Szyfrowanie wiadomości end-to-end nie chroni prywatności

15 stycznia 2025

Mark Zuckerberg, dyrektor generalny Meta, właśnie rzucił nowe światło na kwestię prywatności w komunikatorach internetowych. W trakcie wywiadu w podcaście Joe Rogana przyznał, że nawet najlepsze szyfrowanie wiadomości może okazać się bezsilne w pewnych sytuacjach. To wyznanie pojawiło się w kontekście głośnej sprawy Tuckera Carlsona i jego prób przeprowadzenia wywiadu z Władimirem Putinem.

Zuckerberg szczegółowo wyjaśnił, jak działa szyfrowanie end-to-end w WhatsAppie i innych komunikatorach. Podkreślił, że ta technologia skutecznie uniemożliwia firmie Meta dostęp do treści wiadomości użytkowników – nawet w przypadku włamania do baz danych firmy, prywatne konwersacje pozostają nieczytelne dla intruzów.

Jednak szef Meta zwrócił uwagę na istotną lukę w tym systemie zabezpieczeń. Okazuje się, że szyfrowanie staje się bezużyteczne, gdy ktoś uzyska bezpośredni dostęp do urządzenia użytkownika. „To, co robią [służby], to uzyskują dostęp do twojego telefonu. Wtedy nie ma znaczenia, czy cokolwiek jest zaszyfrowane – mogą po prostu zobaczyć wszystko w jawnej formie" – wyjaśnił Zuckerberg.

W rozmowie wspomniano o zaawansowanych narzędziach szpiegowskich, takich jak Pegasus – oprogramowanie stworzone przez izraelską firmę NSO Group, które może być potajemnie zainstalowane na telefonach komórkowych w celu uzyskania dostępu do danych. To właśnie świadomość takich zagrożeń skłoniła firmę Meta do wprowadzenia funkcji znikających wiadomości, które są automatycznie usuwane po określonym czasie.

Zuckerberg wyjaśnił, że połączenie szyfrowania z funkcją

znikających wiadomości tworzy dodatkową warstwę ochrony. „Jeśli ktoś przejął kontrolę nad twoim telefonem i może widzieć wszystko, co się tam dzieje, oczywiście może zobaczyć wiadomości w momencie ich otrzymania… Dlatego szyfrowanie połączone z automatycznym usuwaniem wiadomości stanowi, moim zdaniem, dobry standard bezpieczeństwa i prywatności” – stwierdził.

Ujawnione informacje nabierają szczególnego znaczenia w świetle dokumentu szkoleniowego FBI z 2021 roku. Według tego dokumentu amerykańskie organy ścigania mogą uzyskać ograniczony dostęp do zaszyfrowanych wiadomości z usług takich jak iMessage, Line czy WhatsApp. Jednocześnie dokument wskazuje, że służby nie mają możliwości dostępu do komunikacji prowadzonej przez platformy takie jak Signal, Telegram, Threema, Viber, WeChat czy Wickr.

Te rewelacje pojawiają się w czasie intensywnej debaty na temat prywatności cyfrowej i nadzoru rządowego. Podczas gdy entuzjaści prywatności chwalą szyfrowanie end-to-end za ochronę danych użytkowników, agencje takie jak CIA i FBI argumentują, że może ono utrudniać walkę z przestępczością i terroryzmem. Dla zwykłych użytkowników oznacza to, że samo korzystanie z szyfrowanych komunikatorów może nie wystarczyć do zapewnienia pełnej prywatności. Równie ważne jest zabezpieczenie swoich urządzeń przed nieautoryzowanym dostępem oraz świadomość, że w niektórych przypadkach służby mogą mieć techniczne możliwości omijania zabezpieczeń.

Źródło: ZmianyNaZiemi.pl