdanie z przeprowadzonych przez siebie czynności.

Warto w tym miejscu przypomnieć, że jeśli przedsiębiorca nie powoła ABI, wówczas kontrole GIODO będą odbywały się na starych zasadach, a więc przedsiębiorcy będą sprawdzani przez pracowników GIODO. Z perspektywy uproszczonej kontroli powołanie ABI wydaje się więc korzystne.

Kolejną i równie istotną zaletą powołania ABI, jest uproszczona procedura rejestracji zbiorów danych osobowych. Uproszczona procedura rejestracji polega na tym, że przedsiębiorca, który powoła i zarejestruje ABI, nie będzie musiał zgłaszać do rejestru występujących u niego zbiorów danych osobowych. Wyjątek od tej reguły stanowić będą dane wrażliwe, które pomimo powołania ABI należy zgłaszać do rejestru. Niezaprzeczalnie, zwolnienie z obowiązku rejestracji zbiorów danych osobowych jest dla przedsiębiorców dużym ułatwieniem. Oprócz wskazanych powyżej korzyści, warto również zwrócić uwagę na wpływ powołania ABI na wizerunek firmy. Korzystanie z ABI, który z założenia profesjonalnie zajmuje się ochroną danych osobowych, w mojej opinii jest wysłaniem sygnału do kontrahentów, że dane osobowe w firmie traktowane są poważnie i podlegają należytej ochronie. Z pewnością walor wizerunkowy dotyczy w głównej mierze dużych podmiotów, które na co dzień zajmują się przetwarzaniem danych osobowych.

Głosy krytyczne

W rozważaniach na temat nowych przepisów związanych z powoływaniem ABI,

nie sposób pominąć głosów krytycznych. Przeciwnicy powoływania ABI podnoszą, iż ustanowienie ABI w organizacji to dodatkowy, wysoki koszt. Ponadto, wskazują, że powołanie ABI wiąże się z dopuszczeniem kolejnej osoby do kluczowych dla firmy informacji, co zwiększa ryzyko wycieku tych informacji poza organizację.

Pojawiają się również głosy, że poprzez przyznanie ABI kompetencji kontrolnych, będą oni traktowani w firmach jako „szpiedzy GIODO", a z drugiej strony GIODO może podchodzić z rezerwą do informacji uzyskiwanych od ABI, gdyż będą to osoby finansowane przez samych zainteresowanych pozytywnym wynikiem kontroli. Biorąc pod uwagę plusy i minusy powołania ABI, nie można jednoznacznie stwierdzić czy powołanie ABI będzie w każdym przypadku i dla każdego administratora danych korzystne. Wydaje się, że dla oceny nowych rozwiązań decydujące znaczenie będą miały z jednej strony specyfika danej organizacji, a z drugiej praktyka która wykształci się w najbliższym czasie. Niewątpliwie jednak, każdy administrator danych powinien przyjrzeć się swojej strukturze organizacyjnej i ocenić czy jest w stanie samodzielnie zadbać o bezpieczeństwo przetwarzanych danych osobowych oraz czy plusy z powołania ABI przeważają nad minusami.

Paulina Skwarek
Autorka jest adwokatem, założycielem Kancelarii Adwokackiej Paulina Skwarek w Katowicach. Specjalizuje się w prawie własności intelektualnej, ze szczególnym uwzględnieniem prawa nowych technologii, prawa autorskiego, ochrony danych osobowych oraz zamówień publicznych.

Autorka bloga www.ip-prawo.pl.

MAGAZYN INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

Adres redakcji
Mediarecovery
40-723 Katowice, ul. Piotrowicka 61
Tel. 32 782 95 95, fax 32 782 95 94
e-mail: magazyn@mediarecovery.pl
www.magazyn.mediarecovery.pl

Redakcja
Sebastian Małycha (red. nacz.),
Przemysław Krejza
Skład, łamanie, grafika: Mariusz Ruski
Reklama: Damian Kowalczyk

Wydawca
Media Sp. z o.o.
40-723 Katowice, ul. Piotrowicka 61
Tel. 32 782 95 95, fax 32 782 95 94
e-mail: biuro@mediarecovery.pl
www.mediarecovery.pl

mediarecovery Lider informatyki śledczej