Wyciek danych pacjentów ALAB Laboratoria

W związku z wyciekiem danych pacjentów ALAB Laboratoria, CERT Polska wspólnie z Centralnym Ośrodkiem Informatyki zasilił stronę bezpiecznedane.gov.pl numerami PESEL upublicznionymi przez hakerów z grupy "RA World". Tu warto sprawdzić czy Państwa dane są bezpieczne.

ALAB Laboratoria to jedna z największych ogólnopolskich sieci laboratoriów medycznych. Firma padła ofiarą ataku hakerskiego skutkującego wyciekiem danych medycznych. Do sieci wyciekły wyniki badań medycznych z ostatnich kilku lat. W związku z wyciekiem danych spółka ALAB Laboratoria opublikowała komunikat, w którym potwierdza, że incydent "jest wynikiem działalności przestępczej mającej na celu wymuszenie na spółce okupu".

Link do komunikatu:
https://www.alablaboratoria.pl/19811-komunikat-incydent-naruszenia-bezpieczenstwa-danych-osobowych

W ramach przeprowadzonego ataku hakerskiego wykradzione zostały całe pakiety danych osobowych Polaków. Wśród nich znajdują się imiona, nazwiska, numery PESEL i adresy zamieszkania pacjentów wraz z przypisanymi do nich wynikami badań.

NASK poinformowała, że eksperci podkreślają, że **narażone na wyciek danych mogą być również osoby, które nie korzystały z usług firmy ALAB. „Analiza wykazała, że doszło również do kradzieży wyników badań wykonywanych na zlecenie innych placówek medycznych, nienależących do grupy ALAB".**

Jeśli chcesz sprawdzić czy Twoje dane nie zostały upublicznione możesz to zrobić za pośrednictwem serwisu bezpiecznedane.gov.pl.

Wystarczy:

- wejść na stronę bezpiecznedane.gov.pl;
- zalogować się za pomocą m.in. aplikacji mObywatel, Profilu Zaufanego, e-Dowodu;
  kliknąć przycisk "Sprawdź wyciek z ALAB".
- Eksperci Zespołu CERT Polska wspólnie z Centralnym Ośrodkiem Informatyki zasilił rządowy serwis bezpiecznedane.gov.pl numerami PESEL upublicznionymi w ramach tego ataku.

Należy zaznaczyć, że w serwisie sprawdzisz wyłącznie, czy Twoje dane znalazły się wśród tych dotychczas upublicznionych. Negatywna weryfikacja nie daje pewności, że Twoje dane również nie zostały wykradzione. Jeżeli atakujący upubliczni kolejną część wykradzionych danych, powyższa baza będzie aktualizowana. Dlatego, sprawdź swoje dane ponownie później.

Co można zrobić, jeśli Twoje znalazły się w bazie ujawnionej przez przestępców?
Możesz skorzystać z możliwości zastrzeżenia numeru PESEL-u. Obecnie można to zrobić na dwa sposoby – samodzielnie przez stronę internetową mobywatel.gov.pl lub w urzędzie gminy.

Jak zastrzec PESEL w mobywatel.gov.pl:

- Zaloguj się do serwisu mobywatel.gov.pl, następnie należy wejść do sekcji „Twoje dane", potem „Rejestr Zastrzeżeń PESEL" i wybrać „Zastrzeż PESEL" lub „Cofnij zastrzeżenie".

Wyłudzenie pożyczki
Aby ograniczyć skutki wycieku danych osobowych, dobrze jest skorzystać z możliwości monitorowania prób zawarcia

umowy pożyczki lub zaciągnięcia innych zobowiązań z wykorzystaniem wykradzionych danych. Usługę w postaci powiadomień o próbach wyłudzenia pożyczki lub kredytu, a także raportów dotyczących zadłużenia wynikającego z niespłaconych należności oferują Biuro Informacji Kredytowej i biura informacji gospodarczej.

Aktualnie działalność prowadzą następujące biura informacji kredytowej i gospodarczej::

- Biuro Informacji Kredytowej SA: https://www.bik.pl/;
- Biuro Informacji Gospodarczej InfoMonitor SA: https://www.big.pl/;
- Krajowy Rejestr Długów Biuro Informacji Gospodarczej SA: https://krd.pl/; Rejestr Dłużników ERIF;
- Biuro Informacji Gospodarczej SA: https://erif.pl/;
- KBIG – Krajowe Biuro Informacji Gospodarczej SA: https://kbig.pl/;
- Krajowa Informacja Długów Telekomunikacyjnych SA: https://kidt.pl/;
- Bisnode Międzynarodowe Biuro Informacji Gospodarczej SA: https://www.m-big.pl/.