

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
Uwzględnić 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 domeny	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

177	Agregacja dzienników	Rozwój oprogramowania	220
177	Analiza przypadków użycia	Wybór języka	221
178	Podsumowanie	Urządzenie	221
178	21. Zestaw nadobowiązkowy		223
179	Serwery pocztowe	Python/Ruby/Perl	223
179	Serwery DNS	< PHP >	225
180	Bezpieczeństwo poprzez zaciemnienie	Wskazówki dotyczące bezpiecznego kodowania	227
181	Przydatne zasoby	Testowanie	227
181	Książki	Zautomatyzowane testy statyczne	228
181	Bлоги	Zautomatyzowane testy dynamiczne	228
182	Podkasty	Wskazania ogólnie	228
182	Narzędzia	cykl rozwoju systemu	228
183	Strony internetowe	Podsumowanie	229
182	A Szablony do edukacji użytkowników		231
185	Skorowidz		235