The dangers that lurk in **mobile apps**

Most agencies are overlooking a significant source of threats to their employees and data

Brian Reed
Chief Mobility Officer, NowSecure

GOVERNMENT EMPLOYEES ARE increasingly reliant on mobile applications to do their jobs. But without formal monitoring programs in place, agencies might be unaware of the risks inherent in commercial and government-built apps. As a result, few agencies are investing resources and time to address this serious problem.

The average mobile device has 60 to 80 apps, representing a huge potential for vulnerabilities at agencies whose employees are using those devices for work. Thousands of apps could be tracking employees or intercepting data.

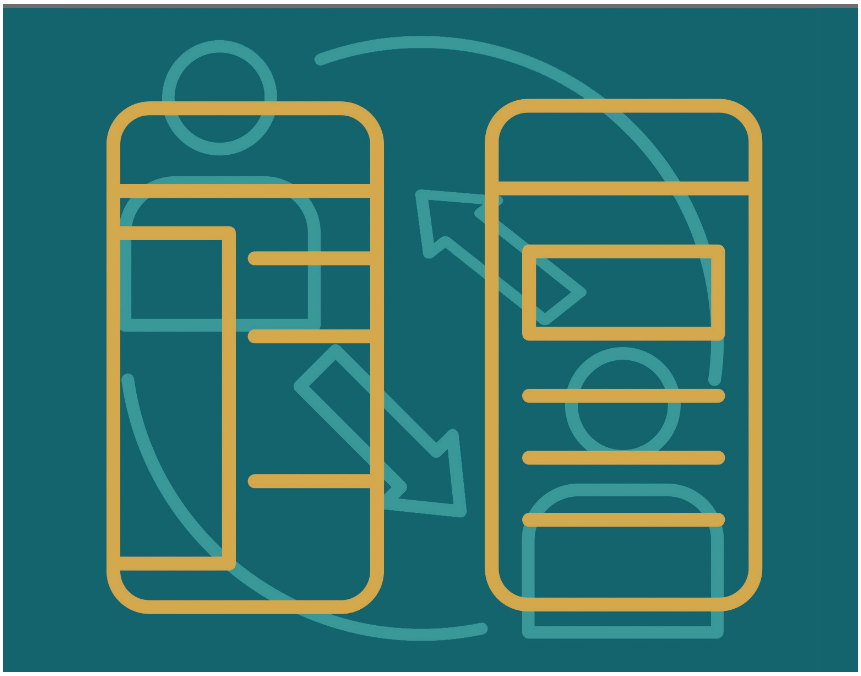
NowSecure founder Andrew Hoog has said "mobile apps are the ultimate surveillance tool, given the mix of personal and mission activities in one space."

Bringing vulnerabilities to light

NowSecure has analyzed millions of mobile apps on the Apple App Store and Google Play and found that about 85% had security vulnerabilities and about 70% handled private data in a manner that could violate multiple agency and industry data-protection requirements.

NowSecure recently reviewed 1,700 apps on employees' phones at one federal agency. We found that 98% had at least one vulnerability, and 22% received a failing grade. Many apps were leaking phone numbers and account numbers and transmitting data to adversarial countries such as Russia and China.

At NowSecure, we're on a mission to help agencies identify and address security vulnerabilities and data leakage issues in their mobile apps.



Protecting app portfolios

First, agencies should commit to securing mobile apps and then define the scale and scope of that commitment. For instance, will personal devices be treated differently from government-furnished equipment (GFE)? And will there be different sets of rules for employee-chosen versus agency-chosen mobile apps?

Next, agencies need to outline mission data protections and access restrictions. Because employees will leverage mobile devices (whether their own or GFE) for a mix of personal and agency requirements, a thorough evaluation of access to mission-oriented mobile apps (both custom and commercial) must be exercised. Agencies should create profile differences based on levels of device control and authority versus mission requirements.

From there, agencies can create a mobile app vetting program. The first step is to create an inventory of all the apps and devices on the network, analyze them for risks and take appropriate action against any apps that pose security risks.

Stage two is to establish a process for evaluating new applications. For example,

Shutterstock/FCW Staff

> **NowSecure recently reviewed 1,700 apps on employees' phones at one federal agency.** We found that 98% had at least one vulnerability, and 22% received a failing grade.

at the Justice Department, employees request permission to add apps on GFE and in a relatively short amount of time receive confirmation that the app is safe for use or receive an explanation of why it was not approved. Leveraging industry standards such as NIAP, FISMA or OWASP helps provide a structure for thorough evaluation and consideration of mobile app dependencies and data-sharing capabilities.

Stage three enables continuous monitoring of every new version of every app on the network when it is released. Many of the most popular mobile apps are updated weekly or even daily, so agencies need a continuous monitoring model that will monitor those updates and catch new vulnerabilities or intentional injection of malicious behavior into apps previously deemed safe.

The NowSecure automated software continuously monitors all mobile apps offered for download in the app stores and also tests custom-built apps so agencies can achieve universal protection for their entire mobile app portfolios. Integrated into agencies' mobile device management (MDM) services, NowSecure provides continuous app review and risk mitigation throughout the life cycle and across an agency's entire device population.

By understanding and addressing the risks associated with mobile apps, agencies can support employee productivity with mobile tools while protecting mission data on the device, in the apps and over the network. ■

Brian Reed is chief mobility officer at NowSecure.