CYBERBEZPIECZEŃSTWO W SAMORZĄDZIE TERYTORIALNYM

Praktyczny przewodnik

Wojciech Dziomdziora

Wolters Kluwer

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

ISBN 978-83-8223-413-8

Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. 22 535 82 19
e-mail: ksiazki@wolterskluwer.pl

księgarnia internetowa www.profinfo.pl

Pracę tę poświęcam
nieodżałowanemu prof. Michałowi Kuleszy,
mojemu nauczycielowi

SPIS TREŚCI

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 dokumenty[1]. 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/kontrole/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.

kować". Konieczne może być na przykład wejście na drogę prawną przeciwko dostarczycielom rozwiązań teleinformatycznych, z których winy lub niedbalstwa dopuszczono do incydentu. Innym przykładem działań ofensywnych są kroki prawne przeciwko pracownikom lub byłym pracownikom, którzy nie dochowali obowiązków pracowniczych, co doprowadziło lub przyczyniło się do zaistnienia incydentu.

3. Bezpieczeństwo cybernetyczne pracy prawnika

Obecnie podstawowym narzędziem pracy każdego prawnika jest komputer i smartfon. Prawnicy stale korzystają z różnego rodzaju oprogramowania służącego do edycji tekstów, komunikacji, archiwizowania czy baz danych. Jednocześnie dane, jakie prawnicy przetwarzają, są danymi podlegającymi szczególnej ochronie. Niejednokrotnie są to informacje poufne lub szczególnie wrażliwe dane osobowe. Zarówno przepisy powszechnie obowiązujące, jak i dokumenty przyjmowane przez korporacje zawodowe prawników, na czele z izbami radców prawnych i radami adwokackimi, zobowiązują do szczególnej ochrony tajemnicy radcowskiej oraz adwokackiej. Dobrym przewodnikiem są materiały opracowywane i ogłaszane przez Krajową Izbę Radców Prawnych oraz okręgowe izby radców prawnych. Przykładem może być *Księga bezpieczeństwa komunikacji elektronicznej w pracy radcy prawnego*[2], w której dwóch wydanych dotąd częściach:

1) przedstawiono stanowisko Komisji Etyki i Wykonywania Zawodu Krajowej Izby Radców Prawnych dotyczące zaleceń dla radców prawnych w zakresie stosowania wideokonferencji jako formy kontaktu z klientami;
2) omówiono ocenę zgodności wykorzystania usług wideokonferencyjnych różnych dostawców (Microsoft Teams, będącej

[2] https://kirp.pl/wp-content/uploads/2020/06/ksiega-bezpieczenstwa-1.pdf i https://kirp.pl/wp-content/uploads/2020/10/ksiega-bezpieczenstwa-2.pdf (dostęp: 23.10.2020 r.).

częścią pakietu Microsoft 365, Zoom 5.0, Cisco Webex) do komunikowania się radców prawnych z klientami w ramach wykonywania zawodu;
3) zawarto analizę porównawczą ogólnej zgodności oraz niektórych elementów bezpieczeństwa aplikacji do telekonferencji;
4) przedstawiono 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 (*electronic mail*);
5) przedstawiono rekomendacje dla radców prawnych dotyczące bezpieczeństwa poczty elektronicznej w praktyce wykonywania zawodu radcy prawnego w kontekście obowiązku zachowania tajemnicy zawodowej oraz ochrony danych osobowych;
6) podjęto kwestie ogólnej zgodności chmurowych systemów najbardziej popularnych dostawców (Microsoft Exchange i Google G Suite);
7) przekazano informację dotyczącą szyfrowania poczty elektronicznej przez wybranych dostawców;
8) omówiono ocenę zgodności Exchange Online, Gmail, iCloud Mail dla celów działalności radców prawnych;
9) oceniono bezpieczeństwo danych przechowywanych przez radców prawnych w wybranych chmurach.

Rekomendacje i opinie wyrażone w *Księdze bezpieczeństwa…* skierowane są do radców prawnych, ale mają charakter uniwersalny i powinny być brane pod uwagę także przez prawników niebędących radcami i przez innych profesjonalistów, w tym urzędników samorządowych, na co dzień posługujących się systemami teleinformatycznymi w swej pracy. Dlatego warto bliżej się im przyjrzeć.

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

W stanowisku z 3.4.2020 r.[3] Komisja Etyki i Wykonywania Zawodu Krajowej Izby Radców Prawnych uznaje stosowanie wideokonferencji jako formy kontaktu z klientami za dopuszczalne, przy zachowaniu następujących warunków:

1) zapewnienie środków technicznych mających zabezpieczyć przed ujawnieniem tajemnicy zawodowej, w szczególności przed dostępem do wideokonferencji osób nieuprawnionych (niepowołanych);
2) w przypadku organizacji wideokonferencji przez radcę prawnego – dołożenie przez radcę prawnego staranności wymaganej od profesjonalisty w zakresie zapewnienia narzędzia posiadającego zabezpieczenia chroniące przed dostępem osób nieuprawnionych do wideokonferencji, ujawnieniem jej przebiegu czy możliwości odtworzenia jej przebiegu, przy czym w przypadku braku wystarczającej wiedzy w tym zakresie – skorzystanie z pomocy osoby dysponującej taką specjalistyczną wiedzą;
3) w przypadku organizacji wideokonferencji przez klienta radca prawny powinien uprzedzić go o możliwych ryzykach związanych z używaniem tego narzędzia oraz o konieczności wyboru odpowiednich zabezpieczeń;
4) w przypadku utrwalenia wideokonferencji na nośniku informacji należy postępować z nim zgodnie z zasadami określonymi w Kodeksie Etyki Radcy Prawnego oraz Regulaminie wykonywania zawodu radcy prawnego.

Ponadto Komisja zaleciła „systematyczne zapoznawanie się radców prawnych z zaleceniami i rekomendacjami właściwych organów i jed-

[3] Krajowa Izba Radców Prawnych, *Księga bezpieczeństwa komunikacji elektronicznej w pracy radcy prawnego*, s. 7 i n., https://kirp.pl/wp-content/uploads/2020/06/ksiega-bezpieczenstwa-1.pdf (dostęp: 23.10.2020 r.).

nostek organizacyjnych administracji państwowej dotyczącymi pracy zdalnej z wykorzystaniem środków komunikacji na odległość oraz rozważenie stosowania się do nich. Tytułem przykładu wskazać można na porady Urzędu Ochrony Danych Osobowych dotyczące ochrony danych osobowych podczas pracy zdalnej z dnia 17 marca 2020 r. (Ochrona danych osobowych podczas pracy zdalnej, https://uodo.gov.pl/pl/138/1459, zamieszczone także na stronie internetowej Krajowej Izby Radców Prawnych: https://kirp.pl/wp-content/uploads/2020/03/ochronadanych-osobowych-podczas-pracy-zdalnej.pdf)".

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

W podsumowaniu opinii prawnej dotyczącej oceny zgodności wykorzystania usług wideokonferencyjnych różnych dostawców w komunikacji przez radców z klientami w ramach wykonywania zawodu[4] jej autorzy stwierdzili w szczególności, że:

1) korzystanie z Teams, Zoom i Webex jest w pełni dozwolone dla radców prawnych, gdyż:
   a) „dostawcy każdej z usług oferują zgodną z wymogami RODO umowę powierzenia przetwarzania danych,
   b) każdy z dostawców oferuje przechowywanie danych klienta (kontent) na terenie UE,
   c) każdy z dostawców przekazuje pewne dane (telemetryczne, dane tożsamościowe użytkowników, dane rozliczeniowe) poza UE na podstawie konkretnych instrumentów prawnych (Tarcza Prywatności i standardowe klauzule umowne – SCC),

[4] M. Gawroński, M. Ćwiakowski, P. Szurmak, *Ocena zgodności wykorzystania usług wideokonferencyjnych Teams, Zoom, Webex w działalności radców prawnych* [w:] Krajowa Izba Radców Prawnych, *Księga bezpieczeństwa*…, s. 14 i n.

d) każdy z dostawców oferuje odpowiednie techniczne i organizacyjne środki bezpieczeństwa danych, dające przekonanie o tym, że treść komunikacji pozostanie poufna,
e) w konsekwencji każdy z dostawców zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą, o których mowa w art. 28 ust. 1 RODO,
f) każdy z dostawców daje wystarczające gwarancje poufności komunikacji";

2) dostawcy ocenianych usług „zapewniają techniczne i organizacyjne środki zapewniające ochronę komunikacji przed dostępem osób trzecich", ale trzeba umieć odpowiednio korzystać z tych narzędzi i właściwie je konfigurować, co zostało omówione szczegółowo w opinii;
3) radcowie prawni jako gospodarze spotkań wideokonferencyjnych powinni informować ich uczestników o sposobie przetwarzania ich danych osobowych (art. 13 RODO) oraz udostępniać im regulamin usługi wideokonferencji, ponieważ ma ona charakter usługi świadczonej drogą elektroniczną w rozumieniu ustawy z 18.07.2002 r. o świadczeniu usług drogą elektroniczną[5].

3.3. Analiza porównawcza ogólnej zgodności oraz niektórych elementów bezpieczeństwa aplikacji do telekonferencji

W podsumowaniu analizy[6] stwierdzono, że wszyscy dostawcy analizowanych usług (Zoom, Teams, Webex) powinni zapewnić taki poziom ochrony, aby móc uznać, że „korzystanie z usług każdego z podmiotów objętych analizą będzie dopuszczalne zgodnie z RODO, a wskazani dostawcy zapewniają odpowiednie

[5] Dz.U. z 2020 r. poz. 344.

[6] M. Wielisiej, *Analiza porównawcza ogólnej zgodności oraz niektórych elementów bezpieczeństwa aplikacji do telekonferencji* [w:] Krajowa Izba Radców Prawnych, *Księga bezpieczeństwa*…, s. 52.

gwarancje stosowania przepisów o ochronie danych", przy czym „absolutną koniecznością jest zapewnienie świadomego korzystania z wybranych narzędzi – zarówno przez użytkowników, organizatorów, jak też przez administratorów tych narzędzi po stronie organizacji".

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

W stanowisku z 18.6.2020 r.[7] Komisja Etyki i Wykonywania Zawodu Krajowej Izby Radców Prawnych wskazała następujące kwestie związane z korzystaniem z poczty elektronicznej jako formy kontaktu z klientami przy wykonywaniu czynności zawodowych w kontekście ogólnej zasady dotyczącej obowiązku przestrzegania tajemnicy zawodowej, rozumianego w szczególności jako obowiązek zachowania, zapewnienia i zabezpieczenia tej tajemnicy:

1) należy zabezpieczać pocztę elektroniczną przed jej ujawnieniem, a w szczególności przed dostępem do niej osób nieuprawnionych (niepowołanych); należy również dokonywać okresowych przeglądów zasobów poczty elektronicznej oraz trwale usuwać wiadomości wraz z załącznikami, których archiwizacja w skrzynce pocztowej nie jest niezbędna albo istnieje obowiązek ich usunięcia;
2) narzędzie, z którego korzysta się dla używania poczty elektronicznej, powinno posiadać „zabezpieczenia chroniące przed dostępem osób nieuprawnionych do poczty elektronicznej, ujawnieniem wiadomości, w tym dokumentów, przekazywanych przy jej wykorzystaniu czy możliwości odtworzenia tych wiadomości, w tym dokumentów, przy czym w przypadku braku wystarczającej wiedzy w tym zakresie – skorzystanie

[7] Krajowa Izba Radców Prawnych, *Księga bezpieczeństwa*…, s. 55 i n.

z pomocy osoby dysponującej specjalistyczną wiedzą w tym zakresie";
3) jeśli klient radcy prawnego korzysta z poczty elektronicznej, powinien on zostać uprzedzony przez radcę prawnego „o możliwych ryzykach związanych z używaniem tego narzędzia oraz o konieczności wyboru odpowiednich zabezpieczeń";
4) „w przypadku utrwalenia wiadomości, w tym dokumentów, przekazywanych z wykorzystaniem poczty elektronicznej na nośniku informacji należy postępować z nim zgodnie z zasadami określonymi w Kodeksie Etyki Radcy Prawnego oraz Regulaminie wykonywania zawodu radcy prawnego".

Ponadto Komisja Etyki i Wykonywania Zawodu zaleciła „systematyczne zapoznawanie się radców prawnych z zaleceniami i rekomendacjami właściwych administratorów poczty elektronicznej dotyczącymi zasad korzystania z tego narzędzia, w tym zasad bezpieczeństwa, oraz rozważenie stosowania się do nich".

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

Omawiany dokument zawiera bardzo długą listę rekomendacji dla radców prawnych. Przedstawiono między innymi rekomendacje dotyczące bezpieczeństwa poczty elektronicznej w praktyce wykonywania zawodu radcy prawnego w kontekście obowiązku zachowania tajemnicy zawodowej oraz ochrony danych osobowych[8]. Ponadto w dokumencie znalazły się rozważania odpowiadające na pytanie, dlaczego radca prawny musi zapewnić bezpieczeństwo poczty elek-

[8] G. Sibiga, I. Małobęcka-Szwast, D. Nowak, K. Syska, *Rekomendacje dla radców prawnych: Bezpieczeństwo poczty elektronicznej w praktyce wykonywania zawodu radcy prawnego w kontekście obowiązku zachowania tajemnicy zawodowej oraz ochrony danych osobowych* [w:] Krajowa Izba Radców Prawnych, *Księga bezpieczeństwa…*, s. 62 i n.

tronicznej. Uzasadnieniem dla rekomendacji jest również zawarta w *Księdze bezpieczeństwa…* „Opinia prawna dotycząca bezpieczeństwa poczty elektronicznej w praktyce wykonywania zawodu radcy prawnego w kontekście obowiązku zachowania tajemnicy zawodowej oraz ochrony danych osobowych”[9].

Warto zapoznać się z całością rekomendacji, które zawierają wiele praktycznych wskazówek, a na potrzeby poradnika przytoczę kilka z nich:

1) nie jest rekomendowane przesyłanie wiadomości e-mail zawierających informacje poufne bez żadnych zabezpieczeń;
2) rozpoczynając współpracę z klientem, warto poinformować go o zagrożeniach związanych z korzystaniem z poczty elektronicznej;
3) należy „stosować odpowiednie zabezpieczenia informacji przekazywanych pocztą elektroniczną także w przypadku przekazywania przez radcę prawnego informacji prawnie chronionych do organów władzy publicznej (…) lub innych podmiotów (…) Odradza się zbędne wysyłanie pocztą elektroniczną korespondencji, która została lub ma być przekazana do organu w inny sposób (np. przez ePUAP, pocztą tradycyjną, osobiście)”;
4) do każdej wiadomości e-mail warto „załączać krótką informację, że treść wiadomości jest poufna i chroniona tajemnicą zawodową, oraz zastrzec, że jeżeli osoba nie jest właściwym adresatem wiadomości, to powinna ona poinformować o tym jej nadawcę (radcę prawnego) i trwale tę wiadomość usunąć”;
5) należy także oznaczać „jako poufne i chronione tajemnicą zawodową (np. w nazwie pliku, na pierwszej stronie dokumentu)” pliki będące załącznikami do korespondencji elektronicznej;
6) zawierając umowę z dostawcą poczty elektronicznej, należy zadbać o to, żeby spełniał on wymogi RODO, oraz zawrzeć

[9] G. Sibiga, I. Małobęcka-Szwast, D. Nowak, K. Syska, *Opinia prawna dotycząca bezpieczeństwa poczty elektronicznej w praktyce wykonywania zawodu radcy prawnego w kontekście obowiązku zachowania tajemnicy zawodowej oraz ochrony danych osobowych* [w:] Krajowa Izba Radców Prawnych, *Księga bezpieczeństwa…*, s. 73 i n.

z nim umowę powierzenia zgodną z RODO; zalecane jest przy tym „ostrożne korzystanie z «darmowych» skrzynek poczty elektronicznej, w tym dokładne sprawdzenie warunków świadczenia usług pod kątem zgodności z przepisami prawa i zasadami bezpieczeństwa informacji"; „przy wyborze dostawcy poczty elektronicznej należy również zwrócić uwagę, czy dane osobowe będą przetwarzane na terenie Europejskiego Obszaru Gospodarczego, czy też poza nim, ze względu na ograniczenia dotyczące transferu danych poza EOG wynikające z RODO. Jeżeli zgodnie z umową dostawca poczty elektronicznej mógłby przechowywać zawartość skrzynki pocztowej radcy prawnego poza EOG, to należy sprawdzić, czy w danym państwie zapewniony jest odpowiedni poziom ochrony lub zapewniono odpowiednie zabezpieczenia w rozumieniu art. 45–47 RODO";

7) zaleca się „każdorazowo weryfikować adres e-mail nadawcy, w tym sprawdzić, czy nadawca jest znany lub czy adres e-mail nadawcy zgadza się z dotychczas stosowanym adresem";
8) „należy zwracać uwagę na treść wiadomości, zwłaszcza jeżeli otrzymana wiadomość pochodzi od nieznanego nadawcy";
9) „należy zachować szczególną ostrożność klikając w linki lub otwierając załączniki zamieszczone w wiadomości";
10) szczególną uwagę należy poświęcić hasłom do poczty elektronicznej (ochrona, regularna zmiana, stopień komplikacji hasła, różnicowanie używanych haseł, korzystanie z dwuetapowego sposobu uwierzytelniania);
11) zalecane jest przestrzeganie zasady, że skrzynka i adres służbowy służą wyłącznie celom służbowym;
12) „należy pamiętać o bieżących aktualizacjach systemu operacyjnego oraz oprogramowania antywirusowego, które powinno również służyć do ochrony poczty elektronicznej";
13) „należy także stosować środki w celu przeciwdziałania innym zagrożeniom bezpieczeństwa informatycznego, chociażby związane z bezpieczeństwem fizycznym sprzętu informatycznego lub bezpieczeństwem sieci".

3.6. Analiza porównawcza ogólnej zgodności chmurowych systemów najbardziej popularnych dostawców (Microsoft Exchange i Google G Suite)

W podsumowaniu analizy porównawczej chmurowych systemów najbardziej popularnych dostawców (Microsoft Exchange i Google G Suite)[10] stwierdzono, że korzystanie z usług zarówno Microsoft, jak i Google, tj. podmiotów objętych analizą, jest dopuszczalne zgodnie z RODO, przy czym „ostateczny wybór rozwiązania powinien być poprzedzony pogłębioną analizą technologiczną/bezpieczeństwa". Ponadto z wybranych narzędzi chmurowych należy korzystać „w sposób świadomy – zarówno przez użytkowników, organizatorów, jak również przez administratorów narzędzi po stronie organizacji".

3.7. Informacja dotycząca szyfrowania poczty elektronicznej przez wybranych dostawców

W informacji dotyczącej szyfrowania poczty elektronicznej oferowanej przez Google (G Suite Gmail – wersja płatna[11]), Microsoft (Microsoft 365, Exchange Online) i Apple (iCloud) przedstawiono między innymi następujące wnioski i rekomendacje[12]:

1) korzystanie z Gmaila (w ramach pakietu G Suite) i usługi Exchange Online spełnia wymogi bezpieczeństwa, które powinny obowiązywać radców prawnych[13];

---

[10] M. Wielisiej, *Analiza porównawcza ogólnej zgodności chmurowych systemów najbardziej popularnych dostawców (Microsoft Exchange i Google G Suite)* [w:] Krajowa Izba Radców Prawnych, *Księga bezpieczeństwa…*, s. 107.

[11] Według autorów wersja bezpłatna nie jest odpowiednia do stosowania przez radców prawnych – zob. D. Nartowski, K. Wątrobiński, *Informacja dotycząca szyfrowania poczty elektronicznej przez wybranych dostawców* [w:] Krajowa Izba Radców Prawnych, *Księga bezpieczeństwa…*, s. 115.

[12] D. Nartowski, K. Wątrobiński, *Informacja dotycząca szyfrowania poczty elektronicznej przez wybranych dostawców* [w:] Krajowa Izba Radców Prawnych, *Księga bezpieczeństwa…*, s. 124 i n.

[13] W odniesieniu do usługi iCloud Mail autorzy wstrzymali się z wydaniem opinii – zob. D. Nartowski, K. Wątrobiński, *Informacja dotycząca szyfrowania poczty elektronicznej przez wybranych dostawców* [w:] Krajowa Izba Radców Prawnych, *Księga bezpieczeństwa…*, s. 124.

2) wszyscy trzej dostawcy jako podmioty globalne zapewniają poziom bezpieczeństwa, „który w praktyce trudno osiągnąć samodzielnie w kancelarii prawnej bez ponoszenia bardzo dużych kosztów";
3) radca prawny powinien poinformować klienta o potencjalnych zagrożeniach związanych z korzystaniem z używanego przez siebie środka komunikacji, „w szczególności w przypadku braku szyfrowania";
4) co prawda standardem powinno być korzystanie z poczty szyfrowanej, ale korzystanie z nieszyfrowanych emaili nie powoduje „powstania większego ryzyka przechwycenia lub ujawnienia niż inne nieelektroniczne formy komunikacji oraz że korzystanie z nieszyfrowanych maili w rutynowych przypadkach pozostaje akceptowalną metodą komunikacji z klientami";
5) warto również stosować „najprostszą ochronę przesyłanych drogą elektroniczną dokumentów, czyli ochronę hasłem załączników", bo choć nie jest ona pozbawiona wad, to „w przypadku, gdy emailem przesyłane są dokumenty zawierające szczególnie poufne informacje, ochrona hasłem powinna być standardem".

3.8. Ocena zgodności Exchange Online, Gmail, iCloud Mail dla celów działalności radców prawnych

W podsumowaniu oceny zgodności Exchange Online, Gmail, iCloud Mail dla celów działalności radców prawnych autorzy przedstawili w szczególności następujące wnioski[14]:

1) „radcowie prawni mogą wykorzystywać dla celów wykonywania zawodu usługi Exchange Online w ramach pakietu Microsoft 365, a także Gmail w ramach pakietu G-Suite, natomiast wątpliwe byłoby wykorzystywanie usługi iCloud Mail";

[14] M. Gawroński, M. Ćwiakowski, K. Koc, P. Szurmak, *Ocena zgodności Exchange Online, Gmail, iCloud Mail dla celów działalności radców prawnych* [w:] Krajowa Izba Radców Prawnych, *Księga bezpieczeństwa komunikacji elektronicznej w pracy radcy prawnego*, cz. 2, *Poczta elektroniczna i chmura w pracy radcy prawnego*, s. 6 i n., https://kirp.pl/wp-content/uploads/2020/10/ksiega-bezpieczenstwa-2.pdf (dostęp: 23.10.2020 r.).

W publikacji szczegółowo omówiono obowiązki jednostek samorządu terytorialnego wynikające z ustawy o krajowym systemie cyberbezpieczeństwa oraz wymogi, jakie stawiają regulacje Krajowych Ram Interoperacyjności.

Ponadto uwzględniono kwestie ochrony danych osobowych, jako istotnego elementu ochrony informacji, oraz regulacje związane z bezpiecznym korzystaniem z usług chmurowych. Zwrócono szczególną uwagę na rolę prawnika w procesie budowy cyberbezpieczeństwa jednostki samorządu terytorialnego i zasady, którymi powinien on kierować się w pracy, korzystając z narzędzi teleinformatycznych.

Książka przybliża startegie ataku i obrony w cyberprzestrzeni oraz procedury postępowania w przypadku wystąpienia incydentu.

Poradnik przeznaczony jest dla pracowników administracji rządowej i samorządowej sprawujących nadzór nad wprowadzaniem i koordynowaniem polityki bezpieczeństwa w urzędzie. Zainteresuje również prawników zajmujących się zagadnieniami bezpieczeństwa cyfrowego.

Wojciech Dziomdziora – radca prawny; główny prawnik w Grupie Nexera; specjalista prawa telekomunikacyjnego, prawa nowych technologii, prawa mediów i prawa autorskiego; członek Komisji Prawa Autorskiego przy Ministrze Kultury i Komisji LegalTech przy Okręgowej Izbie Radców Prawnych w Warszawie; współzałożyciel Stowarzyszenia Prawa Nowych Technologii; współautor komentarza do ustawy o radiofonii i telewizji oraz autor wielu artykułów prawniczych.

9788382234138 W01P01

ISBN 978-83-8223-413-8

9 788382 234138