**27 milionów kont Ticketfly naruszonych przez wyciek danych**

**Po tym jak strona internetowa Ticketfly została zdjęta z sieci z powodu cyberincydentu, firma wystosowała oświadczenie, iż ponad 27 milionów kont klientów może być zagrożonych. Ticketfly wciąż ocenia rozmiar zniszczeń, ale strona już działa, po tym jak została całkowicie zamknięta na parę dni.**

Prawdopodobnym jest, iż do wycieku doszło przez stronę dot. planowania wydarzeń zakupioną przez Eventride od firmy Pandora w 2017. Odwołując się do wiadomości hakera, słabym punktem infrastruktury był fakt, iż strona jest oparta na WordPressie.

„Zawsze dobrym pomysłem w przypadku WordPressa jest przestrzeganie zaleceń dotyczących bezpieczeństwa pochodzących z oficjalnej strony WordPressa lub wdrożenie dwuskładnikowego uwierzytelnienia”, komentuje Mariusz Politowicz, inżynier techniczny Bitdefender z firmy Marken

podatność WordPressa na atak została już wykorzystana przez hakerów wielokrotnie, a tutaj mamy kolejny poważny przypadek.” -dodaje.

Informacje o płatnościach i hasła nie były narażone na niepowołany dostęp podczas ataku, ale Ticketfly przyznało, że hashowane hasła i konta promotorów mogły zostać naruszone. Wprowadzając obowiązkowy reset hasła dostępu, firma ma nadzieję, że uchroni swoich klientów od kradzieży i naruszeń.

Do danych, jakie wyciekły, zalicza się adresy email, numery telefonów, adresy zamieszkania oraz adresy rozliczeniowe.

„Po konsultacjach ze stronę trzecią tj. niezależnymi ekspertami ds. cyberbezpieczeństwa możemy potwierdzić, że nie doszło do wycieku danych kart kredytowych i debetowych”, pisze firma na swoim blogu. „Mimo tego, że dane takie jak nazwiska, adresy i numery telefonów związane z 27 milionami kont Ticketfly, narażone były na niepowołany dostęp, należy zauważyć, iż wiele ludzi kupuje bilety z kilku kont naraz, więc liczba poszkodowanych jest trochę mniejsza.”

Podczas gdy wciąż jest niejasne, czy firma naprawiła lukę bezpieczeństwa, która spowodowała wyciek danych, Ticketfly zapewnia, że wciąż pracuje nad przywróceniem online wszystkich swoich usług. Ci, którzy ucierpieli w wyniku wycieku kierowani są na stronę FAQ po więcej informacji.

źródło: Bitdefender