BARTOSIEWICZ: BEZPIECZNY SMARTFON DLA WOJSKA I SŁUŻB WYMAGA ODWAGI DECYDENTÓW [OPINIA]

Bezpieczeństwo informacji musi być uwzględnione już na etapie tworzenia architektury nowego telefonu komórkowego. Inaczej nie będzie możliwe zaprojektowanie prawdziwie zabezpieczonego urządzenia – pisze w artykule Adam Bartosiewicz, wiceprezes Grupy WB.

6 maja 2020 roku prezydent Federacji Rosyjskiej podpisał dekret zakazujący żołnierzom posiadania urządzeń elektronicznych zdolnych do nagrywania lub przesyłania geolokalizacji, a także nagrywania materiałów audiowizualnych. To między innymi efekt artykułu opublikowanego w „*The Barents Observer*", dotyczącego działań rosyjskich żołnierzy na terenie Ukrainy. Zostali zidentyfikowani na podstawie fotografii opublikowanych w popularnym serwisie społecznościowym.

To jednak problem powszechny i dotyczy wszystkich użytkowników smartfonów. W tym również członków amerykańskich sił zbrojnych, podobnych w swej nonszalancji do żołnierzy rosyjskich. Ba, podobnie postępuje wielu polityków i przedstawicieli świata biznesu.

Czy rozwiązaniem problemu w Rosji stanie się jeden dekret prohibicyjny prezydenta Władimira Putina? Nikt chyba w to nie uwierzy. Nie położy on też kresu wszystkim zagrożeniom związanym z używaniem telefonów komórkowych w rosyjskim wojsku.

Ograniczenia smartfonów

Szczęśliwie, nie cały świat jest zbudowany na dekretach i podobnych rozwiązaniach siłowych. Występuje w nim jeszcze element wolnej woli, choć niestety w tej dziedzinie również nie opartej na wiedzy, ale na marketingu. To reklamy spowodowały, że nie wyobrażamy sobie życia bez smartfonów. Co gorsza, telefon komórkowe są wykorzystywane do wielu czynności, w których się nie sprawdzają, bo nie do nich zostały zaprojektowane.

Smartfony nie nadają się do wykonywania jakichkolwiek działań związanych z poufnością, a ogólniej z bezpieczeństwem informacji. Nie mogą służyć ani do nawiązywania szyfrowanych rozmów, ani do przesyłania czy nawet przechowywania frywolnych zdjęć. Nie powinny być używane do wykonywania płatności, ani do rządzenia państwem. I to nawet, gdy wykorzystywane są teoretycznie „bezpieczne" komunikatory, aplikacje szyfrujące i uwierzytelniające, rozwiązania biometryczne, czy klauzulowane systemy.

Wszystko widzi i słyszy

Dekret poruszył dosyć powierzchownie problem zagrożeń związanych z wykorzystaniem smartfonów. Tak naprawdę to dotknął tylko jednego aspektu – niewłaściwego użytkowania urządzeń. Ale to nie

jedno niebezpieczeństwo.

Wystarczy telefon komórkowy – i nie musi być przy tym włączony, aby możliwy był podsłuch i podgląd otoczenia. Co więcej, w takiej sytuacji możliwe jest umieszczenie na urządzeniu niechcianych treści, wysłanie w imieniu właściciela SMS-a lub e-maila, jego zlokalizowanie w systemach Glonass, Galileo, GPS, COMPASS/BeiDou-2, a nawet bez nich. Można przejąć z niego dane, wykonać fałszywy przelew, zastosować telefon do „kopania" BitCoinów, a nawet użyć go do ataku DDoS.

Można założyć, że wszystko co znalazło się w zasięgu „słuchu i wzroku" smartfonu, o ile tylko ma on naładowaną baterię, może w każdej chwili stać się wiedzą publiczną. Jest to tylko problem kosztu pozyskania, zazwyczaj niezbyt wielkiego. Zwykły użytkownik nie ma się jednak czego specjalnie obawiać, raczej nie stanie się celem ataku, wyjąwszy oczywiście transakcje finansowe.

Grzechy telefonów

Negatywna ocena smartfonów związana jest z tym, że bezpieczeństwo informacji zostało w nich potraktowane jako funkcja pomocnicza. Grzechem głównym jest, że służby nie wyobrażają sobie, aby nie mogły przeciwdziałać przestępstwom, których głównym narzędziem jest oczywiście smartfon. Nie pomaga nawet tłumaczenie, że każdy backdoor, nawet najbardziej prawomyślny, na pewno zostanie wykorzystany niezgodnie z jego przeznaczeniem.

Do grzechu głównego można dodać dwa pomniejsze. Należy do nich wprowadzanie nieodpowiednio zabezpieczonych funkcji serwisowych, czyli *de facto* intencjonalnych backdoorów. Do tego dochodzą pospolite błędy implementacyjne, wynikające z wyższości parametru *time-to-market* (czyli okresu od powstania koncepcji produktu do wprowadzenia go na rynek, dzisiaj wszyscy starają się go maksymalnie skrócić) nad *solution quality* (czyli skupieniu się na jakości rozwiązań).

Niedawny casus afery Roca udowodnił, że jeżeli chodzi o bezpieczeństwo informacji, nie ma godnych zaufania organizacji – ani komercyjnych, ani państwowych. Można ufać tylko sobie, mając jednak świadomość własnych niedoskonałości i stosując odpowiednie środki minimalizujące związane z tym ryzyka.

Dla wojska i służb

Smartfony są nosicielami supertechnologii telekomunikacyjnych, otwierających przez nimi nowe dziedziny zastosowań, w tym w siłach zbrojnych czy formacjach mundurowych. Na wielu polach mają istotne przewagi nad powszechnie stosowanymi radiostacjami.

Konieczne jest jednak uwzględnienie przy ich projektowaniu zabezpieczeń nie tylko dla poufności informacji. Należy zwracać uwagę także na funkcjonalność, co umożliwi żołnierzowi przetrwanie na polu walki. Trzeba zabezpieczyć urządzenie przed atakami poprzez eter i w sieci szkieletowej.

Może to zaskakujące, ale doświadczenia z konfliktów w Syrii i na Ukrainie wykazały wiele pozytywnych cech smartfonów, nawet tych standardowych. Wystarczy przytoczyć znane radiooperatorom zdanie „*widzę cię, ale nie słyszę*", aby zrozumieć główną przewagę telefonów komórkowych nad radiostacjami. Poza pozytywnymi, są również doświadczenia negatywne, ukazujące jak powinien zostać przekonstruowany smartfon, aby spełnić wymagania militarne.

Projekt od podstaw

Bezpieczeństwo informacji musi być uwzględnione już na etapie tworzenia architektury nowego telefonu komórkowego. Inaczej nie będzie możliwe zaprojektowanie prawdziwie zabezpieczonego urządzenia. Konstrukcyjnie bezpieczny smartfon powinien mieć ścisłą separację chronionej informacji

od niezaufanego otoczenia. Musi charakteryzować się odpornością na ataki omijające zabezpieczenia kryptograficzne, mieć poprawnie zaimplementowane funkcję kryptograficzne i być zabezpieczony przed zmanipulowaniem.

Odpowiednio zaprojektowane i wytwarzane telefony komórkowe mogą stać się platformami do rzeczywiście bezpiecznego dokonywania zdalnych operacji, jak transmisje video i głosu, podpis cyfrowy, uwierzytelnienie i autoryzacja. Ich produkcja masowa nie musi być bardziej kosztowna, niż standardowych urządzeń o tej samej odporności na narażenia mechanoklimatyczne.

Bezpieczny smartfon

Inwestycja w projekt i produkcję bezpiecznego smartfonu jest niemała. Jednak, przy pewnych kompromisach projektowych jest ona do zaakceptowania. Na przeszkodzie stoi głównie świadomość decydentów – a raczej jej brak – i zrozumienie potrzeby takiego przedsięwzięcia.

Tymczasem w kręgach specjalistów, zajmujących się bezpieczeństwem informacji i znających dobrze realia komunikacji w Polsce, konieczność posiadania zabezpieczonego smartfonu nie podlega żadnej dyskusji. Ma w dodatku głębokie uzasadnienie biznesowe i to na wielu polach. Kłopot w tym, że bez wsparcia decydentów podjęcie tematu opracowania i wytwarzania bezpiecznego smartfonu jest zbyt ryzykowne. Dowiodła tego historia jedynego opracowanego w Polsce telefonu szyfrującego GSM, modelu Xaos Gamma.

Adam Bartosiewicz, wiceprezes Grupy WB