Rządowe Centrum Bezpieczeństwa Warszawa, dnia 30.04.2021 r.

UZUPEŁNIENIE DO ZAWIADOMIENIA OSOBY KTÓREJ DANE DOTYCZĄ O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Charakter naruszenia ochrony danych osobowych

W związku z przetwarzaniem danych osobowych funkcjonariuszy i pracowników służb mundurowych związanych ze zbieraniem danych niezbędnych do przeprowadzenia szczepień przeciwko COVID-19, Rządowe Centrum Bezpieczeństwa jako podmiot przetwarzający zawiadamia, że mogło dojść do naruszenia poufności Pani/Pana danych osobowych.

Zawiadomienie kierowane jest do osób, które w dniach 12-20 kwietnia br. poprzez stronę internetową http://szczepieniakadry.rcb.gov.pl/ za pomocą formularza przekazali dane zawierające imię i nazwisko, nr PESEL, służbowy adres e-mail, numer telefonu, nazwę macierzystej jednostki organizacyjnej oraz jej adres.

Należy podkreślić, że każda utrata poufności danych osobowych niesie za sobą wzrost ryzyka kradzieży tożsamości oraz nieuprawnionego jej wykorzystania poprzez np. zaciągnięcie kredytu lub pożyczki.

Istotne jest, że zestaw danych, które były przedmiotem podejrzenia wycieku (nie zawierający danych dokumentu tożsamości), najprawdopodobniej będzie niewystarczający do podszycia się pod inną osobę i wzięcia pożyczki lub kredytu na jej dane. Jednak ryzyko istnieje i jest zdecydowanie wyższe niż przed zaistnieniem zdarzenia, z następujących powodów:

- wprawdzie większość instytucji finansowych weryfikuje tożsamość wykorzystując informacje z rejestrów publicznych, co pozwala na potwierdzenie wewnętrznej spójność zestawu danych, w szczególności imienia, nazwiska, numeru PESEL i numeru dowodu osobistego, **jednak niektóre instytucje finansowe nie przeprowadzają takiej weryfikacji, co umożliwia np. zaciągnięcie pożyczki na imię, nazwisko, odpowiadający im numer PESEL i niewłaściwy (nieistniejący w obrocie prawnym) numer dowodu. Istotne jest, iż numer dowodu osobistego można bez przeszkód wygenerować tak, aby jego struktura odpowiadała obowiązującym w tym zakresie wymaganiom**.
- **zakres ujawnionych danych jest na tyle szeroki, że pozwala dość precyzyjnie sprofilować daną osobę i nawiązać z nią kontakt**. Nie można też wykluczyć, że przestępcy już są w posiadaniu innych fragmentarycznych danych osób dotkniętych potencjalnym wyciekiem i mogą połączyć posiadane dane z danymi nowo pozyskanymi.

Opis środków proponowanych osobie w celu zminimalizowania ewentualnych negatywnych skutków

W celu ochrony przed kradzieżą tożsamości zasadne jest **utrzymywanie zwiększonego poziomu ostrożności i uwagi przez osoby, której dane mogły zostać ujawnione.** Rekomendowane są między innymi następujące działania:

1. **Zachowaj szczególną ostrożność w przypadku nieoczekiwanych kontaktów.** Istnieje możliwość, że przestępcy będą podejmować próby uzyskania brakujących danych osobowych, np. poprzez podszycie się pod pracownika obsługi kadrowej instytucji, w której pracujesz.

2. **Zachowaj szczególną ostrożność w przypadku wszelkich aktywności wymagających podawania danych osobowych** (nie tylko w Internecie). Nie należy podawać danych osobowych osobom trzecim, zwłaszcza nieznajomym kontaktującym się z nami przez Internet lub telefon.
3. **Sprawdź czy nie doszło do przejęcia konta mailowego – jeżeli możesz zmień hasło.** Wielu użytkowników sieci Internet posługuje się hasłami opartymi na imieniu, nazwisku lub dacie urodzenia,
4. **Rozważ wprowadzenie dwuskładnikowego uwierzytelnienia[1] na swoim koncie email oraz w serwisach społecznościowych.**
5. **Zachowaj szczególną czujność korzystając z mediów społecznościowych.** Może w nich dojść do przejęcia Twojego profilu.
   - weryfikuj otrzymywane wiadomości dotyczące próśb o pożyczki, numery kodów i hasła;
   - niezwłocznie zmień hasło w mediach społecznościowych.
6. **Nie odpowiadaj na wiadomości email i smsy wysyłane przez spamerów.** Zachowaj najwyższą ostrożność zwłaszcza, gdy takie wiadomości dotyczą płatności.
7. W sytuacji nękania telefonami z zagranicy **zachowaj czujność, nie odbieraj takich połączeń.**
8. **Skorzystaj z bezpłatnego zastrzeżenia swojego nr PESEL.** Możesz to zrobić przy użyciu formularza na https://www.bezpiecznypesel.pl/pesel/. Partnerzy Systemu Bezpieczny Pesel (firmy pożyczkowe z sektora pozabankowego) zostaną poinformowani, że Twój numer PESEL jest zastrzeżony. Zastrzeżenie możesz bezpłatne cofnąć w każdej chwili. **Ponadto, zastrzeż swoje dane na obywatel.gov.pl oraz chronPESEL.pl.**
9. **Sprawdź czy na Twoje dane nie założono rachunków bankowych.** Można to zrobić w centralnym rejestrze rachunków bankowych na .
10. **Rozważ skorzystanie z usług Krajowego Rejestru Długów – załóż konto w Serwisie Ochrony Konsumenta** (www.konsument.krd.pl). Z usług KRD korzystają banki, operatorzy telekomunikacyjni, czy dostarczyciele telewizji. Przed udzieleniem kredytu lub sprzedaży usługi z odroczoną płatnością, sprawdzają naszą rzetelność finansową w biurze informacji gospodarczej KRD. Każde takie sprawdzenie zostawia ślad w systemie do którego masz wgląd.
11. **Rozważ skorzystanie z Alertów BIK.** Alerty informują o próbach zaciągania zobowiązań na dane konkretnej osoby, a także próbach zawarcia umów z operatorami sieci komórkowych czy dostawcami mediów. Ostrzeżenia przychodzą w formie SMS i e-mail.
12. **Możesz sprawdzić historię kredytową w BIK.** Jeśli uruchomiłeś Alerty, możesz sprawdzić całą swoją historię kredytową w BIK. W ten sposób potwierdzisz, że na Twój PESEL nie zostało wcześniej zaciągnięte jakieś zobowiązanie. Istotne jest, że Biuro Informacji Kredytowej współpracuje z całym sektorem bankowym i większością firm pożyczkowych. Dane można sprawdzić rejestrując się na www.bik.pl i pobierając raport.
13. **Zachowaj szczególną ostrożność w sytuacji usiłowania wyłudzenia pieniędzy „metodą na blika”.** Metoda ta polega na wyłudzeniu kodu do płatności przez telefon. Osoba logując się do swojego banku musi wygenerować w aplikacji kod do płatności telefonem, a następnie przesłać go „znajomemu”. Niestety w przeciwieństwie do płatności przelewem, transakcji dokonanych za pomocą tego kodu nie można już cofnąć, gdyż przestępca od razu wpisuje podany kod BLIK w bankomacie i wypłaca z niego pieniądze.
14. **Jeśli otrzymasz prośbę o pożyczkę, nie działaj pochopnie.** Sprawdź czy osoba, która do Ciebie napisała lub której prośba dotyczy rzeczywiście potrzebuje naszej pomocy
15. **Możesz skorzystać również z innych alertów w serwisach informacji gospodarczej**. Ustawienie alertów w kilku serwisach informacji gospodarczej zwiększa

[1] Uwierzytelnianie dwuskładnikowe (ang. Two Factor Authenticaton, 2FA) może pomóc chronić Twoje konta w sieci Internet. Zapewnia „podwójne sprawdzanie” (czy jesteś osobą, za którą się podajesz) przy korzystaniu z usług online. Podczas konfigurowania 2FA usługa poprosi Cię o podanie „drugiego składnika”, do którego masz dostęp tylko Ty. Mogą nim być różne dane, np. kod wysyłany do Ciebie SMS-em lub utworzony przez aplikację zainstalowaną na Twoim urządzeniu mobilnym lub wygenerowana wcześniej lista kodów, którą przechowujesz w bezpiecznym miejscu..

prawdopodobieństwo powodzenia działań zapobiegawczych, ponieważ firmy pożyczkowe korzystają z różnych systemów weryfikacyjnych. Serwisy informacji gospodarczej:

- centralnainformacja.pl
- infoKonsument.pl

16. **Zastrzeż dowód osobisty.** W przypadku podejrzenia, że przestępcy na podstawie posiadanych danych podrobili Twój dowód osobisty, zastrzeż dokument w Systemie Dokumenty Zastrzeżone prowadzonym przez Związek Banków Polskich. W przypadku, gdy sprawdzenie w rejestrze dokumentów zastrzeżonych da wynik pozytywny, umowa na taki numer dowodu nie będzie mogła zostać zawarta. Lista banków zastrzegających dokumenty od wszystkich osób znajduje się pod adresem https://dokumentyzastrzezone.pl/lista-bankow-zastrzegajacych-dokumenty-od-wszystkich-osob/.

Niektóre wskazane usługi mogą być płatne zgodnie z cennikiem ich dostawcy.

Dane kontaktowe w celu uzyskania dodatkowych informacji

Jeżeli ma Pani/Pan jakiekolwiek pytania lub informacje dotyczące przekazanego komunikatu, Rządowe Centrum Bezpieczeństwa uruchomiło specjalne numery telefonów **22 3616932** oraz **22 3616850** obsługiwane przez n/wym. pracowników w dni robocze w godzinach 8:15 – 16:15:

1) Magdalena Kilis-Sokołowska;
2) Ewa Michałkiewicz;
3) Piotr Błaszczyk.

Dodatkowo do kontaktu utworzono adres email: naprawa_naruszenia@rcb.gov.pl

Zastępca Dyrektora
Rządowego Centrum Bezpieczeństwa

Grzegorz Matyasik

/podpisano kwalifikowanym podpisem elektronicznym/