**Uber ukarany grzywną 492 tys. USD. Gdyby naruszenie nastąpiło po 25 maja tego roku, kara wyniosłaby blisko 100 mln USD**

**Dwa lata temu w wyniku naruszenia infrastruktury IT Ubera wyciekły dane osobowe 2,7 mln klientów z Wielkiej Brytanii. Brytyjski organ nadzorczy ICO (ang. Information Commissioner's Office) – odpowiednik polskiego GIODO – w ostatnich dniach poinformował na swojej stronie internetowej o nałożeniu grzywny w wysokości 492 mln USD.**

**Brytyjski organ nadzorczy ICO (ang. Information Commissioner's Office) – odpowiednik polskiego GIODO – w ostatnich dniach poinformował na swojej stronie internetowej o nałożeniu grzywny w wysokości 492 mln USD.**

W oficjalnym [komunikacie](https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/11/ico-fines-uber-385-000-over-data-protection-failings/) ICO czytamy, że kara za brak należytej ochrony danych osobowych klientów została nałożona na mocy ustawy z 1996 roku. Gdyby naruszenie nastąpiło po 25 maja 2018, kwota byłaby 203 razy większa. Podobną karę na Ubera w wysokości 600 tysięcy euro nałożył holenderski Urząd Ochrony Danych Osobowych (Autoriteit Persoonsgegevens).

Ataku dokonano za pomocą metody nazywanej *credential stuffing*. Polega ona na kradzieży loginów i haseł ze słabo zabezpieczonych serwerów lub kupowaniu ich na czarnym rynku. Zdobyte w ten sposób poświadczenia wykorzystywane są przy zautomatyzowanym, masowym logowaniu do atakowanej usługi.

W efekcie przestępcy wykradli dane osobowe 2,7 miliona klientów oraz informacje dotyczące prawie 82 tys. zarejestrowanych kierowców. Przestępcom udało się uzyskać nieautoryzowany dostęp do imion i nazwisk, adresów email, numerów telefonów, danych nt. przebytej trasy oraz informacji o płatnościach.

W uzasadnieniu ICO zwraca uwagę nie tyle na sam problem kradzieży danych osobowych, co na naganne postepowanie Ubera po ataku. Firma nie poinformowała klientów o naruszeniu i w tajemnicy zapłaciła napastnikom okup za zniszczenie wykradzionych danych. Informacja o ataku została upubliczniona dopiero rok po incydencie, co naraziło osoby korzystające z Ubera na kolejne ataki z wykorzystaniem wykradzionych poświadczeń.

„Uber całkowicie zlekceważył bezpieczeństwo swoich klientów i kierowców, których dane trafiły w ręce przestępców. Nie podjęto żadnych kroków w celu poinformowania poszkodowanych o zagrożeniu oraz nikomu nie udzielono wsparcia. Uber pozostawił swoich klientów bezbronnymi wobec przestępców” – powiedział Steve Eckersley, Dyrektor ds. Dochodzeń w ICO.

„Płacenie przestępcom i zatajanie informacji nt. ataku jest według stanowiska ICO postępowaniem nagannym. Wprawdzie zgodnie z ustawą o ochronie danych osobowych z 1996 roku nie ma obowiązku zgłaszania tego typu incydentów, to jednak uważamy, że postepowanie Ubera narażało jego klientów na poważne niebezpieczeństwo” – kontynuuje Eckersley.

Zgodnie z obowiązującym od 25 maja 2018 r. w Unii Europejskiej Rozporządzeniem o Ochronie Danych Osobowych (GDPR), grzywna wyniosłaby 100 mln USD (4% rocznego obrotu przedsiębiorstwa). Grzywna nałożona na Ubera w wysokości 492 tys. USD to maksymalny wymiar kary według rozporządzenia z 1996 r.

Podobna grzywna została nałożona na Facebook za skandal związany z Cambridge Analytica oraz na amerykańskiego potentata kredytowego, firmę Equifax – ofiarę największego naruszenia w historii, które doprowadziło do wycieku numerów ubezpieczeń społecznych niemal połowy Amerykanów.

*W takiej sytuacji, gdy dane już wyciekły, wszyscy zainteresowani powinni zostać natychmiast poinformowani o naruszeniu i konieczności zmiany haseł i loginów we wszystkich usługach, do których z ich pomocą się logują. Może to zapobiec kradzieży danych z innych serwerów klientów. Brak reakcji firm z pewnością negatywnie wpłynie na opinie użytkowników,* komentuje Dariusz Woźniak, inżynier techniczny Bitdefender z firmy Marken.