Are Agencies Ready to Defend Against Mobile Threats?

While mobile devices present greater access for agency workforces, they open up opportunities for cyberattacks.

Kevin McCaney

Mon, 02/11/2019 - 17:10

Photo credit: akindo/iStock

Mobile computing makes government's design for agile, responsive agencies work. But it also gives hackers a lot more to work with. The spread of mobile devices taking advantage of anywhere-anytime access expands what an agency's workforce can do, but it increases the attack surface while creating new vectors that hackers can exploit to gain access to a network and its data.

With the pending arrival of 5G about to turbocharge wireless communications, mobile computing will become even more of a factor, for good and ill. Agencies might want to take a fresh look at mobile threats, how they differ from traditional attacks and what kinds of defenses against mobile threats they might want to employ.

“The enhanced capabilities mobile technologies provide, the ubiquity and diversity of mobile applications and devices and the typical use of the devices outside agencies’ traditional network boundaries require a security approach that differs substantially from the protections developed for desktop workstations,” according to DHS’ Mobile Security R&D Program Guide released April 2018 by the department’s Science and Technology Directorate.

The directorate has instituted a wide-ranging mobile security research and development program focused mostly on two fronts: device security and app security. The program aims to “accelerate the adoption of secure mobile technologies by DHS, the entirety of the federal government, and the global community,” the guide states. DHS is funding research into areas such as mobile software roots of trust, firmware security, developing a virtual mobile infrastructure, and providing continuous validation and threat protection for mobile apps. It also wants to bake in security throughout the development life cycle for mobile apps and is working on improving the security and resilience of mobile network infrastructure.

As well, mobile threat defense is a growing field, as Gartner pointed out in its comparison report on solutions for them.

The Drop on Mobile Threats

Mobile computing is a mighty big field on which to be playing defense. Ninety-five percent of Americans own a cell phone of some kind, and 77 percent have smartphones, according to the Pew Research Center. DHS said nearly 40 percent of its employees have a government-issued mobile device. The app stores from Google, Apple and Amazon, which carry government apps, offer about seven million unique apps combined, from more than 1.5 million sources. The guide noted that the mobile industry has five billion subscribers globally, nearly 396 million in the United States and 1.5 million in the federal government. Those numbers have only gone up since the guide was published in April 2018.

As mobile computing spreads like wildfire in the federal government, mobile threats are becoming evermore sophisticated, DHS' guide said. That "puts data stored or processed on these devices at risk and exposes back-end systems and networks to attacks via mobile malware."

Among the key threats:

Mobile phishing. Phishing has long been a scourge of government, and mobile computing compounds the threat. The screens of smartphones are relatively small and often leave out information in order to enhance the user experience, according to Gartner's Market Guide for Mobile Threat Defense. "There are also numerous channels to reach a mobile device that, unlike email, are not under phishing protection," the report stated, making users into easy prey.

Some things don't change, and one of them is that people are the biggest cyber vulnerability. FireEye said that 91 percent of all cybercrime starts with social engineering tactics in email, rather than with malware. Phishing and the more targeted spear-phishing tactics remain the go-to first step for infiltrating a network.

Unsecured Wi-Fi. Free wireless hotspots are tempting, but they typically are not secured and can leave users open to man-in-the-middle attacks, drive-by downloads of malware or rogue hotspots conducting network spoofing. A cyber criminal can set up access points with friendly-sounding names — posing as a coffee shop, hotel or airport service — and then steal passwords or other sensitive information. If you use public Wi-Fi, experts recommend that you not access sensitive networks that require a password or that you use a virtual private network (VPN) to make the connection secure.

Data leakage. If an app or connection is unsecured, data can leak when a user transfers files into cloud storage, sends an email to an unintended recipient or inadvertently pastes sensitive information into an exposed application. And beware free apps that are actually “riskware,” which work the way they’re supposed to but also send sensitive information to a remote server that could be operated by advertisers, criminals or foreign agents.

Broken cryptography. App developers that don’t use strong encryption or don’t implement it properly can introduce vulnerabilities or leave open back doors, according to the Infosec Institute.

Lost or stolen devices. With all those smartphones and other devices in use, some of them are bound to fall into the wrong hands. And some of those devices are vulnerable to hackers, either because they don’t have protections against accessing confidential information or the hackers are determined and skillful enough to get in.

Cyber Defense on the Go

Defending against mobile threats involves stretching defensive measures out the endpoints of network access, what security company Lookout calls post-perimeter security. (Lookout is one of five companies DHS’ mobile security program has awarded contracts to for R&D projects.)

Good mobile threat defense solutions go beyond antivirus and antimalware protections to address hardware, application and network vulnerabilities. They could look for compliance issues, such as when geolocation features are left on in a secure area, or unauthorized apps are in use. They can identify configuration problems that might make a device vulnerable or flag anomalous user behavior, which could indicate a successful hack or an insider threat.

Machine learning and artificial intelligence can enable these protections by constantly monitoring users and applications and analyzing behaviors. Several of the mobile application security projects under DHS’ program also employ machine learning.

Gartner’s most recent market guide to mobile threat defense solutions includes reviews of offerings from a dozen companies, from Lookout and Zscaler to Symantec and IBM.

All of the new threat data as well as recent cybersecurity efforts make one thing clear: as mobile computing continues to become more abundant, tending to the security landscape will require some new tools. It’s the only way that agencies and organizations can keep taking advantage of the conveniences and productivity benefits that mobile technology provides without facing undue risk because of it.

View printer friendly version
cybersecurity
cyberattacks
data protection
mobile
phishing