Warszawa, 28.04.2025 r.

Zagrożenia związane z przechowywaniem danych w chmurze na przykładzie incydentu w Volkswagenie

W grudniu 2024 roku spółka zależna Volkswagena, **Cariad**, specjalizująca się w oprogramowaniu, doświadczyła **poważnego incydentu naruszenia ochrony danych osobowych**, w ramach którego niechronione dane około **800 000 pojazdów elektrycznych** przez kilka miesięcy były publicznie dostępne w zasobach chmury Amazon Web Services (AWS).

Do naruszenia doszło w wyniku **niewłaściwej konfiguracji ustawień przechowywania danych w chmurze**, co umożliwiło **nieuprawniony dostęp** do danych, w tym:

- szczegółowych danych geolokalizacyjnych (GPS),
- informacji o statusie pojazdu,
- a prawdopodobnie także danych kontaktowych właścicieli pojazdów.

Ten incydent stanowi kolejny przykład na to, jak nieprawidłowe zarządzanie środowiskami chmurowymi może prowadzić do poważnych naruszeń prywatności i bezpieczeństwa danych. Szczególnie niepokojące jest to, że ujawnione informacje mogły zostać wykorzystane do śledzenia lub identyfikacji konkretnych użytkowników pojazdów.

Zdarzenie to uwidacznia narastające zagrożenia związane z przechowywaniem danych w środowiskach chmurowych, szczególnie w sytuacjach, gdy błędy konfiguracyjne lub niedopatrzenia ludzkie prowadzą do ujawnienia znacznych zasobów danych, narażając je na działania cyberprzestępców.

Z uwagi na istotną rolę Volkswagena w przemyśle motoryzacyjnym oraz rosnące znaczenie technologii pojazdów połączonych, zdarzenie to rodzi **poważne obawy w zakresie zgodności z przepisami RODO, ochrony prywatności oraz odpowiedzialności za naruszenie przepisów o ochronie danych**.

Niemieccy politycy „ofiarami incydentu”

Nadja Weippert to polityk, która pełni funkcję członka Landtagu (parlamentu regionalnego) Dolnej Saksonii, a także jest burmistrzynią miasta Tostedt, położonego między Hamburgiem a Bremą. Dodatkowo pełni rolę rzeczniczki ds. ochrony danych osobowych swojej frakcji. W zeszłym roku, po zakupie nowego samochodu elektrycznego VW ID.3, natychmiast zainstalowała aplikację Volkswagen, która umożliwia użytkownikowi zdalne zarządzanie funkcjami pojazdu, takimi jak podgrzewanie samochodu, sprawdzanie stanu naładowania baterii oraz monitorowanie zasięgu.

Jednak po zainstalowaniu aplikacji, okazało się, że samochód zaczyna zbierać szczegółowe dane na temat codziennej lokalizacji i ruchów Weippert. Po wyłączeniu silnika samochód automatycznie przesyłał dane GPS, które zawierały informacje o dokładnym miejscu postoju pojazdu, co w konsekwencji pozwalało stworzyć dokładny obraz jej codziennych tras, w tym takich miejsc jak ratusz w Tostedt, Landtag Dolnej Saksonii, jej ulubiony sportowy klub czy gabinet fizjoterapeuty.

Dane te były łatwe do zidentyfikowania i śledzenia, co stworzyło poważne zagrożenie dla prywatności Weippert. Polityk była zszokowana, gdy dowiedziała się, że jej dane lokalizacyjne były przechowywane w publicznej chmurze Amazon, dostępnej dla osób nieuprawnionych. W związku z tym wyraziła swoje niezadowolenie, oczekując od Volkswagena, że zaprzestanie zbierania nadmiernej ilości danych oraz wprowadzi odpowiednie mechanizmy ochrony prywatności, w tym anonimowość danych.
Drugim politykiem, który padł ofiarą tego incydentu był Markus Grübel, niemiecki polityk z partii CDU, który pełni funkcję członka Bundestagu oraz zasiada w komisji ds. obrony. W przypadku Grübela jego pojazd również przesyłał szczegółowe dane dotyczące lokalizacji, w tym miejsca, w których regularnie zaparkował – jak np. przed domem opieki, gdzie mieszkał jego starszy ojciec, czy przed budynkami o charakterze wojskowym, z racji pełnionej funkcji w komisji obrony. Podobnie jak w przypadku Weippert, dane te były łatwe do powiązania z jego tożsamością i działalnością, co stwarzało zagrożenie dla jego prywatności.
Grübel, podobnie jak Weippert, uznał wyciek danych za skandaliczny i wyraził swoje niezadowolenie, stwierdzając, że cała sytuacja wzmacnia negatywne postrzeganie niemieckiej branży motoryzacyjnej, zwłaszcza w kontekście rozwoju autonomicznych pojazdów, które będą zależne od zbierania danych. Polityk podkreślił, że konieczne jest znaczące podniesienie standardów bezpieczeństwa danych w branży motoryzacyjnej, by uniknąć przyszłych wycieków i manipulacji.

Cariad mówi o „błędnej konfiguracji”

Cariad - firma odpowiedzialna za incydent poinformowała magazyn SPIEGEL[1], że „pseudonimizowane dane dotyczące zachowań i przyzwyczajeń klientów w zakresie ładowania akumulatorów” zostaną wykorzystane do udoskonalenia baterii i powiązanego z nimi oprogramowania. Cariad podkreśla, że dane w ramach grupy nigdy nie są łączone w sposób, który „umożliwiałby identyfikację osób lub tworzenie profili ruchu”.
Firmie, która skompromitowała te dane (Chaos Computer Club, dalej: CCC) udało się to zrobić jedynie poprzez „ominięcie kilku mechanizmów bezpieczeństwa”, co „wymagało wysokiego stopnia wiedzy specjalistycznej i znacznej ilości czasu, a także poprzez połączenie różnych zestawów danych”. Zamiast mówić o luce w zabezpieczeniach, firma woli mówić o „błędnej konfiguracji”. Analiza incydentu wskazała, że „według obecnej wiedzy nikt inny poza CCC nie miał dostępu do systemów i nie mamy żadnych przesłanek wskazujących na niewłaściwe wykorzystanie danych przez osoby trzecie”.
Cariad tłumaczył: „Nie ma potrzeby podejmowania jakichkolwiek działań ze strony klientów, ponieważ żadne poufne informacje, takie jak hasła lub dane dotyczące płatności, nie są naruszane”.

Zagrożenia związane z przechowywaniem danych w chmurze

Przechowywanie danych w chmurze staje się standardem, oferując elastyczność i skalowalność. Jednakże, jak pokazuje przypadek Volkswagena, nawet niewielki błąd

[1] https://www.spiegel.de/netzwelt/web/volkswagen-konzern-datenleck-wir-wissen-wo-dein-auto-steht-a-e12d33d0-97bc-493c-96d1-aa5892861027

konfiguracyjny może skutkować ujawnieniem ogromnych ilości danych osobowych. Do najczęstszych przyczyn takich incydentów należą:

- **brak odpowiedniej kontroli dostępu,**
- **przechowywanie danych w formie niezaszyfrowanej,**
- **brak ciągłego monitorowania i testowania środowiska chmurowego,**
- **nieodpowiednia ocena dostawców usług (np. AWS).**

Mimo wielu zalet, przechowywanie danych w chmurze niesie poważne wyzwania związane z bezpieczeństwem i prywatnością. Ryzyko wycieków danych, nieautoryzowanego dostępu czy błędów konfiguracyjnych można jednak znacząco ograniczyć, stosując odpowiednie środki ostrożności. Do dobrych praktyk należą m.in.: szyfrowanie danych w spoczynku i w trakcie przesyłania, segmentacja dostępów (zasada najmniejszych uprawnień), regularne audyty bezpieczeństwa, testy penetracyjne, korzystanie z zaufanych dostawców chmurowych zgodnych z międzynarodowymi standardami (np. ISO/IEC 27001), a także monitorowanie logów i alertów w czasie rzeczywistym.

W kontekście RODO organizacje przechowujące dane w chmurze mają szereg obowiązków. Należy do nich przede wszystkim zapewnienie, że przetwarzanie danych odbywa się w sposób zgodny z prawem, rzetelny i przejrzysty wobec osób, których dane dotyczą. Administratorzy danych muszą zawrzeć odpowiednie umowy powierzenia przetwarzania z dostawcami usług chmurowych oraz zapewnić, że dane nie są przesyłane do krajów trzecich bez odpowiednich zabezpieczeń. Kluczowe jest również wdrażanie zasady privacy by design i privacy by default – czyli projektowania systemów z myślą o prywatności od samego początku i ograniczania przetwarzania danych do niezbędnego minimum.

Incydenty tego typu miały miejsce również u innych dużych podmiotów, takich jak Alibaba czy AT&T, pokazując, że skala i renoma firmy nie gwarantują automatycznej zgodności z zasadami ochrony danych.

Nieodosobniony przypadek – inne incydenty chmurowe:

Nie jest to przypadek odosobniony – podobne incydenty związane z bezpieczeństwem danych w chmurze miały już wcześniej miejsce na dużą skalę. W lipcu 2022 roku błędna konfiguracja bazy danych w chmurze Alibaba doprowadziła do ujawnienia danych osobowych ponad miliarda chińskich obywateli. Z kolei w styczniu 2023 roku w wyniku błędu jednego z podwykonawców AT&T[2], dane 109 milionów użytkowników – w tym historia połączeń i wiadomości SMS – stały się publicznie dostępne. Te przypadki jasno pokazują, jak niezwykle ważne jest stosowanie rygorystycznych środków bezpieczeństwa przy korzystaniu z technologii chmurowych. Nawet pozornie drobne uchybienie może prowadzić do masowego naruszenia danych i poważnych konsekwencji dla firm oraz użytkowników.

[2] https://www.bleepingcomputer.com/news/security/massive-atandt-data-breach-exposes-call-logs-of-109-million-customers/

Implikacje prawne wynikające z RODO – Czy Volkswagen mógł zrobić coś nieprawidłowo?

Zgodnie z Rozporządzeniem (UE) 2016/679 (RODO), administratorzy danych są zobowiązani do spełniania szeregu wymogów. W omawianym przypadku Volkswagen mógł naruszyć co najmniej następujące obowiązki:

- **Brak odpowiednich środków technicznych i organizacyjnych** → Naruszenie art. 5 ust. 1 lit. f oraz art. 32 RODO, mówiących o obowiązku zapewnienia bezpieczeństwa przetwarzanych danych.
- **Naruszenie zasady minimalizacji danych oraz ograniczenia celu** → Volkswagen mógł przechowywać nadmiarowe dane osobowe, nieadekwatne do celów, dla których zostały zebrane – naruszenie art. 5 ust. 1 lit. c i b RODO.
- **Brak należytej staranności w ocenie ryzyka związanego z podmiotem przetwarzającym (AWS)** → Możliwe naruszenie art. 28 RODO w zakresie wyboru i nadzoru nad podmiotem przetwarzającym dane.
- **Niedopełnienie obowiązku zgłoszenia naruszenia** → Zgodnie z art. 33 i 34 RODO, naruszenie bezpieczeństwa danych musi być zgłoszone organowi nadzorczemu oraz osobom, których dane dotyczą – w ciągu 72 godzin.
- **Brak zastosowania zasady „privacy by design”** (ochrona danych w fazie projektowania) → Artykuł 25 RODO zobowiązuje administratora do wdrażania odpowiednich środków technicznych już na etapie projektowania systemu. Błędnie skonfigurowany serwer w chmurze stanowi rażące naruszenie tej zasady.

Inni producenci również mają problemy z bezpieczeństwem IT

VolksWagen z pewnością nie jest jedynym producentem samochodów, który ma poważne problemy z bezpieczeństwem przetwarzanych danych:

- W styczniu 2023 roku zespół pod przewodnictwem 23-letniego wówczas hakera Sama Curry'ego z Omaha w stanie Nebraska pokazał, jak można włamać się na każde konto użytkownika, pracownika lub dealera BMW, i przejrzeć dokumenty sprzedaży.
- Jeszcze poważniejsze okazały się luki w zabezpieczeniach, jakie odkryli hakerzy w firmie KIA: udało im się zdalnie odblokować, a nawet uruchomić pojazdy tego południowokoreańskiego producenta. Na szczęście Curry i jego zespół byli tzw. hakerami w białych kapeluszach, którzy działali w ten sam sposób, w jaki zrobił to Chaos Computer Club w przypadku Cariad – z wyprzedzeniem poinformowali dotknięte atakiem firmy, dzięki czemu luki zostały usunięte.

Podsumowanie

Technologia, w tym rozwój pojazdów elektrycznych i powiązanych aplikacji, niewątpliwie przynosi wiele korzyści, takich jak wygoda, automatyzacja i poprawa efektywności. Systemy zdalnego zarządzania pojazdami umożliwiają użytkownikom kontrolowanie wielu funkcji pojazdu z poziomu telefonu, co staje się normą w nowoczesnych samochodach. Jednak, jak pokazuje przypadek Volkswagena i niemieckich polityków wskazanych powyżej, rozwój technologii wiąże się z koniecznością szczególnej dbałości o bezpieczeństwo danych użytkowników.

Każdy nowoczesny system zbiera ogromne ilości informacji, które mogą obejmować dane osobowe, lokalizacyjne czy inne, czasami wrażliwe informacje. Bez odpowiednich środków ochrony te dane mogą zostać łatwo narażone na wyciek, a ich wykorzystanie przez nieuprawnione osoby może prowadzić do poważnych konsekwencji – nie tylko w kontekście naruszenia prywatności, ale także ryzyka karnych lub administracyjnych sankcji.
W obliczu takich zagrożeń kluczowe jest, aby producenci technologii, w tym motoryzacyjnych, wprowadzali odpowiednie środki zabezpieczające i dbali o transparentność swoich działań. Z kolei użytkownicy powinni być świadomi zagrożeń i odpowiedzialnie podchodzić do zarządzania swoimi danymi. Zrównoważony rozwój technologii powinien iść w parze z rozwojem praktyk związanych z ochroną prywatności, aby uniknąć zarówno potencjalnych kompromitacji, jak i wysokich kar administracyjnych.
Incydent, omawiany w tym artykule, powinien być traktowany jako przestroga dla wszystkich podmiotów korzystających z rozwiązań chmurowych. Zabezpieczenie danych klientów to nie tylko obowiązek prawny, ale również element budowania zaufania i reputacji firmy w erze cyfrowej.

Nina Zacharska - specjalistka ds. ochrony danych osobowych w iSecure Sp. z o.o.