GIODO

Generalny Inspektor
Ochrony Danych Osobowych

Opinia w sprawie bezpieczeństwa danych przekazywanych przy użyciu poczty elektronicznej.

20-LECIE PRAWA DO OCHRONY DANYCH OSOBOWYCH W POLSCE

Jak zapewnić bezpieczeństwo informacji przekazywanej przy użyciu poczty elektronicznej, to kwestia, która wciąż budzi liczne wątpliwości, zwłaszcza wówczas, gdy przekazywane informacje podlegają ochronie prawnej lub z innych względów powinny być właściwie zabezpieczone, by zapewnić ich poufność, integralność i autentyczność. Mając na uwadze fakt, że wiele narzędzi programowych wykorzystywanych do wysyłania i odbierania poczty elektronicznej nie gwarantuje zapewnienia tych wskazanych wyżej podstawowych atrybutów bezpieczeństwa, nie ma wątpliwości, że ustalenie określonych zasad i środków w tym zakresie jest niezbędne.

1. Problem poufności

W przypadku poczty elektronicznej zapewnienie poufności uzyskać można poprzez szyfrowanie przekazywanych informacji lub odpowiednie zabezpieczenie infrastruktury, na którą składają się komputer nadawcy i odbiorcy, serwery pocztowe nadawcy i odbiorcy oraz kanały komunikacyjne do przesyłania informacji między nimi.

1. 1. Szyfrowanie przekazywanych informacji.

Szyfrowanie przekazywanych informacji jest jedną z najbardziej efektywnych metod zapewnienia poufności. Nie wymaga ona bowiem podejmowania żadnych dodatkowych działań związanych z zabezpieczaniem kanałów komunikacyjnych, serwerów pocztowych i innych serwerów pośredniczących w przekazywaniu informacji. W metodzie tej informacja przed wysłaniem zostaje zaszyfrowana i w takiej postaci trafia do odbiorcy. Przechwycenie jej podczas teletransmisji, jak również odczyt z serwerów pocztowych nadawcy i odbiorcy nie stwarza zagrożenia jej ujawnienia, gdyż jest ona zaszyfrowana. Metoda ta wymaga jednak dodatkowych działań organizacyjnych nadawcy i odbiorcy związanych z przekazaniem klucza do jej odszyfrowania.

Przykładem takiego prostego rozwiązania jest program kompresujący 7-Zip, dostępny nieodpłatnie w ramach licencji Open Source. Umożliwia on tworzenie samorozkodowujących się plików zawierających zaszyfrowane informacje. Odbiorca takiego pliku, aby zaszyfrowane w nim informacje odczytać, nie musi instalować na swoim komputerze programu 7-Zip. Plik taki zostanie bowiem przez system operacyjny komputera uruchomiony bez użycia programu 7-Zip. Do odszyfrowania przekazanej w nim informacji niezbędne jest wprowadzenie klucza kryptograficznego (hasła), który został użyty podczas jego tworzenia. Zgodnie z dobrymi praktykami, klucz taki powinien zostać przesłany do odbiorcy innym, bezpiecznym kanałem komunikacji.

Konieczność wymiany klucza poprzez bezpieczny kanał komunikacji można wyeliminować, wykorzystując infrastrukturę klucza publicznego (PKI). Cały mechanizm opiera się na zasadzie pary kluczy, tj. klucza prywatnego oraz publicznego. Nadawca do szyfrowania danych wykorzystuje klucz publiczny odbiorcy, a odbiorca do deszyfrowania wiadomości wykorzystuje własny klucz prywatny. Klucz publiczny,

ul. Stawki 2, 00-193 Warszawa
tel. 22 531-04-40
fax 22 531-04-41
www.giodo.gov.pl

jak sama nazwa wskazuje, udostępniany jest wszystkim zainteresowanym, zaś klucz prywatny powinien być tajny i znany tylko jego właścicielowi.

Zaletą takiego rozwiązania jest to, że przesyłana informacja jest szyfrowana kluczem publicznym adresata i w związku z tym nie ma potrzeby przekazywania mu klucza użytego do zaszyfrowania, jak ma to miejsce w przypadku użycia np. wspomnianego już programu 7-Zip.

Popularnym rozwiązaniem wprowadzającym taki mechanizm jest system PGP (*Pretty Good Privacy*) bądź jego odpowiednik GPG (*GNU Privacy Guard*). Prawidłowo przeprowadzona operacja takiego szyfrowania uniemożliwia podejrzenie treści przekazywanej informacji. Pamiętać jednak należy, że PGP nie jest pozbawione wad, gdyż w celu zaszyfrowania/odszyfrowania wiadomości, wymaga zainstalowania odpowiedniego oprogramowania na komputerze zarówno nadawcy, jak i odbiorcy, co z różnych powodów nie zawsze może być możliwe.

Do potwierdzania autentyczności klucza publicznego stosuje się ich certyfikaty – dokumenty elektroniczne, które „wiążą" dane identyfikacyjne właściciela danego klucza publicznego z wydaną mu przez centrum certyfikacji parą kluczy. Certyfikaty mogą być generowane wewnętrznie przez podmioty, tj. własne centra certyfikacji, lub przez komercyjne urzędy certyfikacji, tzw. zaufaną trzecią stronę. W profesjonalnych kontaktach, jeśli nadawca i odbiorca wiadomości nie korzystają z usług tego samego centrum certyfikacji wewnętrznej, do zapewnienia poufności i autentyczności przesyłanych informacji należy wykorzystywać komercyjne certyfikaty potwierdzania tożsamości (certyfikaty ID) wydawane przez trzecią zaufaną stronę.

Podmioty publiczne zamiast zakupu komercyjnych certyfikatów ID dla swoich pracowników mogą samodzielnie stworzyć swoje wewnętrzne centrum certyfikacji i wydawać swoim pracownikom certyfikaty ID, które mogą być wykorzystywane do zabezpieczenia komunikacji wewnątrz urzędu, jak również z innymi urzędami, które utworzą swoje własne centrum certyfikacji i wygenerują certyfikaty ID dla swoich pracowników. Rozwiązanie takie przewiduje rekomendacja Komitetu Rady Ministrów ds. Cyfryzacji MAC/SEC/1/15, która zaleca powszechne wprowadzenie mechanizmu zapewnienia integralności i autentyczności korespondencji elektronicznej e-mail, wysyłanej z podmiotów publicznych za pomocą podpisywania jej przy użyciu niekwalifikowanych certyfikatów elektronicznych w standardzie X.509, wydawanych z wewnętrznego centrum CA (Certification Authority) wchodzącego w skład struktury drzewa PKI podmiotu publicznego. Zaleca się również integrację polityk certyfikacyjnych z państwowym drzewem zaufania.

Należy jednak pamiętać, że certyfikat (zarówno w przypadku narzędzia PGP, jak i certyfikatu wydawanego przez Urząd Certyfikacji) nie daje możliwości zaszyfrowania nagłówka wiadomości e-mail, co umożliwia podejrzenie informacji o tym, kto jest nadawcą i adresatem korespondencji. Dopiero zastosowanie protokołu szyfrującego na etapie komunikacji między serwerem pocztowym nadawcy a serwerem pocztowym odbiorcy pozwala ukryć całość korespondencji (patrz pkt. 1.2).

Metody te nie są tylko odpowiedzią na coraz częściej pojawiające się wątpliwości związane z przesyłaniem informacji przy wykorzystaniu sieci publicznej. Szyfrowanie stało się kluczowym

ul. Stawki 2, 00-193 Warszawa
tel. 22 531-04-40
fax 22 531-04-41
www.giodo.gov.pl

narzędziem do ochrony poufności komunikacji w sieciach łączności elektronicznej. Jak wskazuje Grupa Robocza Art. 29 w opinii 03/2016 z 19 czerwca 2016 r. w sprawie oceny i przeglądu Dyrektywy o prywatności i łączności elektronicznej, wykorzystanie szyfrowania wzrosło po medialnych doniesieniach związanych z działaniami, prowadzonymi na szeroką skalę przez podmioty publiczne i prywatne w celu przechwytywania nie kierowanej do nich korespondencji. Do tej samej opinii odniósł się również Europejski Inspektor Ochrony Danych w swojej opinii 5/2016 z 22 czerwca 2016 r., który zachęca do rozwijania standardów technicznych dotyczących szyfrowania, także w celu wspierania wymogów bezpieczeństwa wynikających z nowego rozporządzenia o ochronie danych.

1.2. Zapewnienie bezpieczeństwa infrastruktury i kanałów telekomunikacyjnych.

Dodatkową metodą zapewnienia poufności jest użycie serwerów pocztowych, które w komunikacji między komputerem nadawcy i odbiorcy oraz między sobą wykorzystują szyfrowane kanały komunikacyjne, co powoduje, że jeśli doszłoby do przechwycenia przesyłanej wiadomości, miałaby ona postać zaszyfrowaną. Rozwiązanie takie nie jest jednak łatwe do zastosowania, jeśli nadawca i odbiorca wiadomości korzystają z różnych serwerów pocztowych, co ma miejsce w większości przypadków komunikacji urzędu z obywatelem czy firmy z klientem. Wysyłający wiadomość musi w takim przypadku posiadać informacje dotyczące zarówno bezpieczeństwa przekazywania informacji między serwerami pocztowymi nadawcy i odbiorcy, jak i między urządzeniami nadawcy i odbiorcy z ich serwerami pocztowymi. Praktycznie rozwiązanie takie może zatem mieć zastosowanie jedynie w przypadku, jeśli nadawca i odbiorca wiadomości wykorzystują do komunikacji między sobą ten sam serwer pocztowy, co z powodzeniem może być wykorzystywane do przekazywania informacji w obrębie danej organizacji.

Wspomniana problematyka znajduje odzwierciedlenie w statystykach, jakie regularnie publikuje firma Google, wskazując na skalę wspierania szyfrowania przez operatorów między serwerem pocztowym nadawcy a serwerem pocztowym odbiorcy. Niezbędnym warunkiem zastosowania szyfrowania jest wspieranie go przez oba serwery. Według danych na 2 lutego 2017 r., 87% wiadomości przesyłanych z Gmaila do innych dostawców jest szyfrowanych, natomiast spośród wiadomości przychodzących szyfrowanych jest ok 80%. Powyższe statystyki wskazują na tendencję wzrostową stosowania szyfrowania kanałów komunikacji. Jeszcze dwa lata temu liczba e-maili wysyłanych do użytkowników Gmaila szyfrowanym kanałem wynosiła bowiem ok 56%. Należy jednak pamiętać, że zastosowanie tego rozwiązania nie eliminuje ryzyka odczytania przekazywanej informacji, lecz jedynie je ogranicza.

2. Problem bezpiecznego przechowywania danych na serwerze pocztowym

Nie bez znaczenia w metodzie, o której mowa w punkcie 1.2, ma zapewnienie bezpieczeństwa przesyłanych informacji, w czasie, kiedy są one składowane i przechowywane na serwerach pocztowych zarówno nadawcy, jak i odbiorcy. W metodzie tej przesyłane informacje nie są szyfrowane przed wysłaniem i w takiej samej postaci, tj. w postaci jawnej, są przechowywane w skrzynkach pocztowych serwerów zarówno nadawcy, jak i odbiorcy wiadomości. Za bezpieczeństwo danych przechowywanych na serwerach

ul. Stawki 2, 00-193 Warszawa
tel. 22 531-04-40
fax 22 531-04-41
www.giodo.gov.pl

pocztowych odpowiedzialni są ich administratorzy. Jeśli instytucja wykorzystuje własny serwer pocztowy, wówczas jego bezpieczeństwem może odpowiednio zarządzać i w przypadku korespondencji wewnętrznej (jeśli skrzynka pocztowa nadawcy i odbiorcy zlokalizowana jest na tym samym serwerze) zapewnić jej pełne bezpieczeństwo. W przypadku jednak, gdy instytucja nie posiada własnego serwera lub skrzynka pocztowa adresata wiadomości zlokalizowana jest na zewnętrznym serwerze pocztowym, bezpieczeństwo przechowywanej korespondencji zależne jest od poziomu bezpieczeństwa, jaki zapewnią ich administratorzy. Poziom ten może być niewystarczający, a podmiot korzystający z usług takiego dostawcy może mieć ograniczone możliwości egzekucji odpowiedzialności za nieuprawnione ujawnienie danych, zwłaszcza w przypadku, jeśli nie podlegają oni jurysdykcji prawa polskiego.

W odniesieniu do podmiotów realizujących zadania publiczne konieczność zapewnienia środków uniemożliwiających nieautoryzowany dostęp do przekazywanych informacji wynika z § 20 pkt 1 Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (dalej KRI). Zgodnie z treścią tego przepisu, podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

Z obowiązku zapewnienia ochrony przed nieautoryzowanym dostępem nie są zwolnione również podmioty prywatne, jeśli przetwarzają one informacje podlegające ochronie prawnej, w tym np. dane osobowe. W obliczu często spotykanych w mediach komunikatach, informujących o skanowaniu przez zewnętrznych dostawców poczty elektronicznej, treści przesyłanej korespondencji w celu dostosowania oferty marketingowej, należy mieć ograniczone zaufanie do takich usług i ze szczególną ostrożnością podchodzić do wykorzystywania poczty elektronicznej przy przetwarzaniu danych osobowych.

3. Weryfikacja tożsamości

Kolejnym istotnym problemem związanym z korespondencją elektroniczną jest weryfikacja tożsamości nadawcy. Należy zaznaczyć, że poczta elektroniczna w swym podstawowym standardzie nie była i nie jest narzędziem zapewniającym jakiekolwiek mechanizmy służące weryfikacji tożsamości. W związku z tym domyślnie nie ma ograniczeń technicznych co do możliwości modyfikacji adresu e-mail nadawcy w nagłówku wiadomości. Praktycznie każdy może podszyć się pod prywatną bądź publiczną instytucję, wysyłając korespondencję, w której zamiast faktycznego adresu nadawcy, pojawi się adres osoby lub podmiotu, pod który ów nadawca się podszywa.

W związku z zagrożeniem, jakie niesie taka infrastruktura poczty elektronicznej, stworzono mechanizmy umożliwiające w pewnym stopniu weryfikację adresu e-mail, takie jak SPF (Sender Policy Framework), DKIM (Domain Keys Identified Mail) czy DMARC (Domain-based Message Authentication, Reporting & Conformance). Rozwiązania te nie wiążą się jednak w żaden sposób z weryfikacją tożsamości

ul. Stawki 2, 00-193 Warszawa
tel. 22 531-04-40
fax 22 531-04-41
www.giodo.gov.pl

nadawcy. Ich celem jest jedynie ograniczenie możliwości wysyłania przez serwery pocztowe wiadomości z innych domen niż ta, do której należy dany serwer. Mechanizmy te mają uniemożliwić posługiwanie się adresem IP nie przypisanym do danej domeny. Mechanizm SPF sprawdza się w sytuacji, kiedy serwer pocztowy nadawcy określa, kto ma prawo wysyłać pocztę z jego domeny i jednocześnie serwer pocztowy odbiorcy sprawdza, czy łączący się z nim serwer jest do tego uprawniony. Podkreślić należy, że dla przeważającej liczby użytkowników weryfikacja nadawcy wiadomości ogranicza się do treści pola „Od" („From") widocznego w interfejsie programu pocztowego. Wiadomość e-mail zawiera jednak w swoim nagłówku, oprócz „From", również pole „Return-Path" (domyślnie nie widoczne w interfejsie programu pocztowego). Różnica polega na tym, że przytoczony mechanizm SPF do weryfikacji posługuje się adresem e-mail znajdującym się w tym dodatkowym polu.

Profesjonalnym rozwiązaniem zapewniającym wiarygodną identyfikację adresu e-mail nadawcy oraz skuteczną ochronę przed modyfikacją wiadomości jest stosowanie certyfikatu elektronicznego. Umożliwia ono również szyfrowanie nadawanej wiadomości, co zapewnia skuteczną ochronę jej poufności (patrz pkt 1.1). Zastosowanie tej technologii rekomendowane jest przez Komitet Rady Ministrów ds. Cyfryzacji podmiotom publicznym, realizującym zadania publiczne[1]. W rekomendacji tej oznaczonej jako „Rekomendacja MAC/SEC/1/15" do zapewnienia autentyczności i poufności korespondencji email zaleca się użycie niekwalifikowanych certyfikatów elektronicznych. Certyfikaty takie zgodnie z ww. zaleceniem powinny być wydawane w wewnętrznym centrum CA (Certification Authority) wchodzącego w skład struktury drzewa PKI (Public Key Infrastructure) podmiotu publicznego. W przypadku korzystania z usług zewnętrznych dostawców poczty elektronicznej, którzy nie wydają swoim klientom certyfikatów ID, o których mowa w ww. rekomendacji, alternatywnym rozwiązaniem może być zakup komercyjnych certyfikatów ID.

Niezależnie od wymienionych wyżej mechanizmów potwierdzających tożsamość nadawcy podmioty publiczne, realizując zadania publiczne, powinny wykazywać się profesjonalizmem oraz rzetelnością zarówno w korespondencji wewnętrznej, jak i w kontakcie z obywatelem. Za złą praktykę należy zatem uznać np. wykorzystywanie przez podmioty publiczne adresów o nazwach domeny odmiennych niż wskazywanych na oficjalnych stronach internetowych lub w BIP, bądź jednoznacznie wskazujących na komercyjny podmiot udostępniający bezpłatnie usługę poczty elektronicznej. W maju ubiegłego roku Gazeta Prawna[2] donosiła o inspektoratach nadzoru budowlanego korzystających z darmowych skrzynek e-mailowych w domenie gmail.com, onet.pl, wp.pl czy interia.pl. Korespondencja nadana z adresu innego niż oficjalny adres danej instytucji, może budzić poważne wątpliwości co do tożsamości nadawcy i jej autentyczności oraz obniża zaufanie obywatela do państwa. W związku z powyższym, w celu zwiększenia zaufania, niezbędnym jest wykorzystywanie adresów, które w miarę możliwości identyfikują nadawcę już po

[1] Komitet Rady Ministrów ds. Cyfryzacji; Rekomendacja MAC/SEC/1/15; Zalecenie nr 2, Kwiecień 2015 *krmc.mc.gov.pl/download/50/11997/**Rekomendacje**MAC.pdf*

[2] http://serwisy.gazetaprawna.pl/samorzad/artykuly/945837,urzednicy-inspektoraty-nadzoru-budowlanego-darmowe-skrzynki-mailowe.html

ul. Stawki 2, 00-193 Warszawa
tel. 22 531-04-40
fax 22 531-04-41
www.giodo.gov.pl

składni samego adresu. Oprócz zastosowania wspomnianego niekwalifikowanego certyfikatu elektronicznego, przykładowym rozwiązaniem może być użycie domeny gov.pl, których abonentami mogą być podmioty wskazane w regulaminie określającym warunki świadczenia przez NASK usług w zakresie rejestracji i utrzymywania nazw w domenie gov.pl.

4. Właściwy wybór usługodawcy

Mając na względzie wątpliwości związane z właściwym wyborem dostawcy usługi poczty elektronicznej należy zwrócić uwagę na stopień zabezpieczeń stosowanych przez podmiot ją oferujący. Wskazane w punkcie 1.2 takie rozwiązanie jak zastosowanie szyfrowanego kanału komunikacji jest jednym ze środków spełniających wymogi w zakresie bezpieczeństwa informacji wynikające z normy PN-ISO/IEC 27001. Środek ten (zestawienie szyfrowanego kanału komunikacji miedzy komputerem nadawcy poczty elektronicznej i serwerem pocztowym nadawcy) jest jednak skuteczny tylko wtedy, gdy takie same środki stosuje jej odbiorca i serwer pocztowy odbiorcy wiadomości. Część podmiotów świadczących usługi na rynku hostingowym, w celu poinformowania potencjalnych klientów o bezpieczeństwie swoich usług publikuje informacje o posiadanym certyfikacie ISO w zakresie zarządzania bezpieczeństwem informacji na swojej stronie internetowej, co może być brane pod uwagę przez potencjalnych klientów przy podejmowaniu decyzji o wyborze dostawcy usług poczty elektronicznej.

Należy również wskazać, że przedsiębiorca przesyłając dane osobowe za pośrednictwem poczty e-mail, powierza ich przetwarzanie dostawcy tej usługi. W ramach takiej usługi, jej dostawca, w przypadku, gdy treść przesyłanej wiadomości nie jest szyfrowana przez nadawcę, ma potencjalne możliwości zapoznania się z ich treścią, co w przypadku przesyłania danych osobowych, czy innych informacji prawnie chronionych wymaga zawarcia umowy z dostawcą usługi z klauzulą zachowania w tajemnicy przesyłanych danych na wypadek, gdyby dostawca usługi celowo lub przypadkowe wszedł w ich posiadanie. W związku z powyższym GIODO zaleca korzystanie z usług dostawców poczty elektronicznej, którzy zapewnią ww. warunki bezpieczeństwa i zachowanie w poufności treści przesyłanej korespondencji. Podmiot decydując się na wybór określonego dostawcy usługi powinien zwracać ponadto uwagę na możliwości dochodzenia swoich praw i zobowiązań dostawcy na wypadek niedotrzymania warunków umowy przed sądem. Z dużym prawdopodobieństwem można w związku z powyższym stwierdzić, że łatwiej będzie dla klienta usługi poczty elektronicznej dochodzić swoich praw wynikających z warunków umowy, jeśli dostawca usługi będzie miał siedzibę w kraju i podlegał jurysdykcji prawa polskiego niż w przypadku siedziby w jednym z krajów Europejskiego Obszaru Gospodarczego, czy w krajach trzecich. Przy czym w przypadku siedziby dostawcy usługi w krajach EOG dochodzenie i egzekwowanie tych praw może być znacznie łatwiejsze z uwagi na wspólne przepisy obowiązujące w tym zakresie w UE i krajach EOG niż w przypadku dostawców posiadających siedzibę na terenie państw trzecich.

Właściwe wybór dostawcy usług poczty elektronicznej zarówno pod względem bezpieczeństwa i deklaracji zachowania w poufności przesyłanych danych po stronie nadawcy poczty elektronicznej nie

ul. Stawki 2, 00-193 Warszawa
tel. 22 531-04-40
fax 22 531-04-41
www.giodo.gov.pl

zwalnia go z obowiązku upewnienia się, czy i w jakim zakresie odbiorca przesyłanej informacji zadbał o bezpieczeństwo i zachowanie w poufności przesyłanej informacji po swojej stronie. Problem ten nie wystąpi jeśli nadawca i odbiorca korzystać będą z usług tego samego dostawcy poczty elektronicznej i odpowiednio zadbają o zabezpieczenie swoich praw oraz warunków świadczenia usługi w umowach na ich świadczenie. Nie ulega wątpliwości, że korzystanie przez odbiorcę z poczty elektronicznej oferowanej przez mało rzetelnego usługodawcę nie spełniającego podstawowych standardów w zakresie bezpieczeństwa informacji, naraża obie strony na naruszenie ochrony przesyłanych danych, w tym możliwości ich ujawnienia osobom nieupoważnionym.

ul. Stawki 2, 00-193 Warszawa
tel. 22 531-04-40
fax 22 531-04-41
www.giodo.gov.pl