THE
NATIONAL LAW REVIEW

National Institute of Standards and Technology (NIST) Issues Draft Report Enumerating Risks and Protections to Consider When Evaluating Mobile Apps for Your Enterprise

Article By
Privacy & Security Practice Group at Mintz Levin
Mintz
Privacy & Security Matters Blog

- Biotech, Food, Drug
- Utilities & Transport
- Consumer Protection
- Environmental, Energy & Resources
- Health Law & Managed Care
- Communications, Media & Internet
- Administrative & Regulatory

- All Federal

Friday, September 12, 2014

As the world recovers from the excitement leading up to Tuesday's **Apple Live Event** announcement of the new iPhone 6 and Apple Watch, mobile app developers are chomping at the bit to create software that leverages the new operating system and **Apple**’s widely-anticipated “HealthKit,” a purportedly secure platform that allows mHealth apps to share user’s health and fitness data with the new Health app and with each other. In fact, over 300 apps were created per day in recent years, according to some reports. But because the mobile app market is supersaturated, the quantity of available mobile apps does not equal the number of quality and secure apps that would be appropriate for use at an organization with a high privacy and security risk profile. The draft Technical Considerations for Vetting 3rd Party Mobile Applications (the Vetting Report) issued by National Institute of Standards and Technology (NIST) in August 2014 is an essential document for any organization to use to help weed out the mobile apps that may create unnecessary IT risks.

Why an Organization’s Existing Software Assurance Policies May Be Insufficient for Mobile Apps

Section 2 of the Vetting Report clearly sets out the problems of relying on an enterprise’s existing software assurance policies and procedures in the context of mobile computing. By the very “mobile” nature of today’s devices, organizations must be aware of the following risks, at minimum:

- Where employees bring their own devices and use apps supporting an organization’s on those devices, there is no way to tightly control use of those devices through the use of uniform operating systems, networks, traditional firewalls and common endpoint configuration;

- Because mobile apps generally are not self-contained, their reliance on third-party libraries for necessary information required by the end user can expose the device and the organization to malware or other privacy and security vulnerabilities;

- Mobile apps that purport to be free may have hidden costs – information collected by those apps may be being sold to marketing or other advertising entities, which may result in violations of state and federal privacy laws like the Health Information Portability and Accountability Act (HIPAA);

- The wide variety of networks mobile devices use to run applications (e.g., Wi-Fi, 2G/3G, and 4G/LTE) may be potential gateways for hacking and remote exploitation of mobile app vulnerabilities; and

- Because mobile apps go through constant updates and patching, each new version of the application may create new weaknesses in the software or security capabilities or even compound existing ones.

Based on the above risks, “[m]obile apps should be tested for secure behavior and reliability before being released to the community of users within the organization.” As part of this testing process, “conducting [a] risk analysis before deploying mobile apps should identify the roles of users, the risks, and the available countermeasures” for these risks.

Using Mobile App Vetting Policies and Procedures to Protect Your Organization

Sections 3 through 5 of the Vetting Report provide invaluable guidance for organizations who want to set up a comprehensive mobile app vetting process customized to their operating environments. Relying on the App Store or Android Marketplace is inherently risky; although they "may perform some app vetting processes to verify compliance with their own requirements . . . [o]rganizations should not assume that an app has been fully vetted to their organizational needs." Ideally, organizations should only outsource some or all of their mobile vetting processes to entities that have a particular understanding of their enterprises operations and privacy/security risk profile, such as IT contractors and outside counsel. In addition, it is not enough to vet mobile apps in a static environment. Organizations must test mobile apps in the expected ways that users will operate them as part of their day-to-day activities to adequately understand whether the mobile app may expose the organization to unnecessary privacy, security, and IT infrastructure risks.

Given that NIST is seeking comments until September 18th, there is still time for organizations contemplating a third party mobile app vetting process to inform NIST of any gaps that remain to be addressed in the Vetting Report. Regardless, all organizations seeking to use mobile app technologies in their operations should use the Vetting Report and NIST's other guidance publications to develop their own privacy and security evaluation processes to address the inherent risks of using mobile apps, before focusing too much on the rewards and fame they may bring.

Source URL: https://www.natlawreview.com/article/national-institute-standards-and-technology-nist-issues-draft-report-enumerating-ris