19.08.2014

MOBILE SECURITY

Von: Christopher Dreher

Mobile Anwendungen bergen Gefahren

SICHERE APPS FÜR DEN UNTERNEHMENSEINSATZ

Unabhängig für welchen Zweck mobile Apps in Unternehmen zum Einsatz kommen: Sobald mit sensiblen Geschäftsdaten gearbeitet wird, müssen sich die Verantwortlichen mit der Sicherheit der eingesetzten Apps auseinandersetzen. Dazu gehört es auch, sich mit den Eigenheiten der mobilen Plattformen vertraut machen.

Aufgrund der Marktverbreitung und der App-Verfügbarkeit beschränkt sich diese Betrachtung hier auf Apples iOS- und Googles Android-Plattform. Die Sicherheitsarchitekturen der beiden mobilen Betriebssysteme haben sich im Laufe ihrer Entwicklung stark aneinander angelehnt. Bei beiden Plattformen werden die einzelnen Apps in voneinander getrennten Systemkontexten, sogenannten Sandboxen, ausgeführt. Dies hat den Vorteil, dass Apps gegenseitig nicht auf fremde Daten anderer Apps zugreifen können. Zur Ablage von Zugangsdaten, Zertifikaten und sonstigen sensiblen Informationen bieten beide Plattformen ebenso geeignete Schlüsselspeicher an. Je nach eingesetztem Smartphone oder Tablet wird dieser Schlüsselspeicher durch einen in die Hardware implementierten Cryptochip realisiert. Um auf einzelne Funktionen der mobilen Plattformen, wie z.B. das Recht, Netzwerkverbindungen zu öffnen, auf Kalender oder Kontaktdaten zuzugreifen oder die Kamera des Gerätes zu nutzen, bieten die mobilen Plattformen unterschiedlich feingranulare Rechtemodelle an.

Die Top 10 mobiler Gefahren

Wenn man sich dazu entscheidet, mobile Apps zu entwickeln oder Dienstleister damit beauftragt, bietet das Open Web Application Security Project (OWASP) eine gute Anlaufstelle für Informationen rund um die sichere Entwicklung. Bei der OWASP handelt es sich um eine weltweite Non-Profit-Organisation, die es sich zum Ziel gesetzt hat, das Sicherheitsniveau der Software-Entwicklung zu verbessern. Sie veröffentlicht in regelmäßigen Abständen eine Top-10-Liste der größten Gefahren im mobilen und Webumfeld. Die aktuelle Mobile-Top-10-Liste für 2014 ist noch nicht endgültig verabschiedet, steht aber als Release Candidate zur Verfügung. Neben den einzelnen Risiken, welche sowohl die Angriffsvektoren als auch die technischen und geschäftsbezogenen Auswirkungen skizzieren, gibt die OWASP zugleich auch immer Empfehlungen für die bekannten mobilen Plattformen ab, um den Risiken entgegenzuwirken.

Als ersten Risikofaktor führt die OWASP schwache Kontrollmechanismen der Serverseite auf. Dieser Punkt befasst sich nicht direkt mit der sicheren Entwicklung von mobilen Apps, sondern beleuchtet die serverseitigen Komponenten. Apps kommunizieren oft online mit einer Gegenstelle, um Daten auszutauschen oder Prozesse zu steuern. Unabhängig von den mobilen Apps müssen diese serverseitigen Gegenstellen, die oft in Form von Webservices realisiert werden, eingehende Daten sensibel überprüfen, bevor eine Weiterverarbeitung stattfinden darf. Die OWASP führt hier eine Vielzahl von Risiken, wie etwa unterschiedliche Injection-Angriffe (XSS, SQL, Command), auf. Diese Risiken sind bereits aus der klassischen Webentwicklung bekannt und spiegeln sich hier auf der Serverseite wieder. Aus diesem Grund sollte serverseitig eine strikte Eingabevalidierung aller eingehenden Daten durchgeführt werden. Eine Empfehlung der OWASP ist, diese Überprüfung nach einem Whitelist-Ansatz durchzuführen, so dass nur legitime Eingaben akzeptiert werden, die zuvor definierten Mustern entsprechen.

Der zweite Punkt auf der Risikoliste befasst sich mit der unsicheren Ablage von Daten auf den mobilen Endgeräten. Wenn sensible Daten wie Zertifikate, Authentifizierungs- oder personenbezogene Daten direkt auf den Dateisystemen der mobilen Geräte abgespeichert werden, sind diese oft unzureichend geschützt. Durch den physikalischen Zugriff auf das mobile Endgerät, verursacht durch einen Verlust oder Diebstahl, können eine Vielzahl ungeschützter Daten über eine Kopplung zu einem PC extrahiert werden. Deshalb ist es wichtig, dass die von den mobilen Plattformen angebotenen Möglichkeiten zur sicheren Datenablage den Entwicklern bekannt sind.

Unter iOS können Authentifizierungsdaten und Zertifikate im Schlüsselspeicher (Keychain) abgelegt und mit einer Schutzklasse versehen werden, die angibt, zu welcher Zeit die Daten zugreifbar sind. Größere Dateien können unter iOS mit Apples Data-Protection-API ebenso verschlüsselt werden. Auch unter Android steht dem Entwickler seit der Version 4.0 ein Schlüsselspeicher

(Keystore) zur Verfügung. Je nach Gerätehersteller ist auch bei Android eine vollständige Dateisystemverschlüsselung möglich. Auf die Verwendung dieser Verschlüsselung des gesamten Gerätes hat der App-Entwickler jedoch keinen Einfluss. Somit empfiehlt es sich, unter Android Daten auf Applikationsebene zu verschlüsseln. Ein Beispiel sind SQLite-Datenbanken, die unter Android sehr oft verwendet werden. Möchte man als Entwickler sensible Daten in so einer Datenbank ablegen, so gibt es seitens der OWASP die Empfehlung, eine dedizierte Datenbankverschlüsselung, wie SQLcipher einzusetzen.

Höchst unsichere Netze

Ein interessanter Punkt der besagten Top-10-Liste beschäftigt sich mit der Sicherheit der Netzwerkkommunikation. Diese Thematik ist gerade bei mobilen Apps wichtig, weil die Geräte nicht zwangsläufig in sicheren Netzen betrieben werden. Mobile Endgeräte werden gerne in öffentlichen WLANs in Cafés, Hotels, Bahnhöfen oder Flughäfen benutzt. Diese offenen Netzwerke sollte man als nicht vertrauenswürdig einstufen, da andere Netzwerkteilnehmer sich gezielt als Angreifer in die Kommunikation zwischen der mobilen App und der serverseitigen Gegenstelle setzen können. Aus diesem Grund ist es essenziell, dass sämtliche Verbindungen ausschließlich über verschlüsselte Netzwerkprotokolle kommunizieren.

Bei Apps, wie auch bei gewöhnlichen Webapplikationen hat sich hier das HTTPS-Protokoll etabliert. Hierbei handelt es sich um HTTP-Verbindungen, die per SSL-Verschlüsselung abgesichert und verschlüsselt werden. Bei mobilen Apps geht man inzwischen sogar noch einen Schritt weiter und setzt zusätzlich zu SSL das sogenannte Zertifikats-Pinning ein. Bei diesem Verfahren wird innerhalb der mobilen App der Fingerabdruck des SSL-Zertifikats der serverseitigen Gegenstelle hinterlegt, so dass ausschließlich gesicherte Verbindungen zu der beabsichtigten Serverkomponente möglich sind und es einem Angreifer nicht möglich ist, durch das Vortäuschen eines anderen SSL-Zertifikats die Verbindung aufzubrechen.

App-Wrapping heißt das Zauberwort

Alle bisherigen Entwicklungsempfehlung können nur umgesetzt werden, wenn der Quellcode der App vorliegt. Welche Möglichkeiten bestehen aber für Unternehmen, die Fremd-Apps einsetzen möchten? Wie können sie sicherstellen, dass alle Voraussetzungen für die Verarbeitung von sensiblen Daten erfüllt sind? Der erste und allumfassende Weg ist die Beauftragung eines IT-Sicherheitsdienstleisters wie beispielsweise der Cirosec GmbH. Dieser führt eine Sicherheitsüberprüfung auf Basis eines Blackbox-Ansatzes der ausgewählten App durch. Dabei wird mit unterschiedlichen Testverfahren das komplette Sicherheitsniveau der App analysiert und Defizite aufgezeigt. Basierend auf diesen Ergebnissen kann das Unternehmen dann entscheiden, ob die ausgewählte App den Sicherheitsanforderungen genügt. Eine Alternative hierzu sind Anbieter sogenannter App-Reputations-Diensten. Diese

haben sich darauf spezialisiert, eine Vielzahl von App hinsichtlich ihrer Datensicherheit zu überprüfen. Kunden dieser Reputationsdienste haben die Möglichkeit, in Verzeichnissen des Anbieters das Sicherheitsniveau von aufgelisteten Apps zu überprüfen. Je nach Anbieter und gewählter Dienstleistung besteht auch die Möglichkeit, bisher nicht aufgelistete Apps überprüfen zu lassen.

Hat die Sicherheitsüberprüfung ergeben, dass die ausgewählte App leider nicht den Datenschutzanforderungen genügt, muss es aber nicht zwangsläufig heißen, dass das Unternehmen nach einer Alternative Ausschau halten muss. Der erste Schritt wäre den Ersteller der App auf die Defizite hinzuweisen und gemeinsam an einer Lösung zu arbeiten. Die Erfahrung hat jedoch gezeigt, dass nicht alle App-Hersteller kooperativ sind. Hat ein Unternehmen jedoch keine Wahl und ist genau auf die eine App angewiesen, die den Sicherheitsanforderungen nicht nachkommt, gibt es eine weitere Lösung. Das Zauberwort hierfür heißt App-Wrapping.

Dabei handelt es sich um einen technischen Vorgang, der nicht vorhandene Sicherheitsfunktionen bei bestehenden Apps hinzufügt. Hierfür wird die betroffene App so modifiziert, dass die fehlenden Sicherheitsfunktionen durch dynamische Bibliotheken hinzugefügt werden. App-Wrapping ist sowohl für iOS- als auch für Android-Apps möglich. Technisch gesehen können durch dieses Vorgehen sämtliche Sicherheitsfunktionen hinzugefügt werden. In der Realität funktioniert das jedoch nicht immer, da die angefügten Bibliotheken auf einzelne Besonderheiten der Apps angepasst werden müssten. Auch für das Thema App-Wrapping gibt es inzwischen eine ganze Reihe von Anbietern, die ihren Kunden die Möglichkeit geben, Apps über ein Portal automatisch wrappen zu lassen. Die einzige Restriktion, die bei gewrappten Apps beachtet werden muss ist, dass nach einem erfolgten Wrapping keine Einstellung in die offiziellen Appstores von Apple und Google mehr möglich ist. Die Verteilung dieser Apps erfolgt in der Regel durch Mobile-Device-Management (MDM)-Systeme.

Leitfaden für sichere App-Entwicklung:

Ausschließlich nötige Rechte von der mobilen Plattform einfordern

Die Schwächen der mobilen Plattformen kennen und programmatisch entgegen wirken.

Netzwerkverbindungen dürfen ausschließlich verschlüsselt erfolgen, da den Tansportmedien nicht vertraut

werden kann.

Sämtliche Benutzereingaben müssen vor der weiteren Verarbeitung durch die Apps einer zuverlässigen Eingabevalidierung unterzogen werden.