audatis
Datenschutz und Informationssicherheit | CONSULTING

Whitepaper

Umsetzung von Datenschutz und IT-Sicherheit bei der App-Entwicklung

Zusammenfassung

Für fast alle Lebensbereiche existieren mobile Applikationen (Apps), welche mehr oder weniger personenbezogene und sensible Daten direkt auf dem Smartphone oder in der Cloud verarbeiten. Dabei spielt es bereits bei der Planung einer App eine wichtige Rolle, die Anforderungen des Datenschutzes auf Basis der EU Datenschutz-Grundverordnung (DS-GVO) sowie die Aspekte der Informationssicherheit zu berücksichtigen, unabhängig vom Einsatzgebiet der zukünftigen App.

Dieses Whitepaper skizziert, welche Aspekte schon vor der Umsetzung begutachtet werden sollten. Ferner finden Sie in diesem Whitepaper prägnant zusammengefasst einen grundsätzlichen Ansatz zur Planung und Umsetzung von mobilen Apps, unabhängig vom zugrundeliegenden Betriebssystem. Dabei wird auch eine Integration in agile Entwicklungsprojekte betrachtet.

Problemstellung

Software Entwicklungsprojekte sind häufig einem strengen Zeitplan unterworfen, was darin resultiert, dass grundsätzlich Fragen erst in einem fortgeschrittenen Stadium der entwickelten App gestellt werden. Dabei fällt die Umsetzung datenschutz- und informationssicherheitstechnischer Anforderungen deutlich unkomplizierter und effizienter aus, wenn eine Datenstrategie für das zu entwickelnde System festgelegt wurde.

Lösungsansatz für die App-Entwicklung

1) **Drei zentrale Fragen vor dem Start**
   a) Ist der Schutzbedarf der Daten in der App ermittelt?

      Daten können, unabhängig davon, ob Personenbezug existiert oder nicht, unterschiedlich kritisch sein. Machen Sie sich klar, **welche Daten Ihre App letztlich eigentlich verarbeiten wird**.

   b) Lokal oder Cloud?

      Werden Daten mit hohem Schutzbedarf verarbeitet, entstehen je nachdem welche Cloud-Strategie verfolgt wird, **unterschiedliche Gefährdungsszenarien** und daraus resultierende Sicherheitsanforderungen.

   c) Existiert genügend Expertise?

      Letztlich hängt die Sicherheit der App und der darin verarbeiteten Daten davon ab, wie ich sie schütze. Können rechtliche und technische Anforderungen in Entwicklungsanforderungen „übersetzt“ werden? Wie hoch ist die Security Awareness und das Verständnis von Datensicherheit des Development-Team (Dev-Team)? Aus beruflicher Erfahrung als Entwickler weiß ich, dass Entwicklern und Projektmanagern vor allem eines wichtig ist: Funktionierende Software. Dem steht nichts entgegen, dennoch können mangelnde Sicherheit den Ruf und die Authentizität des Unternehmens vehement gefährden.

2) **Datenstrategie erstellen, Entwicklung starten**

Zunächst sollten Sie die Datenstrategie erstellen und diese in die Praxis überführen. Helfen folgende Fragestellungen:

- Gibt es unterschiedlich kritische Daten (z.B. mit und ohne Personenbezug)? Sprechen Sie dazu unbedingt auch mit Ihrem Verantwortlichen für Datenschutz und Informationssicherheit.
- Wie wollen sie besonders kritische Daten schützen? Sind grundsätzlich Herangehensweisen für Speicherung und Transport von Daten definiert?

Formulieren Sie diese Aspekte in einem kleinen Whitepaper und integrieren Sie es verbindlich in Ihr Entwicklungsprojekt. Lassen Sie bei Bedarf Ihre Datenstrategie durch Experten beurteilen, dies erspart Ihnen im Nachhinein viel doppelte Arbeit.

Bevor Sie mit der Umsetzung beginnen, stellen Sie sicher, dass Ihr Dev-Team das Whitepaper und die darin vorgesehenen Regelungen verinnerlicht und diese in die Praxis überführen kann. Folgende Fragestellungen helfen bei der Sicherstellung:

- Können Mitarbeiter Daten korrekt identifizieren und den definierten Kategorien zuordnen?
- Kennen die Mitarbeiter Behandlungsweisen, die sie auf Daten anwenden sollen (insbesondere in Hinblick auf Vertraulichkeit, Verfügbarkeit und Integrität)

Sind diese Punkte sichergestellt, steht dem Systemdesign nichts mehr im Weg. Die Einhaltung Ihrer Datenstrategie durch die Entwicklung sollten Sie selbstverständlich überprüfen.

3) Rechtliche Anforderungen erfüllen

Die rechtlichen Anforderungen an Ihre App sollten sie regelmäßig im Entwicklungsprozess mit einbeziehen. Folgende Fragen helfen Ihnen dabei:

- Sind die Datenschutzgrundsätze gem. Art. 5 DS-GVO erfüllt?
- Sind (für Deutschland) die Anforderungen des TMG erfüllt?
- Sind die Rechte betroffener Personen gem. Artt. 12-21 DS-GVO umgesetzt?
- Unterliegen Sie mit der Applikation weiteren branchenspezifischen Gesetzen (z.B. bei kritischen Infrastrukturen, Gesundheits- oder Finanzeinrichtungen)?
- Verarbeiten Sie personenbezogene Daten in Staaten außerhalb der EU und des EWR?

4) Security in a nutshell

Die oben beschriebene Vorgehensweise hilft Ihnen eine grundsätzliche Herangehensweise für Datenschutz und Informationssicherheit zu erarbeiten. Die überaus komplexe Anforderungsstruktur erstreckt sich dabei auf diverse Themen. Die folgende Checkliste fasst prägnant zusammen, welchen Themen Sie Aufmerksamkeit schenken sollten. Die Reihenfolge ist dabei nicht ausschlaggebend:

- Identitäts- und Berechtigungsmanagement
- Zugangsdaten und Authentisierung
- Datenübertragung und -transport
- Datensicherung und -wiederherstellung
- Tracking und Tracing

Folgen Sie bei diesen Themen der oben eingeführten Herangehensweise an Sicherheitsthemen, wird Ihre App ein gehöriges Maß an „security increase“ verzeichnen. Dennoch sollten Sie bedenken, dass die IT-Welt eine schnelllebige Welt ist. Die mobile Welt lebt noch schneller und mit ihr die Gefährdungen und Anforderungen an Sicherheit Ihrer und unserer aller Daten. Lassen Sie Ihr System deshalb immer auch von externen Stellen mit Hilfe von Penetrationtests überprüfen. Dies hilft Ihnen, Schwachstellen zu identifizieren und Ihre erarbeiteten Konzepte weiterzuentwickeln.

Autor und Ansprechpartner

Sascha Knicker
Senior Consultant Datenschutz und Informationssicherheit

Schwerpunkte: Datenschutz, TISAX, ISO 27001

Mail: s.knicker@audatis.de
Fon: 05221 87292-07

LinkedIn | Twitter | XING

Haben Sie noch Fragen?

Wir haben versucht, alle wichtigen Aspekte in unserem Whitepaper möglichst verständlich aufzubereiten.

Sollten Sie dennoch Fragen oder Beratungsbedarf haben, nehmen Sie gerne mit uns Kontakt auf.

Wir unterstützen Sie gerne bei der Planung von datenschutzkonformen und sicheren Apps und der Beantwortung aller Fragen in Bezug auf die pragmatische Umsetzung des Datenschutzes und der Informationssicherheit.

Die audatis Consulting GmbH ist als Beratungsunternehmen auf die Bereiche Datenschutz und Informationssicherheit spezialisiert und betreut Kunden im In- und Ausland bereits seit 2011.

Neben der Stellung des externen Datenschutzbeauftragten begleiten und beraten wir Unternehmen, öffentliche Stellen und kirchliche Einrichtungen bei der Umsetzung des Datenschutzes, der Informationssicherheit und der Digitalisierung.

Als Teil der audatis Group hat die audatis Consulting GmbH Ihren Sitz im ostwestfälischen Herford und betreibt eine Niederlassung in Potsdam.

audatis® Datenschutz und Informationssicherheit | CONSULTING

audatis Consulting GmbH
Luisenstr. 1
32052 Herford
Deutschland

Fon: 05221 872 92-0
Fax: 05221 872 92-49

Mail: info@audatis.de
Web: www.audatis.de