

Spis treści

|                                                                                            |            |
|--------------------------------------------------------------------------------------------|------------|
| <b>Wykaz skrótów i akronimów</b>                                                           | <b>9</b>   |
| <b>Wprowadzenie</b>                                                                        | <b>11</b>  |
| <b>Rozdział I. Cyberbezpieczeństwo jako przedmiot zainteresowań naukowych i badawczych</b> | <b>29</b>  |
| 1. Nauka o cyberbezpieczeństwie                                                            | 29         |
| 2. Kluczowe pojęcia                                                                        | 31         |
| 2.1. Etymologia pojęć kluczowych                                                           | 31         |
| 2.2. Cyberprzestępczość, cyberprzestrzeń i cyberbezpieczeństwo                             | 34         |
| 2.3. Bezpieczeństwo informacji, naruszenie bezpieczeństwa informacji i incydent            | 46         |
| 3. Podsumowanie                                                                            | 56         |
| <b>Rozdział II. Wprowadzenie do cyberbezpieczeństwa</b>                                    | <b>59</b>  |
| 1. Cyberbezpieczeństwo w ujęciu międzynarodowym                                            | 60         |
| 1.1. Organizacja Narodów Zjednoczonych                                                     | 62         |
| 1.2. Organizacja Traktatu Północnoatlantyckiego                                            | 67         |
| 1.3. Rada Europy                                                                           | 72         |
| 1.4. Unia Europejska                                                                       | 77         |
| 2. Cyberbezpieczeństwo w Rzeczypospolitej Polskiej                                         | 85         |
| 2.1. Dokumenty strategiczne                                                                | 86         |
| 3. Podsumowanie                                                                            | 93         |
| <b>Rozdział III. Dyrektywa NIS i Ustawa o krajowym systemie cyberbezpieczeństwa</b>        | <b>99</b>  |
| 1. Potrzeba opracowania aktu prawnego w zakresie cyberbezpieczeństwa                       | 101        |
| 2. Prace nad Dyrektywą                                                                     | 107        |
| 2.1. Wczesne prace koncepcyjne                                                             | 107        |
| 2.2. Proces legislacyjny                                                                   | 111        |
| 3. Implementacja postanowień Dyrektywy do porządku krajowego Rzeczypospolitej Polskiej     | 116        |
| 4. Nowelizacja Dyrektywy NIS i Ustawy                                                      | 122        |
| 4.1. Projekt nowelizacji Ustawy                                                            | 122        |
| 4.2. Projekt aktu nowelizującego Dyrektywę NIS                                             | 124        |
| 5. Podsumowanie                                                                            | 128        |
| <b>Rozdział IV. Dostawcy usług cyfrowych w krajowym systemie cyberbezpieczeństwa</b>       | <b>133</b> |
| 1. Zakres podmiotowy ustawy o krajowym systemie cyberbezpieczeństwa                        | 133        |

|                                                                   |     |
|-------------------------------------------------------------------|-----|
| 1.1. Operatorzy usług kluczowych                                  | 136 |
| 1.2. Podmioty publiczne                                           | 144 |
| 1.3. CSIRT                                                        | 146 |
| 2. Dostawcy usług cyfrowych jako odrębna kategoria podmiotowa     | 149 |
| 2.1. Usługa świadczona drogą elektroniczną                        | 152 |
| 2.2. Rodzaje usług cyfrowych                                      | 154 |
| 2. Wymagania bezpieczeństwa dostawców usług cyfrowych             | 158 |
| 3. Obowiązki dostawców usług cyfrowych                            | 166 |
| 3.1. Obowiązek przeprowadzenia czynności związanych z incydentami | 168 |
| 3.2. Klasyfikacja incyduentu jako istotny                         | 169 |
| 3.3. Obowiązek zgłoszeniowy                                       | 172 |
| 3.4. Obowiązek informacyjny                                       | 179 |
| 3.5. Obowiązek obsługi                                            | 181 |
| 3.6. Obowiązek utrzymywania odpowiedniego poziomu bezpieczeństwa  | 183 |
| 3.6.1. Bezpieczeństwo systemów i obiektów                         | 185 |
| 3.6.2. Postępowanie w przypadku incyduentu                        | 186 |
| 3.6.3. Zarządzanie ciągłością działania                           | 187 |
| 3.6.4. Monitorowanie, audyt i testowanie                          | 188 |
| 3.6.5. Stosowanie norm                                            | 190 |
| 4. Pozycja dostawców usług cyfrowych w innych państwach           | 191 |
| 4.1. Francja                                                      | 192 |
| 4.2. Niemcy                                                       | 196 |
| 4.3. Wielka Brytania                                              | 198 |
| 5. Podsumowanie                                                   | 201 |

## **Rozdział V. Spełnianie obowiązków i wymagań nałożonych na dostawców usług cyfrowych**

|                                                                                                                    |     |
|--------------------------------------------------------------------------------------------------------------------|-----|
| 1. Określenie obowiązków dostawców usług cyfrowych                                                                 | 205 |
| 2. Normy ISO                                                                                                       | 208 |
| 2.1. ISO/IEC 27001 i 27002                                                                                         | 211 |
| 2.2. ISO 27032                                                                                                     | 217 |
| 2.3. Standardy przewidziane dla dostawców usług chmurowych                                                         | 219 |
| 3. Dokumenty przygotowane w ramach działalności ENISA                                                              | 224 |
| 3.1. <i>Technical Guidelines for the Implementation of Minimum Security Measures for Digital Service Providers</i> | 227 |
| 3.2. <i>Guidelines on Assessing DSP Security and OES Compliance with the NISD Security Requirements</i>            | 231 |
| 3.3. <i>Incident Notification for DSPs in the Context of the NIS Directive</i>                                     | 233 |
| 3.4. <i>Good Practices on Interdependencies Between OES and DSPs</i>                                               | 236 |
| 4. Pozostałe przypadki dokumentów o charakterze pomocniczym                                                        | 239 |
| 5. Podsumowanie                                                                                                    | 243 |

## **Zakończenie**

## **Bibliografia**