

Spis treści

Przedmowa	XIII
Wstęp	XV
Podziękowania	XIX
Prolog. Przyszłość biznesu	1
Środowisko biznesu zmienia się	1
Zależności w biznesie zmieniają się	3
Informacja biznesowa zmienia się	5
Informatyka zmienia się	10
Bezpieczeństwo informacji musi się zmienić	13
Wstęp. Bezpieczeństwo informacji	15
Informacja jest aktywem firmy	15
Bezpieczeństwo jest podstawą biznesu	17
Bezpieczeństwo informacji jest koniecznością w biznesie	18
Budowanie planu bezpieczeństwa informacji	19
Faza I. Inspekcja	23
Definiowanie zasobów	24
Szacowanie zagrożeń	25
Szacowanie potencjalnych szkód	27
Identyfikowanie podatności	28
Wprowadzanie zabezpieczeń	29
Ocena aktualnego stanu	30
Rozdział 1. Inwentaryzacja zasobów	31
Identyfikacja zasobów	31
Przypisanie własności	33
Określenie wartości	34
Klasyfikacja bezpieczeństwa	36
Rozdział 2. Szacowanie zagrożeń	41
Błąd ludzki	42
Naturalne katastrofy	43

Awarie systemu	45
Złośliwe działania	49
Złośliwe oprogramowanie	52
Szkody uboczne.....	58
Rozdział 3. Analiza strat	63
Odmowa usług	65
Kradzież zasobów	66
Usunięcie informacji	67
Kradzież informacji	68
Ujawnienie informacji	68
Uszkodzenie informacji	70
Kradzież oprogramowania	71
Kradzież sprzętu	72
Uszkodzenie systemów sterowanych komputerowo	73
Rozdział 4. Identyfikowanie podatności	77
Usytuowanie podatności	78
Znane miejsca podatne na uszkodzenia	80
Wadliwe projektowanie bezpieczeństwa	81
Innowacyjne wykorzystanie niezgodne z przeznaczeniem	87
Niepoprawne wdrożenie	88
Inżynieria społeczna	90
Rozdział 5. Projektowanie zabezpieczeń	93
Unikanie ryzyka	94
Przeniesienie ryzyka	95
Ograniczanie ryzyka	97
Akceptacja	98
Rozdział 6. Ocena aktualnego stanu	101
Wymierna ocena zasad i procedur	101
Testowanie	104
Analiza wpływu incydentu na działalność firmy	106
Faza II. Ochrona	109
Koncepcje	110
Zasady funkcjonowania	112
Zasady (polityka) bezpieczeństwa	113
Procedury	114
Praktyki	115
Rozdział 7. Uświadomienie	117
Właściwe użycie	117
Program uświadamiania	120
Różne warianty programu uświadamiania	122

Warianty wdrażania	124
Brak uświadomienia bezpieczeństwa	125
Rozdział 8. Dostęp	129
Dostęp globalny	130
Metody dostępu	131
Punkty dostępu jako punkty kontroli bezpieczeństwa	134
Serwery dostępu	136
Nadużycia dostępu	138
Rozdział 9. Identyfikacja	141
Identyfikacja przedsiębiorstwa	141
Wydawanie identyfikatorów	144
Zakres zastosowania	145
Administrowanie identyfikatorami	145
Warianty realizacji	146
Błędy tożsamości	148
Rozdział 10. Uwierzytelnienie	151
Czynniki uwierzytelnienia	152
Modele uwierzytelnienia	154
Warianty uwierzytelnienia	156
Zarządzanie uwierzytelnieniem	159
Błędne uwierzytelnienia	160
Rozdział 11. Autoryzacja	165
Uprawnienia i przywileje	165
Co zapewniają uprawnienia	166
Ziarnistość (granulacja) uprawnień	167
Wymagania	168
Warianty projektowania	169
Nadużycia uprawnień	171
Rozdział 12. Dostępność	173
Rodzaje przerw funkcjonowania	174
Ochrona wszystkich poziomów	175
Modele dostępności	178
Klasyfikacje dostępności	180
Przerwy w dostępie	181
Rozdział 13. Dokładność	185
Cykl życia informacji	185
Dokładność systemu informacyjnego	187
Metody zapewniania dokładności	189
Brak dokładności	190

Rozdział 14. Poufność	193
Informacja w przedsiębiorstwie	193
Zagadnienia związane z poufnością	194
Metody zapewniania poufności	197
Klasyfikacje wrażliwości	197
Naruszenie prywatności	198
Rozdział 15. Rozliczalność	201
Modele rozliczalności	202
Zasady rozliczalności	203
Rozliczanie zdarzeń	205
Funkcje systemu rozliczalności	206
Błędy rozliczalności	206
Rozdział 16. Administrowanie	209
Administrowanie bezpieczeństwem informacji w przedsiębiorstwie	209
Procesy administracyjne	211
Obszary administrowania	213
Błędy administrowania	214
Faza III. Wykrywanie	217
Typy intruzów	218
Metody wtargnięć	220
Metody wykrywania	221
Rozdział 17. Typy intruzów	223
Intruzi zewnętrzni	223
Intruzi wewnętrzni	227
Intruz profesjonalny	232
Rozdział 18. Metody wtargnięć	239
Wtargnięcia techniczne	239
Bezpieczeństwo fizyczne	241
Inżynieria społeczna	243
Rozdział 19. Proces wtargnięcia	251
Rekonesans	251
Uzyskanie dostępu	255
Uzyskanie uprawnień	257
Osiągnięcie celów	260
Rozdział 20. Metody wykrywania	265
Profile	266
Metody statyczne	271

Metody dynamiczne	272
Meldunki użytkowników	275
Faza IV. Reakcja	277
Koncepcja reakcji na incydent	278
Plan reakcji na incydent	280
Rozdział 21. Plan reakcji	283
Procedury reakcji	283
Uprawnienie do odpowiedzi	284
Zasoby	286
Opinia prawna	287
Rozdział 22. Stwierdzenie incydentu	289
Wskaźniki możliwe	290
Wskaźniki prawdopodobne	292
Wskaźniki wyraźne	294
Z góry zdefiniowane sytuacje	296
Rozdział 23. Powiadamianie o incydencie	299
Czynniki wewnętrzne	300
Instytucje zajmujące się incydentami komputerowymi związanymi z bezpieczeństwem	302
Partnerzy dotknięci atakiem	304
Organy ścigania	305
Środki masowego przekazu	306
Rozdział 24. Ograniczanie incydentu	309
Zatrzymanie rozprzestrzeniania się	309
Odzyskanie kontroli	312
Rozdział 25. Szacowanie szkód	317
Określenie rozmiaru szkód	317
Określenie czasu trwania incydentu	319
Określenie przyczyny	320
Wskazanie sprawcy	321
Rozdział 26. Odtwarzanie po incydencie	325
Ustalanie priorytetów	325
Naprawianie miejsc podatnych na uszkodzenia	326
Ulepszanie zabezpieczeń	328
Uaktualnianie systemu wykrywania	328
Przywrócenie danych	329
Przywrócenie usług	330
Monitorowanie w celu uzyskania dodatkowych sygnałów o ataku	331
Odzyskanie zaufania	332

Rozdział 27. Zautomatyzowana odpowiedź	335
Zautomatyzowana obrona	335
Gromadzenie informacji przez kontrwywiad	336
Kontratak	338
Faza V. Refleksja	341
Dokumentacja <i>post mortem</i>	342
Schemat analizy incydentu	343
Działania po incydencie kierowane na zewnątrz	344
Rozdział 28. Dokumentacja incydentu	347
Źródła informacji o incydencie	347
Kronika incydentu	353
Streszczenie techniczne	358
Streszczenie dla kierownictwa	365
Rozdział 29. Ocena incydentu	373
Wskazanie procesów do ulepszenia	374
Udoskonalenie procesu reakcji	377
Rozdział 30. Public relations	383
Właściwi ludzie	383
Właściwy czas	384
Właściwy komunikat	385
Właściwe forum	385
Właściwe podejście	387
Rozdział 31. Postępowanie prawne	391
Prawodawstwo dotyczące przestępczości komputerowej	392
Jurydykacja	394
Gromadzenie materiału dowodowego	395
Doprowadzenie do skazania	398
Epilog. Przyszłość bezpieczeństwa informacji	403
Świat bez granic	404
Architektura zorientowana na usługi	404
Podstawowe zasady biznesu	407
Wszechobecne bezpieczeństwo	408
Słownik	409
Skorowidz	415