**Czy nowy Android zapewni pełne bezpieczeństwo?**

**Google wprowadzi nowy model separacji danych w systemie Android 11, który ma pozwolić na tworzenie np. oddzielnego profilu do pracy na urządzeniach należących do firmy. Funkcja ta ma zwiększyć bezpieczeństwo telefonów z najnowszą wersją systemu operacyjnego Google’a. Eksperci mają jednak co do tego pewne wątpliwości.**

Profil do pracy w nowej wersji Androida ma zapewnić oddzielenie aplikacji i danych firmowych od wszelkich informacji osobistych. To sprawa bezpieczeństwa – podkreślają eksperci. Wg Yaelle’a Harel, specjalisty ds. cyberbezpieczeństwa z firmy Check Point, z jednej strony rozwiązanie to zwiększy ochronę prywatności na urządzeniach należących do firmy, z drugiej strony wprowadzi nowy wektor ataku, ponieważ złośliwe oprogramowanie w profilu prywatnym może nadal wykorzystywać wspólną infrastrukturę i uzyskiwać dostęp do poufnych danych firmowych.

**Segregacja nie usuwa zagrożeń mobilnych**

Jednym ze sposobów zabezpieczenia danych przed przedostaniem się ich w niepowołane ręce, jest segregacja. Nie może jednak zagwarantować bezpieczeństwa naszego urządzenia w przypadku bardziej zaawansowanych ataków hakerskich. Zainstalowane przez hakera złośliwe oprogramowanie w profilu osobistym może korzystać z usług ułatwień dostępu Androida (AAS) i odczytywać poufne dane na ekranie profilu do pracy – zwraca uwagę ekspert Check Pointa. Może pasywnie pobierać wszystko, co wpisuje użytkownik, w tym poświadczenia i hasła, a nawet może udzielić sobie dodatkowych uprawnień bez pomocy użytkownika. Niestety, uprawnienia AAS nie mogą zostać cofnięte przez rozwiązania UEM (Unified Endpoint Management). Ostatecznie tylko zaawansowane rozwiązania bezpieczeństwa dla urządzeń mobilnych zapobiegają złośliwym atakom zarówno w profilu służbowym, jak i osobistym, w tym atakom opartym o AAS.

Ataki typu phishing to kolejny rodzaj zagrożenia, który nadal będzie występować przy segregacji danych w specjalnie stworzonych do tego sejfach. Wektory phishingu mobilnego obejmują firmowe wiadomości e-mail, osobiste wiadomości e-mail, wiadomości SMS, aplikacje do przesyłania wiadomości oraz przeglądanie stron internetowych zarówno w profilu służbowym, jak i osobistym. Złośliwe witryny mogą wykorzystywać luki w przeglądarce, aby uzyskać dostęp do profili służbowych i osobistych, zainstalować złośliwe oprogramowanie na urządzeniu, zmienić jego konfigurację i zdalnie przejąć kontrolę nad całym urządzeniem.

Eksperci cyberbezpieczeństwa wskazują jednoznacznie - dla zapewnienia rzeczywistego bezpieczeństwa, niezbędnym jest zastosowanie usług dedykowanych dla urządzeń mobilnych, takich jak SandBlast Mobile, które może chronić zarówno dane prywatne, jak i dane firmowe oraz egzekwować różne zasady dla każdego z typów danych.