SFINKS POLSKA S.A.

Zalesie Górne, 17.03.2022r.

Wybrani kontrahenci Spółki
(dane osobowe wskazane
w zawartych ze Spółką umowach,
w większości dostępne publicznie)

Pełnomocnicy Spółki

Dotyczy: naruszenia danych osobowych w związku z atakiem hackerskim z kwietnia 2021 r.

Chcielibyśmy poinformować Państwa, że w kwietniu 2021 r. staliśmy się celem cyberataku. Nieznani sprawcy przy użyciu złośliwego oprogramowania zaatakowali niektóre z naszych systemów informatycznych i zaszyfrowali przechowywane tam dane, wśród których znajdowały się Państwa dane osobowe.

Z chwilą wykrycia naruszenia bezzwłocznie wyłączyliśmy wszystkie zaatakowane serwery w celu uniemożliwienia kopiowania ich zawartości. Nie jest jednak możliwe określenie czy w rzeczywistości zostały pobrane, a jeśli tak ile konkretnie danych mogło zostać pobranych podczas ataku przez hakerów. Z posiadanych przez nas informacji wynika, że z dużym prawdopodobieństwem doszło jedynie do zaszyfrowania danych bez ich skopiowania na dyski zewnętrzne niemniej jednak prosimy Państwa o zachowanie czujności ponieważ nie możemy całkowicie wykluczyć, że jakieś dane mogły zostać skopiowane wskutek czego mogło dojść do naruszenia Państwa danych osobowych.

Jednocześnie informujemy, że podjęliśmy działania zmierzające do zwiększenia bezpieczeństwa infrastruktury informatycznej spółki.

Zaistniały incydent dotyczył danych zapisanych przed kwietniem 2021r. Został on zgłoszony na Policję oraz do Urzędu Ochrony Danych Osobowych, który w lutym br. zwrócił się do nas o poinformowanie Państwa o związanym z nim możliwym naruszeniu Państwa danych osobowych danych oraz o przekazanie informacji dotyczących możliwych jego konsekwencji.

Kategorie danych osobowych, które mogły ulec naruszeniu w odniesieniu do:

kontrahentów: dane osobowe wskazane w zawartych ze Spółką umowach, w większości dostępne publicznie (CEiDG, KRS), w niektórych przypadkach dodatkowo: seria i nr dowodu osobistego, PESEL, służbowy adres e-mail, telefon

Sfinks Polska S.A., 05-540 Zalesie Górne, ul. Młodych Wilczął 36, tel. +48 22 7027 101, faks: +48 22 7027 132,
www.sfinks.pl
NIP 725-17-52-913, REGON 472247798, BDO 000079521,
Sąd Rejonowy dla m. st. Warszawy w Warszawie, XIV Wydział Krajowego Rejestru Sądowego, KRS 0000016481
Kapitał zakładowy 32 199 512,00 PLN wpłacony w całości

Pełnomocników: seria i nr dowodu osobistego, PESEL, adres zamieszkania, numer karty pobytu.

O możliwych skutkach naruszenia oraz działaniach jakie mogą Państw podjąć cele zminimalizowania ewentualnych negatywnych skutków naruszenia informujemy w załączniku do niniejszego pisma.

Bardzo nam przykro, że cyberatak objął dane osobowe. Ściśle współpracowaliśmy ze specjalistami m.in. ds. cyberbezpieczeństwa aby taki incydent się więcej nie powtórzył. Bezpieczeństwo danych jest naszym priorytetem.

Co prawda, do dnia dzisiejszego nie otrzymaliśmy żadnych informacji o podejrzanych zdarzeniach z wykorzystaniem danych które zostały zaszyfrowane, niemniej prosimy o zgłaszanie naszemu Inspektorowi Danych osobowych wszelkich podejrzanych zachowań, w szczególności jeżeli dowiecie się o wykorzystaniu Państwa danych przez osobę nieuprawnioną.

Inspektorem Danych Osobowych w Spółce jest Piotr Czachorowski. Kontakt na adres Spółki: Sfinks Polska S.A., 05-540 Zalesie Górne, ul. Młodych Wilcząt 36 lub poprzez e-mail iod@sfinks.pl z dopiskiem „IOD”

Jeśli mają Państwo pytania w powyższym zakresie, prosimy o kontakt na adresy jak powyżej.

Dziękujemy za zrozumienie.

Prezes Zarządu
Sfinks Polska S.A.

Załącznik do zawiadomienia:

W przypadku pozyskania niektórych danych przez hakerów istnieje ryzyko naruszenia praw lub wolności osób fizycznych poprzez próbę wykorzystania danych dotyczących tożsamości. Następstwem naruszenia Pani/Pana danych osobowych może być:

1. założenie na Pani/Pana dane osobowe konta internetowego (np. w serwisach społecznościowych),
2. podszycie się pod inną osobę lub instytucję w celu wyłudzenia od Pani/Pana dodatkowych określonych informacji (np. danych do logowania, szczegółów karty kredytowej),

3. osoby trzecie mogą podjąć próbę uzyskania na Pani/Pana szkodę, pożyczek w instytucjach pozabankowych np. przez Internet lub telefonicznie, bez konieczności okazywania dokumentu tożsamości;
4. osoby trzecie mogą podjąć próbę uzyskania dostępu do systemów obsługujących udzielanie świadczeń medycznych i uzyskać wgląd do danych o Pani/Pana stanie zdrowia, ponieważ czasem dostęp do systemów rejestracji pacjenta można uzyskać, potwierdzając swoją tożsamość za pomocą numeru PESEL;
5. Pani/Pana dane osobowe mogą zostać wykorzystane np. do oddania głosu w głosowaniu nad środkami budżetu obywatelskiego tym samym skorzystać z Pani/Pana praw obywatelskich;
6. osoby trzecie mogą podjąć próbę zawarcia na Pani/Pana szkodę umów cywilno-prawnych, np. najmu nieruchomości;
7. Pani/Pana dane osobowe mogą zostać wykorzystane przez osoby trzecie do ukrycia swojej tożsamości, np. przy otrzymywaniu mandatu.

W celu zminimalizowania ewentualnych negatywnych skutków naruszenia zalecamy:

- zachowanie ostrożności przy podawaniu danych osobowych innym osobom, zwłaszcza za pośrednictwem Internetu czy telefonu,
- ignorowanie nieoczekiwane wiadomości (e-mail, SMS), w szczególności od nieznanych nadawców,
- rozważenie skorzystanie z możliwości zastrzeżenia dokumentu tożsamości w systemie dokumenty zastrzeżone (więcej informacji www.dokumentyzastrzezone.pl) i jego wymiany,
- skorzystanie z możliwoścí założenia konta w systemie informacji kredytowej celem monitorowania prób uzyskania kredytu w oparciu o wasze dane osobowe.

Sfinks Polska S.A., 05-540 Zalesie Górne, ul. Młodych Wilcząt 36, tel. +48 22 7027 101, faks: +48 22 7027 132,
www.sfinks.pl
NIP 725-17-52-913, REGON 472247798, BDO 000079521,
Sąd Rejonowy dla m. st. Warszawy w Warszawie, XIV Wydział Krajowego Rejestru Sądowego, KRS 0000016481
Kapitał zakładowy 32 199 512,00 PLN wpłacony w całości