

Spis treści

Wstęp	IX
Wykaz skrótów	XI
Literatura	XXI
A. Komentarz	1
Ustawa o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 r. (Dz.U. 2018, poz. 1560)	3
Wprowadzenie	3
Rozdział 1. Przepisy ogólne	21
Art. 1. Zakres przedmiotowy	21
Art. 2. Objasnienie pojęć	28
Art. 3. Cel wdrożenia krajowego systemu cyberbezpieczeństwa	52
Art. 4. Zakres podmiotowy	52
Rozdział 2. Identyfikacja i rejestracja operatorów usług kluczowych ...	67
Art. 5. Uznanie podmiotu za operatora usługi kluczowej	67
Art. 6. Delegacja ustawowa – wykaz usług kluczowych, progi istotności skutku zakłócającego incydentu dla świadczenia usług kluczowych ...	82
Art. 7. Wykaz operatorów usług kluczowych	86
Rozdział 3. Obowiązki operatorów usług kluczowych	101
Art. 8. Obowiązek wdrożenia systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej	101
Art. 9. Obowiązek wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa; obo- wiązek zapewnienia użytkownikowi usługi kluczowej dostępu do wiedzy w zakresie zagrożeń cyberbezpieczeństwa	111
Art. 10. Dokumentacja dotycząca cyberbezpieczeństwa systemu informa- cyjnego	113
Art. 11. Obsługa incydentu	121
Art. 12. Zgłoszenie incydentu poważnego	125
Art. 13. Informacje przekazywane do właściwego CSIRT	130
Art. 14. Powołanie wewnętrznych struktur odpowiedzialnych za cyberbez- pieczeństwo lub zawarcie umowy z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa	132
Art. 15. Audyt bezpieczeństwa systemu informacyjnego wykorzystywa- nego do świadczenia usługi kluczowej	135
Art. 16. Obowiązki operatora usługi kluczowej	139
Rozdział 4. Obowiązki dostawców usług cyfrowych	142
Art. 17. Status i obowiązki dostawcy usługi cyfrowej	142
Art. 18. Obowiązki w zakresie wykrywania, rejestrowania, analizowania oraz klasyfikowania incydentów	163
Art. 19. Zgłoszenie incydentu istotnego	177
Art. 20. Informacje przekazywane do właściwego CSIRT	180

Rozdział 5. Obowiązki podmiotów publicznych	182
Wprowadzenie	182
Art. 21. Osoba odpowiedzialna za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa	182
Art. 22. Zakres obowiązków podmiotu publicznego	186
Art. 23. Zgłoszenie incydentu w podmiocie publicznym	188
Art. 24. Obowiązek przekazywania informacji	190
Art. 25. Odesłanie do przepisów rozdziału 3	191
Rozdział 6. Zadania CSIRT MON, CSIRT NASK i CSIRT GOV	191
Art. 26. Zadania CSIRT MON, CSIRT NASK i CSIRT GOV	191
Art. 27. CSIRT GOV	210
Art. 28. Informowanie przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV innych państw członkowskich UE, których dotyczy ten incydent	211
Art. 29. Informowanie przez właściwy CSIRT MON, CSIRT NASK lub CSIRT GOV w przypadku, gdy incydent istotny dotyczy dwóch lub większej liczby państw członkowskich UE	212
Art. 30. Zgłaszanie incydentu do CSIRT NASK przez podmioty inne niż operatorzy usług kluczowych i dostawcy usług cyfrowych, w tym osoby fizyczne	213
Art. 31. Określenie sposobu dokonywania zgłoszeń i przekazywania informacji w postaci elektronicznej	215
Art. 32. Wykonywanie niezbędnych działań technicznych związanych z analizą zagrożeń, koordynacją obsługi incydentu poważnego, incydentu istotnego i incydentu krytycznego	216
Art. 33. Badanie urządzenia informatycznego lub oprogramowania	217
Art. 34. Współpraca z organami ścigania i wymiaru sprawiedliwości oraz służbami specjalnymi przy realizacji ich ustawowych zadań	220
Art. 35. Wzajemne informowanie o incydencie krytycznym oraz informowanie o nim Rządowego Centrum Bezpieczeństwa	221
Art. 36. Zespół do spraw Incydentów Krytycznych	223
Rozdział 7. Zasady udostępniania informacji i przetwarzania danych osobowych	226
Art. 37. Publikacja informacji o incydentach istotnych	226
Art. 38. Negatywne przesłanki udostępniania informacji przetwarzanych na podstawie ustawy	235
Art. 39. Dane przetwarzane na podstawie ustawy	242
Art. 40. Przetwarzanie danych stanowiących tajemnice prawnie chronione	256
Rozdział 8. Organy właściwe do spraw cyberbezpieczeństwa	261
Art. 41. Organy właściwe	261
Art. 42. Zakres zadań	266
Art. 43. Wystąpienie o udzielenie informacji	273
Art. 44. Sektorowy zespół cyberbezpieczeństwa	275
Rozdział 9. Zadania ministra właściwego do spraw informatyzacji	276
Art. 45. Zadania ministra	276
Art. 46. Obowiązek zapewnienia rozwoju lub utrzymania systemu teleinformatycznego wspierającego współpracę w ramach krajowego systemu cyberbezpieczeństwa	286
Art. 47. Delegowanie realizacji zadań na jednostki podległe lub nadzorowane przez ministra	288
Art. 48. Zadania Pojedynczego Punktu Kontaktowego	292
Art. 49. Dane przekazywane przez Pojedynczy Punkt Kontaktowy Grupie Współpracy	295

Art. 50. Dane przekazywane przez Pojedynczy Punkt Kontaktowy Komisji Europejskiej	298
Rozdział 10. Zadania Ministra Obrony Narodowej	300
Wprowadzenie	300
Art. 51. Zakres zadań Ministra Obrony Narodowej	300
Art. 52. Prowadzenie Narodowego Punktu Kontaktowego	302
Rozdział 11. Nadzór i kontrola operatorów usług kluczowych, dostawców usług cyfrowych i podmiotów świadczących usługi w zakresie cyberbezpieczeństwa	303
Art. 53. Organy nadzoru	303
Art. 54. Odesłanie do ustawy – Prawo przedsiębiorców	304
Art. 55. Uprawnienia osoby kontrolującej	305
Art. 56. Obowiązki podmiotu kontrolowanego	307
Art. 57. Postępowanie dowodowe	309
Art. 58. Protokół kontroli	311
Art. 59. Zalecenia pokontrolne	315
Rozdział 12. Pełnomocnik i Kolegium	316
Art. 60. Realizacja polityki rządu w zakresie zapewnienia cyberbezpieczeństwa przez Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa	316
Art. 61. Powołanie i odwołanie Pełnomocnika; podległość Radzie Ministrów	317
Art. 62. Zadania Pełnomocnika	318
Art. 63. Roczne sprawozdanie Pełnomocnika; przedstawianie wniosków i rekomendacji	320
Art. 64. Status Kolegium do Spraw Cyberbezpieczeństwa	321
Art. 65. Zadania Kolegium	322
Art. 66. Skład Kolegium; Przewodniczący i Sekretarz Kolegium; szczególony zakres działania i tryb pracy Kolegium	323
Art. 67. Wytyczne Prezesa Rady Ministrów wydawane na podstawie rekomendacji Kolegium	326
Rozdział 13. Strategia	327
Art. 68. Uchwała w sprawie przyjęcia Strategii	327
Art. 69. Zakres Strategii	329
Art. 70. Prace nad projektem Strategii	337
Art. 71. Okresowe przeglądy Strategii	339
Art. 72. Przekazanie Strategii Komisji Europejskiej	339
Rozdział 14. Przepisy o karach pieniężnych	340
Art. 73. Katalog kar pieniężnych	340
Art. 74. Nałożenie kary pieniężnej; wpływ z kar pieniężnych jako dochód budżetu państwa	352
Art. 75. Niedochowanie należytej staranności przez kierownika operatora usługi kluczowej	357
Art. 76. Nałożenie kary mimo zaprzestania naruszeń lub naprawienia szkody	358
Rozdział 15. Zmiany w przepisach, przepisy przejściowe, dostosowujące i końcowe	359
Art. 77. Zmiany do ustawy o systemie oświaty	359
Art. 78. Zmiany do ustawy o działach administracji rządowej	361
Art. 79. Zmiany do ustawy o ABW i AW	362
Art. 80. Zmiany do ustawy – Prawo zamówień publicznych	364
Art. 81. Zmiany do ustawy – Prawo telekomunikacyjne	366
Art. 82. Zmiany do ustawy o zarządzaniu kryzysowym	367

Spis treści

Art. 83. Raport o zagrożeniach bezpieczeństwa narodowego	371
Art. 84. Termin powołania Pełnomocnika	372
Art. 85. Zakres informacji dotyczący wyznaczonych organów właściwych do spraw cyberbezpieczeństwa, Pojedynczego Punktu Kontaktowego, CSIRT MON, CSIRT NASK i CSIRT GOV przekazanych Komisji Europejskiej	373
Art. 86. Termin wydania decyzji o uznaniu za operatora usługi kluczowej	374
Art. 87. Termin przekazania sprawozdania podsumowującego	374
Art. 88. Termin przekazania Komisji Europejskiej informacji dotyczących operatorów usług kluczowych oraz ich zakres	376
Art. 89. Termin uruchomienia systemu teleinformatycznego	377
Art. 90. Termin przyjęcia strategii	377
Art. 91. Roczny plan wdrożenia	378
Art. 92. Derogacja przepisów wykonawczych	380
Art. 93. Limit wydatków z budżetu państwa	383
Art. 94. Wejście w życie	387
Załączniki Nr 1–2	
B. Aneks	397
1. Rozporządzenie Rady Ministrów w sprawie progów uznania incydentu za poważny z dnia 31 października 2018 r. (Dz.U. 2018, poz. 2180)	399
2. Rozporządzenie wykonawcze Komisji (UE) 2018/151 z dnia 30 stycznia 2018 r. ustanawiające zasady stosowania dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 w odniesieniu do dalszego doprecyzowania elementów, jakie mają być uwzględnione przez dostawców usług cyfrowych w zakresie zarządzania istniejącymi ryzykami dla bezpieczeństwa sieci i systemów informatycznych, oraz parametrów służących do określenia, czy incydent ma istotny wpływ z dnia 30 stycznia 2018 r. (Dz.Urz. UE L 2018, poz. 48)	424
Indeks rzeczowy	429