DSI.0003.1.2021.MB

Opole, dnia 09 lutego 2021 roku

Tomasz Gabor
Radny Województwa Opolskiego

Szanowny Panie Radny,

Zachowanie poczty, które Pan zaobserwował wiąże się ze standardowym mechanizmem aplikacji do obsługi poczty znajdującej się na tablecie. Mechanizm ten, w celu oszczędzania danych mobilnych synchronizuje pocztę z określonego czasu definiowanego przez dostawcę aplikacji do obsługi poczty email na urządzeniu klienckim. Maksymalny czas synchronizacji jest całkowicie zależny od producenta aplikacji – firmy Google – oraz jest przez niego dowolnie modyfikowany. Typowe zakresy dat to :

- 1 dzień,
- 3 dni,
- 1 tydzień
- 2 tygodnie.

Niezależnie od powyższego, dostęp do pełnej zawartości skrzynki możliwy jest za pomocą przeglądarki. Na moment przygotowywania odpowiedzi na Pana interpelację, tj 26.01.2021r. jest to 430 elementów poczty zajmujących 38% pojemności skrzynki. W celu udzielenia instrukcji dostępowych i instrukcji użytkownika proszę o kontakt z Departamentem Społeczeństwa Informacyjnego i Informatyki UMWO. W odniesieniu do porównania z usługą GMAIL pragnę poinformować, że jest to mechanizm własny producenta – firmy Google i stosują się do niego osobne zasady synchronizacji.
Pragnę również uspokoić i zapewnić, że do Pańskiego konta nie miała dostępu osoba nieupoważniona. Odpowiadając na szczegółowe pytania:

1. Poczta e-mail utrzymywana na systemach informatycznych UMWO jest na bieżąco monitorowana. Dostęp do poczty przyznawany jest użytkownikowi przez serwer na podstawie indywidualnych poświadczeń. Poświadczenia te znał tylko jeden pracownik Departamentu Społeczeństwa Informacyjnego i Informatyki UMWO, który konfigurował tablety przed wydaniem Radnym. Odnosząc się do historii logowań to wszystkie udane logowania będą efektem użycia właściwych poświadczeń – de facto jedynym uprawnionym do używania poczty t….r@opolskie.pl jest Pan. System zabezpieczeń UMWO skonstruowany jest tak, że po podaniu 3 razy nieprawidłowego hasła, konto podlega blokadzie, której usunięcie wymaga ingerencji administratora w celu jej usunięcia. Na Pańskim koncie znacznik złego hasła nie został nigdy ustawiony, co jednoznacznie wskazuje na brak prób wejścia na konto metodą „brute force".
2. Hasła do kont Radnych przechowywane są w zaszyfrowanej postaci. Każda osoba korzystająca z systemu informatycznego posiada własne hasło, które nie jest znane nikomu innemu, nawet administratorowi. Każdy użytkownik ma odpowiedni poziom uprawnień. Zgodnie z zasadami Polityki Bezpieczeństwa w UMWO dane wrażliwe nie mogą być przesyłane za pomocą środków komunikacji elektronicznej bez wcześniejszego zabezpieczenia tych danych np. za pomocą szyfrowania. Charakter wiadomości na Pana koncie jest znany tylko Panu. Mimo tego, wszelka komunikacja pomiędzy serwerami UMWO, a urządzeniami odbywa się zabezpieczonym szyfrowanym kanałem, minimalizując ryzyko ujawnienia przesyłanych danych. Audyt bezpieczeństwa realizowany jest przynajmniej raz w roku.
3. Hasło do systemu pocztowego ustawione dla użytkownika jest niemożliwe do ujawnienia. Dotyczy to także administratora systemu poczty. W przypadku zapomnienia, bądź utraty hasła jedyną możliwością ponownego uzyskania dostępu jest ustanowienia nowego hasła zgodnego z przyjętą w UMWO Polityką Bezpieczeństwa. Natomiast hasło dostępowe do urządzeń, które Państwo użytkujecie znał tylko Pracownik Departamentu Społeczeństwa Informacyjnego i Informatyku UMWO, konfigurujący te urządzenia przed ich wydaniem. Hasło blokady urządzenia powinno być okresowo zmieniane i jak wspomniałem wyżej nie jest znane nikomu oprócz użytkownika. Ponadto informuję, że w trybie administracyjnym, administrator systemu poczty ma dostęp do każdego konta pocztowego w Urzędzie. Co do zasady stwierdzenie to jest prawdziwe dla każdego systemu poczty na świecie.
4. Urządzenia udostępnione Radnym wyposażone są w oprogramowanie zarządzające. Oprogramowanie to pozwala na uzyskanie danych o lokalizacji (wykorzystywane wyłącznie przy zgubieniu bądź kradzieży urządzenia), zdalnego wyczyszczenia urządzenia w przypadku kradzieży, włączenia alarmu w urządzeniu w celu jego lokalizacji, zdalnego zablokowania ekranu w przypadku podejrzenia, że ktoś może mieć nieautoryzowany dostęp do urządzenia. Funkcja ta jest podstawowym i standardowym zabezpieczeniem każdego urządzenia mobilnego typu smartfon lub tablet. Oprogramowanie umożliwia też zdalny podgląd urządzenia ale wymaga to każdorazowego zaakceptowania takiej czynności przez posiadacza urządzenia – jest to funkcja zdalnej pomocy.

   Oprogramowanie do zdalnego zarządzania nie posiada dostępu do kamery i mikrofonu w celu prowadzenia podglądu i nasłuchu. Nawiązując do ostatniej kwestii – każde

uruchomione oprogramowanie przez użytkownika może mieć dostęp do kamery i mikrofonu. Departament Informatyki i Społeczeństwa Informacyjnego nie może włączyć zdalnie takiego oprogramowania – zarówno zainstalowanego przez dział IT jak i użytkownika końcowego. Dotyczy to oprogramowania zainstalowanego obecnie jak i w przyszłości. Kwestia prywatności i bezpieczeństwa użytkowników zawsze była i jest priorytetem.

Z poważaniem

Wicemarszałek Województwa Opolskiego

Zbigniew Kubalańca

Sprawę prowadzi: Mariusz Bogucki