KOMUNIKAT

Szanowni Państwo,

z przykrością informujemy, że w dniu 15.03.2024 r. doszło do doszło do ataku na infrastrukturę informatyczną APAR Control sp. z o.o. Atak, którego padliśmy ofiarą, to atak typu ransomware. Ransomware to rodzaj złośliwego oprogramowania, które infekuje komputer lub system, szyfruje dane ofiary i żąda okupu za ich odblokowanie. Głównym celem takiego ataku jest zmuszenie ofiary do zapłaty okupu, często w postaci kryptowaluty (np. Bitcoin), w zamian za klucz umożliwiający odszyfrowanie danych.

W wyniku naruszenia zostały ujawnione dotyczące Państwa następujące dane osobowe:

- imię i nazwisko;
- adres firmy, którą Państwo reprezentujecie;
- kwoty transakcji;
- numer telefonu;
- adres e-mail;

Rozumiemy, że ta sytuacja może budzić Państwa zaniepokojenie, dlatego przygotowaliśmy odpowiedzi na pytania:

- Jakie skutki naruszenie może nieść dla Państwa?
- Co zrobiliśmy do tej pory, aby minimalizować ryzyko dla Państwa?
- Co Państwo mogą zrobić w tej sprawie?
- Z kim się kontaktować w razie dodatkowych pytań?

Liczymy, że w ten sposób przekażemy Państwu wiedzę i narzędzia potrzebne do zapewnienia bezpieczeństwa.

Jakie skutki naruszenie może nieść dla Państwa?

Stale monitorujemy sytuację.

Nie stwierdziliśmy w tym czasie, aby wykorzystano Państwa dane w niepożądany sposób. Jednak ze względu na zakres ujawnionych danych uważamy, że powinni Państwo wziąć pod uwagę powstałe ryzyko. Ktoś może próbować:

- uzyskać kredyt w instytucjach pozabankowych z wykorzystaniem Państwa danych. Jest to możliwe, ponieważ instytucje te zwykle zapewniają łatwy i szybki proces kredytowy, a nawet nie wymagają, aby klient okazał dokument tożsamości;
- uzyskać dostęp do świadczeń opieki zdrowotnej, które Państwu przysługują, lub do danych o stanie Państwa zdrowia. Może się tak stać, ponieważ często do telefonicznej rejestracji lub weryfikacji pacjenta wystarczy podanie numeru PESEL;
- używając Państwa danych, zawrzeć umowę o świadczenie usług, na przykład telewizji kablowej, telefonu czy Internetu, a potem przestać opłacać rachunki;
- wykorzystując Państwa dane, utworzyć konto w serwisie internetowym, na przykład społecznościowym;
- wysyłać Państwu niechcianą pocztę (spam);
- wykonywać do Państwa niechciane telefony, na przykład o charakterze marketingowym;

- przekazać osobom postronnym informacje, które Państwa dotyczą, w wyniku czego mogą odczuwać Państwo dyskomfort;
- próbować wyłudzić od Państwa dodatkowe informacje, potrzebne na przykład do zaciągnięcia kredytu w Państwa imieniu;
- opublikować Państwa dane w Internecie;

Czujemy się odpowiedzialni za zaistniałą sytuację, dlatego zależy nam, aby możliwie jak najpełniej znali Państwo potencjalne ryzyka. Oczywiście nie muszą one wystąpić w tym przypadku. Mimo to chcemy, aby byli Państwo ich świadomi i wiedzieli, jak się przed nimi bronić.

Co zrobiliśmy do tej pory, aby minimalizować ryzyko dla Państwa?

Prywatność osób, które powierzyły nam swoje dane, ma dla nas kluczowe znaczenie. Chcemy więc poinformować, co zrobiliśmy do tej pory, aby minimalizować ryzyko dla Państwa:

- zgłosiliśmy naruszenie Prezesowi Urzędu Ochrony Danych Osobowych oraz podmiotom odpowiedzialnym za bezpieczeństwo polskiej cyberprzestrzeni – CSIRT NASK oraz Centralnego Biura Zapobiegania Cyberprzestępczości;
- powtórnie przeszkoliliśmy nasz personel z zasad ochrony danych osobowych;
- przywróciliśmy dane dzięki kopii zapasowej;
- zbadaliśmy i zidentyfikowaliśmy rodzaj złośliwego oprogramowania;
- zabezpieczyliśmy zainfekowany sprzęt;
- wykonaliśmy audyt IT naszych systemów;

Dodatkowo, chcemy Państwa zapewnić, że dokładamy wszelkich starań, aby podobna sytuacja nie powtórzyła się w przyszłości. Jesteśmy w pełni zaangażowani w ochronę i bezpieczeństwo Państwa danych. Ufamy, że nasze działania przyczynią się do odbudowy zaufania i poczucia bezpieczeństwa wśród wszystkich osób, których dane zostały naruszone.

Co Państwo mogą zrobić w tej sprawie?

Prosimy, aby rozważyli Państwo podjęcie któregoś (lub nawet kilku) z poniższych działań. Mogą one znacząco zredukować ryzyko nieuprawnionego wykorzystania Państwa danych osobowych. Z uwagi na zakres danych, które zostały ujawnione, zachęcamy Państwa do:

- zweryfikowania, czy przestępcy opublikowali Państwa dane. Można to zrobić na rządowej stronie: https://bezpiecznedane.gov.pl/;
- zgłaszania podejrzanych wiadomości SMS na numer 8080. Jest on obsługiwany przez zespół CERT Polska, którego zadaniem jest reagowanie na zdarzenia naruszające bezpieczeństwo w Internecie;
  Wskazówka: Eksperci z CERT radzą, by podejrzane SMS-y przesyłać im poleceniem "Przekaż" lub "Prześlij dalej", a jeśli nie ma takiej możliwości, wystarczy skopiować treść wiadomości i wysłać ją na wspomniany numer. Dotyczy to wiadomości z linkami, ale też tych, które ich nie zawierają. Zgłoszenia mają pozytywnie wpłynąć na poprawę wspólnego bezpieczeństwa.
- zgłaszania prób oszustw (takich jak: złośliwe domeny, podejrzane wiadomości e-mail, fałszywe sklepy internetowe, złośliwe oprogramowanie, nielegalne treści) na stronie: https://incydent.cert.pl/#!/lang=pl,entityType=notObligatedEntity. Jest ona obsługiwana przez zespół CERT Polska, którego zadaniem jest reagowanie na zdarzenia naruszające bezpieczeństwo w Internecie;

- założenia konta w systemie informacji kredytowej i gospodarczej. Dzięki temu będą mogli Państwo monitorować przypisaną Państwu aktywność kredytową;
  Wskazówka: W niektórych systemach informacji kredytowej mogą Państwo włączyć alerty SMS i e-mail. Otrzymają je Państwo, gdy pojawią się zapytania od podmiotów finansowych o Państwa historię kredytową.
- zgłoszenia właściwym instytucjom publicznym nieuprawnionego wykorzystania Państwa danych osobowych. Można to zrobić na stronie: https://www.gov.pl/web/gov/zglos-nieuprawnione-wykorzystanie-swoich-danych-osobowych-kradziez-tozsamosci--uniewaznij-dowod;
- w przypadku upublicznienia Państwa danych – zwrócenia się do administratora strony, na której pojawiły się Państwa dane, z żądaniem ich usunięcia. Instrukcja, jak to zrobić, znajduje się na stronie wspierającej nas firmy konsultingowej: https://odo24.pl/blog-post.jak-reagowac-na-kradziez-tozsamosci;
- w przypadku kradzieży tożsamości bądź próby szantażu przez cyberprzestępców – zgłoszenia tych przestępstw na policję. W takim przypadku warto rozważyć kontakt z najbliższym Wydziałem Terenowym Centralnego Biura Zwalczania Cyberprzestępczości: https://cbzc.policja.gov.pl;
- sprawdzenia, czy dane które wyciekły, nie były przez Państwa wykorzystywane jako dane do logowania, w celu ich zmiany we wszystkich serwisach, w których były wykorzystywane;
- zachowania ostrożności, gdy podają Państwo swoje dane osobowe innym osobom, zwłaszcza za pośrednictwem Internetu czy telefonu;
- zachowania szczególnej ostrożności w razie otrzymania wiadomości od nieznanych odbiorców;
- weryfikowania numerów rachunków bankowych w wiadomościach i powstrzymania się z zapłatą, jeśli numer rachunku różni się od tego, na który dotychczas wpłacali Państwo należności;
- niewykonywania płatności, których zażądano SMS-owo, telefonicznie, e-mailowo lub w inny sposób, którego firma APAR Control sp. z o.o. nie używa regularnie;
- skontaktowania się z nami, jeśli będą mieć Państwo wątpliwości, czy to na pewno my wysłaliśmy do Państwa wezwanie, lub gdy będą chcieli Państwo ponownie wprowadzić utracone dane.

Jeśli zauważą Państwo jakiekolwiek oznaki nieuprawnionego wykorzystania Państwa danych, prosimy o jak najszybsze przekazanie nam tych informacji.

Z kim się kontaktować w razie dodatkowych pytań?

Jesteśmy do Państwa pełnej dyspozycji. Zapewniamy, że każde z pytań i obaw zostanie potraktowane z należytą powagą i uwagą. Jesteśmy gotowi udzielić wszelkiej pomocy i wsparcia. Pełne dane teleadresowe znajdują się na naszej stronie internetowej.

Z wyrazami szacunku

Zarząd

APAR Control sp. z o.o.