

ZAWIADOMIENIE O POTENCJALNYM NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Szanowni Państwo,

Informujemy, że w dniu dzisiejszym firma Zamoyskiego s.c. otrzymała zgłoszenia od klientów dotyczące prób podszywania się pod nasz obiekt, w celu wyłudzenia danych o kartach płatniczych (pod pozorem potwierdzenia / anulowania rezerwacji). Atakujący próbowali kontaktować się za pomocą aplikacji WhatsApp oraz wysyłając fałszywe wiadomości e-mail.

Mając na uwadze Państwa bezpieczeństwo oraz realizując wymogi obowiązujących przepisów prawa, przygotowaliśmy dla Państwa najważniejsze informacje.

Prosimy o dokładne zapoznanie się z treścią poniższego komunikatu.

Zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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; dalej jako: „RODO”), informujemy, że:

W wyniku przeprowadzonej analizy stwierdziliśmy, że padliśmy ofiarą ataku na systemy informatyczne należące do operatora systemu rezerwacji KW HOTEL, którym jest KajWare Sp. z o.o. Z przekazanych nam informacji wynika, że doszło do włamania na jeden z serwerów, na którym przechowywana była baza danych rezerwacji dokonanych przez naszych Klientów. Dotychczas nie potwierdzono czy atakujący uzyskali dostęp do części, czy też do pełnej zawartości bazy danych, a także czyje konkretnie dane zostały uzyskane.

Mając jednak na uwadze zgłoszenia otrzymane dzisiaj bezpośrednio od naszych klientów nie można wykluczyć, że również Państwa dane osobowe mogły zostać wykradzione.

Zakres kategorii danych, jakie mogły zostać objęte incydem to:

- dane dotyczące rezerwacji (np. imię, nazwisko, adres email, numer telefonu lub inne, które podali Państwo dokonując rezerwacji),
- daty rezerwacji i kwoty rezerwacji,
- dokumenty księgowe (wystawione faktury/paragony).

Możliwe konsekwencje wynikające z naruszenia ochrony danych osobowych

Korzystając z wykradzonych danych osoby trzecie mogą dokonywać prób uzyskania korzyści majątkowej Państwa kosztem (np. wyłudzenie kredytów czy też pożyczek w instytucjach poza bankowych). Mogą wystąpić także potencjalnie próby nakłonienia Państwa do opłacenia fikcyjnych zobowiązań finansowych lub pojawić się próby wyłudzenia innych Państwa danych, które nie zostały wcześniej wykradzione w wyniku naruszenia. Mogą być podejmowane próby dokonywania zakupów w sieci internet, poprzez fikcyjne konta użytkowników zawierające Państwa dane. Mogą być zakładane na Państwa dane osobowe konta w serwisach społecznościowych, a także skrzynki poczty elektronicznej, wykorzystywane później do innych prób wyłudzenia danych.

Proponowane działania jakie mogą Państwo podjąć w celu przeciwdziałania skutkom naruszenia

W przypadku podejrzenia wykorzystania Państwa danych osobowych w sposób nieuprawniony, zalecamy niezwłoczny kontakt z Policją. Prosimy zwracać uwagę na próby kontaktu ze strony osób podających się za przedstawicieli naszego obiektu – w szczególności prosimy zwracać uwagę na próby wyłudzeń poprzez podszywanie się pod naszą tożsamość oraz powoływanie na dane z

rezerwacji, wysyłane drogą e-mail lub komunikatorami internetowymi (np. WhatsApp) – gdy zostaną Państwo proszeni o uregulowanie należności za pobyt w naszym obiekcie lub podanie danych osobowych klikając w linki znajdujące się w treści takich wiadomości. Zalecamy nie odpowiadać na takie próby kontaktu ani nie klikać w linki – jednocześnie proponujemy wyjaśniać takie sytuacje kontaktując się z nami na pod adresem wskazanym na końcu niniejszego komunikatu.

W celu uniknięcia ewentualnych negatywnych następstw oraz zabezpieczenia się przed negatywnymi skutkami naruszenia zalecamy Państwu stosowanie powszechnie zalecanych zasad ostrożności obowiązujących w sytuacjach wzmożonej aktywności phishingowej:

- zachowanie wzmożonej czujności podczas prób weryfikacji Państwa tożsamości, dokumentu tożsamości lub czynności, w których Państwo nie uczestniczyli w trakcie niespodziewanych rozmów telefonicznych, szczególnie z numerów zagranicznych oraz zastrzeżonych,
- weryfikowanie tożsamości osób i instytucji, które proszą o podanie danych,
- zwrócenie szczególnej uwagi na podejrzane załączniki (archiwa, pliki PDF) w wiadomościach e-mail oraz nie otwieranie linków do stron internetowych które są w nich zawarte,
- dokładne zapoznawanie się z treścią korespondencji papierowej, która jest przesyłana na adres, który mogli Państwo podać dokonując rezerwacji,
- założenie konta w systemie informacji kredytowej BIK celem monitorowania swojej aktywności kredytowej – więcej informacji znajdą Państwo pod linkiem <https://www.bik.pl>
- sprawdzenie swoich danych w Krajowym Rejestrze Długów – więcej informacji znajdą Państwo pod linkiem <https://www.krd.pl>

Przypominamy również, że w przypadku umów konsumenckich zawieranych na odległość zazwyczaj w takim przypadku przysługuje prawo odstąpienia od umowy w terminie 14 dni bez ponoszenia żadnych konsekwencji.

Zalecamy również korzystanie z aktualnego oprogramowania antywirusowego, zarówno na komputerach, laptopach jak również urządzeniach mobilnych podłączonych do internetu.

Środki bezpieczeństwa zastosowane w celu zaradzenia naruszeniu ochrony danych osobowych lub zminimalizowania jego ewentualnych negatywnych skutków

Niezwłocznie po ujawnieniu opisanego wyżej incydentu, wspólnie z operatorem systemu rezerwacyjnego, podjęte zostały działania mające na celu jak najszybsze przeciwdziałanie incydentowi oraz jego potencjalnym skutkom. Tymczasowo wyłączono zostały zaatakowane systemy IT u operatora systemu rezerwacyjnego, a przed ich ponownym uruchomieniem wymuszono zmianę haseł dostępowych do bazy danych na serwerach.

Dane kontaktowe w przypadku dodatkowych pytań dotyczących potencjalnego naruszenia:

Obecnie na bieżąco monitorujemy sytuację związaną ze stwierdzonym incydemem i komunikaty ze strony operatora systemu rezerwacyjnego KW HOTEL, który był bezpośrednim obiektem ataku związanego z incydemem naruszenia przetwarzania danych osobowych.

Jednocześnie w przypadku dodatkowych pytań z Państwa strony informujemy, że istnieje możliwość kontaktu z nami pod adresem e-mail:

biuro@noclegistadion.pl