The State of Mobile Application Insecurity

Executive Summary

Sponsored by IBM

Independently conducted by Ponemon Institute LLC

Publication Date: February 2015

The State of Mobile Application Insecurity
Executive Summary

Ponemon Institute, February 2015

We are pleased to present the findings of *The State of Mobile Application Insecurity* sponsored by IBM. The purpose of this research is to understand how companies are reducing the risk of unsecured mobile apps in the workplace. Ponemon Institute surveyed 640 individuals involved in the application development and security process in their organizations.

Following is a summary of key takeaways illustrating why mobile application security eludes many organizations.

Customer needs and demand often affect mobile application security. Sixty-five percent strongly agree or agree that the security of mobile apps is sometimes put at risk because of customer demand or need. The "rush to release" phenomenon challenges an organization's ability to stop the risks of data leakage and malware.

The presence of malware-infected mobile apps/devices will increase over the next 12 months according to 61 percent of respondents and a similar percentage of respondents believe the real risk to mobile apps is data leakage. Because of these concerns, 60 percent say their organization considers mobile app security a high priority. Further, 58 percent say their organizations consider it very important to make applications tamper resistant.

Expertise and budget are needed to reduce mobile app security risks. Fifty-four percent of respondents are concerned that cross-site scripting through insecure mobile apps will increase over the next 12 months. However, only 41 percent believe their organization has sufficient mobile application security expertise. Moreover, only 30 percent believe their organization has ample resources to detect vulnerabilities in mobile apps and 29 percent say resources are available to prevent the use of vulnerable or malware-infected mobile apps.

Are enough resources available to deal with mobile app security? In this study**,** we asked respondents how much their organizations spend on mobile app development each year in terms of technologies, personnel, managed or outsourced services and other cash outlays. While an average of $34 million is spent on mobile app development, only $2 million is earmarked for mobile app security. Most security spending is allocated to reducing vulnerabilities and threats from proprietary software (36 percent) followed by open source software (21 percent). Only 11 percent is spent on pen testing to reduce threats from insecure mobile apps.

If an organization wants to reduce security risks, then control employees' use of mobile apps. Eighty-two percent of respondents say mobile apps in the workplace has very significantly (50 percent) or significantly (32 percent) increased security risks.

More organizations need to have a policy on the acceptable use of mobile apps. Most respondents say employees' use of mobile apps is very heavy (32 percent of respondents) or heavy (34 percent). However, more than half of respondents (55 percent) say their organization does not have a policy that defines the acceptable use of mobile apps in the workplace.

Can an organization's app store reduce the use of unsecured mobile apps? Only 30 percent of respondents say their organization has an app store. Sixty-seven percent of respondents admit that even if they have an app store, employees can use mobile apps from other sources. Fifty-one percent say employees are permitted to download apps from the organizations' app store onto personally owned mobile devices.

When asked what techniques are used to vet mobile apps for security in the app store, 48 percent of respondents say they scan for security flaws. However, 40 percent are not taking any of the precautions.

More mobile apps need testing. On average an organization tests less than half of their mobile apps. But of those tested, 30 percent contain vulnerabilities. The obvious implication is that more testing would reduce risks and prevent the use of unsecured mobile apps in the workplace.

Mobile apps are often tested too late. On average, respondents say their organizations have about 105 mobile apps in use today and an average of only 36 percent are mission critical. This means many apps are not needed by employees to do their work. Thirty-three percent of respondents say their organizations do not test mobile apps at all. Rarely are they tested during production. Most often they are tested in the deployment (22 percent) or in development (21 percent) stage.

How frequent does testing of apps occur? Most respondents say their organization does not test internally developed apps or outsourced or purchased apps. Even if they do test**,** 23 percent of respondents are not certain when testing of internally developed apps occurs followed by no pre-scheduled testing (14 percent). In the case of purchased or outsourced apps, most testing takes place every time the code changes (23 percent). However, 22 percent of respondents are unsure when testing takes place.

Many organizations are not scanning for vulnerabilities. Thirty-eight percent of respondents say their organizations do not scan for vulnerabilities. If they do scan, they mostly use proprietary software or tools (25 percent of respondents) or open source software or tools (14 percent of respondents).

Rush to release and lack of training makes mobile apps insecure. The practices and policies of organizations are to blame for mobile apps that contain vulnerable code**.** Seventy-seven percent of respondents say it is the pressure to release apps before testing for vulnerable code followed by 73 percent who lack understanding or training on secure coding practices. A lack of quality assurance and testing procedures (68 percent of respondents) and internal policies or rules that clarify security requirements (64 percent of respondents) are also to blame.

Effectiveness in securing mobile apps is low. Respondents rate the level of difficulty in securing mobile apps and concern about the threat of malware to mobile apps as very difficult (77 percent and 75 percent, respectively). However, organizations lack the ability to secure mobile apps and stop malware. Only 14 percent of respondents rate their organizations' effectiveness as high.

Keeping the end-user happy is key. Sixty-six percent of respondents rate the importance of end-user convenience when building and/or deploying mobile apps as very important and important. Fifty percent of respondents say security is very important and important and less than half (47 percent of respondents) say end-user privacy is very important and important.

To reduce mobile app risks, do organizations follow guidance from the Open Web Application Security Project (OWASP)? Despite the difficulty, 40 percent of respondents say their organizations do follow the top 10 mobile app security risks. The most difficult risk to minimize, according to 80 percent of respondents is broken cryptography followed by unintended data leakage (75 percent) and poor authorization and authentication (67 percent). The least difficult is security decisions via untrusted inputs.

What are the most frequent practices for securing the application development process? Respondents were asked to rate the practices they most often follow. Because data leakage has been identified as a significant risk to mobile app security, 55 percent of respondents say a priority is to prevent unauthorized users from accessing data security measures to stop data leakage. A similar percentage of respondents (53 percent) say their organizations use automated scanning tools to test applications for vulnerabilities during development and after they have been released. Practices not often followed should be at the top of the list. Specifically, only 27 percent

say their organization ensures the “rush to release” does not impact coding practices and 29 percent say development teams are not often measured against secure coding and architecture standards.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**,we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.