MAGAZYN

NR 18/CZERWIEC 2013

INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

STOP! MALWARE

DIGITAL FORENSIC CHALLENGE

TABLEAU FORENSIC DUPLICATOR TD3

MALWARE OKIEM PRAWNIKA

POŁOWA BANKÓW MA PROBLEM Z NIELOJALNYMI PRACOWNIKAMI

NATOwska instrukcja dotycząca cyberwojny

W ostatnich tygodniach ukazał się „The Tallinn Manual on the International Law Applicable to Cyber Warfare". Jest to próba odniesienia międzynarodowych przepisów dotyczących działań zbrojnych do cybeprzestrzeni. W zamyśle autorów było ukazanie, że prawo dotyczące konfliktów zbrojnych, nawet to pochodzące z XIX wieku jest na tyle uniwersalne, że można je stosować we współczesnej cyberwojnie. Dokument można pobrać ze strony Cooperative Cyber Defence Centre of Excellence.

Alternatywa dla UTM w większych organizacjach

McAfee Web Gateway działa na zasadzie analizy profilu i pochodzenia treści przedostających się do sieci, oferując natychmiastową ochronę przeciwko malware i innym ukrytym zagrożeniom. Łącząc ochronę na poziomie lokalnym z pracą w chmurze McAfee Web Gateway zapewnia ochronę przed atakami typu zero-day, spyware i APT. Co ważne, działa bez użycia sygnatur.

AirTight Secure WiFi

Zabezpiecza firmową sieć WiFi oferując jednocześnie ochronę WIPS (Wireless Intrusion Prevention System). Dzięki technologii Airtight uzyskuje się pewność, że firmowa sieć jest zabezpieczona, jednocześnie ograniczając jej dostępność fizyczną do określonych lokalizacji. AirTight Secure Wi-Fi umożliwia wykrywanie fałszywych AccessPoint`ów i innych podatności sieci bezprzewodowych w celu spełnienia wymagań zgodności np. z PCI. Rozwiązanie zapewnia funkcjonalności filtrowania treści, firewall, QoS, traffic shaping oraz politykę BYOD.

EnCase Forensic ver 7.07

Na początku maja pokazała się na rynku nowa wersja najpopularniejszego narzędzia do analiz śledczych – EnCase Forensic. Najważniejsze zmiany to: skalowanie wydajności „Evidence Processor", możliwość tworzenia zakładek podczas analizy danych w „Case Analyzer", wsparcie dla wiadomości e-mail w systemach MAC OS X oraz Apple iOS 6 czy możliwość sortowania tagów w kolumnach.

E-wsparcie dla compliance

RSA Archer eGRC pozwala budować skuteczny system zarządzania przedsiębiorstwem łączący w sobie zarządzanie ryzykiem i compliance z uwzględnieniem całego IT, finansów, operacji biznesowych i działu prawnego. Poprzez RSA Archer można zarządzać ryzykiem, wykazać zgodność z wymaganiami compliance oraz automatyzacji procesów biznesowych.

Digital Forensic Challenge 2013 w toku

Dużym zainteresowaniem cieszy się konkurs dla informatyków śledczych organizowany przez amerykański DC3 Defence Cyber Crime Centre, czyli Biuro Dochodzeń Specjalnych Sił Powietrznych USA. W bieżącej edycji bierze w nim udział prawie 1000 zespołów. Co ciekawe 47% z nich to teamy spoza Stanów Zjednoczonych. W ostatnich tygodniach do rywalizacji dołączył też zespół laboratorium Mediarecovery.

Bit9 i FireEye zintegrowane

W połowie czerwca 2013 roku odbędzie się premiera nowych wersji Bit9 i FireEye. Połączenie whitelistingu i zautomatyzowanej analizy zachowań aplikacji w ramach sieci wewnętrznej tworzy razem zupełnie nowy standard skutecznej ochrony przed zaawansowanym malware oraz atakami APT i TPT. Ciekawostką jest, że światowa prapremiera odbędzie się w Polsce, podczas konferencji organizowanej przez Mediarecovery. Firma jest polskim partnerem zarówno Bit9, jak i FireEye.

BitTorrent na 3 miejscu w Europie

Serwis internetowy Sandvine opublikował raport dotyczący wykorzystania Internetu z podziałem na kontynenty. W Europie, w przypadku ruchu wychodzącego są to kolejno: przeglądanie stron internetowych (26%), oglądanie filmów na YouTube (24%) oraz pobieranie plików przy użyciu BitTorrent (12%). W przypadku ruchu wychodzącego „liderem" jest BitTorrent. Za pośrednictwem tej aplikacji wysyłanych jest aż 41% danych pochodzących z komputerów internautów. Na kolejnych miejscach znalazło się przeglądanie stron internetowych (11%) oraz wysyłanie filmów do YouTube (8%).

Na walce z piractwem da się zarobić

Jak informuje serwis torrentfreak.com szef amerykańskiej organizacji RIAA (Recording Industry Association of America), Cary Sherman, zarobił 1,4 miliona dolarów w 2011. Organizacja dbająca o interesy przemysłu muzycznego odnotowuje od pewnego czasu spadek przychodów. Wprowadzony program oszczędnościowy objął zwolnienia kilkudziesięciu osób i zmniejszenie wydatków na obsługę prawną (z 6 mln do 1,2 mln dolarów). Nie wpłynął jednak na zmniejszenie pensji zarządu.

T-Mobile ostrzega przed wirusem

Na adresy e-mailowe przesyłane są informacje sugerujące, że pochodzą od operatora telekomunikacyjnego T-Mobile. Przychodzą z adresów nadawcy: noreply@mmsc.t-mobile.pl lub noreply@mms.t-mobile.pl . Załącznik zawiera w sobie wirusa. Operator przestrzega przed otwieraniem tych wiadomości. My ze swojej strony dodamy, że w każdym przypadku do korespondencji e-mail należy podchodzić ze zdrowym rozsądkiem.

Chińczycy znów w akcji

Jak informuje zachodnia prasa doszło do wielkiego wycieku danych dotyczących technologii wojskowych USA. Chińscy hakerzy weszli w posiadanie planów amerykańskich zaawansowanych systemów obrony przeciwrakietowej. Mówi się również o planach myśliwca F/A-18 i śmigłowca Black Hawk. Ataki wymierzone są nie tylko w sektor rządowy ale również prywatne firmy z sektora zbrojeń. Nie tylko jednak Stany Zjednoczone borykają się z tym problemem. Wyciekły również plany budowy nowej siedziby wywiadu australijskiego. W skład planów wchodziły również lokalizacje serwerów i systemów zabezpieczeń. Australijski szef MSZ nie chciał komentować tych doniesień.

EnCase Analytics

Na corocznej konferencji CEIC (Computer and Enterprise Investigations Conference) organizowanej przez Guidance Software zapowiedziano nowe rozwiązanie o nazwie EnCase Analytics. System pozwoli między innymi na wykorzystanie danych z poziomu jądra systemu. Informacje analizowane są w skali całej sieci i wszystkich końcówek roboczych. System pozwala również na wizualizację danych w całej organizacji, bez względu na to jak duży i rozbieżny zakres danych zostanie poddany analizie. System charakteryzować się będzie przejrzystym, przyjaznym dla użytkownika interfejsem.

Malware okiem prawnika

Jarosław Góra

Wprowadzenie

Minęło już ponad 25 lat od pojawienia się pierwszych wirusów komputerowych. Od tej pory natura złośliwego oprogramowania znacząco się zmieniła, w głównej mierze przez rozwój i powstawanie nowych technologii oraz fakt, iż komputery wkroczyły w praktycznie każdą sferę życia. Do niedawna malware wykorzystywany był celem dokonywania drobnych aktów komputerowego wandalizmu oraz przysporzenia rozgłosu i reputacji jego twórcy. Dziś chodzi przede wszystkim o pieniądze i to zarówno w aspekcie tworzenia wirusów i złośliwego oprogramowania (produkcja), jak i korzystania z niego. Obok działających w pojedynkę hackerów pojawiły się dobrze zorganizowane „przedsiębiorstwa cyberprzestępcze". Organizacje przestępcze szybko zauważyły bowiem olbrzymi potencjał w złośliwym oprogramowaniu, jako drogim produkcie lub narzędziu do popełniania przestępstw.

Ludzie zajmujący się tworzeniem systemów i narzędzi bezpieczeństwa informacji stają dziś przed wyzwaniem odparcia ataku zaawansowanego malware-u, który został „uszyty na miarę", w celu dokonania konkretnego rodzaju ataku na konkretną organizację. Powtarzalne wirusy, które mogły zostać zatrzymane przez programy antywirusowe, zostały obecnie zastąpione zindywidualizowanym malwarem, który potrafi przystosować się, w zależności od tego jaki cel zainfekuje. Celem ataków są dziś wszelkie urządzenia (od PC, przez smartfony, po komputery przemysłowe), niezależnie od środowiska systemowego, jaki wykorzystują.

Okiem prawnika

Czy prawo nadąża za zmieniającą się rzeczywistością cyberprzestępczości w zakresie zaawansowanego malware-u ?

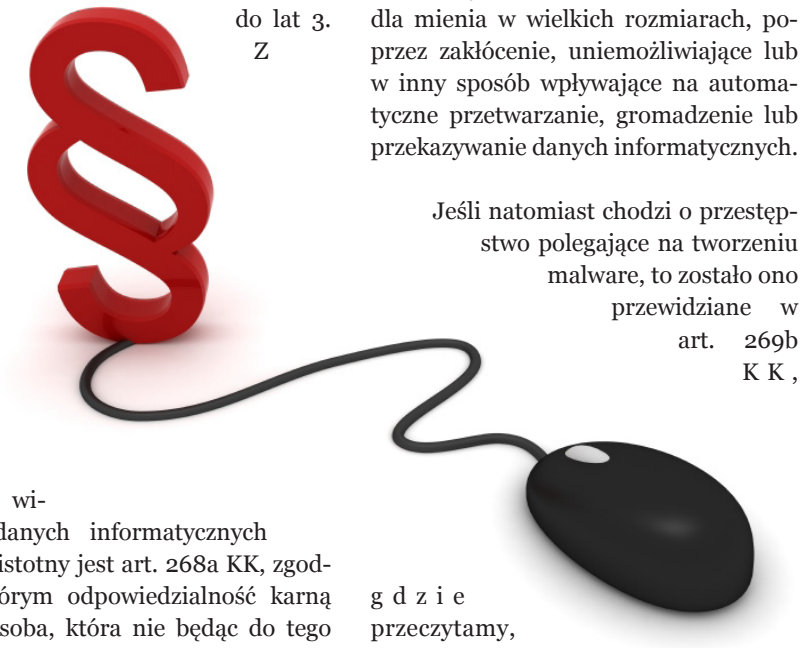
W związku z narastająca aktywnością grup cyberprzestępczych ustawodawcy pracują nad rozwiązaniami prawnymi, które umożliwią organom ścigania skuteczną z nimi walkę. Analizując te właśnie kwestie związane z istnieniem złośliwego oprogramowaniem w pierwszej kolejności należy zwrócić uwagę na dwa akty prawne uchwalone na poziomie europejskim. Chodzi mianowicie o decyzję ramową Rady Unii Europejskiej 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne oraz konwencję Rady Europy o cyberprzestępczości z 23 listopada 2001 r. Konieczność dostosowania polskich regulacji do wskazanych aktów prawnych spowodowała m.in. wprowadzenie do kodeksu karnego (Dz. U. z 1997 r., nr 88, poz. 553 z późn. zm., dalej również KK) zmian oraz nowych przepisów. Mówię tu o artykułach 267-269b w rozdziale XXXIII kodeksu karnego, które określają przestępstwa przeciw ochronie informacji.

Zainfekowanie danego systemu złośliwym oprogramowaniem może nastąpić na kilka sposobów. Oczywiście może wynikać z nieostrożnego zachowania użytkowników tego systemu (klasyczne kliknięcie w nieznany plik/link itp.), jednak równie często następuje to poprzez przełamanie zabezpieczeń danego systemu, uzyskanie do niego dostępu i zainstalowanie malware-u. Złośliwe oprogramowanie umożliwia zaś cyberprzestępcy między innymi pozyskanie chronionych danych.

Zgodnie natomiast z art. 267 § 1 KK uzyskanie, bez uprawnienia, dostępu do informacji dla siebie nieprzeznaczonej poprzez podłączenie się do sieci telekomunikacyjnej lub przełamanie albo ominięcie elektronicznych, magnetycznych, informatycznych lub poprzez inne szczególne jej zabezpieczenie stanowi przestępstwo zagrożone karą grzywny, ograniczenie wolności albo pozbawienia wolności do lat 2. W zakresie cyberprzestępczości i rzeczywistości cyberprzestępczości istotne są następne trzy paragrafy wskazanego przepisu, zgodnie z którymi tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego (§2), kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem (§ 3) oraz kto informację uzyskaną w ten sposób ujawnia innej osobie. ▶

Oprócz wykradzenia danych malware może posłużyć do ich zniszczenia, zmodyfikowania lub zaszyfrowania, np. celem uzyskania okupu. W takim przypadku w grę wchodzą dwa przepisy.

Zgodnie z art. 268 § 1 KK kto nie będąc do tego uprawnionym niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2. Przepis ten dotyczy informacji zapisanych na tradycyjnych nośnikach (np. papier), natomiast jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3. Z punktu widzenia danych informatycznych bardziej istotny jest art. 268a KK, zgodnie z którym odpowiedzialność karną ponosi osoba, która nie będąc do tego uprawniona, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3. Przesłanki tego przepisu zostaną spełnione np. gdy malware umożliwi przejęcie kontroli nad danym komputerem (w szerokim oczywiście rozumieniu).



Warto zwrócić uwagę, iż wskazane wyżej przestępstwa są ścigane jedynie na wniosek pokrzywdzonego. W przypadku złośliwego oprogramowania, które umożliwia przeprowadzania ataków DDoS (Distributed Denial of Service) w grę wchodzi art. 269a KK, zgodnie z którym kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej, ryzykuje odsiadką od 3 miesięcy do lat 5.

Warto wskazać również przepis z art. 165 § 1 pkt. 4 KK, zgodnie z którym przestępstwem jest sprowadzenie niebezpieczeństwa dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach, poprzez zakłócenie, uniemożliwiające lub w inny sposób wpływające na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych.

Jeśli natomiast chodzi o przestępstwo polegające na tworzeniu malware, to zostało ono przewidziane w art. 269b K K , gdzie przeczytamy, że zabronione jest wytwarzanie, pozyskiwanie, zbywanie lub udostępnianie innym osobom urządzeń lub programów komputerowych przystosowanych do popełnienia przestępstw, o których pisałem wyżej. Dotyczy to również haseł komputerowych, kodów dostępu lub innych danych umożliwiających dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej.

Taki proceder zagrożony jest karą pozbawienia wolności do lat 3. Na marginesie warto wskazać, że w USA samo stworzenie i posiadanie złośliwego oprogramowania nie jest karalne. Dopiero jego „szkodliwe użycie" grozi odpowiedzialnością. W Europie nielegalne jest już samo posiadanie malwaru na swoim sprzęcie, co może rodzić pewne wątpliwości w przypadku osób, których sprzęt został bez ich wiedzy zainfekowany.

Jak we wszystkich sprawach karnych związanych z cyberprzestrzenią wykrycie przestępstwa to jedno, natomiast zdecydowanie trudniej zidentyfikować sprawcę, zgromadzić i zabezpieczyć materiał dowodowy, złapać cyberprzestępce i wreszcie doprowadzić go przed oblicze polskiego sądu i udowodnić winę. Mając na uwadze tak wiele przeszkód, zarówno faktycznych jak i prawnych (Internet w końcu nie zna granic i cyberprzestępstw można dokonywać z każdego miejsca na ziemi), w wielu przypadkach ukaranie sprawcy będzie po prostu niemożliwe.

Oczywiście należy również pamiętać, że pokrzywdzeni przez cyberprzestępców mogą wystąpić z roszczeniami cywilnoprawnymi i domagać się odszkodowania. Jednak z cywilistycznego punktu widzenia dużo ciekawsza wydaje się kwestia ewentualnej odpowiedzialności np. administratora danego systemu, który w niedostateczny sposób zabezpieczył system danej firmy przed malwarem albo operatora poczty elektronicznej, którego filtry nie wykryły złośliwego oprogramowania załączonego do maila, czy też operatora strony www, który dopuścił do zainfekowania strony i naraził na to samo odwiedzających ją użytkowników. W pewnych okolicznościach przypisanie odpowiedzialności cywilnej tym podmiotom wydaje się możliwe.

Autor jest aplikantem adwokackim, szefem zespołu prawa IP oraz nowych technologii w kancelarii Ślązak, Zapiór i Wspólnicy.

MAGAZYN INFORMATYKI ŚLEDCZEJ I BEZPIECZEŃSTWA IT

mediarecovery
Lider informatyki śledczej

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

Redakcja i Wydawca nie zwracają tekstów nie zamówionych. Redakcja zastrzega sobie prawo redagowania i skracania tekstów. Redakcja nie odpowiada za treść zamieszczanych ogłoszeń.

Duplikator TD3

Karol Szczyrbowski

Najnowszym duplikatorem firmy Tableau jest urządzenie trzeciej generacji - duplikator TD3. Jest to narzędzie nie tylko dla wyspecjalizowanych techników informatyki śledczej lecz również zespołów bezpieczeństwa oraz funkcjonariuszy służb mundurowych. Wartym zaznaczenia jest fakt, że duplikator TD3 jest bardzo popularny wśród techników FBI.

Nowy duplikator Tableau to przede wszystkim nacisk na prostotę obsługi. Posiada ekran dotykowy, wykonuje kopie binarne z dysków SATA, IDE, USB 3.0/2.0/1.1, SAS oraz FireWire (1394A/B), co czyni z niego urządzenie o dużych możliwościach. W mojej opinii pod względem funkcjonalności duplikator

TD3 nie ma sobie równych pośród narzędzi do informatyki śledczej.

Innowacją, w stosunku do poprzednich generacji duplikatorów Tableau, jest moduł TDS1, będący kieszenią na dysk twardy, na który możemy wykonywać kopie binarne z dysków dowodowych. Dzięki zastosowaniu takiego rozwiązania nie musimy przejmować się okablowaniem dla dysku docelowego oraz jego chłodzeniem, które jest zamontowane w module TDS1. Widać, że dużo uwagi producent skupił na funkcjach sieciowych duplikatora, które pozwalają na przesłanie wykonanych wcześniej kopi binarnych poprzez iSCSI lub udziały sieciowe wykorzystujące protokół CIFS. Następną funkcją związaną z akwizycją danych jest możliwość wykonania kopii binarnej dysku twardego komputera Mac, wykorzystując jego funkcję „Target Mode" oraz kabel FireWire, którym połączymy komputer z duplikatorem.

Ciekawym rozwiązaniem jest możliwość utworzenia kont użytkowników, co umożliwia lepszą administrację pracy urządzenia. Podstawowe możliwości, takie jak wykonywanie kopii binarnych (w przypadku TD3 są to formaty RAW/DD, E01 i Ex01), wyliczanie oraz weryfikacja sum kontrolnych, klonowanie dysków (kopiowanie Disc-to-Disc) i inne, pozostają niezmienione w stosunku do poprzednich wersji duplikatorów Tableau. Wszystkie wymieniono w poprzednim numerze „Magazynu Informatyki Śledczej i Bezpieczeństwa IT".

Kluczowe funkcjonalności:

- Natywne blokowanie interfejsów: SATA, USB 3.0, FireWire.
- Formaty wyjściowe: RAW/DD, E01, Ex01.
- Modułowa budowa urządzenia.
- Moduł do przechowania dysku twardego, na który wykonywana jest kopia binarna (TDS1), zaprojektowany z myślą o ochronie i chłodzeniu dysku. Do obsługi nie jest wymagane dodatkowe okablowanie ani zewnętrzne zasilanie.
- Duplikator działający przez sieć (1Gb).
- Miejsca docelowe na kopie: macierz zewnętrzna przez iSCSI, macierz zewnętrzna przez CIFS, obudowa na dysk zawarta w TD3, macierze Tableau, „czysty" dysk twardy.
- Funkcja sieciowego lub lokalnego blokera zapisu z wykorzystaniem protokołów iSCSI.
- Sprzętowa kompresja formatów E01, Ex01.
- Ekran dotykowy 4,3", wyposażony w funkcje kontroli oraz informacje o statusie. Wysoka rozdzielczość obrazu.
- System operacyjny oparty o dystrybucję LINUX.
- Wbudowany głośnik.
- Opcjonalnie dodatkowe moduły umożliwiające połączenie dysków IDE, SCSI i SAS.
- System operacyjny zapisany na karcie SD.
- Możliwość bezpośredniego połączenia z zewnętrznymi urządzeniami magazynującymi dane (macierze np. Tableau Modular Storage).
- Zasilanie przez akumulatory typu COTS lub zasilacz impulsowy.
- Administracja utworzonymi kontami użytkowników.

Porty:

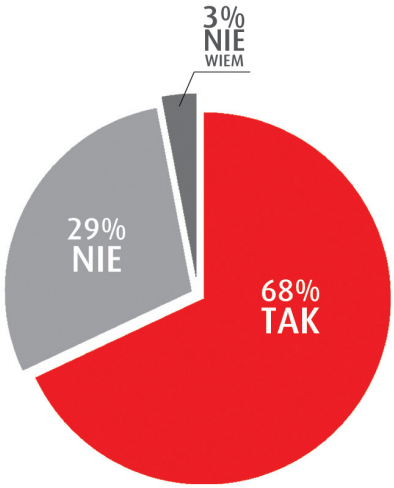
- FireWire800 1394B.
- USB 3.0.
- USB 2.0 (port serwisowy).
- SATA
- SAS, SCSI, IDE (połączenie przez dodatkowe interfejsy).
- HDD Power, zasilanie dysków twardych poprzez nowy port 3M link.
- Internet 1Gb.

Autor jest młodszym specjalistą informatyki śledczej w laboratorium Mediarecovery.

Połowa banków ma problem z nielojalnymi pracownikami

Zbigniew Engiel

Jak informuje Mediarecovery, firma zajmująca się informatyką śledczą i bezpieczeństwem IT, ankietowani szefowie departamentów bezpieczeństwa banków oraz specjaliści w nich zatrudnieni, aż w 50% odpowiedzi wskazali incydenty z udziałem pracowników. Jeszcze większym problemem są ataki spoza organizacji. Takie zdarzenia zasygnalizowano w 68%.



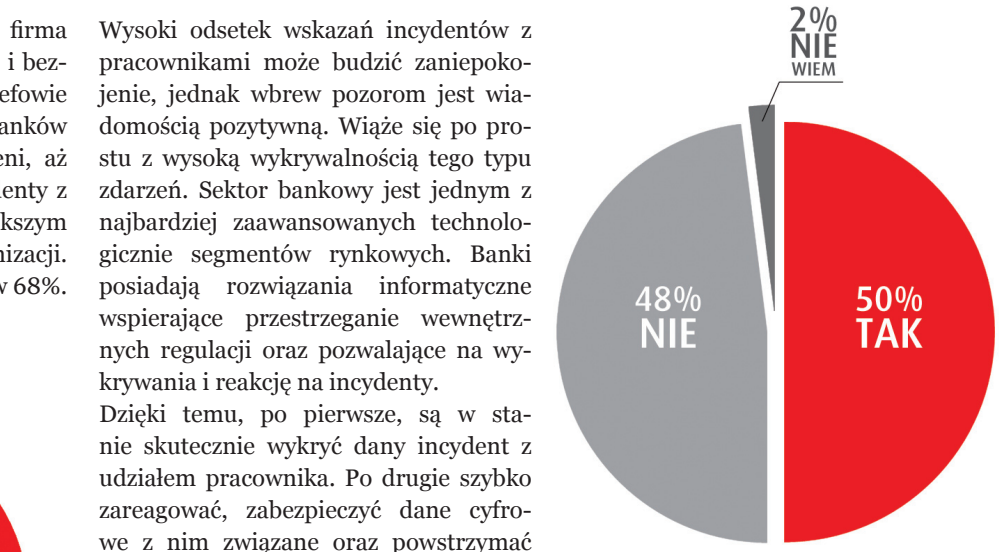
Czy w okresie ostatnich dwunastu miesięcy spotkali się Państwo z przypadkiem zagrożenia z zewnątrz? Np. atakiem poprzez malware, włamaniem do sieci.

Wysoki odsetek wskazań incydentów z pracownikami może budzić zaniepokojenie, jednak wbrew pozorom jest wiadomością pozytywną. Wiąże się po prostu z wysoką wykrywalnością tego typu zdarzeń. Sektor bankowy jest jednym z najbardziej zaawansowanych technologicznie segmentów rynkowych. Banki posiadają rozwiązania informatyczne wspierające przestrzeganie wewnętrznych regulacji oraz pozwalające na wykrywania i reakcję na incydenty.

Dzięki temu, po pierwsze, są w stanie skutecznie wykryć dany incydent z udziałem pracownika. Po drugie szybko zareagować, zabezpieczyć dane cyfrowe z nim związane oraz powstrzymać dalsze jego działania. Po trzecie, część z banków posiada również rozwiązania do etycznego monitoringu pracowników – twierdzą specjaliści z Mediarecovery.

Zagrożenia płyną nie tylko z wewnątrz

Aż 68% ankietowanych potwierdziło, iż ich instytucje w ostatnich 12 miesiącach były narażone na ataki zewnętrzne. 29% specjalistów biorących udział w ankiecie wskazało, że takie sytuacje nie miały miejsca w przypadku ich banków.

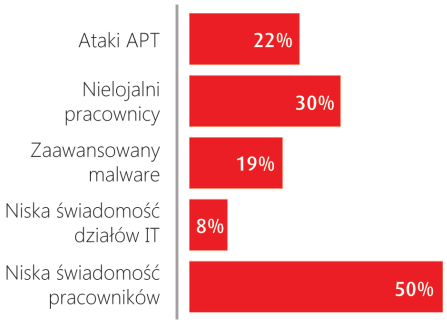


Czy w okresie ostatnich dwunastu miesięcy spotkali się Państwo z przypadkiem nielojalności pracowniczej? Np. wyciekiem informacji, celowym zniszczeniem danych itp.

Era widowiskowych, nagłaśnianych ataków jest już za nami. Obecnie przeprowadza się je w taki sposób żeby

REKLAMA

były niezauważalne. Skoro specjaliści z działów bezpieczeństwa banków o nich wiedzą to znaczy, że się nie udały.



Co według Pana jest obecnie największym zagrożeniem bezpieczeństwa IT: W pytaniu można było zaznaczyć kilka odpowiedzi, wynik nie sumują się do 100.

Największe zagrożenia bezpieczeństwa zdaniem banków

Spośród wszystkich, współczesnych zagrożeń specjaliści bezpieczeństwa, aż w 50% wskazali „niską świadomość pracowników". Wykorzystanie tej podatności jest podstawą większości ataków typu APT (Advanced Persistent Threats). Niską świadomość pracowników z powodzeniem wykorzystuje się przy atakach z użyciem malware.

Kolejnym zagrożeniem wskazanym przez ankietowanych są „nielojalni pracownicy", którzy wykazują zapewne wyższy stopień świadomości lecz równocześnie złą wolę. Ataki APT wymieniono w 22%, a zaawansowany malware 19%. Najmniejszym zagrożeniem zdaniem specjalistów jest „niska świadomość działów IT". Takich wskazań było 8%.

Oprócz zaawansowanych systemów bezpieczeństwa, równie ważne jest podnoszenie stanu wiedzy wszystkich zatrudnionych osób – twierdzspecjaliści z Mediarecovery. Dlatego tego typu szkolenia są stałym elementem naszych ofert związanych z wdrożeniem rozwiązań IT security – dodaje.

Wnioski

Wiedza o tym, że dochodzi do prób infekcji poprzez malware, prób włamań poprzez wykorzystanie podatności, zaniedbania administratorów czy też nielojalnych zachowań pracowników jest dobrym punktem wyjścia do ulepszania istniejących sposobów obrony. Jak mówi Sebastian Małycha, prezes Mediarecovery – Rynek narzędzi do wykrywania i reakcji na incydenty rozwija się bardzo szybko. Zjawisko jest pozytywne nie tylko w kontekście gospodarczym ale przede wszystkim w aspekcie bezpieczeństwa. Duże nasycenie rynku rozwiązaniami IT security wymusza niejako na firmach i instytucjach rozpoczęcie budowy systemów zapewniających wyższy poziom bezpieczeństwa. Tendencję tą widać bardzo dobrze również w wynikach naszej sprzedaży – dodaje prezes Małycha.

REKLAMA