Do: / To:
Pracownicy Intertoll Construction Sp. z o.o.

Nasz nr ref / Our ref: ITC/GDA/MOP/0046/23 Data / Date: 01/06/2023
Was znak sprawy:

Komunikat o naruszeniu ochrony danych osobowych

Zgodnie z rozporządzeniem 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), jako administrator danych osobowych pracowników Intertoll Construction Sp. z o.o. (***dalej: ITC***), informujemy, że w ostatnim czasie doszło do zdarzenia, wskutek którego dostęp do danych osobowych **802 pracowników zatrudnionych w ITC od września 2005 r. do grudnia 2019 r.** zawartych w dokumentacji przekazanej na podstawie umowy powierzenia przetwarzania danych osobowych HK Finance Sp. z o.o. będącej dostawcą usług księgowych, kadrowo-płacowych i doradztwa finansowego, uzyskały osoby, które nie są do tego uprawnione. Poniżej przekazujemy szczegółowe informacje na temat tego zdarzenia.
W związku z brakiem możliwości bezpośredniego skontaktowania się z byłymi pracownikami ITC, których dane dotyczą, niniejszym informujemy o naruszeniu w drodze publicznego komunikatu.

Jak doszło do naruszenia danych osobowych

W dniu 30 maja 2023 r. HK Finance sp. z o.o. (***dalej: HK Finance***) poinformowała ITC, że dane osobowe zawarte w przekazanej HK Finance przez ITC dokumentacji, zostały bezprawnie pozyskane i ujawnione przez osoby trzecie w wyniku przestępstwa - ukierunkowanego ataku hackerskiego na systemy informatyczne. Incydentem zostało objęte środowisko serwerowe HK Finance. Atakujący przy pomocy oprogramowania wirusowego typu ransomware uzyskali dostęp do infrastruktury informatycznej HK Finance, w tym do archiwalnych danych osobowych dotyczących danych pracowników ITC według stanu z roku 2018.
W wyniku ataku ukradzione zostały następujące dane osobowe pracowników ITC:

- ✓ imię i nazwisko,
- ✓ numer PESEL,
- ✓ data urodzenia,
- ✓ adres zamieszkania,
- ✓ informacja o wysokości wynagrodzenia.

Powyższe dane osobowe zostały bezprawnie ukradzione przez hakerów i nie jesteśmy w stanie oszacować, ile osób mogło potencjalnie uzyskać do nich dostęp.

Jakie są potencjalne ryzyka związane z wykorzystaniem wykradzionych danych osobowych

Osoba, która ma dostęp do wykradzionych danych osobowych, może bezprawnie:

- ✓ założyć konto internetowe z użyciem wykradzionych danych osobowych w serwisach internetowych nieweryfikujących danych użytkowników;
- ✓ próbować podszyć się pod inną osobę lub instytucję w celu wyłudzenia od osoby, której dane wykradziono, dodatkowych informacji (np. danych do logowania, szczegółów karty kredytowej);
- ✓ wykorzystać dane osoby, której dane wykradziono, do zarejestrowania karty telefonicznej typu prepaid, która może posłużyć do celów przestępczych;
- ✓ próbować uzyskać pożyczki w instytucjach pozabankowych, w których nie ma konieczności okazywania dokumentu tożsamości, np. przez Internet lub telefonicznie;
- ✓ wykorzystać dane osobowe osoby, której dane wykradziono, do uwierzytelniania (weryfikacji tożsamości) i zaciągania zobowiązań w imieniu takiej osoby, np. w sklepach internetowych;
- ✓ próbować uzyskać wgląd do danych o stanie zdrowia osoby, której dane wykradziono, poprzez pozyskanie dostępu do systemów obsługujących udzielanie świadczeń medycznych, w których dostęp do rejestracji pacjenta można uzyskać, potwierdzając swoją tożsamość za pomocą numeru PESEL;
- ✓ próbować wykorzystać dane osobowe osoby, której dane wykradziono, do wyłudzenia ubezpieczenia, np. na skutek podania fałszywych informacji o wypadku komunikacyjnym;
- ✓ próbować zawrzeć na szkodę osoby, której dane wykradziono, umowy cywilnoprawne - np. najmu nieruchomości lub umowy sprzedaży;
- ✓ próbować wykorzystać dane osobowe osoby, której dane wykradziono, do oddania głosu w głosowaniu nad środkami budżetu obywatelskiego, tym samym skorzystać z praw obywatelskich takiej osoby;
- ✓ próbować wykorzystać dane osobowe osoby, której dane wykradziono, do ukrycia swojej tożsamości, np. przy otrzymywaniu mandatu.

Jakie działania podjęliśmy

- ✓ skierowaliśmy do HK Finance żądanie udzielenia szczegółowych informacji dotyczących naruszenia danych osobowych;
- ✓ poinformowaliśmy Prezesa Urzędu Ochrony Danych Osobowych o naruszeniu ochrony danych osobowych.

Niezależnie od powyższego, HK Finance zgłosiło zdarzenie do CSIRT NASK, Centralnemu Biuru Zwalczania Cyberprzestępczości oraz Prokuraturze Okręgowej w Gdańsku.

Jakie działania mogą podjąć osoby, których ochrona danych osobowych została naruszona, by ograniczyć ryzyko negatywnych konsekwencji

- ✓ Można zabezpieczyć swoje dane osobowe przed nieuprawnionym ich wykorzystaniem zakładając konto w systemie informacji kredytowej lub gospodarczej w celu monitorowania swojej aktywności kredytowej i otrzymywania informacji w sytuacji złożenia wniosku kredytowego. Takie funkcjonalności oferują m.in. system alertów Biura Informacji Kredytowej (www.bik.pl) oraz system Bezpieczny PESEL (www.bezpiecznypesel.pl);
- ✓ Należy zachować szczególną ostrożność przy podawaniu w najbliższym czasie swoich danych osobowych innym osobom. Osoby, które potencjalnie mogły wejść w posiadanie danych osobowych mogą próbować skontaktować się z osobami, których dane zostały wykradzione, celem pozyskania dodatkowych danych, a następnie, dysponując szerszym zakresem danych, próbować wykorzystać je do własnych celów. Dotyczy to w szczególności podawania danych za pośrednictwem Internetu lub przez telefon.

W celu zminimalizowania dalszych ewentualnych negatywnych skutków naruszenia zalecamy także:

- ✓ ignorować nieoczekiwane lub podejrzane wiadomości e-mail, w szczególności od nieznanych nadawców lub pochodzące z adresów mailowych usiłujących podszywać się pod powszechnie znane instytucje (np. banki lub organy państwowe) oraz nie otwierać podejrzanych załączników (np. przesyłanych pocztą elektroniczną plików w nieznanym lub niepopularnym formacie);
- ✓ dokładnie analizować wszelkie komunikaty, przekazywane w szczególności drogą elektroniczną (np. informacje o wygranych w konkursach, specjalnych ofert i promocji), aby uniknąć ataku, którego celem może być wyłudzenie dodatkowych danych;
- ✓ nie korzystać z linków do stron internetowych otrzymanych od nieznanych nadawców w wiadomościach mailowych, SMSach lub poprzez komunikatory internetowe;
- ✓ zachować ostrożność w sytuacji odbierania połączeń telefonicznych od nieznanych numerów telefonów oraz podczas korzystania z bankowości elektronicznej lub płatności internetowych (np. każdorazowe sprawdzanie czy strona internetowa posiada certyfikat SSL, czyli secure socket layer);

- ✓ dokładnie analizować wszelkie otrzymywane rachunki lub wezwania do zapłaty pod kątem możliwości podszywania się pod instytucje, z którymi zostały wcześniej zawarte umowy (np. sprawdzanie czy zmianie nie uległ numer konta bankowego do wpłat).

Gdzie można uzyskać więcej informacji?
Dodatkowe informacje w związku z zaistniałym zdarzeniem można uzyskać kierując zapytanie do Mireli Opinc - adres e-mail: mirela.opinc@intertoll.pl.

Z poważaniem,

Piotr Rotter

INTERTOLL Elektronicznie podpisany przez PIOTR ROTTER
Data: 2023.06.01 11:53:16 +02'00'

Członek Zarządu

Maciej Nafalski

INTERTOLL Elektronicznie podpisany przez MACIEJ NAFALSKI
Data: 2023.06.01 12:06:06 +02'00'

Członek Zarządu