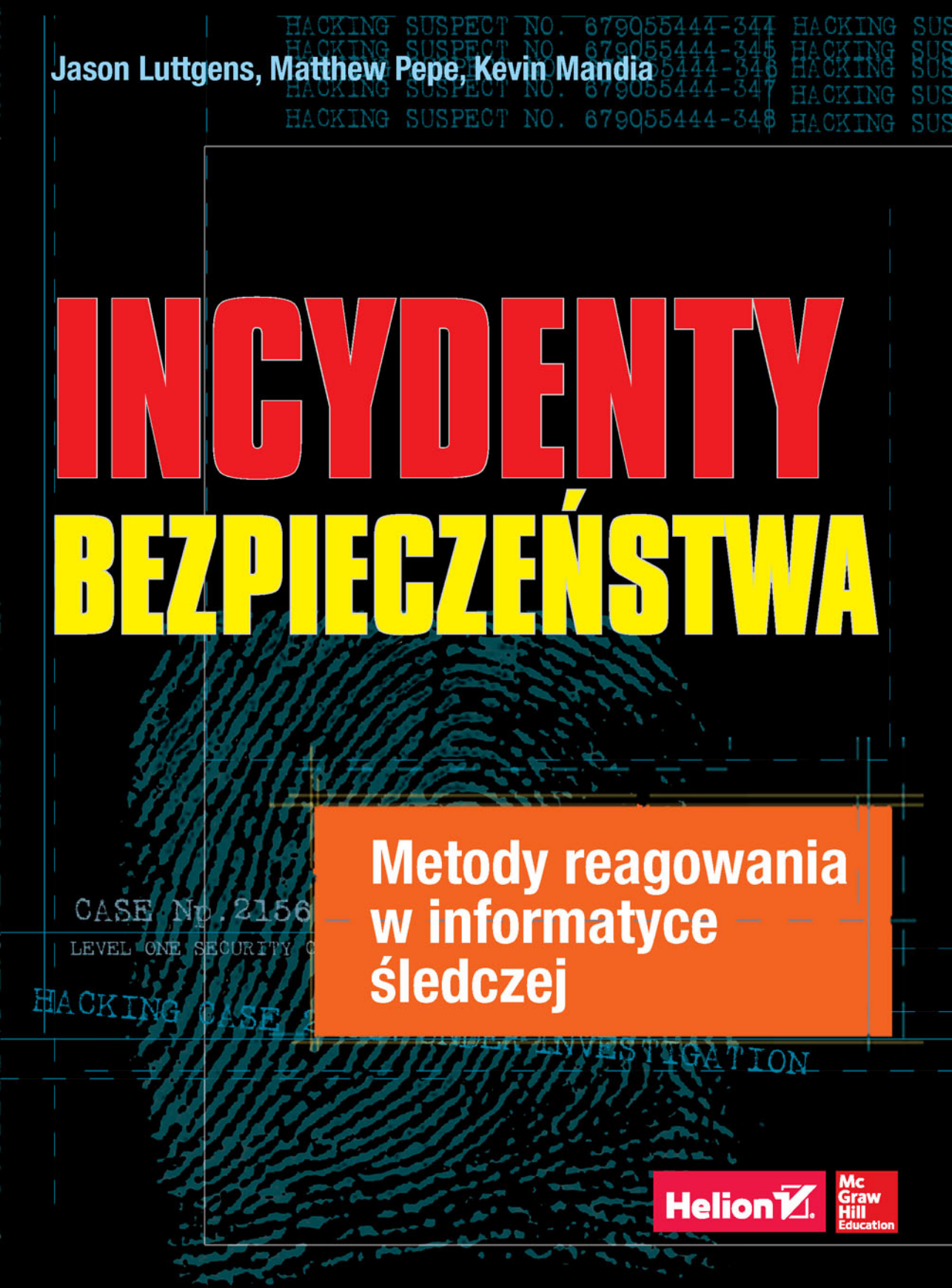
Jason Luttgens, Matthew Pepe, Kevin Mandia

INCYDENTY BEZPIECZEŃSTWA

Metody reagowania w informatyce śledczej



Helion
Mc Graw Hill Education

Tytuł oryginału: Incident Response & Computer Forensics, Third Edition

Tłumaczenie: Łukasz Piwko

ISBN: 978-83-283-1483-2

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/incbez
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

Spis treści

CZĘŚĆ V Naprawa

ROZDZIAŁ 2.

Podręcznik reagowania na incydenty bezpieczeństwa

Przygotowanie się na incydent bezpieczeństwa komputerowego i odpowiednia reakcja to duże wyzwanie. Technologia nie stoi w miejscu, przez co czasami może się wydawać, że trudno za nią nadążyć. Jednak wspólnie mamy już ponad trzydzieści lat doświadczenia w tej branży i pracowaliśmy nad setkami przypadków w organizacjach każdej wielkości. W odniesieniu do tego rozdziału do głowy przychodzą dwie konkretne myśli. Po pierwsze, największe trudności przy reagowaniu na incydenty powodują sprawy nietechniczne. Po drugie, podstawowe zasady badania incydentów bezpieczeństwa komputerowego nie różnią się od nietechnicznych śledztw. Największą trudnością jest przedarcie się przez szum marketingowy, którego celem jest przekonanie nas, że jest inaczej.

W rozdziale tym pragniemy pomóc Ci w przejściu przez gąszcz modnych słów i marketingowy szum, abyś wiedział, co naprawdę jest ważne, i mógł sporządzić solidny program reagowania na incydenty bezpieczeństwa. Zaczynamy od podstaw, czyli wyjaśniamy, co oznacza bezpieczeństwo komputerowe, jakie są cele reakcji na incydent oraz kto bierze udział w tym procesie. Następnie opisujemy fazy cyklu śledztwa, metody zdobywania najważniejszych informacji oraz techniki raportowania. Z doświadczenia wiemy, że organizacje, które poświęcają dużo czasu na przemyślenie tych kwestii, znacznie skuteczniej radzą sobie z incydentami bezpieczeństwa.

CO TO JEST INCYDENT BEZPIECZEŃSTWA KOMPUTEROWEGO

Definicja incydentu bezpieczeństwa komputerowego określa zakres działań utworzonego zespołu specjalistów i pozwala skupić działania na odpowiednich obszarach. Definicja jest bardzo ważna, ponieważ dzięki niej każdy członek drużyny zna swoje obowiązki. Jeśli jeszcze jej nie sformułowałeś, powinieneś jak najszybciej określić, co w Twojej organizacji oznacza pojęcie „incydent bezpieczeństwa komputerowego". Nie istnieje jedyna powszechnie przyjęta definicja, ale uważa się, że incydent bezpieczeństwa komputerowego to każde zdarzenie:

- którego celem jest spowodowanie szkody,
- którego sprawcą jest człowiek,
- w którym wykorzystywane są zasoby komputerowe.

Przyjrzymy się krótko tym cechom. Pierwsze dwie są zbieżne z wieloma typami incydentów nietechnicznych, np. podpaleniem, kradzieżą czy napaścią. Jeśli celem nie jest wyrządzenie krzywdy, trudno zdarzenie nazwać incydentem. Należy przy tym podkreślić, że szkoda może nie być *natychmiastowa*. Przykładowo skanowanie systemu w poszukiwaniu luk w zabezpieczeniach, które później zostaną wykorzystane w szkodliwy sposób, samo w sobie nie powoduje szkody — ale bez wątpienia jest to działanie, którego celem jest wyrządzenie krzywdy. Druga cecha, czyli udział człowieka, wyklucza takie zdarzenia jak losowe awarie systemu i czynniki niezależne od nas, np. pogodę. To, że z powodu przerwy w dopływie energii przestała działać zapora sieciowa, wcale nie oznacza, że wystąpił incydent bezpieczeństwa, chyba że sprawcą tej przerwy jest działający umyślnie człowiek albo ktoś wykorzysta nadarzającą się okazję do zrobienia czegoś niedozwolonego.

Trzecia cecha decyduje o tym, że dane zdarzenie to właśnie incydent bezpieczeństwa komputerowego, ponieważ dotyczy zasobów komputerowych. Pojęcia „zasoby komputerowe" używamy, ponieważ obejmuje szeroki wachlarz różnych technologii. Czasami zasoby komputerowe pozostają niezauważone — są to nośniki do archiwizacji danych, telefony, drukarki, karty dostępu do budynków, tokeny dwuskładnikowe, kamery, automaty, urządzenia GPS, tablety, telewizory i wiele innych. Urządzenia komputerowe są wszędzie i czasami zapominamy, jak dużo informacji się w nich znajduje, czym sterują oraz do czego są podłączone.

Czasami możemy nie mieć pewności, czy dane zdarzenie jest incydentem, dopóki nie przeprowadzimy pewnych analiz wstępnych. Podejrzaną aktywność zawsze należy traktować jako potencjalny incydent, który trzeba zbadać i ewentualnie udowodnić, że nim nie jest. Może też się zdarzyć, że w toku śledztwa prowadzonego w sprawie incydentu okaże się, że to wcale nie był incydent bezpieczeństwa.

Oto kilka przykładów typowych incydentów bezpieczeństwa komputerowego:

- kradzież danych, takich jak poufne informacje osobiste, wiadomości e-mail i dokumenty;
- kradzież funduszy, np. nieuprawniony dostęp do konta bankowego, skorzystanie z karty kredytowej lub oszustwo dotyczące przelewów;
- wyłudzenie;
- nieuprawniony dostęp do zasobów komputerowych;
- obecność szkodliwego oprogramowania, np. narzędzi zdalnego dostępu i programów szpiegujących;
- posiadanie nielegalnych lub nieautoryzowanych materiałów.

Skutkiem tych incydentów może być konieczność przeinstalowania kilku komputerów, poniesienie dużych kosztów związanych z czynnościami naprawczymi, a nawet zamknięcie całej organizacji. Decyzje, które podejmiesz, zarówno przed incydentem, podczas jego trwania, jak i po incydencie, będą miały bezpośredni wpływ na to, co się wydarzy.

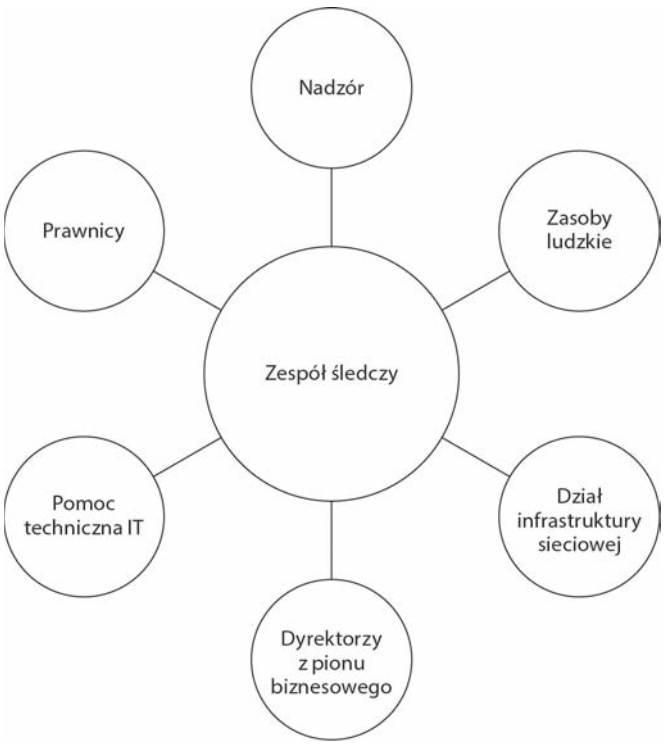
CELE REAKCJI NA INCYDENT

Głównym celem reagowania na incydent bezpieczeństwa jest pozbycie się zagrożenia ze środowiska komputerowego organizacji, zminimalizowanie szkód oraz przywrócenie normalnej działalności. Cel ten osiąga się, wykonując dwie ważne czynności. Oto one.

- Śledztwo
  - Ustalenie początkowej metody przeprowadzenia ataku.
  - Ustalenie użytych szkodliwych programów i narzędzi.
  - Ustalenie, które systemy zostały zainfekowane i w jaki sposób się to stało.
  - Ustalenie, czego hakerowi udało się dokonać (szacowanie szkód).
  - Ustalenie, czy incydent trwa.
  - Ustalenie czasu trwania incydentu.
- Czynności naprawcze
  - Wykorzystanie informacji zdobytych w toku śledztwa oraz opracowanie i wdrożenie planu naprawczego.

KTO BIERZE UDZIAŁ W PROCESIE REAKCJI NA INCYDENT

Reakcja na incydent (ang. *incident response* — IR) to dyscyplina obejmująca wiele dziedzin. Wymaga znajomości zasobów z kilku różnych jednostek operacyjnych organizacji. Jak wynika z rysunku 2.1, w proces reagowania na incydent bezpieczeństwa może zostać zaangażowanych wiele osób z różnych działów firmy, np. specjaliści od zasobów ludzkich, prawnicy, informatycy, specjaliści od PR, specjaliści od zabezpieczeń, ochroniarze, dyrektorzy, pracownicy pomocy technicznej i inni.



RYSUNEK 2.1. *Skład zespołu*

Na czas trwania procesu reakcji na incydent firmy zazwyczaj tworzą zespoły złożone z wyznaczonych osób, których zadaniem jest przeprowadzenie dochodzenia i pozbycie się problemu. Zespołem dowodzi doświadczony kierownik, najlepiej jeśli jest to ktoś potrafiący kierować innymi jednostkami biznesowymi podczas śledztwa. Tego, jak ważny jest ten ostatni punkt, nie da się przecenić. Kierownik zespołu musi szybko zdobywać informacje i zlecać zadania do wykonania wszystkim zasobom w organizacji. Dlatego jest nim często dyrektor ds. informatyki i zabezpieczeń albo ktoś mu bezpośrednio podległy. Osoba ta staje się osią całego przedsięwzięcia,

nadzoruje wiele działań oraz dba o to, by wszystko było wykonywane, jak należy. Zespołem naprawczym kieruje doświadczony pracownik działu informatycznego. Jest to postać, na której spoczywa obowiązek koordynowania wszystkich czynności naprawczych, włącznie z działaniami podjętymi na podstawie wyników śledztwa, oceną stopnia poufności skradzionych danych oraz wprowadzeniem strategicznych zmian mających na celu zapewnienie większego bezpieczeństwa firmy.

Większość organizacji obsadza zespoły reagowania i naprawczy osobami z różnych szczebli i działów. Wśród nich podczas śledztwa często można znaleźć pracowników wyższego szczebla z działów IT, zwłaszcza mających doświadczenie w analizowaniu dzienników, informatyce śledczej i rozpoznawaniu wirusów. Zespół śledczy powinien też mieć szybki dostęp do miejsc przechowywania dzienników, konfiguracji systemu oraz musi posiadać uprawnienia do wyszukiwania potrzebnych materiałów, jeżeli w użyciu jest obejmująca całe przedsiębiorstwo platforma reagowania na incydenty. Ponadto w grupie mogą znaleźć się konsultanci, którzy będą opracowywać taktykę śledztwa, jeśli mają odpowiednie doświadczenie. Zespół naprawczy z kolei powinien mieć uprawnienia do tego, aby nakazać wprowadzenie zmian potrzebnych do pozbycia się problemu.

Uwaga

Uzyskanie uprawnień do wyszukiwania informacji w całym przedsiębiorstwie może być trudne, ponieważ istnieją regulacje prawne i lokalne, które mogą w tym przeszkadzać, zwłaszcza na terenie Unii Europejskiej.

W zespołach pomocniczych tworzonych w razie potrzeby z reguły nie muszą znajdować się ludzie związani ze śledztwem ani czynnościami naprawczymi. Ich praca zazwyczaj polega na wykonywaniu konkretnych zadań na żądanie kierownika śledztwa. Typowymi członkami zespołów pomocniczych są:

- wewnętrzni i zewnętrzni radcy prawni;
- inspektorzy nadzoru (np. PCI, HIPAA, FISMA oraz NERC);
- pracownicy pomocy technicznej;
- członkowie zespołów zajmujących się infrastrukturą sieci;
- dyrektorzy z pionu biznesowego;
- przedstawiciele działu zasobów ludzkich;
- pracownicy działu PR.

Skład zespołów śledczych i naprawczych opisujemy w rozdziale 3., ale należy pamiętać, że relacje i oczekiwania należy ustalić z góry. Najgorszym momentem do otrzymania wytycznych od rady lub inspektorów jest czas, gdy śledztwo już trwa. Bardzo dobrym pomysłem jest określenie wszystkich wymogów dotyczących raportowania i całego procesu w sposób odpowiedni dla swojej branży.

Co powinno się wiedzieć z perspektywy nadzoru? Jeśli jeszcze nie odbyłeś spotkania z inspektorami wewnętrznymi, którzy jednocześnie mogą być głównymi radcami prawnymi firmy, poświęć dzień na rozmowy o cyklu incydentu. Dowiedz się, jakie systemy informatyczne są objęte atakiem i jakie obowiązują wymagania dotyczące składania raportów.

W niektórych sytuacjach odpowiedź na pytanie o zasięg może być znaleziona innymi środkami (mogą to być np. oceny zgodności z normami PCI DSS). Dowiedz się, kogo należy informować o potencjalnych włamaniach i przypadkach złamania zabezpieczeń, a także jakie są zdefiniowane progi powiadomień. Co najważniejsze, znajdź wewnętrzną jednostkę odpowiedzialną za komunikację na zewnętrz i upewnij się, że członkowie Twojego zespołu mogą rozmawiać z decydentami bez owijania w bawełnę.

Wewnętrzna rada prawników powinna pomóc w określeniu odpowiadających jej progów raportowania. Różne parametry (czas od identyfikacji zdarzenia, możliwość wycieku danych, zakres potencjalnego wycieku) mogą nie pasować do parametrów określonych przez strony zewnętrzne.

Uwaga

Jedną z branż, która notorycznie narzuca procesy i standardy śledczym, jest branża kart płatniczych. Gdy przedstawiciele tej gałęzi zostaną zaangażowani w proces śledczy, prowadzone przez Ciebie działania naprawcze mają drugorzędne znaczenie w porównaniu z ich celem ochrony marki i zmotywowania organizacji do spełnienia wymogów standardu PCI DSS.

Wyszukiwanie utalentowanych specjalistów do zespołu reagowania na incydenty

Pracujemy w firmie świadczącej usługi konsultacyjne na rzecz organizacji borykających się z poważnymi problemami dotyczącymi bezpieczeństwa informacji. Biorąc to pod uwagę, wiemy, że z całego serca powinniśmy zalecać zatrudnianie konsultantów, jeśli tylko wystąpią jakiekolwiek incydenty. To trochę tak, jakby pytać przedstawiciela firmy Porsche, czy potrzebujemy najnowszego modelu ich samochodu. Szczera odpowiedź na pytanie, czy dana firma powinna skorzystać z usług konsultanta, czy zlecić wykonanie wszystkich prac firmie konsultacyjnej, zależy od wielu czynników. Oto one.

- **Koszt utrzymywania zespołu reagowania na incydenty** — jeśli tempo operacji nie jest wysokie i nie można wykazać ich wyników, wiele firm nie może sobie pozwolić na utrzymywanie zespołu doświadczonych specjalistów od reagowania na incydenty ani uzasadnić jego istnienia.
- **Kultura zlecania zadań na zewnątrz** — wiele organizacji zleca różne zadania biznesowe, włącznie z usługami IT. Ku naszemu zaskoczeniu kilka firm z listy „Fortune" 500 zleca ogromną większość swoich usług informatycznych na zewnątrz. Zjawisko to i jego implikacje dla powodzenia reakcji na incydent omawiamy w jednym z kolejnych rozdziałów.
- **Upoważnienie przez władze nadzorujące i urząd certyfikacji** — przykładem zewnętrznej organizacji, która może dyktować, w jaki sposób ma być prowadzona akcja, jest Rada PCI Security Standards Council. Jeżeli Twoja firma działa w branży związanej z kartami kredytowymi, wspomniana rada może narzucić wymóg, aby śledztwo prowadziły „zatwierdzone" firmy.

- **Brak doświadczenia w prowadzeniu śledztw** — wynajęcie doświadczonej firmy konsultacyjnej może być najlepszym sposobem na utworzenie zalążka własnego zespołu reagowania na incydenty (RI). Prowadzenie dochodzeń to działalność wymagająca doświadczenia i umiejętności w tym zakresie rosną wraz ze zdobywanym doświadczeniem.
- **Brak lub ograniczone zasoby własnych specjalistów** — prowadzenie śledztw, zwłaszcza dotyczących włamań, wymaga dużych umiejętności i szerokiej wiedzy, od znajomości sposobu działania systemów operacyjnych, aplikacji i sieci po umiejętność analizowania szkodliwych programów i przeprowadzenia czynności naprawczych.

Z wyjątkiem sytuacji, gdy firma nie ma w ogóle żadnego wewnętrznego działu IT, z naszego doświadczenia wynika, że organizacje utrzymujące własne zespoły ds. reagowania na incydenty mają większą szansę na skuteczne śledztwo i szybkie rozwiązanie problemu. Jest tak nawet wtedy, kiedy zespół RI przeprowadzi tylko wstępne czynności śledcze przy zaangażowaniu pomocy z zewnątrz.

Uwaga

Kiedy zatrudniamy zewnętrznych ekspertów do pomocy w śledztwie, warto napisać umowę przy pomocy radców prawnych, aby jej postanowienia były zabezpieczone przed ujawnieniem.

Jak zatrudnić talent

Zatrudnianie odpowiednich ludzi sprawia trudności wszystkim dyrektorom. Jeśli masz zespół i chcesz go powiększyć, znalezienie odpowiedniej osoby może być łatwiejsze, ponieważ w ocenie umiejętności i osobowości aplikanta możesz liczyć na pomoc członków zespołu. Ponadto już wiesz, jak się to robi i do jakich ról potrzebujesz ludzi, co ułatwia sporządzenie profilu idealnego kandydata. Jeżeli jednak znajdujesz się w sytuacji typowej dla specjalisty od zabezpieczeń informatycznych, który musi utworzyć niewielki zespół RI, to od czego zaczniesz? Zalecamy podzielenie procesu szukania pracownika na dwa etapy, czyli znalezienie kandydatów, a następnie ocenienie ich kwalifikacji i tego, czy pasują do Twojej firmy.

Znajdowanie kandydatów

Jednym z narzucających się pomysłów jest rekrutowanie członków innych zespołów RI. Dobrym pomysłem jest też umieszczenie ogłoszeń w portalach typu LinkedIn, choć jest to metoda pasywna. Szybsze efekty daje aktywne poszukiwanie kandydata np. w grupach technicznych, odpowiednich mediach społecznościowych i na tablicach ogłoszeń. Do wielu specjalistów od informatyki śledczej o różnym poziomie umiejętności można dotrzeć właśnie poprzez tablice ogłoszeń, takie jak np. Forensic Focus.

Jeśli masz możliwość skontaktowania się z biurami karier ośrodków uniwersyteckich, na uczelniach z dobrym programem nauczania w dziedzinach informatyki, inżynierii i informatyki śledczej możesz znaleźć początkujących analityków do zespołu. Z naszego doświadczenia wynika, że najlepszych kandydatów do naszej pracy można znaleźć tam, gdzie program obejmuje jako przedmiot główny czteroletni kurs informatyki i inżynierii oraz istnieje możliwość odbywania dodatkowych kursów z informatyki śledczej albo zdobywania certyfikatów z tej dziedziny.

Odwrotnie jest natomiast w miejscach uczących wszystkiego w ramach głównego programu nauczania. Podstawowe zdolności, jakie powinien posiadać idealny kandydat, są takie same jak w większości innych dziedzin naukowych: są to zmysł obserwacji oraz umiejętność porozumiewania się, klasyfikowania, mierzenia, wnioskowania i przewidywania. Osoby obdarzone takimi talentami są z reguły najlepszymi członkami zespołów RI. Jeśli znajdziesz w pobliżu swojej firmy uczelnię, której program nauczania skupia się najpierw na podstawach nauki i inżynierii oraz przewiduje seminaria lub przedmioty fakultatywne z informatyki śledczej, masz szczęście.

Ocenianie przydatności kandydata: zdolności i cechy

Jakie zdolności powinni mieć członkowie Twojego zespołu RI? Generalnie zespół taki powinien składać się z osób o różnych talentach, takich, które mają wiedzę i umiejętności pozwalające im przechodzić między kolejnymi fazami śledztwa. Patrząc na naszą grupę konsultacyjną, dostrzegamy pewne cechy, które wydają się cenne. Jeśli zatrudniasz doświadczonych kandydatów, weź pod uwagę to, czy mają poniższe kwalifikacje.

- **Doświadczenie w prowadzeniu śledztw w środowisku technologicznym** — jest to szerokie pole obejmujące zarządzanie informacjami i analizowanie tropów, umiejętność współdziałania z innymi jednostkami biznesowymi, zdolność analizowania dowodów i danych oraz podstawowe umiejętności techniczne.
- **Doświadczenie w prowadzeniu ekspertyz z zakresu informatyki śledczej** — na doświadczenie takie składa się znajomość podstaw działania systemów operacyjnych, znajomość artefaktów systemów i aplikacji, umiejętność analizowania dzienników oraz pisania zrozumiałej dokumentacji.
- **Doświadczenie w analizowaniu ruchu sieciowego** — jest to umiejętność badania ruchu sieciowego i protokołów oraz znajomość technologii pozwalających na wykorzystanie zdobytych informacji w systemie detekcyjnym.
- **Znajomość aplikacji z branży działalności organizacji** — większość firm posiada specjalne systemy przetwarzające dane na specjalnych platformach (np. transakcje finansowe odbywające się na komputerach mainframe).
- **Znajomość zagadnień IT dla przedsiębiorstw** — przy braku platformy RI nie ma nic lepszego od administratora umiejącego napisać dwulinijkowy skrypt przeszukujący wszystkie znajdujące się pod jego kontrolą serwery.
- **Umiejętność analizowania szkodliwego kodu źródłowego** — osoba potrafiąca to robić jest bardzo ważnym członkiem zespołu, ale większość zespołów RI może się bez niej obyć, wykonując podstawową analizę automatycznie „w piaskownicy". Jeśli masz trzy wolne miejsca pracy, zatrudnij wszechstronne osoby posiadające podstawową wiedzę w zakresie wykrywania szkodliwej działalności.

Jakie cechy osobowości powinien mieć członek zespołu RI? Podczas rozmów o pracę próbujemy dowiedzieć się, czy kandydat ma następujące cechy:

- wysokie kompetencje analityczne,
- wysokie kompetencje komunikacyjne,

- umiejętność dostrzegania szczegółów,
- metodyczne i zorganizowane podejście do rozwiązywania problemów,
- udowodnione sukcesy w rozwiązywaniu problemów.

Często jesteśmy pytani o to, czy różne certyfikaty, od których roi się w branżach informatyki śledczej i RI, są coś warte. Zasadniczo wszystkie certyfikaty wymagające okresowego zdawania testów i wykazywania, że ktoś cały czas się uczy, są dobrym wskaźnikiem, że taka osoba aktywnie działa na pewnym polu. Jeśli aplikant ma niewielkie doświadczenie w pracy, na podstawie odbytych przez niego szkoleń możemy wytypować tematy do poruszenia podczas rozmowy o pracę. Ponadto, jeśli testy certyfikacyjne są dostępne w internecie, możemy przy okazji sprawdzić zdolności komunikacyjne kandydata oraz jego styl pisania. Jeśli nie, to mamy dobry wskaźnik prawdziwych umiejętności kandydata. W istocie zauważamy odwrotną zależność między głębią wiedzy aplikanta i liczbą posiadanych przez niego certyfikatów, jeśli jego doświadczenie zawodowe jest solidne. Nieprzydatne z reguły są certyfikaty wydawane przez konkretne firmy, ponieważ stanowią one tylko poświadczenie umiejętności w zakresie posługiwania się konkretnymi narzędziami, a nie posiadania gruntownej wiedzy teoretycznej i możliwości działania.

PROCES REAKCJI NA INCYDENT

Proces reakcji na incydent składa się z wszystkich czynności, których wykonanie jest konieczne, aby osiągnąć cele tej reakcji. Cały proces i poszczególne działania powinno się skrupulatnie udokumentować i przedstawić zespołowi RI oraz akcjonariuszom organizacji. Reakcja na incydent składa się z trzech podstawowych czynności i z naszych doświadczeń wynika, że najlepiej, aby każdą z nich wykonywała wyspecjalizowana grupa. Są to:

- czynności wstępne,
- śledztwo,
- naprawa.

Wstępna reakcja na incydent to czynność, która rozpoczyna właściwy proces reakcji na incydent. Gdy zespół potwierdzi, że rzeczywiście doszło do złamania zabezpieczeń, i przeprowadzi czynności wstępne polegające na zebraniu początkowego materiału dowodowego oraz podjęciu wstępnych środków zaradczych, działania śledcze i zaradcze są z reguły prowadzone równolegle. Celem zespołu śledczego jest wyłącznie przeprowadzenie śledztwa, w czasie którego specjaliści tworzą listy tzw. „tropów". Tropy to dające się wykorzystać informacje o skradzionych danych, wskaźniki sieciowe, zidentyfikowane potencjalne podmioty lub problemy, które przyczyniły się do zaistnienia danej sytuacji zagrożenia lub złamania zabezpieczeń. Wszystkie mogą być natychmiast wykorzystane przez specjalistów, których procesy też muszą być koordynowane i planowane, co wymaga czasu. Często zdarza się tak, że odkryta aktywność jest na tyle groźna, iż trzeba natychmiast zareagować, aby zapobiec dalszej działalności intruza.

Czynności wstępne

Na tym etapie głównym celem jest zebranie zespołu RI, przejrzenie danych sieciowych i innych, które są od razu dostępne, ustalenie rodzaju incydentu oraz ocena potencjalnych skutków. Chodzi o to, by zgromadzić informacje potrzebne zespołowi do podjęcia decyzji, w jaki sposób zareagować.

Zazwyczaj na etapie tym nie zbiera się danych bezpośrednio z dotkniętego systemu. Najczęściej informacje zdobyte w tej fazie dotyczą sieci, dzienników oraz innych dowodów historycznych i kontekstowych. Na ich podstawie można podjąć decyzję, jakie środki zaradcze przedsięwziąć. Jeśli np. koń trojański zostanie znaleziony w laptopie dyrektora finansowego banku, sposób działania będzie całkiem inny niż w przypadku wykrycia tego szkodliwego programu w komputerze recepcjonisty. Jeżeli ponadto konieczne jest przeprowadzenie pełnego śledztwa, informacje te będą częścią pierwszych tropów. Oto lista niektórych czynności, które typowo wykonuje się na tym etapie.

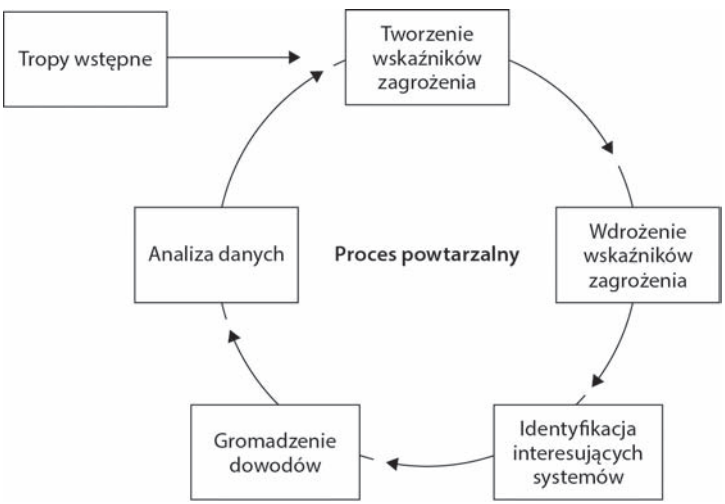
- Przeprowadzenie rozmów z osobami, które zgłosiły incydent, aby wydobyć jak najwięcej przydatnych informacji.
- Przeprowadzenie rozmów z pracownikami IT, którzy mogą coś wiedzieć o szczegółach incydentu.
- Przeprowadzenie rozmów z pracownikami z pionu biznesowego, którzy mogą coś wiedzieć na temat zdarzeń biznesowych mogących mieć związek z incydentem.
- Przejrzenie dzienników sieci i zabezpieczeń w celu znalezienia informacji pozwalających na potwierdzenie, że incydent miał miejsce.
- Udokumentowanie informacji zebranych ze wszystkich źródeł.

Śledztwo

Celem śledztwa jest ustalenie faktów dotyczących tego, co się stało, jak do tego doszło oraz w niektórych przypadkach kto jest za to odpowiedzialny. Dla komercyjnego zespołu RI znalezienie sprawcy może być niemożliwe, ale ważne jest, aby wiedzieć, kiedy należy szukać pomocy na zewnątrz i u prawników. Bez znajomości takich faktów jak te, w jaki sposób haker w ogóle uzyskał dostęp do sieci albo co zrobił, mamy małe szanse na skuteczne pozbycie się problemu. Jednym z pomysłów może być po prostu odłączenie komputerów od prądu i zbudowanie zainfekowanego systemu od nowa, ale czy można spać spokojnie, skoro nie wiadomo, jak haker się włamał i co zrobił? Ponieważ bardzo cenimy zdrowy sen, opracowaliśmy i doszlifowaliśmy pięciostopniowy proces przedstawiony na rysunku 2.2., który umożliwia przeprowadzenie skutecznego śledztwa. W następnych podpunktach opisujemy każdy etap tego procesu.

Lepiej nie działać pochopnie

Podczas śledztwa zapewne natkniesz się na znaleziska, które Twoim zdaniem będą wymagały natychmiastowej reakcji. Normalnie zespoły śledcze od razu zgłaszają takie krytyczne odkrycia odpowiednim osobom w zainfekowanej organizacji. Osoby te muszą wówczas rozważyć z jednej strony ryzyko podjęcia czynności bez dostatecznego rozumienia sytuacji, a z drugiej ryzyko prowadzenia dalszych czynności rozpoznawczych. Z naszego doświadczenia wynika, że najczęściej lepszym rozwiązaniem jest bardzo dobre rozpoznanie sytuacji i dopiero wtedy podjęcie odpowiedniej decyzji. Jest to oczywiście ryzykowne, ponieważ dajemy hakerowi możliwość dalszego szkodzenia w systemie. Jednak wiemy też, że działanie bez posiadania kompletnych i dokładnych informacji jest jeszcze bardziej ryzykowne. Krótko mówiąc, każdy przypadek jest inny i decydenci w organizacji muszą samodzielnie podjąć jak najlepszą decyzję.



RYSUNEK 2.2. *Fazy cyklu reakcji na incydent*

Tropy wstępne

Śledztwo bez jakichkolwiek tropów mija się z celem i dlatego zgromadzenie wstępnego materiału ma krytyczne znaczenie dla powodzenia całej operacji. W wielu organizacjach spostrzegliśmy błędną praktykę polegającą na koncentrowaniu się wyłącznie na szukaniu szkodliwego oprogramowania. Jest mało prawdopodobne, aby jedynym celem hakera było zainstalowanie swojego programu. Najczęściej jego zamiary są całkiem inne, np. chce wykraść wiadomości e-mail albo dokumenty, przechwycić hasła, zakłócić działanie sieci lub zmodyfikować dane. Gdy przestępca wejdzie do Twojej sieci i będzie miał poprawne dane poświadczające, nie będzie musiał używać szkodliwego

oprogramowania, aby dostać się do innych systemów. Dlatego koncentrowanie się wyłącznie na obecności programów może sprawić, że umknie coś ważnego.

Pamiętaj, że każde śledztwo powinno skupiać się na badaniu tropów. Niejednokrotnie prowadziliśmy dochodzenia w przypadkach, gdy inne zespoły niewiele wykryły. Przyczyną wielu takich niepowodzeń jest właśnie to, że specjaliści nie skupiają się na szukaniu tropów, tylko na mało znaczących „błyskotkach", które nie przybliżają nikogo do rozwiązania problemu. Wielokrotnie udawało nam się dokonywać ważnych dodatkowych odkryć, takich jak np. utrata dużych ilości danych albo zdarzenia dostępu do poufnych systemów komputerowych. Wystarczyło tylko podążać dobrym tropem.

Często też zapomina się o ewaluacji nowych tropów pod kątem ich przydatności. Dodatkowy czas poświęcony na taką ocenę zwraca się później w postaci lepszego skupienia śledztwa na ważnych sprawach. W naszej pracy wyróżniamy trzy typowe cechy dobrych tropów.

- **Istotność** — trop dotyczy aktualnie badanego incydentu. Może się to wydawać oczywiste, ale często się o tym zapomina. Organizacje zwykle popełniają błąd polegający na kwalifikowaniu wszystkiego, co wydaje się podejrzane, jako rzeczy istotnej we właśnie prowadzonym śledztwie. Ponadto incydenty rzucają nowe światło na środowisko organizacji, ukazując je w całkiem nowym wymiarze i odkrywając wiele „podejrzanych działań", które w rzeczywistości nie są niczym niezwykłym. To powoduje przeciążenie zespołu pracą i utrudnia śledztwo.
- **Szczegółowość** — trop ma cechy określające potencjalny kierunek śledztwa, np. zewnętrzna jednostka może dostarczyć trop wskazujący, że komputer z Twojego środowiska komunikował się z zewnętrzną witryną internetową, na której wykryto szkodliwe oprogramowanie. Choć to miłe z ich strony, że Cię o tym poinformowali, jednak taki trop nie jest zbyt szczegółowy. W takim przypadku należy postarać się o więcej szczegółów. Spytaj o datę i godzinę zdarzenia oraz adres IP — kto, co, kiedy, gdzie, dlaczego i jak. Bez tych szczegółów będziesz tylko marnować czas.
- **Przydatność** — trop zawiera informacje, które można wykorzystać, a Twoja organizacja posiada środki potrzebne do pójścia tym tropem. Wyobraź sobie, że trop wskazuje na transfer dużych ilości danych do zewnętrznej strony internetowej związanej z botnetem. Masz dokładną datę i godzinę oraz docelowy adres IP, ale Twoja organizacja nie dysponuje dziennikami ruchu sieciowego i zapory sieciowej, które są potrzebne do zidentyfikowania wewnętrznego zasobu, z którego wypłynęły dane. W takim przypadku trop jest niezbyt przydatny, ponieważ nie da się powiązać określonej aktywności z konkretnym komputerem w Twojej sieci.

Tworzenie wskaźników zagrożenia

Tworzenie wskaźników zagrożenia (ang. *Indicators of Compromise* — IOC) to proces polegający na dokumentowaniu cech charakterystycznych i artefaktów incydentu w zorganizowany sposób. Dokumentuje się wszystko zarówno z perspektywy hosta, jak i sieci — nie tylko szkodliwe oprogramowanie. Mogą to być takie elementy jak nazwy katalogów roboczych, nazwy plików

wyjściowych, zdarzenia logowania, mechanizmy utrwalania danych, adresy IP, nazwy domenowe, a nawet sygnatury protokołów sieciowych wykorzystywanych przez szkodliwe oprogramowanie. Celem czynności IOC jest opisanie, wyrażenie i znalezienie artefaktów związanych z incydentem. Jako że IOC to tylko definicja, nie obejmuje konkretnego mechanizmu wyszukiwania. Konieczne jest stworzenie lub zakupienie technologii wykorzystującej język IOC.

Ważnym czynnikiem, który należy wziąć pod uwagę przy wybieraniu sposobu reprezentacji wskaźników zagrożenia, jest to, czy danego formatu można używać w organizacji. Sieciowe wskaźniki zagrożenia są najczęściej reprezentowane za pomocą reguł Snort i można znaleźć zarówno darmowe, jak i komercyjne produkty dla przedsiębiorstw do ich obsługi. Z perspektywy hosta niektóre z dostępnych formatów IOC to:

- OpenIOC firmy Mandiant (*www.openioc.org*),
- CybOX firmy Mitre (*cybox.mitre.org*),
- YARA (*code.google.com/p/yara-project*).

Dla dwóch z tych formatów, OpenIOC i YARA, istnieją darmowe narzędzia do tworzenia wskaźników zagrożenia. Firma Mandiant stworzyła narzędzie dla systemu Windows o nazwie IOC Editor, za pomocą którego można tworzyć i modyfikować wskaźniki zagrożenia w standardzie OpenIOC. Dla formatu YARA istnieje kilka narzędzi umożliwiających opracowanie i edytowanie reguł, a nawet automatycznie tworzących reguły na podstawie otrzymanego szkodliwego programu. Cechy dobrych wskaźników zagrożenia i techniki ich tworzenia opisujemy w rozdziale 5.

W INTERNECIE

IOC Editor — *www.mandiant.com/resources/download/ioc-editor*
Narzędzia YARA — *www.deependresearch.org/2013/02/yara-resources.html*

Wdrażanie wskaźników zagrożenia

Dokumentowanie wskaźników zagrożenia za pomocą formatu IOC to doskonały pomysł, ale najwięcej korzyści przynosi umożliwienie zespołowi RI wyszukiwania niepożądanych elementów w sposób automatyczny przy użyciu platformy RI albo za pomocą skryptów Visual Basic (VB) i technologii WMI (ang. *Windows Management Instrumentation*). Powodzenie śledztwa zależy od możliwości szukania wskaźników zagrożenia w całym przedsiębiorstwie i automatycznego ich zgłaszania — to właśnie oznacza w naszym pojęciu „wdrażanie wskaźników zagrożenia". Zatem organizacja musi mieć możliwość implementowania wskaźników zagrożenia albo nie będzie miała z nich żadnego pożytku. Jeśli chodzi o wskaźniki sieciowe, sposób postępowania jest prosty — większość rozwiązań obsługuje reguły Snort. Nie ma natomiast jeszcze powszechnie przyjętego standardu opisywania wskaźników zagrożeń hosta. Z tego powodu korzystanie z takich wskaźników w śledztwie może być trudne. Zobaczmy, jakie są aktualnie możliwości.

Branża a formaty wskaźników zagrożenia

Cała branża bezpieczeństwa komputerowego cierpi z powodu pewnego dotkliwego braku — nie ma powszechnie zaakceptowanego standardu dla hostowych wskaźników zagrożenia. Dla wskaźników sieciowych jako standard traktowany jest Snort, natomiast dla rozwiązań hostowych nie ma darmowego rozwiązania składającego się z języka i narzędzi, które można by było wykorzystać w przedsiębiorstwie. Bez tego specjaliści RI mają utrudnioną pracę, gdy trzeba zdefiniować hostowe wskaźniki zagrożenia.

Gdy pisaliśmy tę książkę, istniały trzy dominujące definicje hostowych wskaźników zagrożeń — OpenIOC firmy Mandiant, CybOX firmy Mitre oraz YARA. Przyjrzymy się każdemu z nich. YARA to dość dobrze ugruntowane język i narzędzie, chociaż w ich centrum zainteresowania leżą głównie szkodliwe programy. Standard OpenIOC firmy Mandiant jest znacznie bardziej rozbudowany i istnieje ogólnodostępne narzędzie o nazwie Redline, z którym można go używać. Standard CybOX też jest rozbudowany, ale nie ma żadnych narzędzi do współpracy z nim oprócz skryptów do konwersji formatu wskaźników zagrożenia. Żaden z tych trzech standardów nie doczekał się jeszcze darmowego narzędzia nadającego się do użycia w przedsiębiorstwach, takiego jak Snort.

Aby korzystać ze wskaźników zagrożenia, nie musisz mieć dużych środków, choć jeśli chcesz ich efektywnie używać w całym przedsiębiorstwie, prawdopodobnie będziesz musiał przeznaczyć na to duże sumy. Istnieją zarówno darmowe, jak płatne narzędzia obsługujące standardy YARA i OpenIOC do szukania wskaźników zagrożenia. Jeśli chodzi o rozwiązania darmowe, to projekt YARA zapewnia narzędzia do wyszukiwania reguł YARA. Ponadto jest kilka otwartych projektów również obsługujących reguły YARA — niektóre z nich są wymienione na podanej wcześniej stronie. Firma Mandiant udostępnia darmowe narzędzie Redline, za pomocą którego można szukać reguł OpenIOC w systemach. Bezpłatne narzędzia są dość skuteczne przy niewielkiej liczbie systemów, ale jakość ich pracy znacznie pogarsza się w większej skali. Aby skutecznie wyszukiwać wskaźniki zagrożeń w przedsiębiorstwie, należy zainwestować w rozwiązanie na dużą skalę. Przykładowo narzędzie FireEye obsługuje reguły YARA, a komercyjne programy Mandiant rozpoznają format OpenIOC. Pamiętaj jednak, że oprogramowanie i procesy obsługujące wskaźniki zagrożenia to wciąż niezbyt ugruntowane narzędzia. Ten aspekt branży zabezpieczeń zapewne jeszcze się zmieni w najbliższych latach, więc miej oczy i uszy otwarte.

Identyfikowanie interesujących systemów

Po wdrożeniu wskaźników zagrożenia zaczniesz otrzymywać tzw. **trafienia** (ang. *hit*). Trafienie to zdarzenie dopasowania przez narzędzie czegoś do reguły IOC. Przed podjęciem jakichkolwiek działań związanych z tym zajściem należy dobrze przyjrzeć się otrzymanym informacjom i upewnić, czy nie jest to fałszywy alarm. Jest to konieczne, ponieważ niektóre trafienia są bardzo ogólne, więc nie dają wysokiego stopnia pewności, a czasami zdarzają się też po prostu fałszywe alarmy. Niekiedy udaje się zdobyć niewielką ilość dodatkowych danych na temat zdarzenia. Jeżeli trafienie nie daje

wysokiego stopnia pewności, nie można od razu stwierdzić, że doszło do incydentu. Aby potwierdzić, że należy zainteresować się systemem, trzeba wykonać kilka czynności.

Podczas identyfikowania systemów należy przeprowadzać wstępną segregację nowych informacji. Postępując zgodnie z poniższymi punktami, będziesz mieć pewność, że więcej czasu poświęcisz na robienie tego, co trzeba, i nie rozproszysz działań śledczych.

- **Weryfikacja** — zbadaj wstępnie informacje o znalezionych elementach i sprawdź, czy są wiarygodne. Jeżeli np. wskaźnik zagrożenia pasuje tylko do nazwy jednego pliku, to czy może to być fałszywy alarm? Czy nowe dane są spójne ze znanymi ramami czasowymi prowadzonego śledztwa?
- **Kategoryzacja** — przyporządkuj zidentyfikowany system do jednej lub większej liczby kategorii ułatwiających prowadzenie śledztwa w uporządkowany sposób. Doświadczenie nauczyło nas, że oznaczenie systemu jako „złamanego" to za mało i powinno się unikać tego określenia. O wiele bardziej pomocne są kategorie, które wskazują na rodzaj odkrytych działań hakera, np. „Zainstalowane tylne drzwi", „Dostęp przy użyciu prawidłowych danych poświadczających", „*SQL Injection*", „Kradzież danych poświadczających do wielu kont" lub „Kradzież danych".
- **Szeregowanie względem ważności** — zidentyfikowanemu systemowi przypisz względny numer w szeregu w odniesieniu do ważności odkrycia. Często stosowanym rozwiązaniem jest szeregowanie na podstawie czynników biznesowych, takich jak główny użytkownik albo typ przetwarzanych informacji. Metoda ta jednak pomija ważną kwestię, a mianowicie nie uwzględnia innych czynników śledczych. Jeżeli np. początkowe szczegóły zidentyfikowanego zagrożenia w systemie zgadzają się z odkryciami z innych systemów, dalsze badanie tego systemu może nie dostarczyć żadnych nowych tropów, więc system ten można oznaczyć jako mniej ważny. Z drugiej strony, jeżeli szczegóły sugerują coś nowego, np. inne tylne drzwi, dobrym pomysłem może być nadanie systemowi wyższego priorytetu do analizy, bez względu na inne czynniki.

Zachowywanie dowodów

Po zidentyfikowaniu systemów i wykryciu aktywnych wskaźników zagrożenia kolejnym krokiem jest zbieranie dodatkowych danych do analizy. Zespół musi opracować plan gromadzenia i zachowywania materiału dowodowego, niezależnie od tego, czy ma to być robione w firmie, czy poza nią. Głównym celem zachowywania dowodów jest wykorzystanie procesu minimalizującego zmiany w systemie i czas interakcji z systemem oraz pozwalającego na utworzenie odpowiedniej dokumentacji. Materiał dowodowy można zbierać w działającym systemie lub wyłączyć system w celu zrobienia jego obrazu.

Jako że każdy zespół ma ograniczone środki, nie ma sensu gromadzić wielkich ilości danych, które nigdy nie zostaną przebadane (chyba że będzie ku temu bardzo dobry powód). Zatem dla każdego nowego systemu, który zostanie zidentyfikowany, należy podjąć decyzję, jakiego rodzaju dowodów szukać. Zawsze bierz pod uwagę kontekst działania każdego systemu, włącznie z tym, czy wyróżnia się on czymś od pozostałych lub czy przegląd danych na żywo przyczynia się do nowych odkryć. Jeśli uważasz, że system ma jakąś wyjątkową cechę albo masz jakiś inny przekonujący powód, zachowaj dowody, które są Twoim zdaniem niezbędne do rozwoju śledztwa.

Do typowych materiałów dowodowych, które należy zachować, zalicza się dane z analizy na żywo działającego systemu, pobieranie zawartości pamięci oraz obrazy dysków na potrzeby śledztwa.

- **Analiza na żywo** — jest to najczęściej stosowana metoda zdobywania dowodów w ramach reakcji na incydent bezpieczeństwa. Polega ona na zgromadzeniu za pomocą automatu standardowego zestawu danych o działającym systemie. Dane te zawierają zarówno ulotne, jak i nieulotne informacje, które dostarczają szybkich odpowiedzi na niektóre pytania śledczych. Typowe dane gromadzone w ten sposób to listy procesów, aktywne połączenia sieciowe, dzienniki zdarzeń, listy obiektów w systemie plików oraz zawartość rejestru. Ponadto możemy zdobyć treść określonych plików, np. dzienników i podejrzanego szkodliwego oprogramowania. Jako że proces przebiega automatycznie, a ilość danych nie jest zbyt duża, analiza na żywo jest wykonywana w większości interesujących systemów. W wyniku tej analizy z reguły udaje się zdobyć dodatkowe dowody na potwierdzenie zagrożenia, dodatkowe informacje na temat tego, co haker zrobił w systemie, oraz tropy, które pozwalają na wyznaczenie dalszego kierunku śledztwa.
- **Pobieranie zawartości pamięci** — technika ta jest najbardziej przydatna w przypadkach, gdy istnieje podejrzenie, że haker wykorzystuje jakiś mechanizm do ukrywania swojej działalności, np. rootkit, i nie można zrobić obrazu dysku. Ponadto badanie pamięci jest potrzebne wtedy, gdy szkodliwa działalność ogranicza się właśnie tylko do pamięci albo pozostawia bardzo mało śladów na dysku. Mimo to, w większości systemów, w których pracujemy, zawartość pamięci nie jest pobierana. Może niektórym wyda się to zaskakujące, ale z naszych doświadczeń wynika, że analiza pamięci daje niewiele korzyści dla śledztwa, ponieważ dostarcza za mało danych, aby można było znaleźć w nich odpowiedzi na ogólniejsze pytania. Może i uda się wykryć działanie szkodliwego programu w systemie, ale raczej nie dowiesz się, skąd się on tam wziął ani co haker robił w systemie.
- **Wykonanie obrazu dysku** — obrazy dysków to kompletne kopie dysków twardych z systemu. W trakcie reakcji na incydent zazwyczaj wykonujemy obrazy „na żywo", tzn. system nie jest wyłączany, podczas gdy tworzony jest jego obraz na zewnętrznym nośniku. Obrazy dysków są bardzo duże i ich analiza może zajmować dużo czasu, więc wykonujemy je wyłącznie wtedy, gdy uważamy, że będzie to korzystne dla śledztwa. Obrazy dysków są przydatne w sytuacjach, gdy haker aktywnie działał w systemie przez długi czas, gdy brakuje odpowiedzi na pewne pytania i inne dowody nie przybliżają nas do nich oraz gdy liczymy na znalezienie dodatkowych informacji, które naszym zdaniem mogą znajdować się tylko na dysku. W przypadku incydentów, w których nie ma podejrzenia włamania, wykonanie pełnego obrazu dysku jest normą.

Analiza danych

Analiza danych to proces polegający na pobraniu materiału dowodowego zachowanego wcześniej i zbadaniu go pod kątem szukania odpowiedzi na pytania postawione w śledztwie. Wyniki tej analizy są zazwyczaj przedstawiane w postaci formalnego raportu. Jest to ten etap cyklu reakcji na incydent, który z reguły zajmuje najwięcej czasu. Twoja organizacja musi wybrać, które ekspertyzy masz wykonać samodzielnie, a które, jeśli w ogóle jakiekolwiek, zlecić do wykonania jednostkom zewnętrznym. Wyróżnia się trzy podstawowe obszary analizy.

- **Analiza szkodliwego oprogramowania** — podczas większości śledztw napotykamy pliki, które podejrzewamy o to, że są szkodliwymi programami. Mamy specjalny zespół ekspertów od szkodliwego oprogramowania, który te pliki bada. Po skończeniu pracy sporządzają raport zawierający wskaźniki zagrożenia i szczegółowy opis funkcjonalności. Choć utrzymywanie specjalnego zespołu ds. szkodliwego oprogramowania przekracza możliwości większości budżetów, organizacje powinny rozważyć możliwość zainwestowania przynajmniej w podstawowe instrumenty segregacji podejrzanych programów.
- **Analiza danych zebranych na żywo** — badanie danych zgromadzonych w działającym systemie to jeden z najważniejszych etapów całego śledztwa. Jeśli przeszukujesz tego typu informacje, znaczy to że w systemie pojawiły się oznaki podejrzanej działalności, ale masz za mało szczegółowych danych. W toku badania postarasz się znaleźć więcej tropów i wyjaśnić, co się stało. Jeśli teraz czegoś nie zauważysz, możesz przeoczyć niektóre działania hakera albo całkowicie wyrzucić system z kręgu swoich zainteresowań. Wyniki analizy na żywo powinny pomóc w określeniu wpływu, jaki nieautoryzowany dostęp wywarł na system, oraz wyznaczeniu dalszego toku postępowania. Każda organizacja zajmująca się bezpieczeństwem IT powinna posiadać podstawowe narzędzia do analizy systemów na żywo.
- **Analiza śledcza** — taka analiza obrazów dysków wykonywana podczas reakcji na incydent jest zadaniem wymagającym skoncentrowania na celu i szybkiego wykonania. Kiedy kule latają, nie ma czasu na metodyczne, dokładne badanie. Zazwyczaj zapisujemy kilka realistycznych pytań, na które chcielibyśmy znać odpowiedzi, wybieramy strategię, która powinna pozwolić nam na znalezienie tych odpowiedzi, a następnie przystępujemy do działania. Jeżeli nie znajdziemy odpowiedzi, możemy spróbować czegoś innego, ale to zależy od tego, ile mamy czasu i co chcemy osiągnąć. Nie twierdzimy, że nie poświęcamy dużo czasu na analizy, tylko że bardzo starannie planujemy czas. Jeśli incydent ma bardziej tradycyjny charakter, np. jest nim wewnętrzne śledztwo niezwiązane z włamaniem, większość czasu spędzisz właśnie na takiej analizie. Analizy tradycyjnych materiałów śledczych powinno się wykonywać bardzo dokładnie, a większość członków zespołów RI i firm nie ma takich doświadczeń.

Podczas analizy włamania pamiętaj, że może nie uda się „znaleźć wszystkich dowodów". Mieliśmy okazję współpracować z organizacjami, które były dotknięte czymś, co nazywamy „efektem CSI", tzn. pracownicy myślą, że są w stanie znaleźć i wyjaśnić wszystko za pomocą „świetnych i drogich narzędzi". W sumie mamy kilkadziesiąt lat doświadczenia w pracy przy setkach śledztw incydentów bezpieczeństwa i jeszcze nie natknęliśmy się na takie magiczne narzędzie. Oczywiście są programy, które mogą bardzo pomóc w pracy. Niektóre najlepsze z możliwych narzędzi już masz — używasz ich teraz po to, by zrozumieć treść tego zdania.

Uwaga

W innych rodzajach dochodzeń stosuje się metodyczne podejście do ekspertyz śledczych. Celem jest zdobycie wszystkich informacji, które potwierdzają lub wykluczają oskarżenia. Jeśli Twój zespół przeprowadza także inne rodzaje dochodzeń, musisz odpowiednio dostosowywać swoje działania i wiedzieć, jak utrzymać umiejętności potrzebne w innych typach śledztw. W tej książce koncentrujemy się na prowadzeniu śledztw związanych z wykrywaniem przypadków naruszenia bezpieczeństwa systemu i naprawianiu szkód w sposób szybki i jednocześnie dokładny w skali przedsiębiorstwa.

Czynności naprawcze

Plany naprawcze mogą być bardzo różne, w zależności od warunków, w jakich doszło do incydentu i jego potencjalnych skutków. Plan powinien uwzględniać czynniki z wszystkich aspektów sytuacji, włącznie z kwestiami prawnymi, biznesowymi, politycznymi i technicznymi. Ponadto plan powinien obejmować protokół komunikacyjny określający, co i kiedy mogą mówić poszczególne osoby z organizacji. W końcu niebagatelne znaczenie ma też czas naprawy. Jeśli zrobi się to zbyt szybko, można pominąć jeszcze nieodkryte nowe informacje. Jeśli zrobi się to za późno, może dojść do poważnych szkód albo haker np. zmieni taktykę. Z naszych doświadczeń wynika, że najlepszym czasem na rozpoczęcie czynności naprawczych jest moment po uciszeniu się stosowanych metod detekcyjnych. Innymi słowy, jest to czas, kiedy narzędzia szukające wskaźników zagrożenia przestaną zgłaszać nowe zdarzenia.

Zalecamy rozpoczynanie tworzenia planu naprawczego jak najwcześniej w procesie reakcji na incydent, tak aby uniknąć przeciążenia zespołu i popełnienia błędów. Likwidacja skutków niektórych incydentów wymaga znacznie więcej wysiłku niż samo śledztwo. W organizacji jest wiele ruchomych części, przez co przeprowadzenie skoordynowanej akcji usuwania zagrożenia jest niełatwym zadaniem. Nasza strategia polega na zdefiniowaniu odpowiednich działań do wykonania dla wymienionych obszarów, takich jak:

- zajęcie pozycji,
- taktyka (krótkoterminowa),
- strategia (długoterminowa).

Zajęcie pozycji polega na podjęciu kroków mających na celu pomoc w zapewnieniu powodzenia akcji naprawczej. Do procesu tego zalicza się ustalenie protokołu, wymianę informacji kontaktowych, określenie zakresu obowiązków, zwiększenie widoczności, zaplanowanie wykorzystania zasobów oraz koordynację czasową. **Taktyka** to podjęcie działań, które są uważane za słuszne w celu rozwiązania bieżącego problemu. Do działań tych mogą zaliczać się: odbudowa zagrożonych systemów, zmiana haseł, blokowanie adresów IP, poinformowanie klientów o zaistniałej sytuacji, rozprowadzenie wewnętrznych lub publicznych ogłoszeń oraz zmiana procesu biznesowego. Poza tym w trakcie trwania śledztwa organizacje zazwyczaj dostrzegają miejsca, które można poprawić. Nie oznacza to jednak, że należy próbować naprawić każdy problem z zabezpieczeniami podczas trwania incydentu. Lepiej utworzyć listę czynności do wykonania i zająć się nimi później. Odpowiednim na to momentem jest etap, który nazywamy **strategią**. Polega on na wprowadzaniu długofalowych udoskonaleń, które mogą wymagać poważnych zmian w organizacji. Choć strategiczna naprawa nie jest elementem typowego cyklu RI, piszemy o niej tutaj, aby zasygnalizować istnienie takiej kategorii, która pomaga skupić się na tym, co w danym czasie jest najważniejsze.

Rejestrowanie istotnych informacji śledczych

Wcześniej napisaliśmy, że wiele z wyzwań, jakie należy pokonać, aby przeprowadzić skuteczne śledztwo w sprawie incydentu bezpieczeństwa, to sprawy nietechniczne. Jedną z nich jest dobra organizacja pracy. To zresztą bardzo szerokie zagadnienie. Nie lubimy określenia „świadomość sytuacji", ale właśnie o tym teraz mówimy. Prowadzący śledztwo musi w jakiś sposób rejestrować krytyczne informacje i mieć możliwość udostępniania ich zespołom pomocniczym i kadrze kierowniczej. Ponadto powinno się wypracować jakiś efektywny model odnoszenia się do określonych incydentów, coś lepszego niż stwierdzenia typu „to, co się stało w zeszły wtorek". Najlepiej ustanowić system numeracji lub nazewnictwa i posługiwać się nim w rozmowach oraz dokumentacji danych i dowodów.

Co to są „istotne informacje śledcze"? Odkryliśmy kilka rodzajów danych, które są krytyczne dla każdego śledztwa. Elementy te najlepiej rejestrować na bieżąco, ponieważ członkowie zespołu będą się nimi posługiwać jako „podstawową prawdą" do opisywania stanu śledztwa. Ponadto od danych tych zespół będzie zaczynał odpowiadać na pytania kadry kierowniczej.

- **Lista zgromadzonych dowodów** — lista ta powinna zawierać datę i godzinę oraz źródło odkrycia — tzn. osobę lub serwer. Skrupulatnie zapisuj informacje dotyczące pochodzenia każdej pozycji. Przechowuj je razem, ponieważ obecność tych zapisków na liście jest znakiem, że dana pozycja została odpowiednio zbadana.
- **Lista dotkniętych systemów** — zapisuj, jak i kiedy dany system został zidentyfikowany. Zauważ, że za „dotknięte" uważa się też systemy podejrzane o problemy z bezpieczeństwem oraz takie, do których ktoś uzyskał dostęp przy użyciu podejrzanego konta.
- **Lista interesujących plików** — na liście tej zazwyczaj figurują tylko szkodliwe programy, ale mogą znaleźć się też pliki z danymi i przechwycone wyniki poleceń. Należy zarejestrować system, na którym został znaleziony taki plik, jak również metadane systemu plików.
- **Lista użytych plików i skradzionych danych** — powinna ona zawierać nazwy plików, ich treść oraz datę ujawnienia.
- **Lista istotnych działań hakera** — podczas analizy systemu na żywo lub danych śledczych można odkryć ślady istotnych działań, np. przypadków logowania lub uruchomienia szkodliwych programów. Zapisz, w którym systemie to miało miejsce oraz datę i godzinę tego zdarzenia.
- **Lista sieciowych wskaźników zagrożenia** — rejestruj adresy IP i nazwy domen.
- **Lista hostowych wskaźników zagrożenia** — rejestruj wszystkie cechy charakterystyczne niezbędne do sformułowania dobrego wskaźnika.
- **Lista kont, na których doszło do włamania** — zbadaj zakres penetracji konta — lokalny czy domenowy.
- **Lista aktualnie wykonywanych i zaplanowanych działań Twoich zespołów** — zazwyczaj podczas prowadzonych śledztw na każdym etapie mamy mnóstwo rzeczy do zrobienia. Musimy dostarczać dodatkowe informacje na prośbę zespołów pomocniczych, wykonywać ekspertyzy itd. Przy braku dobrej organizacji łatwo o czymś zapomnieć.

Zeznania naocznych świadków

Kilka lat temu prowadziliśmy śledztwo w niewielkiej firmie z branży obronnej, która miała sieć około 2000 hostów. Niektóre inne nasze śledztwa prowadziliśmy w środowiskach dochodzących do ponad 100 000 hostów, zatem wydawało się, że to śledztwo będzie łatwe. Zaczęliśmy od zastanowienia się, czy jest w ogóle sens tworzenia kompletnej dokumentacji, zwłaszcza że klient miał mocno ograniczone środki finansowe. Jednak wkrótce odkryliśmy, że w prawie 200 systemach znajduje się szkodliwe oprogramowanie, a w jeszcze większej liczbie systemów ktoś szperał, posługując się poprawnymi danymi poświadczającymi! Niektóre te przypadki były powiązane z prowadzonym przez nas śledztwem, a inne nie. Bez takiej dokumentacji, jaką zazwyczaj prowadzimy, straciliśmy koncentrację i zmarnowaliśmy więcej czasu, niż zabrałoby nam napisanie tej dokumentacji. Wniosek z tego taki, że zawsze należy notować ważne informacje podczas śledztwa, bez względu na jego rozmiar.

Gdy pisaliśmy tę książkę, byliśmy w trakcie przechodzenia ze starego i wypróbowanego arkusza kalkulacyjnego Microsoft Excel z piętnastoma zakładkami na uproszczony interfejs sieciowy obsługujący wielu użytkowników naraz. Postanowiliśmy zbudować własny system, bo nie udało się znaleźć żadnego narzędzia do zarządzania sprawami, które spełniałoby wszystkie nasze oczekiwania. Czekało nas dużo trudnej pracy, ponieważ Excel to bardzo elastyczny i łatwy w obsłudze program, którego funkcjonalność niełatwo odtworzyć w interfejsie internetowym. Bez względu na to, jakie rozwiązanie wybierzesz w swojej organizacji, pamiętaj, że powinno ono jak najlepiej współgrać z Twoimi procesami.

W INTERNECIE

Systemy do zarządzania sprawami
RTIR — *www.bestpractical.com/rtir/*

Raportowanie

Jesteśmy konsultantami, więc nasze raporty są dla klientów podstawowym dokumentem. Sporządzenie dobrego raportu wymaga czasu, który zdaniem niektórych można lepiej spożytkować. Jednak bez raportów łatwo się pogubić w tym, co się już wykonało. Nauczyliśmy się, iż nawet w jednym śledztwie może być tyle odkryć, że przekazanie klientowi wszystkich informacji na raz, bez sporządzania okresowych raportów, może być niemożliwe. Ogólne odkrycia często są dokonywane na podstawie wielu technicznych faktów, których przekazanie bez odpowiedniej dokumentacji może być bardzo trudne.

Ponadto uważamy, że raporty są podstawowym produktem powstającym w toku działalności zespołu RI. Raporty nie tylko zawierają dokumentację wyników podejmowanych działań, ale również pomagają utrzymać koncentrację i prowadzić śledztwo w odpowiedni sposób. Posługujemy się standardowym szablonem oraz stosujemy do wytycznych językowych określających sposób pisania raportów, dzięki czemu efekty naszych prac są spójne. Tworzenie raportu zmusza do zwolnienia pracy, opisania odkryć w standardowym formacie, zweryfikowania materiału dowodowego oraz przemyślenia tego, co się wydarzyło.

Prawie każdy ma jakieś ciekawe doświadczenia z dokumentacją. Jej tworzenie przypomina zastanawianie się nad tym, czy umieścić zadanie na liście czynności do wykonania. Jeśli się tego nie zrobi, istnieje wysokie ryzyko, że się o tym zapomni. Po zakończeniu pisania nawet nie trzeba patrzeć na listę — zna się ją już na pamięć. Z doświadczenia wiemy, że pisanie, czy nieformalnych zapisków, czy oficjalnych raportów, wspomaga zapamiętywanie, co z kolei sprawia, że lepiej wykonujemy swoją pracę.

Kwestiami dotyczącymi metod pisania raportów zajmujemy się szczegółowo w rozdziale 17.

I CO Z TEGO

Przedstawione w tym rozdziale informacje mogą przydać się dyrektorom, którzy chcą skompletować lub unowocześnić zespół reagowania na incydenty. Poniżej znajduje się lista czynności, jakie powinno się wykonać w tym procesie.

- Sformułowanie definicji „incydentu bezpieczeństwa komputerowego” dla swojej organizacji.
- Identyfikacja krytycznych danych oraz miejsc ich przechowywania i osób, które za nie odpowiadają.
- Opracowanie procesu i systemu śledzenia incydentów w celu identyfikowania osobnych incydentów.
- Zbadanie wymogów prawnych i regulacyjnych wobec organizacji i danych, którymi się posługuje.
- Określenie tego, co będzie robione samodzielnie w firmie, a co zostanie zlecone jednostkom zewnętrznym.
- Znalezienie i przeszkolenie zdolnych członków zespołu RI.
- Stworzenie szablonów formalnej dokumentacji na potrzeby procesów reakcji na incydenty.
- Opracowanie procedur przechowywania materiału dowodowego w systemach operacyjnych obecnych w środowisku organizacji.
- Zaimplementowanie sieciowych i hostowych rozwiązań do tworzenia wskaźników zagrożenia i ich wyszukiwania.
- Zdefiniowanie szablonów i wytycznych do pisania raportów.
- Utworzenie mechanizmu lub procesu do rejestrowania istotnych informacji śledczych.

PYTANIA

1. Wymień grupy w organizacji, które mogą być zaangażowane w proces reakcji na incydent. Wyjaśnij, dlaczego należy porozumiewać się z tymi grupami w przypadku wystąpienia incydentu.
2. Twoja organizacja otrzymuje telefon od organu ochrony porządku publicznego z informacją, że istnieje podejrzenie, iż doszło u was do wycieku danych. Przedstawiciel organu podaje kilka szczegółów, m.in. datę i godzinę przepływu poufnych informacji z waszej sieci, docelowy adres IP oraz rodzaj treści. Czy te informacje mają cechy dobrego tropu? Wyjaśnij swoją odpowiedź. O co jeszcze można zapytać? Jak można zamienić te dane w trop do czynnego wykorzystania?
3. Jakie są zalety i wady zbierania materiału dowodowego na działającym systemie w porównaniu z analizowaniem obrazu dysku? Dlaczego analiza na żywo jest najczęściej stosowaną metodą zachowywania dowodów podczas procesów RI?
4. Podczas śledztwa znajdujesz dowody na to, że w systemie działa szkodliwe oprogramowanie. Jak zareagujesz i dlaczego właśnie tak?
5. Wyjaśnij, dlaczego tworzenie i szukanie wskaźników zagrożenia jest krytycznym elementem śledztwa.
6. Kiedy zaczyna się proces naprawy? Wyjaśnij, dlaczego.

Skorowidz

A

B

C

D

E

F

G

H

I

J

K

L

Ł

M

N

O

P

R

S

Ś

T

U

V

W

Z

Ź

Bądź czujny i nie daj się zaskoczyć!

Pomiędzy administratorami systemów informatycznych a cyberprzestępcami trwa ciągły wyścig zbrojeń. Ewoluują zarówno stosowane zabezpieczenia, jak i metody kradzieży — jedne i drugie stają się coraz bardziej wyrafinowane. W grę wchodzą przecież duże pieniądze, prestiż, zaufanie, a bywa, że stawka jest o wiele większa. Praca osoby zajmującej się bezpieczeństwem urządzeń informatycznych wymaga ogromnej wiedzy, zmusza do bezustannej nauki, ciągłej analizy i doskonalenia procedur, a przede wszystkim do konsekwentnego wyciągania wniosków z wykrytych incydentów.

Niniejsza książka jest wyczerpującym podręcznikiem bezpieczeństwa systemów informatycznych, a ściślej rzecz ujmując — procedur reagowania na incydenty bezpieczeństwa. To lektura obowiązkowa zarówno dla osób z najwyższego kierownictwa, jak i dla koordynatorów oraz specjalistów zajmujących się bezpieczeństwem systemów informatycznych. Przedstawiono tu sposoby przygotowania zabezpieczeń, ale także opisano, co należy zrobić (i w jakiej kolejności) w przypadku wykrycia ich naruszeń. Co ważne, ta wiedza jest aktualna i oparta na najlepszych doświadczeniach wybitnych specjalistów.

Przedstawiono tu między innymi:

- zasady budowy infrastruktury umożliwiającej metodyczne reagowanie na incydenty bezpieczeństwa
- metody wykrywania śladów włamań i identyfikacji wskaźników zagrożeń
- sposoby prowadzenia czynności śledczych i analizy danych zgromadzonych w tym procesie
- metodykę analizy szkodliwego kodu
- techniki raportowania procesów reakcji na incydent
- zasady tworzenia i wdrażania kompleksowych planów naprawczych

Jason T. Luttgens, Matthew Pepe i Kevin Mandia — od wielu lat są związani z bezpieczeństwem systemów informatycznych oraz informatyką śledczą. Przeprowadzili wiele śledztw w sprawie szpiegostwa przemysłowego czy kradzieży danych, w tym danych z kart kredytowych; zajmowali się także badaniem i rozwojem metod śledczych, testowaniem sprzętu i oprogramowania. Wszyscy trzej pracowali w instytucjach państwowych (Air Force) i agencjach rządowych (NASA).

sięgnij po WIĘCEJ
KOD KORZYŚCI

Helion
40879 numer katalogowy
księgarnia internetowa
http://helion.pl
zamówienia telefoniczne
0 801 339900
0 601 339900

Sprawdź najnowsze promocje:
http://helion.pl/promocje
Książki najchętniej czytane:
http://helion.pl/bestsellery
Zamów informacje o nowościach:
http://helion.pl/nowosci

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: helion@helion.pl
http://helion.pl

ISBN 978-83-283-1483-2
9 788328 314832

Informatyka w najlepszym wydaniu
cena: 99,00 zł