

Komunikat WFOŚiGW w Poznaniu

Wojewódzki Fundusz Ochrony Środowiska i Gospodarki Wodnej w Poznaniu informuje, że w dniu 04 października 2024 r. stwierdzono wystąpienie incydentu bezpieczeństwa polegającego na ataku złośliwego oprogramowania szyfrującego pliki przechowywane na serwerach. Do zdarzenia doszło w wyniku ataku cyberprzestępców polegającego na przełamaniu zabezpieczeń.

Zdarzenie to doprowadziło do utraty dostępności oraz najprawdopodobniej również poufności danych osobowych m.in. beneficjentów, kontrahentów i pracowników WFOŚiGW w Poznaniu.

Jakie działania podjęto w związku ze zdarzeniem?

Niezwłocznie po wykryciu incydentu bezpieczeństwa podjęto niezbędne działania zapobiegające dalszym naruszeniom danych osobowych oraz zawiadomiono organy ścigania i instytucje właściwe w sprawach cyberbezpieczeństwa. Obecnie zdarzenie jest przedmiotem czynności wyjaśniających realizowanych przez Policję oraz CERT Polska (Computer Emergency Response Team Polska). Ponadto, zdarzenie zostało zgłoszone do Prezesa Urzędu Ochrony Danych Osobowych jako naruszenie ochrony danych związane z wysokim ryzykiem naruszenia praw i wolności osób fizycznych.

Wojewódzki Fundusz Ochrony Środowiska i Gospodarki Wodnej w Poznaniu dokłada wszelkich starań, aby zminimalizować skutki ataku oraz przywrócić pełną funkcjonalność systemów informatycznych w możliwie najkrótszym czasie.

Jakie dane osobowe obejmowało naruszenie?

Wskutek ataku doszło do naruszenia dostępności oraz poufności Państwa danych osobowych mogących obejmować w szczególności:

- dane identyfikacyjne;
- dane adresowe;
- dane kontaktowe;
- numer PESEL;
- seria i numer dowodu osobistego;
- numer rachunku bankowego;
- dane o zarobkach i/lub posiadanym majątku;
- informacja o wysokości przyznanych środków publicznych;
- dane szczególnej kategorii (o stanie zdrowia oraz o przynależności związkowej).

Z kim mogą się Państwo kontaktować w sprawie naruszenia ochrony danych osobowych?

W przypadku jakichkolwiek pytań związanych z naruszeniem mogą się Państwo skontaktować z WFOŚiGW w Poznaniu kierując zapytanie mailowe na adres: iod@wfosgw.poznan.pl.

Jakie mogą być potencjalne konsekwencje naruszenia ochrony danych osobowych?

Następstwem naruszenia Państwa danych osobowych może być:

- publikacja lub ujawnienie danych osobowych co może naruszać Państwa dobra osobiste;
- zagrożenie nękaniami lub szantażem przy wykorzystaniu ujawnionych danych;
- narażenie na wzmożone ataki phishingowe, zmierzające do wyłudzenia danych osobowych;
- założenie konta internetowego przy wykorzystaniu danych osobowych (np. w serwisach społecznościowych);
- podjęcie przez osobę trzecią próby uzyskania na Państwa szkodę pożyczek w instytucjach poza bankowych, np. przez internet lub telefonicznie, bez konieczności okazywania dokumentu tożsamości;
- podjęcie przez osobę trzecią próby uzyskania dostępu do systemów obsługujących udzielanie świadczeń medycznych i uzyskania wglądu do danych o Państwa stanie zdrowia (często dostęp do systemów rejestracji pacjenta można uzyskać, potwierdzając swoją tożsamość za pomocą numeru PESEL);
- wykorzystanie danych osobowych celem korzystania z praw obywatelskich np. poprzez oddanie głosu w

- głosowaniu nad środkami budżetu obywatelskiego;
- wykorzystanie przez osobę trzecią danych osobowych do próby wyłudzenia ubezpieczenia lub środków z ubezpieczenia;
- wykorzystanie przez osobę trzecią danych osobowych do próby zawarcia umów cywilno-prawnych;
- wykorzystanie danych osobowych przez osoby trzecie do ukrycia swojej tożsamości (np. przy otrzymywaniu mandatów);
- zarejestrowanie przedpłaconej karty telefonicznej (pre- paid), która może służyć do celów przestępczych;
- przetwarzanie danych osobowych w celach marketingowych bez uprzedniego uzyskania zgody (w przypadku prowadzenia marketingu drogą tradycyjną, tj. wysyłki treści marketingowych na adres zamieszkania).

Co mogą Państwo zrobić, aby zminimalizować negatywne skutki naruszenia:

W celu zminimalizowania ewentualnych negatywnych skutków zdarzenia zalecamy:

- zastrzec swój numer PESEL (zastrzeżenie numeru PESEL jest możliwe przez internet – kliknij przycisk Zastrzeż PESEL i zaloguj się, system przeniesie cię do mObywatel.gov.pl lub pobierz i wypełnij wniosek w domu albo zrób to w swoim urzędzie gminy) – od 1 czerwca 2024 r. instytucje finansowe (np. banki) mają obowiązek weryfikować, czy numer PESEL jest zastrzeżony przy zawieraniu np. umowy kredytu lub pożyczki;
- założyć konto w systemie informacji kredytowej i gospodarczej celem monitorowania swojej aktywności kredytowej (na rynku dostępne są systemy, instytucje i przedsiębiorstwa, które oferują usługi pozwalające na monitorowanie swojej aktywności kredytowej. Podajemy przykładowe: Biuro Informacji Kredytowej S.A. strona <https://www.bik.pl>, Biuro Informacji Gospodarczej InfoMonitor S.A. strona <https://big.pl>, Krajowy Rejestr Długów Biuro Informacji Gospodarczej S.A. stron <https://krd.pl>, Serwis CHRONPESEL strona <https://www.chronpesel.pl>);
- zmienić login lub hasło do systemów, w których loginem lub hasłem był numer PESEL;
- włączyć dodatkowe zabezpieczenie w serwisach, które umożliwiają weryfikację dwuetapową;
- zwracać szczególną uwagę na próby logowania na konta i sprawdzania alertów przesyłanych na adres e-mail;
- zachować ostrożność w kontakcie ze strony banków lub innych instytucji finansowych, w szczególności gdy rozmówca chce, powołując się na numer PESEL, uzyskać dane takie jak nr dowodu osobistego, nr konta bankowego, itp.;
- zachować ostrożność przy korzystaniu z mediów społecznościowych, w szczególności przy odbieraniu wiadomości prywatnych zawierających linki;
- w razie stwierdzenia podszywania się pod Państwa – zawiadomić organy ścigania o możliwości popełnienia przestępstwa;
- w razie stwierdzenia naruszenia Państwa dóbr osobistych przez wykorzystanie danych osobowych, które zostały objęte niniejszym naruszeniem, rekomendujemy wykorzystanie środków ochrony dóbr osobistych określonych w przepisach Kodeksu cywilnego.

Bezpieczeństwo Państwa danych we własnym zakresie można sprawdzić na:

<https://bezpiecznedane.gov.pl/>.

Podjęcie tych działań powinno zminimalizować negatywne skutki naruszenia i zabezpieczyć dane osobowe przed ich niewłaściwym wykorzystaniem.

Więcej informacji na stronie:

- wfosgw.poznan.pl/aktualnosci-z-funduszu/komunikat-w-sprawie-naruszenia-bezpieczenstwa-danych-osobowych
- wfosgw.poznan.pl/aktualnosci-z-funduszu/aktualizacja-komunikatu-w-sprawie-naruszenia-danych-osobowych
- wfosgw.poznan.pl/aktualnosci-z-funduszu/aktualizacja-komunikatu-w-sprawie-naruszenia-danych-osobowych-2