MAGAZYN

NR 24 / GRUDZIEŃ 2014

www.magazyn.mediarecovery.pl

INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

Sposoby na przyspieszenie odzyskiwania haseł

Vladimir Katalov

Licencje na narzędzia informatyki śledczej

Jarosław Góra

Mobile Forensics zmienia urządzenia przenośne w dowody

Peter Warnke

Informatyka śledcza zgodna z ISO 27001:2013

TÜV NORD PN-EN ISO 27001

Potężne wsparcie do analizy śledczej

Polski Duplikator mediaimager GM4

Od redakcji

O konieczności stosowania informatyki śledczej nie trzeba chyba przekonywać żadnego z czytelników naszego Magazynu. Jak jednak robić to efektywnie i skutecznie? O czym pamiętać stosując oprogramowanie śledcze? O tym wszystkim pisze grono naszych Autorów.

W bieżącym wydaniu gościmy na łamach dwóch specjalistów z zagranicy. Pierwszy z nich, Rosjanin założyciel Elcomsoftu przedstawia sposoby na przyspieszenie odzyskiwania danych. Drugi z autorów – Niemiec – przybliża problematykę urządzeń przenośnych, jako cennego źródła dowodów.

Przedstawiamy również pierwszą, polską kopiarkę danych. Nie ustępuje ona produktom zagranicznym, co więcej, śmiemy twierdzić, że nawet je przewyższa. Powstanie kopiarki oznacza też nową erę w polskiej informatyce śledczej. Nasz rodzimy rynek stał się na tyle dojrzały, że polskim firmom zaczyna opłacać się nie tylko wykonywać usługi, ale również produkować specjalistyczne narzędzia.

Nasz stały autor, Jarosław Góra, tym razem przyjrzał się bliżej licencjom na oprogramowanie śledcze. Temat niby oczywisty, a jednak część biegłych zdaje się o nim zapominać. Zresztą nie tylko w Polsce. Znana jest w naszym środowisku historia z Włoch. Dowody zdobyte w komputerze podejrzanego zostały odrzucone przez Sąd bo biegły korzystał z pirackiej wersji EnCase...

Jesteśmy ciekawi Państwa opinii dotyczących zapraszania na łamy Magazynu autorów z zagranicy. Dajcie im wyraz na przykład poprzez adres e-mail: redakcja@mediarecovery.pl Przeczytamy każdą wiadomość, a każdą rzeczową uwagę rozważymy.

Miłej lektury!
Redakcja

Sposoby na przyspieszenie odzyskiwania haseł

Vladimir Katalov

Zabezpieczanie danych przed nieuprawnionym dostępem poprzez hasło stosowane jest od bardzo dawna. Hasła są wykorzystywane zarówno do ochrony smartfonów, kont internetowych czy wejść do budynków. Wykorzystuje się je także do ochrony plików, dokumentów i archiwów w komputerach.

W przeciągu ostatniej dekady ochrona dostępu poprzez hasło bardzo się rozwinęła. Jeśli podczas pierwszych implementacji, lata temu można było oznaczyć plik flagą, że jest on „chroniony", tak współczesność wymaga pełnego szyfrowania danych. Nawet gdy firmy zaczęły już używać prawdziwej enkrypcji, to nadal miały związane ręce. Dla przykładu, z powodu licznych ograniczeń prawnych narzuconych przez rząd USA, Microsoft w międzynarodowych wersjach Office mogło posługiwać się jedynie szyfrowaniem 40 bitowym. Było ono słabe, w 2008 roku Elcomsoft wbił ostatni gwoździ do trumny, dostarczając natychmiastowe odszyfrowywanie plików zabezpieczonych kluczem 40-bitowym. Przez dłuższy czas używano oryginalnego algorytmu 56-bitowego do szyfrowania danych. Co i tak nigdy nie było zbyt mocnym standardem. Już w 1999 roku, amatorzy byli w stanie publicznie rozszyfrować klucz 56-bitowy w 22 godziny i 15 minut. Były to czasy gdy atakowanie algorytmu lub podmiana kodu binarnego było najlepszą metodą do łamania szyfru. W międzyczasie, standardy ochrony danych rozwijały się w celu zastosowania innych, bardziej bezpiecznych algorytmów, wykorzystujących o wiele dłuższy klucz. AES wybrano na oficjalny standard w USA, który zamienił się w faktycznie obowiązujący standard na całym świecie.

AES wykorzystuje dłuższe klucze zawierające 128, 192 lub 256 bitów, ale nawet ich najkrótszy klucz składający się „jedynie" z 128 bitów sprawia, że próby złamania szyfru są bezowocne. Stało się jasne że, na celowniku musi się znaleźć zwykle hasło wybrane przez użytkownika aby uzyskać dostęp do zabezpieczonych danych. Dzisiejsze, mocno zaawansowane, algorytmy szyfrowania wykorzystują skomplikowane i celowo powolne przetwarzania w celu uwierzytelnienia jednego hasła. Rozszyfrowania hasła metodą „na siłę" stało się bardzo powolne. Priorytetem stało się przyspieszenie odzyskiwania długich, skomplikowanych haseł.

Istnieje kilka sposobów na przyspieszenie odzyskiwania hasła:

1. Ograniczenie ilości haseł do wypróbowania.

Socjotechnika, listy haseł i słowniki to tylko kilka rzeczy kierujących się w „czynnik ludzki", w celu zredukowania liczby potencjalnych haseł do wypróbowania.

2. Korzystanie z szybszego sprzętu komputerowego.

Najczęściej jedyna możliwa droga odzyskania hasła to nadal metoda siłowa, o ile nic nie wiemy o danym zabezpieczeniu. Im więcej „siły", tym większą szybkość odzyskania hasła. Rozwój technologii w ostatnim czasie pozwala wykorzystać ultra szybkie karty graficzne do odzyskiwania haseł. Wszakże, karty video są w stanie wytworzyć kompleksowe obrazy 3D zawierające tysiące wielokątów w tempie 60 klatek na sekundę (w przeciwieństwie do zwykłego CPU, który ma tylko 1 lub 2 FPS). Musi to być dobra metoda na przyspieszenie odzyskania hasła.

3. Rozdzielenie pracy na większą liczbę urządzeń lub rozładowanie zadania do chmury.

Poprzez wykorzystanie setek lub nawet tysięcy komputerów w tym samym czasie, można proporcjonalnie przyśpieszyć odzyskiwanie hasła. Która z tych metod jest odpowiednia dla Ciebie? Jeśli masz inne hasła danego użytkownika, prawdopodobnie możesz już dostrzec jakiś wzór. Czy użytkownik wybiera tylko małe litery i cyfrę na końcu? Czy wszystkie jego hasła zaczynają się od dużej litery? Czy kiedykolwiek używał znaków specjalnych? Tworząc maskę obejmującą najczęściej używane hasła przez użytkownika, możesz mocno zredukować liczbę kombinacji do wypróbowania, sprawiając że odzyskanie hasła staje się możliwe nawet w najmocniej zabezpieczonych przypadkach. Czy twój komputer ma jedną lub więcej kart wideo? Dzisiejsze akceleratory grafiki mogą (i rzeczywiście tak robią) przyśpieszyć odzyskanie hasła o 20 do 50 razy, w porównaniu z użyciem wyłącznie CPU - i to wszystko za około 200-300 dolarów. Czy stać cię na to aby tego nie używać? Wreszcie, czy twoja sieć zawiera więcej niż jeden komputer? W takim wypadku można wykorzystać ją całą do złamania jednego hasła - jest to o tyle szybsze, o ile więcej komputerów udostępnisz w sieci. Czy chcesz używać tego wszystkiego naraz? Oprogramowanie Elcomsoft Distributed Password Recovery posiada wszystko: ataki słownikowe, zaawansowane maski ze słownymi kombinacjami (advanced masks with word permutations), akcelerację GPU i rozproszone działanie poprzez LAN i internet. Co więcej możesz sobie wymarzyć?

Autor jest Prezesem Zarządu, współwłaścicielem i współzałożycielem ElcomSoft Co. Ltd. Stworzenie przez niego pierwszego programu do odzyskiwania haseł było jednocześnie początkiem firmy. Obecnie zajmuje się koordynacją badań i rozwoju oprogramowania. Prowadzi szkolenia z zakresu bezpieczeństwa oraz informatyki śledczej dla rosyjskich i nie tylko rosyjskich organizacji specjalistycznych i organów ścigania.

Mobile forensics zmienia urządzenia przenośne w dowody

Peter Warnke

Dzięki rozwojowi technologii, telefony komórkowe zmieniają się coraz bardziej z prostych urządzeń w główny przedmiot w naszym życiu. Organizujemy spotkania, robimy zdjęcia i nagrywamy filmiki, piszemy wiadomości, maile, korzystamy z nawigacji, zbieramy mnóstwo danych i komunikujemy się z całym światem, a wszystko to mamy w zasięgu naszych palców.

Z tego powodu urządzenia mobilne stały się narzędziem również dla przestępców, pozwalające im

szpiegować potencjalne cele, szantażować, lub być w ciągłym kontakcie z gangiem. Zatem telefony komórkowe okazują się coraz ważniejszymi świadkami w walce z przestępczością. Dane przechowywane na urządzeniach mobilnych skupiają coraz większą uwagę w śledztwach, i od tej pory będą równie ważne jak cyfrowe dokumenty i e-maile.

Szeroki wachlarz producentów i urządzeń na rynku mobilnym sprawia, że badanie treści urządzeń mobilnych jest ogromnym wyzwaniem. Jednak wraz z rozwojem nowych technologii i oprogramowania zrewolucjonizowano proces gromadzenia dowodów z podejrzanych urządzeń mobilnych. Specjalne urządzenia, takie jak UFED (Universal Forensic Extraction Device) może analizować telefony komórkowe, smartfony, tablety, oraz urządzenia nawigacyjne i palmtopy w sposób zgodny z informatyka śledczą, pomagając odkryć relacje pomiędzy poszczególnymi telefonami komórkowymi.

Odzyskiwanie skasowanych informacji

Odzyskiwanie danych z dysku twardego komputera w porównaniu z pozyskaniem skasowanych danych z telefonu jest dość łatwą sprawą, ale skasowane dane z telefonu komórkowego są prawie niemożliwe do odzyskania.

Ogólnie rzecz biorąc, telefony komórkowe zachowują się podobnie do komputerów stacjonarnych. Jednak, wskutek standardów własnych wszystkie informacje są inaczej traktowane i przechowywane. Obszerne badania i ogromne wysiłki rozwojowe wreszcie doprowadziły do rozwiązania, które zapewnia wsparcie dla szerokiego zakresu - ponad 13 000 - profilów urządzeń mobilnych, działających na większości znanych platform, w tym Android, iPhone, Windows Mobile, Blackberry i innych.

Powiązania pomiędzy telefonami komórkowymi

Aby śledzić zorganizowana przestępczość, bardzo ważne jest aby pokazać i udowodnić powiązania i relacje pomiędzy poszczególnymi telefonami komórkowymi. Umiejętność zobrazowania wzorów komunikacji wśród podejrzanych może doprowadzić do szybkiego zamknięcia śledztwa. W celu skrócenia czasu dochodzenia śledczy pilnie potrzebują narzędzi do odnajdywania i obrazowania relacji komunikacyjnych

Zachowanie czystości dowodów

Śledczy zmagają się z dwoma głównymi zadaniami: po pierwsze, zebrane dane musza być przekształcone w odpowiedni format, który jest czytelny, konkretny i łatwy do zrozumienia, również przez sędziego, który może dysponować mniejsza wiedza techniczną. Po drugie, telefon komórkowy musi być zachowany dokładnie w takim samym stanie w jakim został znaleziony w miejscu zbrodni. Dlatego tez rozwiązania takie jak UFED musza być zgodne z tymi wymaganiami.

Pożytek w terenie

Kluczowym elementem sukcesu nowej generacji urządzeń informatyki śledczej jest z pewnością fakt iż policjanci bez specjalnych technicznych umiejętności czy intensywnego szkolenia powinni być w stanie zabezpieczyć dowody z urządzeń mobilnych. To zaoszczędziłoby czas i pieniądze. W skutek ostatnich osiągnięć, możliwość wydobycia nawet utraconych danych z urządzeń mobilnych otworzyły nowe możliwości w walce z przestępczością dla organów ścigania. Tym samym doskonale narzędzie dla przestępców stało się jednocześnie narzędziem ułatwiającym ich schwytanie.

Autor jest ekspertem technologii informatyki śledczej u niemieckiego producenta rozwiązań mobile forensic Cellebrite GmbH.

Potężne wsparcie dla analiz śledczych

Mediarecovery ogłosiła właśnie zakończenie testów i rozpoczęcie produkcji duplikatora MediaImager. To pierwszy polski produkt tej kategorii sprzętu dla informatyki śledczej. Co najważniejsze nie ustępuje duplikatorom amerykańskim, a nawet je przewyższa.

Duplikatory pozwalają na wykonywanie kopii binarnych. Są zatem niezbędne każdemu specjaliście, który musi je wykonywać. Czy to w terenie, towarzysząc policji w zabezpieczeniach, czy to w laboratorium do którego zwożone są dyski zarekwirowane przez organa ścigania, czy też w końcu w dziale bezpieczeństwa firm, które wykonują kopie binarne dysków odchodzących pracowników.

Na rynku jest wiele urządzeń tego typu, chyba najpowszechniejsze są duplikatory pozwalające na wykonanie jednej maksymalnie dwóch kopii naraz. Ich użycie w sytuacji kiedy zabezpieczonych dysków jest 100 powoduje kilka dni bezczynności informatyka śledczego podczas, których cały proces się odbywa. Szybkość przesyłu danych też bywa dyskusyjna.

Specjaliści z laboratorium informatyki śledczej Mediarecovery, w oparciu o swoje prawie 10-letnie doświadczenia, i tysiące godzin przepracowane z użyciem duplikatorów mieli aktywny wkład w zaprojektowanie MediaImager. Można powiedzieć, że jest to urządzenie zaprojektowane przez praktyków dla praktyków. I widać to chociażby w specyfikacji technicznej. Jeśli dodamy do tego niewielkie rozmiary (276 x 202 x 103 mm) i wagę mamy narzędzie odpowiadające współczesnym realiom i będące poważnym wsparcie każdego specjalisty informatyki śledczej.

Design and assembled by

mediarecovery

Więcej informacji o produkcie udziela:

Tomasz Tatar | Mediarecovery
ttatar@mediarecovery.pl
tel.: +48 509 921 713

Agata Machura | Mediarecovery
amachura@mediarecovery.pl
tel.: +48 517 918 156

Polski Duplikator mediaimager GM^4

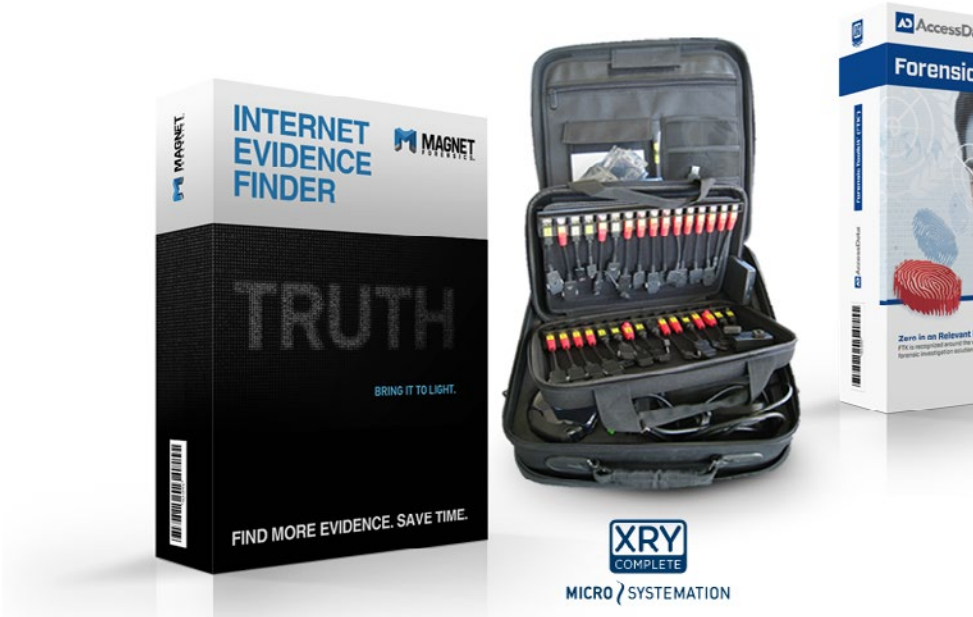
- Maksymalna przepustowość 6Gbps.
- Pełne bezpieczeństwo wykonywania kopii źródła (MediaBlocker).
- Obsługa dysków: SATA, IDE, mSATA, SCSI, pamięci FLASH, SAS, USB, SDD.
- 8 portów USB 3.0, 4 porty SATA/SAS, 2 porty USB 2.0, 1 port SFF-8088 (x4 SATA/SAS), 1 port: DisplayPort, PS2, eSATA oraz LAN.
- Możliwość podłączenia dodatkowo 4 twardych dysków oraz 4 dysków USB.
- Równoczesne tworzenie wielu kopii tego samego dysku oraz kopii różnych dysków.
- System operacyjny Microsoft Windows 7.
- Opcja tworzenia „w locie" zaszyfrowanego obrazu dysku algorytmem AES-128, AES-192, AES-256.
- Mechanizmy weryfikacji akwizycji (MD5, SHA1, SHA2).
- Podgląd struktur danych i systemu plików „na żywo" – najpopularniejsze formaty plików NTFS, FAT.
- Możliwość usuwania danych poprzez nadpisywanie 1, 2, 3, 6, 7, 9, 35-krotne.
- Intuicyjny dotykowy interfejs użytkownika o przekątnej 10,4", dający pełną kontrolę nad procesem zabezpieczania dysków.
- Wyjście HDMI/DVI.

Licencje na narzędzia informatyki śledczej

Jarosław Góra

Wprowadzenie

Zgodnie z aktualnie obowiązującymi regulacjami prawnymi programy komputerowe mogą podlegać ochronie na gruncie prawa autorskiego. Warto wskazać, że ochronie podlega kod źródłowy oraz wynikowy, lecz zbiór funkcjonalności, język programowania, czy też format plików używanych w programie komputerowym, które nie są wyrażeniem programu już nie. Program komputerowy jest przy tym utworem specyficznym, bowiem już samo korzystanie z niego, zgodnie z jego przeznaczeniem, wkracza w monopol prawnoautorski podmiotu uprawnionego i wymaga uzyskania zgody. Zgoda ta przybiera postać licencji, która określa zakres zgodnego z prawem i nienaruszającego praw podmiotu uprawnionego korzystania z programu. Każdy informatyk śledczy powinien doskonale znać swoje narzędzia, a zatem powinien znać również treść licencji związanej z oprogramowaniem, z którego korzysta. Osobiście spotkałem niewielu informatyków śledczych, którzy rzeczywiście przeczytali licencje związane z programami, jakich używali, a szkoda, bo można w nich znaleźć bardzo interesujące zapisy.



Po lekturze

Zadałem sobie trochę trudu i przeczytałem dziesiątki licencji na oprogramowanie przeznaczone do informatyki śledczej. Były to licencje zarówno komercyjne, trialowe, freeware'owe, jak i rozpowszechniane na tzw. wolnych licencjach. Poniżej kilka spostrzeżeń oraz ciekawostek. Oczywiście zasadą jest, że programy te rozpowszechniane są na zasadzie licencji niewyłącznych. Programów „szytych na miarę", co do których udzielana byłaby licencja wyłączna albo przenoszone byłyby autorskie prawa majątkowe nie miałem okazji przeanalizować. W wielu dokumentach licencyjnych podkreślano, iż oprogramowanie jest licencjonowane, a nie sprzedawane, co związane jest zapewne z problematyką możliwości lub braku możliwości dalszej odsprzedaży oprogramowania. Do tego tematu producenci oprogramowania podchodzą różnie. Niektórzy kategorycznie wyłączają możliwość przenoszenia licencji na inne podmioty, inne uzależniają to od uzyskania zgody, jeszcze inne przewidują konieczność uiszczenia opłaty z tego tytułu, a jeden z producentów chwali się nawet, że inaczej niż konkurenci on pozwala na przenoszenie praw z licencji na dowolny podmiot. Kwestia prawnej możliwości przenoszenia praw wynikających z licencji na oprogramowanie w ogóle jest problematyczna, nawet bez wyłączania takiej możliwości (czy skutecznie?) w umowach. Warto przypomnieć tylko w tym miejscu głośny wyrok w sprawie Oracle vs. UsedSoft, gdzie Trybunał Sprawiedliwości UE dnia 3 lipca 2012 r. (C – 128/11) orzekł na korzyść UsedSoft w oparciu o zasadę wyczerpania prawa. W wielu licencjach pojawiały się warunki co do osób, które mogą korzystać z oprogramowania oraz miejsc i sprzętu. Niektóre ograniczały możliwość korzystania z oprogramowania jedynie przez pracowników licencjobiorcy, co w czasach popularnych umów cywilnoprawnych, tzw. samozatrudnienia lub współpracy z podmiotami zewnętrznymi może być problematyczne. Inne z kolei szeroko

określały krąg osób uprawnionych. Jeśli chodzi o miejsce i sprzęt, jedne licencje wymagały instalacji na sprzęcie będącym własnością licencjobiorcy (co z leasingiem? co z BYOD?), inne bardziej liberalnie podchodziły do tematu. W przypadku miejsca, w którym korzystać można z programu, ciekawe okazały się niektóre ograniczenia zabraniające tego poza siedzibą licencjobiorcy – odpada praca w terenie. Część licencji wyłączała odpowiedzialność licencjodawcy w przypadku wykorzystania oprogramowania w miejscach wrażliwych, tj. szpitale, czy elektrownie. Co jednak ciekawsze licencje te wskazywały, iż licencjodawca nie daje gwarancji, że w takich miejscach oprogramowanie będzie działało prawidłowo – zabezpieczenie danych w szpitalu odpada. Niektóre wyłączały możliwość uzyskania licencji w ogóle, w przypadku gdy licencjobiorca pochodziłby z kraju wspierającego zdaniem USA terroryzm. W tych krajach informatycy śledczy mają zdaje się utrudnione życie. Jeśli chodzi o narzędzia darmowe, to w wielu przypadkach okazywało się, iż tak całkiem darmowe one nie są lub ograniczają możliwości ich wykorzystania. Jedne, które rzeczywiście nie zawierały ukrytych kosztów, zabraniały komercyjnego wykorzystywania, inne przewidywały ograniczenia w funkcjonalności. Jeśli natomiast chodzi o ukryte koszty dotyczące freeware'owego oprogramowania, to w jednym przypadku licencja przewidywała konieczność wzięcia przez licencjobiorcę udziału w szkoleniu, już nie darmowym.

Podsumowanie

Rodzajów licencji i przeróżnych klauzul związanych z korzystaniem z oprogramowania wykorzystywanego w informatyce śledczej jest mnóstwo. Informatyk śledczy korzystający z danego narzędzia z całą pewnością powinien dokładnie zapoznać się z jego licencją, aby później jego brak wiedzy w tym zakresie nie został wykorzystany przeciwko niemu, podważając jego kompetencje, np. w oczach sądu.

Autor jest adwokatem, szefem zespołu prawa własności intelektualnej i nowych technologii w kancelarii Ślązak, Zapiór i Wspólnicy. Trener w Akademii Informatyki Śledczej.

Informatyka śledcza zgodna z ISO 27001:2013

Jednostka certyfikująca TÜV Nord Polska zakończyła proces certyfikacji na zgodności z normą ISO 27001:2013 w laboratorium informatyki śledczej Mediarecovery. Jest to pierwszy wydany przez TUV Nord Polska certyfikat systemu zarządzania bezpieczeństwem informacji po aktualizacji normy we wrześniu ubiegłego roku.

Jak mówi Przemysław Szczurek, product manager ds. bezpieczeństwa informacji w TÜV Nord – Certyfikacja przebiegła niezwykle sprawnie z uwagi na fakt, że Mediarecovery miała już wcześniej opracowane procedury wewnętrzne zbieżne z wymaganiami ISO 27001:2013. Certyfikat potwierdza, że laboratorium informatyki śledczej skutecznie wdrożyło i utrzymuje system zarządzania bezpieczeństwem informacji. Warto przypomnieć, że poprzednia wersja normy ISO 27001 pochodziła z 2005 roku. Jej nowelizacja była niezbędna gdyż nie do końca odpowiadała współczesnym realiom. Rewolucja urządzeń mobilnych z jaką mamy do czynienia od kilku lat, nagły boom portali społecznościach wymusiły wprowadzenie zmian. Warto przypomnieć, że iPhone pojawił się w sprzedaży w 2007 roku, a rok później Mark Zuckberg, twórca Facebook'a został najmłodszym miliarderem świata.

Wykorzystanie urządzeń prywatnych do realizacji zadań służbowych, tzw. BYOD, również wymagało zmian w zakresie zabezpieczeń wymaganych przez międzynarodowy standard. Nowe wydanie, jeszcze silniej niż wydanie z roku 2005, akcentuje potrzebę ciągłej analizy ryzyk i posiadania przez firmy pewności, iż zidentyfikowane ryzyka będą odpowiednio zarządzone.

Sebastian Małycha, prezes Mediarecovery uważa, że uzyskany certyfikat ugruntowuje pozycję firmy na rynku bezpieczeństwa IT. Jak mówi – Cieszę się, że wypracowane przez nas praktyki dotyczące bezpieczeństwa danych znalazły swoje odzwierciedlenie w normie ISO 27001. Dodaje również, że certyfikat potwierdza kompetencje dotyczące implementacji systemów bezpieczeństwa i prowadzonych analiz informatyki śledczej.

Firma swoją ofertę kieruje przede wszystkim do sektora bankowego, finansowego, energetycznego i przemysłu ciężkiego. Nowością w ofercie jest tworzenie tzw. Security Operations Centre. Składają się na nie zaawansowane rozwiązania informatyczne ale również zmiana procedur i zasad organizacyjnych bezpieczeństwa.

Jednak najbardziej istotna jest zmiana mentalna w podejściu do bezpieczeństwa IT – twierdzi Sebastian Małycha. Przeciwko obecnym cyberzagrożeniom nie można stosować zabezpieczeń opartych o zasady sprzed 10 lat. Dziś bezpieczeństwo IT wymaga holistycznego spojrzenia na problem – dodaje prezes Mediarecovery.

VI Ogólnopolska Konferencja Informatyki Śledczej

Wśród prelegentów tegorocznej konferencji znaleźć można było m.in. Polaka pracującego Centralnym Laboratorium Kryminologii Komputerowej Metropolitan Police w Londynie. Przybliżył on praktyki policji brytyjskiej związane z analizami elektronicznego materiału dowodowego. Swój wykład zaprezentowali również przedstawiciele rosyjskiej firmy specjalizującej się w tworzeniu narzędzi do analiz śledczych.

Grono wykładowców było jednak szersze, a wśród nich znaleźć można było Osoby od dawna znane w naszym środowisku. Dzięki temu uczestnicy zyskali możliwie szeroki przegląd najnowszych narzędzi oraz spojrzeń taktycznych i proceduralnych.

Jak mówi Przemysław Krejza, prezes Stowarzyszenia Instytut Informatyki Śledczej – Nasze coroczne konferencje są dla wielu specjalistów jedyną szansą na wymianę doświadczeń i poszerzenie wiedzy. Paradoks polega na tym, że informatyka śledcza jest obecnie niezbędna do właściwej analizy materiału dowodowego ale polscy fachowcy nie mają skąd czerpać wiedzy w kraju. *Misją naszego stowarzyszenia jest popularyzowanie najlepszych praktyk informatyk śledczej. Robimy to poprzez cykl szkoleń o nazwie „Certyfikowany Informatyk Śledczy" oraz coroczne konferencje* – dodaje Krejza.

Ze szkoleń organizowanych przez Instytut Informatyki Śledczej korzysta corocznie kilkadziesiąt osób. Po jego ukończeniu specjalista, jest w stanie poradzić sobie z praktycznie każdą analizą śledczą. Zdaniem Przemysława Krejzy jest to ciągle zbyt mała liczba fachowo przygotowanych ludzi. Część opinii z zakresie informatyki śledczej przygotowywanych jest w sposób urągający wypracowanym przez lata najlepszym praktykom – twierdzi. Prowadzić to może do podważania zdobytych w ten sposób dowodów i poszlak.

VI Ogólnopolska Konferencja Informatyk Śledczej odbyła się pod patronatem honorowym Biura Bezpieczeństwa Narodowego, Ministerstwa Sprawiedliwości i Prokuratury Generalnej.

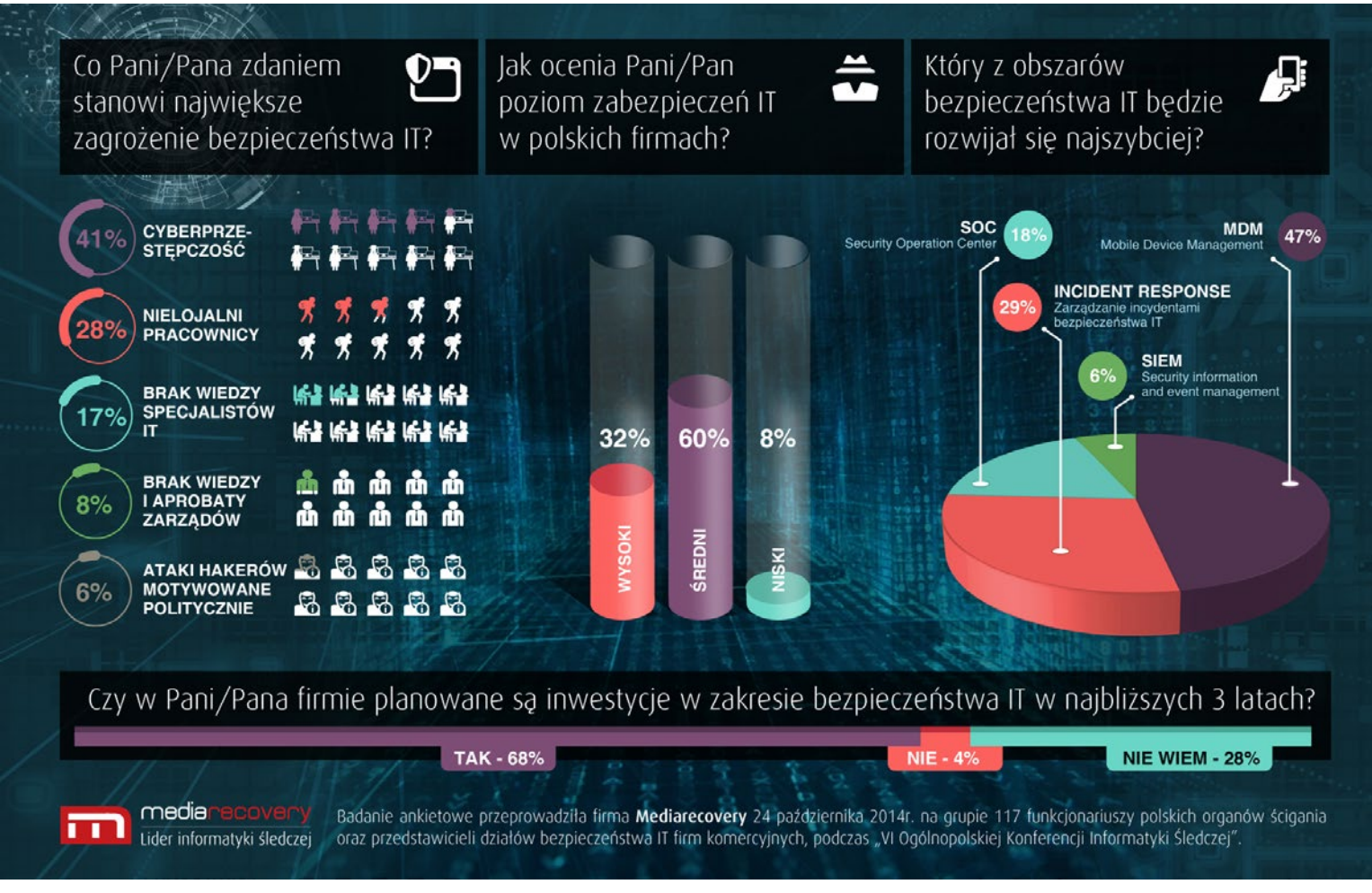
Cyberprzestępczość, MDM i średni poziom

Ciekawe badania zaprezentowało ostatnio laboratorium informatyki śledczej Mediarecovery.

Wynika z nich, że polscy specjaliści bezpieczeństwa IT obawiają się przede wszystkim cyberprzestępczości. Wskazało tak 41% badanych. Jak podejrzewam oparte jest to na konkretnych przesłankach. Środowisko IT, a szczególnie „security" raczej sceptycznie podchodzi do rewelacji przekazywanych przez producentów sprzętu i oprogramowania. Węszą w tym intencje marketingowe, nie informacyjne. Dlatego sądzę, że tą odpowiedź wskazali ci, którzy mieli już z tego typu przypadkami do czynienia.

Jeszcze ciekawiej jest w kolejnych pytaniach. Jeśli przyjmiemy, że właściwy jest jedynie wysoki poziom zabezpieczeń to wychodzi na to, że w 92% firm jest z tym źle. Co prawda 60% oceniło go jako średni, jednak można zakładać, że i tak nie jest to to czego ankietowany specjalista IT security sobie by życzył. Pozostaje zazdrościć tym 8%, które uznały poziom za wysoki. Nie będzie zaskoczeniem jeśli podamy, że wśród najszybciej rozwijających się obszarów bezpieczeństwa IT aż 47% padło na Mobile Device Management. To rzeczywiście coraz bardziej powszechny problem. I wszystko na to wskazuje, że będzie narastał. Interesujące jest na przykład, w którą stronę będą ewoluować te wszystkie „iWatch" czy „Google Watch". Sądzę, że to z czym mamy teraz do czynienia w zakresie urządzeń przenośnych to dopiero czubek góry lodowej.

Poziom bezpieczeństwa IT w polskich firmach i instytucjach.



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