Warszawa, 2025-01-21

EuroCert Sp. z o.o.

Nip: 9512352379

ul. Puławska 472

02-884 Warszawa

Szanowni Państwo,

EuroCert Sp. z o.o. z siedzibą w Warszawie dopełniając swoich obowiązków jako administrator danych w rozumieniu art. 4 ust. 7 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) niniejszym informuje, że w dniu 12.01.2025r r. w godzinach nocnych został stwierdzony atak hakerski (ransomware), który doprowadził do naruszenia ochrony danych osobowych poprzez atak złośliwego oprogramowania szyfrującego pliki przechowywane na naszych serwerach z dużym prawdopodobieństwem ich kradzieży. Naruszenie mogło dotyczyć Pani/Pana danych osobowych.

Zdarzenie to doprowadziło do utraty dostępności oraz najprawdopodobniej również poufności danych osobowych m. in. klientów, kontrahentów i pracowników EuroCert Sp. z o.o.

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.

EuroCert Sp. z o.o. 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, które mogą obejmować:

- adres e-mail, numer telefonu podane podczas wydania certyfikatu;
- numer PESEL;
- imię, imiona i nazwisko;
- data i miejsce urodzenia;
- obywatelstwo;
- seria i numer dowodu osobistego oraz data ważności;
- nazwa użytkownika i/lub hasło;
- wizerunek (tylko w przypadku weryfikacji zdalnej).

Obecnie nie mamy pewności, że Państwa dane zostały wykradzione, ale zachodzi takie prawdopodobieństwo. Nadal trwa ustalanie skali incydentu, stąd dla ostrożności prosimy o uważne przeczytanie niniejszych zaleceń bezpieczeństwa oraz śledzenie komunikatów na stronie głównej www.eurocert.pl.

Czy doszło do naruszenia bezpieczeństwa certyfikatów kwalifikowanych?

Wykluczyliśmy ponad wszelką wątpliwość skompromitowanie wydanych Państwu certyfikatów. Nie zostały wykradzione. Nie ma potrzeby unieważniania certyfikatów.

- certyfikaty na fizycznych urządzeniach (kartach/tokenach) są w posiadaniu właścicieli a nie w zasobach infrastruktury EuroCert; Przypominamy, że użycie certyfikatu wymaga dostępu do urządzenia oraz kodu PIN;
- w przypadku certyfikatów chmurowych ECSigner klucze kryptograficzne nie zostały skompromitowane, a wszystkie hasła zostały zresetowane i użytkownik przed użyciem musi nadać swoje nowe hasło. Ponadto, oprócz hasła następuje uwierzytelnienie również przy pomocy jednorazowego kodu w aplikacji na telefonie komórkowym (uwierzytelnienie dwuskładnikowe).

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

W przypadku jakichkolwiek pytań związanych z naruszeniem mogą się Państwo skontaktować z EuroCert Sp. z o.o. kierując zapytanie mailowe na adres: iod@eurocert.pl

Jakie mogą być potencjalne konsekwencje naruszenia ochrony danych osobowych?

Następstwem naruszenia Państwa danych osobowych może być:

- przetwarzanie danych osobowych w celach marketingowych bez uprzedniego uzyskania zgody (w przypadku prowadzenia marketingu drogą tradycyjną, tj. wysyłki treści marketingowych na adres zamieszkania).
- publikacja lub ujawnienie danych osobowych co może naruszać Państwa dobra osobiste;

- zagrożenie nękaniem 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.

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.

Łukasz Konikiewicz

Prezes Zarządu

EuroCert Sp. z o.o.