SYSTEM PEGASUS. CZY POLSKIE SŁUŻBY WYKORZYSTUJĄ NIELEGALNIE OPROGRAMOWANIE INWIGILUJĄCE?

Sprawa wykrycia w Polsce oprogramowania szpiegowskiego Pegasus stworzonego przez izraelską firmę NSO Group powraca do debaty publicznej. Możliwe nielegalne wykorzystanie oprogramowania przez polskie służby może stanowić jedynie jeden z problemów. Okolicznością wymagającą wyjaśnienia jest również zmiana prawna w kontekście sądownictwa i nakazu uwzględniania dowodów zdobytych w ten sposób – donosi w programie „Czarno na białym" telewizja TVN24.

We wczorajszym programie redaktorzy TVN24 zadali pytanie skierowane m.in. do zastępcy koordynatora służb specjalnych Macieja Wąsika, szefa CBA Ernesta Bejdę o wykorzystanie tego oprogramowania przez polskie służby do pracy operacyjnej. Zarówno Bejda jak i Wąsik stwierdzili w programie, że nie znają tego systemu.

Zgodnie z opinią mecenasa Piotra Schramma, przywołanego w materiale TVN24, jak dotychczas używanie takich systemów (np. Pegasus) było niezgodnie z polskim prawem. Chyba, że taką zgodę wyraził sąd. Oznacza to, że pozyskane za pomocą oprogramowania dane nie mogłyby zostać wykorzystane w sądzie jako dowody w sprawie. Jednak zdaniem mecenasa, przepisy zostały zmienione na tyle, żeby możliwe było wykorzystywanie tych danych w oficjalnym procesie sądowym. Jak informuje TVN24 przepisy zostały zmienione tak, że przed zmianą Kodeksu postępowania karnego niemożliwe było wykorzystanie dowodów pozyskanych w wyniku czynu zabronionego. Rządzący uchylili zakaz używania dowodów pochodzących z nielegalnego źródła, ale również w wyniku naniesionych zmian zobowiązali sądy do uwzględniania tych dowodów.

System Pegasus budzi spore emocję z uwagi na brak realnej możliwości kontrolowania służb nad wykorzystywaniem systemu do inwigilowania wybranych jednostek. System ten nie wymaga zaangażowania telekomów ani dostawców Internetu. Zgodnie z przepisami do wykorzystania podsłuchów przez służby wymagana jest zgoda sądu. Jednak z braku możliwości kontroli obywatele muszą liczyć jedynie na uczciwość szefów służb.

Były oficer służb specjalnych, na którego wypowiedz powołuje się TVN24, stwierdził, że w Polsce „nie ma takiej kontroli".

Co wiemy o oprogramowaniu Pegasus? Przypominamy wcześniejsze doniesienia

Jak donosił we wrześniu ubiegłego roku PAP, oprogramowanie szpiegowskie Pegasus stworzone przez izraelską firmę NSO Group zostało wykryte w 45 krajach, w tym w Polsce. Lokalny operator Pegasusa, działający na terenie naszego kraju, występuje pod kryptonimem "ORZELBIALY" i z pomocą programu podszywa się pod domeny firm telekomunikacyjnych. O systemie poinformowała jako pierwsza w raporcie organizacja Citizen Lab (Uniwersytet Toronto w Kanadzie). W opinii organizacji Pegasus jest

skutecznym narzędziem umożliwiającym zdobycie dostępu do dowolnego urządzenia nienależnie czy pracuje na systemie Android czy iOS. Zdaniem ekspertów oprogramowanie może być wykorzystywane poprzez użycie wbudowanego w telefon aparatu fotograficznego i podsłuchiwania przez mikrofon urządzenia, a także wykradania dokumentów i treści przesyłanych przez sieć komórkową wiadomości.

Raport, na który powoływał się PAP wskazał na pięciu operatorów oprogramowania Pegasus działających w Europie. W opinii autorów raportu ich działania były skupione na celach zlokalizowanych na terenie Polski, Szwajcarii, Łotwy, Węgier i Chorwacji. Zgodnie z informacjami przekazanymi w raporcie działania prowadzone były od listopada 2017 roku a Operator "ORZELBIALY" z wykorzystaniem Pegasusa prowadził operacje względem łączności zapewnianej przez takie firmy, jak Polkomtel, FIBERLINK, Orange, T-Mobile, PROSAT, a także Netia i Vectra.

Natomiast przed niespełna dwoma miesiącami w lipcu 2019 roku "Financial Times" donosił, że oprogramowanie zostało zaktualizowane. Uzupełniono również system o nowe funkcjonalności, umożliwiające pobieranie danych również z chmury połączonej z usługami właściciela telefonu. Dziennik wskazywał również, że aktualizacja umożliwiała pozyskanie danych takich jak historia lokalizacji, zarchiwizowane wiadomości tekstowe oraz rozmowy z komunikatorów i zdjęcia. Nowe funkcje Pegasusa, zgodnie z doniesieniami, miały działać w oparciu o skopiowane mechanizmy uwierzytelniania usług takich jak m.in. Google Drive, Messenger Facebooka czy chmura iCloud Apple'a.

Jak podkreślał ówcześnie Łukasz Olejnik, system Pegasus działa na zasadzie przełamywania zabezpieczeń smartfonów z Androidem i systemem iOS, które umożliwiały przechwytywanie haseł, dokumentów i treści przesyłanych wiadomości. Pozwalało również na monitorowanie otoczenia urządzenia z użyciem kamery i mikrofonu. Jak podkreślił ekspert wykorzystanie systemu jest „stosunkowo proste i nie wymaga wiedzy technicznej”.

Financial Times wskazywał również, powołując się na komentarz izraelskiego producenta oprogramowania, że technologia sprzedawana jest jedynie odpowiedzialnym rządom państw, które działają na rzecz zapobiegania atakom terrorystycznym i innym aktom przestępczym. Jednak jak twierdził dziennik, Pegasus był wcześniej wykryty przez badaczy cyberbezpieczństwa m.in. w telefonach aktywistów broniących praw człowieka i dziennikarzy z całego świata, co kłoci się z oficjalnym przekazem firmy.

Sprawa wykorzystania oprogramowania przez polskie służby oraz wymijające wypowiedzi osób odpowiedzialnych za koordynacje służb po raz kolejny wzbudziły kontrowersję. Problem stanowi nie tylko legalność stosowanych przez polskie służby działań, ale również brak realnej kontroli nad nimi w kontekście stosowanych środków oraz możliwość wykorzystania w sądzie dowodów zdobytych w sposób nielegalny.