

CYBERBEZPIECZEŃSTWO W SAMORZĄDZIE TERYTORIALNYM

Praktyczny przewodnik

Wojciech Dziomdziora

CYBERBEZPIECZEŃSTWO W SAMORZĄDZIE TERYTORIALNYM

Praktyczny przewodnik

CYBERBEZPIECZEŃSTWO W SAMORZĄDZIE TERYTORIALNYM

Praktyczny przewodnik

Wojciech Dziomdziora



Wolters Kluwer

WARSZAWA 2021

Stan prawny na 1 stycznia 2021 r.

Wydawca

Anna Kubuj-Kacperek

Redaktor prowadzący

Paulina Ambroży

Opracowanie redakcyjne

Agnieszka Witczak

Projekt okładek serii

Wojtek Kwiecień-Janikowski, Przemek Dębowski

prawolubni

Ta książka jest wspólnym dziełem twórcy i wydawcy. Prosimy, byś przestrzegał przysługujących im praw. Książkę możesz udostępnić osobom bliskim lub osobiście znanym, ale nie publikuj jej w internecie. Jeśli cytujesz fragmenty, nie zmieniaj ich treści i koniecznie zaznacz, czyje to dzieło. A jeśli musisz skopiować część, rób to jedynie na użytek osobisty.

Szanujemy prawo i własność

Więcej na www.legalnakultura.pl

Polska Izba Książki

© Copyright by Wolters Kluwer Polska Sp. z o.o., 2021

ISBN 978-83-8223-413-8

Dział Praw Autorskich

01-208 Warszawa, ul. Przyokopowa 33

tel. 22 535 82 19

e-mail: ksiazki@wolterskluger.pl

księgarnia internetowa www.profinfo.pl

Pracę tę poświęcam
nieodżałowanemu prof. Michałowi Kuleszy,
mojemu nauczycielowi

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 incydemem w podmiocie publicznym	36
10. Zgłoszenie incydentu w podmiocie publicznym	37
11. Zgłoszenie incydentu – zbieg z innymi przepisami	41
12. Zgłoszenie incydentu – zbieg z innymi przepisami, zestawienie	44
13. Zapewnienie obsługi incydentu i incydentu 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 nadzorczemu	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

WYKAZ SKRÓTÓW

Akty prawne

- dyrektywa NIS** – dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6.07.2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE L 194, s. 1)
- RODO** – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1)
- rozp. KRI** – rozporządzenie Rady Ministrów z 12.04.2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r. poz. 2247)
- u.ABW** – ustawa z 24.05.2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2020 r. poz. 27 ze zm.)
- u.i.d.p.** – ustawa z 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2020 r. poz. 346 ze zm.)
- u.k.s.c.** – ustawa z 5.07.2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369 ze zm.)
- WIIP** – uchwała nr 97 Rady Ministrów z 11.09.2019 r. w sprawie Inicjatywy „Wspólna Infrastruktura Informatyczna Państwa” (M.P. poz. 862)

Inne

CSIRT	– Computer Security Incident Response Team (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego)
Dz.U.	– Dziennik Ustaw
Dz.Urz. Min. Fin.	– Dziennik Urzędowy Ministra Finansów
Dz.Urz. UE	– Dziennik Urzędowy Unii Europejskiej
EOG	– Europejski Obszar Gospodarczy
ePUAP	– Elektroniczna Platforma Usług Administracji Publicznej
MAiC	– Ministerstwo Administracji i Cyfryzacji
MF	– Ministerstwo Finansów
M.P.	– Monitor Polski
NIST	– National Institute of Standards and Technology
PBI	– polityka bezpieczeństwa informacji
SCCO	– Standardy Cyberbezpieczeństwa Chmur Obliczeniowych
UODO	– Urząd Ochrony Danych Osobowych

WSTĘP

Stan cyberbezpieczeństwa, w szczególności bezpieczeństwa informacji, w jednostkach samorządu terytorialnego jest niewystarczający, co potwierdzają oficjalne dokumenty¹. Jednocześnie aktywność cyberprzestępców rośnie, a jednostki samorządu terytorialnego stają się ich coraz łatwiejszym i atrakcyjniejszym łupem. Wraz z wejściem w życie ustawy o krajowym systemie cyberbezpieczeństwa oraz RODO i towarzyszącej mu nowej ustawy o ochronie danych osobowych pojawiły się nowe narzędzia prawne dotyczące cyberbezpieczeństwa. Dzięki aktywności NASK-u oraz takim inicjatywom, jak Rządowa Chmura Obliczeniowa jednostki samorządu terytorialnego zyskują coraz więcej skutecznych narzędzi do dbania o swoje cyberbezpieczeństwo.

Niniejszy poradnik ma na celu pomóc w realizacji zadań z zakresu cyberbezpieczeństwa, wskazując przede wszystkim jego aspekty prawne. We wprowadzeniu (rozdział 1) przedstawiono zarys ram prawnych cyberbezpieczeństwa i wskazano na konieczność koordynacji stosowania przepisów różnych aktów prawnych, w szczególności ustawy o krajowym systemie cyberbezpieczeństwa, Krajowych Ram Interoperacyjności oraz RODO. Ten wątek przewija się również w innych częściach poradnika. W rozdziale 2 omówiono definicję cyberbezpieczeństwa oraz typowe rodzaje ataków cybernetycznych.

¹ Informacja o wynikach kontroli – *Zarządzanie bezpieczeństwem informacji w jednostkach samorządu terytorialnego*, Najwyższa Izba Kontroli, 10.05.2019 r., <https://www.nik.gov.pl/kontrola/P/18/006/> (dostęp: 20.11.2020 r.).

Rozdział 3 zawiera omówienie przepisów ustawy o krajowym systemie cyberbezpieczeństwa dotyczących jednostek samorządu terytorialnego. Kolejny rozdział poświęcony został analizie postanowień Krajowych Ram Interoperacyjności, które stanowią dopełnienie regulacji zawartych w ustawie o krajowym systemie cyberbezpieczeństwa. Rozdział 5 ukazuje ścisłe relacje, jakie występują między przepisami o cyberbezpieczeństwie a przepisami regulującymi ochronę danych osobowych. Celem było podkreślenie, że w dużej mierze są to te same procesy i nie wolno patrzeć na te dwie sfery w sposób odmienny. Rozdział 6 przedstawia kwestie prawne związane z korzystaniem z chmury obliczeniowej, które może w sposób znaczny przyczynić się zarówno do podniesienia poziomu usług informatycznych, jak i do zwiększenia cyberbezpieczeństwa w jednostkach samorządu terytorialnego. W rozdziale 7 przedstawiono zasady dbania o bezpieczeństwo informacji, jakimi powinni kierować się prawnicy w swojej codziennej pracy. Podsumowanie zaś przyjęło formę pytań i odpowiedzi.