**Wyciekły dane 9,4 mln klientów linii lotniczych Hong Kong Airlines**

**Cathay Pacific, właściciel linii lotniczych Hong Kong Airlines, w oficjalnym komunikacie prasowym oświadczył, że odkryto nieautoryzowany dostęp do danych 9,4 miliona pasażerów, w tym do nazwisk, narodowości, numerów telefonów, adresów email, adresów pocztowych, numerów paszportów, numerów dowodów tożsamości i innych.**

W wydanym oświadczeniu możemy przeczytać: „Jesteśmy świadomi nieautoryzowanego dostępu do danych około 9,4 miliona pasażerów. Nie ma jednak żadnych dowodów na to, że dane te zostały przez przestępców w jakikolwiek sposób wykorzystane. Systemy informatyczne obsługujące rezerwację i sprzedaż biletów, które zostały spenetrowane przez hakerów, są całkowicie odizolowane od systemów realizujących obsługę lotów. Naruszenie nie ma żadnego wpływu na bezpieczeństwo podróżnych”.

Nie podano szczegółów technicznych dotyczących przeprowadzonego ataku. Wiadomo jedynie, że naruszenie zaobserwowano już w marcu 2018 roku. Lukę wykorzystaną przez hakerów natychmiast załatano. Wszczęto też oficjalne dochodzenie. Nie zmienia to jednak faktu, że dane klientów były dostępne dla przestępców i mogą zostać przez nich wykorzystane.

Przestępcy, poza danymi osobowymi, uzyskali też dostęp do 403 numerów nieaktywnych kart kredytowych oraz 27 kart aktywnych, jednak bez numerów CVV. Nie uzyskali natomiast dostępu do haseł klientów. Jest to o tyle istotne, że znajomość haseł otworzyłaby im furtkę do kolejnych usług, z których korzystają klienciHong Kong Airlines (mało kto używa innego hasła do każdej usługi). Wykradzione dane mogą jednak z powodzeniem zostać użyte przez przestępców w atakach phishingowych oraz do wyłudzeń finansowych.

Przedstawiciele Cathay Pacific kontaktują się obecnie z poszkodowanymi, informując o naruszeniu. Linie zwróciły się również o pomoc do policji i władz Hongkongu, prosząc o przeprowadzenie śledztwa i ustalenie, kto stoi za atakiem.

*„Warto zwrócić uwagę, że Cathay Pacific czekał z publicznym ujawnieniem informacji o wycieku aż pięć miesięcy. Zaniedbanie to spowoduje prawdopodobnie konieczność zapłacenia przez linie bardzo wysokiej kary, ustalanej zgodnie z prawem zachodnim”* *komentuje Dariusz Woźniak, inżynier techniczny Bitdefender z firmy Marken.*