

Spis treści

Wprowadzenie	1
1. Sytuacja problemowa	3
2. Metodologia	7
3. Definicje i skróty	17
CZĘŚĆ PIERWSZA	
Zarządzanie ryzykiem bezpieczeństwa informacji	23
4. Znaczenie informacji we współczesnym świecie	27
5. Własności bezpieczeństwa informacji	37
6. Elementy zarządzania	45
7. Zarządzanie ryzykiem	51
7.1. Zjawisko niepewności	51
7.2. Pojęcie „ryzyka”	54
7.3. Proces zarządzania ryzykiem	57
7.4. Metodyka identyfikacji scenariuszy ryzyka IT	68
8. Podział cyberzagrożeń metodą A:F (model)	75
8.1. Ataki fizyczne	77
8.2. Awarie techniczne	79
8.3. Cyberataki	81
8.4. Katastrofy naturalne	84
8.5. Błędy ludzkie	85
8.6. Zagrożenia prawne	86
9. Mechanizmy kontrolne	91
10. Podsumowanie	97

Zarządzanie bezpieczeństwem informacji	99
11. Złożoność zapewniania cyberbezpieczeństwa	101
12. Kompetencje z zakresu cyberbezpieczeństwa	105
12.1. Modele kompetencji w zakresie cyberbezpieczeństwa	108
12.2. Cyberbezpieczeństwo w strukturze organizacyjnej	112
13. Model wielowarstwowego zarządzania bezpieczeństwem informacji	119
13.1. Normy i standardy z zakresu zarządzania cyberbezpieczeństwem	120
13.2. Koncepcja skutecznego zarządzania cyberbezpieczeństwem	122
13.2.1. Czworowarstwowa ochrona informacji	122
13.2.2. Trzy fazy ochrony informacji	124
13.2.3. Trzy przepływy wartości dodanej	124
13.2.4. Różne rodzaje mechanizmów kontrolnych	125
13.3. Wielowarstwowe zarządzanie bezpieczeństwem informacji (model)	125
13.3.1. Procesy dotyczące eksploatacji Systemu Zarządzania Bezpieczeństwem Informacji	128
13.3.2. Procesy doskonalące Systemu Zarządzania Bezpieczeństwem Informacji	147
13.3.3. Procesy reagowania na incydenty bezpieczeństwa informacji	154
13.4. Metodyka budowania łańcucha procesów cyberbezpieczeństwa	160
13.5. Podsumowanie	162
14. Narzędzia z zakresu cyberbezpieczeństwa	163
14.1. Przeciwdziałanie cyberzagrożeniom	163
14.1.1. Aktualizacja systemów operacyjnych i aplikacji	165
14.1.2. Segmentacja sieci wewnętrznej	166
14.1.3. Bezpieczne uwierzytelnienie	166
14.1.4. Praca z wykorzystaniem minimalnych uprawnień	167
14.1.5. Szyfrowanie	168
14.1.6. Kopie bezpieczeństwa	168
14.1.7. Stosowanie standardów utwardzania systemów	169
14.1.8. Gromadzenie logów	169
14.1.9. Współpracowanie wyłącznie z zaufanymi partnerami	170
14.1.10. Bezpieczny cykl tworzenia oprogramowania	170
14.2. Skuteczne monitorowanie cyberbezpieczeństwa (model)	171
14.2.1. Security Incident and Event Management (SIEM) i Security Orchestration, Automation and Response (SOAR)	173
14.2.2. Źródła ze zdarzeniami dotyczącymi ruchu sieciowego	176
14.2.3. Źródła ze zdarzeniami identyfikowanymi na urządzeniach końcowych	179
14.2.4. Wzbogacanie logów	181
14.2.5. Security Operations Center (SOC)	183
14.2.6. Cyber Threat Intelligence	186
14.2.7. Przechwytywanie pakietów	188
14.3. Metodyka wyboru narzędzi monitorowania cyberbezpieczeństwa	188
14.4. Podsumowanie	192

Przyszłość cyberbezpieczeństwa	195
15. Rosnące ryzyko cyberincydentów	199
15.1. Rosnąca liczba podatności	199
15.2. Rosnące prawdopodobieństwo ataku	202
16. Nowe mechanizmy kontrolne	205
16.1. Rosnąca rola regulacji dotyczących ochrony informacji	205
16.2. Zasady bezpiecznego programowania	207
16.3. Nowe rodzaje usług cyberbezpieczeństwa	208
16.3.1. Pakiety usług cyberbezpieczeństwa	209
16.3.2. Usługi monitoringu z wysokim poziomem pewności	210
16.4. Nowe warianty narzędzi cyberbezpieczeństwa	210
16.4.1. Systemy klasy „deception”	211
16.4.2. Automatyzacja usług cyberbezpieczeństwa z wykorzystaniem AI	211
Podsumowanie	212
Zakończenie	213
Podziękowania	223
Bibliografia	225
Spis rysunków	235
Spis tabel	236