Nowe komunikatory urzędników państwowych Tchap i Olvid

Zgodnie z zarządzeniem francuskiej premier lisabeth Borne członkowie tamtejszego rządu od 8 grudnia br. muszą korzystać z **francuskich komunikatorów Tchap i Olvid**. Pierwszy jest komunikatorem opracowanym dla urzędników państwowych (obecnie ma korzystać z niego 400 tys. oficjeli), a drugi jest dziełem francuskiego start-upu. **Jednocześnie ministrowie będą mieli zakaz korzystania z popularnych narzędzi takich jak Signal, WhatsApp i Telegram.**

Powodem tego mają być potrzeba panowania nad technologiami wykorzystywanymi do wrażliwej komunikacji oraz luki bezpieczeństwa w ogólnodostępnych komunikatorach Z pierwszym argumentem trudno się nie zgodzić. Francja znana jest z dążenia do suwerenności technologicznej i strategicznej autonomii. Dodatkowo Olvid otrzymał certyfikat od francuskiej agencji cyberbezpieczeństwa ANSSI i ma szyfrować end-to-end nie tylko wiadomości, ale i metadane. Natomiast kontrowersyjna jest druga przesłanka związana z lukami bezpieczeństwa z uwagi na to, że rządowe (lub opracowane przez krajowe podmioty) aplikacje też mogą je mieć, zwłaszcza, że Olvid zaliczył wpadkę w tym zakresie zaraz po swojej premierze w 2019 r. (znaleziono błąd w kodzie, który umożliwiał założenie konta każdemu, a nie tylko zdefiniowanym użytkownikom z sektora publicznego). W tym kontekście warto pamiętać, że Signal jest oprogramowaniem open source.

Narzędzia do bezpiecznej komunikacji zostały również wdrożone na potrzeby polskich instytucji publicznych. Dla administracji rządowej i podmiotów Krajowego Systemu Cyberbezpieczeństwa (KSC) na urządzeniach służbowych dostępny jest bezpieczny komunikator oparty o najnowsze trendy kryptograficzne i szyfrowanie end-to-end oraz „postawiony" lokalnie (on-premises). W ramach dotacji Ministerstwa Cyfryzacji dla NASK-PIB uruchomiono system łączności mobilnej SKR-Z umożliwiający przetwarzanie informacji niejawnych do klauzuli „zastrzeżone". Powstał on w oparciu o system CATEL opracowany przez Agencję Bezpieczeństwa Wewnętrznego. Również poprzez dotację MC dla NASK-PIB realizowany jest projekt PCOC, który dotyczy wyposażenia wybranych podmiotów KSC uczestniczących w Połączonym Centrum Operacyjnego Cyberbezpieczeństwa w niezbędne urządzenia i sprzęt ICT. Pozwala to na zbudowanie bezpiecznej komunikacji (w tym niejawnej) pomiędzy instytucjami istotnymi z punktu widzenia bezpieczeństwa państwa. Pamiętajmy także, że wykorzystanie do służbowej komunikacji wyłącznie służbowych urządzeń i kont oraz dopuszczonego przez naszą instytucję oprogramowania jest nie tylko podstawową zasadą cyber higieny, ale może wynikać także z wewnętrznych przepisów naszej organizacji.

Źródła: lePoint, Euractiv, Telepolis, justgeek, PBSG.