MAGAZYN

NR 14/CZERWIEC 2012

INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

8 LAT WIĘZIENIA ZA 90 EURO?
UWAGA NA CYBERPRZESTĘPCÓW

JAK SKUTECZNIE CHRONIĆ
INTERESY PRZEDSIĘBIORCY?

IV OGÓLNOPOLSKA KONFERENCJA
INFORMATYKI ŚLEDCZEJ

GDZIE SZUKAĆ DOWODÓW
ELEKTRONICZNYCH?

8 lat więzienia za 90 euro? Uwaga na cyberprzestępców

W ostatnich dwóch tygodniach zarejestrowaliśmy duże ilości spamu mającego na celu „złowienie" jak największej liczby ofiar, które będą częścią struktury piorącej brudne pieniądze – mówi Elżbieta Kasprzyk z gateProtect, producenta zabezpieczeń sieciowych dla firm. Warto zauważyć, że w obecnym wydaniu akcji, cyberprzestępcy posługują się poprawną polszczyzną co zmniejsza poziom czujności internautów.taki w żadem sposób nie umożliwia natomiast, powiązania go z osobą potencjalnego podejrzanego lub oskarżonego.

Złego dobre początki

Zaczyna się niewinnie od e-maila proponującego współpracę z zagraniczną kliniką jako zdalny pomocnik bez specjalistycznej wiedzy i wykształcenia. Stawka - 90 euro za godzinę. Inna propozycja to po prostu sposób na dorobienie sobie polegające na „przetwarzaniu napływających do Twojego miasta zamówień". Tu można zarobić od 200 do 500 euro za każde zamówienie.

Obraz malowany przez cyberprzestępców

W niektórych przypadkach cyberprzestępcy proponują nawet podpisanie umowy o pracę, dzwonią lub smsują ze swoimi „pracownikami" za pomocą bramek internetowych. Wszystko wygląda bardzo prawdziwie jednak wcale takim nie jest – mówi Zbigniew Engiel z laboratorium Mediarecovery. W większości przypadków „praca" kończy się na wykonaniu jednego zlecenia – dodaje.

Rzeczywistość

Cyberprzestępcy wchodzą w posiadanie danych dostępowych do bankowych kont internetowych. Następnie wysyłają pieniądze na konta osób, tzw. „słupów", którzy zostali przez nich „zatrudnieni". Zadaniem „słupa" jest wypłacenie tych pieniędzy i po odjęciu swojej części przekazanie dalej za pośrednictwem firm zajmujących się międzynarodowym transferem gotówki. Ucieszeni szybkim i prostym zarobkiem niecierpliwie oczekują na kolejne zadanie, które zazwyczaj nie przychodzi.

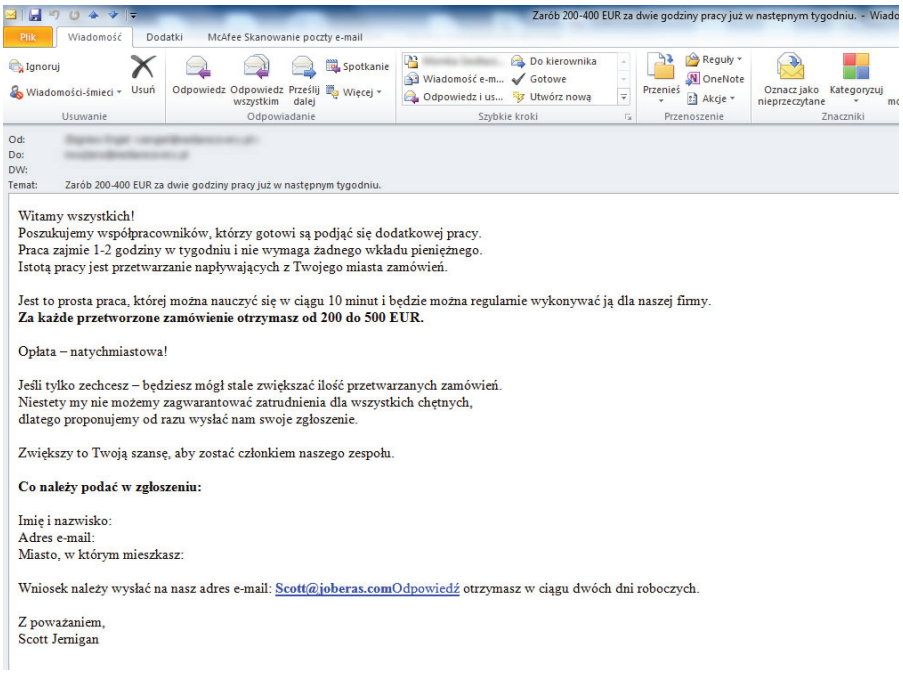
Kara

Jak mówi Emil Melka, adwokat, były szef wydziału przestępczości gospodarczej Prokuratury Okręgowej w Katowicach – *Organa ścigania mogą zakwalifikować takie działania jako współudział w tzw. przestępstwie „prania brudnych pieniędzy" z art. 299 par. 1 kodeksu karnego albo pomocnictwo w tym procederze.* Jest to zagrożone karą pozbawienia wolności do lat 8. *W przypadku znalezienia dowodów na istnienie porozumienia sprawcy z innymi osobami lub w wypadku osiągnięcia znacznej korzyści majątkowej – zagrożenie karą pozbawienia wolności zwiększa się do górnej granicy 10 lat* – dodaje.

Specjaliści z laboratorium informatyki śledczej Mediarecovery ostrzegają przed nową odsłoną akcji cyberprzestępców skierowaną w polskich internautów.

Jak nie zostać „słupem"?

Ofiarą sprytu cyberprzestępców może zostać każdy, licealista, student, matka wychowująca dzieci, emeryt czy osoba aktywna zawodowo. Dlatego warto zachować zdrowy rozsądek czytając niecodzienne propozycje otrzymane mailem – mów Elżbieta Kasprzyk z gateProtect. Firmy mogą chronić swoich pracowników korzystając z systemów antyspamowych wyposażonych również w moduł antyphishingowy, chroniący użytkowników przed wyłudzeniem danych dostępowych do konta – dodaje. Użytkownicy prywatni powinni wyposażyć swoje komputery w oprogramowanie chroniące. Wiele takich programów jest dostępnych w sieci za darmo. ■



Zarób 200-400 EUR za dwie godziny pracy już w następnym tygodniu. - Wiadomość

Plik | Wiadomość | Dodatki | McAfee Skanowanie poczty e-mail

Ignoruj | Usuń | Odpowiedz | Odpowiedz wszystkim | Prześlij dalej | Spotkanie | Więcej | Do kierownika | Wiadomość e-m... | Gotowe | Odpowiedz i us... | Utwórz nową | Przenieś | Reguły | OneNote | Akcje | Oznacz jako nieprzeczytane | Kategoryzuj

Usuwanie | Odpowiadanie | Szybkie kroki | Przenoszenie | Znaczniki

Od:
Do:
DW:
Temat: Zarób 200-400 EUR za dwie godziny pracy już w następnym tygodniu.

Witamy wszystkich!
Poszukujemy współpracowników, którzy gotowi są podjąć się dodatkowej pracy.
Praca zajmie 1-2 godziny w tygodniu i nie wymaga żadnego wkładu pieniężnego.
Istotą pracy jest przetwarzanie napływających z Twojego miasta zamówień.

Jest to prosta praca, której można nauczyć się w ciągu 10 minut i będzie można regularnie wykonywać ją dla naszej firmy.
Za każde przetworzone zamówienie otrzymasz od 200 do 500 EUR.

Opłata – natychmiastowa!

Jeśli tylko zechcesz – będziesz mógł stale zwiększać ilość przetwarzanych zamówień.
Niestety my nie możemy zagwarantować zatrudnienia dla wszystkich chętnych,
dlatego proponujemy od razu wysłać nam swoje zgłoszenie.

Zwiększy to Twoją szansę, aby zostać członkiem naszego zespołu.

Co należy podać w zgłoszeniu:

Imię i nazwisko:
Adres e-mail:
Miasto, w którym mieszkasz:

Wniosek należy wysłać na nasz adres e-mail: Scott@joberas.comOdpowiedź otrzymasz w ciągu dwóch dni roboczych.

Z poważaniem,
Scott Jernigan

Jak skutecznie chronić interesy przedsiębiorcy?

Jakub Ślązak

Przed niespełna pięciu laty, światowe media zainteresowały się przypadkiem Joy'i Williams (pracownicy Coca – Coli), która została podejrzana o kradzież jednej z najbardziej skrywanych tajemnic współczesnego świata – składu flagowego napoju koncernu.

NAJWIĘKSZYM ZAGROŻENIEM DLA PRZEDSIĘBIORCY STAĆ MOGĄ SIĘ JEGO WŁASNI PRACOWNICY

Pomimo licznych zabezpieczeń, receptura ta, znana dotychczas jedynie wąskiej grupie osób, została wykradziona i udostępniona konkurencji. Pepsi, bo o niej mowa, nie zdecydowała się jednakże na dokonanie zakupu. Zamiast tego, złożyła zawiadomienie o popełnieniu przestępstwa i wykorzystała całą sytuację na własną korzyść - o sprawie powiadomiona została prasa, która przedstawiła Pepsi, jako koncern praworządny oraz uważający, iż jego napój jest lepszy od serwowanego przez głównego konkurenta. Coca – Cola z całej sytuacji wyszła z nieco nadszarpniętą reputacją, jednakże uniknęła wielomilionowych strat finansowych. Zasady bezpieczeństwa w firmie zostały zaostrzone, a sama receptura nadal pozostaje tajemnicą dla opinii publicznej. Powyższy przykład ilustruje problem, który na znaczeniu przybrał w przeciągu ostatnich kilku lat - największym zagrożeniem dla przedsiębiorcy stać mogą się jego własni pracownicy. O ile bowiem stosunkowo łatwo zabezpieczyć firmę przed atakami z zewnątrz, o tyle niezmiernie ciężko jest uchronić tajemnicę przedsiębiorstwa przed próbami jej kradzieży, pochodzącymi od osób, na co dzień mających z nią do czynienia. Przed takim właśnie problemem stają każdego dnia przedsiębiorcy, dla których informacja stanowi o posiadanej przez nich przewadze konkurencyjnej. Niestety, jak dowodzą publikowane obecnie badania, „statystyczny" przedsiębiorca nie posiada świadomości dot. wartości posiadanych informacji, jak również w niemalże żaden sposób ich nie zabezpiecza. Najczęściej z problemem styka się dopiero, gdy do kradzieży tych informacji dochodzi. Wtedy na jaw wychodzi brak możliwości podjęcia działań mających na celu odzyskanie utraconych zasobów oraz niemożność zgromadzenia materiału dowodowego umożliwiającego identyfikację sprawcy i jego ukaranie. Co gorsza, często bezpośrednia konkurencja wchodzi w posiadanie wykradzionych informacji, które następnie wykorzystuje we własnej działalności. Dostępna technologia pozwala na znaczny wzrost poziomu ochrony interesów przedsiębiorcy. Odpowiednie oprogramowanie umożliwia precyzyjne śledzenie ruchu w sieci, blokowanie możliwości kopiowania określonych informacji, bądź limitowanie dostępu do nich. W myśl zasady „chcieć to móc", każdy pracodawca może istotnie ograniczyć ryzyko wycieku tajemnicy przedsiębiorstwa. Ważne jest natomiast, aby samej świadomości zagrożeń, towarzyszyła determinacja w działaniu, oraz oczywiście chęć przeznaczenia na ten cel określonego zasobu środków. W treści kolejnych artykułów, postaram się przybliżyć aspekty prawne związane z ochroną interesów przedsiębiorcy. Warto bowiem podkreślić, iż zabezpieczeniu informatycznemu towarzyszyć musi określona profilaktyka prawna. Wszystkie podejmowane przez przedsiębiorców działania muszą pozostawać w zgodzie z obecnym prawodawstwem tak, aby to przedsiębiorca nie naraził się na zarzut, iż swoimi działaniami nie-

WARTO BOWIEM PODKREŚLIĆ, IŻ ZABEZPIECZENIU INFORMATYCZNEMU TOWARZYSZYĆ MUSI OKREŚLONA PROFILAKTYKA PRAWNA

dopuszczalnie narusza dobra osobiste pracowników, bądź też akty prawne regulujące całkowicie odrębną materię. Nieprzemyślane posunięcia mogą skutkować licznymi negatywnymi następstwami – od odpowiedzialności karnej poczynając (art. 267 k.k., art. 49 – 54 ustawy o ochronie danych osobowych), poprzez odpowiedzialność cywilną (odszkodowanie, zadośćuczynienie), a na powstaniu uszczerbku, w tworzonym przez lata wizerunku, kończąc. Z drugiej natomiast strony, o ile zabezpieczeniu informatycznemu towarzyszyć będzie zabezpieczenie prawne, wówczas działania podejmowane przez przedsiębiorców mogą przynieść, w dłuższej perspektywie czasu, same niemalże korzyści. Pierwszą i najistotniejszą rzeczą jest zdanie sobie sprawy z istniejących ograniczeń, co zostało zasygnalizowane już powyżej – tj. praw posiadanych ▸

przez pracowników oraz możliwości (a w zasadzie braku możliwości) ich naruszania. Obowiązujący system prawny przewiduje szeroki katalog regulacji, które gwarantują pracownikom (jako osobom fizycznym), w szczególności:

- prawo do ochrony życia prywatnego, dobrego imienia (art. 47 Konstytucji RP),
- prawo do wolności komunikowania się (art. 49 Konstytucji RP),
- prawo do ochrony danych osobowych (art. 1 ust. 1 ustawy o ochronie danych osobowych)
- obowiązek poszanowania ich godności oraz innych dóbr osobistych przez pracodawcę (art. 11 (1) kodeksu pracy),
- ochronę posiadanych dóbr osobistych - których katalog jest w zasadzie nieograniczony (art. 23 kodeksu cywilnego),

oraz wiele innych uprawnień, mających swoje źródło w odrębnych aktach prawnych. W/w prawa pracowników, w istotny sposób zawężają pracodawcy dopuszczalne możliwości działania. Wszelkie bowiem kroki pracodawcy, prowadzące do zwiększenia poziomu ochrony własności przedsiębiorstwa, naruszać mogą prawnie chronione interesy pracowników. Przykładowo, pracodawcy często próbują uzyskać wgląd w całość prowadzonej przez pracowników korespondencji (w tym prywatnej). Technika nie tylko daje możliwość archiwizacji wszelkich przychodzących oraz wychodzących e-maili, lecz również uzyskiwania wglądu w treść wiadomości szyfrowanych, które wysyłane są za pośrednictwem służbowego komputera. Działania takie, jakkolwiek często uzasadniane słusznymi pobudkami, w niedopuszczalny sposób wkraczają w sferę prywatności zatrudnionych osób. Odpowiednio przygotowany regulamin pracy może jednakże zapobiec wykorzystywaniu sprzętu służbowego do celów prywatnych (np. pod groźbą kar dyscyplinarnych, bądź rozwiązania stosunku pracy).

Świadomość istniejących ograniczeń oraz respektowanie prawnie chronionych interesów pracowników spowoduje, iż pracownicy Ci nabiorą przekonania, że pracodawca dostrzega oraz szanuje ich prawa. Z drugiej strony, ograniczenia te uświadomią samemu przedsiębiorcy, że liczba skutecznych sposobów ochrony jego interesów jest istotnie ograniczona. Szeroko pojmowany monitoring, bo do niego zmierzam, wydaje się jedynym środkiem łączącym prewencję oraz możliwość skutecznej reakcji na pojawiające się incydenty. Kolejny wpis poświęcę właśnie pojęciu monitoringu, korzyściach jakie ze sobą niesie oraz potrzebie przygotowania przedsiębiorstwa od strony prawnej na jego wprowadzenie. ■

Autor jest aplikantem radcowskim w Kancelarii Adwokatów i Radców Prawnych Ślązak, Zapiór i Wspólnicy, Spółka Komandytowa w Katowicach.

Gdzie szukać dowodów elektronicznych?

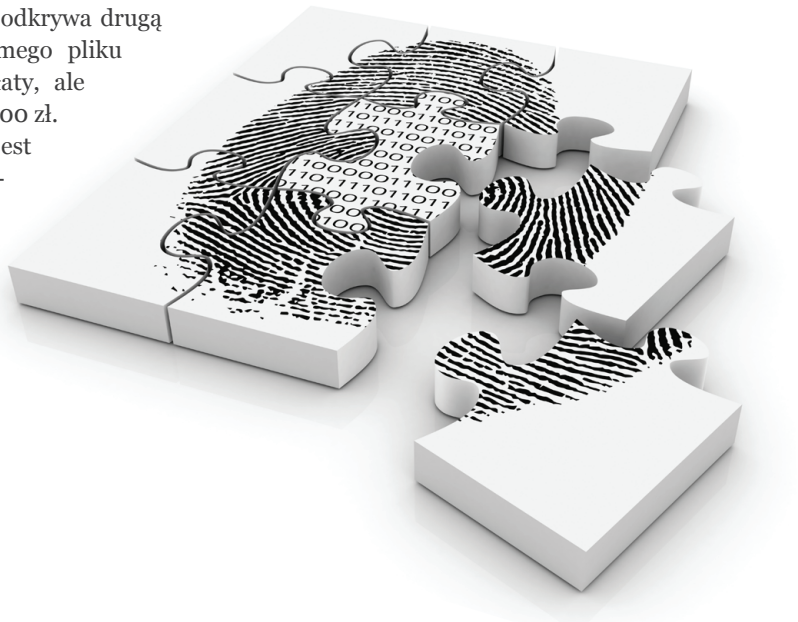
–dokończenie z poprzedniego numeru

Emil Melka

Jak wszechobecność dowodów elektronicznych ma się do życia codziennego przeciętnego sprawcy przestępstwa – Jana Kowalskiego ? Oto przykład. Jan Kowalski przerabia dowód wpłaty kwoty, którą winien jest operatorowi telefonii komórkowej i czyni to za pomocą przerobienia pliku „pdf". Dokonuje rzeczywistej wpłaty kwoty 1 zł. przez bankowe konto internetowe, należące do jego byłej narzeczonej. Następnie edytuje plik „pdf", który jest potwierdzeniem dokonania przelewu i dopisuje na nim trzy zera, uzyskując kwotę wpłaty 1.000 zł., którą winien jest operatorowi.

Taki wydruk Jan Kowalski przesyła pocztą do swojego operatora jako dowód zapłaty za usługi abonenckie. Proceder ten wykrywa oczywiście po jakimś niedługim czasie system księgowy operatora telefonicznego i – tu pomijamy wewnętrzny, nieskuteczny tryb wyjaśnienia sprawy przez samego operatora – sprawa zostaje skierowana na policję, która wszczyna postępowanie o wyłudzenie mienia w kwocie 999 zł. i podrobienie dokumentu. Policji Jan Kowalski tłumaczy, że jest niewinny i o niczym nie wie, a poprosił jedynie swoją byłą już narzeczoną o przysługę w postaci zapłaty tysiąca złotych z jej konta bankowego za niego, bo sam nie miał wówczas żadnych dochodów. Jan Kowalski tłumaczy, iż nie wie, że jego była narzeczona dokonała jakiegokolwiek fałszerstwa i że był święcie przekonany, iż jest rozliczony względem operatora, bo była już narzeczona obiecała przelewu dokonać. Jan Kowalski dodaje także ze złośliwym uśmieszkiem, iż była narzeczona wyszła za mąż, zmieniła nazwisko i wyjechała z obecnym mężem za granicę i sugeruje policji wszczęcie poszukiwań międzynarodowych za „przestępczynią". Tłumaczenie to pozornie wiarygodne i w dawnych, słusznie minionych czasach Jan Kowalski zapewne zostałby wypuszczony do domu przez policję, a sam funkcjonariusz złożyłby mu wyrazy współczucia z powodu nieuczciwej byłej narzeczonej. Jednak czasy i wiedza organów ścigania się zmieniły. Jan Kowalski zostaje odwieziony co prawda do domu, ale celem dokonania czynności przeszukania i zabezpieczenia komputera wraz z twardym dyskiem i zabezpieczenia wszelkich nośników pamięci i innych dowodów w sprawie. Tu pamiętać trzeba, iż zgodnie z treścią art. 217 § 1 in fine kodeksu postępowania karnego (k.p.k.) funkcjonariusz policji nie potrzebuje odrębnego postanowienia prokuratora nadzorującego postępowanie przygotowawcze o wydaniu, odebraniu rzeczy, dokonaniu przeszukania osoby i pomieszczeń, lecz wobec sytuacji niecierpiącej zwłoki funkcjonariusz ten dokonuje powyższych czynności na podstawie własnej decyzji i okazaniu legitymacji służbowej lub też po okazaniu polecania jego przełożonego, czy też kierownika jednostki (może nim być dyżurny tejże jednostki policji). Janowi Kowalskiemu w wyniku czynności przeszukania pomieszczeń mieszkalnych i gospodarczych do niego należących, zostaje zabrany komputer i wszystkie nośniki pamięci, które prowadzący postępowanie uzna za ważne, a także drukarka i telefon komórkowy. Komputer zostaje oddany Janowi Kowalskiemu następnego dnia w stanie nienaruszonym, co utwierdza go w przekonaniu, iż zostanie oczyszczony z zarzutów. Jan Kowalski nie wie jednak, iż policja wraz z biegłym z zakresu techniki komputerowej utworzyła tzw. „kopię binarną" dysku twardego jego komputera i na kopii będą dokonane dalsze badania, podczas których zostanie odkryty fakt logowania się na koncie bankowym przez użytkownika komputera, a nadto to, że wśród plików nieaktywnych – usuniętych przez użytkownika z poziomu komputera, znajdował się edytowalny plik „pdf" – dowód zapłaty z wersją pierwotną opiewającą na kwotę 1 zł. Natomiast w pamięci drukarki biegły odkrywa drugą wersję tego samego pliku – dowodu zapłaty, ale już na kwotę 1.000 zł. Jan Kowalski jest ponownie poproszony przez policję na przesłuchanie, tym razem już mniej sympatyczne i teraz tłumaczy się w desperacji tym, iż widocznie to była narzeczona dokonała fałszerstwa w jego domu, podczas jego nieobecności. Wyszkolony policjant uzyskuje z pomocą prokuratora wykaz logowania się telefonu komórkowego Jana Kowalskiego, z którego jasno wynika, że w chwili logowania się na koncie bankowym, tworzenia pliku „pdf" i jego edycji, telefon komórkowy Jana Kowalskiego znajdował się w jego własnym domu. Na takie postawienie faktów Jan Kowalski broni się tym, iż często zdarza mu się wychodzić z domu bez zabierania ze sobą telefonu komórkowego, co istotnie dawałoby mu pewne alibi. Jednak wykaz połączeń wychodzących, co odczytuje biegły w telefonie, wskazuje na połącz nie na numer telefonu byłej narzeczonej w chwili logowania się na jej konto bankowe. Czyżby Jan Kowalski pytał wtedy byłą narzeczoną o hasło ▸

Jan Kowalski tłumaczy, że jest niewinny i o niczym nie wie, a poprosił jedynie swoją byłą już narzeczoną o przysługę w postaci zapłaty tysiąca złotych z jej konta bankowego za niego, bo sam nie miał wówczas żadnych dochodów



dostępu do konta ? Wszystko wskazuje na to, że tak. Tenże dowód stawia przysłowiową kropkę nad „i", a wnioskiem końcowym może być jedynie uzasadnione podejrzenie, iż Jan Kowalski dopuścił się przestępstw wyłudzenia mienia i podrobienia dokumentu i to bez angażowania obcych służb policyjnych w poszukiwanie jego byłej już narzeczonej. Ktoś zapyta, czy warto ponosić tak wysokie koszty postępowania przygotowawczego, koszty ekspertyz i pracy biegłego w sprawie wyłudzenia niewielkiej w sumie kwoty i podrobienia jednego raptem dokumentu. Niżej podpisany twierdzi, że zawsze warto. Po pierwsze dlatego, by nasz Jan Kowalski nie pomyślał nigdy o powtórzeniu swojego „wyczynu"; po drugie, aby nikt inny, kto pozna jego przypadek nie zabrał się za podobną przestępczą działalność, a po trzecie ... Jan Kowalski w wyroku skazującym zostanie obciążony wszystkimi kosztami postępowania karnego, które będzie musiał zwrócić Skarbowi Państwa, nad czym czuwał będzie już niezawisły Sąd. Czuwał będzie skutecznie, bo alternatywą dla Jana Kowalskiego w wypadku niespłacenia kosztów może być odwieszenie wykonania kary pozbawienia wolności, którą Sąd zawiesi jedynie tytułem próby.

Jak organ ochrony porządku prawnego może procesowo zabezpieczyć od Jana Kowalskiego dowód elektroniczny ? Częściowo wskazano to już powyżej, w opisanym przykładzie. Jak takie czynności wyglądają i kiedy mogą się odbyć oraz jakie prawa przysługują osobie, u której czynności te są wykonywane ? To już temat na kolejne, odrębne rozważania. ■

Autor jest obecnie adwokatem specjalizującym się w kwestiach z zakresu cyberprzestępczości, w latach 2008-2009 kierował Wydziałem do Spraw Przestępczości Gospodarczej Prokuratury Okręgowej w Katowicach, jest uznanym wykładowcą wielu konferencji i szkoleń.

W skrócie

EnCase App Central od Guidance Software

Na konferencji CEIC, CTO Guidance Software Shawn McCreight, zaprezentował koncepcję EnCase App Central. Będzie to miejsce gdzie programiści mogą sprzedawać swoje dzieła tworzone na bazie EnScript. Na tą chwilę jest ponad 40 000 użytkowników EnCase na całym świecie więc stanowi to całkiem duży rynek. Jest to również plus z punktu widzenia klientów, którzy będą mogli poprzez App Central uzyskać wsparcie dla rozwiązania swoich problemów, a także przedstawiać swoje opinie i ukierunkowywać programistów pod kątem swoich potrzeb. Start EnCase App Cetnral przewidziano na jesień tego roku.

Hakerzy kontra Piraci?

Jak donosi serwis TorrentFreak znana strona internetowa The Pirate Bay padła ofiarą ataku DDOS i była niedostępna przez 24 godziny. Początkowo spekulowano, że było to wynikiem nieporozumienia pomiędzy Anonymous i Zatoką Piratów. Ofiara ataku zaprzecza jednak by atak był wykonany przez Anonymous. W swoim oświadczeniu piszą m.in. „Wiemy, że to nie Anonimowi stoją za tym atakiem. Możemy nie zgadzać się z nimi we wszystkim, ale i oni, i my chcemy, żeby internet był wolny i otwarty". Póki co zatem nie wiadomo kto był napastnikiem.

„Potwór" kopiujący dane

W ofercie forensictools.pl pojawiła się nowa kopiarka binarna Image MASSter Solo-4 RUGGEDIZED. Urządzenie oferuje kopiowanie 2:2 z pełną przepustowością SATA-2. Można do niego podpiąć zestaw dysków w macierzy przez USB 3.0 czy dodawać karty rozszerzeń na PCI-e. Pełna specyfikacja na witrynie internetowej sklepu. Całość w mogącej wiele znieść walizie.

Podsumowanie pierwszego międzynarodowego CIS-FORUM

Przemysław Bańko

Jeszcze kilkadziesiąt lat temu, synonimem bezpiecznego biznesu były mocne mury, wysoki płot i skuteczna ochrona na bramie. W czasach rozkwitu nowych metod przechowywania danych i elektronicznej komunikacji, te tradycyjne sposoby przestały być sku-

teczne. Dzisiaj, o wiele trudniej upilnować własnego pracownika z pendrivem, niż ówczesnego intruza z łomem.

26 kwietnia 2012 r zorganizowano Pierwsze Międzynarodowe CIS-Forum Bezpieczeństwa Informacji i Zarządzania Usługami IT. Forum odbyło się w Wyższej Szkole Technicznej w Katowicach. Głównym organizatorem Forum był CIS-Certification & Information Security Services – niezależna jednostka certyfikacyjna w zakresie Systemów Zarządzania Bezpieczeństwem Informacji oraz Systemów Zarządzania Usługami IT.

Podczas konferencji wystąpili między innymi:
dr Krzysztof Janik – znamy go wszyscy jako Ministra Spraw Wewnętrznych i Administracji, Posła, Doradcę Prezydenta RP. Pan Minister omówił raport w zakresie bezpieczeństwa wewnętrznego oraz informacyjnego tworzony na potrzeby biura Prezydenta RP Bronisława Komorowskiego.

Profesor Czesław Martysz – znakomity ekspert prawniczy, Prorektor Uniwersytetu Śląskiego, członek kolegium NIK wygłosił prelekcję „Przestępstwa przeciw ochronie bezpieczeństwu informacji – odpowiedzialność wynikająca z KPA".

Druga część naszego Forum dotyczyła aspektów organizacyjnych oraz zarządczych. Prelekcja Prezydenta CIS CERT Pana **Ericha Scheibera** oraz Prezesa polskiego Oddziału CIS CERT Pana **Mirosława Bienioszka** pozwoliły uczestnikom na poznanie misji i zasad, którymi kieruje się ta jednostka.

W swojej prezentacji postarałem się przybliżyć trudne aspekty zarządzania ryzykiem w bezpieczeństwie informacji i kontroli zarządczej. Pokazałem w niej, jak istotne jest prawidłowe przeprowadzenie analizy ryzyka przy wdrażaniu systemów zarządzania.

Ostatnią część Forum stanowiły eksperckie, technologiczne prezentacje firm Mediarecovery oraz IBM. Prezentacja **Przemysława Krejzy** reprezentującego Mediarecovery „Bezpieczeństwo – Informatyka śledcza" uzmysłowiło uczestnikom Forum, jak ważnym elementem jest zabezpieczanie dowodów, przy użyciu nowoczesnych technik i technologii.

Krystian Chmiel reprezentujący IBM wygłosił prelekcję „Bezpieczeństwo informacji w oparciu o technologie IBM".

Kolejka dawka światowych technologii niezbędnych w zabezpieczeniu elektronicznie przetwarzanej informacji.

Już dziś wiemy, że w kwietniu 2013 roku odbędzie się Drugie Międzynarodowe CIS-Forum Bezpieczeństwa Informacji i Zarządzania Usługami IT. Po raz kolejny będziemy gościli w przepięknym obiekcie Wyższej Szkoły Technicznej w Katowicach. ■

Już dziś wszystkich serdecznie zapraszam.

Autor jest Dyrektorem ds. Bezpieczeństwa firmy 2Business Consulting Group, Trenerem CIS – Certification & Information Security Services, ekspertem ds. bezpieczeństwa Okręgowej Rady Adwokackiej w Katowicach, audytorem wiodącym norm ISO 27001 oraz BS 25999, Koordynatorem Projektu „Godny zaufania". Kierował projektami w zakresie systemów zarządzania bezpieczeństwem informacji oraz systemów zarządzania ciągłością działania w ponad 200 projektach realizowanych na terenie całego kraju.

MAGAZYN
INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

mediarecovery
Lider informatyki śledczej

Adres redakcji
Mediarecovery
40-723 Katowice, ul. Piotrowicka 61
Tel. 032 782 95 95, fax 032 782 95 94
e-mail: redakcja@mediarecovery.pl

Redakcja
Zbigniew Engiel (red. nacz.),
Przemysław Krejza
Skład, łamanie, grafika: Marcin Wojtera
Reklama: Zbigniew Engiel

Wydawca
Media Sp. z o.o.
40-723 Katowice, ul. Piotrowicka 61
Tel. 032 782 95 95, fax 032 782 95 94
e-mail: biuro@mediarecovery.pl

Technologie mobilne -
IV Ogólnopolska Konferencja Informatyki Śledczej

Czy wiesz, że w 1880 roku w pierwszych budkach telefonicznych oprócz telefonu znajdował się również kasjer pobierający opłaty? Tak zaczyna się treść **zaproszenia na IV Ogólnopolską Konferencję Informatyki Śledczej**, jakie wpłynęło do naszej redakcji. Po początkowym zaskoczeniu z dalszej części tekstu można się dowiedzieć, iż jest to jedynie przykład mający na celu zobrazowanie postępu, jaki dokonał się w zakresie technologii komunikacyjnych, które dziś zwie się coraz częściej technologiami mobilnymi. I rzeczywiście z punktu widzenia Bella i jego konkurenta Graya dzisiejsze możliwości przesyłu danych i komunikacji międzyludzkiej byłyby niewiarygodne. Oprócz niewątpliwych plusów takiego stanu rzeczy, **ceną za postęp i rozwój są nowe formy nadużyć, przestępstw czy sposobów na obejście prawa**. Przypominają o tym organizatorzy Konferencji, która w tym roku odbędzie się pod tytułem „**Technologie mobilne – wyzwania informatyki śledczej**". Niezwykle **silnym atutem jest grono wykładowców**. To cecha charakterystyczna SIIŚ lecz tym razem udało się zgromadzić naprawdę **znaczące nazwiska w polskiej branży bezpieczeństwa IT**. Będą to **szefowie działów bezpieczeństwa operatorów telefonii, dużych portali społecznościowych** i firm zajmujących się nowymi technologiami. Organizatorzy zaplanowali również wykład prawny dotyczący technologii mobilnych, a na koniec warsztaty pod nazwą „**Analiza urządzeń mobilnych w praktyce**". Warto również wspomnieć o dr inż. Jerzym Kosińskim z Wyższej Szkoły Policji w Szczytnie, który opowie o technikach social forensics.

Podsumowując **IV Ogólnopolska Konferencja Informatyki Śledczej zapowiada się niezwykle interesująco**. Jako patrona medialny tego wydarzenia, **serdecznie zapraszamy naszych czytelników do udziału.** Będzie tam mnóstwo wartościowej wiedzy i osobiście żałuję, że ta konferencja odbywa się tylko raz w roku. ■

Zbigniew Engiel