protego
www.protego-odo.pl

WYCIEK DANYCH

W związku z oficjalnym komunikatem firmy ALAB laboratoria sp. z o.o. świadczącej usługi z zakresu diagnostyki medycznej o incydencie **naruszenia bezpieczeństwa danych osobowych** przekazuję Państwu do wiadomości.

W dniu 19 listopada 2023 r. miała miejsce próba ataku na serwery spółki ALAB laboratoria. Wg komunikatu z dnia 27 listopada 2023 r. ustalono, że hakerzy wykradli dane medyczne osób, które korzystały z usług spółki. Wyciek określa się jako poważny, nie tylko dlatego, że wyniki badań medycznych opisują stan zdrowia poszczególnych pacjentów, ale także ze względu na to jak wiele danych osobowych znajduje się w udostępnionych plikach.

Są to: **imię i nazwisko, PESEL (a więc i data urodzenia), adres zamieszkania (choć nie zawsze pełny), rezultat badań (cytologia, krew, mocz, w różnym zakresie), numery identyfikacyjne pacjenta, informacje o zleceniodawcy lub lekarzu zlecającym, daty wykonania badań.**

Ujawnione na chwilę obecną dane dotyczą pacjentów z okolic Warszawy, Łodzi i Łomianek w okresie badań za lata 2017 – 2023, jednak hakerzy grożą, że ujawnią pełną wykradzioną bazę danych.

Spółka w swoim oficjalnym komunikacie informuje o możliwych negatywnych skutkach incydentu:

- uzyskanie przez osoby trzecie, kredytów w instytucjach poza bankowych, ponieważ wiele takich instytucji umożliwia uzyskanie pożyczki lub kredytu w łatwy i szybki sposób np. przez Internet lub telefonicznie bez konieczności okazywania dokumentu tożsamości;
- uzyskanie dostępu do korzystania ze świadczeń opieki zdrowotnej przysługujących osobom, których dane naruszono oraz ich danych o stanie zdrowia, ponieważ często dostęp do systemów rejestracji pacjenta można uzyskać telefonicznie potwierdzając swoją tożsamość za pomocą numeru PESEL;
- korzystanie z praw obywatelskich osób, których dane naruszono, np.: do głosowania nad środkami budżetu obywatelskiego co z kolei uniemożliwiałoby to osobom których dane w sposób nieuprawniony użyto skorzystanie z przysługującego im prawa;
- wyłudzenie ubezpieczenia lub środków z ubezpieczenia, co może spowodować dla osób, których dane dotyczą, negatywne konsekwencje w postaci problemów

związanych z próbą przypisania im odpowiedzialności za dokonanie takiego oszustwa;
- zarejestrowanie przedpłaconej karty telefonicznej (pre-paid), która może posłużyć do celów przestępczych.

Rekomendowane działania mogące zminimalizować szkodliwość takich konsekwencji:

- założenie konta w systemie informacji kredytowej i gospodarczej w celu monitorowania swojej aktywności kredytowej, rozporządzenie RODO daje możliwość, uzyskania darmowego dostępu do zebranych na swój temat danych w formie „kopii danych“, którą mamy prawo uzyskać od BIK;
- zachowanie szczególnej ostrożności przy podawaniu danych osobowych innym osobom, zwłaszcza za pośrednictwem Internetu czy telefonu;
- zgłoszenia faktu naruszenia danych właściwym organom w celu zapobieżenia tzw. „kradzieży tożsamości“.

Zastrzeżenie numeru PESEL w serwisie mobywatel.gov.pl poprzez:
1. zalogowanie się do systemu,
2. wejście do sekcji „Twoje dane”,
3. potem Rejestr Zastrzeżeń PESEL
4. i wybrać „Zastrzeż PESEL” lub „Cofnij zastrzeżenie”.

W związku z powyższym bardzo proszę przekazać pracownikom, współpracownikom i osobom zainteresowanym niniejszy komunikat.

Można też wywiesić dołączone rekomendacje na tablicy ogłoszeń.

Inspektor ochrony danych
Rafał Guzik

REKOMENDOWANE DZIAŁA NA SKUTEK WYCIEKU DANYCH OSOBOWYCH

IGNORUJ nieoczekiwane wiadomości, w szczególności namawiające do podjęcia dodatkowego działania, jak odesłanie wiadomości SMS lub zrobienie przelewu na niewielką kwotę.

ZACHOWAJ OSTROŻNOŚĆ przy odbieraniu połączeń telefonicznych lub wiadomości e-mail lub wiadomości SMS od nieznanej osoby, która np. będzie próbować podając ujawniony nr PESEL, podszyć się pod bank, ubezpieczyciela, czy inną instytucję lub osobę w celu namówienia do podania hasła do konta bankowego.

POINFORMUJ ZNAJOMYCH w mediach społecznościowych (Facebook, Instagram, Tweeter itp.) o możliwości wysyłania przez osobę nieuprawnioną zaproszeń, komunikatów i innych informacji.

NIE PODAWAJ nikomu swoich danych osobowych przez telefon.

NIE WYSYŁAJ swoich danych osobowych e-mailem.

ZASTRZEŻ SWÓJ PESEL na portalu www.bezpiecznypesel.pl

lub bezpłatnie na stronie **GOV.PL**

(https://www.gov.pl/web/gov/zastrzez-swoj-numer-pesel-lub-cofnij-zastrzezenie).