Guidance Regarding Security of Custom Developed Mobile and Web Applications

Background:

Mobile and web-based applications (apps) contain inherent risks as a result of vulnerabilities that exist within software and/or processes used in development. Unsecure apps may result in exploits that threaten the integrity, availability, or confidentiality of the apps, the data that they process, or the device on which they are installed.

Approach:

The threat landscape with regard to mobile/web apps is dynamic. New vulnerabilities are routinely discovered or exposed. Rather than listing specific settings or vulnerabilities, this guidance recommends that application development incorporates security as a component of the software development life-cycle (SDLC). While developers retain the professional latitude to determine security settings that are appropriate for each use case in consultation with risk owners, their decision should be informed by reputable, timely guidance.

Resources/Industry Standards:

The following resources provide guidance about security best practices and should be reviewed, and followed where appropriate:

JH mobile application security checklist (for development of mobile apps)

JH Web Application Security Guidance (for development of web apps)

Open Web Application Security Project® (OWASP) (Industry mobile app security standards)

Availability of internally developed apps should be restricted to intended potential users (e.g. Hopkins personnel, study participants). This is especially important when apps are distributed through application markets like Apple App Store and Google Play.

Data Protection:

The most effective approach to protection of sensitive data is to avoid the collection or storage of it. Data security plans should include a review of data collection with a genuine effort to ensure that only the minimum necessary sensitive data is collected.

When sensitive data is collected there must be a plan for the protection of them, and any copies or extracts of them, through their complete lifespans. The plan must include provisions for the eventual destruction or deidentification of sensitive data using industry best practices available at that time.

Apps that store sensitive data in cloud resources should align with Johns Hopkins Institutional Cloud Standards.

Application Lifecycle:

Apps that have been published or deployed are at risk from vulnerabilities that are uncovered following publication. Published Apps must include a mechanism for developing, testing, publishing, and deploying updates so that newly discovered vulnerabilities are mitigated, even on devices on which the app was previously installed.

It is reasonable to expect that the utility of all developed apps will eventually end, or be superseded by others. When that happens, the app should not be simply abandoned, leaving code that is no longer receiving post deployment security updates on the devices to which it was deployed. A proactive plan for removing the app, or informing the installers that they should remove it, should exist from the beginning. Apps that have temporary or limited utility should recommend removal when the utility of the app expires.

Compliance:

Risk owners (principal investigators, department heads, project leads, etc.) are responsible for ensuring that mobile and web-based apps contain security provisions that are appropriate based on the type, sensitivity, and volume of data being collected or processed by the app.

Data security plans should include the following attestations regarding the development and operation of mobile applications:

- Application development aligns with JH security checklist.
- Application developers are familiar with OWASP and have incorporated recommendations as appropriate.
- Cloud storage (if used) aligns with JH Cloud Standards.
- Data collection review confirms that only the minimum necessary sensitive data is being collected.
- Requirements for JH Mobile App Solution have been reviewed, and the app has been submitted for review if required.
- Application has been tested for security vulnerabilities using appropriate tools consistent with OWASP standards.
- Plan for the removal of the app has been created, or recommendation for removal following expiration of utility has been incorporated into installation instructions.
- Plan for ongoing support (including development and deployment of patches) has been created, and includes allocation of necessary funding.

Data security review of research plans will look for these attestations and will request them if not provided.

Effective: 10/23/2020