APP.1.4: Mobile Anwendungen (Apps)

1 Beschreibung

1.1 Einleitung

Smartphones, Tablets und ähnliche mobile Geräte sind heute auch in Behörden und Unternehmen weit verbreitet. Mitarbeiter können so unabhängig von Ort und Zeit auf Daten der Institution, auf Informationen und Anwendungen zugreifen.

Mobile Anwendungen (Applikationen, kurz Apps) sind Anwendungen, die auf mobil genutzten Betriebssystemen wie iOS oder Android auf entsprechenden Endgeräten installiert und ausgeführt werden. Apps werden üblicherweise aus sogenannten App Stores bezogen. Diese werden von den Herstellern der mobil genutzten Betriebssysteme und Endgeräte betrieben und gepflegt. Im professionellen Umfeld ist es aber auch üblich, Apps selbst zu entwickeln und z. B. über Mobile-Device-Management-Lösungen (MDM) auf den Endgeräten zu installieren und zu verwalten. Im Vergleich zu Anwendungen auf Desktop-Betriebssystemen unterliegen Apps unter iOS oder Android besonderen Rahmenbedingungen, wie etwa einem durch das Betriebssystem sichergestellten Berechtigungsmanagement.

Für die unterschiedlichen mobilen Betriebssysteme gibt es mittlerweile eine große Auswahl an verfügbaren Apps. Auch gibt es standardisierte Bibliotheken und Entwicklungsumgebungen, mit deren Hilfe sich Apps im Vergleich zu klassischen Anwendungen schnell selbst entwickeln lassen.

1.2 Zielsetzung

Ziel dieses Bausteins ist es, Informationen zu schützen, die auf mobilen Endgeräten mit Apps verarbeitet werden. Auch die Einbindung von Apps in eine bestehende IT-Infrastruktur wird dabei betrachtet. Der Baustein definiert zudem Anforderungen, um Apps richtig auszuwählen und sicher betreiben zu können. Dabei werden die Apps unabhängig von ihrer Quelle (App Store oder eigene Installation) betrachtet.

1.3 Abgrenzung und Modellierung

Der Baustein APP.1.4 *Mobile Anwendungen (Apps)* ist auf alle Anwendungen anzuwenden, die auf mobilen Endgeräten eingesetzt werden.

Der Baustein betrachtet Apps unter mobilen Betriebssystemen wie iOS und Android. Anforderungen, welche die zugrundeliegenden Betriebssysteme betreffen, werden hier nicht berücksichtigt. Diese Anforderungen finden sich beispielsweise in den Bausteinen SYS.3.2.3 *iOS (for Enterprise)* sowie

SYS.3.2.4 *Android*. Oft werden Apps zentral über ein Mobile Device Management verwaltet. Anforderungen hierzu können dem Baustein SYS.3.2.2 *Mobile Device Management (MDM)* entnommen werden.

Ebenso sind anwendungsspezifische Aspekte von Apps nicht Gegenstand des Bausteins zu mobilen Anwendungen. Diese werden in den entsprechenden Bausteinen der Schicht APP *Anwendungen, wie z. B.* APP.1.2 *Web-Browser* behandelt.

Apps greifen häufig auf Backend-Systeme oder Server bzw. Anwendungsdienste zurück. Werden die Backend-Systeme oder Server selber betrieben, werden Sicherheitsempfehlungen dazu nicht an dieser Stelle gegeben, sondern in den entsprechenden Bausteinen des IT-Grundschutz-Kompendiums. Dazu gehören beispielsweise APP.3.1 *Webanwendungen*, APP.3.5 *Webservices* oder APP.4.3 *Relationale Datenbanksysteme*. Zusätzlich sollten die Bausteine berücksichtigt werden, die sich mit allgemeinen Aspekten von Anwendungen befassen, etwa OPS.1.1.6 *Software-Tests und -Freigaben* oder APP.6 *Allgemeine Software*, da diese Aspekte nicht im vorliegenden Baustein berücksichtigt werden. Bei der Entwicklung eigener Apps sollten die Anforderungen des Bausteins CON.8 *Software-Entwicklung* berücksichtigt werden.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein APP.1.4 *Mobile Anwendungen (Apps)* von besonderer Bedeutung:

2.1 Ungeeignete Auswahl von Apps

Die ausgewählten Apps wirken sich stark auf die damit verarbeiteten Informationen, auf das mobile Endgerät sowie häufig auf die IT-Infrastruktur der Institution aus. Wird dies bei der Auswahl der Apps nicht berücksichtigt, können weitreichende Probleme entstehen. Besonders hoch ist die Gefahr, wenn es sich dabei um Apps handelt, die nicht eigens für die abzubildenden Geschäftsprozesse entwickelt wurden. So könnten beispielsweise die für den Betrieb einer App erforderlichen Voraussetzungen nicht ausreichend betrachtet werden. Möglicherweise ist dann z. B. die mobile Netzanbindung nicht leistungsfähig genug oder die Hardware nicht kompatibel. Apps können auch dann ungeeignet sein, wenn sie keine ausreichende langfristige Einsatzstabilität und -planung bieten oder vom Hersteller nicht ausreichend gepflegt werden.

2.2 Zu weitreichende Berechtigungen

Apps benötigen bestimmte Berechtigungen, um auf bestimmte Funktionen und Dienste zugreifen zu können. So kann eine App in der Regel immer auf die Internetverbindung des mobilen Endgeräts zugreifen. Der Standort oder das Adressbuch müssen hingegen meist gesondert freigegeben werden. Werden Apps eingesetzt, die zu weitgehende Berechtigungen erfordern, oder werden die Berechtigungen nicht ausreichend eingeschränkt, so kann sich das insbesondere auf die Vertraulichkeit und Integrität der Informationen auf dem Endgerät auswirken. Apps können zudem Informationen an unberechtigte Dritte weitergeben, wie z. B. den Standort, Fotos oder Kontakt- und Kalenderdaten. Außerdem sind Apps in der Lage, lokal abgespeicherte Daten zu verändern oder zu löschen. Schließlich können Apps auch Kosten verursachen, etwa durch Telefonanrufe, versendete SMS oder In-App-Käufe.

2.3 Ungewollte Funktionen in Apps

Zwar prüfen manche App-Store-Betreiber die angebotenen Apps, dennoch können diese Sicherheitslücken oder bewusst eingesetzte Schadfunktionen enthalten. Das Risiko ist insbesondere dann hoch, wenn Apps aus ungeprüften oder unzuverlässigen Quellen bezogen werden. Dann kann die Vertraulichkeit, Integrität und Verfügbarkeit der Informationen gefährdet werden.

2.4 Software-Schwachstellen und Fehler in Apps

Apps können Schwachstellen enthalten, über die sie direkt am Gerät oder über Netzverbindungen angegriffen werden können. Außerdem werden viele Apps nach einiger Zeit von ihren Entwicklern nicht mehr weiter gepflegt. Dadurch werden erkannte Sicherheitsmängel nicht mehr durch entsprechende Updates behoben.

2.5 Unsichere Speicherung lokaler Anwendungsdaten

Einige Apps speichern Daten auf dem Endgerät, beispielsweise Benutzerprofile oder Dokumente. Falls diese Daten unzureichend geschützt sind, können möglicherweise andere Apps darauf zugreifen. Dies betrifft neben bewusst abgelegten Daten auch temporäre Daten, wie beispielsweise im Cache zwischengespeicherte Informationen. Auch sind sie für Unberechtigte leicht lesbar, z. B. wenn ein Mitarbeiter sein Gerät verloren hat. Außerdem werden lokal gespeicherte Informationen oft nicht im Datensicherungskonzept berücksichtigt. Fällt das Endgerät aus oder geht verloren, sind die lokal gespeicherten Informationen ebenfalls nicht mehr verfügbar.

2.6 Ableitung vertraulicher Informationen aus Metadaten

Durch Apps sammeln sich viele Metadaten an. Mithilfe dieser Metadaten können Dritte auf vertrauliche Informationen schließen, z. B. über Telefon- und Netzverbindungen, Bewegungsdaten oder besuchte Webseiten. Daraus lassen sich dann weitere Informationen ableiten, beispielsweise die Organisationsstruktur der Institution, genaue Positionen von Standorten sowie deren personelle Besetzung.

2.7 Abfluss von vertraulichen Daten

Daten werden über verschiedene Wege von und zu einer App übertragen. Dafür stellen mobile Betriebssysteme verschiedene Schnittstellen bereit. Der Benutzer hat ebenfalls verschiedene Möglichkeiten, Daten mit einer App auszutauschen, etwa lokal über eine Speicherkarte, die Zwischenablage, die Gerätekamera oder andere Anwendungen. Außerdem können Daten über Cloud-Dienste oder Server des App- oder Geräte-Anbieters übertragen werden. Darüber können Dritte Zugriff auf die vertraulichen Daten erlangen. Schließlich kann auch das Betriebssystem selbst Daten für den schnelleren Zugriff zwischenspeichern (Caching). Dabei können Daten versehentlich abfließen oder Angreifer auf vertrauliche Informationen zugreifen.

2.8 Unsichere Kommunikation mit Backend-Systemen

Viele Apps kommunizieren mit Backend-Systemen, über die Daten mit dem Datennetz der Institution ausgetauscht werden. Die Daten werden bei mobilen Geräten zumeist über unsichere Netze wie ein Mobilfunknetz oder WLAN-Hotspots übertragen. Werden für die Kommunikation mit Backend-Systemen aber unsichere Protokolle verwendet, können Informationen abgehört oder manipuliert werden.

2.9 Kommunikationswege außerhalb der Infrastruktur der Institution

Wenn Apps unkontrolliert mit Dritten kommunizieren können, kann dies Kommunikationswege schaffen, die nicht von der Institution erkannt und kontrolliert werden können. So kann ein Benutzer beispielsweise die App eines Cloud-Datenspeicherdienstes nutzen, um Informationen vom Endgerät nach außen zu übertragen. Auch die enge Verzahnung von Social-Media-Diensten mit vielen Apps erschwert die Kontrolle, ob und wie Informationen das Endgerät verlassen. Diese Art von Kommunikationswegen sind nur schwer nachzuvollziehen. Dies kann noch weitere Probleme verursachen, etwa wenn der Anwender oder die Institution verpflichtet sind, Informationen oder Vorgänge zu archivieren.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins APP.1.4 *Mobile Anwendungen (Apps)* aufgeführt. Grundsätzlich ist der IT-Betrieb für die Erfüllung der Anforderungen zuständig. Der Informationssicherheitsbeauftragte (ISB) ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür zuständig, dass alle Anforderungen gemäß dem festgelegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Zuständigkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Zuständigkeiten	**Rollen**
Grundsätzlich zuständig	IT-Betrieb
Weitere Zuständigkeiten	Fachverantwortliche

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein APP.1.4 *Mobile Anwendungen (Apps)* vorrangig erfüllt werden:

APP.1.4.A1 Anforderungsanalyse für die Nutzung von Apps [Fachverantwortliche] (B)

In der Anforderungsanalyse MÜSSEN insbesondere Risiken betrachtet werden, die sich aus der mobilen Nutzung ergeben. Die Institution MUSS prüfen, ob ihre Kontroll- und Einflussmöglichkeiten auf die Betriebssystemumgebung mobiler Endgeräte ausreichend sind, um sie sicher nutzen zu können.

APP.1.4.A2 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.1.4.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.1.4.A5 Minimierung und Kontrolle von App-Berechtigungen [Fachverantwortliche] (B)

Sicherheitsrelevante Berechtigungseinstellungen MÜSSEN so fixiert werden, dass sie nicht durch Benutzer oder Apps geändert werden können. Wo dies technisch nicht möglich ist, MÜSSEN die Berechtigungseinstellungen regelmäßig geprüft und erneut gesetzt werden.

Bevor eine App in einer Institution eingeführt wird, MUSS sichergestellt werden, dass sie nur die minimal benötigten App-Berechtigungen für ihre Funktion erhält. Nicht unbedingt notwendige Berechtigungen MÜSSEN hinterfragt und gegebenenfalls unterbunden werden.

APP.1.4.A6 ENTFALLEN (B)

Diese Anforderung ist entfallen.

APP.1.4.A7 Sichere Speicherung lokaler App-Daten (B)

Wenn Apps auf interne Dokumente der Institution zugreifen können, MUSS sichergestellt sein, dass die lokale Datenhaltung der App angemessen abgesichert ist. Insbesondere MÜSSEN Zugriffsschlüssel verschlüsselt abgelegt werden. Außerdem DÜRFEN vertrauliche Daten NICHT vom Betriebssystem an anderen Ablageorten zwischengespeichert werden.

APP.1.4.A8 Verhinderung von Datenabfluss (B)

Um zu verhindern, dass Apps ungewollt vertrauliche Daten versenden oder aus den gesendeten Daten Profile über die Benutzer erstellt werden, MUSS die App-Kommunikation geeignet eingeschränkt werden. Dazu SOLLTE die Kommunikation im Rahmen des Test- und Freigabeverfahrens analysiert

werden. Weiterhin SOLLTE überprüft werden, ob eine App ungewollte Protokollierungs- oder Hilfsdateien schreibt, die möglicherweise vertrauliche Informationen enthalten.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein APP.1.4 *Mobile Anwendungen (Apps)*. Sie SOLLTEN grundsätzlich erfüllt werden.

APP.1.4.A3 Verteilung schutzbedürftiger Apps (S)
Interne Apps der Institution und Apps, die schutzbedürftige Informationen verarbeiten, SOLLTEN über einen institutionseigenen App Store oder via MDM verteilt werden.

APP.1.4.A9 ENTFALLEN (S)
Diese Anforderung ist entfallen.

APP.1.4.A10 ENTFALLEN (S)
Diese Anforderung ist entfallen.

APP.1.4.A11 ENTFALLEN (S)
Diese Anforderung ist entfallen.

APP.1.4.A12 Sichere Deinstallation von Apps (S)
Werden Apps deinstalliert, SOLLTEN auch Daten gelöscht werden, die auf externen Systemen, beispielsweise beim App-Anbieter, gespeichert wurden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein APP.1.4 *Mobile Anwendungen (Apps)* exemplarische Vorschläge für Anforderungen aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und BEI ERHÖHTEM SCHUTZBEDARF in Betracht gezogen werden SOLLTEN. Die konkrete Festlegung erfolgt im Rahmen einer Risikoanalyse.

APP.1.4.A13 ENTFALLEN (H)
Diese Anforderung ist entfallen.

APP.1.4.A14 Unterstützung zusätzlicher Authentisierungsmerkmale bei Apps (H)
Falls möglich, SOLLTE für die Authentisierung der Benutzer in Apps ein zweiter Faktor benutzt werden. Hierbei SOLLTE darauf geachtet werden, dass eventuell benötigte Sensoren oder Schnittstellen in allen verwendeten Geräten vorhanden sind. Zusätzlich SOLLTE bei biometrischen Verfahren berücksichtigt werden, wie resistent die Authentisierung gegen mögliche Fälschungsversuche ist.

APP.1.4.A15 Durchführung von Penetrationstests für Apps (H)
Bevor eine App für den Einsatz freigegeben wird, SOLLTE ein Penetrationstest durchgeführt werden. Dabei SOLLTEN alle Kommunikationsschnittstellen zu Backend-Systemen sowie die lokale Speicherung von Daten auf mögliche Sicherheitslücken untersucht werden. Die Penetrationstests SOLLTEN regelmäßig und zusätzlich bei größeren Änderungen an der App wiederholt werden.

APP.1.4.A16 Mobile Application Management (H)
Falls möglich, SOLLTE für das zentrale Konfigurieren von dienstlichen Apps ein Mobile Application Management verwendet werden.

4 Weiterführende Informationen

4.1 Wissenswertes

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (Bitkom) stellt mit dem Leitfaden „Apps & Mobile Services – Tipps für Unternehmen“ (2. Auflage, 2014) eine

Entscheidungshilfe zum Thema Apps und Mobile Services in Unternehmen bereit.

Das Information Security Forum (ISF) bietet eine Broschüre mit dem Titel „ Securing Mobile Apps – Embracing mobile, balancing control“ (2018) an.

Auch die „NIST Special Publication 800-163: Vetting the Security of Mobile Applications“ (2015) bietet weiterführende Informationen zum Thema Apps.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die Kreuzreferenztabelle enthält die Zuordnung von elementaren Gefährdungen zu den Anforderungen. Anhand dieser Tabelle lässt sich ermitteln, welche elementaren Gefährdungen durch welche Anforderungen abgedeckt sind. Durch die Umsetzung der aus den Anforderungen abgeleiteten Sicherheitsmaßnahmen wird den entsprechenden elementaren Gefährdungen entgegengewirkt. Die Buchstaben in der zweiten Spalte (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit) zeigen an, welche Grundwerte der Informationssicherheit durch die Anforderung vorrangig geschützt werden. Die folgenden elementaren Gefährdungen sind für den Baustein APP.1.4 *Mobile Anwendungen (Apps)* von Bedeutung.

G 0.9	Ausfall oder Störung von Kommunikationsnetzen
G 0.14	Ausspähen von Informationen (Spionage)
G 0.15	Abhören
G 0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten
G 0.17	Verlust von Geräten, Datenträgern oder Dokumenten
G 0.18	Fehlplanung oder fehlende Anpassung
G 0.19	Offenlegung schützenswerter Informationen
G 0.20	Informationen oder Produkte aus unzuverlässiger Quelle
G 0.21	Manipulation von Hard- oder Software
G 0.23	Unbefugtes Eindringen in IT-Systeme
G 0.25	Ausfall von Geräten oder Systemen
G 0.26	Fehlfunktion von Geräten oder Systemen
G 0.28	Software-Schwachstellen oder -Fehler
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen
G 0.32	Missbrauch von Berechtigungen
G 0.36	Identitätsdiebstahl
G 0.38	Missbrauch personenbezogener Daten
G 0.39	Schadprogramme
G 0.42	Social Engineering