

Spis treści

Wykaz skrótów	13
Wstęp	21
Rozdział 1	
Hacking – zagadnienia ogólne	27
1.1. Uwagi wstępne	27
1.1.1. Zarys historii komputerów i sieci komputerowych	27
1.1.2. Pojawienie się hackerów	31
1.1.3. Sprzęt komputerowy	32
1.2. Ogólne informacje o sieciach komputerowych	34
1.2.1. Kodowanie	34
1.2.2. Składniki sieci	35
1.2.2.1. Medium sieciowe	36
1.2.2.2. Urządzenia sieciowe	40
1.2.2.3. Oprogramowanie	43
1.2.2.4. Metody dostępu do medium sieciowego	43
1.2.3. Podział sieci komputerowych	45
1.2.3.1. Podział sieci ze względu na zasięg	45
1.2.3.2. Podział sieci ze względu na sposób konfiguracji	46
1.2.4. Topologie sieciowe	48
1.2.5. Wąskopasmowe i szerokopasmowe technologie dostępowe	51
1.2.6. Modele sieci	53
1.2.7. Przesyłanie danych siecią	60
1.2.7.1. Protokoły	60
1.2.7.2. Adresy	61
1.2.7.3. Routing	64
1.2.7.4. Nazwy komputerów i adresy URL	67

1.2.8.	Usługi sieciowe	69
1.2.9.	Sieci <i>peer-to-peer</i>	72
1.3.	Techniczne aspekty hackingu	74
1.3.1.	Uwagi wstępne	74
1.3.2.	Przebieg ataku	76
1.3.3.	Czynności przygotowawcze	77
1.3.4.	Rodzaje ataków	79
1.3.4.1.	Złośliwe oprogramowanie	80
1.3.4.2.	Przechwytywanie pakietów i analiza protokołów (<i>sniffing</i>)	89
1.3.4.3.	<i>Spoofing</i>	92
1.3.4.4.	<i>Session hijacking</i>	94
1.3.4.5.	<i>Pharming</i>	95
1.3.4.6.	<i>Drive-by pharming</i>	96
1.3.4.7.	<i>Man-in-the-middle</i>	97
1.3.4.8.	Wykorzystanie luk – manipulacja danymi wejściowymi	97
1.3.4.9.	Wykorzystanie właściwości <i>source routing</i>	103
1.3.4.10.	Łamanie hasel	103
1.3.4.11.	Socjotechnika	105
1.3.4.12.	<i>Phishing</i>	107
1.3.4.13.	Ataki odmowy usługi (DoS)	108
1.3.4.14.	„Bomba mailowa”	112
1.3.4.15.	<i>Bluejacking</i> i <i>bluehacking</i>	113
1.3.5.	Czynności końcowe	113
1.3.6.	Wykrywanie ataków i włamań	114
1.3.7.	Zabezpieczanie dowodów w postaci elektronicznej	116

Rozdział 2

Wprowadzenie do problematyki przestępczości komputerowej		119
2.1.	Pojęcie przestępstwa komputerowego	119
2.2.	Klasyfikacja przestępstw komputerowych	122
2.3.	Wyzwania związane z pojawieniem się przestępczości komputerowej	128
2.4.	Zarys historii kryminalizacji zjawiska przestępczości komputerowej	129
2.5.	Wyjaśnienie podstawowych pojęć	131
2.5.1.	Pojęcie informacji	131

2.5.2. Informacja a dane	133
2.5.3. Program komputerowy	138
2.5.4. Poufność, integralność i dostępność danych komputerowych	142
2.5.5. Społeczeństwo informacyjne i gospodarka oparta na wiedzy	144

Rozdział 3

Inicjatywy międzynarodowe mające na celu zwalczanie

cyberprzestępczości	146
3.1. Uwagi wstępne	146
3.2. OECD	152
3.3. Rada Europy	157
3.3.1. Działania Rady Europy w okresie poprzedzającym przyjęcie Konwencji o cyberprzestępczości	157
3.3.2. Konwencja o cyberprzestępczości	162
3.3.2.1. Uwagi wstępne	162
3.3.2.2. Terminologia	166
3.3.2.3. Uzyskanie bezprawnego dostępu do systemu komputerowego	170
3.3.2.4. Bezprawne przechwytywanie transmisji	173
3.3.2.5. Bezprawna ingerencja w dane komputerowe	178
3.3.2.6. Bezprawna ingerencja w system komputerowy	180
3.3.2.7. „Nadużycie urządzeń”	182
3.3.2.8. Formy zjawiskowe i stadialne	191
3.3.2.9. Sankcje	192
3.3.2.10. Uwagi końcowe	193
3.3.3. Inne inicjatywy Rady Europy	194
3.4. ONZ	195
3.4.1. Uwagi wstępne	195
3.4.2. Rezolucje Zgromadzenia Ogólnego	196
3.4.3. Biuro ds. Narkotyków i Przestępczości	200
3.5. Międzynarodowy Związek Telekomunikacyjny (ITU)	204
3.6. Grupa G7/G8	209
3.7. Działalność organizacji pozarządowych	213
3.7.1. Międzynarodowa Organizacja Policji Kryminalnych – Interpol	213

3.7.2. Międzynarodowe Stowarzyszenie Prawa Karnego – AIDP/IAPL	217
3.7.3. EastWest Institute – EWI	219
3.7.4. Światowy Protokół dotyczący Cyberbezpieczeństwa i Cyberprzestępczości	220

Rozdział 4

Cyberprzestępczość w prawie Unii Europejskiej	224
4.1. Zagadnienia wstępne	224
4.2. Akty niewiążące	233
4.3. Program eEurope	236
4.4. Decyzja ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne	242
4.4.1. Uwagi wstępne	242
4.4.2. Terminologia	244
4.4.3. Typy czynów	250
4.4.4. Formy zjawiskowe i stadialne	251
4.4.5. Sankcje	252
4.4.6. Kwestie proceduralne	254
4.5. Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne	256
4.5.1. Uwagi wstępne	256
4.5.2. Typy czynów	259
4.5.3. Formy zjawiskowe i stadialne	264
4.5.4. Sankcje	266
4.5.5. Uwagi końcowe	268
4.6. Działalność Unii Europejskiej a Konwencja o cyberprzestępczości	269

Rozdział 5

Przestępstwa przeciwko danym komputerowym i systemom informatycznym w polskim kodeksie karnym	271
5.1. Uwagi wstępne	271
5.2. Artykuł 267 § 1 k.k. – nieuprawniony dostęp do informacji	285
5.3. Artykuł 267 § 2 k.k. – nieuprawniony dostęp do systemu informatycznego	295

5.4. Artykuł 267 § 3 k.k. – nielegalny podsłuch i inwigilacja za pomocą urządzeń technicznych i programów komputerowych .	303
5.5. Artykuł 267 § 4 k.k. – ujawnienie informacji uzyskanej nielegalnie	308
5.6. Artykuł 268 § 2 i 3 k.k. – naruszenie integralności zapisu informacji na informatycznym nośniku danych	310
5.7. Artykuł 268a k.k. – naruszenie integralności danych, utrudnianie dostępu do danych oraz zakłócanie ich przetwarzania	316
5.8. Artykuł 269 k.k. – sabotaż informatyczny	322
5.9. Artykuł 269a k.k. – zakłócenie pracy systemu komputerowego lub sieci teleinformatycznej	327
5.10. Artykuł 269b k.k. – tzw. bezprawne wykorzystanie urządzeń, programów i danych	330
5.11. Zbiegi przepisów i przestępstw	337
5.11.1. Uwagi ogólne	337
5.11.2. Uwagi szczegółowe	341
5.12. Problematyka wymiaru kary	349
5.13. Tryb ścigania	353
5.14. Przepisy rozdziału XXXIII kodeksu karnego a postanowienia Konwencji o cyberprzestępczości oraz dyrektywy 2013/40	353

Rozdział 6

Uwagi prawnoporównawcze	359
6.1. Uwagi wstępne	359
6.2. Albania	362
6.3. Czechy	364
6.4. Estonia	370
6.5. Finlandia	372
6.6. Francja	377
6.7. Litwa	381
6.8. Bułgaria	385
6.9. Hiszpania	389
6.10. Niemcy	394
6.11. Norwegia	398
6.12. Szwajcaria	400
6.13. Rosja	402
6.14. Ukraina	404

6.15. Wielka Brytania	408
6.16. Malta	417
Rozdział 7	
Zjawisko hackingu w Polsce	422
7.1. Obraz statystyczny przestępczości komputerowej w Polsce	422
7.2. Wyniki badań empirycznych – uwagi wprowadzające	427
7.3. Sposób załatwienia spraw	428
7.3.1. Odmowa wszczęcia postępowania	428
7.3.2. Umorzenie postępowania	430
7.3.3. „Inny sposób” załatwienia sprawy	432
7.4. Wykrywalność	433
7.5. Kwalifikacje prawne	434
7.6. Oskarżenia	440
7.7. Wymiar kary	442
7.8. Wybrane stany faktyczne	445
7.8.1. „Skasowane” dane	445
7.8.2. Przejęcie konta poczty elektronicznej, konta w komunikatorze internetowym oraz profilu na portalu społecznościowym	446
7.8.3. Atak DDoS na serwery sklepu internetowego	447
7.8.4. Włamanie na konto poczty elektronicznej oraz zlikwidowanie profilu na portalu społecznościowym	448
7.8.5. Nielegalne podłączenie się do sieci radiowej	448
7.8.6. Fałszywe konto na portalu społecznościowym	449
7.8.7. „Kradzież” wirtualnych przedmiotów	450
7.8.8. <i>Pharming</i>	451
7.8.9. Oszustwo na Allegro	452
7.8.10. Przejęcie profilu na portalu społecznościowym	453
7.8.11. „Stup”	454
Uwagi końcowe	457
Bibliografia	467
Wykaz aktów prawnych	483
Orzecznictwo	503