Spis treści

Przedmowa 9
Wprowadzenie 11

1. INFORMACJE. 14
   1.1. Zasady przetwarzania informacji 14
   1.2. Klasyfikacja informacji 15
   1.3. Postępowanie z informacjami 17

2. OGÓLNY MODEL BEZPIECZEŃSTWA INFORMACJI 20
   2.1. Model znormalizowany. 20
   2.2. Podstawy metodyczne. 21
   2.3. Klasy bezpieczeństwa systemów informatycznych 23

3. ZARZĄDZANIE RYZYKIEM 25
   3.1. Ryzyko 25
   3.2. Proces zarządzania ryzykiem 25
   3.3. Ustanowienie kontekstu 28
   3.4. Zakres procesu zarządzania ryzykiem 30
   3.5. Szacowanie ryzyka 32
   3.6. Postępowanie z ryzykiem 38
   3.7. Akceptowanie ryzyka 40
   3.8. Monitoring i przegląd ryzyka 41

4. ZAGROŻENIA 43
   4.1. Identyfikacja zagrożeń 43
   4.2. Nieobliczalne oprogramowanie 45
   4.3. Ewolucja zagrożeń 47
      4.3.1. Ataki ukierunkowane. 47
      4.3.2. Podatność Internetu Rzeczy (IoT). 50
      4.3.3. Oprogramowanie ransomware 52

5. BEZPIECZEŃSTWO SYSTEMÓW OPERACYJNYCH 55
   5.1. Podstawy systemów operacyjnych 55
   5.2. Zagrożenia dla systemów operacyjnych i sposoby ochrony. 57

5.2.1. Ataki na systemy WINDOWS i metody przeciwdziałania
5.2.2. Ataki na systemy UNIX

6. BEZPIECZEŃSTWO SIECI 67
6.1. Sieć informatyczna 67
6.2. Mechanizmy bezpieczeństwa usług sieciowych 67
6.3. Detekcja 68
6.4. Podatności w zabezpieczeniach sieci 69
6.5. Zarządzanie bezpieczeństwem sieci 72

7. ZAGROŻENIA DLA APLIKACJI WEBOWYCH I ŚRODKI PRZECIWDZIAŁANIA 76
7.1. Ataki na serwery aplikacji 76
7.2. Ataki na aplikacje webowe 78

8. KONTROLA DOSTĘPU 82
8.1. Kryteria dostępu 82
8.2. Usługi sieciowe 83
8.3. Dane wrażliwe 86
8.4. Urządzenia mobilne 86
8.5. System kontroli dostępu 87

9. KRYPTOGRAFIA 89

10. ZARZĄDZANIE BEZPIECZEŃSTWEM EKSPLOATACJI 93
10.1. Zasady bezpiecznej eksploatacji 93
10.2. Integralność oprogramowania 94
10.3. Kopie zapasowe 95
10.4. Ujawnianie informacji 96
10.5. Transakcje elektroniczne 97
10.6. Nowe protokoły komunikacyjne 99
10.7. Monitorowanie zdarzeń 100
10.8. Zarządzanie podatnościami technicznymi 101
10.9. Serwis systemów informatycznych 102

11. ZARZĄDZANIE INCYDENTAMI BEZPIECZEŃSTWA 104
11.1. Zasady podstawowe 104
11.2. Obsługa zdarzeń i incydentów bezpieczeństwa 105
11.3. Metodologia zarządzania incydentami bezpieczeństwa 108

12. KRYTERIA WYBORU ZABEZPIECZEŃ 111
12.1. Zasady ogólne 111
12.2. Polityka dotycząca haseł 112
12.3. Wytyczne dotyczące różnych platform technologicznych 115
12.4. Przetwarzanie transakcyjne 117
12.5. Technologie biometryczne 118

13. WDRAŻANIE SYSTEMÓW INFORMATYCZNYCH 121
13.1. Metodologia projektowania systemów informatycznych 121

13.2. Błędy programistyczne 122
13.3. Projektowanie zabezpieczeń 128
13.4. Zasady bezpiecznego programowania 129

14. POMIARY BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH 132
14.1. Problem badawczy 132
14.2. Procesy pomiarowe 132
14.3. Model pomiarowy 134
14.4. Wskaźniki pomiarowe 135
14.5. Ocena skuteczności zabezpieczeń 136

15. METODOLOGIA TESTÓW BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH 138
15.1. Testy bezpieczeństwa 138
15.2. Testy penetracyjne 139
15.3. Zakres przeprowadzenia testu penetracyjnego 140
15.4. Etapy testów penetracyjnych 142
15.5. Metodyka OWASP Top 10 144
15.6. Inne metodyki 147
15.7. Narzędzia do prowadzenie testów 150

16. AUDYT BEZPIECZEŃSTWA 155
16.1. Zasady ogólne 155
16.2. Metodyka audytu według norm międzynarodowych 156
16.3. Oprogramowanie klasy SIEM 157
16.4. Raport z audytu bezpieczeństwa 159

17. PODSUMOWANIE 161

BIBLIOGRAFIA 164

Załącznik A. RAPORT Z TESTU PENETRACYJNEGO 168

Załącznik B. METODY TESTOWANIA ZABEZPIECZEŃ 183