

Zawiadomienie o naruszeniu ochrony Pani/Pana danych osobowych

W ostatnich dniach doszło do incydentu, wskutek którego Pani/Pana dane osobowe mogły dostać się w niepowołane ręce. Poniżej przekazujemy informacje dotyczące tego incydentu, a także działań, jakie w związku z tym podejmujemy. Poniżej znajduje się opis kroków, które Pani/Pan może podjąć w związku z incydem. Prosimy o uważną lekturę niniejszego zawiadomienia.

Co się stało?

16 sierpnia 2022 roku stwierdziliśmy potencjalne naruszenie ochrony danych osobowych naszych pracowników, kontrahentów oraz klientów. Nasza baza danych została całkowicie zaszyfrowana przez nieznaną sprawcę. Nie mamy jednak pewności czy oprócz zamierzonego uszkodzenia infrastruktury informatycznej poprzez nieodwracalne uszkodzenie systemu szkodliwym oprogramowaniem, zostały jednocześnie skopiowane posiadane przez nas Pani/Pana dane osobowe.

Po stwierdzeniu naruszenia, w trybie pilnym, wszystkie dane zostały przywrócone na nowych serwerach, a nasza od nowa budowana infrastruktura informatyczna zostanie docelowo poddana analizie przez specjalistów zewnętrznych specjalizujących się w zabezpieczaniu systemów informatycznych, co powinno znacznie zminimalizować ewentualną możliwość wystąpienia podobnych zdarzeń w przyszłości.

W naszym systemie znajdowały następujące dane osobowe:

- imię i nazwisko
- numer PESEL
- seria i numer dowodu osobistego
- numer telefonu
- adres
- adres email

We współpracy z firmą Zeto Białystok, wspierającą nas w zabezpieczaniu systemu informatycznego, dokonaliśmy wszelkich niezbędnych kroków, aby odtworzyć system informatyczny oraz zabezpieczyć dane przed potencjalnym wystąpieniem podobnego incydentu. Zgodnie z polskim prawem sytuacja została zgłoszona do Prezesa Urzędu Ochrony Danych Osobowych

Możliwe konsekwencje

Wskutek niekontrolowanego dostępu niezidentyfikowanych sprawców do naszego systemu informatycznego, może dojść do sytuacji, w której dostęp do danych uzyskała osoba nieupoważniona. Osoba ta miałaby więc informacje o danych wskazanych powyżej. Na chwilę obecną nie mamy żadnych sygnałów, że wskazane powyżej dane zostały gdzieś upublicznione lub są wykorzystywane przez osobę niepowołaną. Jednak, w dalszym ciągu istnieje ryzyko, że dane osobowe zostaną wykorzystane w celu podszycia się pod Panią/Pana (tzw. kradzież tożsamości).

Może to wynikać z faktu, że:

- istnieją instytucje pozabankowe, które umożliwiają realizację procedury uzyskania kredytu przez Internet lub telefonicznie i wymagają jedynie podania podstawowych danych identyfikacyjnych, w tym numeru PESEL, bez okazywania dokumentów;
- niektóre firmy ubezpieczeniowe wydają polisy ubezpieczeniowe, a także wypłacają odszkodowania z ubezpieczenia bez weryfikacji oryginalnych dokumentów tożsamości ubezpieczonego;
- pewni dostawcy różnego rodzaju usług dopuszczają skuteczne zawarcie umowy na dostawę usługi (np. telewizja kablowa, telefon, Internet) bez konieczności okazywania dokumentu tożsamości, a jedynie po podaniu podstawowych danych identyfikacyjnych,
- samorządy lub inne instytucje administracji publicznej udostępniają niektóre swoje usługi w oparciu o identyfikację użytkownika za pomocą numeru PESEL;
- istnieją systemy rejestracji pacjenta, do których dostęp można uzyskać telefonicznie podając numer PESEL;
- osoby, które uzyskały dostęp do Pani/Pana danych, mogą podejmować próby wyłudzenia środków finansowych zgromadzonych na Pani/Pana prywatnych kontach bankowych podszywając się pod instytucje finansowe za pomocą SMS-ów;
- operatorzy telekomunikacyjni umożliwiają rejestrację przedpłaconej karty telefonicznej (pre-paid) jedynie w oparciu o podstawowe dane identyfikacyjne, w tym numer PESEL, bez konieczności okazywania dokumentów.

Konsekwencjami nieuprawnionego wykorzystania Pani/Pana danych w tego typu sytuacjach

mogą być na przykład:

- uzyskanie przez osoby trzecie kredytów na Pani/Pana szkodę;
- powstania w stosunku do Pani/Pana zadłużenia w przypadku nieopłacania nabytych usług przez nieuczciwe osoby;
- próba przypisania Pani/Panu oszustwa w postaci wyłudzenia odszkodowania od ubezpieczyciela;
- ograniczenie możliwości korzystania z praw obywatelskich i usług kierowanych do ogółu obywateli (np. głosowania w ramach budżetu obywatelskiego, internetowej rejestracji wizyt w urzędach);
- uzyskanie dostępu do korzystania ze świadczeń opieki zdrowotnej oraz danych o stanie zdrowia;
- uzyskanie dostępu do środków finansowych zgromadzonych na Pani/Pana prywatnych kontach bankowych;
- próby przypisania Pani/Panu odpowiedzialności za przestępstwo, do popełnienia, którego posłużono przedpłaconą kartą telefoniczną (pre-paid) zarejestrowaną na Pani/Pana.

Ponadto, świadomość możliwego upublicznienia Pani/Pana danych osobowych może wywoływać stres lub inne negatywne odczucia.

Działania podjęte przez nas

Niezwłocznie po wykryciu incydentu podjęliśmy działania mające na celu przeciwdziałanie naruszeniu i zminimalizowanie jego negatywnych skutków dla osób, których dane dotyczą. O nieuprawnionym

dostępie do Pani/Pana danych osobowych zawiadomiliśmy również Prezesa Urzędu Ochrony Danych Osobowych. Na bieżąco monitorujemy, czy ww. dane zostały gdzieś upublicznione lub wykorzystane przez osobę nieuprawnioną. Na chwilę obecną nie mamy żadnych sygnałów o takim nieuprawnionym wykorzystaniu danych lub o ich upublicznieniu.

Niezależnie od powyższego, przeprowadziliśmy analizę przyczyn wystąpienia naruszenia i zdecydowaliśmy się na wprowadzenie odpowiednich środków, które mają na celu przeciwdziałać wystąpieniu podobnego incydentu w przyszłości.

Co może Pani/Pan zrobić?

W związku z ryzykiem kradzieży tożsamości, zalecamy Pani/Panu podjęcie następujących działań, które zminimalizują ewentualne negatywne skutki naruszenia:

- rekomendujemy skorzystanie z możliwości uzyskania informacji z systemu informacji kredytowej. W tym celu może Pani/Pan zarejestrować się na stronie Biura Informacji Kredytowej (BIK) i ściągnąć raport na temat swoich zobowiązań kredytowych i finansowych. Więcej informacji może Pani/Pan uzyskać na stronie BIK (www.bik.pl/).
- rekomendujemy skorzystanie z możliwości uzyskania informacji na temat Pani/Pana zobowiązań pieniężnych z biur informacji gospodarczych (BIG). Dostęp do informacji gospodarczych Pani/Pana dotyczących jest bezpłatny, jeżeli następuje nie częściej niż raz na 6 miesięcy (art. 23 ustawy o udostępnianiu informacji gospodarczej i wymianie danych gospodarczych). Wykaz biur informacji gospodarczych oraz lista stron internetowych, na których może Pan uzyskać więcej informacji znajdują się na stronie internetowej: <https://www.gov.pl/web/rozwoj-technologie/wykaz-biur-wykonujacych-dzialalnosc-gospodarcza>
- rekomendujemy poinformowanie właściwych organów, w szczególności Policji, o fakcie naruszenia Pani/Pana danych osobowych w celu zapobieżenia tzw. kradzieży tożsamości.
- rekomendujemy zachowanie ostrożności przy podawaniu Pani/Pana danych osobowych innym osobom. Dotyczy to w szczególności podawania danych za pośrednictwem Internetu lub przez telefon.

PEŁNOMOCCNIK ZARZADU
DYREKTOR GENERALNY
„ENERGO” Sp. z o.o.

Karol Barowski