

SPIS TREŚCI

Wykaz skrótów	11
Wstęp	13
Rozdział 1	
Wprowadzenie	15
1. Uwagi ogólne	15
2. Ramy prawne cyberbezpieczeństwa w jednostkach samorządu terytorialnego – konieczność koordynacji przepisów	18
Rozdział 2	
Czym jest cyberbezpieczeństwo?	19
1. Definicja cyberbezpieczeństwa	19
2. Najbardziej rozpowszechnione rodzaje cyberataków	22
2.1. <i>Phishing</i>	22
2.2. <i>Malware</i>	22
2.3. DDoS	23
Rozdział 3	
Ustawa o krajowym systemie cyberbezpieczeństwa	24
1. Krajowy system cyberbezpieczeństwa	24
2. Operatorzy usług kluczowych	26
3. Dostawcy usług cyfrowych	29
4. Obowiązki podmiotów publicznych	29
5. Realizacja zadania publicznego zależnego od systemu informacyjnego	30

6. Wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa	31
7. Zgłoszenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa do właściwego CSIRT	34
8. Pozostałe obowiązki podmiotu publicznego	35
9. Zapewnienie zarządzania incydem w podmiocie publicznym	36
10. Zgłoszenie incydemu w podmiocie publicznym	37
11. Zgłoszenie incydemu – zbieg z innymi przepisami	41
12. Zgłoszenie incydemu – zbieg z innymi przepisami, zestawienie	44
13. Zapewnienie obsługi incydemu i incydemu krytycznego ...	47
14. Zapewnianie dostępu do wiedzy osobom, na rzecz których zadanie publiczne jest realizowane	49
15. CSIRT NASK – CSIRT właściwy dla jednostek samorządu terytorialnego?	50

Rozdział 4

Krajowe Ramy Interoperacyjności	51
1. Uwagi wstępne	51
2. Główne wymagania dotyczące systemu zarządzania bezpieczeństwem informacji	53
3. Obowiązki kierownictwa podmiotu publicznego w odniesieniu do zarządzania bezpieczeństwem informacji	55
3.1. Dokumentacja	56
3.2. Inwentaryzacja systemów IT	58
3.3. Analiza ryzyka	60
3.3.1. Kroki szacowania ryzyka	61
3.4. Uprawnienia personelu	67
3.5. Szkolenia	67
3.6. Ochrona, zabezpieczenie i ogólne zasady postępowania z informacjami	68
3.7. Praca mobilna/praca zdalna	69
3.8. Umowy	74
3.9. Odpowiedni poziom bezpieczeństwa w systemach teleinformatycznych	75
3.10. Reagowanie na incydenty	77
3.11. Audyt	78

3.12. Dodatkowe zabezpieczenia wprowadzone na podstawie analizy ryzyka	82
4. Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego – Informacja o wynikach kontroli Najwyższej Izby Kontroli	83
5. Realizacja obowiązków w odniesieniu do zarządzania bezpieczeństwem informacji a Polskie Normy	84

Rozdział 5

Przetwarzanie i ochrona danych osobowych w kontekście cyberbezpieczeństwa	86
1. Uwagi wstępne	86
2. Przetwarzane danych w sposób zapewniający ich odpowiednie bezpieczeństwo – zasada integralności i poufności danych	87
3. Obowiązki ogólne administratora danych osobowych	90
4. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorcemu	91

Rozdział 6

Chmura obliczeniowa a cyberbezpieczeństwo	92
1. Uwagi wstępne	92
2. Standardy Cyberbezpieczeństwa Chmur Obliczeniowych ...	95
2.1. Uwagi ogólne	95
2.2. Poziomy Wymagań Bezpieczeństwa SCCO	96
2.3. Proces przygotowania do przetwarzania informacji w modelach chmur obliczeniowych	99
2.4. Wymagania bezpieczeństwa dotyczące korzystania z usług chmur obliczeniowych przez jednostki administracji publicznej	104

Rozdział 7

Rola prawnika urzędu w budowie cyberbezpieczeństwa	106
1. Uwagi wstępne	106
2. Trzy etapy cyberbezpieczeństwa	107
3. Bezpieczeństwo cybernetyczne pracy prawnika	109
3.1. Stanowisko Komisji Etyki i Wykonywania Zawodu Krajowej Izby Radców Prawnych dotyczące zaleceń dla radców prawnych w zakresie stosowania wideokonferencji jako formy kontaktu z klientami	111

3.2. Ocena zgodności wykorzystania usług wideokonferencyjnych różnych dostawców (Microsoft Teams, będącej częścią pakietu Microsoft 365, Zoom 5.0, Cisco Webex) do komunikowania się radców prawnych z klientami w ramach wykonywania zawodu	112
3.3. Analiza porównawcza ogólnej zgodności oraz niektórych elementów bezpieczeństwa aplikacji do telekonferencji	113
3.4. Stanowisko Komisji Etyki i Wykonywania Zawodu Krajowej Izby Radców Prawnych dotyczące zaleceń dla radców prawnych w zakresie stosowania jako formy kontaktu z klientami przy wykonywaniu czynności zawodowych poczty elektronicznej	114
3.5. Rekomendacje dla radców prawnych dotyczące bezpieczeństwa poczty elektronicznej w praktyce wykonywania zawodu radcy prawnego w kontekście obowiązku zachowania tajemnicy zawodowej oraz ochrony danych osobowych	115
3.6. Analiza porównawcza ogólnej zgodności chmurowych systemów najbardziej popularnych dostawców (Microsoft Exchange i Google G Suite)	118
3.7. Informacja dotycząca szyfrowania poczty elektronicznej przez wybranych dostawców	118
3.8. Ocena zgodności Exchange Online, Gmail, iCloud Mail dla celów działalności radców prawnych	119
3.9. Ocena bezpieczeństwa danych przechowywanych przez radców prawnych w wybranych chmurach	120
4. Uwagi końcowe	121
Podsumowanie – odpowiedzi na często zadawane pytania	122
Bibliografia	133