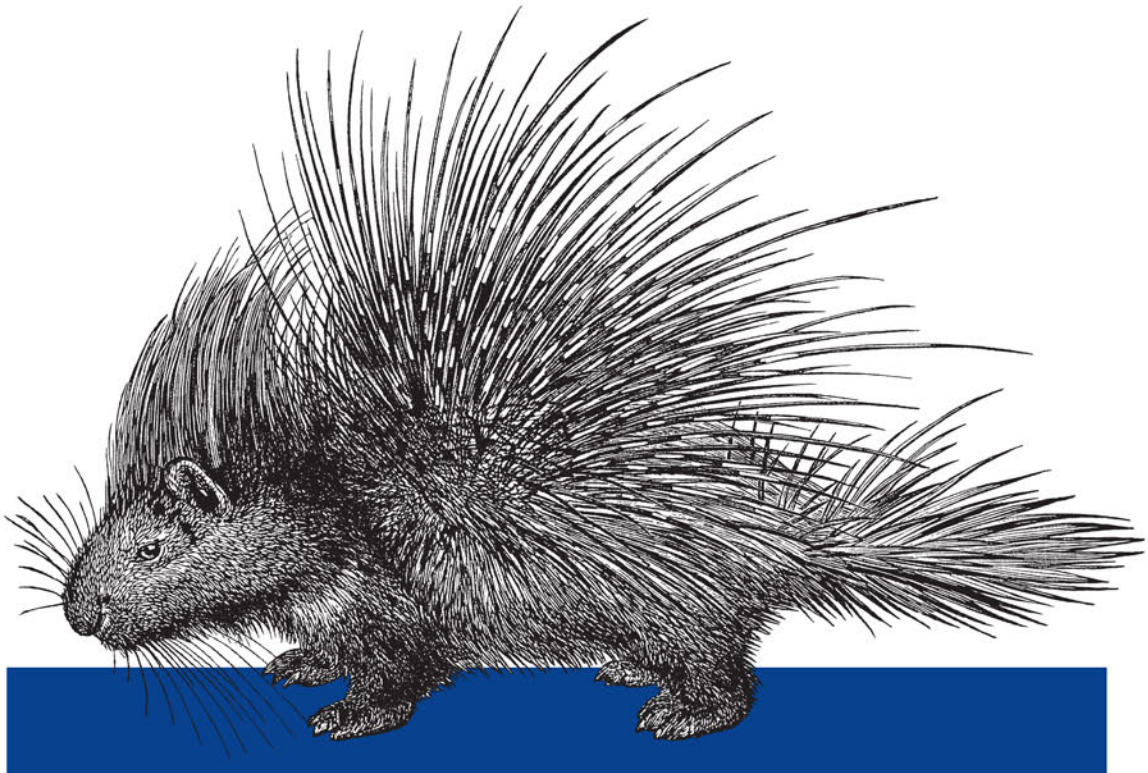
O'REILLY®



Bezpieczeństwo defensywne

PODSTAWY I NAJLEPSZE PRAKTYKI

Helion

Lee Brotherston, Amanda Berlin

Tytuł oryginału: Defensive Security Handbook: Best Practices for Securing Infrastructure

Tłumaczenie: Lech Lachowski

ISBN: 978-83-283-4722-9

HELION SA
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/bezdef
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

Spis treści

ROZDZIAŁ 1.

Tworzenie programu bezpieczeństwa

Tworzenie lub ulepszanie programu bezpieczeństwa może być zniechęcającym zadaniem. Przy tak wielu aspektach do rozważenia, im więcej wstępnych przemyśleń i planowania wprowadzimy do procesu tworzenia tego programu, tym łatwiej będzie nim zarządzać na dłuższą metę. W tym rozdziale omówimy szkielet programu bezpieczeństwa i wstępne kroki administracyjne.

Nie popadaj w nawyk wykonywania zadań poprzez przeprowadzanie rutynowych czynności lub tworzenie konfiguracji z nastawieniem „Tak to zawsze robiliśmy". Ten sposób myślenia będzie tylko hamować postęp i w miarę upływu czasu zmniejszać poziom bezpieczeństwa.

> Ludzie są uczuleni na zmiany. Uwielbiają mówić: „Zawsze robiliśmy to w ten sposób". Próbuję z tym walczyć. Dlatego powiesiłam na ścianie zegar, którego wskazówki biegną w przeciwnym kierunku.
>
> Grace Hopper, *The Wit and Wisdom of Grace Hopper* (1987)

Zalecamy, żeby podczas tworzenia programu postępować zgodnie ze wskazówkami z tego rozdziału w podanej kolejności. Chociaż staraliśmy się odpowiednio pogrupować pozostałe rozdziały, można je stosować w taki sposób, jaki najlepiej odpowiada potrzebom firmy.

Podwaliny

Aby położyć podwaliny pod program bezpieczeństwa informacji, nie trzeba wyważać zamkniętych drzwi. W rozdziale 8. omówimy kilka standardów, które mogą okazać się bardzo przydatne. Amerykański Narodowy Instytut Standaryzacji i Technologii (ang. *National Institute of Standards & Technology* — NIST) opracował oparty na ryzyku framework cyberbezpieczeństwa, który obejmuje wiele aspektów programu. Rdzeń frameworka NIST (ang. *Framework Core*) składa się z pięciu współbieżnych i ciągłych funkcji: identyfikowania (ang. *identify*), ochraniania (ang. *protect*), wykrywania (ang. *detect*), reagowania (ang. *respond*) i odtwarzania (ang. *recover*). Gdy rozpatrujemy te funkcje razem, kreślą one ogólny strategiczny obraz cyklu zarządzania ryzykiem cyberbezpieczeństwa w organizacji (*http://bit.ly/2mPhsY1*). Jednak do możliwych atutów można zaliczyć nie tylko taki framework, ale również standardy zgodności. Chociaż słabo wdrożone standardy zgodności mogą obniżać ogólny poziom bezpieczeństwa organizacji, mogą również okazać się świetnym punktem wyjścia do nowego programu. Standardy zgodności zostaną omówione szczegółowo w rozdziale 8. O ile takie zasoby mogą być doskonałą wartością dodaną, o tyle trzeba zawsze pamiętać, że każda organizacja jest inna i niektóre z omówionych aspektów mogą być nieistotne (o czym będziemy stale przypominać w całej książce).

Definiowanie zespołów

Podobnie jak w przypadku wielu innych działów, również w zakresie bezpieczeństwa ważne jest posiadanie odpowiedniego personelu we właściwie zdefiniowanych zespołach. Otwarta komunikacja między zespołami powinna być głównym celem, ponieważ bez tego system bezpieczeństwa jest poważnie osłabiony. Zespoły do spraw bezpieczeństwa można zorganizować w następujący sposób:

Zespół wykonawczy
: Biuro dyrektora działu informatyki lub biuro dyrektora ds. bezpieczeństwa informacji zapewni siłę i autorytet potrzebne do podejmowania decyzji dotyczących całego przedsiębiorstwa i wprowadzania zmian. Zespół wykonawczy będzie również w stanie zapewnić długoterminową wizję, wskazywać ryzyko korporacyjne, ustalać cele, zapewniać finansowanie i sugerować kamienie milowe.

Zespół ds. ryzyka
: Wiele organizacji posiada już zespół ds. oceny ryzyka, a zespół ds. ryzyka może być jego częścią. W większości organizacji bezpieczeństwo nie będzie priorytetem numer jeden. Zespół ten określi ryzyko związane z wieloma innymi obszarami biznesu, od sprzedaży po marketing i finanse. Jego członkowie nie muszą być biegli w kwestiach bezpieczeństwa. W takiej sytuacji można ich uczyć podstaw bezpieczeństwa na podstawie konkretnych przypadków lub wprowadzić do zespołu analityka ryzyka. Pomocny może być framework, taki jak OCTAVE (ang. *Operationally Critical Threat, Asset, and Vulnerability Evaluation*).

Zespół ds. bezpieczeństwa
: Zespół ds. bezpieczeństwa będzie wykonywać zadania mające na celu ocenę i wzmocnienie bezpieczeństwa środowiska. Większość tej książki skupia się na tym zespole oraz zespole wykonawczym. Są one odpowiedzialne za codzienne operacje związane z bezpieczeństwem, w tym zarządzanie aktywami, ocenianie zagrożeń i słabych punktów, monitorowanie środowiska pod kątem ataków i zagrożeń, zarządzanie ryzykiem i zapewnianie szkoleń. W odpowiednio dużym środowisku zespół ten może być podzielony na różne podgrupy, takie jak sieci, operacje, aplikacje i aktywne zabezpieczenia.

Zespół audytujący
: Zawsze dobrze jest mieć system kontroli i gwarantowania równowagi. Nie chodzi tylko o wyszukiwanie luk w procesach i kontrolach bezpieczeństwa, ale także o zapewnianie, że realizowane są właściwe zadania i kamienie milowe.

Podstawowe podejście do systemu bezpieczeństwa

Rzeczy nieznane w każdym środowisku będą przerażające. Jak ocenić poziom sukcesu programu, nie wiedząc, w którym miejscu się rozpoczął? Na początku każdego nowego programu bezpieczeństwa lub gruntownej analizy istniejącego jednymi z pierwszych i najważniejszych zadań dla wszystkich zespołów powinny być fazy podstawowa i wykrywania. W całej tej książce kilkakrotnie omówimy zarządzanie aktywami na różne sposoby. Podstawy bezpieczeństwa organizacji to jedynie kolejny krok w tym zarządzaniu. Należy przygotować zestawienie takich elementów jak:

- reguły i procedury;
- punkty końcowe — komputery stacjonarne i serwery, w tym data wdrożenia i wersja oprogramowania;
- licencjonowanie i odnawianie oprogramowania, a także certyfikaty SSL;
- ślady internetowe — domeny, serwery pocztowe, urządzenia dmz;
- urządzenia sieciowe — routery, przełączniki, punkty dostępu bezprzewodowego, IDS/IPS i ruch sieciowy;
- rejestrowanie i monitorowanie;
- punkty wejścia-wyjścia — kontakty ISP, numery kont i adresy IP;
- zewnętrzni dostawcy, ze zdalnym dostępem lub bez, i podstawowe kontakty.

Ocena zagrożeń i ryzyka

Ocena zagrożeń i ryzyka będzie się znacznie różnić w zależności od organizacji. Każdy wewnętrzny i zewnętrzny ślad w połączeniu z indywidualną infrastrukturą jest niepowtarzalny. Taka ocena obejmuje zarówno ogólny przegląd, jak i szczegółową analizę aktywów. Bez wiedzy o zagrożeniach i ryzyku, z którymi musi mierzyć się dana organizacja, trudniej jest dostosować technologie i rekomendacje w celu zapewnienia odpowiedniej ochrony. Zarządzanie ryzykiem jest często podzielone na cztery etapy: identyfikowanie, ocena, ograniczanie ryzyka i monitorowanie.

Identyfikowanie

Organizacje powinny obawiać się dużej liczby zagrożeń i ryzyka występującego w różnych sektorach gospodarki. Skoncentrowanie się na trendach branżowych i określonych zagrożeniach umożliwi spersonalizowanie i spriorytetyzowanie programu bezpieczeństwa, aby stał się bardziej wydajny. Większość organizacji bardzo niewiele uwagi poświęca zagrożeniom i ryzyku, które napotykają na co dzień, i będzie w dalszym ciągu tak robić, dopóki nie padnie ich ofiarą. W Stanach Zjednoczonych dostęp do nieocenionych zasobów można uzyskać dzięki centrom wymiany i analizy informacji (ang. *Information Sharing and Analysis Centers* — ISAC), które są zrzeszane przez Krajową Radę ISAC (*http://www.nationalisacs.org*) w celu udostępnienia informacji z zakresu bezpieczeństwa charakterystycznych dla poszczególnych sektorów. „Centra ISAC gromadzą, analizują i rozpowszechniają informacje o zagrożeniach oraz dostarczają swoim członkom narzędzia do ograniczania ryzyka i zwiększania odporności”[1].

Należy zidentyfikować nie tylko zagrożenia charakterystyczne dla branży, ale także ogólne tendencje w tym zakresie, takie jak złośliwe oprogramowanie, oprogramowanie ransomware, phishing i zdalne exploity. Dwoma istotnymi źródłami informacji na ten temat są listy OWASP Top 10 i CIS 20 (wcześniej znana jako SANS Top 20) Critical Security Controls. Każda organizacja może skorzystać z obu tych źródeł oraz ze standardów określonych przez Cloud Security Alliance. Większość elementów z tych list zostanie szczegółowo omówiona w tej książce, ale aktualizacja tych informacji powinna być kluczowym elementem każdego planu strategicznego.

[1] *https://www.nationalisacs.org/about-isacs*

Ocena

Po zidentyfikowaniu potencjalnych zagrożeń należy je ocenić, aby określić, czy mają zastosowanie do określonego środowiska. Zadania, takie jak wewnętrzne i zewnętrzne skanowania luk w zabezpieczeniach, inspekcje reguł zapory ogniowej oraz zarządzanie zasobami i ich wykrywanie, pozwolą uzyskać szerszy obraz tego, z jakiego rodzaju ogólną ekspozycją na ryzyko mamy do czynienia.

Ograniczanie ryzyka

Ograniczanie ryzyka to główny powód naszej obecności w tym miejscu. Jest to również tematem znacznej części tej książki. Dostępne opcje to: unikanie, renegocjowanie, przenoszenie lub akceptowanie ryzyka. Oto kilka przykładów:

Unikanie ryzyka
: Dawid decyduje, że przechowywanie numerów ubezpieczenia społecznego dla klientów jest niepotrzebnym procesem i kończy z tą praktyką.

Renegocjowanie ryzyka
: Antek zaczyna wyłączać otwarte porty, wprowadzać bardziej rygorystyczne reguły zapory sieciowej i łatać punkty końcowe.

Przenoszenie ryzyka
: Janek zleca przetwarzanie kart kredytowych podmiotom zewnętrznym, zamiast przechowywać dane na miejscu.

Akceptowanie ryzyka
: Kasia wie, że pewien punkt końcowy nie ma dostępu do innych punktów końcowych i uruchamia na nim zewnętrzną aplikację. Ta aplikacja zawiera lukę niskiego poziomu ryzyka wymaganą do jej funkcjonowania. Chociaż na tym etapie nic nie można zmienić lub renegocjować w kwestii tej luki w zabezpieczeniach, ryzyko jest wystarczająco niskie, aby je zaakceptować.

Ryzyko należy akceptować tylko w ostateczności. Jeśli kiedykolwiek dojdziesz do tego punktu, poproś o pełną dokumentację od dostawców zewnętrznych oraz zespołu wykonawczego, a także o dokumentację procesów, które zostały wykonane przed podjęciem tej decyzji. Dodaj do tego przynajmniej coroczny przegląd każdego zaakceptowanego ryzyka, aby zagwarantować jego odpowiednie zrewidowanie.

Monitorowanie

Śledź ryzyko w czasie dzięki zaplanowanym kwartalnym lub rocznym spotkaniom. Przez cały rok wprowadzonych zostanie wiele zmian mających wpływ na ilość i rodzaj ryzyka, który należy wziąć pod uwagę. W ramach każdego monitorowania lub kontrolowania zmian określaj, czy zmiana w jakikolwiek sposób wpływa na ryzyko.

Nadawanie priorytetów

Po zidentyfikowaniu i ocenie zagrożeń i ryzyka trzeba im również nadać priorytety od najwyższego do najniższego procentu ryzyka dla renegocjacji, ze skoncentrowaniem się na stałej ochronie. Jednak nie zawsze musi to być kosztowne przedsięwzięcie. Znaczną ilość ograniczeń ochronnych można wprowadzić z niewielkim lub zerowym kosztem dla organizacji. Daje to wiele możliwości uruchomienia programu bezpieczeństwa bez konieczności posiadania wydzielonego budżetu. Bezpłatne przeprowadzenie badania *due diligence*, wymaganego do wystartowania z programem, powinno przemówić do zespołu wykonawczego.

Przy ustalaniu priorytetów nie zawsze korzystaj z porad producentów lub zewnętrznych dostawców. Każde środowisko jest inne i w taki sposób powinno być traktowane. Nadawaj zadaniom priorytety na podstawie szerszego obrazu, gdy wszystkie informacje zostaną już zebrane.

Tej książki nie należy traktować jako listy kolejnych zadań z zakresu bezpieczeństwa, które trzeba wykonać. Ustalanie priorytetów może znacznie się różnić w zależności od środowiska. Zapamiętaj tylko, że jeśli dane środowisko znalazło się już w sytuacji zagrożenia i jest atakowane, nie rozpoczynaj od tworzenia reguł lub usuwania skutków działania złośliwego oprogramowania. Jako szef służby przeciwpożarowej nie powinieneś się zajmować szukaniem podpalacza i punktu zapalnego, jeśli nie ugasiłeś jeszcze ognia.

Tworzenie kamieni milowych

Kamienie milowe (ang. *milestones*) zabiorą Cię z miejsca, w którym jesteś, do miejsca, w którym chcesz być. Będą reprezentować ogólny postęp na drodze do bezpiecznego środowiska. Jest to trochę zbieżne z obowiązkami kierownika projektu, ale w wielu przypadkach firmy nie mają takiego dedykowanego stanowiska. Kamienie milowe można luźno podzielić na cztery długości lub poziomy:

Poziom 1. Szybkie korzyści
: Najkrótszymi kamieniami milowymi powinny być szybkie korzyści, które można osiągnąć w kilka godzin lub dni, czyli duże luki w zabezpieczeniach, takie jak jednorazowe, nieużywane punkty końcowe możliwe do wyeliminowania, starsze urządzenia, które można przenieść do bezpieczniejszej sieci, oraz aktualizacje produktów zewnętrznych dostawców. Przedstawimy wiele bezpłatnych rozwiązań, ponieważ proces ich zakupu może zająć dużo czasu.

Poziom 2. Bieżący rok
: Do poziomu 1. mogą nie zaliczać się większe luki w zabezpieczeniach, które będą wymagały zatwierdzenia zmian przez zarząd, tworzenia zmian w procesie lub zgłoszenia znacznej ilości osób. Są to główne zmiany w routingu, wdrożenie edukacji użytkowników oraz likwidacja współdzielonych kont, ulepszenie usług i urządzeń, które również wymagają niewielkiego lub zerowego budżetu.

Poziom 3. Przyszły rok

Do tego poziomu zaliczają się luki w zabezpieczeniach i zmiany wymagające znacznej ilości planowania lub opierające się na innych poprawkach, które muszą być wprowadzone w pierwszej kolejności. Dobrymi przykładami są aktualizacje domen, wymiana serwerów i głównych urządzeń infrastruktury oraz zmiany w monitorowaniu i uwierzytelnianiu.

Poziom 4. Długoterminowo

Nierzadko osiągnięcie kamienia milowego może zająć kilka lat ze względu na długość projektu, brak budżetu, konieczność odnowienia umów lub trudności związane z wprowadzaniem zmian. Może to uwzględniać takie elementy, jak: restrukturyzacja sieci, wymiana podstawowego oprogramowania lub nowe centra danych.

Pomocne jest powiązanie kamieni milowych z kluczowymi kontrolami i ryzykami, które zostały już zidentyfikowane. Chociaż rozpoczęcie od poważniejszych zagrożeń i większych luk w zabezpieczeniach jest dobrym pomysłem, nie będą to poprawki łatwe do wprowadzenia. W wielu przypadkach te kwestie będą wymagały nie tylko znacznej ilość czasu i projektowania, ale także budżetu, który może nie być dostępny. Przy tworzeniu każdego poziomu należy uwzględniać wszystkie aspekty.

Przypadki użycia, ćwiczenia symulacyjne i praktyczne

Przypadki użycia są istotne dla pokazania sytuacji, które mogą narażać na ryzyko kluczową infrastrukturę, wrażliwe dane lub inne aktywa. Należy przeprowadzić burzę mózgów z właścicielami danych i kierownikami zespołów, aby zaplanować, jak ustrzec się przed złośliwymi atakami. Najlepiej na początek skupić się na mniej więcej trzech różnych przypadkach użycia i na ich podstawie zaplanować ograniczanie zagrożeń i monitorowanie. Dobrymi przykładami przypadków użycia są takie kwestie, jak: oprogramowanie ransomware, ataki DDoS (ang. *Distributed Denial of Service*), niezadowolony pracownik, zagrożenie wewnętrzne i eksfiltracja danych. Po wybraniu kilku przypadków użycia można je rozłożyć na czynniki pierwsze, przeanalizować i skorelować z każdym krokiem łańcucha niszczenia intruzów Lockheeda Martina (*http://lmt.co/2miXqrZ*).

Łańcuch niszczenia intruzów (ang. *Intrusion Kill Chain*), nazywany niekiedy cybernetycznym łańcuchem niszczenia (ang. *Cyber Kill Chain*), to „model praktycznego wywiadu, gdy obrońcy dostosowują defensywne zdolności przedsiębiorstwa do konkretnych procesów podejmowanych przez przeciwnika w celu zaatakowania tego przedsiębiorstwa". Składa się z siedmiu kroków opisanych w białej księdze Lockheeda Martina (*http://lmt.co/2miXqrZ*):

1. Rozpoznanie (ang. *reconnaissance*): badanie, identyfikacja i wybór celów, często w formie indeksowania stron internetowych, na przykład materiałów konferencyjnych i list mailingowych, pod kątem adresów e-mailowych, relacji społecznych lub informacji o konkretnych technologiach.
2. Uzbrojenie (ang. *weaponization*): połączenie trojana zdalnego dostępu z exploitem w możliwy do dostarczenia ładunek zwykle za pomocą zautomatyzowanego narzędzia. Coraz częściej jako uzbrojone ładunki dostarczalne służą pliki danych aplikacji, takie jak Adobe Portable Document Format (PDF) lub dokumenty Microsoft Office.
3. Dostarczenie (ang. *delivery*): przekazanie broni do docelowego środowiska. Trzy najbardziej rozpowszechnione wektory dostarczania uzbrojonego ładunku to załączniki wiadomości e-mail, strony internetowe i wymienne nośniki USB.

4. Eksploatacja (ang. *exploitation*): po dostarczeniu broni do hosta ofiary wyzwalany jest kod intruza. Najczęściej eksploatacja jest ukierunkowana na lukę w zabezpieczeniach aplikacji lub systemu operacyjnego, ale może również wykorzystywać samych użytkowników lub funkcję systemu operacyjnego, która automatycznie wykonuje kod.
5. Instalacja (ang. *installation*): instalacja trojana lub backdoora zdalnego dostępu w systemie ofiary pozwala przeciwnikowi utrzymać trwałą obecność w środowisku.
6. Wydawanie poleceń i kontrolowanie (ang. *command and control* — C2): zazwyczaj przejęte hosty muszą wysłać sygnał wychodzący do serwera kontrolera internetowego w celu ustanowienia kanału C2. Manualnej interakcji wymaga w szczególności złośliwe oprogramowanie APT (ang. *advanced persistent threat*), które nie przeprowadza automatycznych działań. Po ustanowieniu kanału C2 intruz ma dostęp do środowiska docelowego poprzez wpisywanie poleceń na klawiaturze.
7. Działania na celach (ang. *actions on objectives*): dopiero teraz, po przejściu przez pierwszych sześć etapów, intruz może podejmować działania w celu osiągnięcia pierwotnych celów. Zazwyczaj tym celem jest eksfiltracja danych, która polega na gromadzeniu, szyfrowaniu i wydobywaniu informacji ze środowiska ofiary. Potencjalnymi celami są również naruszenia integralności lub dostępności danych. Ewentualnie intruz może chcieć jedynie uzyskać dostęp do stanowiska pracy początkowej ofiary, aby wykorzystać je jako punkt do zaatakowania dodatkowych systemów i poruszania się bocznymi drogami wewnątrz sieci.

Ta biała księga zawiera wiele przydatnych informacji, które można wykorzystać również do tworzenia przypadków użycia.

Tabela 1.1 jest przykładem przypadku użycia dla łańcucha niszczenia krok po kroku, który utworzyliśmy dla ataku ransomware.

Na każdym etapie łańcucha niszczenia można dodać wiele różnych środków defensywnych w celu ogólnego zmniejszenia ryzyka na każdej warstwie.

Po utworzeniu i wdrożeniu kontroli bezpieczeństwa na podstawie przypadków użycia jako dowód poprawności koncepcji posłużyć mogą ćwiczenia symulacyjne i praktyczne. **Ćwiczenie symulacyjne** to spotkanie kluczowych interesariuszy i pracowników, którzy w warunkach niskiego poziomu stresu krok po kroku omawiają etapy pewnego rodzaju katastrofy, awarii, ataku lub innej sytuacji kryzysowej. Ćwiczenie praktyczne polega na tym, że personel wykonuje możliwie jak najwięcej procesów, procedur i działań defensywnych, które byłyby wykonywane podczas jednej z sytuacji kryzysowych.

Chociaż ćwiczenia praktyczne mają ograniczony zakres, mogą być bardzo przydatne do testowania określonych procedur kontroli dla luk i możliwych ulepszeń. Można do pewnego stopnia przećwiczyć plan odzyskiwania sprawności po awarii, przetestować przywracanie plików z kopii zapasowych oraz awaryjne przełączanie usług do członków zapasowego klastra.

W ćwiczeniu symulacyjnym powinny brać udział następujące osoby lub grupy.

- W ćwiczeniu tym powinien uczestniczyć moderator lub koordynator, który dostarczy scenariusz do rozegrania. Ten moderator może odpowiadać na pytania „co jeśli” dotyczące wymyślonych sytuacji kryzysowych oraz prowadzić dyskusję, wprowadzać dodatkowe zasoby i kontrolować

Tabela 1.1. Przypadek użycia dla ransomware

Krok w łańcuchu niszczenia	Złośliwe działanie	Działanie defensywne	Potencjalne monitorowanie
Rozpoznanie	Atakujący pozyskuje adresy e-mailowe oraz informacje o wykorzystywanych technologiach, a następnie na tej podstawie tworzy profil organizacyjny.	Utwórz reguły dotyczące udostępniania wewnętrznych informacji na stronach, takich jak LinkedIn, lub używania firmowych adresów e-mailowych do celów prywatnych. Po zauważeniu poważnych naruszeń bezpieczeństwa uruchamiaj resetowanie haseł. Pracownicy z reguły wykorzystują swoje hasła również do innych usług lub stron, chociaż nie powinni tego robić.	Czy firmowe adresy e-mailowe można również znaleźć w kontekście naruszeń bezpieczeństwa innych podmiotów? Ile adresów e-mailowych udało się odnaleźć za pomocą białego wywiadu?
Uzbrojenie	Atakujący tworzy złośliwy exploit (lub wykorzystuje istniejący), który ma zostać wysłany do ofiary.	Poznanie i świadomość bieżących zagrożeń i technik stosowanych przez atakujących pozwala lepiej skonstruować i dostosować działania defensywne.	Nie dotyczy.
Dostarczenie	Użytkownik otrzymuje e-mail typu phishing.	Oceń, jakie rodzaje załączników są wymagane w organizacji. Pliki z rozszerzeniem *.js* mogą być wyjątkowo szkodliwe i są rzadko wymieniane z zewnętrznymi źródłami. Zaimplementuj czarne i szare listy mailingowe, takie jak Spamhaus i DNSBL, aby zablokować znane złośliwe serwery pocztowe.	Zaszczep swoim użytkownikom koncepcję „ufaj, ale weryfikuj”. Zaimplementuj blokowanie niektórych rodzajów plików o określonym rozmiarze, o których wiadomo, że są złośliwe i powiązane z oprogramowaniem ransomware. (Oznacz pliki *.scr* powyżej 22 MB i *.js* powyżej 15 MB).
Eksploatacja	Punkty końcowe pobierają plik JavaScript lub dokument Worda ze złośliwym makro.	Wyłącz obsługę makr i złośliwych typów plików poprzez reguły grup. Upewnij się, że na każdym punkcie końcowym jest zainstalowana i zaktualizowana ochrona.	Monitoruj dzienniki proxy pod kątem niespodziewanych pobrań (na przykład JavaScript jest pierwszym plikiem pobranym z tego hosta, host jest na czarnej liście itd.). Używaj serwerów proxy lub systemów IDS (w przypadku zwykłego tekstu) do monitorowania zamaskowanych łańcuchów znaków.

Tabela 1.1. Przypadek użycia dla ransomware — ciąg dalszy

Krok w łańcuchu niszczenia	Złośliwe działanie	Działanie defensywne	Potencjalne monitorowanie
Instalacja	Ładunek jest wykonywany na urządzeniu użytkownika końcowego. (Lucky, Cerber i CryptoWall wykorzystują wbudowany interfejs Crypto API systemu Windows, aby poradzić sobie z szyfrowaniem).	Przechowuj kopie zapasowe (które nie są dołączone na stałe), aby można było łatwo odtworzyć zaszyfrowane pliki. W zależności od systemu operacyjnego możesz użyć „zapór sieciowych systemu plików", takich jak XFENCE (*https://campaigns.f-secure.com/xfence*), aby umożliwić dostęp do plików na podstawie procesu. Oznacza to, że możesz na przykład umożliwić odczyt aplikacji MS Word, ale nie przeglądarce IE. Istnieją eksperymentalne techniki, których możesz użyć do blokowania oprogramowania ransomware opartego na szyfrowaniu (na przykład Decryptonite: *http://bit.ly/2miUj3w*).	Wysoki wzrost w Crypto API systemu Windows w krótkim przedziale czasu. Nadmierne liczby w domenie lub niski procent znaczących łańcuchów znaków w domenie.
Polecenia i kontrola (C2)	Ransomware komunikuje się z serwerem C2 w internecie, aby przesłać klucz deszyfrowania.	Zaimplementuj sinkhole DNS i automatyczne blokowanie połączeń wychodzących do znanych złośliwych adresów IP.	Połączenia ze znanymi serwerami C2.
Działania i cele	Malware rozpoczyna szyfrowanie plików na dysku twardym, zmapowanych napędach sieciowych i urządzeniach USB. Po zakończeniu tego procesu wyświetlane są: ekran powitalny, obraz pulpitu, strona internetowa lub plik tekstowy z instrukcjami zapłacenia okupu.	Zaimplementuj pułapkę w postaci tzw. *Honey Directories* — ransomware przechodzi do lokalizacji *C:\$$* i widzi kolejny katalog *$$*; kiedy przechodzi do *C:\$$\$$*, widzi kolejny katalog *$$* itd.	Można włączyć zaawansowany audyt plików w celu ostrzegania w przypadku ekstremalnego wzrostu poziomu zmian w systemie plików.

tempo ćwiczenia. Należy poinformować uczestników, że podczas tego ćwiczenia dopuszczalna jest sytuacja, iż nie będą w stanie udzielić odpowiedzi na niektóre pytania. Celem ćwiczeń symulacyjnych jest znalezienie słabych punktów w bieżących procedurach, aby zabezpieczyć je, zanim wydarzy się prawdziwy incydent.

- Jeden z uczestników ćwiczenia powinien również ocenić jego ogólny przebieg oraz sporządzić raport podsumowujący. Osoba oceniająca powinna robić drobiazgowe notatki i śledzić wszystkie omawiane procedury w celu zapewnienia dokładności. Chociaż będzie to główna osoba sporządzająca notatki, konkretną wiedzę w jakimś zakresie i zrozumienie sytuacji mogą mieć inne

grupy lub poszczególni uczestnicy. W takim przypadku dobrym rozwiązaniem jest, aby na zakończenie każdego ćwiczenia symulacyjnego wszyscy jego uczestnicy przekazali oceniającemu kopie własnych notatek.

- Spośród osób obecnych w trakcie ćwiczenia symulacyjnego największą część stanowią jego uczestnicy. Należy uwzględnić obecność następujących grup pracowników: dział finansowy, zasoby ludzkie, dział prawny, działy bezpieczeństwa (zarówno fizycznego, jak i informacyjnego), zarządzanie, dział marketingu i wszelkie inne kluczowe działy, które mogą być wymagane. Uczestnicy powinni być skłonni do angażowania się w rozmowę, stawiania wyzwań samym sobie i innym oraz pracy w ramach parametrów ćwiczenia.

Do ćwiczenia symulacyjnego należy przygotować następujące materiały:

- ulotkę dla uczestników ze scenariuszem i miejscem na notatki,
- aktualny przewodnik opisujący sposób postępowania w sytuacjach związanych z bezpieczeństwem,
- wszelkie instrukcje dotyczące zasad i procedur,
- listę narzędzi i zewnętrznych usług.

Działania i pytania po ćwiczeniach:

- Co poszło dobrze?
- Co mogło pójść lepiej?
- Czy zabrakło jakichś usług lub procesów, które skróciłyby czas rozwiązywania problemu lub zwiększyłyby dokładność?
- Czy jakiekolwiek kroki są niepotrzebne lub nieistotne?
- Zidentyfikuj i udokumentuj problemy pod kątem działań naprawczych.
- Zmień odpowiednio plan na następny raz.

Szablony ćwiczeń symulacyjnych

Zbiór scenariuszy, prezentacji i ćwiczeń symulacyjnych, które mogą być wykorzystane jako szablony, można znaleźć na stronie Federalnej Agencji Zarządzania Kryzysowego (ang. *Federal Emergency Management Agency* — FEMA): *http://bit.ly/2lHuOVP*.

Powiększanie zespołu i poszerzanie zestawu umiejętności

Znalezienie oddanego, pełnego pasji i inteligentnego zespołu może być jednym z najtrudniejszych aspektów życia każdego profesjonalisty.

Co Ty i Twój zespół możecie zrobić, aby poszerzyć wiedzę i umiejętności?

- Zachęć personel do założenia domowego laboratorium lub zapewnij mu laboratorium. Może ono służyć do testowania rzeczywistych scenariuszy, a także do ćwiczenia umiejętności i uczenia się nowych. Laboratoria można tworzyć stosunkowo niskim kosztem, kupując używany sprzęt. Dla większości osób najlepszym sposobem nauki jest praktyka, a dzięki laboratorium unika się wprowadzania ryzyka do środowiska produkcyjnego.

- Organizuj gry typu „zdobądź flagę” (ang. *Capture the Flag* — **CTF**) i uczestnicz w nich. Takie gry stanowią wyzwania i mogą zapewniać szkolenia przekrojowe i umożliwić budowanie zespołu, a także zwiększać umiejętności komunikacyjne. Konkursy CTF (*https://ctftime.org*) odbywają się na większości konferencji dotyczących bezpieczeństwa informacji. Jeśli chcesz powiększyć zespół, „zdobądź flagę” to wspaniała okazja do szukanie nowych talentów. Uczestnicy prezentują nie tylko swój poziom wiedzy, ale także umiejętności komunikacyjne, zdolności do współpracy z innymi członkami zespołu oraz gotowość do pomocy i uczenia innych.
- Wyszukaj lub utwórz projekt. Zautomatyzuj coś w przedsiębiorstwie, znajdź jakąś potrzebę i ją zaspokój. Nie jest ważny zestaw umiejętności, ponieważ zawsze jest jakiś projekt, który potrzebuje pomocy. W przypadku co najmniej 99% istniejących projektów otwartego oprogramowania wymagana jest dokumentacja.
- Uczestnicz, organizuj, zgłaszaj się jako wolontariusz, przemawiaj, sponsoruj lub przeprowadzaj szkolenia na konferencjach branżowych lub lokalnych spotkaniach. Przykładowo, w Stanach Zjednoczonych są ich setki i prawie zawsze potrzebni są ochotnicy. Sam udział w konferencji ma swoje zalety, ale dopiero całkowite zaangażowanie się w jakieś wydarzenie zainspiruje Cię, żeby uczyć się i doświadczać więcej. Wiele karier zawodowych miało swój początek podczas zwykłej rozmowy o pasji w trakcie lunchu lub przy piwie. Sieci wprowadziły zmianę zasad gry w naszej branży, ale nie jest to złoty środek dla wszystkich. Możesz połączyć w sieć cokolwiek, ale jeśli nie jesteś pożądanym kandydatem, nie będzie to miało znaczenia. W tak szybko rozwijającej się branży idealne cechy to chęć do nauki, słuchania, współpracy oraz umiejętność samodzielnego myślenia.
- Bierz udział w mentoringu. Bez względu na to, czy sam jesteś mentorem, czy tylko jego podopiecznym, czy ten mentoring jest zorganizowany, czy nie, zawsze może być cennym procesem uczenia się zarówno w pracy, jak i poza nią.

Podsumowanie

Tworzenie programu bezpieczeństwa informacji nie jest łatwym zadaniem. Wiele programów jest zepsutych lub nie istnieje w praktyce, co potęguje ogólny brak bezpieczeństwa w środowisku przedsiębiorstw. Wykorzystaj tę książkę jako przewodnik do pracy nad różnymi obszarami i do tego, by dopasować je do szytego na miarę planu. Umiejętności organizacyjne, kompetentny, pracowity zespół, silne przywództwo i zrozumienie specyficznego środowiska będą kluczowe dla utworzenia skutecznego programu.

Skorowidz

Ć

D

E

F

G

H

I

O

P

R

S

T

U

V

W

X

Z

Notatki

O'REILLY®

Chcesz być bezpieczny, przygotuj się na atak!

Obecnie ataki na systemy informatyczne są prowadzone z wielu powodów i dokonywane przez różnych ludzi: od zorganizowanych grup przestępczych dążących do wzbogacenia się na kradzieży danych po haktywistów, których celem jest ukaranie organizacji uznawanych przez nich za niemoralne. Co gorsza, coraz częściej ataki są dziełem osób wykwalifikowanych i odpowiednio finansowanych. Systematycznie do mediów dostają się informacje o głośnych włamaniach hakerskich, rekordowych wyciekach danych czy atakach ransomware. Skutki tych incydentów bywają bardzo poważne. Wdrożenie przemyślanego programu bezpieczeństwa jest dziś koniecznością dla każdej firmy czy instytucji, która korzysta z rozwiązań informatycznych.

Ta książka jest praktycznym i pragmatycznym przewodnikiem po tematyce bezpieczeństwa. Znalazły się tu konkretne instrukcje, wskazówki, opis narzędzi i procesów, a także sporo pomysłów, dzięki którym można wdrożyć i utrzymać system bezpieczeństwa przy zerowych lub niewielkich nakładach. Inżynierowie sieci, administratorzy systemów i specjaliści ds. bezpieczeństwa dowiedzą się, jak radzić sobie z incydentami, zapewnianiem zgodności z przepisami, zarządzaniem infrastrukturą sieci i hasłami, skanowaniem luk w zabezpieczeniach i testami penetracyjnymi. Zagadnienia techniczne uzupełniono informacjami z zakresu inżynierii społecznej. Dzięki temu książka jest wyczerpującym, przydatnym kompendium dla każdego, kto zajmuje się na co dzień bezpieczeństwem systemu.

W tej książce znajdziesz między innymi:

- podstawy uruchamiania i przeprojektowywania programu InfoSec
- projektowanie reguł, standardów i procedur, wdrażanie systemu bezpieczeństwa
- zabezpieczanie systemów Microsoft i Unix oraz infrastruktury sieciowej
- praktyki i projekty segmentacyjne
- automatyzacja zarządzania lukami w zabezpieczeniach
- podstawowe koncepcje związane z testami penetracyjnymi

Lee Brotherston – zawodowo zajmuje się bezpieczeństwem systemów informatycznych od ponad dziesięciu lat. Problematykę tę poznał od podszewki w czasie pracy na różnych stanowiskach: od inżyniera zabezpieczeń po dyrektora ds. bezpieczeństwa. Pracował w wielu branżach, w tym w finansach, telekomunikacji, hotelarstwie, rozrywce i dla instytucji rządowych.

Amanda Berlin – co najmniej od dekady jest architektem bezpieczeństwa informacji. Pracuje dla firmy doradczej w północnym Ohio. Uczestniczyła we wdrażaniu standardu PCI, który ma zapewnić bezpieczne stosowanie kart płatniczych, oraz w budowie kompleksowego programu edukacyjnego na temat phishingu.

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 978-83-283-4722-9
9 788328 347229

INFORMATYKA W NAJLEPSZYM WYDANIU

Cena: 59,00 zł