Poczta elektroniczna jako środowisko przetwarzania danych i potencjalne źródło naruszeń

Posted on 2026-04-30

Wśród naruszeń ochrony danych osobowych zgłaszanych do Prezesa UODO znaczną część stanowią te związane z niewłaściwym zabezpieczeniem danych przetwarzanych za pośrednictwem poczty elektronicznej. Najczęściej są to incydenty wynikające z włamania na służbowe skrzynki oraz przesyłania niezabezpieczonych dokumentów, co bezpośrednio zagraża ich poufności i integralności.

W związku z tym kluczowe jest, aby organizacje regularnie dokonywały przeglądu procesów biznesowych opartych na komunikacji elektronicznej. Pozwoli to na identyfikację miejsc, w których dane mogą być narażone na nieautoryzowany dostęp lub przypadkowe ujawnienie. Analiza naruszeń ochrony danych osobowych wskazuje na niepokojący trend: wiele organizacji traktuje skrzynki poczty elektronicznej jako domyślne archiwum dokumentów oraz bezpieczne repozytorium do długotrwałego przetwarzania danych. Często brakuje przy tym refleksji nad fizyczną lokalizacją serwerów przechowujących te tysiące wiadomości, a także nad tym, czy standardowa obsługa codziennej korespondencji zapewnia poziom bezpieczeństwa adekwatny do wagi przesyłanych informacji.

Konieczność wprowadzenia i przestrzegania zasad retencji danych

Kluczowe jest, aby każda organizacja uwzględniła pocztę elektroniczną w swojej analizie ryzyka naruszenia praw lub wolności osób fizycznych. Wykorzystywanie poczty elektronicznej do przesyłania danych osobowych wiąże się ze specyficznymi zagrożeniami, które administrator musi zidentyfikować, aby skutecznie zminimalizować prawdopodobieństwo ich wystąpienia oraz ograniczyć ich potencjalne skutki. Dane przetwarzane za pośrednictwem poczty elektronicznej muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów ich przetwarzania. W związku z tym niezbędne jest określenie i wdrożenie polityki retencji danych, a następnie regularna weryfikacja jej przestrzegania. Brak polityki retencji lub jej nieprzestrzeganie prowadzi do przechowywania wiadomości bez podstawy prawnej, co narusza zasady określone w art. 5 RODO.

Poza aspektem prawnym istotny jest również wymiar biznesowy: przechowywanie zbędnej korespondencji generuje dodatkowe koszty operacyjne związane z utrzymaniem zasobów serwerowych, które nie przekładają się na żadną wartość dla organizacji.

Główne kategorie naruszeń ochrony danych osobowych dot. poczty elektronicznej

Analiza zgłoszeń naruszeń ochrony danych pozwala na wyodrębnienie dwóch kluczowych kategorii naruszeń ochrony danych osobowych związanych z wykorzystaniem poczty elektronicznej:

1. NIEUPRAWNIONY DOSTĘP DO SKRZYNEK POCZTOWYCH
2. TRANSMISJA DANYCH BEZ ODPOWIEDNICH ZABEZPIECZEŃ

Nieuprawniony dostęp do skrzynek pocztowych – przyczyny

Analiza naruszeń pozwala wskazać trzy główne źródła sytuacji, w których dochodzi do przejęcia kontroli nad służbową pocztą elektroniczną:

1. Phishing i brak świadomości zagrożeń

Wielu administratorów danych wciąż nie przywiązuje należytej wagi do budowania świadomości zagrożeń wśród pracowników. Braki te objawiają się szczególnie w obszarze ataków socjotechnicznych. W wielu organizacjach:

·Kwestie bezpieczeństwa są pomijane w procesach szkoleniowych.

·Nie przeprowadza się kontrolowanych symulacji ataków, które pozwoliłyby zweryfikować czujność personelu.

·Brakuje rozwiązań technicznych wspierających wykrywanie i blokowanie podejrzanych wiadomości.

2. Niewłaściwa higiena poświadczeń

Znaczna część naruszeń wynika z błędów w zarządzaniu hasłami. Do najczęstszych problemów należą:

·Powtarzalność haseł: używanie tych samych danych logowania w wielu różnych serwisach (prywatnych i służbowych).

·Niewłaściwe przechowywanie: Zapisywanie haseł na fizycznych nośnikach (np.

karteczkach) w pobliżu stanowiska pracy.

·Synchronizacja z kontami prywatnymi: wykorzystywanie wbudowanych w przeglądarki mechanizmów synchronizacji haseł z prywatnym kontem pracownika. W przypadku włamania na konto prywatne cyberprzestępcy automatycznie uzyskują dostęp do wszystkich poświadczeń służbowych zapamiętanych w przeglądarce.

·Brak poufności: przeprowadzanie procesu uwierzytelniania w sposób umożliwiający podejrzenie danych przez osoby postronne.

Złośliwe oprogramowanie typu „info stealer”

Infekcje tym typem malware’u wynikają zazwyczaj z nieświadomego uruchomienia przez użytkownika pliku podszywającego się pod bezpieczny dokument (np. instalator, aktualizacja lub faktura).

·Mechanizm działania: Po uruchomieniu złośliwy kod działa w tle, gromadząc dane z przeglądarek i systemów, a następnie przesyła je do atakującego.

·Manipulacja: Infekcje info-stealerami są zwykle poprzedzone socjotechniką — np. fałszywymi komunikatami o błędach lub stronami podszywającymi się pod legalne oprogramowanie. Kluczowym momentem jest interakcja użytkownika; system rzadko instaluje takie oprogramowanie samodzielnie bez otwarcia zainfekowanego pliku.

·Uprawnienia administratora: Ryzyko potęguje praca na kontach z pełnymi uprawnieniami administracyjnymi bez wyraźnej potrzeby biznesowej. W takim środowisku malware może głębiej infiltrować system, modyfikować ustawienia i skuteczniej omijać zabezpieczenia.

Dobre praktyki:

Mając świadomość zagrożeń, należy podejmować działania minimalizujące ryzyko ich materializacji. Kluczowym krokiem jest uwzględnienie tych scenariuszy w analizie ryzyka oraz wdrożenie poniższych środków kontrolnych:

1. Budowanie świadomości

Regularna edukacja to pierwsza linia obrony. Oto środki, które warto wdrożyć w tym zakresie.

·Cykliczne szkolenia: powinny bazować na aktualnych trendach (np. socjotechnika, vishing) i opisywać rzeczywiste przypadki naruszeń, z którymi pracownik może zetknąć się w codziennej pracy.

·Symulacje ataków: warto aktywnie weryfikować wiedzę poprzez kontrolowane kampanie phishingowe. Pozwala to zidentyfikować „słabe punkty” i dopasować program szkoleniowy do realnych potrzeb.

2. Uwierzytelnianie wieloskładnikowe (MFA)

Wdrożenie dodatkowego składnika uwierzytelniającego sprawia, że samo przejęcie loginu i hasła nie wystarczy do włamania.

·Zasada „coś wiesz i coś masz”: nawet jeśli hasło wycieknie, cyberprzestępca nie uzyska dostępu bez dodatkowego „sekretu” (np. kodu z aplikacji, klucza sprzętowego czy powiadomienia „push”).

·Prewencja zamiast reakcji: MFA powinno być standardem od samego początku, a nie funkcjonalnością włączaną dopiero po wykryciu incydentu.

3. Dostęp warunkowy

Ograniczenie powierzchni ataku poprzez restrykcje lokalizacyjne.

·Białe listy IP: tam, gdzie to możliwe, dostęp do systemów pocztowych i administracyjnych powinien być ograniczony do firmowych adresów IP.

·Ograniczenia geograficzne: jeśli organizacja nie prowadzi operacji w egzotycznych regionach świata (tj. poza EOG), warto zablokować możliwość logowania z tych lokalizacji. Większość przejętych kont jest wykorzystywana do masowej wysyłki spamu właśnie z serwerów zlokalizowanych w odległych państwach.

4. Ochrona przed atakami siłowymi (Brute Force)

Automatyczne mechanizmy blokujące próby siłowego odgadnięcia hasła. Warto rozważyć wdrożenie m.in. następujących rozwiązań:

·Limity prób logowania: System powinien automatycznie blokować konto (tymczasowo lub

do interwencji administratora) po określonej liczbie nieudanych prób logowania.

·Monitorowanie logów: Analiza nieudanych logowań pozwala na wczesne wykrycie trwającego ataku na infrastrukturę organizacji.

Transmisja danych bez odpowiednich zabezpieczeń

Właściwe zabezpieczenie dostępu do poczty elektronicznej nie zawsze wystarczy do tego, żeby uniknąć naruszenia ochrony danych osobowych. Duża liczba zgłoszeń wynika z faktu, że procesy biznesowe realizowane organizacji nie uwzględniają potrzeby zabezpieczania dokumentów i danych przesyłanych za pomocą poczty elektronicznej.

1. Przyczyny:

Niewłaściwe procesy biznesowe i błędy ludzkie są równie groźne jak ataki hakerskie. Poniżej przedstawiono główne przyczyny naruszeń ochrony danych osobowych związanych z obsługą poczty elektronicznej:

Przesyłanie dokumentów zawierających dane osobowe (np. skany dowodów, umowy, wnioski) w formie otwartych, niezabezpieczonych plików.

·Mechanizm działania: Poczta elektroniczna nie zapewnia domyślnie szyfrowania „end-to-end”, co oznacza, że treść wiadomości może być dostępna dla podmiotów pośredniczących oraz całkowicie niechroniona w przypadku błędnego adresata. Wiadomość bez zaszyfrowanego załącznika można porównać do karty pocztowej – jej treść jest widoczna

dla każdego, kto wejdzie w jej posiadanie. Podczas transmisji dane przechodzą przez liczne węzły i serwery pośredniczące, na których mogą zostać odczytane. Co kluczowe, brak szyfrowania powoduje, że plik nie posiada żadnej „warstwy ochronnej", która chroniłaby dane w przypadku pomyłki nadawcy.

·Skutek: Wysłanie wiadomości do błędnego adresata skutkuje natychmiastowym ujawnieniem danych, nad którymi administrator traci kontrolę w chwili naciśnięcia „Wyślij". Osoba nieuprawniona zyskuje pełny wgląd w treść dokumentów bez konieczności podejmowania jakichkolwiek działań technicznych. Brak hasła sprawia, że administrator traci jakąkolwiek kontrolę nad zakresem ujawnionych informacji już w sekundzie kliknięcia przycisku „Wyślij".

2. Nadmierne zaufanie do mechanizmu autouzupełniania adresów

Nadmierne zaufanie do mechanizmu autouzupełniania adresów może prowadzić do wysyłki danych do niewłaściwych osób.

·Mechanizm działania: Po wpisaniu pierwszych liter imienia lub nazwiska system sugeruje adresy z książki adresowej lub historii korespondencji. Chwila nieuwagi powoduje wybranie osoby o podobnych danych, ale z zupełnie innego kontekstu biznesowego.

·Manipulacja/Błąd: Pośpiech i rutyna sprawiają, że użytkownik nie weryfikuje pełnego adresu przed kliknięciem przycisku „Wyślij", co w połączeniu z brakiem szyfrowania plików prowadzi do utraty poufności.

3. Błędy edytorskie w adresach e-mail

Pomyłki powstające na etapie wprowadzania danych do systemów, szczególnie podczas przepisywania ich z formularzy papierowych lub rozmów telefonicznych.

·Mechanizm działania: Pojedyncza literówka (tzw. „czeski błąd”) lub błąd w domenie może spowodować, że wiadomość trafi do przypadkowego odbiorcy lub na serwer przeznaczony do przejmowania błędnie zaadresowanej poczty.

·Skutek: Dane trafiają do zupełnie obcej osoby, co stwarza ryzyko ich nieuprawnionego wykorzystania lub dalszego upublicznienia.

4. Wysyłka masowa bez użycia pola „UDW”

Ujawnienie list adresowych poprzez umieszczenie wielu odbiorców w widocznym polu „Do” lub „DW”.

·Mechanizm działania: Pracownik wysyła wiadomość do grupy osób (np. pacjentów), nie ukrywając ich tożsamości przed pozostałymi uczestnikami korespondencji.

·Skutek: Każdy z odbiorców dowiaduje się o tożsamości pozostałych osób z grupy. Sam fakt przynależności do określonej listy (np. grupy terapeutycznej) jest informacją „wrażliwą”, której ujawnienie stanowi naruszenie ochrony danych osobowych.

Dobre praktyki:

Wdrożenie odpowiednich nawyków oraz standardów technicznych pozwala niemal całkowicie wyeliminować ryzyko naruszenia ochrony danych, nawet w przypadku pomyłki adresata. Poniższe zasady stanowią fundament kultury bezpieczeństwa w organizacji, łącząc proste rytuały uważności z profesjonalnymi mechanizmami ochrony poufności przesyłanych informacji.

1. Szyfrowanie załączników jako fundament poufności

Szyfrowanie minimalizuje skutki ewentualnego naruszenia, ponieważ uniemożliwia osobom nieuprawnionym dostęp do treści.

·Szyfrowanie pełni funkcję warstwy ochronnej — zabezpiecza dane zarówno przed błędnym adresatem, jak i przed dostępem podmiotów pośredniczących.

·Standardy haseł: Zgodnie z międzynarodowymi normami (np. ISO/IEC 27002) hasła nie mogą zawierać informacji łatwych do powiązania z użytkownikiem. Ponadto numer PESEL nie spełnia kryteriów silnego hasła ze względu na niską entropię. Ma stałą długość (11 cyfr) i przewidywalną strukturę — pierwszych sześć cyfr to data urodzenia, a pozostałe są generowane według znanych reguł. To sprawia, że liczba możliwych kombinacji jest ograniczona i podatna na ataki siłowe.

·Zasada dwóch kanałów: Hasło do zaszyfrowanego pliku nigdy nie powinno być przesyłane w tej samej wiadomości co załącznik. Prawidłowa procedura zakłada przekazanie hasła innym

kanałem komunikacji (np. SMS, telefon, bezpieczny komunikator).

2. Weryfikacja przedwysyłkowa (Rytuały uważności)

Mechanizmy kontrolne mające na celu przełamanie rutyny i automatyzmów, które są najczęstszą przyczyną incydentów typu „błąd ludzki”.

·Reguła 3 sekund: Tuż przed kliknięciem przycisku „Wyślij” należy zatrzymać się i ponownie zweryfikować pole adresata. To kluczowy moment na sprawdzenie, czy mechanizm autouzupełniania nie zasugerował błędnej osoby o podobnym nazwisku.

·Test otwartego załącznika: Dobrym nawykiem jest otwarcie pliku na moment tuż przed jego dołączeniem do wiadomości. Pozwala to na ostateczne upewnienie się, że przesyłamy właściwy dokument z danymi osoby, do której faktycznie kierujemy wiadomość.

·Odpowiedzialność nadawcy: Należy przyjąć zasadę ograniczonego zaufania do algorytmów programu pocztowego. System jest jedynie narzędziem wspomagającym, a ostateczna odpowiedzialność za poufność przesyłanych danych spoczywa na pracowniku wysyłającym wiadomość.

3. Ochrona tożsamości zbiorowej (Zasada UDW)

Stosowanie pola UDW przy wysyłkach masowych jest konieczne, ponieważ ujawnienie listy odbiorców może naruszać zasadę poufności wynikającą z RODO.

·Poufność kontekstowa: Sam fakt figurowania adresu na określonej liście (np. „Grupa wsparcia X", „Dłużnicy Y") ujawnia wrażliwe informacje o sytuacji życiowej odbiorcy. Stosowanie pola UDW (Ukryta Do Wiadomości) chroni te informacje przed nieuprawnionym wglądem pozostałych uczestników korespondencji.

Podsumowanie

Skuteczna ochrona danych osobowych w komunikacji e-mail wymaga odejścia od traktowania poczty jako „bezpiecznego sejfu" na rzecz świadomego zarządzania dynamicznym kanałem przesyłu informacji. Klucz do minimalizacji ryzyka naruszeń leży w synergii trzech obszarów:

·Technologii: Powszechne wdrożenie uwierzytelniania wieloskładnikowego (MFA), szyfrowania załączników oraz mechanizmów ochrony przed atakami siłowymi.

·Procedur: Rygorystyczne przestrzeganie polityki retencji danych, stosowanie bezpiecznych standardów haseł oraz bezwzględne wykorzystywanie pola UDW w komunikacji zbiorowej.

·Świadomości: Wypracowanie u pracowników „rytuałów uważności" oraz regularne testowanie czujności personelu poprzez symulacje ataków.

Ostatecznie bezpieczeństwo organizacji nie zależy wyłącznie od systemów teleinformatycznych — jego kluczowym elementem jest odpowiedzialność i czujność

nadawcy w momencie wysyłania wiadomości.