

# SPIS TREŚCI

|                                                                                                                                |           |
|--------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>I. Ogólne zasady bezpieczeństwa: dobre praktyki</b><br>[B. Marek, M. Juszczyk, M. Hornowski]                                | <b>6</b>  |
| <b>II. Bezpieczeństwo urządzeń</b>                                                                                             | <b>14</b> |
| 1. Informacje wprowadzające [K. Pszczółkowski, B. Marek]                                                                       | 14        |
| 2. Dlaczego warto szyfrować pliki, foldery, dyski?<br>Jak to zrobić? [G. Cenquier]                                             | 15        |
| 3. Jak i po co zmienić hasło routera / komunikacji Wi-Fi? [G. Cenquier]                                                        | 18        |
| 4. Zasady dotyczące haseł [K. Pszczółkowski]                                                                                   | 20        |
| 5. Jak wyłączyć skradziony telefon komórkowy? [G. Cenquier]                                                                    | 21        |
| 6. Lista kontrolna – jak dbam o bezpieczeństwo urządzeń,<br>na których przetwarzam dane klientów [B. Marek]                    | 22        |
| 7. Uwierzytelnienie wieloskładnikowe (MFA) [G. Cenquier]                                                                       | 23        |
| <b>III. Usługi chmurowe [K. Grzela]</b>                                                                                        | <b>24</b> |
| 1. Informacje wprowadzające                                                                                                    | 24        |
| 2. Zagrożenia                                                                                                                  | 29        |
| 3. Dobre praktyki – czym warto kierować się jeśli organizacja<br>ma przetwarzać dane w chmurze                                 | 30        |
| <b>IV. Wymiana informacji z klientem</b>                                                                                       | <b>34</b> |
| 1. Dlaczego przysyłanie wiadomości przez formularz na stronie<br>www po HTTPS jest bezpieczniejsze niż po HTTP? [M. Hornowski] | 34        |
| 2. Jakie pliki warto szyfrować przy przysyłaniu ich do klienta? [B. Marek]                                                     | 35        |
| 3. W jaki sposób przysyłać większe ilości plików? [B. Marek]                                                                   | 36        |
| 4. Lista kontrolna - jak dbam o wymianę informacji<br>z klientami? [B. Marek]                                                  | 37        |
| <b>V. Przetwarzanie danych osobowych zgodnie<br/>z RODO [B. Marek, G. Cenquier]</b>                                            | <b>38</b> |
| 1. Obowiązki prawne [G. Cenquier]                                                                                              | 38        |

|                                                                                                                 |           |
|-----------------------------------------------------------------------------------------------------------------|-----------|
| 2. Wymagania bezpieczeństwa dla systemu teleinformatycznego przetwarzającego dane osobowe [K. Pszczółkowski]    | 44        |
| 3. Zabezpieczenia organizacyjne dot. przetwarzania danych osobowych [K. Pszczółkowski]                          | 46        |
| 4. Zasady odbioru nowego systemu teleinformatycznego, który planuje przetwarzać dane osobowe [K. Pszczółkowski] | 48        |
| 5. Zasady tworzenia, testowania i przechowywania kopii zapasowych [K. Pszczółkowski]                            | 49        |
| 6. Lista kontrolna [K. Pszczółkowski, B. Marek]                                                                 | 51        |
| <b>VI. Prywatność w sieci [B. Gębura]</b>                                                                       | <b>53</b> |
| 1. Wprowadzenie                                                                                                 | 53        |
| <b>VII. Przykładowe ataki i jak się przed nimi bronić [P. Brogowski, G. Cenquier, M. Hornowski, B. Marek]</b>   | <b>63</b> |
| 1. Kradzież sprzętu i wyciek danych [P. Brogowski]                                                              | 63        |
| 2. DDoS [P. Brogowski]                                                                                          | 66        |
| 3. Phishing [G. Cenquier]                                                                                       | 67        |
| 4. Ransomware [M. Hornowski, B. Marek]                                                                          | 69        |
| 5. Socjotechniczna ucieczka [G. Cenquier]                                                                       | 71        |
| 6. Cyberstalking [P. Brogowski]                                                                                 | 71        |
| <b>VIII. Cyberhigiena [P. Brogowski]</b>                                                                        | <b>74</b> |
| <b>IX. Scam, czyli jak nie dać się oszukać i jak bezpiecznie robić zakupy w sieci [P. Brogowski]</b>            | <b>79</b> |
| <b>X. Nigdy nie wierz, zawsze sprawdzaj - Zero Trust [G. Cenquier]</b>                                          | <b>85</b> |
| <b>Zasady korzystania z publikacji</b>                                                                          | <b>87</b> |