Kluczowe informacje dotyczące zgłoszenia

Data zgłoszenia: 20.04.2023.	
Charakter naruszenia	Miał miejsce incydent bezpieczeństwa polegający na uzyskaniu nieautoryzowanego dostępu do fragmentu bazy danych zawierającej powierzone dane, w tym o przeprowadzonych wysyłkach
Data naruszenia	od 12.04.2023 godz. 9.30 do 14.04.2023 godz. 11.32
Czas trwania naruszenia	od 12.04.2023 godz. 9.30 do 14.04.2023 godz. 11.32
Data stwierdzenia naruszenia	19.04.2023
Kategorie danych osobowych, których dotyczy naruszenie	Nazwę Państwa firmy, NIP, Login konta głównego, oraz dane osoby kontaktowej z ramienia Państwa firmy (imię i nazwisko) oraz jej nr telefonu.
Opis możliwych konsekwencji naruszenia	☒ Utrata kontroli nad własnymi danymi osobowymi ☒ Ograniczenie możliwości realizowania praw z art. 15-22 RODO
Opis środków zastosowanych lub proponowanych przez podmiot przetwarzający w celu zaradzenia naruszeniu, w tym w stosownych przypadkach środków w celu zminimalizowania jego ewentualnych negatywnych skutków	**Działania tuż po incydencie** Podatność w systemie wykorzystana do przeprowadzenia ataku została natychmiast zidentyfikowana i usunięta. Wymusiliśmy zmianę haseł na kontach klientów. Ograniczyliśmy możliwość logowania z nieautoryzowanych adresów IP poza tymi, które zidentyfikowaliśmy jako bezpieczne. Rozszerzyliśmy zakres monitoringu platformy, w szczególności monitoring live ruchu HTTP. Potwierdziliśmy brak naruszenia integralności danych klientów. Serwery zostały przeskanowane pod względem obecności złośliwego oprogramowania. **Działania w trakcie i na przyszłość** Wdrożenie w systemie funkcjonalności umożliwiające anonimizację danych według indywidualnych parametrów (zakres, czas) per konto użytkownika. Wdrożenie systemu SIEM (security information and event management) dla wszystkich podsystemów usługi. Rozszerzenie i uszczegółowienie reguł systemu WAF (Web Application Firewall) Wdrożenie NIPS/NIDS (Network Intrusion Prevention / Detection System) do monitorowania ruchu sieciowego. Przeprowadzenie dodatkowych testów penetracyjnych systemu przez zewnętrzny i niezależny podmiot, który zakończy się uzyskaniem certyfikatu bezpieczeństwa. Przeprowadzenie sesji lessons learned oraz wprowadzenie modyfikacji do procedur bezpieczeństwa wynikających z zaistniałego incydentu. Przeprowadzenie szkolenia z zakresu nowych procedur bezpieczeństwa dla pracowników.
Czy stwierdzono działanie złośliwego oprogramowania	nie
Przyczyna zdarzenia	zewnętrzne działanie zamierzone (atak hakerski)
Charakter zdarzenia	naruszenie poufności danych
Czy podane informacje stanowią wszystkie informacje, które dotyczą naruszenia ochrony danych osobowych?	• W zakresie danych administrowanych przez Spółkę - tak • W zakresie danych powierzonych do przetwarzania - informacje zostały udostępnione w panelu klienta oraz dodatkowe informacje zostały wysłane drogą e-mail.
Możliwe skutki naruszenia ochrony danych osobowych	• Kierowanie do Państwa wiadomości SMS, email, zawierających informacje handlowe, na które nie wyrazili Państwo zgody; • Podszycie się pod inną osobę lub instytucję w celu wyłudzenia od Państwa dodatkowych określonych informacji (np. danych do logowania)
Zalecane środki ostrożności	Zgodnie z zaleceniami ogólnymi: https://www.gov.pl/web/baza-wiedzy/jak-chronic-sie-przed-atakami-cyberprzestepcow https://it-szkola.edu.pl/publikacje,plik,90
O zaistniałym zdarzeniu poinformowaliśmy	Urząd Ochrony Danych Osobowych, Prokuraturę, Centralne Biuro Zwalczania Cyberprzestępczości
Zabezpieczono i przekazano odpowiednim służbom	Szczegółowy opis oraz logi dotyczące zdarzenia.