URZĄD MIASTA OTWOCKA

ul. Armii Krajowej 5, 05-400 Otwock
tel.: +48 (22) 779 20 01 (do 06); fax: +48 (22) 779 42 25
www.otwock.pl e-mail: umotwock@otwock.pl

Otwock, dnia 16.11.2021 roku

Szanowni Państwo,

mimo zabezpieczeń i procedur mających na celu ochronę danych osobowych, Urząd Miasta Otwocka padł ofiarą ataku hakerskiego. W ostatnim czasie do tego typu zdarzeń doszło w całej Polsce. Cyberprzestępcy dopuścili się podobnego ataku m.in. na Małopolski Urząd Marszałkowski, Starostwo Powiatowe w Oświęcimiu, Urząd Gminy Kościerzyna, a także firmy takie jak Media Markt czy CD Projekt.

W tego typu sytuacjach, zgodnie z przepisami prawa art. 34 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 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 zwanej RODO, Urząd Miasta Otwocka ma obowiązek poinformować o możliwości naruszenia ochrony Pani/Pana danych osobowych.

Włamanie na serwery Urzędu Miasta Otwocka i zaszyfrowanie baz danych przy wykorzystaniu oprogramowania typu ransomware, stwierdzono 18.10.2021 roku. W konsekwencji tego zdarzenia istnieje możliwość nieuprawnionego pozyskania danych przez osoby trzecie. Były to działania o charakterze przestępczym, które zostały niezwłocznie zgłoszone na policję, do Urzędu Ochrony Danych Osobowych oraz do Certu. Prokuratura prowadzi w tej sprawie śledztwo.

Atakujący mogli uzyskać nieuprawniony dostęp do niektórych spośród danych osobowych przetwarzanych przez Urząd Miasta Otwocka takich jak: imię, nazwisko, adres zamieszkania, numer PESEL, NIP, seria i numer dowodu osobistego lub paszportu, data i miejsce urodzenia, numer telefonu, wykonywany zawód, wysokość wynagrodzenia, wizerunek, stan cywilny, obywatelstwo, stan zdrowia, wykształcenie, karalność, adres e-mail, numer konta bankowego.

Podkreślamy jednak, że obecnie nie ma potwierdzenia co do wycieku wyżej wymienionych danych.

Dla zapewnienia najwyższego standardu bezpieczeństwa danych osobowych w Urzędzie Miasta Otwocka został powołany specjalny zespół, który podjął natychmiastowe czynności:

- Zabezpieczono dostęp do baz danych w systemie informatycznym.
- Zabezpieczono obszary informatyczne zawierające dowody przestępstwa.
- 18 października 2021 poinformowaliśmy publicznie o zdarzeniu za pośrednictwem strony www.otwock.pl.
- Zarządzono audyt bezpieczeństwa systemów informatycznych przez firmę zewnętrzną.
- Poinformowano osoby, których naruszenie ochrony danych dotyczy poprzez wysłanie niniejszego pisma.
- Zainicjowano proces odtworzenia systemów informatycznych z kopii zapasowych.

W zakresie środków związanych bezpośrednio z bezpieczeństwem informacji, w odpowiedzi na zdarzenie:

- Odcięty został dostęp do zainfekowanych systemów.
- Rozpoczęto analizę logów w podanym okresie, analizę komputerów, urządzeń informatycznych oraz przeprowadziliśmy wywiad z pracownikami urzędu w poszukiwaniu wszystkich metod uzyskania dostępów, jakie mogli uzyskać przestępcy.
- Urząd Miasta Otwocka podjął radykalną decyzję o re-instalacji wszystkich stacji roboczych w celu wyeliminowania i zabezpieczenia systemów informatycznych.
- Wzmocniono politykę haseł i wymuszono zmianę haseł personelu do wszystkich systemów (w tym także nieobjętych incydentem).
- Udzielono pracownikom dodatkowe instrukcje i ostrzeżenia dot. ochrony danych osobowych oraz cyberbezpieczeństwa.

Dysponując wskazanymi wyżej danymi, osoba nieuprawniona może podejmować działania związane z możliwością posługiwania się nimi tam, gdzie uwierzytelnienie wymaga podania imienia i nazwiska, numeru telefonu lub/oraz adresu e-mail czy też numeru PESEL lub numeru dowodu osobistego i tym samym osoba może:

- Podejmować próby uzyskania na Pani/Pana szkodę, pożyczek w instytucjach poza bankowych np. przez Internet lub telefonicznie, w przypadkach niewymagających okazywania dokumentu tożsamości.
- Podejmować próby uzyskania dostępu do systemów obsługujących udzielenie świadczeń medycznych i uzyskać wgląd do danych o Pani/Pana stanie zdrowia, w przypadkach,

gdy dostęp do systemów rejestracji pacjenta będzie oparty na potwierdzeniu swojej tożsamości z wykorzystaniem numeru PESEL.

- Pani/Pana dane osobowe mogą zostać wykorzystane przez osobę trzecią do próby wyłudzenia odszkodowania.
- Osoby trzecie mogą podjąć próbę zawarcia na Pani/Pana szkodę umów cywilnoprawnych.
- Pani/Pana dane mogą zostać wykorzystane do zakładania konta na stronach internetowych, forach, sklepach i innych serwisach tam, gdzie brak jest weryfikacji zwrotnej za pomocą wiadomości

  e-mail lub numeru telefonu (sms/mms).
- Pani/Pana dane osobowe mogą zostać wykorzystane np. do oddania głosu w głosowaniu nad środkami budżetu obywatelskiego, tym samym osoby trzecie mogą skorzystać z Pani/Pana praw obywatelskich.

Rekomendowane działania

Urząd Miasta Otwocka przygotował przydatną listę środków zaradczych, których podjęcie zwiększy bezpieczeństwo Pani/Pana danych:

- Założenie konta w systemie informacji kredytowej, w celu otrzymywania powiadomień o każdej próbie uzyskania pożyczki na Pani/Pana nazwisko, np. BIK https://www.bik.pl/klienci-indywidualni/alerty-bik lub https://chronpesel.pl.
- Zastrzeżenie dowodu osobistego lub innego dokumentu w banku, w którym Pani/Pan posiada konto, lub w innym, nawet jeśli Pani/Pan nie ma tam założonego konta – lista polskich banków przyjmujących takie zgłoszenia znajduje się na stronie: https://dokumentyzastrzezone.pl/lista-bankow-zastrzegajacych-dokumenty-od-wszystkich-osob/.
- Jeśli Pani/Pan jest obywatelem Polski – wyrobienie nowego dowodu osobistego poprzez kontakt z właściwym urzędem miasta, gminy lub dzielnicy. Aktualny dokument można unieważnić przez Internet wykorzystując Profil Zaufany, osobiście w urzędzie lub za pośrednictwem tradycyjnej poczty, jeśli Pani/Pan znajduje się za granicą. Więcej informacji znajduje się na tej stronie: https://www.gov.pl/web/gov/zglos-utrate-lub-uszkodzenie-swojego-dowodu-osobistego-uniewaznij-dowod.
- Jeśli Pani/Pan podejrzewa, że mogła/mógł stać się ofiarą przestępstwa, niezwłocznie proszę zgłosić się na policję. Jeśli przestępstwo zostało popełnione z wykorzystaniem Pani/Pana

danych osobowych, należy powiadomić podmioty używające tych danych, np. bank, pożyczkodawców lub sieć telekomunikacyjną. Należy zebrać oraz zachować dowody wszelkich formalnych czynności podjętych w związku z zajściem, aby móc je wykorzystać podczas ewentualnego procesu sądowego.

- Jeśli Pani/Pan używa numeru PESEL jako loginu na jakimkolwiek portalu lub koncie internetowym – należy zmienić login (o ile dany serwis dopuszcza taką zmianę).
- Należy zwracać szczególną uwagę na linki i wypatrywać nieprawidłowości.
- Jeśli Pani/Pan zaobserwuje jakiekolwiek nieprawidłowości, należy nie udostępniać żadnych danych osobowych tylko zgłosić ten fakt organom ścigania.
- Należy zachować szczególną ostrożność w przypadku, gdy:
    a) otrzymamy niespodziewane maile lub wiadomości tekstowe, w szczególności od nieznanych nadawców;
    b) odbierzemy połączenia wykonywane z nieznanych numerów, w szczególności gdy dotyczą one przekazywania danych „w celach weryfikacyjnych" – nawet jeśli rozmówca podaje Pani/Pana aktualne dane. Może być to próba wyłudzenia dodatkowych informacji, innych niż te wykradzione;
    c) udostępniamy lub wykorzystujemy swoje dane osobowe za pośrednictwem Internetu, w szczególności za pośrednictwem linków znajdujących się w mailach lub wiadomościach.

Inspektorem Ochrony Danych w Urzędzie Miasta Otwocka jest Pan Witold Ciara. W przypadku dodatkowych pytań prosimy o kontakt: rodo@otwock.pl.

Z poważaniem

Z up. Prezydenta Miasta Otwocka
Naczelnik Wydziału Informatyki
Łukasz Samorański