MAGAZYN

NR 27 / WRZESIEŃ 2015

www.magazyn.mediarecovery.pl

INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

Nowa, międzynarodowa formuła organizowanej od 2009 roku Ogólnopolskiej Konferencji Informatyki Śledczej.

Ultimate Response and Digital Investigations

18-19 listopada 2015, Warszawa

www.urdi.eu

Co w numerze?

Ultimate Response and Digital Investigations

nowa formuła Ogólnopolskiej Konferencji Informatyki Śledczej

URDI 2015 to jedyna konferencja w Europie łącząca ze sobą tak ściśle bezpieczeństwo IT i informatykę śledczą. Jest odpowiedzią na rzeczywiste potrzeby środowiska specjalistów bezpieczeństwa. Przy obecnym poziomie cyberzagrożeń konieczna jest współpraca ekspertów z obu dziedzin i skuteczne wykorzystanie zależności jakie między nimi zachodzą.

URDI 2015 to:

- 2 dni, 2 równoległe ścieżki tematyczne, a podczas nich
  - 420 minut wykładów
  - 720 minut warsztatów praktycznych
  - międzynarodowa grupa ekspertów z USA, Niemiec, Francji, Szwecji, Węgier, Rosji i Polski

Dlaczego URDI 2015?

Tematyka konferencji to zupełnie nowe spojrzenie na kwestie bezpieczeństwa IT i analiz śledczych. Udział w URDI 2015 pozwoli na poznanie najnowszych cyberzagrożeń i reakcji na nie w wykonaniu ekspertów z obszaru bezpieczeństwa IT i informatyki śledczej. Uczestnik konferencji zyskuje:

- dostęp do eksperckiej wiedzy międzynarodowych praktyków i specjalistów.
- możliwość aktualizacji poziomu wiedzy dotyczącej obecnych cyberzagrożeń dla firm i instytucji
- praktyczne umiejętności ochrony przed atakami hakerskimi
- sposobność wymiany doświadczeń z ekspertami informatyki śledczej i bezpieczeństwa IT z całej Europy i USA
- pogłębienie znajomości nowoczesnych systemów bezpieczeństwa IT i narzędzi informatyki śledczej

UWAGA Promocja!

Dla czytelników Magazynu Informatyki Śledczej promocyjna cena 850 złotych netto za udział dwóch dniach konferencji obowiązuje do końca października!

Wypełniając formularz zgłoszeniowy wpisz kod ***MIS2015*** żeby skorzystać z promocji.

Promocja obowiązuje również w przypadku zgłoszeń grupowych.

Więcej informacji na:

www.urdi.eu

Program konferencji*

URDI 2015
Ultimate Response & Digital Investigations

Godzina	Środa 18 listopada 2015 – Co się będzie działo	
9.00 – 9.15	Rejestracja uczestników	
9.15 – 9.20	Rozpoczęcie konferencji – Przemysław Krejza, prezes SIIŚ	
9.20 – 9.50	Wykład wprowadzający – Keynote	
9.55 – 10.25	CSX (Cybersecurity Nexus) – Adam Rafajeński, ISACA	
10.25 – 10.45	Przerwa kawowa	
10.45 – 11.15	Owoce zatrutego drzewa, czyli problematyka wykorzystania dowodów zdobytych z naruszeniem prawa. – Jarosława Góra, Kancelaria Adwokatów i Radców Prawnych Ślązak, Zapiór i Wspólnicy	
11.20 – 11.50	Pozytywne aspekty incydentów bezpieczeństwa – Piotr Szeptyński	
11.50 – 12.00	Przerwa kawowa	
	Ścieżka Ultimate Response	**Ścieżka Digital Investigations**
12.00 – 12.30	Polowanie na „pacjenta Zero” - Francis Ia, Senior Solution Consultant, Guidance Software	Jak dotrzeć do ukrytych i skasowanych danych w urządzeniach mobilnych? - Tatiana Pankova – Oxygen Forensics
12.35 – 13.05	Zagrożenia SSL już tu są. Czy Twoja architektura systemów jest na nie gotowa? - Patrick Kuttruff, Cyberdefense Strategist, Advanced Threat Protection Group, Blue Coat Systems Inc.	Jak wykonać analizę śledczą danych z prywatnych kont Google? - Andrey Malyshev – Elcomsoft
13.05 – 14.00	Lunch	
14.00 – 14.30	Na ile prawdziwe są zagrożenia wewnętrzne? - Rashmi Knowles, Chief Security Architect, RSA	Analiza i eksploracja danych pochodzących z chmury (cloud data) w urządzeniach mobilnych. - Joachim Müller, Peter Zontek – Cellebrite
14.35 – 15.05	Nowe podejście do bezpieczeństwa: Contextual Security Intelligence - BalaBit	Tablet. Przenośne narzędzie do informatyki śledczej. - Jonas Andersson – MSAB
15.10 – 15.45	Wykład, w trakcie ustaleń	Budujemy laboratorium informatyki śledczej. - Karol Szczyrbowski – Mediarecovery
20:00 –	Impreza integracyjna	

Godzina	Czwartek 19 listopada 2015 – Co się będzie działo	
	Ścieżka Ultimate Response	**Ścieżka Digital Investigations**
9.00 – 10.00	Top 3 najpopularniejszych zagrożeń w oparciu o case studies klientów w Europie. - Francis Ia, Senior Solution Consultant, Guidance Software	Informatyka śledcza w chmurze. Dekrypcja danych. - Dmitry Sumin, Nataly Koukouskina – Passware Inc.
10.00 – 10.10	Przerwa	
10.10 – 11.10	Jak sprawdzić gotowość do odparcia ataków SLL/TLS? - Patrick Kuttruff, Cyberdefense Strategist, Advanced Threat Protection Group, Blue Coat Systems Inc.	Co można zrobić z zabezpieczonym iPhone? - Andrey Malyshev, Alexey Shtol – Elcomsoft
11.10 – 11.20	Przerwa	
11.20 – 12.20	Zagrożenia wewnętrzne. Praktyczne sposoby przeciwdziałania. - Marcin Filipiak, Inżynier Wsparcia Technicznego, Arrow ECS/RSA	Jak analizować dane skasowane i ukryte? - Tatiana Pankova – Oxygen Forensics
12.20 – 12.30	Przerwa	
12.30 – 13.30	People-centric security - Balabit	Analiza danych w chmurze w praktyce. - Joachim Müller, Peter Zontek – Cellebrite
13.30 – 14.10	Lunch	
14.10 – 15.10	Warsztat praktyczny – szczegóły wkrótce	Tips&tricks w analizach urządzeń mobilnych. - Michał Tatar – MSAB
15.10 – 15.20	Przerwa	
15.20 – 16.20	Warsztat praktyczny – szczegóły wkrótce	Incydent pracowniczy. Jak poradzić sobie ze sztuczkami anti-forensics? - Karol Szczyrbowski – Mediarecovery
16.20 – 16.40	Zakończenie konferencji	

** Tematy poszczególnych prelekcji i wykładów mogą ulec zmianie*

www.urdi.eu

10 lat informatyki śledczej w Polsce

Hakerzy wykradają dane osobiste **35 milionów** mieszkańców Korei Południowej. Atak przeprowadzono za pomocą zaawansowanego malware.

2011

Mediarecovery wykonało jedną z największych analiz informatyki śledczej w Polsce. Cyfrowe dochodzenie objęło **ponad 1000 komputerów.**

2012

627 analiz komputerów, laptopów, telefonów, smartfonów i nawigacji GPS wykonano w laboratorium informatyki śledczej Mediarecovery.

2013

Analiza komputera **Katarzyny W.** pomogła prokuraturze w przygotowaniu aktu oskarżenia.

mediaimager GM⁴ 2014

Powstaje prototyp pierwszego, polskiego duplikatora danych - **MediaImager** - podstawowego narzędzia informatyków śledczych.

2015

Informatyka śledcza elementem uruchomionego **Security Operations Center (SOC).** To wyższy poziom bezpieczeństwa w praktyce.

2005

Pierwsza sprawa z zakresu informatyki śledczej dotyczyła **piractwa komputerowego.**

2006

Katastrofa budowlana MTK. Specjaliści Mediarecovery znajdują w komputerach prezesów dane, które wzbogacą akt oskarżenia.

2007

Mediarecovery rozpoczęło cykl szkoleń z informatyki śledczej dla **1700 prokuratorów i policjantów.**

2008

Mediarecovery wdraża w jednym z banków pierwszy w Polsce system do reakcji na incydenty i informatyki śledczej.

2009

Zdalne kasowanie danych w trakcie ich zabezpieczania nie pomogło. Sąd wydaje wyrok w sprawie byłego posła Samoobrony m.in. w oparciu o **dowody cyfrowe.**

2010

7 laboratoriów kryminalistycznych policji wyposażonych w sprzęt i oprogramowanie do informatyki śledczej.

Wykryto robaka komputerowego **Stuxnet,** który znacząco opóźnił realizację narodowego planu rozwoju atomistyki w Iranie.

Wykryto t… **najbardzi… oprogram…** wykryto.

Włamanie do **Google, Yahoo!** i innych firm w Silicon Valley. Hakerom udało się dostać do sieci wewnętrznych dzięki nieaktualnym wersjom Internet Explorera.

Powstaje **Stowarzyszenie Instytut Informatyki Śledczej.**

Dyktafon pokazany przez **Ministra Ziobro** miał być "gwoździem do politycznej trumny Andrzeja Leppera".

90% wszystkich e-maili była spamem. 2006 rok ogłoszono krótkowzrocznie "rokiem cyberprzestępczości".

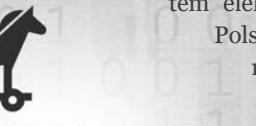
Bronisław Wildstein wyniósł z IPN na pendrive spis agentów PRL. Taki był wówczas **poziom zabezpieczeń.**

IPN / PRL

mediarecovery
Lider informatyki śledczej

Komputer z monitorem oraz kilkadziesiąt płyt CD to dowody rzeczowe w pierwszej sprawie, jaka trafiła do tworzonego właśnie laboratorium informatyki śledczej Mediarecovery. Zadaniem inżynierów było wykazanie czy gry i programy są legalne. W 2005 roku był to zdarzenie przełomowe.

Pomimo dużego nasycenia sprzętem elektronicznym ówczesnej Polski organy ścigania nie miały świadomości, że oprócz funkcji użytkowych taki sprzęt może być źródłem dowodów i poszlak. Zupełnie inaczej było na Zachodzie Europy i USA. Tam informatyka śledcza rozwijała się już od lat 80 XX wieku.



rojana Flame. Nazywany jest
ej zaawansowanym szkodliwym
owaniem, jakie do tej pory

Z sieci amerykańskich sklepów Target wyciekły dane **110 milionów** kart kredytowych.

Cyber wojna na Ukrainie. Kradzież e-maili, włamania do sieci telekomunikacyjnych, dostęp do SMS parlamentarzystów.

Internet Rzeczy na celowniku cyberprzestępców. Celem hakerów staną się urządzenia domowe podłączone do sieci. Uważajcie na swoją lodówkę!

Początkowo właśnie na Zachodzie polscy specjaliści przechodzili szkolenia i stamtąd pochodził sprzęt do analiz. Dziś sytuacja wygląda nieco inaczej, a w Polsce powstaje sprzęt dla informatyków śledczych.

Rok 2007. Informatyka śledcza wkracza do firm i „gwóźdź" Ministra Ziobro

Wraz z ilością spraw i ekspertyz zlecanych przez policję, prokuraturę i sądy rosło zainteresowanie możliwościami analiz śledczych u szefów firm. Chcieli oni przede wszystkim sprawdzić lojalność swoich pracowników. Kradzież danych i udostępnianie ich konkurencji stawała się coraz prostsza. W końcu wszystkie informacje były w formie elektronicznej.

Z tamtego okresu pochodzi historia pracownika działu handlowego, który udostępniał ceny ofert przetargowych konkurencji za pośrednictwem czatu w przeglądarkowej grze on-line. To również rok, w którym dowód elektroniczny trafił na pierwsze strony gazet. Minister Ziobro przedstawił dziennikarzom „gwóźdź do politycznej trumny Andrzeja Leppera". Jak wykazali specjaliści Mediarecovery Pan Minister nie do końca miał rację mówiąc, że nagrania z dyktafonu nie można zmanipulować.

Rok 2010. Polska Policja zwiększa możliwości dochodzeniowe o sprzęt i oprogramowanie do informatyki śledczej

7 laboratoriów kryminalistycznych Policji zostało wyposażonych w kompletne zestawy do analiz informatyki śledczej. Oprócz dostarczenia narzędzi specjaliści Mediarecovery przeprowadzili cykl szkoleń teoretycznych i praktycznych.

Był to pierwszy duży przetarg tego typu. Nie rozwiązał on wszystkich problemów ale był z pewnością krokiem w dobrym kierunku. W kolejnych latach inżynierowie Mediarecovery pomogli stworzyć laboratoria informatyki śledczej w innych służbach.

Rok 2011. Ogromne, cyfrowe śledztwo

Zarząd jednej z korporacji działających w Polsce miał uzasadnione podejrzenia, że w firmie dochodzi do nieprawidłowości na dużą skalę. Cyfrowe śledztwo objęło ponad 1000 komputerów. Zadaniem specjalistów Mediarecovery było zmniejszyć krąg podejrzanych, a potem wskazać konkretne osoby dokonujące nadużyć.

Cały proces zajął kilka tygodni i był prowadzony w sposób niezauważalny dla pracowników. W efekcie wskazano osoby, najprawdopodobniej zaangażowane w nieuczciwy proceder. Dalsze działania wobec nich podjął już zarząd korporacji.

Rok 2014. Polskie narzędzia do informatyki śledczej

Kopiarka danych jest podstawowym narzędziem informatyki śledczej. Żaden z profesjonalistów nie pracuje na oryginalnym nośniku danych. Wykonuje się tzw. kopie binarne i dopiero na nich prowadzi się analizę. Do niedawna tego typu sprzęt był domeną producentów z USA. Polskie laboratrium informatyki śledczej chce przełamać oligopol amerykański w branży. W ubiegłym roku powstał prototyp urządzenia MediaImager.

W tym roku rozpoczęły się testy w podobnych laboratoriach na całym świecie, m.in. w Japonii. Wyniki są bardzo pozytywne. Polski MediaImager nie ustępuje jakościowo i technologicznie dominującym na globalnych rynkach rozwiązaniom. Właśnie rozpoczęła się seryjna produkcja polskiej kopiarki danych.

Rok 2015. Security Operations Center

Do niedawna informatyka śledcza rozwijała się równolegle do bezpieczeństwa IT. Jednak wraz ze wzrostem ilości incydentów, włamań hakerskich czy wycieków danych pojawiła się potrzeba wsparcia systemów bezpieczeństwa IT możliwościami informatyki śledczej. W przypadku cyberataku oprócz oczywistej potrzeby jego odparcia niezbędne jest zabezpieczenie dowodów elektronicznych. Pisze o tym więcej w swoim artykule Przemysław Krejza.

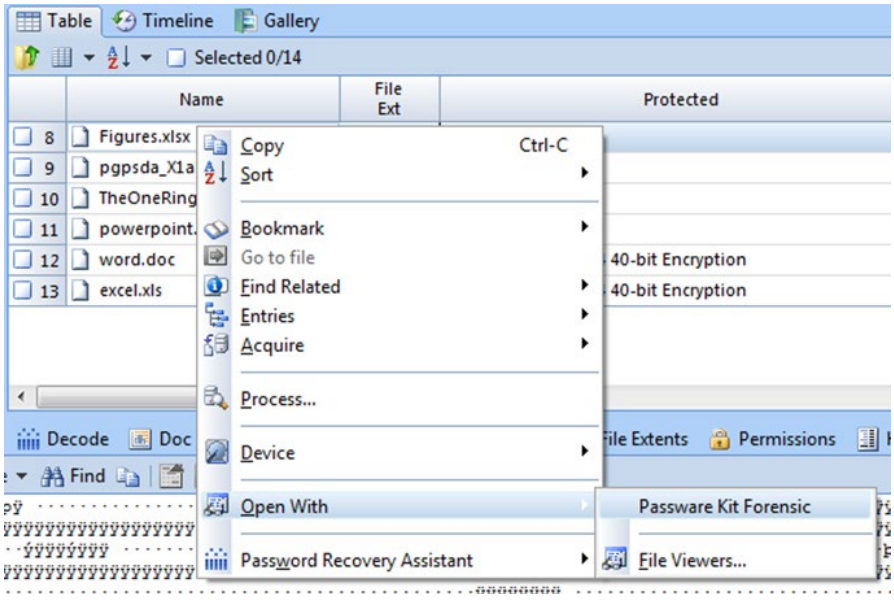
Pozwolą one ustalić w jaki sposób i kiedy doszło do włamania, a w niektórych przypadkach nawet kto brał w nim udział. Tego typu informacje dla specjalistów stanowią ważne źródło wiedzy pozwalające lepiej zabezpieczyć się na przyszłość, a z drugiej strony mogą stać się materiałem dowodowym w przypadku postępowania prokuratorskiego.

Rozwiązania informatyki śledczej są stałym elementem zaawansowanych technologicznie Security Operations Center tworzonych przez Mediarecovery. Takie centra zarządzania bezpieczeństwem to zarówno sprzęt i oprogramowanie, jak i szczegółowe procedury, normy i zasady postępowania w sytuacjach kryzysowych.

Koalicja na rzecz łamania haseł

Karol Szczyrbowski

Szyfrowanie, kiedyś dostępne tylko dla specjalistów i najbardziej zaawansowanych użytkowników, w ostatnich latach stało się technologią dostępną dla każdego. Zmiany te spowodowały znaczny wzrost zabezpieczonych danych. Oczywiście, należy cieszyć się z rosnącej świadomości oraz możliwości użytkowników ale fakt ten nie pozostał obojętny dla osób zajmujących się analizą cyfrowego materiału dowodowego.



Odzyskiwanie haseł może być szybkie i skuteczne

Zabezpieczanie

Szyfrowaniem można zabezpieczyć pojedynczy plik, wolumen danych, a nawet cały dysk twardy z pracującym na nim systemem operacyjnym (tzw. FDE – Full Disk Encryption). Zwłaszcza FDE ma wpływ na pracę informatyków śledczych, ponieważ technologia ta wymusiła zmiany w podejściu do zabezpieczenia nośników danych, gdzie przed wyłączeniem komputera należy upewnić się, że nie jest on zaszyfrowany. W takiej sytuacji, możemy później nie otrzymać informacji potrzebnych do deszyfracji co poskutkuje brakiem możliwości dalszej analizy. Warto w tym miejscu wspomnieć o potrzebie wykonywania zrzutów pamięci RAM (tzw. memory dump) w przypadku zabezpieczania uruchomionego komputera. W zrzucie możemy znaleźć bardzo przydatne dane, m.in. potrzebne do późniejszej deszyfracji nośnika. Informacje te przepadną wraz z wyłączeniem komputera (pomijając możliwość wykonania ataku typu cold boot).

Deszyfracja

Na rynku informatyki śledczej w ostatnim czasie powstają ciekawe sojusze, mające na celu przyniesienie korzyści nam, użytkownikom. Mowa tu o następujących rozwiązaniach:

- EnCase Forensic
- Tableau Password Recovery (nowość na rynku)
- Passware Kit Forensic / Enterprise

EnCase Forensic to czołowy program dla informatyków śledczych, za pomocą którego można zabezpieczyć oraz poddać analizie szerokie spektrum danych. Program rozpoznaje i pozwala na deszyfrację najbardziej popularnych formatów szyfrowania FDE, jak również rozpoznaje zaszyfrowane pliki na badanym nośniku. Sama detekcja to dopiero pierwszy krok. Następnie pliki trzeba poddać próbom mającym na celu deszyfrację/uzyskanie hasła dostępowego do danych. Bezpośrednio z poziomu interfejsu EnCase Forensic użytkownik może zabezpieczone pliki wysłać do programu Passware, za pomocą którego można deszyfrować wskazane dane.

Obliczenia

Deszyfracja deszyfracji nierówna o czym warto pamiętać wyposażając laboratorium w rozwiązania do tego typu działań. Najważniejszym elementem, na który należy zwrócić uwagę to moc obliczeniowa dostępna dla rozwiązań deszyfrujących nasze dane. Od dawna już wiadomo, że znacznie więcej osiągniemy, opierając nasze działania o procesory graficzne (GPU) niż tylko o procesor z płyty głównej (CPU). Passware Kit Forensic pozwala na korzystanie z procesorów graficznych, nawet kilku kart w jednym komputerze co umożliwia znaczne przyspieszenie deszyfracji. Należy pamiętać, że prędkość obliczeń zależy nie tylko od wykorzystanego sprzętu ale także od algorytmu, który został wykorzystany przy szyfrowaniu danych. Inna prędkość będzie przy próbie odblokowania archiwum ZIP a inna przy zahasłowanym dokumencie *.docx programu Microsoft Word.

Tableau Password Recovery

W osiągnieciu najlepszych wyników, przychodzi z pomocą najnowszy produkt lidera hardware dla informatyków śledczych – Tableau – rozwiązanie Tableau Password Recovery. Tableau Password Recovery jest ekonomicznym, skalowalnym rozwiązaniem zaprojektowanym w celu uproszczenia i przyspieszenia procesu identyfikacji, od-

blokowania i odkrywania dodatkowych informacji w plikach chronionych hasłem. Oparty na podstawie akceleratora pierwszej generacji popularnego TACC, Tableau Password Recovery jest zasilany przez cztery karty z akceleratorem sprzętowym Tableau Field-Programmable Gate Array (FPGA) w wersji 2 (TACC2). Karty TACC2 zostały zaprojektowane specjalnie w celu przyspieszenia ataków słownikowych i brute-force za pomocą rozwiązania firmy Passware. Tableau Password Recovery integruje się bezpośrednio z EnCase Forensic, EnCase eDiscovery i EnCase Endpoint Security. EnCase plugin o nazwie Password Recovery Assistant, za pomocą zaledwie kilku kliknięć upraszcza proces wskazywania chronionych plików, ich odblokowania i aktualizację aktywnej sprawy o nowo odblokowane dane. Wspomniane oprogramowanie Passware jest skalowalne za pomocą liczby agentów w dystrybuowanych atakach, a rozwiązanie sprzętowe Tableau Password Recovery w postaci liczby urządzeń pracujących razem, co pozwala na dopasowanie do potrzeb nawet najbardziej wymagających użytkowników.

Współpraca pomiędzy rozwiązaniami EnCase, a Tableau Password Recovery

Taka kompilacja rozwiązań wskazuje, że ich producenci rozumieją rynek i poprzez współpracę przy obecnych produktach oraz tworzenie nowych, pozwalają użytkownikom na lepszą i bardziej wydajną pracę. Obecne możliwości deszyfracji dla poszczególnych użytkowników oraz instytucji umożliwiają wydajne próby uzyskiwania dostępu do zaszyfrowanych danych bez potrzeby wysyłania ich poza sieć wewnętrzną, np. do klastrów obliczeniowych w chmurze co zawsze rodziło wątpliwości pod kątem bezpieczeństwa badanych danych.

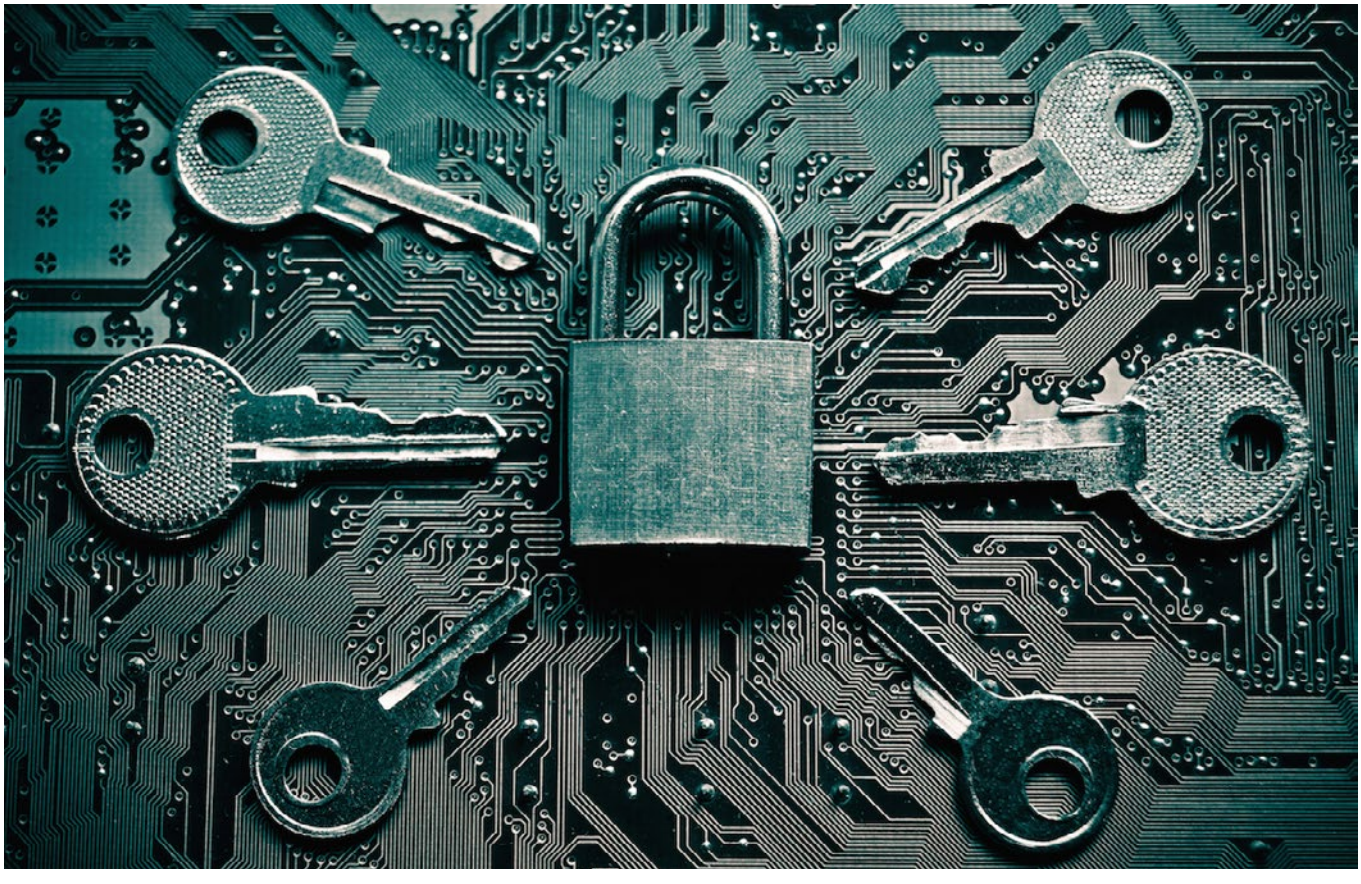
Autor jest specjalistą informatyki śledczej w laboratoriuym Mediarecovery oraz trenerem w Akademii Informatyki Śledczej.

Cyberprzestępczość – hacking / cracking

Jarosław Góra

Przestępców działających w cyberprzestrzeni, wykorzystujących nowe technologie do prowadzenia swojej „działalności", polegającej najczęściej na włamywaniu się do zabezpieczonych systemów komputerowych, potocznie nazywa się hakerami. Czy słusznie? Co kryje się pod pojęciem hackingu z informatycznego i prawnego punktu widzenia?

Wśród czynów zabronionych zaliczanych do tzw. cyberprzestępstw wyróżnić możemy działania mające na celu bezprawne uzyskanie dostępu do informacji. Jeśli działania te mają miejsce w sieci, wiążą się z przełamywaniem elektronicznych lub informatycznych zabezpieczeń albo nielegalnym uzyskaniem dostępu do całości lub części systemu informatycznego, prawnicy najczęściej zakwalifikują je jako przestępstwo tzw. hacking. Niemniej jednak, z informatycznego i kulturowego punktu widzenia określenie to jest dla przedstawicieli środowiska hakerów bardzo krzywdzące. Kultura hakerska, w której wartościami nadrzędnymi są wolność, technika (technologia informatyczna) i jej wykorzystanie, sprzeciwia się bowiem wszelkim działaniom niezgodnym z prawem. Działania polegające na bezprawnym łamaniu zabezpieczeń to tzw. cracking i takim określeniem będę się posługiwał. Cracking regulują dwa przepisy kodeksu karnego, dostarczając niezliczoną ilość problemów interpretacyjnych, których kilka postaram się zasygnalizować. Zgodnie z art. 267 § 1 kodeksu karnego przestępstwo popełnia kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie. Popełnienie przestępstwa crackingu zagrożone jest karą grzywny, ograniczenia wolności albo pozbawienia wolności do lat 2. Uzyskanie dostępu do informacji będzie stanowić przestępstwo jedynie w przypadku, gdy będzie mieć charakter bezprawny, a więc gdy sprawca naruszy prawo innej osoby do dysponowania informacją i uzyska do niej dostęp, nie będąc do tego uprawnionym. Nie popełni przestępstwa osoba, która uzyska informacje wprawdzie dla niego nieprzeznaczone, jednak w sposób zgodny z prawem, np. policjant w przypadku prowadzenia podsłuchu zgodnie z obowiązującymi w tym zakresie przepisami, czy tez pentester zaangażowany przez właściciela systemu. Dla popełnienia przestępstwa wystarczające jest uzyskanie dostępu do informacji, a więc doprowadzenie do sytuacji, w której zapoznanie się z informacją jest możliwe, nie jest natomiast konieczne samo zapoznanie się z nią. Kwestia ta nie była oczywista przed nowelizacją



z 2008 r. (wcześniej redakcja przepisu brzmiała: Kto bez uprawnienia uzyskuje informację dla niego nie przeznaczoną...). Nie jest istotne również to, czy informacja do której dostęp uzyskał sprawca jest tą, której szukał, jak i to, czy informacja jest dla niego w jakikolwiek sposób przydatna. Zatem przestępca poszukujący informacji o klientach banku i numerach ich kart kredytowych, który po przełamaniu zabezpieczeń uzyska dostęp do danych zupełnie innych, mających jednak charakter niepubliczny, zrealizuje przesłankę bezprawnego uzyskania dostępu do informacji, pomimo nieznalezienia tych, których szukał. Podłączenie się do sieci telekomunikacyjnej, celem uzyskania dostępu do informacji, polega na wykorzystaniu urządzenia odbiorczego, umożliwiającego pozyskanie przekazywanych za jej pośrednictwem danych. Definicje „sieci telekomunikacyjnej" znajdziemy w ustawie Prawo telekomunikacyjne (art. 2 pkt. 35), zgodnie z którą to systemy transmisyjne oraz urządzenia komutacyjne lub przekierowujące, a także inne zasoby, w tym nieaktywne elementy sieci, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju. Prosta sprawa. Z kolei przełamanie albo omijanie zabezpieczeń należy rozumieć szeroko, jako każdą czynność, która ma umożliwić sprawcy dostęp do informacji. Różnica pomiędzy przełamaniem, a ominięciem zabezpieczenia sprowadza się do tego, czy sprawca ingeruje w system zabezpieczeń, czy też uzyskuje dostęp bez jakichkolwiek ingerencji w nie. Obok elektronicznych i informatycznych zabezpieczeń przepis wspomina również o przełamywaniu innych szczególnych zabezpieczeń informacji, a więc takich, których usunięcie/ominięcie wymaga umiejętności ponad przeciętnych. Zgodnie z art. 267 § 2 kodeksu karnego tej samej karze podlega ten kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego. W tym przypadku już sam fakt uzyskania dostępu do systemu, bez konieczności przełamania lub ominięcia zabezpieczeń, stanowi przestępstwo, jeśli sprawca nie jest uprawniony, aby taki dostęp uzyskać. Jak należy rozumieć pojęcie systemu informatycznego? W prawie europejskim i międzynarodowym znajdziemy kilka krzyżujących się definicji. Również na gruncie prawa polskiego odmiennie definiuje się to pojęcie, czy to w ustawie o ochronie danych osobowych, czy też w ustawie o świadczeniu usług drogą elektroniczną. Spotkać się można z głosami, iż skoro przepis penalizuje również dostęp do systemu niezabezpieczonego, to odpowiedzialność karna może dotknąć właściciela telefonu ustawionego na automatyczne łączenie się z niezabezpieczonymi sieciami WiFi. Prawdą jest, że brak zabezpieczeń nie oznacza „zaproszenia do korzystania", jednak wszystkie omawiane wyżej przestępstwa mogą być popełnione jedynie umyślnie i to z zamiarem bezpośrednim, zatem nieświadome uzyskanie dostępu do systemu nie będzie stanowiło przestępstwa.

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

Zarządzanie incydentem, a informatyka śledcza

Przemysław Krejza

10 lat temu, kiedy zaczynaliśmy informatykę śledczą (digital investigation) w Polsce, była ona głównie narzędziem w rękach dochodzeniowców policyjnych. Choć z czasem pojawiały się coraz bardziej złożone sprawy, jak na przykład afera paliwowa, oszustwa na VAT byłego posła czy też sprawa Katarzyny W., to w organizacjach śledztwa komputerowe pojawiały się niezwykle rzadko.

Bezpieczeństwo informatyczne w przedsiębiorstwach koncentrowało się na budowaniu odpowiedniego poziomu zabezpieczeń, które w założeniu miały uchronić biznes przed wszelkimi zagrożeniami, nie dopuszczając do występowania incydentów. Było tak, pomimo, że normy dotyczące systemów bezpieczeństwa informacji, jak na przykład ISO27001, wskazywały na konieczność bycia przygotowanym na wystąpienie „problemów", a w momencie kiedy takowe wystąpią, zastosowanie odpowiednich procesów w celu wyjaśnienia danego incydentu oraz zgromadzenia odpowiednich dowodów (zob. PN/ISO 27001:2005).

Dziś wiemy już, że koncepcja oparta tylko o systemy zabezpieczeń nie sprawdziła się. W ciągu ostatnich lat przekonaliśmy się, że żadne z nich nie jest w stanie zapewnić stuprocentowej ochrony, szczególnie w otoczeniu w którym informacja stała się bardziej cenna niż narkotyki. Przykłady kompromitacji zabezpieczeń można by wymieniać dziesiątkami, a straty z nimi związane są ogromne. I nie mówimy tu tylko o kwestiach finansowych. Dlatego organizacje przygotowane powinny dziś zakładać, że system bezpieczeństwa musi być wzbogacony o sprawnie działający element response, którego niezbędnym składnikiem jest informatyka śledcza. Oznacza to, że rola informatyka śledczego w systemach bezpieczeństwa znacznie wzrosła, a w przyszłości funkcjonowanie tych systemów bez nas stanie się niemożliwe.

Incident response, a informatyka śledcza

Przeciętnie zorientowany czytelnik wyczuwa różnicę pomiędzy zdarzeniem, a incydentem bezpieczeństwa. Warto jednak przypomnieć, że w rozumieniu normatywnym, zdarzeniem jest wystąpienie „epizodu", który ma związek z systemem bezpieczeństwa informacji ale nie musi to być naruszenie poufności, integralności bądź dostępności, czyli incydent bezpieczeństwa. Posłużmy się tu przykładem logu z jednej ze stacji roboczych dostarczanych do naszego SIEM, który wykazał próbę wielokrotnego logowania na konto użytkownika z uprawnieniami administracyjnymi na tej stacji. Sam fakt logowania nie określa jednak czy mamy do czynienia z zagrożeniem. Być może użytkownik zapomniał wyłączyć capslock. Może być jednak tak, że inny pracownik próbuje użyć hasła z kartki przyklejonej pod klawiaturą niefrasobliwego admina, na której ten nie dość czytelnie je zapisał. Żeby ustalić czy mamy do czynienia z incydentem czy zdarzeniem, w dojrzałej organizacji powinien uruchomić się mechanizm, który powinien zdecydować, czy problemem należy zarządzać czy nie. Decyzja o sklasyfikowaniu zdarzenia jako incydentu oznacza przejście w kierunku eskalacji i czynności związanych z reakcją (response).

Formalnie rzecz biorąc oznacza to konieczność podjęcia określonej akcji, zależnej od klasy incydentu. Ważne przy tym jest, że podstawowym celem zarządzania incydentem jest powstrzymanie strat (wycieku danych) a następnie remediacja. W tym przypadku reakcją może być niezwłoczne zablokowanie podejrzanej stacji i telefon do użytkownika z pytaniem „o co chodzi?". Krótkie wyjaśnienie może zamknąć sprawę. Inaczej jednak będzie jeśli użytkownik, na którego konto wystąpiły próby logowania, akurat jest na L4 i nie korzystał z komputera. W tym momencie konieczne może stać się przeprowadzenie dochodzenia i wykorzystanie informatyki śledczej. Jak wiemy, dla tego procesu, najważniejsze jest zgromadzenie dowodów zdatnych do przedstawienia w sądzie (jeśli zajdzie taka potrzeba) oraz przedstawienie raportu z wykrytych podatności w celu zapobieżenia takim incydentom w przyszłości. Efektem może być na przykład zwolnienie pracownika, który próbował logowania na cudze konto, co wykazał monitoring video, potwierdzony logami z systemu. Powyższy przykład obrazuje codzienność dzisiejszych systemów bezpieczeństwa. Wśród tysięcy zdarzeń część jest incydentami, a część wymaga przeprowadzenia analiz z wykorzystaniem informatyki śledczej. Przedstawia to poniższy rysunek: W praktyce im lepiej przygotowany sys-

tem tym czas pomiędzy zdarzeniem, a reakcją jest krótszy. Informatyka śledcza jest tu niezbędna, choć postrzegana jest jako element fazy post-incydentalnej, gdy sam incydent jest już powstrzymany, a systemy zabezpieczone. Analitycy informatyki śledczej nie zajmują się reakcją na incydent, a raport informatyki śledczej dotyczący danego zdarzenia może powstać po jakimś czasie i należy do fazy lessons learnt zarządzania incydentem. Sprawa niby prosta ale patrząc na „życie" od razu nasuwa się pytanie czy ten model wykorzystania informatyki śledczej jest naprawdę skuteczny?

Nowy model bezpieczeństwa

Wróćmy do naszego przykładu. Wyobraźmy sobie, że telefon do pracownika niczego nie wyjaśnił. Pracownik pracował na swoim koncie i nie pamięta czy próbował logować się na drugie konto z uprawnieniami administracyjnymi. Nie jest też w stanie powiedzieć, czy miał jakieś problemy z capslock, a na pewno był przy komputerze w momencie zdarzenia. W sieci nie odnotowano również żadnych połączeń do podejrzanej stacji. Co zatem się stało? Może SIEM się pomylił? To mało prawdopodobne, a jeśli przyjrzymy się zdarzeniu to zobaczymy, że próby logowania nastąpiły lokalnie z konta podstawowego na konto administracyjne. A więc być może malware?

W tym wypadku właściwa reakcja nie jest możliwa bez stwierdzenia faktycznej przyczyny problemu. Zablokowanie stacji może być niewystarczające, bo atak może być bardziej złożony, a skala problemu znacznie większa. Zignorowanie indykatorów może oznaczać poważną kompromitację – jeśli malware posiada pulę haseł i tylko próbkował konto administracyjne na podejrzanej stacji to być może inne systemy są również zarażone? Zaangażowanie informatyków śledczych okazuje się tu niezbędne aby w ogóle wiedzieć jak reagować. Okazuje się, że w przypadku tego typu zagrożeń jesteśmy niezbędni już nie na końcu łańcucha reakcji ale tuż po wystąpieniu zdarzenia. Bez naszej diagnozy nie sposób przygotować właściwej odpowiedzi a nawet zdecydować czy mamy do czynienia z incydentem!

Zagrożenia malware, APT, itd. powodują, że model systemu bezpieczeństwa musi ewoluować. Informatyk śledczy stanie się ważnym elementem response. Nie oznacza to jednak, że będzie odpowiedzialny za reakcję. Jego rolą będzie dostarczenie wiedzy dla zespołu reakcji. Takie podejście całkowicie zmieni perspektywę, gdyż jak wiemy, czas pomiędzy zdarzeniem a wynikiem analizy i reakcją musi być maksymalnie krótki aby zapobiec wyciekowi informacji. To wymaga całkowitej przebudowy sposobu pracy systemu bezpieczeństwa. Poszczególne role w systemie bezpieczeństwa muszą ze sobą ściśle współpracować tak, aby zależności między zdarzeniami i incydentami, reakcją i analizą miały formę dynamiczną.

Taka ewolucja jest możliwa i w najbardziej zaawansowanej formie jest realizowana w Security Operations Center.

Tam sprawne połączenie procesów response i digital investigations daje w efekcie nieosiągalne w „tradycyjnym podejściu" możliwości. Włączenie analizy w proces response powoduje, że nawet najtrudniejsze zdarzenie może być dynamicznie zarządzane, a odpowiedź na dowolny incydent niemal natychmiastowa. Warunkiem jest jednak odpowiednie przygotowanie procesów, zespołów i narzędzi którymi się posługują tak, aby przepływ pracy był w pełni ustrukturyzowany, a świadomość sytuacyjna pełna. W efekcie wpływ procesu response na systemy prewencji osiąga niespotykane wcześniej możliwości.

Potwierdza to tezę o niezbędności informatyki śledczej w systemie bezpieczeństwa. Również jako Stowarzyszenie Instytut Informatyki Śledczej dostrzegamy coraz silniejszą zależność pomiędzy procesem response, a wykorzystaniem digital investigations. Stąd też nowa formuła naszej konferencji. W tym roku łączymy informatykę śledczą i bezpieczeństwo IT w dwóch równoległych ścieżkach tematycznych. Taka koncepcja pozwoli działom bezpieczeństwa zdobyć komplementarną wiedzę w obu tematach. Dzięki temu ich działanie zespołowe będzie zdecydowanie bardziej skuteczne. Również dobry informatyk śledczy musi rozumieć i znać rozwiązania security i związane z nimi możliwości analityczne. Dziś każdy z producentów rozwiązań zaczyna dostrzegać naszą rolę w procesie zapewnienia bezpieczeństwa informacji. Dlatego oprócz ochrony wprowadzają możliwości analityczne pozwalające na identyfikowanie nowych zagrożeń i aktywne podejście do problematyki zabezpieczeń.

Więcej o samej konferencji dowiecie się w innej części Magazynu, a pełną agendę znajdziecie na **www.urdi.eu.** Korzystając z okazji serdecznie zapraszam czytelników Magazynu Informatyki Śledczej i Bezpieczeństwa IT do udziłu w konferencji.

Przemysław Krejza jest prezesem Stowarzyszenia Instytut Informatyki Śledczej.

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