Defence 24

27.05.2020

MUSIAŁ: JAK WYKORZYSTAĆ SIECI KOMÓRKOWE DLA WOJSKA [OPINIA]

Żołnierz powinien otrzymać buty, mundur, karabin i bezpieczną łączność do komunikacji służbowej i prywatnej w czasie pokoju. W domu, w jednostce i na poligonie – pisze Roman Musiał, prezes zarządu spółki MindMade Sp z o.o., należącej do Grupy WB.

Zgodnie z raportem „*Digital 2019*", w ubiegłym roku na świecie było 5,11 miliarda użytkowników telefonów komórkowych. Banałem jest sformułowanie, że smartfon stał się immanentnym elementem ludzkiego życia. Jednocześnie to życie może być nieustannie podglądane, właśnie dlatego, że powszechnie korzysta się z telefonów komórkowych. A jednak ludzie żyją ze świadomością jednego i drugiego, ale robią bardzo niewiele, aby zabezpieczyć się przed negatywnymi skutkami.

Zagrożenie

Narażenie na penetrację życia prywatnego stanowi zasadniczo problem dla konkretnej osoby, a nieupoważniony dostęp do danych należących do przedsiębiorstwa naraża je na ryzyko lub stratę finansową, do upadłości włącznie. Gorzej jest w przypadku żołnierzy lub funkcjonariuszy. Przejęcie kontroli nad informacjami z ich telefonów komórkowych może nie tylko spowodować utratę zdrowia lub życia, ale także wywołać poważne zagrożenie dla bezpieczeństwa państwa. Za negatywne skutki użycia smartfonów w pierwszej kolejności odpowiada technika, ale w drugiej sam użytkownik.

Smartfon to urządzenie opracowane po to, aby sprawnie pracowało w sieci komórkowej. W pierwszej kolejności oznacza to bezwzględne wykonywanie jej poleceń. Dlatego podszycie się pod jeden z nadajników sieci jest najprostszym – i obecnie wcale nietrudnym – sposobem, by uzyskać dostęp do wszystkich informacji, które smartfon z nią wymienia. Kolejną, niezwykle skuteczną choć trudniejszą metodą na przejęcie kontroli nad telefonem komórkowym jest zainfekowanie go odpowiednim oprogramowaniem, pozwalającym na penetrację systemu i dostępnych na nim danych.

Czytaj też: Bartosiewicz: Bezpieczny smartfon dla wojska i służb wymaga odwagi decydentów [OPINIA]

Wojsko, służby i komórki

W przypadku stosowania przez żołnierzy i funkcjonariuszy komercyjnych telefonów komórkowych można się zastanowić, po co wojsko i służby z nich korzystają do wymiany wrażliwych danych, skoro i tak kupują skomplikowane systemy łączności radiowej. Z drugiej strony warto pamiętać, że militarna radiołączność jest ograniczona zasięgami i zdolnością do transmisji danych.

Dodatkowo, biorąc pod uwagę kolektywną „inwestycję" ponad pięciu miliardów użytkowników

smartfonów w rozwój sieci komórkowych, to wynik wyścigu w tym obszarze łatwo przewidzieć i jest przesądzony. Oczywiście w czasie wojny specjalizowana łączność radiowa jest koniecznością, zwłaszcza w przypadku konfliktu z przeciwnikiem sprawnie operującym w obszarze wojny elektronicznej i cybernetycznej.

Jednak siły zbrojne istnieją i działają głównie w warunkach pokoju. Wówczas wojskowa radiołączność powinna być ograniczona do minimum. Wszystko po to, aby nie dawać szansy ewentualnemu przeciwnikowi na prowadzenie nasłuchu i rozpoznania technologii oraz procedur. To wymusza zastosowanie innego modelu komunikacji, co więcej – można też zgodzić się na pewnym poziomie na rozluźnienie jej reżimu. Jednocześnie ogromny zasięg i możliwość transmisji gigantycznej liczby danych, to zalety bez których trudno funkcjonować. Przyszłość należy bezdyskusyjnie do masowych sieci komórkowych i pytanie nie brzmi czy, tylko jak?

Roman Musiał, prezes zarządu spółki MindMade Sp z o.o., należącej do Grupy WB.

Specjalistyczne systemy

Odpowiedzią są wyspecjalizowane systemy komunikacji, działające w oparciu o publiczne sieci komórkowe. Przykładem takiego rozwiązania jest Platforma Integracji Komunikacji (PIK) opracowana przez warszawską spółkę MindMade wchodzącą w skład Grupy WB. PIK oparty jest o własny system serwerowy, który umożliwia integrację rożnych systemów radiowych w jedną spójną sieć komunikacji. Platforma jest przy tym zdolna do transmisji danych chronionych kryptograficznie nawet do czterech różnych sieci komórkowych jednocześnie.

PIK to doskonały przykład zapewnienia standardowemu terminalowi radiowemu praktycznie

nieograniczonej, ale wciąż bezpiecznej łączności, dzięki wykorzystaniu sieci komórkowych. Te ostatnie, od standardu 5G, mogą dysponować mechanizmami kategorii *Mission Critical*. Te wspierają działanie służb mundurowych i sił zbrojnych w sytuacjach kryzysu lub przeciążenia sieci.

Smartfony i PIK

W przypadku zagrożeń związanych z telefonami komórkowymi, w ramach Platformy Integracji Komunikacji można na takich urządzeniach zainstalować aplikację PiM (Przyciśnij i Mów)/PoC (Push to talk over Cellular). Dzięki temu smartfon zamienia się w specjalistyczny terminal do łączności w ramach w pełni zarządzalnej grupy użytkowników. Cała komunikacja jest wówczas prowadzona pod przykryciem kryptograficznym, natomiast sam terminal i aplikacja są autoryzowane jednorazowymi kluczami.

Systemy klasy PiM/PoC to kolejny krok w stronę łączności radiowej, polegający na przeniesieniu jej w całości do sieci komórkowych. Coraz powszechniejsze na świecie staje się zastępowanie sieci Tetra takimi rozwiązaniami. Systemy PiM/PoC są już dostępne w ofertach globalnych dostawców technologii radiokomunikacji.

Najsłabsze ogniwo

Wypada tutaj wspomnieć, że najsłabszym ogniwem systemu łączności z reguły bywa człowiek. Ale niejednokrotnie słabość tę wspierają brak mechanizmów bezpieczeństwa, słabo przemyślane procedury, kiepskie szkolenie i wreszcie niedostępność odpowiednich rozwiązań.

Nie trzeba od razu włamywać się telefonów komórkowych należących do wyższych rangą wojskowych lub funkcjonariuszy lub przełamywać zaawansowane zabezpieczenia systemów militarnych. Przy dzisiejszym potencjale analitycznym i powszechnej masowej wymianie informacji, zaskakujące efekty może przynieść *biały wywiad* oparty o same media społecznościowe.

Głośne wypadki prostej analizy zdjęć opublikowanych w sieci (Rosjanie za kołem podbiegunowym) lub nagranych rozmów obsług broni (zestrzelenie pasażerskiego odrzutowca MH17) nie miałyby miejsca, gdyby zastosowano podstawowe środki bezpieczeństwa. Takie mogą obejmować obligatoryjne instalowanie na smartfonach aplikacji uniemożliwiających wykonywanie fotografii w określonych lokalizacjach lub wykorzystanie do rozmów głosowych szyfrowanej aplikacji klasy PiM/PoC.

Bezpieczna sieć komórkowa

Teza, że łączność prowadzona przez żołnierzy i funkcjonariuszy przy użyciu sieci komórkowych stanowi zagrożenie, nie jest prawdziwa. Bowiem to nie sieci komórkowe tworzą niebezpieczeństwo dla komunikacji, ale niewłaściwe przygotowane urządzenie w rękach użytkownika. Oczywiście sprzęt musi być wspierany przez zewnętrzny system, pozwalający na pośredniczenie, rejestrację i nadzór nad bezpieczeństwem całej sieci łączności.

Terminal powinien także umożliwić komunikację prywatną z rodziną, wspierając jednocześnie rutynowe działania użytkownika, w ramach jasno zdefiniowanych procedur bezpieczeństwa (dotyczy to przesyłania fotografii, danych topograficznych i innych). Takie rozwiązania, jak Platforma Integracji Komunikacji tworzą wydzielone, prywatne sieci łączności w publicznych sieciach komórkowych.

Roman Musiał, prezes zarządu spółki MindMade Sp z o.o., należącej do Grupy WB.