

DANE 14 MILIONÓW UŻYTKOWNIKÓW KEY RING W SIECI. BŁĄD ZABEZPIECZEŃ?

Dane na temat 14 mln użytkowników Key Ring wyciekły do Internetu. Aplikacja służy między innymi do przechowywania zeskanowanych kart lojalnościowych oraz członkowskich do klubów konsumenckich na urządzeniu.

Key Ring często bywa wykorzystywany również jako sposób przechowywania cyfrowych kopii dokumentów tożsamości, na przykład prawa jazdy czy dowodu osobistego, a także kart płatniczych.

Wyciek z aplikacji objął 44 mln plików zdjęciowych, które znajdowały się w nieprawidłowo zabezpieczonym klastrze chmury AWS S3 Amazonu. Wśród informacji, których bezpieczeństwo naruszono, znajdowały się między innymi kopie oficjalnych dokumentów tożsamości, skany kart płatniczych wraz z ich kodami zabezpieczającymi, a także karty ubezpieczenia medycznego osób mieszkających w USA.

W wycieku ujawnionym przez firmę vpnMentor naruszono również bezpieczeństwo plików CSV zawierających informacje na temat osób partycypujących w programach lojalnościowych dużych sieci handlowych działających na terenie Ameryki Północnej, które korzystały z aplikacji Key Ring jako platformy marketingowej. To między innymi Walmart, Kleenex, La Madeleine, Foot Locker i Mattel.

Według ekspertów, którzy odkryli niezabezpieczone pliki Key Ring w Internecie, można było je w dowolnym momencie pobrać i zapisać na własnym dysku, co sprawia że śledzenie wszystkich kopii danych staje się niemożliwe. "To żyła złota dla cyberprzestępców" - ocenili badacze. "Przez ten wyciek miliony mieszkańców Ameryki Północnej zostały narażone na różne formy ataków oraz nadużyć". Jak dodali przedstawiciele vpnMentor, po odkryciu wycieku danych od razu poinformowali na ten temat producenta aplikacji Key Ring.

Czytaj też: [Wyciek danych z Amazon i eBay. Miliony osób poszkodowanych](#)