Mobilizing Your Enterprise Securely

Mobile applications introduce new security vulnerabilities. ***Brian Reed****, chief mobility officer for NowSecure, describes the risk landscape and shares key steps to a mobile application security program.*

How have mobile apps and mobile-first strategies changed the government landscape?

The introduction of mobile applications has enabled state and local governments to directly communicate with their constituents and communities and provide services in new ways. Employees are free to work in the field or wherever they need to be. Information is available instantly wherever users are, on the mobile devices they're carrying. Most organizations we work with now are leveraging mobile apps as much as or more than they're leveraging laptops in the field.

What types of attacks are mobile apps vulnerable to?

There are two general types: direct attacks, where the attacker's goal is to breach a system, and surveillance, where cybercriminals harvest data and use it for resale or other nefarious acts. We're finding that too many mobile applications are insecure. They'll allow a bad actor to surveil, monitor and collect data about a user. Or they have insecure network connections, where a bad actor can steal a user ID and password and then use those credentials to attack, steal or commit espionage against backend systems. Some mobile apps leak data such as the user's GPS location, which could be used to track the location of employees. Some applications collect and transmit data to cybercriminals. The list never ends.

What challenges do organizations typically encounter when building a mobile app security program?

The first challenge is education — understanding what mobile app security means; what the risks are; and what tools, techniques and processes should be employed. The second challenge is determining whether to build the program internally or leverage third parties. Setting up your own program and building a security team to do things like continuous testing, penetration testing, security analysis and supply chain risk management is costly and complicated. Most agencies are turning to commercial off-the-shelf packages or managed service providers that scan and vet mobile apps. Doing so provides instant intelligence on what security risks might live in those mobile apps, so organizations can decide whether to allow them.

How can organizations securely mobilize their enterprise?

First, establish a risk policy. Define risks and understand what is secure and insecure from a mobile perspective. Second, provide training as needed to technology and security teams working in this space. Third, leverage commercial software tools to test for risks in new mobile apps that you build or download. Fourth, continuously monitor mobile apps you have already approved to ensure updates haven't introduced new vulnerabilities. You also need a mechanism to educate your organization about phishing and other risks and making the right decisions about which applications are safe to use. Finally, I advise leveraging programs offered by the big carriers — AT&T's FirstNet and Verizon's Frontline, for example — which help organizations vet and deploy secure mobile apps and infrastructure for use in public safety scenarios.

Why has mobile supply chain security become so important?

The SolarWinds and Colonial Pipeline attacks were supply chain attacks. Supply chain attacks occur on mobile apps as well. Organizations must be sure the mobile applications they use and deploy to constituents are safe. Organizations need a thorough testing program to ensure those apps are properly vetted and continuously monitored over time. We're also seeing a need for a software bill of materials, where your app-vetting vendor or services supplier provides an inventory of components used to create an application, so you can track and understand potentially nefarious components.

How does 5G impact mobile app security?

What's exciting about 5G is that it has security controls at the network layer. Some of the most common attack vectors for web and mobile applications are at the network communications layer, where data is transmitted between, say, the mobile application and the back end. With 5G, you can deploy fine-grain security controls at the network level, which prevents bad guys from seeing and harvesting data from insecure network connections. Because 5G's inherent network-level security controls are below the layers that attackers traditionally use, it's substantially harder to do bad things. 5G is like a wrapper around every piece of data that gets transmitted.

NowSecure™

To achieve their mission, intelligence, military and civilian agencies rely on mobile apps and devices.

Secure mobile app vetting, **speed** mobile app deployments & **accelerate** ATO across federal agencies with the **NowSecure Mobile App Supply Chain Solution**.