PUBLICATION

NIST Releases Guidelines for Vetting the Security of Mobile Applications Used by Businesses and Their Employees

February 03, 2015

Companies and their employees are increasingly using mobile devices and mobile applications (apps) to improve connectivity, communication and productivity. Unfortunately, these same companies may be unintentionally exposing themselves to significant security and privacy risks relating to their confidential, proprietary, personal or other data.

The National Institute of Standards and Technology (NIST), a non-regulatory agency within the U.S. Department of Commerce, has released a new guide, *Vetting the Security of Mobile Applications*, to help businesses and other organizations evaluate the security of mobile apps.

This guide is designed to assist organizations in understanding and implementing an app vetting process, developing app security requirements, understanding various app vulnerabilities and ultimately determining whether an app is secure enough to be used on the organization's mobile devices. It is also a guide for developers interested in understanding their app's potential software vulnerabilities.

According to the guide, before an organization begins vetting the security of a mobile app, it first needs to develop its own security requirements, including specifying "how data use by an app should be secured, the environment in which an app will be deployed, and the acceptable level of risk for an app." The app vetting process involves a series of activities aimed at determining whether an app satisfies the organization's security requirements and management plan. The process should be implemented after the app is developed and released for distribution, but before the app is deployed on the organization's mobile devices.

NIST warns that organizations "should not assume that an app has been fully vetted and conforms to their security requirements simply because it is available through an official app store." While the app store may verify compliance with its own requirements, the store's vetting process will not have taken into consideration the organization's specific security risks and requirements. Further, NIST recommends that an organization's app vetting process "be included as part of the organization's overall security strategy."

NIST's free guide provides recommendations on developing organization-specific security criteria, planning and implementing the app vetting process, testing apps and app approval/rejection activities.

As discussed in a December 2014 Baker Donelson Alert, the recently enacted Cybersecurity Enhancement Act of 2014 permits NIST to "facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures and processes to cost-effectively reduce cyber risks to critical infrastructure assets." Therefore, we expect to see NIST actively providing more and more resources, which likely will become the industry standard for whether a company acted reasonably in its privacy/security assessments and precautions.

If you need assistance developing and implementing your company's privacy and security policies, its breach management protocols or its app vetting process, please contact the authors of this alert, or a member of Baker Donelson's Privacy and Information Security Group.