

Spis treści |

O autorze	11
O korektorze merytorycznej	12
Przedmowa	13
Wstęp	15
ROZDZIAŁ 1	
Wprowadzenie	19
Różne typy (spektrum) CISO	21
Jak przedsiębiorstwa ulegają pierwszym atakom i podstawy cyberbezpieczeństwa	23
Niezałatane luki w zabezpieczeniach	24
Błędy w konfiguracji	26
Słabe, ujawnione i wykradzione poświadczenia	28
Socjotechnika	30
Zagrożenia wewnętrzne	31
Koncentracja na podstawach cyberbezpieczeństwa	32
Różnice między motywacją a taktyką hakera	33
Podsumowanie	36
Przypisy	36
ROZDZIAŁ 2	
Co trzeba wiedzieć o analizie zagrożeń?	38
Czym jest analiza zagrożeń?	38
Skąd pochodzą dane CTI?	39
Korzystanie z analiz zagrożeń	41
Klucz do korzystania z analizy zagrożeń	44
Udostępnianie analiz zagrożeń	45
Protokoły udostępniania analiz CTI	46
Powody nieudostępniania analiz CTI	49

Jak sprawdzać wiarygodność analiz CTI?	50
Źródła danych	50
Skala czasu	51
Rozpoznawanie szumu	52
Przewidywanie przyszłości	52
Motywy dostawców	53
Podsumowanie	53
Przypisy	54

ROZDZIAŁ 3

Wykorzystanie trendów podatności

w celu zmniejszenia ryzyka i kosztów

Wprowadzenie	55
Podstawy zarządzania lukami w zabezpieczeniach	57
Źródła informacji o ujawnianych lukach w zabezpieczeniach	65
Trendy w ujawnianiu luk w zabezpieczeniach	65
Trendy dotyczące luk w zabezpieczeniach dostawców i produktów	72
Zmniejszanie ryzyka i kosztów: mierzenie usprawnień dostawców i produktów	75
Trendy dotyczące luk w systemach operacyjnych	87
Trendy dotyczące luk w przeglądarkach	99
Podsumowanie planu zmniejszania podatności na ataki	102
Wskazówki dotyczące zarządzania lukami w zabezpieczeniach	103
Podsumowanie	106
Przypisy	107

ROZDZIAŁ 4

Ewolucja szkodliwego oprogramowania

Wprowadzenie	113
Dlaczego dla Windows jest znacznie więcej szkodliwego oprogramowania niż dla innych systemów operacyjnych?	115
Źródła danych	116
Malicious Software Removal Tool	116
Narzędzia antywirusowe działające w czasie rzeczywistym	118
Źródła danych niezwiązane z bezpieczeństwem	119
O szkodliwym oprogramowaniu	119
Jak rozprzestrzenia się szkodliwe oprogramowanie	120
Trojany	121
Potencjalnie niechciane oprogramowanie	122
Eksploity i zestawy exploitów	123
Robaki	124

Ransomware	126
Wirusy	127
Modyfikatory przeglądarek	128
Wskaźniki rozpowszechnienia szkodliwego oprogramowania	128
Globalna analiza infekcji systemów Windows szkodliwym oprogramowaniem	129
Regionalna analiza infekcji systemów Windows szkodliwym oprogramowaniem	132
Obraz zagrożeń na Bliskim Wschodzie i w Afryce Północnej	135
Obraz zagrożeń w Unii Europejskiej i Europie Wschodniej	138
Obraz zagrożeń w wybranych krajach Azji i Oceanii	142
Obraz zagrożeń w wybranych krajach obu Ameryk	146
Wnioski z regionalnej analizy infekcji systemu Windows szkodliwym oprogramowaniem	149
Co to wszystko oznacza dla specjalistów CISO i zespołów ds. bezpieczeństwa w organizacjach?	150
Globalna ewolucja szkodliwego oprogramowania	151
Wnioski dotyczące globalnej ewolucji szkodliwego oprogramowania	156
Ewolucja oprogramowania ransomware	157
Mechanizmy rozpowszechniania	160
Mechanizmy działania	161
Metody płatności	162
Żądania okupu i komunikacja	163
Model biznesowy	164
Wielki dylemat: Czy rzeczywiście warto stosować rozwiązania chroniące przed szkodliwym oprogramowaniem?	165
Podsumowanie	167
Przypisy	167

ROZDZIAŁ 5

Zagrożenia internetowe	173
Wprowadzenie	173
Typowy atak	174
Ataki phishingowe	175
Obrona przed phishingiem	180
Ataki drive-by download	182
Obrona przed atakami drive-by download	184
Strony hostujące szkodliwe oprogramowanie	185
Obrona przed stronami rozpowszechniającymi szkodliwe oprogramowanie	186

Po włamaniu: botnety i ataki DDoS	187
Podsumowanie	190
Przypisy	191

ROZDZIAŁ 6

Role instytucji rządowych w cyberbezpieczeństwie 194

Dążenie do szczęćcia	195
Rząd jako uczestnik rynku cyberbezpieczeństwa	198
Rząd jako organ normalizacyjny	199
Rząd jako egzekutor prawa	203
Organ regulacyjny	203
Egzekwowanie prawa	205
Rząd jako obrońca	207
Bezpieczeństwo publiczne	208
Bezpieczeństwo kraju	208
Wojsko	210
Podsumowanie	213
Przypisy	213

ROZDZIAŁ 7

Dostęp instytucji rządowych do danych 217

Istota dostępu instytucji rządowych do danych	219
Scenariusz wywiadu sygnałowego	219
Scenariusz nielegalnego dostępu instytucji rządowych do danych	220
Scenariusz legalnego dostępu instytucji rządowych do danych	221
Legalny dostęp instytucji rządowych do danych	222
Ustawy CLOUD i PATRIOT	226
Kontrolowanie ryzyka dostępu instytucji rządowych do danych	231
Ograniczanie instytucjom rządowym dostępu do danych	250
Ustalenie i zrozumienie zakresu	250
Wyznaczenie realistycznych celów	251
Planowanie środków ochrony danych	252
Wnioski	256
Podsumowanie	257
Przypisy	258

ROZDZIAŁ 8**Elementy skutecznej strategii cyberbezpieczeństwa 264**

Czym jest strategia cyberbezpieczeństwa?	264
Inne elementy skutecznej strategii	268
Dopasowanie do celów biznesowych	268
Wizja, misja i imperatywy cyberbezpieczeństwa	269
Wsparcie kierownictwa wyższego szczebla i zarządu	270
Określenie tolerancji ryzyka	271
Prawdziwy obraz obecnych możliwości w zakresie cyberbezpieczeństwa i kompetencji technicznych	272
Dostosowanie programu zgodności i procedur kontrolnych	273
Efektywna relacja pomiędzy działami cyberbezpieczeństwa i IT	275
Kultura bezpieczeństwa	277
Podsumowanie	277
Przypisy	278

ROZDZIAŁ 9**Strategie cyberbezpieczeństwa 279**

Wprowadzenie	279
Ocena skuteczności strategii cyberbezpieczeństwa	281
Strategie cyberbezpieczeństwa	285
Strategia ochrony i odzyskiwania danych	286
Ocena strategii	288
Podsumowanie strategii ochrony i odzyskiwania danych	290
Strategia ochrony endpointów	290
Ocena strategii	293
Podsumowanie strategii ochrony endpointów	294
Strategia kontroli fizycznej i poświadczeń bezpieczeństwa	295
Ocena strategii	299
Podsumowanie strategii kontroli fizycznej i poświadczeń bezpieczeństwa	300
Strategia zgodności z normami	301
Ocena strategii	303
Podsumowanie strategii zgodności z normami	303
Strategia orientacji na aplikacje	304
Ocena strategii	306
Podsumowanie strategii orientacji na aplikacje	306
Strategia orientacji na tożsamość	307
Ocena strategii	309
Podsumowanie strategii orientacji na tożsamość	310

Strategia orientacji na dane	311
Ocena strategii	315
Podsumowanie strategii orientacji na dane	316
Strategia orientacji na ataki	317
Ocena strategii	319
Podsumowanie strategii orientacji na ataki	320
Strategia „zero zaufania”	321
Ocena strategii	324
Podsumowanie strategii bezpieczeństwa	326
Metodyki DevOps i DevSecOps	327
Podsumowanie	329
Przypisy	330

ROZDZIAŁ 10

Wdrażanie strategii	332
Wprowadzenie	332
Co to jest hakerski łańcuch zabójstw?	333
Modyfikacja hakerskiego łańcucha zabójstw	336
Mapowanie typowych sprawców cyberzagrożeń	336
Modyfikacja tabeli	337
Hakerski łańcuch zabójstw czy ATT&CK?	338
Pierwsze kroki	340
Dojrzałość bieżących funkcji cyberbezpieczeństwa	340
Rozpowszechnienie bieżących funkcji cyberbezpieczeństwa	342
Kto wykorzystuje dane?	342
Odnawianie licencji na funkcje cyberbezpieczeństwa	343
Implementacja strategii	344
Optymalizowanie tabeli: luki, niedoinwestowanie i przeinwestowanie ...	346
Planowanie wdrożenia	348
Projektowanie zestawów środków zaradczych	350
Faza Rozpoznanie I	351
Faza Dostawa	354
Faza Eksploatacja	359
Faza Instalacja	363
Faza Dowodzenie i kontrola	373
Faza Rozpoznanie II	376
Faza Operacje na celach	380
Wnioski	384
Podsumowanie	385
Przypisy	386

ROZDZIAŁ 11**Ocena wydajności i skuteczności strategii cyberbezpieczeństwa 388**

Wprowadzenie	388
Zastosowania danych o lukach w zabezpieczeniach	390
Zasoby zarządzane w porównaniu ze wszystkimi zasobami	391
Znane niezatacane luki w zabezpieczeniach	393
Klasyfikacja niezatacanych luk według wag	394
Klasyfikacja niezatacanych luk według typów produktów	395
Ocena wydajności i skuteczności strategii orientacji na ataki	396
Rekonstrukcja włamania	397
Zastosowanie wyników rekonstrukcji	403
Zastosowanie modelu ATT&CK do symulowania aktywności hakerów	408
Podsumowanie	409
Przypisy	410

ROZDZIAŁ 12**Nowoczesne podejście do bezpieczeństwa i zgodności 412**

Wprowadzenie	413
W czym chmura obliczeniowa jest inna?	414
Dostawcy CSP i MSP	415
Migracja do chmury	416
Kwestionariusze oceny cyberbezpieczeństwa	417
Zmiany w zakresie bezpieczeństwa i zgodności ze standardami	418
Siła interfejsów API	418
Zalety automatyzacji	423
Zmiany w podejściu do bezpieczeństwa i zgodności ze standardami — podsumowanie	428
Strategia cyberbezpieczeństwa w chmurze	429
Strategia ochrony i odzyskiwania danych w chmurze	430
Strategia zgodności z normami w chmurze	430
Strategia orientacji na ataki w chmurze	432
DevOps — nowoczesne podejście do bezpieczeństwa w chmurze	433
Odtwarzanie awaryjne w chmurze	437
Szyfrowanie danych i zarządzanie kluczami	438
Wnioski	442
Podsumowanie	442
Przypisy	443