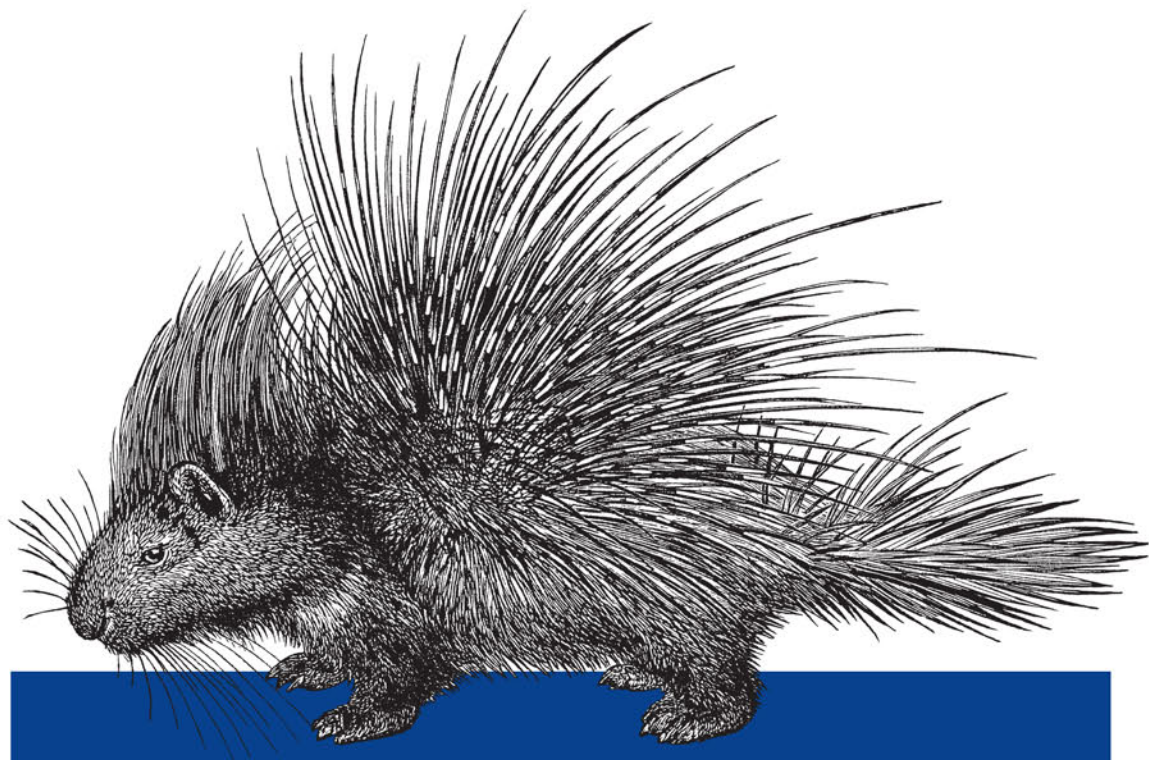




Bezpieczeństwo defensywne

PODSTAWY I NAJLEPSZE PRAKTYKI

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

Tłumaczenie: Lech Lachowski

ISBN: 978-83-283-4722-9

© 2018 Helion S.A.

Authorized Polish translation of the English edition of Defensive Security Handbook
ISBN 9781491960387 © 2017 Lee Brotherston and Amanda Berlin

This translation is published and sold by permission of O'Reilly Media, Inc.,
which owns or controls all rights to publish and sell the same.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means,
electronic or mechanical, including photocopying, recording or by any information storage retrieval system,
without permission from the Publisher.

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej
publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną,
fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje
naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich
właścicieli.

Autor oraz HELION SA dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne
i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym
ewentualne naruszenie praw patentowych lub autorskich. Autor oraz Wydawnictwo HELION nie ponoszą
również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych
w książce.

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.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

Spis treści

Przedmowa	11
Wstęp	13
1. Tworzenie programu bezpieczeństwa	19
Podwaliny	19
Definiowanie zespołów	20
Podstawowe podejście do systemu bezpieczeństwa	20
Ocena zagrożeń i ryzyka	21
Identyfikowanie	21
Ocena	22
Ograniczanie ryzyka	22
Monitorowanie	22
Nadawanie priorytetów	23
Tworzenie kamieni milowych	23
Przypadki użycia, ćwiczenia symulacyjne i praktyczne	24
Powiększanie zespołu i poszerzanie zestawu umiejętności	28
Podsumowanie	29
2. Zarządzanie aktywami i dokumentacja	31
Klasyfikacja informacji	31
Kroki wdrażania zarządzania aktywami	32
Definiowanie cyklu życia	32
Gromadzenie informacji	34
Śledzenie zmian	35
Monitorowanie i raportowanie	35
Wytyczne dotyczące zarządzania aktywami	36
Automatyzacja	36
Jedno źródło prawdy	36
Organizowanie międzywydziałowego zespołu	36
Przedstawiciele kadry kierowniczej	37

Licencjonowanie oprogramowania	37
Definiowanie aktywów	37
Dokumentacja	37
Sprzęt sieciowy	38
Sieć	39
Serwery	39
Komputery stacjonarne	39
Użytkownicy	39
Aplikacje	40
Inne	40
Podsumowanie	40
3. Reguły	41
Język	42
Treść dokumentu	42
Tematy	44
Przechowywanie i komunikacja	45
Podsumowanie	45
4. Standardy i procedury	47
Standardy	48
Język	48
Procedury	49
Język	49
Treść dokumentu	50
Podsumowanie	51
5. Edukowanie użytkowników	53
Niedziałające procesy	53
Niwelowanie różnic	54
Budowanie własnego programu	55
Wytyczanie celów	55
Ustalanie podstaw	55
Zakres i tworzenie reguł i wytycznych programu	56
Implementacja i dokumentowanie infrastruktury programu	56
Wprowadzanie pozytywnego czynnika	56
Grywalizacja	56
Definiowanie procesów reagowania na incydenty	57
Pozyskiwanie istotnych wskaźników	57
Pomiary	57
Śledzenie stopnia powodzenia i postępu	58
Ważne wskaźniki	58
Podsumowanie	58

6. Reagowanie na incydenty	59
Procesy	59
Procesy poprzedzające incydent	59
Procesy związane z incydentami	60
Procesy następujące po incydentach	62
Narzędzia i technologie	62
Analiza dzienników zdarzeń	63
Analiza dysków i plików	63
Analiza pamięci	64
Analiza PCAP	64
Wszystko w jednym	65
Podsumowanie	65
7. Odtwarzanie awaryjne	67
Ustalanie celów	67
Zakładany punkt odtworzenia	67
Zakładany czas odtworzenia	68
Strategie odtwarzania awaryjnego	68
Kopie zapasowe	68
Rezerwy dynamiczne	69
Duża dostępność	69
Alternatywny system	70
Zmiana przypisania funkcji systemu	70
Zależności	71
Scenariusze	71
Wywoływanie przełączania awaryjnego i powrót na systemy podstawowe	72
Testowanie	72
Kwestie bezpieczeństwa	73
Podsumowanie	74
8. Standardy zgodności z przepisami branżowymi a frameworki	75
Standardy zgodności z przepisami branżowymi	75
Standard bezpieczeństwa danych kart płatniczych (PCI DSS)	76
Ustawa o przenośności i odpowiedzialności w ubezpieczeniach zdrowotnych (HIPAA)	76
Ustawa Gramm-Leach-Bliley	77
Ustawa o prawach rodzinnych w zakresie edukacji i prywatności	78
Ustawa Sarbanesa-Oxleya	78
Frameworki	79
Cloud Control Matrix	79
Center for Internet Security	79
Control Objectives for Information and Related Technologies	79

The Committee of Sponsoring Organizations of the Treadway Commission	79
Seria ISO27000	80
Framework CyberSecurity instytutu NIST	80
Branże objęte przepisami	81
Sektor budżetowy	81
Sektor rządowy	81
Opieka zdrowotna	82
Podsumowanie	83
9. Bezpieczeństwo fizyczne	85
Aspekt fizyczny	85
Ograniczanie dostępu	85
Monitoring wideo	86
Utrzymywanie urządzeń uwierzytelniających	87
Bezpieczne media	87
Centra danych	89
Aspekt operacyjny	89
Identyfikacja osób odwiedzających i podwykonawców	89
Działania osób odwiedzających	89
Działania podwykonawców	89
Identyfikatory	90
Uwzględnij szkolenie z zakresu bezpieczeństwa fizycznego	90
Podsumowanie	92
10. Infrastruktura Microsoft Windows	93
Szybkie korzyści	93
Aktualizacja	93
Aktualizacja oprogramowania innych dostawców	94
Otwarte udziały	95
Usługi domenowe w usłudze Active Directory	95
Las	95
Domena	97
Kontrolery domen	97
Jednostki organizacyjne	98
Grupy	98
Konta	98
Obiekty reguł grupy	99
EMET	100
Podstawowa konfiguracja	101
Niestandardowa konfiguracja	103
Strategie wdrażania w przedsiębiorstwie	104

Serwer MS SQL	106
Gdy dostawcy zewnętrzni mają dostęp	106
Uwierzytelnienie MS SQL	107
Bezpieczeństwo użytkownika SA	107
Podsumowanie	108
11. Uniksowe serwery aplikacji	109
Aktualizowanie na bieżąco	110
Aktualizacje oprogramowania zewnętrznych dostawców	110
Podstawowe aktualizacje systemu operacyjnego	112
Zabezpieczanie uniksowego serwera aplikacji	113
Podsumowanie	118
12. Punkty końcowe	119
Aktualizowanie na bieżąco	119
Microsoft Windows	120
macOS	120
Uniksowe komputery stacjonarne	121
Aktualizacje oprogramowania zewnętrznych dostawców	121
Zabezpieczanie punktów końcowych	122
Wyłączanie usług	122
Firewalle osobiste	124
Szyfrowanie całego dysku	125
Narzędzia ochrony punktów końcowych	126
Zarządzanie urządzeniami mobilnymi	127
Widoczność punktów końcowych	127
Centralizacja	128
Podsumowanie	128
13. Zarządzanie hasłami i uwierzytelnianie wieloskładnikowe	129
Podstawowe praktyki postępowania z hasłami	129
Oprogramowanie do zarządzania hasłami	130
Resetowanie hasła	132
Naruszenie hasła	132
Szyfrowanie, mieszanie i solenie	133
Szyfrowanie	133
Mieszanie	133
Solenie	134
Lokalizacje i metody przechowywania haseł	135
Obiekty zabezpieczania hasłem	136
Definiowanie szczegółowych reguł haseł	136

Uwierzytelnianie wieloskładnikowe	140
Dlaczego 2FA?	140
Metody uwierzytelniania dwuskładnikowego	142
Jak to działa	142
Zagrożenia	142
Gdzie należy zaimplementować 2FA	143
Podsumowanie	143
14. Infrastruktura sieciowa	145
Aktualizowanie firmware'u i oprogramowania	145
Zabezpieczanie urządzeń	147
Usługi	147
SNMP	148
Protokoły szyfrowane	149
Sieć służąca do zarządzania	150
Routery	150
Przełączniki	151
Filtrowanie ruchu wychodzącego	152
IPv6: ostrzeżenie	153
TACACS+	153
Podsumowanie	154
15. Segmentacja	155
Segmentacja sieci	155
Podział fizyczny	155
Podział logiczny	156
Przykład sieci fizycznej i logicznej	162
Programowalna sieć komputerowa	162
Aplikacja	162
Role i obowiązki	164
Podsumowanie	166
16. Zarządzanie lukami w zabezpieczeniach	167
Jak działa skanowanie luk w zabezpieczeniach?	168
Skanowanie uwierzytelnione i niewierzytelnione	168
Narzędzia oceny luk w zabezpieczeniach	170
Program zarządzania lukami w zabezpieczeniach	171
Inicjowanie programu	171
Standardowe działania	172
Ustalanie priorytetów działań naprawczych	173
Akceptacja ryzyka	175
Podsumowanie	176

17. Rozwój oprogramowania	177
Wybór języka	177
0xAsembler	178
/* C i C++ */	178
GO func()	178
#!/Python/Ruby/Perl	179
<? PHP ?>	179
Wskazówki dotyczące bezpiecznego kodowania	180
Testowanie	181
Zautomatyzowane testy statyczne	181
Zautomatyzowane testy dynamiczne	181
Wzajemna ocena	182
Cykl rozwoju systemu	182
Podsumowanie	183
18. Fioletowy zespół	185
Biały wywiad	185
Rodzaje informacji i dostępu	185
Narzędzia białego wywiadu	188
Czerwony zespół	200
Podsumowanie	203
19. Systemy IDS i IPS	207
Rodzaje systemów IDS i IPS	207
Sieciowe systemy IDS (NIDS)	207
Systemy IDS oparte na hostach (HIDS)	208
Systemy IPS	209
Wycinanie hałasu	209
Pisanie własnych sygnatur	210
Lokalizowanie systemów NIDS i IPS	212
Protokoły szyfrowane	213
Podsumowanie	214
20. Rejestrowanie i monitorowanie	215
Co należy rejestrować?	215
Gdzie należy rejestrować?	216
Platforma SIEM	216
Projektowanie systemu SIEM	217
Analiza dzienników	218
Przykłady rejestrowania i alarmowania	218
Systemy uwierzytelniania	218
Dzienniki aplikacji	219
Dzienniki serwerów proxy i firewalli	220

Agregacja dzienników	220
Analiza przypadków użycia	221
Podsumowanie	221
21. Zestaw nadobowiązkowy	223
Serwery pocztowe	223
Serwery DNS	225
Bezpieczeństwo poprzez zaciemnienie	227
Przydatne zasoby	227
Książki	228
Blogi	228
Podkasty	228
Narzędzia	228
Strony internetowe	229
A Szablony do edukacji użytkowników	231
Skorowidz	237

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”. Próbuje z tym walczyć. Dlatego powiesiłam na ścianie zegar, którego wskazówki będą 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*), ochraniać (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 nieznanne 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 łączyć 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 dojdiesz 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 ugasileś 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 ilości 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 wyzwany 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 przeglądarkę 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. <i>Honey Directories</i> — 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 drobne 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 jakiegokolwiek 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 szukania 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 sztytu na miarę planu. Umiejętności organizacyjne, kompetentny, pracowity zespół, silne przywództwo i zrozumienie specyficznego środowiska będą kluczowe dla utworzenia skutecznego programu.

2FA, *Patrz*: uwierzytelnianie dwuskładnikowe

A

ACL, 32, 150, 158

action on objectives, *Patrz*: działania na celach

Active Directory, *Patrz*: AD DS

AD DS, 95, 100

 baza danych, 97

 las, *Patrz*: las Active Directory

adres IP zarezerwowany, 34

aktywa

 cykl życia, 32

 definiowanie, 37

 firmy, 185, 186

 monitorowanie, 32, 33, 35, 38

 raportowanie, 32, 35, 38

 śledzenie zmian, 32, 35

 zarządzanie, *Patrz*: zarządzanie aktywami

alarm, 209, 210

algorytm szyfrowania, 133, 134

aplikacja, 162

 dziennik, *Patrz*: dziennik aplikacji

 serwer, *Patrz*: serwer aplikacji

architektura AAA, 153

atak, 53

 brute force, *Patrz*: atak siłowy

 celem, 25

 DDoS, 24

 DDoS Amplification, 149

 DoS, 145

 man-in-the-middle, 151

 na serwer lub usługę, 103

 nieuchronność, 56

 niezadowolony pracownik, 24

 phishing, *Patrz*: phishing

 po stronie klienta, 103

 pomijanie, 213

 rejestrowanie, *Patrz*: rejestrowanie

 siłowy, 129, 130, 134, 221

 słownikowy, 129

 tęczowa tablica, 129, 130

 zapobieganie, 24, 185, 207, 209, 212, 227

audyt roczny, 32

autoryzacja, 154

B

badanie due diligence, 23

baza danych rozproszona, *Patrz*: dane rozproszone

BCP, 67, 71, 72

bezpieczeństwo, 188

 fizyczne, 85, 186

 bezpieczne media, 87, 88

 centrum danych, 89

 monitoring wideo, 86

 szkolenie, 90

 urządzenia uwierzytelniające, 87

 ograniczenie dostępu, 86, 118

 poprzez zaciemnienie, 227

BitLocker, 125

Bro, 208

business continuity planning, *Patrz*: BCP

BYOD, 36, 160

C

C2, 25, 27

CAINE, 65

Capture the Flag, *Patrz*: CTF

cardholder data, *Patrz*: CHD

Center Configuration Manager, *Patrz*: SCCM

Cerber, 27

CHD, 76
chmura, 79
command and control, *Patrz:* C2
Common Vulnerability Scoring System, *Patrz:* CVSS
Cross Domain and Forest Trust, *Patrz:* las
CryptoWall, 27
CTF, 29
CTSS, 129
CVSS, 173
Cyber Kill Chain, *Patrz:* łańcuch niszczenia intruzów
cyberatak, 79
cykl rozwoju systemu, *Patrz:* SDLC
czas odtworzenia zakładany, *Patrz:* RTO

Ć

ćwiczenie, 231
 symulacyjne, 25, 27
 materiały, 28
 moderator, 25
 szablon, 28
 uczestnicy, 25, 28

D

dane
 dostępność, 73
 eksfiltracja, 24, 25, 152, 188, 220, 221
 klientów, 188
 kluczowe, 32, 37
 krytyczne, 37
 naruszenie integralności, 25
 osobowe, 156, 185, 188
 uczniów, 78
 posiadaczy kart, *Patrz:* CHD
 poufne, 88
 przenoszone, 73
 rozproszone, 95
 sprawdzanie poprawności, 180
 telemetryczne, 215
 w chmurze, 79
 w spoczynku, 73
 wrażliwe, 32, 37, 156
 szyfrowanie, 125
 źródła, 32
DC, 97
Decrytonite, 27

defense in depth, *Patrz:* obrona w głąb
delivery, *Patrz:* dostarczenie
disaster recovery, *Patrz:* DR
DMZ, 156, 212
dokument Microsoft Office, 24, 26
domena, 97, 136
 kontroler, 97, *Patrz:* DC
 serwer strefy DNS, *Patrz:* serwer strefy DNS
 domeny
dostarczenie, 24, 26
DR, 67, 72
 koszt, 68
 strategia, 68, 70, 71
 testowanie, 72
działanie na celach, 25, 27
dziennik, 215
 agregacja, 220
 analiza, 63, 218, 220, 221
 logowanie, 218
 aplikacji, 219
 firewalla, 220
 lokalizacja, 216
 proxy, 26
 serwerów proxy, 220
 zdarzeń, 210
dziennik zdarzeń, 63, 210

E

Ebbinghausa krzywa zapominania, 54
eksploatacja, 25, 26
e-mail, 24
 do celów prywatnych, 26
 phishing, *Patrz:* phishing
 załącznik, 26
EMET, 100, 104
 konfiguracja, 101, 102, 103
 obejście, 101
 wsparcie, 100
emulator PDC, 97
encryption, *Patrz:* szyfrowanie
Enhanced Mitigation Experience Toolkit, *Patrz:* EMET
Ethernet Tap, 208
Ethertap, 208
exploit, 24, 26, 100
 wyszukiwanie Google, 188
exploitation, *Patrz:* eksploatacja

F

FERPA, 78
FGPP, 136
firewall, *Patrz:* zaporę ogniową
firmware, 145
Flexible Single Master Operation, *Patrz:* FSMO
framework
 CCM, 79
 CIS, 79
 COBIT, 78
 COSO, 78, 79
 CyberSecurity, 80
 dla celów zabezpieczania krytycznej
 infrastruktury, 79
 NIST, 19, 100
 OCTAVE, 20
 Volatility, *Patrz:* narzędzie Volatility
FSMO, 97

G

GC, 97
GHDB, 197, 198
GLBA, 77
Global Catalog, *Patrz:* GC
Google Dorking, 188
Google Hacking Database, *Patrz:* GHDB
GPO, 98, 99, 135
gra, *Patrz też:* grywalizacja
 zdobądź flagę, 29
gromadzenie informacji, 32, 34
Group Policy Object, *Patrz:* GPO
grupa
 AD, 98
 NIST, 100
 obiekt reguł, *Patrz:* GPO
grywalizacja, 56, *Patrz też:* gra

H

Harvester, 197
hashing, *Patrz:* mieszanie
hasło, 129
 administrowanie, 99
 łamanie, 130
 przechowywanie, 135
 resetowanie, 26, 132
 skrót, 129, 130, 133

zarządzanie, 129, 135, 136
 menedżer, *Patrz:* menedżer haseł
HIDS, 208
HIPAA, 77
host-based IDS, *Patrz:* HIDS
HVAC, 128

I

identyfikator, 89, 90
 klonowanie, 91
 SID, 98
identyfikowanie, 19, 21, 167, 207, 213, 215, 221,
 Patrz też: alarm
IDS, 207, 213
 konfiguracja, 209, 210
 oparty na hostach, *Patrz:* HIDS
 sieciowy, *Patrz:* IDS
incident response, *Patrz:* IR
incydent
 awaria sprzętowa, 71
 definiowanie, 60
 kierownik, 60
 komunikacja
 wewnętrzna, 60
 zewnętrzna, 61
 pandemia, 71
 reagowanie, *Patrz:* IR
 utrata centrum danych, 71
informacji gromadzenie, 32, 34
instalacja, 25, 27
installation, *Patrz:* instalacja
interfejs HTTP, 148
intrusion detection system, *Patrz:* IDS
Intrusion Kill Chain, *Patrz:* łańcuch niszczenia
 intruzów
intrusion prevention system, *Patrz:* IPS
inżynieria społeczna, 85, 132
 szkolenie, 90
IPS, 207, 209, 212, 213
 konfiguracja, 209, 210
IR, 56, 57, 59, 60, 61, 62
 analiza
 artefaktów, 63, 64, 65
 dysków, 63, 64
 dzienników zdarzeń, 63
 pamięci, 64
 PCAP, 64, 65
 plików, 63

J

jednostka organizacyjna, *Patrz:* OU
język programowania, 177, 178, 179

K

kamień milowy, 23
kanał C2, 25, 27
katalog globalny, *Patrz:* GC
klasa informacyjna, 32
klasyfikacja informacji, 31, 32
klatka chroot, 117
kod
 język programowania, *Patrz:* język programowania
 przegląd, 182
 testowanie, *Patrz:* test
 wykonanie zdalne, *Patrz:* RCE
 zajemna ocena, *Patrz:* kod przeglądu
konto użytkownika, 98
kontroler domeny, *Patrz:* DC
kopia zapasowa, 27, 68, 69, 73, 87
 alternatywa, 70
krzywa zapomnienia Ebbinghausa, 54

L

LAPS, 99
las, 96
 Active Directory, 95
 serwer strefy DNS, *Patrz:* serwer strefy DNS lasu
LinkedIn, 26
lista
 ACL, *Patrz:* ACL
 kontroli dostępu, *Patrz:* ACL
Local Administrator Password Solution, *Patrz:* LAPS
Long Johnny, 198
Lucky, 27
luka
 systemu operacyjnego, 25, 93, 135, 136
 w zabezpieczeniach, *Patrz:* skanowanie luk aplikacji, 25
 kodu, 179, 180

Ł

łańcuch niszczenia
 cybernetyczny, *Patrz:* łańcuch niszczenia intruzów intruzów, 24, 25

M

MAC, 118
Maltego, 189
Mandatory Access Control, *Patrz:* MAC
maszyna wirtualna, 32
Matherly John, 199
MDM, 127
media społecznościowe, 188
menedżer haseł, 131
mentoring, 29
MFA, *Patrz:* uwierzytelnianie wieloskładnikowe
Microsoft Office, 24, 26
Microsoft Windows, 93
Microsoft Windows Update, 120
mieszanie, 133
milestone, *Patrz:* kamień milowy

N

NAC, 159
narzędzie, 228
 Autopsy, 64
 awk, 63
 białego wywiadu, *Patrz:* OSINT narzędzia
 Bro, 208
 chroot, *Patrz:* klatka chroot
 cut, 63
 EMET, *Patrz:* EMET
 grep, 63, 65
 NIDS, 208
 nmap, 34, 95
 oceny luk w zabezpieczeniach,
 Patrz: skanowanie luk narzędzia
ochrony punktów końcowych, 126
PhotoRec, 64
PowerShell, *Patrz:* PowerShell
Rawr, 201
Responder, 201
Security Onion, 208
sed, 63, 65
SID Walker, 98
Snort, 208, 211
Suricata, 208, 211
tcpdump, 65
The Sleuth Kit, 64
tshark, 65
Volatility, 64
Wireshark, 65

Netdisco, 34, 38
network-based IDS, *Patrz:* NIDS
NIDS, 207, 208, 212
nośnik USB, 24

O

obiekt
 reguł grupy, *Patrz:* GPO
 zabezpieczenia hasłem, *Patrz:* PSO
obrona w głąb, 85
 sekcja
 fizyczna, *Patrz:* bezpieczeństwo fizyczne
 operacyjna, 85, 89
ochronianie, 19
odtworzenie, 19
 awaryjne, *Patrz:* DR
open source intelligence, *Patrz:* OSINT
oprogramowanie
 aktualizacja, 94, 121, 122
 do łamania haseł, 129, 130
 do zarządzania aktywami, *Patrz:* zarządzanie
 aktywami oprogramowanie
 do zarządzania poprawkami, *Patrz:* SCCM,
 zarządzanie poprawkami
 firewall, *Patrz:* zapora ogniowa
 oprogramowanie
 licencjonowanie, 37
 ransomware, 24, 26, 27
 złośliwe APT, 25
organizacji profil, *Patrz:* profil organizacyjny
Organizational Unit, *Patrz:* OU
OSINT, 185
 aktywa firmy, 185, 186
 dane osobiste, 185, 188
 narzędzia, 188, 189, 191, 193, 195, 197
 technologie, 185, 187
 zasoby fizyczne, 185, 186
OU, 95, 98

P

pamięć podręczna ARP, 34
password security object, *Patrz:* PSO
PCAP, 65
PCI, 217
PCI DSS, 76
phishing, 26, 53, 234
planowanie ciągłości działania, *Patrz:* BCP

plik
 dostęp na podstawie procesu, 27
 EMET.dll, 100
 JavaScript, 26
 ntds.dit, 97
 PDF, 24
 przechwytywania pakietów, *Patrz:* PCAP
 szyfrowanie, 27
 zarządzanie integralnością, *Patrz:* zarządzanie
 integralnością plików
polecenie WMIC, 35
port
 lustrzany, 207
 SPAN, 151
 TCP, 147
PowerShell, 34, 95, 100
pretexting, 188
procedura, 47, 49, 87
 język, 49
 reagowania na zdarzenia, *Patrz:* IR
 wersja, 50
proces, 87
 po incydencie, 62
 poprzedzający incydent, 59, 60
 reagowania na incydenty, *Patrz:* IR
 zarządzania aktywami, *Patrz:* zarządzanie
 aktywami
Process Explorer, 123
Process Monitor, 123
profil organizacyjny, 26
program
 bezpieczeństwa, 19, 20
 cel, 55
 dokumentowanie, 56
 implementacja, 56
 koszty, 23
 plan, 55
 szkolenie, *Patrz:* szkolenie
 tworzenie, 55, 57
 wskaźniki, *Patrz:* wskaźnik
 zespół, *Patrz:* zespół
 Netdisco, *Patrz:* Netdisco
protokół
 6in4, 153
 6rd, 153
 6to4, 153
 802.1X, 159
 DHCP, 34
 dynamicznego routingu, 151

- protokół
 - IEEE 802.1, 159
 - in4, 153
 - IPv4, 153
 - IPv6, 153
 - SNMP, 34, *Patrz:* SNMP
 - szyfrowany, 149
 - Teredo, 153
- przełączanie awaryjne, 72
- przełącznik, 151, 157
- PSO, 136, 138
- pułapka, 27
- punkt
 - końcowy, 21, 23, 26, 35, 90, 91, 119, 120, 128, 157, 213
 - ochrona, 126
 - widoczność, 127
 - zabezpieczanie, 122
- odtworzenia
 - zakładany, *Patrz:* RPO
- wejściowy, 156
- wyjściowy, 156

R

- ransomware, 221
- Rawr, 201
- RCE, 103
- reagowanie, 19
- reconnaissance, *Patrz:* rozpoznanie
- recon-ng, 191, 193, 195
- recovery point objective, *Patrz:* RPO
- recovery time objective, *Patrz:* RTO
- reguła, 41
 - czystego biura, 44
 - domenowa, 99
 - dotycząca
 - konstrukcji haseł, 44
 - planu reakcji na zagrożenia, 44
 - poczty elektronicznej, 44
 - dystrybucja, 41
 - hasel, 136, *Patrz też:* FGPP
 - instalacji oprogramowania, 45
 - lokalna, 99
 - monitorowanie, 43
 - ochrony haseł, 44
 - przechowywanie, 45
 - ról FSMO, 97
 - spójność, 41, 43

- standard, *Patrz:* standard
- szyfrowania, 44
- tworzenie, 42, 56
- usuwania sprzętu technologicznego, 44
- użytkowania, 44
- wdrożenie, 43
- wersja, 42
- właściciel, 43
- zakres, 43, 44, 56
- zatwierdzanie, 42
- zdalnego dostępu, 44
- zmiana, 42, 43
- rejestrowanie, 215
- miejsce, 216, *Patrz też:* dziennik
- zakres, 215
- remote code execution, *Patrz:* RCE
- Responder, 201
- rezerwa dynamiczna, 69, 73
 - RPO, *Patrz:* RPO rezerw dynamicznych
 - RTO, *Patrz:* RTO rezerw dynamicznych
- router, 155, 155
- rozpoznanie, 24, 26
- RPO, 67, 68, 70
 - koszt, 68
 - rezerw dynamicznych, 69
- RTO, 68, 70
 - rezerw dynamicznych, 69
- ryzyko
 - akceptowanie, 22, 175
 - monitorowanie, 22, 169
 - ograniczanie, 22
 - przenoszenie, 22
 - renegocjowanie, 22, 23
 - unikanie, 22, 167

S

- salting, *Patrz:* solenie
- SCCM, 36, 94, 104
- scenariusz, 72
 - awaria sprzętowa, 71
 - pandemia, 71
 - utrata centrum danych, 71
 - zagrożenia, 217
- SDLC, 182
- SDN, 162
- Security Information and Event Management,
Patrz: SIEM
- Security Onion, 208

- SELinux, 118
- serwer
 - aplikacji, 109, 113
 - DNS, 225
 - pocztowy, 223
 - proxy, 26
 - dziennik, 220
 - SQL, 106
 - SA, 107
 - uwierzytelnianie, 107
 - strefy DNS, 97
- Shodan, 197, 199
- sieć
 - fizyczna, 162, 164
 - gościnna, 156
 - logiczna, 162, 164
 - programowalna, *Patrz:* SDN
 - rozwojowa, 156
 - segmentacja, 155, 164
 - logiczna, 156, 157
 - testowa, 156
 - VLAN, 157
 - zawierająca wrażliwe dane, 156
 - zdemilitaryzowana, *Patrz:* DMZ
- SIEM, 63, 216, 217, 218
 - projektowanie, 217
- sinkhole DNS, 27
- skaner, 38
 - luk w zabezpieczeniach, 35
- skanowanie
 - luk, 167, 168, 172
 - akceptacja ryzyka, 175
 - narzędzia, 170, 171
 - nieuwierzytelnione, 168, 170
 - priorytety, 173, 174
 - program zarządzania, 171, 172
 - uwierzytelnione, 168, 169
- SNMP, 148, 151
 - dostęp, 149
- Snort, 208, 211
- Software Update Service, 120
- Software-Defined Networking, *Patrz:* SDN
- solenie, 134
- SOX, 78
- sól, 134
- spoofing, 149
- stacja bazowa ufortyfikowana, 150
- standard, 47, 48
- bezpieczeństwa danych kart płatniczych,
 - Patrz:* PCI DSS
- HIPAA, 157
- ISO, 80
- język, 48
- PCI DSS, 157
- wersja, 50
- zgodności, 19, 31, 75, 80
 - branżowych, 75, 80, 81, 82
 - FERPA, 78
 - GLBA, 77
 - HIPAA, 76
 - SOX, 78
- stos LAMP, 164
- Suricata, 208, 211
- system
 - alternatywny, 70
 - cykl rozwoju, *Patrz:* SDLC
 - dostępność wysoka, 70
 - dzielenia czasu, 129
 - operacyjny
 - aktualizacja, 93, 94, 112, 113, 120, 121
 - Debian Linux, 110, 111
 - FreeBSD, 110
 - Linux, 126
 - luka, *Patrz:* luka systemu operacyjnego
 - macOS, 120, 125
 - Microsoft Windows, *Patrz:* Microsoft Windows
 - SUSE Linux, 110
 - Unix, 110, 112, 121, 123, 124
 - wykrywania włamań, *Patrz:* IDS
 - zależności, 71
 - zapobiegania włamaniom, *Patrz:* IPS
 - zarządzania pakietami, 110
 - zmiana przypisania funkcji, 70
- System Center Configuration Manager, *Patrz:* SCCM
- szkolenie, 53, 54, 56
 - CBT, 53, 54
 - na temat
 - bezpieczeństwa fizycznego, *Patrz:* bezpieczeństwo fizyczne szkolenie
 - inżynierii społecznej, *Patrz:* inżynieria społeczna szkolenie
 - powtarzanie, 54, 56
 - SDLC, 182
- szyfr, 133

szyfrowanie, 32, 133
algorytm, *Patrz:* algorytm szyfrowania
dysków, 125, 126

T

tablica tęczowa, 130
TACACS+, 153
telewizja przemysłowa, 86
test, 181
dynamiczny, 181
ofensywny, 200
penetracyjny, 167, 171, 201
porównawczy, 79
statyczny, 181
Tomes Tim, 191
TPM, 98
triada CIA, 67
trojan zdalnego dostępu, 24
Trusted Platform Module, *Patrz:* TPM
TrustedBSD, 118

U

urządzenie sieciowe, 157
filtrowanie ruchu wychodzącego, 152
port, 147, 149
przełącznik, 151
router, 150
zabezpieczanie, 147, 149, 150, 151, 153
usługa
Active Directory, *Patrz:* AD DS
zarządzanie, *Patrz:* zarządzanie usługami
ustawa
Gramm-Leach-Bliley, *Patrz:* GLBA
o prawach rodzinnych w zakresie edukacji
i prywatności, 78
o przenośności i odpowiedzialności
w ubezpieczeniach zdrowotnych, *Patrz:* HIPAA
Sarbanesa-Oxleya, *Patrz:* SOX
uwierzytelnianie, 32, 154
dwuskładnikowe, 131, 132, 140, 143
metody, 142
SMS, 142
standard, 142
zagrożenia, 142, 143
rejestrowanie, 218
wieloskładnikowe, 140

uzbrojenie, 24, 26
użytkownik
konto, *Patrz:* konto użytkownika
obowiązk, 164
rola, 164, 165
uprawnienia, 99, 114, 156, 157, 165

V

VLAN, 151, 157, 158
VPN, 160
IPSec, 160
SSL/TLS, 160, 161

W

weaponization, *Patrz:* uzbrojenie
Weiss Kenneth, 140
wiadomość e-mail, *Patrz:* e-mail
Windows, *Patrz:* Microsoft Windows
Windows Server Update Services, *Patrz:* WSUS
Windows Update for Business, 120
WordPress, 35
wskaźnik, 57, 58
WSUS, 94
wydawanie poleceń i kontrolowanie, *Patrz:* C2
wykrywanie, 19
wywiad biały, *Patrz:* OSINT
wzorzec, 97

X

XFENCE, 27

Z

zagrożenie
identyfikowanie, *Patrz:* identyfikowanie
ocena, 22
priorytet, 23, 217
rejestrowanie, *Patrz:* rejestrowanie
scenariusz, 217
sektor
finansowy, 81
ochrony zdrowia, 82
rządowy, 81
wewnętrzne, 24
wskaźniki, 173

zapora
 ogniowa, 22, 32, 37, 115, 155, 157
 dziennik, 220
 oprogramowanie, 115
 osobista, 124
 wdrażanie, 157
 Windows, 124
 sieciowa, 22, 155, 157
 systemu plików, 27

zarządzanie
 aktywami, 31, 32, 35, 36, 94
 automatyzacja, 36
 dokumentacja, 37
 oprogramowanie, 35, 36, 37
 wdrażanie, 32
 hasłami, *Patrz:* hasło zarządzanie
 integralnością plików, 116
 lukami, *Patrz:* luka w zabezpieczeniach
 pakietami, 110
 poprawkami, 104, 110, 111, 120, 121, 122
 firmware, 145, 146, 147
 sieć dedykowana, 150
 urządzeniami mobilnymi, *Patrz:* ochrony
 usługami, 113, 114
 wyłączanie, 122, 123

zespół, 20
 audytujący, 20
 czerwony, 16, 185, 200
 ds. bezpieczeństwa, 20
 ds. ryzyka, 20
 fioletowy, 16, 185
 niebieski, 16, 185, 201
 wykonawczy, 20
 zarządzający aktywami, 36, 37

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

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 hakywistów, 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.pl  HELION SA ul. Kościuszki 1c 44-100 Gliwice tel.: 32 230 98 63 helion@helion.pl	<i>Sprawdź nasze szkolenia!</i>  AKADEMIA IT & BUSINESS WWW.SZKOLENIA.HELION.PL	KOD KORZYŚCI <i>Ściągnij po więcej!</i>  ISBN 978-83-283-4722-9  9 788328 347229 Cena: 59,00 zł
---	---	--

INFORMATYKA W NAJLEPSZYM WYDANIU