

Spis treści

O autorach	13
Wstęp	15
Podziękowania	17
Wprowadzenie	19

CZĘŚĆ I Przygotowywanie się na nieuniknione

1 Prawdziwe incydenty	25
Co to jest incydent bezpieczeństwa	26
Co to jest reakcja na incydent	27
Aktualny stan wiedzy	28
Dlaczego powinieneś interesować się kwestiami reakcji na incydenty bezpieczeństwa	30
Studia przypadku	30
Studium przypadku 1. Gdzie są pieniądze	31
Studium przypadku 2. Certyfikat autentyczności	37
Fazy cyklu ataku	40
I co z tego	43
Pytania	43
2 Podręcznik reagowania na incydenty bezpieczeństwa	45
Co to jest incydent bezpieczeństwa komputerowego	46
Cele reakcji na incydent	47
Kto bierze udział w procesie reakcji na incydent	48
Wyszukiwanie utalentowanych specjalistów do zespołu reagowania na incydenty	50

Proces reakcji na incydent	53
Czynności wstępne	54
Śledztwo	54
Czynności naprawcze	62
Rejestrowanie istotnych informacji śledczych	63
Raportowanie	64
I co z tego	65
Pytania	66
3 Przygotowanie na incydent	67
Przygotowywanie organizacji na incydent	68
Identyfikacja ryzyka	69
Zasady ułatwiające skuteczne zareagowanie na incydent	69
Współpraca z zewnętrznymi firmami informatycznymi	70
Kwestie związane z infrastrukturą globalną	71
Szkolenie użytkowników w zakresie bezpieczeństwa hostów	71
Przygotowywanie zespołu RI	72
Definiowanie misji	72
Procedury komunikacji	73
Informowanie o wynikach śledztwa	75
Zasoby dla zespołu RI	76
Przygotowywanie infrastruktury do reakcji na incydent	83
Konfiguracja urządzeń komputerowych	84
Konfiguracja sieci	91
I co z tego	100
Pytania	100

CZĘŚĆ II Wykrywanie incydentów i ich charakterystyka

4 Prawidłowe rozpoczynanie śledztwa	103
Zbieranie wstępnych faktów	104
Listy kontrolne	105
Robienie notatek na temat sprawy	111
Chronologiczne zapisywanie informacji o ataku	112
Priorytety śledztwa	113
Co to są elementy dowodu	113
Ustalanie oczekiwań z kierownictwem	114
I co z tego	114
Pytania	115
5 Zdobywanie tropów	117
Definiowanie wartościowych tropów	118

Postępowanie z tropami	119
Zamienianie tropów we wskaźniki	120
Cykl generowania wskaźnika	120
Analizowanie tropów wewnętrznych	133
Analizowanie tropów zewnętrznych	134
I co z tego	136
Pytania	137
6 Określanie zasięgu incyduentu	139
Co mam zrobić	141
Analizowanie danych początkowych	141
Zbieranie i analiza dowodów początkowych	142
Określanie sposobu działania	143
Wyciek danych klientów	144
Wyciek danych klientów — przykłady niepoprawnego określania zasięgu incyduentu	148
Oszustwo w automatycznym systemie rozrachunkowym (ACH)	149
Oszustwo ACH — nieprawidłowa identyfikacja zasięgu incyduentu	151
I co z tego	152
Pytania	152

CZĘŚĆ III Gromadzenie danych

7 Zbieranie danych na żywo	155
Kiedy wykonywać analizę na żywo	156
Wybór narzędzia do analizy na żywo	158
Jakie informacje zbierać	159
Najlepsze praktyki gromadzenia danych	161
Gromadzenie danych na żywo w systemach Microsoft Windows	165
Gotowe zestawy narzędzi	165
Narzędzia własnej roboty	168
Zbieranie informacji z pamięci	170
Zbieranie danych na żywo w systemach uniksowych	174
Zestawy narzędzi do analizy na żywo	175
Wykonywanie zrzutów pamięci	178
I co z tego	183
Pytania	184
8 Duplikacja danych śledczych	185
Formaty obrazów na potrzeby śledztwa	187
Kompletny obraz dysku	188
Wykonywanie obrazu partycji	190

Wykonywanie obrazu logicznego	190
Integralność obrazu	191
Tradycyjne metody duplikacji	193
Sprzętowe blokady zapisu	193
Narzędzia do tworzenia obrazów	195
Duplikowanie działającego systemu	199
Duplikowanie środków firmowych	200
Duplikowanie maszyn wirtualnych	201
I co z tego	202
Pytania	202
9 Dowody z sieci	203
Argumenty za monitorowaniem sieci	204
Rodzaje monitoringu sieciowego	205
Monitorowanie zdarzeń	205
Rejestrowanie nagłówków i całych pakietów	207
Modelowanie statystyczne	208
Tworzenie systemu monitorowania sieci	211
Wybór sprzętu	211
Instalacja gotowej dystrybucji	213
Wdrażanie czujnika sieciowego	214
Ocenianie jakości monitora sieciowego	215
Analiza danych sieciowych	215
Kradzież danych	217
Rekonesans za pomocą konsoli sieciowej	223
Inne narzędzia do analizy sieciowej	229
Zbieranie dzienników generowanych przez zdarzenia sieciowe	231
I co z tego	232
Pytania	232
10 Usługi dla przedsiębiorstw	233
Usługi infrastruktury sieciowej	234
DHCP	234
Usługa DHCP ISC	237
DNS	238
Aplikacje do zarządzania przedsiębiorstwem	243
Program Software Management Suite firmy LANDesk	244
Program Altiris Client Management Suite firmy Symantec	246
Programy antywirusowe	249
Kwarantanna programu antywirusowego	249
Program Symantec Endpoint Protection	250
Program McAfee VirusScan	252
Program Trend Micro OfficeScan	255

Serwery sieciowe	257
Podstawowe informacje o serwerach sieciowych	257
Serwer HTTP Apache	259
Serwer Microsoft Information Services	260
Serwery baz danych	263
Microsoft SQL	264
MySQL	265
Oracle	267
I co z tego	268
Pytania	268

CZĘŚĆ IV Analiza danych

11 Metody analizy	271
Definicja celów	272
Zapoznanie się z danymi	274
Miejsca przechowywania danych	274
Co jest dostępne	276
Dostęp do zdobytych danych	277
Obrazy dysków	277
Jak to wygląda	279
Analiza danych	280
Zarys proponowanej metody działania	281
Wybór metod	282
Ewaluacja wyników	286
I co z tego	287
Pytania	287
12 Prowadzenie czynności śledczych w systemach Windows	289
Analiza systemu plików	291
Główna tabela plików	291
Atrybuty INDX	300
Dzienniki zmian	302
Kopie zapasowe woluminów wykonywane w tle	303
Readresator systemu plików	305
Pobieranie zasobów z wyprzedzeniem	306
Dowody	307
Analiza	308
Dzienniki zdarzeń	311
Dowody	311
Analiza	312

Zadania zaplanowane	322
Tworzenie zadań za pomocą polecenia at	322
Tworzenie zadań za pomocą polecenia schtasks	324
Dowody	324
Analiza	325
Rejestr systemu Windows	330
Dowody	331
Analiza	336
Narzędzia do analizy rejestru	363
Inne ślady sesji interaktywnych	365
Pliki LNK	366
Listy szybkiego dostępu	367
Kosz	369
Pamięć	372
Dowody	372
Analiza pamięci	376
Inne mechanizmy utrwalania	386
Foldery startowe	387
Zadania cykliczne	387
Modyfikacja systemowych plików binarnych	388
Modyfikowanie kolejności wczytywania bibliotek DLL	389
Powtórzenie — odpowiedzi na często pojawiające się pytania	392
I co z tego	396
Pytania	397
13 Prowadzenie czynności śledczych w systemach Mac OS X	399
System plików HFS+ i metody jego analizy	400
Układ woluminu	401
Usługi systemu plików	407
Podstawowe dane systemu operacyjnego	410
Układ systemu plików	410
Konfiguracja użytkownika i usług	415
Kosz i pliki usunięte	418
Inspekcja systemu, bazy danych i dzienniki	419
Zadania zaplanowane i usługi	429
Instalatory aplikacji	432
Powtórzenie — odpowiedzi na często zadawane pytania	433
I co z tego	435
Pytania	436
14 Badanie aplikacji	437
Co to są dane aplikacji	438
Gdzie aplikacje przechowują dane	439
System Windows	439

System OS X	440
System Linux	440
Ogólne zasady badania aplikacji na potrzeby śledztwa	441
Przeglądarki internetowe	445
Internet Explorer	447
Google Chrome	453
Mozilla Firefox	458
Klienty poczty elektronicznej	463
Internetowe klienty poczty elektronicznej	464
Microsoft Outlook dla systemów Windows	465
Apple Mail	469
Microsoft Outlook for Mac	470
Komunikatory internetowe	472
Metody analizy	472
Najpopularniejsze komunikatory i protokoły	473
I co z tego	481
Pytania	481
15 Sortowanie szkodliwych programów	483
Postępowanie ze szkodliwym oprogramowaniem	485
Bezpieczeństwo	485
Dokumentacja	486
Dystrybucja	487
Dostęp do szkodliwych witryn internetowych	488
Środowisko do sortowania	489
Konfiguracja środowiska wirtualnego	491
Analiza statyczna	491
Co to za plik	492
Przenośne pliki wykonywalne	501
Analiza dynamiczna	506
Zautomatyzowana analiza dynamiczna — piaskownice	507
Ręczna analiza dynamiczna	507
I co z tego	513
Pytania	514
16 Pisanie raportów	515
Po co pisać raporty	516
Standardy raportowania	517
Styl i formatowanie raportu	518
Treść i organizacja treści raportu	521
Kontrola jakości	524
I co z tego	525
Pytania	525

CZĘŚĆ V Naprawa

17	Wprowadzenie do technik naprawczych	529
	Podstawowe pojęcia	530
	Testy wstępne	536
	Kompletowanie zespołu naprawczego	536
	Kiedy utworzyć zespół naprawczy	536
	Wyznaczanie lidera procesu naprawczego	537
	Członkowie zespołu naprawczego	539
	Czas rozpoczęcia akcji	540
	Opracowywanie i wdrażanie wstępnych środków zaradczych	542
	Skutki zaalarmowania hakera	544
	Opracowywanie i wdrażanie środków ograniczania zasięgu incydentu	545
	Plan ostatecznej likwidacji zagrożenia	548
	Wybór momentu wykonania planu likwidacji zagrożenia i jego wdrażanie	552
	Formułowanie zaleceń strategicznych	557
	Dokumentacja zdobytego doświadczenia	557
	Podsumowanie	559
	Typowe błędy będące przyczyną niepowodzenia procesu naprawczego	565
	I co z tego	566
	Pytania	566
18	Studium przypadku procesu naprawczego	567
	Plan naprawczy dla pierwszego przypadku — pokaż pieniądze	568
	Wybór członków zespołu	569
	Czas prowadzenia działań naprawczych	570
	Ograniczanie zasięgu incydentu	570
	Wstępna akcja naprawcza	574
	Pozbywanie się hakera ze środowiska	578
	Strategia na przyszłość	582
	I co z tego	584
	Pytania	585
A	Odpowiedzi na pytania	ftp://ftp.helion.pl/przyklady/incbez.zip
B	Formularze	ftp://ftp.helion.pl/przyklady/incbez.zip
	Skorowidz	587