Podstawy bezpieczeństwa informacji

Praktyczne wprowadzenie

Jason Andress

no starch press

Helion

Tytuł oryginału: Foundations of Information Security: A Straightforward Introduction

Tłumaczenie: Grzegorz Kowalczyk

ISBN: 978-83-283-8342-5

Helion S.A.
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/pobein
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

Spis treści

1

Czym jest bezpieczeństwo informacji?

Obecnie wielu z nas wykorzystuje komputery w codziennej pracy, używa ich w domu do gier, bierze udział w zajęciach szkolnych online, kupuje towary od sprzedawców przez internet, zabiera laptopy do kawiarni, aby przeczytać pocztę elektroniczną, używa smartfonów do sprawdzania stanu konta bankowego i śledzi swój wysiłek fizyczny za pomocą czujników umieszczonych na nadgarstkach. Innymi słowy: komputery są wszechobecne.

Chociaż technologia umożliwia nam dostęp do wielu informacji za pomocą jednego kliknięcia myszką, stwarza również poważne zagrożenie dla naszego bezpieczeństwa. Na przykład jeżeli informacje przechowywane i przetwarzane w systemach Twoich pracodawców lub banków zostaną przejęte przez złośliwych napastników, konsekwencje mogą być naprawdę tragiczne. Może się nagle okazać, że Twoje konto bankowe zostało wyczyszczone, a jego zawartość w środku nocy przeniesiono do banku w jakimś egzotycznym kraju. Twój pracodawca może stracić miliony złotych i stanąć przed sądem, a jego reputacja może poważnie ucierpieć z powodu jakiegoś pozornie błahego błędu w konfiguracji systemu, który to błąd pozwolił atakującemu przełamać zabezpieczenia i uzyskać dostęp do bazy danych zawierającej wrażliwe dane osobowe (ang. *Personally Identifiable Information* — PII) czy tajemnice handlowe firmy. Podobne informacje pojawiają się ostatnio w mediach z niepokojącą regularnością.

Trzydzieści lat temu takich zdarzeń prawie nie było, głównie dlatego, że technologia stała na stosunkowo niskim poziomie i niewiele osób z niej korzystało.

Chociaż zmienia się to w coraz szybszym tempie, wiele popularnych teorii dotyczących zachowania bezpieczeństwa nadal pozostaje daleko w tyle. Jeżeli jednak dobrze poznasz podstawowe zagadnienia związane z bezpieczeństwem informacji, będziesz miał wystarczającą wiedzę, aby poradzić sobie z nadchodzącymi zmianami.

W tym rozdziale omówię niektóre podstawowe pojęcia związane z bezpieczeństwem informacji, w tym modele bezpieczeństwa, rodzaje ataków, zagrożenia, luki w zabezpieczeniach i związane z nimi ryzyko. Zagłębię się również w nieco bardziej złożone koncepcje, omawiając dokładnie zarządzanie ryzykiem, reagowanie na incydenty bezpieczeństwa i obronę przed zagrożeniami.

Definicja bezpieczeństwa informacji

Ogólnie mówiąc, *bezpieczeństwo* oznacza ochronę Twoich zasobów przed napastnikami atakującymi sieci komputerowe, klęskami żywiołowymi, wandalizmem, utratą czy nadużyciem. W zasadzie powinieneś podjąć próbę zabezpieczenia się przed najbardziej prawdopodobnymi formami ataku i w najlepszym możliwym zakresie, biorąc pod uwagę środowisko, w którym się znajdujesz.

W praktyce możesz posiadać bardzo szeroki zakres potencjalnych aktywów, które chcesz zabezpieczyć. Mogą to być przedmioty o dużej wartości, takie jak biżuteria czy sztabki złota, lub po prostu urządzenia, które mają wartość dla Twojej firmy, takie jak sprzęt komputerowy. Mogą to być również zasoby o nieco bardziej eterycznej naturze, takie jak oprogramowanie, kody źródłowe lub dane.

W dzisiejszych środowiskach komputerowych zasoby logiczne (czyli zasoby, które istnieją jako dane lub własność intelektualna) są co najmniej tak samo cenne jak zasoby fizyczne (czyli takie, które mają postać przedmiotów materialnych), jeżeli nie bardziej wartościowe. W tym właśnie miejscu pojawiają się zagadnienia związane z bezpieczeństwem informacji.

Zgodnie z prawem w wielu krajach **bezpieczeństwo informacji** definiujemy jako „ochronę informacji i systemów informatycznych przed nieautoryzowanym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem, modyfikacją lub zniszczeniem". Innymi słowy: musimy chronić nasze dane i systemy przed osobami, które chcą ich nadużywać, celowo lub nieumyślnie, a także przed tymi, które w ogóle nie powinny mieć do nich dostępu.

Kiedy jesteś bezpieczny?

Profesor Eugene Spafford powiedział kiedyś: „Jedyny naprawdę bezpieczny system to taki, który jest odłączony od zasilania, zalany w bloku betonu i zamknięty w wyłożonym ołowiem pokoju patrolowanym przez uzbrojonych strażników — ale nawet w takiej sytuacji mam pewne wątpliwości"[1]. Choć tak zabezpieczony system z pewnością będzie względnie bezpieczny, zupełnie nie będzie się nadawał do użytku ani nie będzie produktywny. Innymi słowy: zwiększając poziom bezpieczeństwa systemu, zwykle obniżasz poziom jego produktywności.

Ponadto zabezpieczając zasoby systemu lub środowiska, należy rozważyć, jak planowany poziom zabezpieczeń ma się do wartości zabezpieczanego elementu. Jeżeli jesteś gotów pogodzić się ze spadkiem wydajności, możesz zaimplementować bardzo wysoki poziom bezpieczeństwa dla każdego chronionego zasobu. W teorii mógłbyś zbudować wart miliard dolarów obiekt otoczony ogrodzeniem z drutu kolczastego, patrolowany przez uzbrojonych po zęby strażników oraz bezwzględne, znakomicie wyszkolone psy bojowe i wyposażony w hermetycznie zamknięty skarbiec, w którym umieścisz przepis na czekoladowe ciasteczka Twojej mamy, ale to byłaby chyba lekka przesada. Koszt wprowadzanych zabezpieczeń nigdy nie powinien przewyższać wartości tego, co one chronią.

Jednak w niektórych sytuacjach nawet takie imponujące środki bezpieczeństwa mogą się okazać niewystarczające. W każdym środowisku, w którym planowane jest wprowadzenie podwyższonych poziomów bezpieczeństwa, należy również wziąć pod uwagę potencjalny koszt zastąpienia zasobów w przypadku ich utraty i upewnić się, że poziom ochrony został dobrany adekwatnie do ich wartości.

Określenie dokładnego punktu, w którym można uznać, że dane środowisko jest bezpieczne, stanowi pewne wyzwanie. Czy jesteś bezpieczny, jeżeli Twoje systemy są odpowiednio i na czas aktualizowane? Czy jesteś bezpieczny, jeżeli używasz silnych haseł? Czy jesteś bezpieczny, jeżeli jesteś całkowicie odłączony od internetu? Z mojego punktu widzenia odpowiedź na te wszystkie pytania brzmi: nie. Żadna pojedyncza czynność lub działanie nie zapewni Ci bezpieczeństwa w każdej sytuacji.

Dzieje się tak dlatego, że nawet jeżeli Twoje systemy są na bieżąco aktualizowane, zawsze mogą pojawić się nowe ataki, na które Twoje środowisko będzie podatne. Gdy używasz silnych haseł, atakujący wykorzysta inną drogę. Gdy jesteś odłączony od internetu, napastnik nadal może fizycznie uzyskać dostęp do Twoich systemów lub je ukraść. Krótko mówiąc: trudno zdefiniować, kiedy jesteś naprawdę bezpieczny. Z drugiej strony, zdefiniowanie okoliczności, kiedy nie jesteś zabezpieczony, jest znacznie łatwiejsze. Oto kilka przykładów, które mogą postawić Cię w takiej sytuacji:

- Nieinstalowanie lub instalowanie z opóźnieniem poprawek bezpieczeństwa i aktualizacji aplikacji oraz systemów operacyjnych.
- Używanie słabych haseł, takich jak *password* czy *1234*.
- Pobieranie programów z internetu.
- Otwieranie załączników poczty elektronicznej pochodzących od nieznanych nadawców.
- Używanie sieci bezprzewodowych bez odpowiedniego szyfrowania.

Taką listę można by kontynuować jeszcze przez długi czas, ciągle dodając do niej nowe elementy. Dobrą rzeczą jest to, że po zidentyfikowaniu w środowisku obszarów, które mogą uczynić je podatnym na ataki, możemy podjąć kroki w celu usunięcia tych problemów. Przypomina to sytuację, w której dzielimy jakiś przedmiot na pół, potem otrzymane połówki znów dzielimy na pół itd. Niezależnie od tego, jak wiele podziałów uda nam się zrobić, zawsze pozostanie jakaś mała

część, którą można ponownie przeciąć na pół. Chodzi zatem o to, że choć nigdy nie uda się osiągnąć stanu, który można będzie definitywnie określić „całkowitym bezpieczeństwem", zawsze powinniśmy podejmować działania zmierzające we właściwym kierunku.

TO PRAWO JEST TWOIM PRAWEM...

Przepisy prawne, które definiują standardy bezpieczeństwa, różnią się znacznie w zależności od branży i kraju. Przykładem jest różnica w przepisach dotyczących prywatności danych pomiędzy Stanami Zjednoczonymi a Unią Europejską. Organizacje, które działają globalnie, muszą zadbać o to, aby nie naruszać żadnego z tych praw podczas prowadzenia działalności. W razie wątpliwości przed podjęciem działań należy skonsultować się z radcą prawnym.

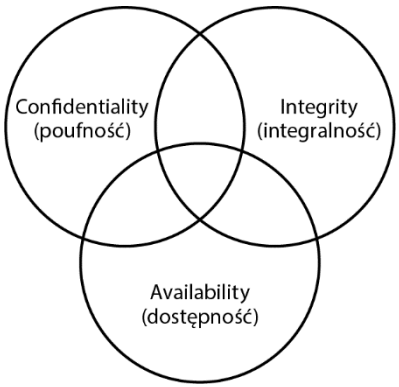
Niektóre instytucje prawne i regulacje próbują zdefiniować, co oznacza bezpieczeństwo lub przynajmniej jakie kroki należy podjąć, aby być „wystarczająco bezpiecznym". Standard bezpieczeństwa danych w branży kart płatniczych (ang. *Payment Card Industry Data Security Standard* — PCI DSS) ma zastosowanie do firm, które przetwarzają płatności kartami kredytowymi. W Stanach Zjednoczonych HIPAA (ang. *Health Insurance Portability and Accountability Act*), czyli ustawa o przenoszeniu i odpowiedzialności za ubezpieczenia zdrowotne, podpisana w 1996 r., dotyczy organizacji, które zajmują się opieką zdrowotną i dokumentacją pacjentów. Z kolei PN-EN ISO/IEC 27001:2017 to międzynarodowa norma standaryzująca wytyczne w zakresie zarządzania bezpieczeństwem informacji, której celem jest dostarczenie wymagań dotyczących ustanowienia, wdrożenia, utrzymania i ciągłego doskonalenia systemu pozwalającego na zachowanie bezpieczeństwa informacji w różnych organizacjach. Istnieje całe mnóstwo takich ustaw, rozporządzeń i standardów. To, czy są one skuteczne, jest zapewne dyskusyjne, ale przestrzeganie standardów bezpieczeństwa zdefiniowanych dla branży, w której działasz, jest mocno zalecane, a w wielu przypadkach wręcz obowiązkowe.

Modele dyskusji nad kwestiami bezpieczeństwa

Podczas omawiania zagadnień związanych z bezpieczeństwem często pomocne jest posiadanie modelu, który można wykorzystać jako podstawę lub punkt odniesienia. Takie rozwiązanie zapewnia spójny zestaw terminologii i koncepcji, do których my, jako specjaliści ds. bezpieczeństwa, możemy się później odwoływać.

Triada poufności, integralności i dostępności

Trzy podstawowe atrybuty zapewniające bezpieczeństwo informacji to *poufność*, *integralność* i *dostępność*, powszechnie określane jako *triada PID* lub *triada CIA* (od ang. *Confidentiality, Integrity and Availability*), jak pokazano na rysunku 1.1.



Rysunek 1.1. Triada CIA

Triada CIA to model znakomicie ułatwiający myślenie i dyskutowanie o koncepcjach bezpieczeństwa. Czasami jej nazwa jest również zapisywana jako *triada CAI* (ang. *Confidentiality, Availability and Integrity*) lub wyrażana w formie negatywnej jako tzw. *triada DAD* (ang. *Disclosure, Alteration and Denial* — ujawnianie, zmiana i odmowa).

Poufność

Poufność (ang. *Confidentiality*) odnosi się do Twojej zdolności do ochrony danych przed osobami, które nie są upoważnione do ich przeglądania. Poufność możesz wdrożyć na wielu poziomach całego procesu.

Wyobraźmy sobie osobę, która wypłaca pieniądze z bankomatu. Osoba ta prawdopodobnie będzie dążyła do zachowania poufności swojego numeru PIN, który pozwala jej na pobranie pieniędzy z bankomatu przy użyciu odpowiedniej karty. Dodatkowo właściciel bankomatu zachowuje w tajemnicy numer konta, wysokość salda i wszelkie inne informacje potrzebne do przekazania bankowi, z którego pobierane są środki pieniężne. Bank również zachowuje poufność transakcji bankomatowej oraz informacje o zmianie salda na koncie po wypłacie pieniędzy.

Poufność może zostać naruszona na wiele sposobów. Na przykład możesz zgubić laptopa zawierającego wrażliwe dane. Jakaś osoba może zaglądać Ci przez ramię, gdy wprowadzasz hasło. Pisząc e-maila, możesz przez pomyłkę wysłać załącznik z poufnymi informacjami do niewłaściwej osoby lub po prostu zdolny, zdeterminowany napastnik może przeniknąć do Twojego systemu i uzyskać dostęp do wrażliwych informacji. A to tylko kilka sposobów.

Integralność

Integralność (ang. *Integrity*) to zdolność do zapobiegania zmianom danych w nieuprawniony lub niepożądany sposób. Aby zachować integralność, nie tylko potrzebujesz środków zapobiegających nieautoryzowanym zmianom danych, ale także musisz mieć możliwość cofnięcia niechcianych, autoryzowanych zmian.

Dobrym przykładem mechanizmów, które pozwalają kontrolować integralność, są systemy plików wielu nowoczesnych systemów operacyjnych, takich jak Windows i Linux. W celu zapobiegania nieautoryzowanym zmianom w takich systemach zaimplementowane są odpowiednie mechanizmy uprawnień, które ograniczają działania, jakie nieautoryzowany użytkownik może wykonać na danym pliku. Na przykład właściciel pliku może mieć uprawnienia do odczytu i zapisu, podczas gdy inni użytkownicy mogą mieć uprawnienia tylko do odczytu pliku lub w ogóle mogą nie mieć do niego dostępu. Dodatkowo niektóre systemy tego typu i inne aplikacje, takie jak bazy danych, pozwalają na odwracanie czy wycofanie niepożądanych zmian.

Integralność jest szczególnie ważna, gdy dotyczy danych, które stanowią podstawę podejmowania ważnych decyzji. Na przykład gdyby napastnik zmienił dane zawierające wyniki badań medycznych, lekarz mógłby zaordynować niewłaściwe leczenie, co mogłoby doprowadzić do śmierci pacjenta.

Dostępność

Ostatnim atrybutem triady CIA jest **dostępność** (ang. *Availability*). Dostępność oznacza możliwość dostępu do Twoich danych, gdy ich potrzebujesz. Dostępność można utracić np. z powodu awarii zasilania, problemów z systemem operacyjnym lub z aplikacjami, ataków sieciowych czy naruszenia bezpieczeństwa systemu. Kiedy takie problemy są spowodowane przez osobę z zewnątrz, np. złośliwego napastnika, zazwyczaj nazywamy to atakiem typu *odmowa usługi* (ang. *Denial of Service* — DoS).

Jak triada CIA odnosi się do bezpieczeństwa?

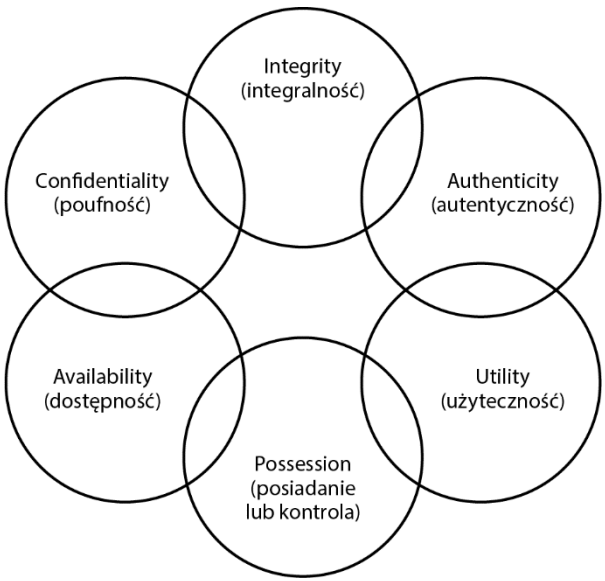
Biorąc pod uwagę atrybuty triady CIA, można zacząć omawiać kwestie bezpieczeństwa bardziej szczegółowo, niż byłoby to możliwe w innym przypadku. Rozważmy przesyłkę taśm z kopiami zapasowymi, na których przechowujesz jedyne istniejące, niezaszyfrowane kopie pewnych wrażliwych danych.

Gdyby taka przesyłka zaginęła podczas transportu, zdarzenie to powinno zostać zakwalifikowane jako incydent bezpieczeństwa. Może on oznaczać naruszenie poufności, ponieważ pliki danych nie były zaszyfrowane. Brak szyfrowania może również powodować problemy z integralnością. Jeżeli kiedyś odzyskasz zagubione taśmy, nie będziesz miał pewności, czy potencjalny napastnik nie zmienił zawartości niezaszyfrowanych plików, ponieważ nie będzie dobrego sposobu na zweryfikowanie danych. Jeżeli chodzi o dostępność danych, również będziesz miał poważny problem, ponieważ nie istnieją inne kopie zapasowe plików (no chyba, że taśmy zostaną odzyskane).

Chociaż sytuację w tym przykładzie można opisać ze względną dokładnością za pomocą triady CIA, może się okazać, że model ten jest zbyt ograniczony, aby sprawdzić się w innych, złożonych scenariuszach. Dla takich przypadków istnieje bardziej rozbudowany model, nazywany heksadą Parkera.

Heksada Parkera

Heksada Parkera to mniej znany model, nazwany na cześć Donna Parkera i przedstawiony w jego książce *Fighting Computer Crime*, który stanowi nieco bardziej złożoną odmianę klasycznej triady CIA. Podczas gdy triada CIA zbudowana jest na poufności, integralności i dostępności, w skład heksady Parkera oprócz tych trzech podstawowych elementów wchodzą również: posiadanie lub sprawowanie kontroli (ang. *Possesion*), autentyczność (ang. *Authenticity*) i użyteczność[2] (ang. *Utility*), co daje w sumie sześć atrybutów, jak pokazano na rysunku 1.2.



Rysunek 1.2. Heksada Parkera

Poufność, integralność i dostępność

Jak już wspominałem, heksada Parkera obejmuje wszystkie trzy elementy składowe triady CIA, zdefiniowane tak samo, jak przed chwilą omówiłem. Parker opisuje jednak integralność w nieco inny sposób — nie uwzględnia autoryzowanych, ale niepoprawnych modyfikacji danych. Z jego punktu widzenia dane muszą być kompletne i niezmienione w stosunku do poprzedniego stanu.

Posiadanie lub sprawowanie kontroli

W heksadzie Parkera *posiadanie lub sprawowanie kontroli* (ang. *possession or control*) odnosi się do fizycznego dysponowania nośnikiem, na którym przechowywane są dane. Pozwala to na opisanie utraty danych przechowywanych na danym fizycznym nośniku bez angażowania innych czynników, takich jak dostępność. Wróćmy zatem na chwilę do przykładu utraconej przesyłki z taśmami zawierającymi kopie zapasowe danych i załóżmy, że niektóre z nich były zaszyfrowane,

a inne nie. W takiej sytuacji atrybut posiadania umożliwia bardziej precyzyjne opisanie zakresu incydentu, ponieważ utrata zaszyfrowanych taśm powoduje problem z posiadaniem, ale nie zagraża poufności, natomiast taśmy niezaszyfrowane powodują problem w dziedzinie każdego z tych atrybutów.

Autentyczność

Atrybut *autentyczności* pozwala stwierdzić, czy dane zostały przypisane do odpowiedniego właściciela lub twórcy. Na przykład jeżeli wysyłasz wiadomość e-mail, która została zmieniona w taki sposób, że wydaje się pochodzić z innego adresu e-mailowego niż ten, z którego została faktycznie wysłana, naruszasz autentyczność tej wiadomości. Autentyczność może być egzekwowana za pomocą podpisów cyfrowych, które omówię w rozdziale 5.

Podobną, ale odwróconą koncepcją jest *niezaprzeczalność* (ang. *non-repudiation*), która zapobiega podejmowaniu przez ludzi działań takich jak wysłanie wiadomości e-mail, a następnie zaprzeczanie, że to zrobili. O atrybucie niepodważalności szerzej piszę również w rozdziale 4.

Użyteczność

Atrybut *użyteczności* (ang. *utility*) odnosi się do tego, w jaki sposób dane są użyteczne dla użytkownika. Użyteczność to jedyny atrybut heksady Parkera, który niekoniecznie ma charakter binarny, ponieważ w zależności od danych i ich formatu mogą istnieć różne stopnie ich użyteczności. Jest to nieco abstrakcyjna koncepcja, ale okazuje się zaskakująco przydatna przy omawianiu pewnych sytuacji w kontekście bezpieczeństwa.

Aby to zilustrować, powróćmy jeszcze raz do przykładu z transportem taśm zawierających kopie zapasowe danych i ponownie wyobraźmy sobie, że niektóre z nich były zaszyfrowane, a inne nie. Dla napastnika lub innej niepowołanej osoby zaszyfrowane taśmy będą prawdopodobnie bardzo mało użyteczne, bo po prostu odczytanie danych nie będzie możliwe. Z kolei taśmy niezaszyfrowane będą dla nich znacznie bardziej użyteczne, ponieważ napastnik lub inna nieupoważniona osoba będą mogli bez żadnych problemów uzyskać dostęp do danych.

Koncepcje zawarte w triadzie CIA i heksadzie Parkera stanowią praktyczną podstawę do omówienia wszystkich scenariuszy, w których coś poszło nie tak, jak powinno, w świecie bezpieczeństwa informacji. Oba modele pozwalają na lepsze opisywanie ataków, z którymi możesz się spotkać, oraz mechanizmów zabezpieczających, jakie należy wdrożyć, aby takim atakom zapobiegać.

Ataki

Ataki mogą być przeprowadzane na wiele różnych sposobów i na wielu różnych płaszczyznach. Można je podzielić ze względu na *rodzaj* ataku, *ryzyko*, jakie ze sobą niesie, oraz *mechanizmy zabezpieczające*, które wdraża się w celu ich ograniczenia.

Rodzaje ataków

Ataki można ogólnie podzielić na cztery kategorie: przechwycenie (ang. *interception*), przerywanie (ang. *interruption*), modyfikowanie (ang. *modification*) i podrabianie (ang. *fabrication*). Każda z tych kategorii może mieć wpływ na jeden lub więcej atrybutów triady CIA, jak pokazano na rysunku 1.3.

Rysunek 1.3. Triada CIA i kategorie ataków

Granica między kategoriami ataków a ich skutkami jest nieco rozmyta. W zależności od danego ataku można zaliczyć go do więcej niż jednej kategorii i może on wywołać skutki więcej niż jednego rodzaju.

Przechwytywanie

Ataki przechwytujące umożliwiają nieautoryzowanym użytkownikom dostęp do danych, aplikacji lub środowiska celu i są przede wszystkim atakami przeciwko poufności. Przechwytywanie może przybrać formę nieautoryzowanego przeglądania lub kopiowania plików, podsłuchiwania rozmów telefonicznych lub czytania cudzych wiadomości e-mail, a można je przeprowadzić na dane znajdujące się w stanie spoczynku lub w tranzycie (pojęcia te zostały wyjaśnione w ramce „Dane w spoczynku i w tranzycie"). Prawidłowo przeprowadzone ataki przechwytujące mogą być bardzo trudne do wykrycia.

DANE W SPOCZYNKU I W TRANZYCIE

W tej książce wielokrotnie pojawia się określenie, że dane są albo „w spoczynku", albo „w tranzycie", więc porozmawiajmy o tym, co to oznacza. *Dane w spoczynku* (ang. *data at rest*) to dane przechowywane, które nie są w trakcie przenoszenia z jednego miejsca na drugie. Mogą się one znajdować na dysku twardym czy w pamięci flash lub mogą być przechowywane np. w bazie danych. Tego typu dane są zazwyczaj chronione za pomocą jakiegoś rodzaju szyfrowania, często na poziomie pliku lub nawet całego urządzenia pamięci masowej.

Dane w ruchu (ang. *data in motion*), określane również jako *dane w tranzycie* albo *dane w locie*, to dane, które przemieszczają się z jednego miejsca do drugiego. Gdy korzystasz z bankowości internetowej, wrażliwe dane przesyłane między przeglądarką internetową a bankiem są danymi w ruchu. Dane w ruchu również są chronione za pomocą szyfrowania, ale w tym przypadku szyfrowanie chroni protokół sieciowy lub ścieżkę używaną do przenoszenia danych z jednego miejsca do drugiego.

W niektórych opracowaniach można się spotkać z trzecim stanem danych, opisywanym jako *dane w użyciu* (ang. *data in use*). Dane w użyciu to dane, do których aplikacja lub osoba fizyczna miała aktywny dostęp lub które modyfikowała. Ochrona danych w użyciu może obejmować odpowiednie uprawnienia i uwierzytelnianie użytkowników. W praktyce pojęcie danych w użyciu jest bardzo często mylone z pojęciem danych w ruchu, ale zarówno przeciwnicy, jak i zwolennicy takiego podziału przedstawiają wiele konkretnych argumentów na poparcie tego, czy powinno się traktować ten rodzaj danych jako odrębną kategorię, czy też nie.

Przerywanie

Ataki przerywające czy też zakłócające działanie sprawiają, że Twoje zasoby mogą się stać tymczasowo lub na stałe bezużyteczne lub niedostępne. Ataki takie wpływają przede wszystkim na dostępność, ale mogą również wpływać na integralność. Na przykład atak typu DoS na serwer pocztowy możemy sklasyfikować jako atak na dostępność.

Z drugiej strony, jeżeli napastnik manipulował procesami odpowiedzialnymi za funkcjonowanie bazy danych, aby uniemożliwić dostęp do zawartych w niej danych, to ze względu na możliwą utratę lub uszkodzenie danych możemy równie dobrze uznać to za atak na integralność albo za kombinację tych dwóch czynników. W zasadzie można nawet uznać taki atak na bazę danych za atak modyfikujący, a nie atak przerywający, o czym przekonasz się już za chwilę.

Modyfikacja

Ataki modyfikujące polegają na manipulowaniu zasobami. Takie ataki mogą być przede wszystkim uważane za ataki na integralność, ale mogą również zostać sklasyfikowane jako ataki na dostępność. Jeżeli napastnik uzyska dostęp do pliku w nieautoryzowany sposób i zmieni zawarte w nim dane, narusza to integralność danych zawartych w pliku. Jeżeli jednak plik, o którym mowa, jest plikiem konfiguracyjnym, który zarządza zachowaniem usługi — np. serwera WWW — to zmiana zawartości pliku może wpłynąć na dostępność tej usługi. Co więcej, jeżeli zmiana ustawień w pliku konfiguracyjnym serwera WWW spowoduje zmianę sposobu, w jaki serwer obsługuje połączenia szyfrowane, wówczas możemy to nawet nazwać atakiem na poufność.

Podrabianie

Ataki z podrabianiem polegają na generowaniu danych, procesów, komunikacji lub innych podobnych elementów systemu. Podobnie jak dwa ostatnie typy ataków, ataki z podrabianiem wpływają przede wszystkim na integralność, ale mogą również wpływać na dostępność. Na przykład generowanie fałszywych informacji w bazie danych możemy zaklasyfikować jako atak z podrabianiem. W takich atakach bardzo często wykorzystywane będą również wiadomości rozsyłane za pomocą poczty elektronicznej, które są popularną metodą rozprzestrzeniania złośliwego oprogramowania. Jeżeli napastnik wygeneruje wystarczająco dużo dodatkowych procesów, ruchu sieciowego, wiadomości poczty elektronicznej lub czegokolwiek innego, co zużywa zasoby, może przeprowadzić atak na dostępność, sprawiając, że usługa obsługująca taki ruch stanie się niedostępna dla swoich prawowitych użytkowników.

Zagrożenia, podatności i ryzyko

Aby bardziej szczegółowo pisać o różnych atakach, muszę wprowadzić kilka nowych terminów. Kiedy z pewnego dystansu spojrzymy na to, jak atak może na nas wpłynąć, możemy mówić o nim w kategoriach zagrożeń, podatności i związanego z nimi ryzyka.

Zagrożenia

Kiedy wcześniej w tym rozdziale pisałem o typach ataków, z jakimi możemy się spotykać, omówiłem kilka rodzajów ataków, które mogą wyrządzić mniejsze lub większe szkody zasobom — np. ataki z nieautoryzowaną modyfikacją danych. Można zatem powiedzieć, że zagrożenie to coś, co ma potencjał wyrządzenia szkody. Zagrożenia są zwykle specyficzne dla określonych środowisk, zwłaszcza w świecie bezpieczeństwa informacji. Na przykład choć dany wirus może sprawiać ogromne kłopoty w systemie Windows, zwykle nie będzie miał żadnego wpływu na funkcjonowanie komputerów z systemem Linux.

Podatności

Podatności to słabe punkty lub luki w zabezpieczeniach, które mogą być wykorzystane przez napastnika do wyrządzenia szkody. Podatności mogą dotyczyć konkretnego systemu operacyjnego lub aplikacji, z której korzystasz, fizycznej lokalizacji budynku biurowego, centrum danych, które jest przepełnione serwerami i wytwarza więcej ciepła, niż jest w stanie wytrzymać system klimatyzacji, braku zapasowych generatorów lub innych czynników.

Ryzyko

Ryzyko to prawdopodobieństwo, że wydarzy się coś złego. Aby w danym środowisku istniało ryzyko, musi pojawić się w nim zarówno zagrożenie, jak i podatność, którą takie zagrożenie może wykorzystać. Na przykład jeżeli mamy konstrukcję wykonaną z drewna i w jej pobliżu rozpalimy ogień, istnieje zarówno zagrożenie

(pożar), jak i odpowiadająca mu podatność (konstrukcja z drewna) — w takim przypadku zdecydowanie mamy do czynienia z ryzykiem.

Natomiast jeżeli istnieje takie samo zagrożenie pożarem, ale konstrukcja jest wykonana z betonu, nie ma już istotnego ryzyka, ponieważ zagrożenie nie ma podatności, którą mogłoby wykorzystać. Co prawda można argumentować, że wystarczająco gorący płomień potrafi uszkodzić również beton, ale takie zdarzenie jest znacznie mniej prawdopodobne.

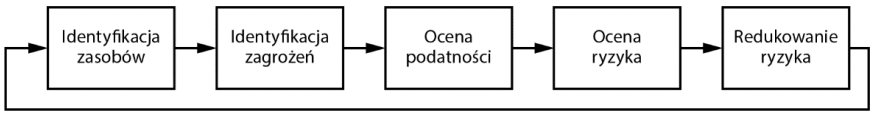
Często mówimy również o potencjalnych, ale mało prawdopodobnych atakach w środowiskach komputerowych. Najlepszą strategią jest zatem ukierunkowanie wysiłków na zapobieganie najbardziej prawdopodobnym atakom. Jeżeli będziemy zużywać cenne zasoby na próby zapobiegania wszystkim możliwym rodzajom ataków, nawet tym bardzo mało prawdopodobnym, niepotrzebnie rozproszymy siły i z pewnością zabraknie nam ochrony tam, gdzie jest ona najbardziej potrzebna.

Oddziaływanie

Niektóre organizacje, takie jak amerykańska Agencja Bezpieczeństwa Narodowego (ang. *National Security Agency* — NSA), dodają do triady *zagrożenie – podatność – ryzyko* jeszcze jeden czynnik, nazywany *oddziaływaniem* (ang. *impact*). Oddziaływanie uwzględnia wartość zagrożonego zasobu i wykorzystuje ją do kalkulacji ryzyka. W naszym przykładzie z taśmami zapasowymi, jeżeli weźmiemy pod uwagę fakt, że niezaszyfrowane taśmy zawierały tylko kolekcję przepisów na ciasteczka z czekoladą, możemy w rzeczywistości nie mieć do czynienia z ryzykiem, ponieważ ujawnione dane nie zawierają niczego wrażliwego i zawsze można wykonać dodatkowe kopie zapasowe danych źródłowych. W tym konkretnym przypadku możemy zatem bezpiecznie powiedzieć, że nie stanowi to dla nas ryzyka.

Zarządzanie ryzykiem

Odpowiednie procesy zarządzania ryzykiem pozwalają na skompensowanie zagrożeń występujących w danym środowisku. Rysunek 1.4 przedstawia typowy proces zarządzania ryzykiem na wysokim poziomie.



Rysunek 1.4. Etapy procesu zarządzania ryzykiem

Jak widać, w procesie zarządzania ryzykiem należy zidentyfikować ważne zasoby, określić potencjalne zagrożenia, określić słabe punkty i podatności, a następnie podjąć kroki w celu zredukowania ryzyka.

Identyfikacja zasobów

Jednym z pierwszych i prawdopodobnie najważniejszych etapów procesu zarządzania ryzykiem jest inwentaryzacja chronionych zasobów. Jeżeli nie potrafisz wymienić swoich zasobów i ocenić znaczenia każdego z nich, ich ochrona może stać się naprawdę trudnym wyzwaniem.

Może to być bardziej złożony problem, niż mogłoby się na pierwszy rzut oka wydawać, szczególnie w większych przedsiębiorstwach. W wielu przypadkach dana firma czy organizacja posiada wiele różnych generacji sprzętu, zasoby pochodzące z przejęcia innych firm, znajdujące się w mało oczywistych i często nieco zapomnianych miejscach, czy dziesiątki albo i setki niezbyt dokładnie opisanych maszyn wirtualnych i serwerów, a każdy z nich może być krytyczny dla dalszego funkcjonowania firmy.

Po zidentyfikowaniu wykorzystywanych zasobów kolejnym etapem działania jest określenie, które z nich są krytycznymi zasobami biznesowymi, a to już zupełnie inna kwestia. Dokładne określenie, które zasoby mają krytyczne znaczenie dla działania firmy, będzie generalnie wymagało uwzględnienia szczegółowych informacji od użytkowników, którzy korzystają z tych zasobów, podmiotów, które zajmują się ich obsługą i wsparciem technicznym, a także od innych potencjalnie zaangażowanych stron.

Identyfikacja zagrożeń

Po zidentyfikowaniu krytycznych zasobów można przystąpić do identyfikacji zagrożeń, które mogą mieć na nie wpływ. Dużym ułatwieniem w realizacji tego zadania jest posłużenie się określonym modelem pozwalającym na precyzyjne omówienie natury danego zagrożenia — triada CIA lub heksada Parkera, omówione wcześniej w tym rozdziale, sprawdzą się tutaj znakomicie.

Spróbujmy zastosować heksadę Parkera do przeanalizowania zagrożeń, na jakie może być narażona aplikacja przetwarzająca płatności kartami kredytowymi.

- **Poufność** — jeżeli dane o transakcjach zostaną ujawnione podmiotom do tego nieuprawnionym, będzie to skutkowało wystąpieniem potencjalnego incydentu bezpieczeństwa.
- **Integralność** — jeżeli dane zostaną uszkodzone, płatności kartami kredytowymi mogą być przetwarzane w nieprawidłowy sposób.
- **Dostępność** — jeżeli system lub aplikacja ulegnie awarii, nie będziemy w stanie przetwarzać płatności.
- **Posiadanie** — w przypadku utraty nośników kopii zapasowych będzie to skutkowało wystąpieniem potencjalnego incydentu bezpieczeństwa.
- **Autentyczność** — jeżeli nie posiadamy poprawnych, autentycznych informacji o kliencie, może to prowadzić do przetwarzania sfałszowanych transakcji.
- **Użyteczność** — jeżeli gromadzone dane będą nieważne lub nieprawidłowe, ich użyteczność będzie mocno ograniczona.

Choć jest to oczywiście bardzo ogólna ocena zagrożeń dla tego systemu, od razu wskazuje kilka problematycznych obszarów. Sen z powiek może nam spędzać możliwość utraty kontroli nad danymi, gromadzenie i przetwarzanie poprawnych danych oraz utrzymanie systemu w stanie gotowości do pracy. Biorąc pod uwagę wymienione czynniki, możemy zacząć przyglądać się obszarom podatności i potencjalnego ryzyka.

Ocena podatności

Oceniając podatności, należy dokonać tego w kontekście potencjalnych zagrożeń. Dla poszczególnych zasobów możemy zidentyfikować setki czy nawet tysiące potencjalnych zagrożeń, które mogą mieć na nie mniejszy bądź większy wpływ, ale tylko niewielka część tych zagrożeń będzie naprawdę istotna.

W poprzednim podrozdziale zidentyfikowaliśmy potencjalne zagrożenia dla systemu przetwarzającego transakcje kartami kredytowymi — przyjrzyjmy się im zatem i spróbujmy określić, czy istnieją jakieś podatności, które mogłyby zostać przez nie wykorzystane.

- **Poufność** — jeżeli dane o transakcjach zostaną ujawnione podmiotom do tego nieuprawnionym, będzie to skutkowało wystąpieniem potencjalnego incydentu bezpieczeństwa.

  W naszym przypadku dane są szyfrowane zarówno w stanie spoczynku, jak i w ruchu, a przetwarzające je systemy są regularnie sprawdzane przez zewnętrzną firmę przeprowadzającą zlecone testy penetracyjne. *To nie jest ryzyko.*

- **Integralność** — jeżeli dane zostaną uszkodzone, płatności kartami kredytowymi mogą być przetwarzane w nieprawidłowy sposób.

  W ramach procesu przetwarzania danych dokładnie sprawdzamy poprawność danych dotyczących płatności. Nieprawidłowe dane skutkują odrzuceniem transakcji. *To nie jest ryzyko.*

- **Dostępność** — jeżeli system lub aplikacja ulegnie awarii, nie będziemy w stanie przetwarzać płatności.

  Nie mamy zaimplementowanej nadmiarowości dla bazy danych na zapleczu systemu przetwarzania płatności. Jeżeli nasza baza danych ulegnie awarii, nie będziemy w stanie przetwarzać płatności. *To jest ryzyko.*

- **Posiadanie** — w przypadku utraty nośników kopii zapasowych będzie to skutkowało wystąpieniem potencjalnego incydentu bezpieczeństwa.

  Nasze nośniki kopii zapasowych są zaszyfrowane i przekazywane ręcznie przez kuriera. *To nie jest ryzyko.*

- **Autentyczność** — jeżeli nie posiadamy poprawnych, autentycznych informacji o kliencie, może to prowadzić do przetwarzania sfałszowanych transakcji.

  Zapewnienie, że przetwarzane informacje dotyczące płatności kartą rzeczywiście należą do osoby przeprowadzającej transakcję, jest dosyć trudne. Nie ma na to dobrego sposobu. *To jest ryzyko.*

- **Użyteczność** — jeżeli gromadzone dane będą nieważne lub nieprawidłowe, ich użyteczność będzie mocno ograniczona.

  Aby chronić użyteczność przetwarzanych danych, sprawdzamy sumy kontrolne numerów kart kredytowych, upewniamy się, że adresy rozliczeniowe i adresy e-mail klientów są prawidłowe, i wykonujemy wiele innych operacji, aby mieć pewność, że przetwarzane dane są poprawne. *To nie jest ryzyko.*

Powyższe przykłady stanowią tylko ogólny opis procesu oceny podatności, mimo to całkiem dobrze ilustrują specyfikę takiego zadania. Rzetelne przeprowadzenie podobnego oszacowania pozwala zidentyfikować obszary, które potencjalnie mogą budzić obawy (w naszym przykładzie były to zagadnienia związane z autentycznością i dostępnością), i rozpocząć proces oceny związanego z nimi ryzyka.

Ocena ryzyka

Po zidentyfikowaniu zagrożeń i podatności poszczególnych zasobów możemy ocenić ogólne ryzyko. Jak już wspominałem wcześniej w tym rozdziale, ryzyko to połączenie zagrożenia i podatności. Podatność bez odpowiadającego mu zagrożenia lub zagrożenie bez pasującej do niego luki w zabezpieczeniach nie stanowi ryzyka.

W naszym przykładzie następująca pozycja jest zarówno potencjalnym zagrożeniem, jak i obszarem podatności:

- **Dostępność** — jeżeli system lub aplikacja ulegnie awarii, nie będziemy w stanie przetwarzać płatności.

  Nie mamy zaimplementowanej nadmiarowości dla bazy danych na zapleczu systemu przetwarzania płatności. Jeżeli nasza baza danych ulegnie awarii, nie będziemy w stanie przetwarzać płatności. *To jest ryzyko.*

W takim przypadku mamy zarówno zagrożenie, jak i odpowiadającą mu podatność, co oznacza, że ryzykujemy utratę możliwości przetwarzania płatności kartą kredytową z powodu pojedynczego punktu awarii na zapleczu bazy danych. Dzięki odpowiedniemu oszacowaniu zagrożeń oraz podatności i luk w zabezpieczeniach możemy w ten sposób znacząco ograniczyć powiązane z nimi ryzyko.

Redukowanie ryzyka

Aby zredukować ryzyko, możemy zastosować kilka środków uwzględniających każde zagrożenie. Środki te nazywane są *mechanizmami kontrolnymi* (ang. *controls*). Mechanizmy kontrolne można podzielić na trzy kategorie: fizyczne, logiczne i administracyjne.

Fizyczne mechanizmy kontrolne (ang. *physical controls*) chronią środowisko fizyczne, w którym znajdują się systemy lub w którym przechowywane są dane. Te mechanizmy kontrolują również dostęp do i z takich środowisk. Fizyczne mechanizmy kontrolne obejmują takie elementy jak ogrodzenia, bramy, zamki, pachołki, osłony i kamery, ale także systemy utrzymujące środowisko fizyczne, jak systemy ogrzewania i klimatyzacji, systemy gaszenia ognia i rezerwowe generatory mocy.

Chociaż może się wydawać, że fizyczne mechanizmy kontrolne nie są integralnie związane z bezpieczeństwem informacji, są one jednym z jej najbardziej krytycznych elementów: jeżeli nie jesteśmy w stanie fizycznie zabezpieczyć naszych systemów i danych, wszelkie inne mechanizmy zabezpieczające, jakie możemy wdrożyć, staną się bezużyteczne. Jeżeli napastnicy będą mogli uzyskać fizyczny dostęp do chronionych systemów, to będą również mogli je ukraść lub zniszczyć, co w najlepszym przypadku uniemożliwi ich wykorzystanie przez użytkownika. W najgorszym przypadku atakujący będą mogli uzyskać bezpośredni dostęp do aplikacji i danych, wykraść poufne informacje i zasoby lub wykorzystać je do własnych celów.

Logiczne mechanizmy kontrolne (ang. *logical controls*), czasami nazywane też *technicznymi mechanizmami kontrolnymi* (ang. *technical controls*), chronią systemy, sieci i środowiska, które przetwarzają, przesyłają i przechowują dane. Logiczne mechanizmy kontrolne mogą obejmować takie elementy, jak hasła, szyfrowanie, kontrolę dostępu, zapory sieciowe i systemy wykrywania włamań.

Logiczne mechanizmy kontrolne umożliwiają zapobieganie nieautoryzowanym działaniom: jeżeli takie mechanizmy zostaną prawidłowo zaimplementowane i są skuteczne, potencjalny napastnik lub nieautoryzowany użytkownik nie będzie w stanie uzyskać dostępu do aplikacji i danych bez uprzedniego naruszenia tych mechanizmów.

Administracyjne mechanizmy kontrolne (ang. *administrative controls*) opierają się na regułach, prawach, politykach, procedurach, wytycznych i innych elementach, które mają charakter „papierowy". Mechanizmy administracyjne określają, jak powinni zachowywać się użytkownicy danego środowiska. W zależności od rodzaju środowiska i poziomu kontroli takie mechanizmy mogą działać na różnych poziomach. Może to być prosta reguła, np. „wyłącz ekspres do kawy przed wyjściem z biura", mająca na celu uniknięcie problemów związanych z bezpieczeństwem fizycznym (np. pożar budynku w nocy), ale równie dobrze mogą to być bardziej rygorystyczne mechanizmy administracyjne, np. nakazujące, by użytkownicy zmieniali swoje hasła dostępu co 90 dni.

Ważnym aspektem administracyjnych mechanizmów kontrolnych jest możliwość ich egzekwowania. Jeżeli nie mamy uprawnień lub możliwości upewnienia się, że użytkownicy przestrzegają narzuconych wymagań i ograniczeń, to takie mechanizmy są bardziej niż bezużyteczne, ponieważ stwarzają fałszywe poczucie bezpieczeństwa. Na przykład jeżeli utworzymy zasadę, zgodnie z którą pracownicy nie mogą korzystać z zasobów biznesowych do celów prywatnych, musimy mieć możliwość jej egzekwowania. Poza bezpiecznym środowiskiem pracy może to być trudne zadanie. W takiej sytuacji konieczne byłoby monitorowanie korzystania ze służbowych telefonów stacjonarnych i komórkowych, dostępu do internetu, korzystania z poczty elektronicznej, rozmów za pośrednictwem komunikatorów, zainstalowanego oprogramowania i innych potencjalnych obszarów nadużyć. Jeżeli nie będziemy w stanie poświęcić dużej ilości sił i środków na monitorowanie tych obszarów i reagowanie na naruszenia ustalonych reguł, szybko doprowadzimy do sytuacji, w której nie zdołamy ich wyegzekwować i następnym razem, gdy zostaniemy poddani audytowi i poproszeni o przedstawienie dowodów na egzekwowanie zasad, będziemy mieli z tym poważny problem.

Reagowanie na incydenty

Jeżeli Twoje działania w zakresie zarządzania ryzykiem nie były tak dokładne, jak się spodziewałeś, lub gdy zaskoczy Cię jakaś zupełnie nieoczekiwana sytuacja, możesz na nią zareagować za pomocą odpowiednich procedur reagowania na incydenty. Reagowanie na incydenty powinno być ukierunkowane na czynniki, które w Twoim odczuciu mogą najbardziej zaszkodzić Twojej organizacji. Lista tych czynników powinna być wcześniej przygotowana w ramach działań związanych z zarządzaniem ryzykiem.

W miarę możliwości sposób reagowania na incydenty powinien być oparty na dobrze udokumentowanych procedurach postępowania, regularnie przeglądanych, testowanych i ćwiczonych przez zespoły, które powinny podejmować działania w przypadku rzeczywistego incydentu. Nie będzie dobrze, jeżeli dopiero w chwili wystąpienia rzeczywistej sytuacji kryzysowej okaże się, że zalegające na półkach procedury postępowania w przypadku reagowania na incydenty są już nieaktualne i odnoszą się do procesów lub systemów, które dawno temu zostały zmodyfikowane, przeniesione, zastąpione czy wręcz zlikwidowane.

Ogólnie mówiąc, proces reagowania na incydenty składa się z następujących etapów:

- Przygotowanie (ang. *Preparation*).
- Wykrywanie i analiza (ang. *Detections and analysis*).
- Ograniczanie (ang. *Containment*).
- Eliminacja (ang. *Eradication*).
- Odzyskiwanie (ang. *Recovery*).
- Działania po incydencie (ang. *Post-incident activity*).

W kolejnych podrozdziałach omówię bardziej szczegółowo poszczególne etapy.

Przygotowanie

Faza przygotowania reakcji na incydent obejmuje wszystkie działania, które można wykonać z wyprzedzeniem, aby lepiej poradzić sobie z incydentem. Jest to zazwyczaj tworzenie polityk działania i procedur, które regulują sposób reagowania na incydenty, prowadzenie szkoleń i edukacji zarówno dla użytkowników zajmujących się obsługą incydentów, jak i tych, którzy będą zgłaszać incydenty, oraz opracowywanie i utrzymywanie odpowiedniej dokumentacji.

Nigdy nie powinieneś lekceważyć znaczenia tej fazy. Bez odpowiednich przygotowań znacząco maleje szansa na to, że reakcja na incydent przebiegnie prawidłowo i zgodnie z niesprawdzonymi i nieprzetestowanymi procedurami. Dzień, w którym staniesz oko w oko z rzeczywistym incydentem bezpieczeństwa, z pewnością nie będzie najlepszą porą na zastanawianie się, co należy teraz zrobić, kto powinien to zrobić, od czego zacząć i jak w ogóle się za to zabrać.

Wykrywanie i analiza

Faza wykrywania i analizy to moment, w którym rozpoczyna się właściwe działanie. W tej fazie następuje wykrycie problemu, podjęcie decyzji, czy jest to rzeczywiście incydent bezpieczeństwa, i rozpoczęcie procedury reagowania.

Najczęściej problemy są wykrywane za pomocą narzędzi lub usług bezpieczeństwa, takich jak systemy wykrywania włamań (ang. *Intrusion Detection Systems* — IDS), oprogramowanie antywirusowe, logi zapory sieciowej, logi serwerów proxy, alerty z systemów monitorowania informacji i zdarzeń bezpieczeństwa (ang. *Security Information and Event Monitoring* — SIEM) lub od dostawcy zarządzanych usług bezpieczeństwa (ang. *Managed Security Service Provider* — MSSP).

Część analityczna tej fazy jest często połączeniem informacji dostarczanych przez zautomatyzowane narzędzia lub usługi, takie jak systemy SIEM, oraz oceny ludzkiej. Chociaż często można ustawić pewne wartości graniczne, pozwalające stwierdzić, że określona liczba zdarzeń w danym czasie jest normalna lub że jakaś sekwencja zdarzeń nie jest normalna (np. dwa kolejne nieudane logowania, po których następuje poprawne zalogowanie, zmiana hasła i utworzenie nowego konta), to jednak zazwyczaj na pewnym etapie potrzebna jest interwencja człowieka, która może obejmować przegląd logów z różnych systemów bezpieczeństwa, urządzeń sieciowych i infrastruktury, kontakt z osobą, która zgłosiła incydent, oraz ogólną ocenę sytuacji (na nieszczęście dla specjalistów zajmujących się reagowaniem na incydenty i zgodnie z prawem Murphy'ego takie sytuacje zwykle przydarzają się późnym popołudniem w piątek albo w środku nocy z niedzieli na poniedziałek).

Kiedy osoba zajmująca się obsługą incydentu zakończy ocenę sytuacji, podejmuje decyzję, czy sprawa jest incydentem, określa jego krytyczność i kontaktuje się z dodatkowymi osobami niezbędnymi do rozpoczęcia kolejnej fazy obsługi incydentu.

Ograniczanie, eliminowanie i odzyskiwanie

Faza ograniczania strat, eliminowania zagrożenia i przywracania normalnego działania jest etapem, na którym odbywa się większość prac mających na celu rozwiązanie incydentu, przynajmniej w krótkim okresie.

Ograniczanie strat obejmuje podjęcie kroków mających na celu zapewnienie, że sytuacja nie spowoduje więcej szkód, niż już spowodowała, lub przynajmniej zmniejszy bieżące szkody. Na przykład jeżeli incydent dotyczy zainfekowanego złośliwym oprogramowaniem serwera, który jest aktywnie kontrolowany przez zdalnego napastnika, może to oznaczać odłączenie serwera od sieci, wprowadzenie nowych reguł zapory sieciowej blokujących ruch od napastnika oraz aktualizację sygnatur lub reguł systemu zapobiegania włamaniom (ang. *Intrusion Prevention System* — IPS) w celu zatrzymania ruchu generowanego przez złośliwe oprogramowanie.

Podczas *eliminacji* próbujemy usunąć skutki incydentu z naszego środowiska. W przypadku zainfekowanego złośliwym oprogramowaniem serwera, skoro udało nam się już odizolować ten system i odciąć go od sieci dowodzenia i kontroli, musimy usunąć złośliwe oprogramowanie z serwera i upewnić się, że nie występuje ono w innych miejscach w naszym środowisku. Może to wymagać

dodatkowego skanowania innych hostów działających w naszej sieci, a także przeanalizowania logów serwerów i urządzeń sieciowych w celu określenia, z jakimi innymi systemami komunikował się zainfekowany serwer. W przypadku złośliwego oprogramowania, zwłaszcza bardzo nowego lub jego nowych wariantów, może to być bardzo trudne zadanie. Jeżeli masz jakiekolwiek wątpliwości, czy naprawdę usunąłeś złośliwe oprogramowanie lub napastników ze swojego środowiska, powinieneś zachować szczególną czujność i ostrożność.

Na koniec musimy przywrócić stan, w jakim znajdowało się środowisko użytkownika przed incydentem. *Odzyskiwanie* może obejmować przywracanie urządzeń lub danych z nośników zapasowych, przebudowę systemów lub ponowne ładowanie aplikacji. Podobnie jak w poprzednich fazach, może to być znacznie trudniejsze zadanie, niż się początkowo wydaje, ponieważ nasza wiedza o zakresie incydentu i bieżącej sytuacji może być niekompletna lub niejasna. Na przykład może się okazać, że nie jesteśmy całkowicie pewni, czy nośnik kopii zapasowej nie został wcześniej zainfekowany lub uszkodzony i nie daje się odczytać. Możemy też napotkać problem z brakiem nośników instalacyjnych aplikacji, pliki konfiguracyjne mogą być niedostępne lub może wystąpić wiele innych problemów.

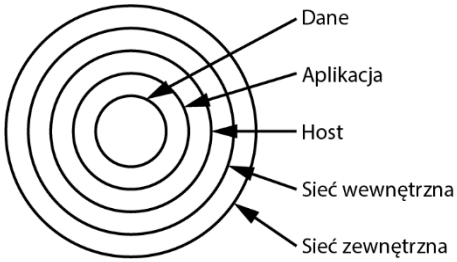
Działania po incydencie

Podobnie jak w przypadku przygotowań, faza działań po zakończeniu incydentu jest bardzo często pomijana, aczkolwiek powinniśmy uczynić wszystko, aby jej nie zaniedbywać. W fazie działań po zakończeniu incydentu, często nazywanej fazą *post mortem* (z łac. *po śmierci*), próbujemy zwykle ustalić, co konkretnie się stało, dlaczego tak się stało i co możemy zrobić, aby to się nie powtórzyło. Celem tej fazy nie jest wskazywanie palcem lub obarczanie kogokolwiek winą (choć czasem się to zdarza), ale zmniejszenie prawdopodobieństwa powtórzenia się takich incydentów w przyszłości (lub ostateczne zapobieżenie temu).

Obrona wielopoziomowa

Teraz, gdy poznałeś już potencjalne skutki naruszenia bezpieczeństwa, rodzaje ataków, z jakimi możesz się spotkać, oraz strategie radzenia sobie z nimi, omówię sposoby zapobiegania takim atakom. Obrona wielopoziomowa (ang. *defence in depth*), nazywana również *obroną w głąb*, jest strategią wykorzystywaną zarówno w dziedzinie wojskowości, jak i bezpieczeństwa informacji. Podstawowa koncepcja tego rozwiązania polega na sformułowaniu wielowarstwowej obrony, która pozwoli na skuteczne stawianie oporu w przypadku, gdy jeden lub więcej mechanizmów obronnych zostanie przełamanych.

Na rysunku 1.5 przedstawiono przykład wielopoziomowego rozwiązania, które można zaimplementować w celu ochrony swoich zasobów.



Rysunek 1.5. Obrona wielopoziomowa

W najprostszym przypadku obrona w głąb powinna być wdrożona przynajmniej na poziomie sieci zewnętrznej, sieci wewnętrznej, hosta, aplikacji i danych. Dobrze zaimplementowana obrona na każdym z tych poziomów powinna skutecznie utrudnić lub wręcz uniemożliwić napastnikowi przeniknięcie do sieci i przeprowadzenie bezpośredniego ataku na zasoby.

Powinieneś jednak pamiętać, że obrona wielopoziomowa nie jest panaceum na wszelkie istniejące zagrożenia. Bez względu na to, ile wydzielisz warstw i jak wiele środków obronnych umieścisz na każdej z nich, nigdy nie będziesz w stanie w nieskończoność utrzymywać zdeterminowanego napastnika z dala od serca swojej sieci. Nie to jednak jest celem takiej obrony w kontekście bezpieczeństwa informacji. Prawdziwym celem takiego rozwiązania jest wydzielenie i umieszczenie wystarczającej ilości środków obronnych pomiędzy naprawdę ważnymi zasobami a napastnikiem, tak byś mógł zauważyć, że atak jest w toku, i byś miał wystarczająco dużo czasu, aby go skutecznie zneutralizować.

Przykładem takiej taktyki opóźniającej jest narzucenie wymagania, aby użytkownicy zmieniali swoje hasła co 60 lub 90 dni. Dzięki temu rozwiązaniu napastnikowi znacznie trudniej jest złamać hasło w takim okresie, aby móc je jeszcze wykorzystać.

Inną taktyką opóźniającą jest wdrożenie złożonych zasad tworzenia haseł. Rozważmy hasło *mypassword*, które składa się z dziesięciu znaków i wykorzystuje tylko jeden zestaw znaków (małe litery). Przy użyciu prostego, powszechnie dostępnego oprogramowania i zwykłego komputera domowego złamanie takiego hasła może zająć atakującemu od kilkunastu do kilkudziesięciu godzin. W przypadku specjalnie zbudowanego systemu do łamania haseł lub wykorzystania botneta proces ten może zająć już tylko kilka czy kilkanaście minut.

Jeżeli zastosujesz nieco bezpieczniejsze zasady konstruowania haseł i wybierzesz hasło takie jak *MyP@ssword1*, które również składa się z dziesięciu znaków, ale używa czterech zestawów znaków (małe i wielkie litery, cyfry i znaki specjalne), to czas jego złamania wydłuży się do kilku czy kilkunastu dni, a nawet tygodni.

Jeżeli będziesz wymagał od swoich pracowników zarówno tworzenia złożonych haseł, jak i częstej ich zmiany, znacząco zwiększysz prawdopodobieństwo tego, że napastnik nie będzie w stanie złamać jednego hasła tak szybko, aby zdążyć go użyć przed kolejną zmianą.

ENTROPIA W HASŁACH

Omówiony wcześniej przykład wykorzystuje klasyczny schemat budowy względnie silnego hasła, składającego się z ośmiu lub więcej znaków i obejmującego wiele zestawów znaków (małe i wielkie litery, cyfry i znaki specjalne). Niektórzy badacze twierdzą jednak, że takie hasła wykazują zbyt mało entropii (nieprzewidywalności), aby były naprawdę bezpieczne, i że lepiej byłoby użyć dłuższego, trudniejszego do złamania i łatwiejszego do zapamiętania hasła, takiego jak *correcthorsebatterystaple*[3].

W ostatecznym rozrachunku najważniejszą kwestią powinno być skonstruowanie rozsądnie bezpiecznych haseł i zmienianie ich w regularnych odstępach czasu.

Warstwy, które należy uwzględnić w strategii obrony wielopoziomowej, będą się różnić w zależności od sytuacji i rodzaju chronionego środowiska. Jak już wspominałem, z perspektywy ściśle logicznego (niefizycznego) bezpieczeństwa informacji obszary, w których powinieneś przeanalizować możliwość zaimplementowania mechanizmów obronnych, to sieć zewnętrzna, perymetr sieciowy, sieć wewnętrzna, hosty, aplikacje i dane.

Złożoność modelu zabezpieczeń można zwiększyć poprzez dołożenie kolejnych warstw obrony, takich jak ochrona fizyczna, polityki bezpieczeństwa, szkolenia zwiększające świadomość użytkowników i inne, ale na razie pozostaniemy przy naszym prostszym przykładzie.

W tabeli 1.1 zamieszczono listę mechanizmów obronnych, które możesz zastosować w każdej z omawianych warstw.

Tabela 1.1. Mechanizmy obronne na poszczególnych warstwach

Warstwa	Mechanizmy obronne
Sieć zewnętrzna	Strefy DMZ
	Tunele VPN
	Logowanie
	Audytowanie
	Testy penetracyjne
	Analiza podatności
Perymetr sieciowy	Zapory sieciowe
	Serwery proxy
	Logowanie
	Pełnostanowa inspekcja pakietów
	Audytowanie
	Testy penetracyjne
	Analiza podatności

Warstwa	Mechanizmy obronne
Sieć wewnętrzna	Systemy IDS
	Systemy IPS
	Logowanie
	Audytowanie
	Testy penetracyjne
	Analiza podatności
Hosty	Uwierzytelnianie
	Systemy antywirusowe
	Zapory sieciowe
	Systemy IDS
	Systemy IPS
	Hasła
	Haszowanie
	Logowanie
	Audytowanie
	Testy penetracyjne
	Analiza podatności
Aplikacje	Pojedyncze logowanie (SSO)
	Filtrowanie zawartości
	Weryfikacja danych
	Audytowanie
	Testy penetracyjne
	Analiza podatności
Dane	Szyfrowanie
	Kontrola dostępu
	Kopie zapasowe
	Testy penetracyjne
	Analiza podatności

W niektórych przypadkach te same mechanizmy obronne pojawiają się na wielu warstwach, ponieważ mają zastosowanie do więcej niż jednego obszaru. Dobrym tego przykładem są *testy penetracyjne*, czyli metoda wyszukiwania podatności i luk w zabezpieczeniach poprzez wykorzystanie tych samych strategii, których użyłby napastnik podczas ataku. Więcej informacji na temat testów penetracyjnych znajdziesz w rozdziale 14. W zależności od potrzeb testy penetracyjne możesz wykorzystywać na każdej warstwie obrony. Z drugiej strony, niektóre mechanizmy obronne są powiązane tylko z określonymi warstwami obrony. Dobrym przykładem mogą być zapory sieciowe i serwery proxy, wykorzystywane na perymetrze sieciowym. Jak w wielu innych przypadkach w dziedzinie bezpieczeństwa można się zastanawiać, czy niektóre lub nawet wszystkie te mechanizmy

obronne mogą istnieć w innych warstwach niż te, które zostały tutaj zaprezentowane, ale generalnie jest to całkiem dobry punkt wyjścia. W dalszej części książki omówię bardziej szczegółowo poszczególne obszary przedstawione w tabeli 1.1 oraz konkretne mechanizmy obronne, które można zastosować w każdym z nich.

Podsumowanie

Przy omawianiu zagadnień związanych z bezpieczeństwem informacji, takich jak rodzaje ataków czy mechanizmów obronnych, pomocne jest posiadanie modelu ułatwiającego precyzyjny opis poszczególnych elementów i scenariuszy. W tym rozdziale omówiłem dwa potencjalne modele bezpieczeństwa: triadę CIA, w skład której wchodzą poufność, integralność i dostępność, oraz heksadę Parkera, składającą się z poufności, integralności, dostępności, posiadania lub kontroli, autentyczności i użyteczności.

Mając na względzie zapobieganie atakom, warto również oszacować rodzaje szkód, które mogą wystąpić w rezultacie ataków. Działania napastników mogą wpływać na środowisko celu poprzez przechwytywanie, zakłócanie, modyfikowanie lub podrabianie. Każdy z tych efektów będzie miał wpływ na poszczególne atrybuty triady CIA.

Podczas omawiania konkretnych zagrożeń, z którymi możesz się zetknąć, powinieneś dobrze zrozumieć, czym jest ryzyko. Ryzyko związane z atakami pojawia się tylko wtedy, gdy obecne jest jakieś zagrożenie, a jednocześnie istnieją podatności i luki w zabezpieczeniach, które dane zagrożenie może wykorzystać. Aby ograniczyć ryzyko, możesz stosować trzy główne rodzaje mechanizmów obronnych: fizyczne, logiczne i administracyjne.

W tym rozdziale omówiłem również koncepcję obrony w głąb, inaczej: obrony wielopoziomowej, która jest szczególnie ważna w świecie bezpieczeństwa informacji. Aby skutecznie chronić swoje środowisko, opierając się na tej koncepcji, należy wprowadzić wiele warstw obrony, tak by skutecznie opóźniać działania napastnika, co daje nam czas na wykrycie ataku i umożliwia bardziej aktywną obronę.

Koncepcje opisane w tym rozdziale mają kluczowe znaczenie dla bezpieczeństwa informacji i są powszechnie używane podczas wykonywania zadań związanych z bezpieczeństwem informacji w wielu firmach i organizacjach; często możesz usłyszeć, jak ktoś mówi o naruszeniu poufności lub autentyczności danej wiadomości e-mail.

Bezpieczeństwo informacji jest przedmiotem codziennej troski w firmach i organizacjach każdej wielkości, szczególnie tych, które zajmują się przetwarzaniem wszelkiego rodzaju danych osobowych, finansowych, medycznych, naukowych lub innych rodzajów informacji podlegających regulacjom prawnym w kraju, w którym działa dany podmiot. Gdy firmy czy organizacje nie inwestują w bezpieczeństwo informacji, konsekwencje mogą być bardzo poważne. W przypadku utraty kontroli nad krytycznymi lub wrażliwymi danymi firma może być narażona na utratę wiarygodności, grzywny, pozwy sądowe, a nawet niemożność dalszego prowadzenia działalności. Krótko mówiąc: bezpieczeństwo informacji jest kluczowym elementem współczesnego świata biznesu.

Ćwiczenia

Oto kilka pytań, które pomogą Ci utrwalić sobie kluczowe pojęcia omawiane w tym rozdziale.

1. Wyjaśnij różnicę pomiędzy podatnością a zagrożeniem.
2. Wymień sześć elementów, które mogą być uznane za logiczne mechanizmy kontrolne.
3. Jakiego terminu mógłbyś użyć do opisania użyteczności danych?
4. Jakie kategorie ataków są atakami na poufność?
5. Skąd wiesz, w którym momencie możesz uznać swoje środowisko za bezpieczne?
6. Korzystając z koncepcji obrony w głąb, jakich warstw mógłbyś użyć, aby zabezpieczyć się przed wyniesieniem przez kogoś poufnych danych z Twojego środowiska na dysku USB?
7. Zgodnie z heksadą Parkera jakie zasady zostaną naruszone w przypadku utraty przesyłki z zaszyfrowanymi taśmami zawierającymi kopie zapasowe, na których umieszczono dane osobowe i informacje o płatnościach klientów?
8. Jeżeli serwery WWW w Twojej firmie oparte są na serwerach IIS firmy Microsoft, a badacze bezpieczeństwa właśnie odkryli nowego wirusa, który atakuje serwery WWW Apache, to czy nowe zagrożenie stanowi ryzyko dla Twojego środowiska?
9. Jeżeli zamierzasz wdrożyć nową politykę bezpieczeństwa dla swojego środowiska, która wymaga stosowania złożonych i automatycznie generowanych haseł, unikalnych dla każdego systemu i składających się z co najmniej 30 losowych znaków, takich jak *!Qa4(j0nO$&xn1%2AL34ca#!Ps321$*, na co będzie to miało negatywny wpływ?
10. Biorąc pod uwagę triadę CIA i heksadę Parkera, jakie są zalety i wady każdego z tych modeli?

Skorowidz

A

B

C

M

N

O

P

R

S

Ś

T

U

V

W

Z

Ż

Notatki


PROGRAM
PARTNERSKI
GRUPY HELION
1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ
Zmień swoją stronę WWW w działający bankomat!
Dowiedz się więcej i dołącz już dzisiaj!
http://program-partnerski.helion.pl
GRUPA
Helion

Bezpieczeństwo informacji: rozpoznaj zagrożenie i użyj właściwego narzędzia!

Bezpieczeństwo informacji od dawna nie jest domeną wyłącznie inżynierów. Zajmują się nim menedżerowie, stratedzy, ekonomiści czy politycy, jednak każda z tych grup najczęściej bierze pod uwagę tylko część tej dziedziny. Istnieje też mnóstwo technologii służących organizacjom do zabezpieczania zasobów informacyjnych. Jakby tego było mało, zastosowanie właściwych strategii obronnych i wybór optymalnych narzędzi wymaga ugruntowania znajomości podstaw zagadnienia, a także nieco szerszego spojrzenia na bezpieczeństwo informacji.

Ta książka stanowi wszechstronny i praktyczny przegląd dziedziny bezpieczeństwa informacji. Posłuży każdemu, kto jest zainteresowany tym problemem, chce zdobyć ogólną wiedzę na ten temat albo zastanawia się, od czego zacząć wdrażanie systemu bezpieczeństwa we własnej organizacji. Znalazły się tutaj jasne, przystępne i konkretne wyjaśnienia zasad bezpieczeństwa informacji, a także wskazówki, jak przełożyć je na praktykę. Wyczerpująco omówiono kluczowe dla tej dziedziny koncepcje, a następnie opisano rzeczywiste zastosowania przedstawionych idei w obszarach bezpieczeństwa operacyjnego, ludzkiego, fizycznego, sieciowego, systemu operacyjnego, mobilnego, wbudowanego, internetu rzeczy (IoT) i bezpieczeństwa aplikacji. Ważnym elementem publikacji jest również prezentacja praktycznych sposobów oceny bezpieczeństwa informacji.

W książce:

- utwardzanie procesu uwierzytelniania za pomocą biometrii i tokenów sprzętowych
- algorytmy nowoczesnej kryptografii
- prawo a ochrona systemów i danych
- narzędzia antywirusowe, zapory sieciowe i systemy wykrywania włamań
- podatności i ich eliminowanie

Dr Jason Andress jest ekspertem w dziedzinie bezpieczeństwa systemów informatycznych, a także badaczem i miłośnikiem nowoczesnych technologii. Od ponad dziesięciu lat pisze na tematy związane z bezpieczeństwem, zajmuje się między innymi bezpieczeństwem danych, bezpieczeństwem sieciowym, bezpieczeństwem sprzętu, testami penetracyjnymi i informatyką śledczą.

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-283-8342-5
9 788328 383425
INFORMATYKA W NAJLEPSZYM WYDANIU
Cena: 59,00 zł