**Komunikat o możliwości naruszenia ochrony danych osobowych**

Usługi Komunalne spółka z ograniczoną odpowiedzialnością jako Administrator Danych Osobowych przetwarzanych w ramach jej działalności informuje o naruszeniu ochrony danych osobowych związanych z incydentem do jakiego doszło w dniu 25 lipca 2019 roku polegającym na ataku hakerskim typu ransomware na jedną z wirtualnych instancji na serwerze należącym do spółki Środa XXI sp. z o.o. dostarczającą usługi hostingowe dla spółki Usługi Komunalne sp. z o.o.. Atak rozpoczął się od około godziny 1.20 (godzinę stwierdzono po analizie plików tj. taką godzinę miał pierwszy zaszyfrowany plik). Ponadto wykryta została informacja, żądanie okupu wypłaty określonej kwoty w Bitcoinach w celu odzyskania utraconych plików.

Utracone zostały, więc dane znajdujące się na pulpitach zdalnych, z których korzystają pracownicy spółki. Ponieważ znajdowały się tam rejestry, np. wykazy zawierające dane osobowe kontrahentów zawierających umowy w ramach świadczonych przez spółkę usług (w zakresie gospodarki mieszkaniowej, gospodarowania odpadami czy prowadzonym zakładem pogrzebowym), czy też pracowników możliwe jest naruszenie ochrony danych osobowych. Bazy danych programu służącego do obsługi administracyjnej spółki ze względu na to, że znajdowały się w odrębnym środowisku nie zostały naruszone, nie doszło również do wycieku danych (byłoby to praktycznie niemożliwe w tak krótkim czasie ze względu na bardzo niską prędkość i jakość połączenia z siecią Internet). Prewencyjnie w dniu zdarzenia zostały wykonane kopie tych baz na zewnętrznym nośniku na wypadek rozprzestrzenienia się szkodliwego oprogramowania, które jednak nie zostało wykryte. Zainfekowany został serwer, do którego łączyli się wszyscy użytkownicy z 3 podmiotów (administratora, a także podmiotów korzystających z serwera spółek Usługi Komunalne sp. z o.o. oraz Lidera Usług Komunalno-Samorządowych w Środzie Wielkopolskiej) na każdym koncie "osobistym" zainstalowana była aplikacja.

Wprawdzie charakter ataku powoduje, że możliwe jest iż dane zostały w trakcie ataku trwale zniszczone i nie ma możliwości ich odczytania, to ponieważ nie można ponad wszelką wątpliwość wykluczyć takiej sytuacji, której w posiadanie danych weszłaby osoba nieuprawniona. Możliwymi konsekwencjami jest nieuprawnione wykorzystanie danych osobowych w celu m.in.:

- uzyskania przez osoby trzecie, na szkodę osób, których dane naruszono, kredytów w instytucjach poza bankowych, ponieważ wiele takich instytucji umożliwia uzyskanie pożyczki lub kredytu w łatwy i szybki sposób np. przez Internet lub telefonicznie bez konieczności okazywania dokumentu tożsamości,

- uzyskania dostępu do korzystania ze świadczeń opieki zdrowotnej przysługujących osobom, których dane naruszono oraz ich danych o stanie zdrowia, ponieważ często dostęp do systemów rejestracji pacjenta można uzyskać telefonicznie potwierdzając swoją tożsamość za pomocą numeru PESEL,

- korzystania z praw obywatelskich osób, których dane naruszono, np.: do głosowania nad środkami budżetu obywatelskiego co z kolei uniemożliwiałoby to osobom których dane w sposób nieuprawniony użyto skorzystanie z przysługującego im prawa,

- wyłudzenia ubezpieczenia lub środków z ubezpieczenia, co może spowodować dla osób, których dane dotyczą, negatywne konsekwencje w postaci problemów związanych z próbą przypisania im odpowiedzialności za dokonanie takiego oszustwa,

- zarejestrowanie przedpłaconej karty telefonicznej (pre-paid), która może posłużyć do celów przestępczych.

Aby zabezpieczyć się przed negatywnymi skutkami zaistniałego naruszenia Administrator zaleca aby osoby, których dane osobowe mogły brać udział w wyżej opisanym naruszeniu, podjęły kroki minimalizujące negatywne ryzyko opisanego nieuprawnionego pozyskania danych np. poprzez:

- założenie konta w systemie informacji kredytowej i gospodarczej w celu monitorowania swojej aktywności kredytowej, rozporządzenie RODO daje możliwość, uzyskania darmowego dostępu do zebranych na swój temat danych w formie „kopii danych", którą mamy prawo uzyskać od BIK,

- zachowanie szczególnej ostrożności przy podawaniu danych osobowych innym osobom, zwłaszcza za pośrednictwem Internetu czy telefonu,

- zgłoszenia faktu naruszenia danych właściwym organom w celu zapobieżenia tzw. „kradzieży tożsamości".

Podjęcie tych działań ma na celu zabezpieczenie danych osobowych przed ich niewłaściwym wykorzystaniem.

Administrator aby zapewnić właściwą ochronę danych osobowych oraz w celu niedopuszczenia do zaistnienia podobnych naruszeń danych wprowadził nowe polityki określające zasady ochrony danych osobowych, planuje wprowadzenie zmian w sferze stosowanych rozwiązań informatycznych mających na celu zapewnienie wzmocnionej ochrony przed takimi atakami w przyszłości.

Administrator danych osobowych informuje, że zostały podjęte niezbędne działania, aby podobna sytuacja nie miała miejsca w przyszłości. W razie dodatkowych pytań lub wątpliwości prosimy o kontakt z Inspektorem Danych Osobowych: Łukasz Gąsiorek pod numerem tel. 61 4244033, e-mail: iod@lesny.com.pl

Niniejszy komunikat został przygotowany zgodnie z wymogami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. 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) Dz. U. UE. L. 2016.119.1. z dnia 4 maja 2016 r.