Podstawy bezpieczeństwa informacji : praktyczne wprowadzenie / Jason Andress. – Gliwice, copyright © 2022

Spis treści

O autorze **4**

O korektorach merytorycznych **4**

Podziękowania **11**

WPROWADZENIE **13**
Kto powinien przeczytać tę książkę? 14
O książce 14

1
CZYM JEST BEZPIECZEŃSTWO INFORMACJI? **17**
Definicja bezpieczeństwa informacji 18
Kiedy jesteś bezpieczny? 18
Modele dyskusji nad kwestiami bezpieczeństwa 20
Triada poufności, integralności i dostępności 20
Heksada Parkera 23
Ataki 24
Rodzaje ataków 25
Zagrożenia, podatności i ryzyko 27
Zarządzanie ryzykiem 28
Reagowanie na incydenty 33
Obrona wielopoziomowa 35
Podsumowanie 39
Ćwiczenia 40

2
IDENTYFIKACJA I UWIERZYTELNIANIE **41**
Identyfikacja 42
Za kogo się podajemy 42
Weryfikacja tożsamości 42
Fałszowanie tożsamości 43
Uwierzytelnianie 43
Metody uwierzytelniania 44
Uwierzytelnianie wieloskładnikowe 45
Uwierzytelnianie wzajemne 46
Popularne metody identyfikacji i uwierzytelniania 47
Hasła 47
Biometria 48
Tokeny sprzętowe 52

Podsumowanie 53
Ćwiczenia 53

3
AUTORYZACJA I KONTROLA DOSTĘPU 55
Czym są mechanizmy kontroli dostępu? 55
Wdrażanie kontroli dostępu 57
Listy kontroli dostępu 57
Tokeny dostępu 63
Modele kontroli dostępu 64
Uznaniowa kontrola dostępu 64
Obowiązkowa kontrola dostępu 64
Kontrola dostępu oparta na regułach 65
Kontrola dostępu oparta na rolach 65
Kontrola dostępu oparta na atrybutach 66
Wielopoziomowa kontrola dostępu 67
Fizyczna kontrola dostępu 70
Podsumowanie 72
Ćwiczenia 72

4
AUDYTOWANIE I ROZLICZALNOŚĆ 73
Rozliczalność 74
Korzyści dla bezpieczeństwa wynikające z rozliczalności 76
Niezaprzeczalność 76
Efekt odstraszania 76
Wykrywanie włamań i zapobieganie im 77
Dopuszczalność zapisów jako materiału dowodowego 77
Audytowanie 78
Co. może podlegać audytowi? 78
Rejestrowanie (logowanie) zdarzeń 79
Monitorowanie 80
Audyt z oceną podatności 80
Podsumowanie 82
Ćwiczenia 82

5
KRYPTOGRAFIA 84
Historia kryptografii 85
Szyfr Cezara 85
Maszyny kryptograficzne 85
Reguły Kerckhoffsa 90
Nowoczesne narzędzia kryptograficzne 90
Szyfry oparte na słowach kluczowych i jednorazowych bloczkach szyfrowych 91
Kryptografia symetryczna i asymetryczna 93
Funkcje haszujące 97

Podpisy cyfrowe 98
Certyfikaty 98
Ochrona danych w spoczynku, w ruchu i w użyciu 100
Ochrona danych w spoczynku 100
Ochrona danych w ruchu 101
Ochrona danych w użyciu 102
Podsumowanie 103
Ćwiczenia 104

6
ZGODNOŚĆ, PRAWO I PRZEPISY 105
Czym jest zgodność z przepisami? 105
Rodzaje zgodności z przepisami 106
Konsekwencje braku zgodności z przepisami 107
Osiąganie zgodności z przepisami dzięki mechanizmom kontrolnym 107
Rodzaje mechanizmów kontrolnych 108
Kluczowe i kompensacyjne mechanizmy kontrolne 108
Utrzymywanie zgodności 109
Bezpieczeństwo informacji i przepisy prawa 110
Zgodność z przepisami dotyczącymi agencji rządowych 110
Zgodność z wymaganiami branżowymi 112
Przepisy prawne poza Stanami Zjednoczonymi 114
Przyjęcie ram dla zgodności 115
Międzynarodowa Organizacja Normalizacyjna 115
Instytut NIST 116
Niestandardowe ramy zarządzania ryzykiem 117
Zgodność z przepisami w obliczu zmian technologicznych 117
Zgodność w rozwiązaniach chmurowych 118
Zgodność z blockchalnem 120
Zgodność a kryptowaluty 120
Podsumowanie 121
Ćwiczenia 122

7
BEZPIECZEŃSTWO OPERACYJNE 123
Proces bezpieczeństwa operacyjnego 123
Identyfikacja informacji o krytycznym znaczeniu 124
Analiza zagrożeń 124
Analiza podatności 125
Ocena ryzyka 126
Zastosowanie środków zaradczych 126
Podstawowe reguły bezpieczeństwa operacyjnego 127
Reguła pierwsza: poznaj zagrożenia 127
Reguła druga: wiedz, co należy chronić 127
Reguła trzecia: chroń informacje 128
Bezpieczeństwo operacyjne w życiu prywatnym 129
Początki bezpieczeństwa operacyjnego 130

SunTzu 130
George Washington 131
Wojna w Wietnamie 131
Biznes 132
Agencja lOSS 132
Podsumowanie 134
Ćwiczenia 134

8
BEZPIECZEŃSTWO CZYNNIKA LUDZKIEGO 135
Gromadzenie informacji przydatnych do przeprowadzania ataków socjotechnicznych 136
HUMINT — rozpoznanie osobowe 136
OSINT — biały wywiad 137
Inne rodzaje źródeł informacji 142
Rodzaje ataków socjotechnicznych 143
Atak pretekstowy 143
Phishing 143
Tailgating 145
Budowanie świadomości bezpieczeństwa użytkowników poprzez programy szkoleniowe 146
Hasła 146
Szkolenia z zakresu inżynierii społecznej 146
Korzystanie z sieci 147
Złośliwe oprogramowanie 148
Prywatny sprzęt komputerowy 148
Polityka czystego biurka 149
Znajomość polityki bezpieczeństwa i uregulowań prawnych 149
Podsumowanie 149
Ćwiczenia 150

9
BEZPIECZEŃSTWO FIZYCZNE 151
Identyfikacja zagrożeń fizycznych 152
Fizyczne środki bezpieczeństwa 152
Odstraszające środki bezpieczeństwa 153
Systemy wykrywania 153
Zapobiegawcze środki bezpieczeństwa 154
Zastosowanie fizycznej kontroli dostępu 155
Ochrona ludzi 155
Zagadnienia związane z ochroną ludzi 155
Zapewnienie bezpieczeństwa 157
Ewakuacja 157
Kontrole administracyjne 158
Ochrona danych 158
Fizyczne zagrożenia dla danych 159
Dostępność danych 160

Szczątkowe pozostałości danych 160
Ochrona wyposażenia 161
Fizyczne zagrożenia dla sprzętu 161
Wybór lokalizacji obiektu 163
Zabezpieczenie dostępu 163
Warunki środowiskowe 164
Podsumowanie 164
Ćwiczenia 165

10
BEZPIECZEŃSTWO SIECIOWE 166
Ochrona sieci 167
Projektowanie bezpiecznych sieci 167
Zastosowanie zapór sieciowych 168
Wdrażanie sieciowych systemów wykrywania włamań 171
Ochrona ruchu sieciowego 172
Zastosowanie sieci VPN 172
Ochrona danych w sieciach bezprzewodowych 173
Używanie bezpiecznych protokołów komunikacyjnych 174
Narzędzia do zabezpieczania sieci 174
Narzędzia do ochrony sieci bezprzewodowych 175
Skanery 175
Sniffery 175
System honeypot 177
Narzędzia dla zapór sieciowych 177
Podsumowanie 178
Ćwiczenia 178

11
BEZPIECZEŃSTWO SYSTEMU OPERACYJNEGO 180
Utwardzanie systemu operacyjnego 181
Usuń całe niepotrzebne oprogramowanie 181
Usuń wszystkie niepotrzebne usługi 182
Zmiana domyślnych kont 184
Stosuj zasadę najmniejszego uprzywilejowania 184
Pamiętaj o aktualizacjach 185
Włącz logowanie i audytowanie 186
Ochrona przed złośliwym oprogramowaniem 186
Narzędzia antywirusowe 187
Ochrona przestrzeni wykonywalnej 187
Programowe zapory sieciowe i systemy HID 188
Narzędzia bezpieczeństwa dla systemu operacyjnego 189
Skanery 189
Narzędzia do wyszukiwania podatności i luk w zabezpieczeniach 191
Frameworki exploitów 191
Podsumowanie 193
Ćwiczenia 194

12
BEZPIECZEŃSTWO URZĄDZEŃ MOBILNYCH, URZĄDZEŃ WBUDOWANYCH ORAZ INTERNETU RZECZY **195**
Bezpieczeństwo urządzeń mobilnych 196
Ochrona urządzeń mobilnych 196
Kwestie bezpieczeństwa urządzeń przenośnych 198
Bezpieczeństwo urządzeń wbudowanych 201
Gdzie się używa urządzeń wbudowanych 201
Problemy bezpieczeństwa urządzeń wbudowanych 204
Bezpieczeństwo internetu rzeczy 205
Czym są urządzenia internetu rzeczy? 205
Problemy bezpieczeństwa urządzeń IoT 207
Podsumowanie 209
Ćwiczenia 209

13
BEZPIECZEŃSTWO APLIKACJI **211**
Luki w zabezpieczeniach oprogramowania 212
Przepełnienia bufora 212
Warunki wyścigu 213
Ataki na weryfikację danych wejściowych 214
Ataki uwierzytelniające 215
Ataki autoryzacyjne 215
Ataki kryptograficzne 216
Bezpieczeństwo sieci Web 216
Ataki po stronie klienta 216
Ataki po stronie serwera 218
Bezpieczeństwo baz danych 219
Problemy z protokołami 221
Dostęp do funkcjonalności bez uwierzytelnienia 221
Arbitralne wykonanie kodu 222
Eskalacja uprawnień 222
Narzędzia do oceny bezpieczeństwa aplikacji 223
Sniffery 223
Narzędzia do analizy aplikacji internetowych 225
Fuzzery 227
Podsumowanie 227
Ćwiczenia 228

14
OCENA BEZPIECZEŃSTWA **229**
Ocena podatności 229
Mapowanie i wykrywanie 230
Skanowanie 231
Wyzwania technologiczne związane z oceną podatności 233
Testy penetracyjne 234

Przeprowadzanie testów penetracyjnych 234
Klasyfikacja testów penetracyjnych 236
Cele testów penetracyjnych 237
Programy bug bounty 240
Wyzwania technologiczne związane z testami penetracyjnymi 240
Czy to oznacza, że naprawdę jesteś bezpieczny? 241
Realistyczne testy 241
Czy potrafisz wykryć własne ataki? 243
Bezpieczeństwo dzisiaj nie oznacza bezpieczeństwa jutro 244
Usuwanie luk w zabezpieczeniach jest kosztowne 245
Podsumowanie 246
Ćwiczenia 246

PRZYPISY **247**

SKOROWIDZ **255**

oprac. BPK