

Cyberbezpieczeństwo / redakcja naukowa Cezary Banasiński, Marcin Rojszczak ; Cezary Banasiński, Jacek Maria Chmielewski, Władysław Hydzyk, Jacek Łuczak, Włodzimierz Nowak, Marcin Rojszczak, Kazimierz Waćkowski. – Warszawa, 2020

Spis treści

WYKAZ SKRÓTÓW	9
WSTĘP	13
ROZDZIAŁ I	
PRAWNE I POZAPRAWNE ŹRÓDŁA WYMAGAŃ DLA SYSTEMÓW CYBERBEZPIECZEŃSTWA	15
1. Wprowadzenie	15
2. Krajowy system cyberbezpieczeństwa	15
3. Rekomendacje i zalecenia	28
3.1. Sektor bankowy	28
3.2. Inne organy regulacyjne oraz organy branżowe	31
4. Działania własne przedsiębiorców i innych organizacji	34
ROZDZIAŁ II	
PRAKTYCZNE ASPEKTY CYBERBEZPIECZEŃSTWA Z PERSPEKTYWY UŻYTKOWNIKA	39
1. Wprowadzenie	39
2. Dobre praktyki w zakresie bezpieczeństwa IT	41
3. Dane osobowe - mechanizmy ochrony prawnej	52
4. Zwalczanie nieprawdziwych i szkalujących informacji, zjawisko mowy nienawiści z perspektywy użytkownika	58
5. Postępowanie w przypadku podejrzenia popełnienia cyberprzestępstwa	62
6. Podsumowanie	65
ROZDZIAŁ III	
ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI ORAZ CYBERBEZPIECZEŃSTWO W UJĘCIU PROCESOWYM	69
1. Istota systemowego zarządzania bezpieczeństwem informacji oraz cyberbezpieczeństwo	69
2. Podstawy normatywne systemu zarządzania bezpieczeństwem informacji i cyberbezpieczeństwem (ISO/IEC 27001, ISO/IEC 27032)	71
3. Zabezpieczenia wymagane w ISO/IEC 27001	75
4. Podejście procesowe	77
5. Identyfikacja i charakterystyka procesów	80
6. Współczynniki monitorujące w procesie cyberbezpieczeństwa	89
7. Doskonalenie procesów	101

ROZDZIAŁ IV	
SPECYFIKA ZAGROŻEŃ W CYBERPRZESTRZENI	103
1. Zagrożenia w cyberprzestrzeni	103
2. Szkodliwe oprogramowanie	104
3. Standardy cyberbezpieczeństwa	108
4. Priorytety dla przedsiębiorców (instytucji) w zakresie bezpieczeństwa w cyberprzestrzeni	109
5. Polityki bezpieczeństwa informacji	111
6. Co w praktyce może być zagrożeniem?	113
7. Problemy, z którymi należy się zmierzyć, aby zapewnić bezpieczeństwo w cyberprzestrzeni	114
7.1. Bezpieczeństwo wewnętrzne	114
7.2. Zagrożenia zewnętrzne	115
8. Podsumowanie	124
ROZDZIAŁ V	
PRZEGLĄD NAJWAŻNIEJSZYCH ZABEZPIECZEŃ INFORMATYCZNYCH	127
1. Wprowadzenie	127
2. Najgroźniejsze ataki 2018-2019	129
3. Wektor ataku	142
4. Zarządzanie podatnościami oprogramowania i systemów IT	149
4.1. Testy penetracyjne	156
4.2. Skanowanie	157
5. Wykrywanie i zapobieganie włamaniom intruzów do sieci korporacyjnej, systemy IDS/IPS	161
5.1. System wykrywania intruzów, IDS	161
5.1.1. Rodzaje klasyfikacji systemów wykrywania intruzów	163
5.1.1.1. Klasyfikacja IDS wg źródeł informacji	163
5.1.1.2. Klasyfikacja IDS wg zastosowanych metod analitycznych	169
5.1.1.3. Klasyfikacja IDS wg typów odpowiedzi	171
5.1.2. Pułapka internetowa, Honey Pot	173
5.2. ARAKIS, polski system wczesnego ostrzegania o cyberzagrożeniach	178
5.2.1. System ARAKIS 2.0	178
5.2.2. System ARAKIS-GOV	180
5.3. System wykrywania i blokowania ataków, IPS	183
5.3.1. Różnice w działaniu IDS a IPS	184
5.3.2. Rodzaje klasyfikacji systemów IPS	184
5.3.2.1. Klasyfikacja IPS wg topologii sieci	184
5.3.2.2. Klasyfikacja IPS wg źródeł informacji	185
6. Systemy DLP blokujące nieautoryzowane przekazanie cennej informacji z wnętrza sieci	187
7. Rejestrowanie zdarzeń	192
7.1. Dziennik zdarzeń systemu Windows	195
7.2. Syslog i logi systemowe w Linuksie	198
8. Centralne systemy zarządzania tożsamością, IAM	199

9. Podsumowanie	206
-----------------	-----

ROZDZIAŁ VI

WYBRANE ASPEKTY OCHRONY KRYPTOGRAFICZNEJ	211
1. Wprowadzenie	211
2. Funkcja skrótu (ang. <i>hash</i>)	212
3. Kryptograficzne utajnianie wiadomości	214
4. Przykładowe zastosowania kryptografii w teleinformatyce	217
4.1. Protokoły komunikacyjne	217
4.2. Ataki na protokoły komunikacyjne	219
4.3. Zastosowania kryptografii w protokołach warstwy aplikacji	220
5. Kryptografia symetryczna	222
6. Kryptografia asymetryczna	224
7. Hasło w kryptografii i uwierzytelnianiu	230
8. Metody ataków kryptograficznych na hasła	236
8.1. Atak siłowy	236
8.2. Atak słownikowy	239
8.3. Odwrócony atak siłowy	239
8.4. Tęczowe tablice	239
9. Obrona kryptograficzna przed atakami na hasła	240
9.1. Ciąg zaburzający, tzw. sól	240
9.2. Token kryptograficzny	242
9.3. Uwierzytelnianie za pomocą klucza	245
10. Infrastruktura klucza publicznego	246
10.1. Certyfikat podpisywania	250
10.2. Hierarchia urzędów certyfikacyjnych	252
10.3. Podpis cyfrowy	253
10.4. Znacznik czasu	270
11. Podsumowanie	271

ROZDZIAŁ VII

POSTĘPOWANIE W PRZYPADKU WYSTĄPIENIA INCYDENTU	277
1. Wprowadzenie: zarządzanie incydentami oraz współdzielenie informacji o incydentach	277
1.1. Kluczowe terminy i definicje	278
1.2. Zarządzanie incydentami a ogólne rozporządzenie o ochronie danych (RODO)	279
2. Zarządzanie incydentami a ustawa o krajowym systemie cyberbezpieczeństwa	281
3. Standaryzacja w zarządzaniu incydentami oraz rola zapewnienia ciągłości działania	281
3.1. Metodyka Cyber Kill Chain	282
3.2. Zarządzanie incydentami według metodyki PDCA	285
3.3. Zarządzanie incydentami według standardu NIST oraz wytycznych ENISA	291
4. Podsumowanie	297

ROZDZIAŁ VIII	
STRATEGIE ATAKÓW I OBRONY - ANALIZA PRZYPADKÓW	299
1. Wprowadzenie	299
2. Schemat typowego cyberataku	302
3. Specyfika zagrożeń APT	305
4. Omówienie przykładowych ataków	306
4.1. Estonia 2007 (DDoS)	306
4.2. Iran 2010 (Stuxnet)	309
4.3. Sony Pictures Entertainment 2014 (Destover)	311
4.4. Ukraina 2015 (BlackEnergy/KillDisk)	314
4.5. Ukraina 2017 (NonPetya)	316
5. Podsumowanie	318
ROZDZIAŁ IX	
CYBERBEZPIECZEŃSTWO 2.0: W POSZUKIWANIU NOWYCH RAM	
OCHRONY CYBERPRZESTRZENI	323
1. Wprowadzenie	323
2. Cyberbezpieczeństwo 1.0 - próba charakterystyki	324
3. Nowy model cyberbezpieczeństwa - aspekty prawne	329
4. Nowy model cyberbezpieczeństwa - aspekty technologiczne	332
5. Paradoks bezpiecznego Internetu	338
6. Podsumowanie	339
BIBLIOGRAFIA	341

oprac. BPK