

[jaga](#)

Bezpieczeństwo poczty elektronicznej – wskazówki GODO

publikacja: 01.03.2017 aktualizacja: 28.02.2017, 11:00

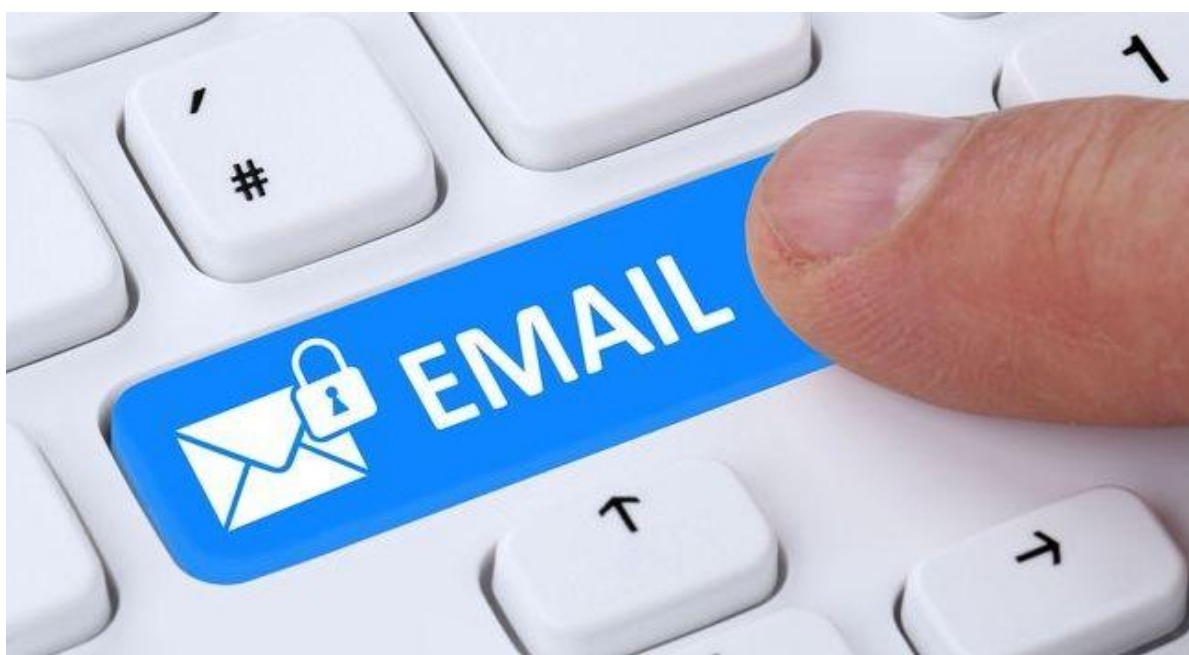


Foto: 123RF

Do otrzymywanych e-maili trzeba podchodzić z ograniczonym zaufaniem, a zwykłej, niezabezpieczonej poczty elektronicznej nie powinno się używać do przekazywania ważnych informacji, w tym prawnie chronionych, takich jak np. dane osobowe.

Generalny Inspektor Ochrony Danych Osobowych przygotował zestaw wskazówek pomocnych w zapewnieniu poufności, integralności i autentyczności informacji przesyłanych pocztą elektroniczną, która stała się popularnym narzędziem wymiany informacji zarówno w komunikacji prywatnej, jak i służbowej.

GIODO podkreśla, że zastosowanie właściwych zabezpieczeń wymaga uwzględnienia – jak wskazuje art. 36 ust. 1 ustawy o ochronie danych osobowych – zarówno kategorii przesyłanych danych, jak i możliwych zagrożeń, które wiążą się z przesyłaniem informacji. Te drugie to możliwość nieuprawnionego ujawnienia, zniszczenia lub modyfikacji. Ogólne unijne rozporządzenie o ochronie danych, które będzie stosowane od 25 maja 2018 r.,

wskazuje zaś na takie elementy wpływające na bezpieczeństwo danych, jak: charakter, zakres, kontekst i cele, jakim ma służyć przekazywana informacja oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia (art. 32 ust. 1 rozporządzenia UE 2016/679).

- W przypadku, gdy pocztę elektroniczną chcemy wykorzystać do przesyłania własnych danych – decyzja należy do nas. Bez większego ryzyka możemy ją także wykorzystać np. do poinformowania znajomych o naszej nieobecności na spotkaniu czy zmianie jego terminu. Pocztą bez obawy możemy przesłać link do interesującej nas publikacji, gdyż jest mało prawdopodobne, aby odczytanie jej przez nieuprawnioną osobę naraziło nadawcę lub odbiorcę na jakieś nieprzyjemności. Zwyklej, niezabezpieczonej poczty elektronicznej nie powinniśmy jednak już używać w celach służbowych do przekazywania informacji o czasie i miejscu spotkania, w którym uczestniczyć będą tak ważne osoby, jak np. ambasadorzy, premierzy czy prezydenci - wskazuje GİODO.

Z ograniczonym zaufaniem należy podchodzić do otrzymywanych e-maili. GİODO radzi zachować ostrożność choćby w takim przypadku, gdy np. zleceniobiorca usługi prześle zleceniodawcy informację, aby ustalone wynagrodzenie przelać mu na inny niż ustalono wcześniej numer konta bankowego.

- To może być bowiem sygnał świadczący o tym, że korespondencja jest podsłuchiwana i ktoś, podszywając się pod zleceniobiorcę, próbuje wyłudzić w ten sposób pieniądze - wyjaśnia GİODO.

Pocztą elektroniczną bez dodatkowych zabezpieczeń nie powinniśmy również przekazywać innych ważnych informacji, w tym informacji prawnie chronionych, takich jak np. dane osobowe.

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. Metoda ta wymaga jednak dodatkowych działań organizacyjnych nadawcy i odbiorcy związanych z przekazaniem klucza do jej odszyfrowania.

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, a tak jest w większości przypadków komunikacji urzędu z obywatelom 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 - pisze GİODO.

Przytacza statystyki, 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 proc. wiadomości przesyłanych z Gmaila do innych dostawców jest szyfrowanych, natomiast spośród wiadomości przychodzących szyfrowanych jest ok 80 proc.

- 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 proc. Należy jednak pamiętać, że zastosowanie tego rozwiązania nie eliminuje ryzyka odczytania przekazywanej informacji, lecz jedynie je ogranicza - zauważa GODO.

GODO przypomina, że za bezpieczeństwo danych przechowywanych na serwerach pocztowych odpowiedzialni są ich administratorzy. Jeśli instytucja czy przedsiębiorstwo 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 - podkreśla GODO.

Podmioty realizujące zadania publiczne mają obowiązek zapewnienia środków uniemożliwiających nieautoryzowany dostęp do przekazywanych informacji. Obowiązek ten wynika z § 20 pkt 1 rozporządzenia Rady Ministrów z 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.

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 - pisze GODO.

Kolejnym ważnym problemem związanym z korespondencją elektroniczną jest weryfikacja tożsamości nadawcy. GODO podkreśla, że poczta elektroniczna w swym podstawowym standardzie nie była i nie jest narzędziem zapewniającym jakiekolwiek mechanizmy służące weryfikacji tożsamości.

- 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 - wyjaśnia GİODO.

Dodaje, że wprawdzie istnieją 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 nadawcy. Ich celem jest jedynie ograniczenie możliwości wysyłania przez serwery pocztowe wiadomości z innych domen niż ta, do której należy dany serwer.

Profesjonalnym rozwiązaniem zapewniającym wiarygodną identyfikację adresu e-mail nadawcy oraz skuteczną ochronę przed modyfikacją wiadomości jest natomiast stosowanie certyfikatu elektronicznego. Zastosowanie tej technologii rekomendowane jest przez Komitet Rady Ministrów ds. Cyfryzacji podmiotom publicznym, realizującym zadania publiczne. W rekomendacji tej, oznaczonej jako „Rekomendacja MAC/SEC/1/15”, do zapewnienia autentyczności i poufności korespondencji e-mail zaleca się użycie niekwalifikowanych certyfikatów elektronicznych. Certyfikaty takie powinny być wydawane w wewnętrznym centrum CA (Certification Authority) wchodzącym 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 rekomendacji, alternatywnym rozwiązaniem może być zakup komercyjnych certyfikatów ID.

Niezależnie od mechanizmów potwierdzających tożsamość nadawcy, podmioty publiczne, realizując zadania publiczne (czyli np. organy administracji), powinny wykazywać się profesjonalizmem oraz rzetelnością zarówno w korespondencji wewnętrznej, jak i w kontakcie z obywatelem - zaznacza GİODO. Za złą praktykę uznaje np. wykorzystywanie przez podmioty publiczne adresów o nazwach domeny odmiennych niż wskazywana na oficjalnych stronach internetowych lub w BIP, bądź jednoznacznie wskazujących na komercyjny podmiot udostępniający bezpłatnie usługę poczty elektronicznej. Przykład? W maju 2016 roku „Dziennik Gazeta Prawna” donosił 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 celu zwiększenia zaufania niezbędne jest wykorzystywanie adresów, które w miarę możliwości identyfikują nadawcę już po składni samego adresu - wskazuje GİODO.

Oprócz zastosowania niekwalifikowanego certyfikatu elektronicznego, przykładowym rozwiązaniem zalecanym przez GİODO może być użycie domeny gov.pl, której abonentami mogą być organy władzy publicznej, z wyłączeniem wójtów, burmistrzów i prezydentów miast oraz stowarzyszeń gmin, ale także organy samorządu zawodowego, reprezentujące osoby wykonujące zawody zaufania publicznego.