TÜV TRUST IT

TÜV AUSTRIA Group

Leitfaden

Sichere App-Entwicklung

Inhalt

TÜV TRUST IT GmbH
Unternehmensgruppe TÜV Austria
Waltherstr. 49–51
51069 Köln

Weitere Informationen zum Thema:
Christina Münchhausen
Tel.: +49 (0)221 / 96 97 89-0
Mail: stefan.moeller@it-tuv.com
Web: www.it-tuv.com
www.app-sicherheit.de

Vorbemerkungen

Es ist längst kein Geheimnis mehr, dass Apps auf mobilen Endgeräten nicht nur einen vielfältigen Nutzen bieten können, sondern gleichzeitig auch deutliche Risikoquellen für die Datensicherheit und den Datenschutz darstellen. So werden im Markt Apps angeboten, deren tatsächliches Geschäftsmodell darin besteht, wertvolle Informationen auszuspähen und Daten der Benutzer zur wirtschaftlichen Verwertung zu sammeln.

Allerdings weisen auch zahlreiche mobile Anwendungen unbeabsichtigterweise Sicherheitsrisiken auf. Apps werden oftmals durch das Marketing oder die Fachabteilungen beauftragt, wobei der Fokus primär auf den Funktionalitäten und dem Design liegt, dabei jedoch Sicherheitsaspekte lange vernachlässigt werden. Auch die Auslagerung der Entwicklung an nicht für Sicherheitsaspekte sensibilisierte Entwickler sowie die Wiederverwendung von Programmteilen aus bereits vorhandenen Apps gehören zu häufigen Ursachen. Insofern liegen hier die Ursachen von Sicherheitsrisiken im Entwicklungsprozess – ein bislang kaum öffentlich diskutiertes Problem.

Der vorliegende Leitfaden beschäftigt sich deshalb mit der Frage, wie Anforderungen an den Datenschutz- und die Datensicherheit systematisch in die App-Entwicklung einfließen können. Dabei widmet er sich zunächst einer generellen Betrachtung der Bedrohungslage, um anschließend konkrete Lösungsmethoden vorzustellen. Dazu gehört auch eine Charakterisierung verschiedener im Markt verbreiteter Experten-systeme, die der Entwicklung sicherer Apps dienen.

Darüber hinaus enthält die Praxishilfe einen Selfcheck zur Statusanalyse. Er hinterfragt, ob sich die Sicherheitsthematik ausreichend in den Entwicklungskonzepten des individuellen Unternehmens wiederfindet, um einen möglichen Handlungsbedarf zur Optimierung zu identifizieren.

Betrachtungen der App-Bedrohungen

In Zeiten immer mobilerer Arbeitsprozesse und eines gleichzeitig stark wachsenden Marktes an mobilen Anwendungen verwenden auch immer mehr Mitarbeiter auf ihren Endgeräten Apps. Laut Branchenverband BITKOM sind im Durchschnitt auf jedem Smartphone rund 23 zusätzliche zu den werkseitig mitgelieferten Apps installiert. Welche neuen Sicherheitsbedrohungen damit auf die Unternehmen zukommen, zeigen die Ergebnisse einer Analyse von über 1.000 mobilen Anwendungen, die die Security-Spezialisten der TÜV TRUST IT durchgeführt haben. Danach erwiesen sich 45 Prozent der geprüften Apps als kritisch, weil sie einen potenziellen Datendiebstahl ermöglichen und durch verschiedene Arten der Profilbildung die Privatsphäre der Nutzer verletzen können.

Aus Sicht des Datenschutzes stellt das sog. Device-Tracking durch Dritte – wie etwa spezialisierte Werbenetzwerke – ein besonders großes Problem dar. Hierbei werden gerätespezifische und unveränderbare Merkmale wie die Device ID oder die Hardware-Adresse der WLAN- oder Bluetooth-Schnittstelle verwendet, um das Endgerät an verschiedenen Orten oder bei der Verwendung bestimmter Apps wiederzuerkennen. Anders als bei den internetfähigen PCs, bei denen der Nutzer im Browser datenschutzfreundliche Einstellungen wählen kann (beispielsweise die Löschung von Cookies), bedarf es bei Smartphones häufig eines expliziten Zurücksetzens auf die Werkseinstellungen. Dabei werden allerdings auch alle nützlichen Einstellungen, wie gespeicherte Profile, entfernt.

Nutzer versuchen einen solchen radikalen Schritt typischerweise zu vermeiden. Durch die Verwendung von an die Hardware gebundenen IDs bleibt das Gerät dann aber während seiner gesamten Nutzungsdauer jederzeit identifizierbar. „Damit können Dritte über verschiedene Apps mit dem selben Datenaggregator gezielt die Nutzungsgewohnheiten des Smartphone- oder Tablet-Nutzers zusammenführen und nach ihrem Bedarf Persönlichkeits-, Reise- und zahlreiche andere Profile erstellen“, stellt Dirk Münchhausen, Mitglied der Geschäftsführung der TÜV TRUST IT, klar.

Eine gewisse Entwarnung gibt es hier für die iPhone-Nutzer. Denn im Falle der Apple-Geräte wurde mit der Betriebssystemversion iOS 7 eine Funktion eingeführt, die ein Auslesen der WLAN-MAC, der Unique Device ID (UDID) und der MAC-Adresse der Bluetoothschnittstelle unterbindet. Weiterhin wird mit der Einführung des sogenannten Advertising Identifier vermieden, dass Querverbindungen zwischen unterschiedlichen Apps herausgefunden werden können.

Zu exzessive Geolokation

Ein zweites Kernproblem besteht darin, dass bei eingeschalteter Geolokalisierung über das Smartphone permanent der Aufenthaltsort des Benutzers an beliebige Stellen übertragen werden kann. Geolokalisierung stellt zwar in vielen Applikationen eine nützliche Funktion dar, daher ist sie bei den meisten Endgeräten auch standardmäßig eingeschaltet. Vielen Anwendern ist allerdings nicht bewusst, dass Apps diese Daten häufig auch ohne konkreten Bedarf abgreifen und versenden. „Wie detailliert und wie lange seine Bewegungen aufgezeichnet werden, bleibt dem Nutzer häufig verborgen, da er mit seiner Zustimmung der App eine ‚carte blanche' für alle zukünftigen Zugriffe ausgestellt hat", erläutert Dirk Münchhausen.

Sammelwut der Apps statt Datensparsamkeit

Dabei muss isoliert betrachtet nicht zwangsläufig jede einzelne unnötige Datenübertragung Sorgen bereiten. Problematisch wird es für den Benutzer mobiler Endgeräte jedoch, wenn es an einem Grundsatz der Datensparsamkeit und Datenvermeidung fehlt oder dieser bewusst unterlaufen wird. Nach den Analysen der TÜV TRUST IT übermitteln die Smartphone-Anwendungen im Regelfall deutlich mehr Informationen, als dies rein für die Diensterfüllung notwendig wäre. Dazu gehören bevorzugt Telefonnummern und E-Mail-Adressen oder Positionsdaten.

„Dies hat System", vermutet Münchhausen. „Auch wenn Bequemlichkeiten der Programmierer oder konzeptionelle Schwächen der Anwendungen mitunter die Ursache für den übermäßigen Zugriff auf sensitive Personendaten darstellen können, so erscheint das Motiv der App-Anbieter zu überwiegen, eine möglichst umfangreiche Datensammlung vorzunehmen. Insbesondere die Nutzer kostenloser Apps ‚bezahlen' häufig mit ihren persönlichen Daten."

Benutzerdaten liegen offen

Ein drittes Problemfeld stellt die häufig fehlende Sicherung von Nutzerdaten innerhalb der App-Funktionen dar. Nutzerdaten wie Benutzername und Kennwort werden zwar oftmals aus legitimen Gründen gespeichert, etwa für den wiederholten Zugriff auf einen Webservice. Auch individuelle Konfigurationen wie beispielsweise Favoriten für Busverbindungen im öffentlichen Nahverkehr gehören dazu.

Doch bei fehlenden Sicherungsfunktionen innerhalb der App können häufig diese sensiblen Daten durch Dritte ausgelesen oder verändert werden, falls das Handy verloren geht oder leihweise in andere Hände gelangt. Wo und wie die Daten abgeflossen sind oder manipuliert wurden, lässt sich dann im Nachhinein nur schwer feststellen. Moderne Smartphone-Betriebssysteme bieten zwar hierfür prinzipiell Schutzmaßnahmen. Deren Handhabung ist vielen Herstellern von Apps jedoch unbekannt oder es wird aus Bequemlichkeitsgründen darauf verzichtet, sie konsequent einzubinden.

„Diese generellen Bedrohungen von außen sind für den einzelnen Benutzer ebenso wie für die Sicherheitsverantwortlichen in den Unternehmen nicht beeinflussbar“, erklärt Münchhausen. Insofern müssten Unternehmen ihren Fokus auf den Selbstschutz richten. Die Herausforderung bestehe einerseits darin, den Nutzen von mobiler Kommunikation im geschäftlichen Umfeld nicht durch sehr restriktive Maßnahmen übermäßig zu beschränken und andererseits für ein bedarfsgerechtes Sicherheitsniveau zu sorgen. „Es muss also eine Balance zwischen den Chancen und Risiken geschaffen werden.“

Reality Check

- **45% der Apps lesen gerätespezifische Daten aus.** Dazu gehören Seriennummern, MAC-Adressen, Android-IDs usw. Dieses Tracking erfolgt während der gesamten Lebensdauer des Geräts.
- **40% der Apps nutzen Lokalisierungsfunktionen.** Dies erfolgt häufig auch dann, wenn es dafür keine sachliche Begründung gibt. Somit besteht die Gefahr, dass mittels dieser Daten Bewegungsprofile erstellt werden können.
- **10% der Apps übertragen Inhalte aus dem Adressbuch,** obwohl datenschutzfreundliche Lösungen möglich sind.

Expertensysteme zur Entwicklung sicherer Apps

Das Bundesdatenschutzgesetz und andere sicherheitsrelevante Vorgaben sind nicht nur für die Betreiber und Nutzer mobiler Anwendungen und Services relevant, sondern auch für App-Entwickler. Danach muss eine App die Daten schützen, sofern sie personenbezogene Informationen verarbeitet.

Doch über diesen rein rechtlichen Aspekt hinaus gibt es hier noch weitere wichtige Aspekte, die einen sensiblen Umgang mit der Datensicherheit von Apps begründen. Dazu gehört einerseits die Wahrnehmung der Anwender und der Öffentlichkeit. Denn gerät eine App aufgrund von Sicherheitslücken in Verruf, beschädigt dies die Reputation des betroffenen Unternehmens. Gibt beispielsweise eine Bank eine unsichere App für das Online Banking heraus, wird sie von den Kunden als wenig vertrauenswürdig gesehen und dies schlägt auf das Image des Kreditinstituts insgesamt zurück.

Sehr unterschiedliche Entwickler-Unterstützung

Zwar stellen alle Anbieter von Betriebssystemen für die App-Entwicklung über kostenlose Software Development Kits (SDK) eine Sammlung von Werkzeugen und Anwendungen zur Verfügung, mit denen sich native Applikationen für die jeweilige Plattform entwickeln lassen. Allerdings sind die Themenbereiche Datensicherheit und Datenschutz in diesen SDKs in der Regel für die Verarbeitung sensibler Daten nicht prominent genug dargestellt und in der nötigen Detailtiefe berücksichtigt. Deshalb stehen die Entwickler vor der Frage, wie sie zu den notwendigen und richtigen Informationen gelangen können. Hierfür bieten sich derzeit drei Möglichkeiten an:

1. Der autodidaktische Weg: Über eigene Recherchen im Internet oder durch den Kauf von Handbüchern kann das entsprechende Know how aufgebaut werden. Das Problem hierbei ist jedoch, valide Quellen im Internet zu finden und das Wissen aktuell zu halten. Außerdem besteht erfahrungsgemäß eine große Schwierigkeit darin, aus der Fülle des recherchierbaren Contents die relevanten Informationen zu selektieren und dabei zusätzlich dedizierte Hinweise für die richtige Implementierung im spezifischen Projekt herauszufiltern.

2. Einfache Expertensysteme: Von ersten Anbietern werden im Markt Unterstützungsleistungen für die Entwicklung sicherer Apps angeboten. Meist handelt es sich dabei um Checklisten, Whitepapers und ähnliche Dokumente, die zum Download bereitgestellt werden. Sie enthalten generische Maßnahmen und Hinweise für die Absicherung von Apps. Diese Angebote sind zumeist kostenfrei, richten sich eher aber an ambitionierte, wenig erfahrene Entwickler und eignen sich vor allem zur Aneignung von Basiswissen zu sicherer App-Entwicklung. Dass es sich dabei um eine Unterstützung für die semiprofessionelle Entwicklung handelt, zeigt sich insbesondere in folgendem Nachteil: Für die Begleitung von Projekten mit spezifischen Risikopotenzialen, wozu beispielsweise die Verarbeitung besonders sensibler Daten, personenbezogener Daten oder eine sichere Kommunikation mit Backend-Systemen gehören, besitzen die einfachen Expertensysteme oftmals nicht die notwendige Detailtiefe.

3. Kontextspezifische Expertensysteme: Diese ausgefeilteren Systeme sind für professionelle Entwickler gedacht, die ausgerichtet an den Funktionalitäten der zu entwickelnden App und kontextabhängiger Rahmenbedingungen eine spezifische Sicherheitsrichtlinie für dieses Projekt erzeugen. Darin enthalten sind alle bekannten Bedrohungen, übergeordnete generische Sicherungsmaßnahmen und plattformspezifische Implementierungshinweise. Außerdem enthalten diese Expertensysteme Best Practices als konkrete Code-Beispiele, die für die dedizierte Umsetzung im Projekt mit niedrigen Einstiegshürden genutzt werden können.

Der Vorteil dieser Systeme liegt neben der größeren Detailtiefe und dem größeren Umfang der Hinweise auch darin, dass durch ihren methodischen Ansatz handhabbare, schlanke Vorgabedokumente entstehen. Sie beschreiben nur die für das spezifische Projekt notwendigen und relevanten Maßnahmen statt ein umfangreiches Gesamtkompendium für die App-Entwicklung, welches alle Bedrohungen und Risiken für Apps beschreibt. Durch das gelieferte Know-how mit den kontinuierlich aktualisierten Informationen sind solche Expertensysteme jedoch nicht kostenfrei.

Restriktionen in der App-Entwicklung

Apps für den Einsatz in Unternehmen unterliegen in der Regel einem höheren Schutzbedarf als öffentlich angebotene Consumer-Apps. Schließlich dürfen die beruflichen Daten, die mit diesen Apps verarbeitet werden, nicht in die Hände Unbefugter gelangen. Ebenso muss sichergestellt sein, dass die Kommunikationswege zwischen den mobilen Endgeräten und der firmeneigenen IT-Infrastruktur nicht kompromittierbar sind.

Diesen Anspruch müssen Unternehmen bei der Entwicklung mobiler Anwendungen erfüllen. Doch sie sind dabei häufig mit dem Problem kleiner Budgets konfrontiert, außerdem verfügen sie oftmals nicht über Ressourcen mit ausreichenden Erfahrungen in der Programmierung sicherer Apps. Die Beschränkungen auf der fachlichen bzw. Erfahrungsebene sind insofern nicht verwunderlich, weil die Entwickler mit vergleichsweise neuen Plattformen konfrontiert werden, die zudem eine große Vielfalt und Komplexität aufweisen. Hinzu kommt, dass Vorgehensmodelle aus der klassischen Softwareentwicklung wie etwa ein ausformulierter Secure Development Lifecycle (SDL) in den meisten Fällen aus Kostengründen von vornherein ausgeschlossen sind.

Entwicklung mit dem Threat Model

Genau wie bei der Einführung mobiler Services gilt auch hier: eine fundierte Risikoanalyse ist das Fundament für die Entwicklung sicherer Apps. Das dafür aus dem SDL entliehene Vorgehensmodell ist das Threat Model, die methodische Bedrohungsmodellierung. Im Threat Model tragen Entwickler, Software-Architekten und Sicherheitsexperten die spezifischen Bedrohungen einer App zusammen, da sie häufig Dreh- und Angelpunkt einer Client-Server-Architektur ist und somit ein hohes Gefährdungspotenzial aufweist. Zu jeder Bedrohung wird anschließend eine Maßnahme definiert, die es bei der Implementierung zu berücksichtigen gilt.

Für die Implementierung sollten dann wiederum Sicherheitsvorgaben existieren, um den Entwicklern möglichst gut verwendbare Unterstützung bei der Umsetzung der sicherheitskritischen Funktionalitäten der App an die Hand zu geben. Doch je unkonkreter die Anforderungen und Vorgaben sind, desto weniger wirksam werden anschließend die implementierten Sicherheitsmaßnahmen sein.

Das Threat Model unterstützt jedoch nicht nur den eigentlichen Entwicklungsprozess, sondern ist auch die Basis für eine kontextspezifische Sicherheitsdokumentation für die jeweiligen Apps und Entwicklungsprojekte. Diese bietet eine ideale Grundlage für den sicherheitstechnischen Abnahmetest. Die Überprüfung sollte aus einem konventionellen Penetrationstest gegen App und Server bestehen. Sofern es das Budget zulässt, empfiehlt sich eine ergänzende Prüfung der Teile des Programmcodes, welche die sicherheitskritischen Funktionalitäten steuern. Nur so lassen sich Detailfehler in der Absicherung wirksam aufdecken, besonders wenn ausgefeilte kryptographische Schutzmaßnahmen zum Einsatz kommen sollen. Dies stellt selbst erfahrene Programmierer oftmals noch vor deutliche Herausforderungen.

Richtlinien-Tool zur sicheren App-Entwicklung

Nur allzu oft wird durch Experten festgestellt, dass fehlende Kenntnisse über die Entwicklung sicherer Anwendungen unliebsame Einfallstore öffnen. Zu den typischen Ursachen gehört, dass im Regelfall keine spezifischen Sicherheitsspezifikationen für das Entwicklungsprojekt bestehen.

Die TÜV TRUST IT hat deshalb mit dem TÜV AppSpecs-Generator ein Richtlinien-Tool entwickelt, das auf dem vorher beschriebenen Threat Model als methodische Bedrohungsmodellierung basiert. Dabei sind für jede Bedrohung generische Maßnahmen und plattformspezifische Implementierungsrichtlinien hinterlegt, die bis auf Code-Ebene ausformuliert sind und einem Entwickler, der keinerlei Vorkenntnisse in Datenschutz und Datensicherheit besitzt, somit das Erstellen sicherer und unangreifbarer Apps erlaubt.

Darüber hinaus bezieht der TÜV AppSpecs-Generator die Art der von einer App verarbeiteten Daten ausdrücklich in die Auswahl der empfohlenen Richtlinien mit ein und beachtet auf diese Weise gesetzliche Vorgaben und gängige Best Practices zum Umgang mit Daten (z.B. pseudonyme Daten, personenbezogene Daten, sensible Daten). Bisher sind die vier gängigsten Mobilplattformen im Richtlinien-Tool hinterlegt: Apple iOS, Android, Blackberry und Windows Phone 7.5. – Windows Phone 8 folgt.

Nutzen durch den AppSpecs-Generator

- **Kontextspezifische und an den individuellen Anforderungen ausgerichtete Vorgaben**
- **Einfache Bedienung:** Generierung von Entwicklerrichtlinien auch durch Nicht-Fachleute
- Für die **gängisten Mobilplattformen verfügbar**
- **Möglichkeit zum Exportieren der Entwicklerrichtlinien** als PDF-Datei
- **Mehrsprachigkeit** (deutsch/englisch)

Die Funktion des TÜV AppSpecs-Generators besteht darin, aus der Matrix der vom Auftraggeber oder Entwickler definierten Merkmale, bestehend aus der zu verwendenden Plattform, der Art der zu verarbeitenden Daten sowie den sicherheitsrelevanten Features einer App eine spezifische, auf die jeweilige App bezogene Implementierungsrichtlinie zu erstellen.

Diese Richtlinie kann als sicherheitsspezifischer Anhang zu einem Lastenheft fungieren, in jedem Fall dient sie dem Programmierer als Implementierungsrichtlinie und erlaubt überdies die gezielte Prüfung der Vorgaben im Anschluss an die Implementierung der App. In Abgrenzung

zu statischen Entwicklerrichtlinien ermöglicht das Richtlinien-Tool das kontextbezogene Anwenden von Sicherheitsvorgaben und versetzt dadurch auch solche Entwickler in die Lage, sichere Apps zu programmieren, die über keine Erfahrung und Fachkenntnis im Umgang mit IT-Sicherheit verfügen.

Das bedeutet, dass dem Entwickler die Richtlinien individuell bezogen auf ein Entwicklungsprojekt zur Verfügung gestellt werden. Damit deckt der AppSpecs-Generator die größtmögliche Zielgruppe ab, wohingegen statische Entwicklerrichtlinien aufgrund des fehlenden konkreten Kontextbezugs allzu häufig gar nicht oder falsch verstanden werden.

Gliederung der Entwicklerrichtlinien u.a. nach folgenden Kategorien

- **Adressbuchzugriff**
- **Audio-/Video-Aufnahme**
- **Verwendung von Cloud-Diensten**
- **Zugriff auf Foto-Bibliothek**
- **Auslesen von gerätespezifischen Daten**
- **Kommunikation der App mit Systemen aus dem Internet**
- **Kalenderzugriff**
- **Zugriff auf Foto-Kamera**
- **Speicherung von Daten im Dateisystem**
- **Verwendung von Lokalisierungsfunktionen**
- **Zugriff auf Musik-Bibliothek**
- **Nutzung von lokalen Serverdiensten**

App-Zertifizierung als Sicherheitsnachweis

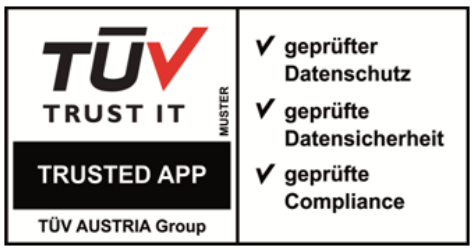
Kundenbeziehungen erfordern Vertrauen. Der Missbrauch von Daten auf mobilen Geräten wie Smartphones und Tablets verunsichert die Nutzer, deshalb benötigen sie Anhaltspunkte, um sichere und vertrauenswürdige Apps identifizieren zu können.

Um die Sicherheit der eigenen App gegenüber dem Nutzer nachweisen zu können, hat die TÜV TRUST IT ein Testverfahren für Apps entwickelt, um die Einhaltung von Sicherheits- und Datenschutzkriterien zu zertifizieren. Das „Trusted App“-Siegel der TÜV TRUST IT zeigt, dass eine App sicher ist und keine Daten ausspäht oder andere unerwünschte Funktionen beinhaltet. In einem Zertifizierungsprojekt werden eine sicherheitstechnische Untersuchung der App sowie eine Quellcode-Analyse durchgeführt. Prüfgrundlagen hierfür sind Standards, Normen und Gesetze sowie etablierte Best Practices zur App-Sicherheit.

Die Prüfung der Apps erfolgt toolbasiert und manuell durch erfahrene Experten:

1. **Positiv-Prüfung (toolbasiert):** Überprüfung des App-Quellcodes auf korrekte Umsetzung der in Richtlinien bzw. in allgemein anerkannten Best Practices beschriebenen Implementierungsvorgaben.
2. **Negativ-Prüfung (durch TÜV-Experten):** Überprüfung des App-Quellcodes auf Verstoß gegen Richtlinien bzw. die Best Practices, z.B. durch die Verwendung eigener, von den Richtlinien abweichender Mechanismen (Implementierung eigener kryptographischer Verfahren, Verwendung nicht erlaubter Funktionen, etc.).
3. **Prüfung der Projekt-Metadaten (semiautomatisiert):** Überprüfung, ob die Projektkonfiguration geeignet ist, ein angemessenes Sicherheitsniveau herzustellen.
4. **Laufzeitprüfung (durch TÜV-Experten):** Prüfung auf Fehler u.a. in den Bereichen Event Handling, Netzwerkverkehr und Dateiablage.

Bei positivem Prüfergebnis auf Basis des aktuellen Anforderungskataloges „Trusted App“ der TÜV TRUST IT bescheinigen wir dies für die untersuchte Version der App in einem Zertifikat, das die Qualität der App dokumentiert.



Das Zertifikat ist gültig für die geprüfte Version der App. Zur Aufrechterhaltung der Zertifizierung für eine neue Version der App muss diese zur erneuten Prüfung eingereicht werden.

Selfcheck Development Risks

Werden mobile Anwendungen herausgegeben, die sich in der Praxis der Benutzer als sicherheitskritisch erweisen, kann ein erheblicher Imageschaden entstehen und die Entwicklungsaufwendungen nachträglich in Frage stellen. Mit diesem Selfcheck kann eine systematische Bewertung vorgenommen werden, ob die notwendigen Voraussetzungen zur Entwicklung sicherer Apps vorhanden sind bzw. wo ein konkreter Handlungsbedarf zur Optimierung besteht.

1. Sind in den Datenschutz- und Datensicherheitsrichtlinien des Unternehmens die mobilen Anwendungen explizit berücksichtigt? ☐ ☐
2. Besteht bei den auftragsgebenden Unternehmensbereichen die erforderliche Sensibilität für die Sicherheitsanforderungen von Apps? ☐ ☐
3. Werden in den technischen Konzeptionen von Apps grundsätzlich auch die erforderlichen Sicherheitsanforderungen in messbar definierter Form berücksichtigt? ☐ ☐
4. Beinhalten die entsprechenden Lastenhefte grundsätzlich einen entsprechenden sicherheitsspezifischen Anhang? ☐ ☐
5. Werden etablierte Expertensysteme zur Entwicklung sicherer mobiler Anwendungen eingesetzt? ☐ ☐
6. Sind in den Entwicklungsbudgets Aufwendungen für die Realisierung der Sicherheitsanforderungen enthalten? ☐ ☐
7. Verfügen die App-Entwickler über die notwendigen Kompetenzen zur Abbildung der Datenschutz- und Datensicherheitsanforderungen? ☐ ☐
8. Erfolgen vor dem Going-live der Apps systematische Sicherheitstests? ☐ ☐
9. Kann eine Sicherheitszertifizierung zur Vertrauens- und Imagebildung Ihrer Apps beitragen? ☐ ☐