Bundesamt
für Sicherheit in der
Informationstechnik

SYS.3.2: Tablet und Smartphone

SYS.3.2.3: iOS (for Enterprise)

1 Beschreibung

1.1 Einleitung

Aufgrund von modernen, einfachen Bedienkonzepten sowie ihrer hohen Leistungsfähigkeit sind Smartphones und Tablets heutzutage weit verbreitet. Dazu zählen auch die von der Firma Apple produzierten Mobilgeräte iPhone und iPad mit den Betriebssystemen iOS und iPadOS. Da iPadOS auf iOS basiert, werden beide in diesem Baustein zur einfachen Lesbarkeit als „iOS“ zusammengefasst. Die beiden Betriebssysteme haben aktuell vor allem funktionale Unterschiede, die den abweichenden Formfaktor der Geräte berücksichtigen.

Ursprünglich wurden diese Geräte für den privaten Gebrauch konzipiert. Durch die Umgestaltung der Infrastrukturen und die Art der Informationserhebung und -verarbeitung werden sie jedoch immer häufiger auch im beruflichen Umfeld verwendet und lösen teilweise sogar Notebooks ab.

Durch die Integration von Business-Funktionen wurde iOS seit der Version 4 schrittweise für den Einsatz in Unternehmen und Behörden ausgebaut und Funktionen für die Verwaltung aus Sicht einer Institution integriert. Hierzu gehören die Möglichkeit zur zentralisierten Geräteregistrierung (Apple Business Manager) sowie Optionen wie Single Sign-On (SSO).

1.2 Zielsetzung

Ziel dieses Bausteins ist es, aufzuzeigen, wie mit iOS (for Enterprise) betriebene Geräte sicher in Institutionen eingesetzt werden können. Dazu werden Anforderungen für Einstellungen der iOS-basierten Endgeräte aufgestellt, die in Form von Konfigurationsprofilen auf den Endgeräten verteilt werden können. iOS-Konfigurationsprofile enthalten einheitlich definierte Einstellungen, z. B. für Sicherheitsrichtlinien oder einzelne Systemaspekte, um iOS-basierte Geräte einheitlich und zentral zu verwalten und automatisch zu konfigurieren.

1.3 Abgrenzung und Modellierung

Der Baustein SYS.3.2.3 *iOS (for Enterprise)* ist für alle dienstlich verwendeten Smartphones und Tablets mit dem Betriebssystem Apple iOS anzuwenden.

Dieser Baustein enthält grundsätzliche Anforderungen, die beim Betrieb von iOS-basierten Geräten, die in die Prozesse der Institution integriert sind, zu beachten und zu erfüllen sind. Anforderungen an die Integration in die Sicherheits- oder Kollaborationsinfrastruktur der Institution stehen nicht im Fokus dieses Bausteins. Mit einem sogenannten „Mobile Device Management“ (MDM) besteht die Möglichkeit, die Geräte zentral zu verwalten und Konfigurationsprofile pro Benutzergruppe oder Einsatzzweck auszurollen. Über ein MDM lassen sich auch Sicherheitsmaßnahmen einheitlich umsetzen. Dieser

Baustein setzt voraus, dass zu verwaltende iOS-Geräte in eine MDM-Infrastruktur integriert sind. Wird eine geringe Anzahl von Geräten verwaltet, können diese aus wirtschaftlichen Gründen ausnahmsweise ohne MDM eingesetzt werden. Anforderungen für den Betrieb von MDM finden sich im Baustein SYS.3.2.2 *Mobile Device Management (MDM)*. Für kleinere Umgebungen kann der Apple Configurator verwendet werden, um die in diesem Baustein aufgeführten Anforderungen auf mehreren Endgeräte einheitlich umzusetzen. Allgemeine und übergreifende Aspekte zum Betrieb von Smartphones und Tablets, unabhängig vom darauf eingesetzten Betriebssystem, finden sich im Baustein SYS.3.2.1 *Allgemeine Smartphones und Tablets* und sind ebenfalls umzusetzen, wenn iOS-basierte Geräte verwendet werden.

Für die Nutzung von biometrischen Authentisierungsmechanismen enthält der Baustein SYS.3.2.1 *Allgemeine Smartphones und Tablets* entsprechende Anforderungen.

2 Gefährdungslage

Folgende spezifische Bedrohungen und Schwachstellen sind für den Baustein SYS.3.2.3 *iOS (for Enterprise)* von besonderer Bedeutung:

2.1 Risikokonzentration durch ein Benutzerkonto (Apple-ID) für alle Apple-Dienste

Mit der Apple-ID gibt es einen zentralen Zugang zu allen von der Firma Apple zur Verfügung gestellten Diensten (z. B. „iMessage“, „FaceTime“, „iCloud“, „App Store“, „iTunes“, „iBook-Store“, „iPhone-Suche“ oder Synchronisationsdienste). Wenn Unbefugte auf eine nicht ausreichend abgesicherte Apple-ID zugreifen können, können sie diese Apple-Dienste unter Umständen nutzen, die Verfügbarkeit der Apple-ID-basierten Dienste stören, iOS-basierte Geräte aus der Ferne lokalisieren oder auf Werkseinstellungen zurücksetzen sowie auf Informationen des Cloud-Dienstes iCloud zugreifen. Insbesondere ist es einem Angreifer bei aktivierten iCloud-Backups möglich, die gespeicherten Daten auf ein eigenes iOS-Gerät zu klonen.

2.2 Feste Integration von vorinstallierten Apps und deren Funktionen

Mit iOS liefert Apple bereits fest integrierte und vorinstallierte Apps (z. B. „Mail“ und „Safari“) aus. Diese Apps werden teilweise mit höheren Berechtigungen als die aus dem App Store herunterladbaren Apps ausgeführt, wodurch sich die Angriffsfläche des iOS-basierten Geräts vergrößert.

2.3 Missbräuchlicher Zugriff auf ausgelagerte Daten

Für eine Reihe iOS-spezifischer Funktionen muss die von der Firma Apple betriebene Infrastruktur verwendet werden. Werden die Funktioen „iCloud-Schlüsselbund“, „iMessage“, „FaceTime“, „Siri“, „Continuity“, „Spotlight-Vorschläge“ sowie Funktionen der iCloud zum Anlegen von Backups oder zum gemeinsamen Arbeiten an Dokumenten verwendet, werden die Daten zwischen unterschiedlichen Geräten oder Benutzern stets über die Infrastruktur der Firma Apple synchronisiert. Ebenfalls werden Push-Nachrichten für iOS-basierte Geräte über diese Infrastruktur weitergeleitet. Es besteht somit prinzipiell die Gefahr, dass auf Apple-Server zugegriffen wird und die dort gespeicherten oder übertragenen Daten für andere Zwecke missbraucht werden.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen des Bausteins SYS.3.2.3 *iOS (for Enterprise)* 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	

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein SYS.3.2.3 *iOS (for Enterprise)* vorrangig erfüllt werden:

SYS.3.2.3.A1 Strategie für die iOS-Nutzung (B)

Wird ein MDM eingesetzt, so MÜSSEN die iOS-basierten Geräte über das MDM verwaltet und konfiguriert werden. Hierzu MUSS eine Strategie zur iOS-Nutzung vorliegen, in der Aspekte wie die Auswahl der Endgeräte oder Strategien für Datensicherungen festgelegt werden. Es MUSS geregelt werden, ob zusätzliche Apps von Drittanbietern genutzt werden sollen bzw. dürfen. Außerdem MÜSSEN Jailbreaks organisatorisch untersagt und nach Möglichkeit technisch verhindert werden.

SYS.3.2.3.A2 Planung des Einsatzes von Cloud-Diensten (B)

Bevor iOS-basierte Geräte verwendet werden, MUSS festgelegt werden, welche Cloud-Services in welchem Umfang genutzt werden sollen bzw. dürfen. Dabei SOLLTE berücksichtigt werden, dass iOS-basierte Geräte grundsätzlich eng mit iCloud-Diensten des Herstellers Apple verzahnt sind. Außerdem SOLLTE berücksichtigt werden, dass beispielsweise bereits die Aktivierung von Einzelgeräten mit einer Apple-ID hiervon betroffen ist. Daher SOLLTE geprüft werden, ob zur Geräteregistrierung Apple Business Manager (früher Device Enrollment Program, DEP) genutzt werden kann.

SYS.3.2.3.A3 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.3.2.3.A4 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.3.2.3.A5 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.3.2.3.A6 ENTFALLEN (B)

Diese Anforderung ist entfallen.

SYS.3.2.3.A7 Verhinderung des unautorisierten Löschens von Konfigurationsprofilen (B)

Damit Konfigurationsprofile nicht unautorisiert gelöscht werden können, MÜSSEN geeignete technische (z. B. durch den betreuten Modus) oder organisatorische Maßnahmen getroffen und umgesetzt werden. Benutzer von mobilen Endgeräten SOLLTEN für den Sinn und Zweck der Sicherheitsmaßnahmen sensibilisiert werden.

SYS.3.2.3.A8 ENTFALLEN (B)

Diese Anforderung ist entfallen.

3.2 Standard-Anforderungen

Gemeinsam mit den Basis-Anforderungen entsprechen die folgenden Anforderungen dem Stand der Technik für den Baustein SYS.3.2.3 *iOS (for Enterprise)*. Sie SOLLTEN grundsätzlich erfüllt werden.

SYS.3.2.3.A9 ENTFALLEN (S)

Diese Anforderung ist entfallen.

SYS.3.2.3.A10 ENTFALLEN (S)
Diese Anforderung ist entfallen.

SYS.3.2.3.A11 ENTFALLEN (S)
Diese Anforderung ist entfallen.

SYS.3.2.3.A12 Verwendung von Apple-IDs (S)
Statt einer persönlichen Apple-ID des Benutzers SOLLTE eine anonymisierte Apple-ID verwendet werden. Falls möglich, SOLLTE der Apple Business Manager für Volumenlizenzen (früher Volume Purchase Program, VPP) sowie eine zentralisierte Installation von Apps verwendet werden.

SYS.3.2.3.A13 Verwendung der Konfigurationsoption „Einschränkungen unter iOS“ (S)
Alle nicht benötigten oder erlaubten Funktionen bzw. Dienste von iOS SOLLTEN deaktiviert werden. Basierend auf dem Einsatzzweck und dem zugrundeliegenden Schutzbedarf SOLLTE geprüft werden, welche der Funktionen „Sperrbildschirm“, „Unified Communication“, „Siri“, „Hintergrundbild“, „Verbindung mit Host-Systemen“ und „Diagnose- und Nutzungsdaten“ einzusetzen sind.

SYS.3.2.3.A14 Verwendung der iCloud-Infrastruktur (S)
Bevor die umfängliche oder selektive Nutzung der iCloud-Infrastruktur für eine dienstliche Nutzung freigegeben wird, SOLLTE bewertet werden, ob die allgemeinen Geschäftsbedingungen der Firma Apple mit den internen Richtlinien hinsichtlich Verfügbarkeit, Vertraulichkeit, Integrität und Datenschutz vereinbar sind. Wird die Nutzung der iCloud-Infrastruktur erlaubt, SOLLTE die Identität am iCloud-Webservice durch eine Zwei-Faktor-Authentisierung geprüft werden. Ansonsten SOLLTE die iCloud-Nutzung für einen rein dienstlichen Bedarf auf ein geringes Maß reduziert oder komplett ausgeschlossen werden.

SYS.3.2.3.A15 Verwendung der Continuity-Funktionen (S)
Wurde die Nutzung der iCloud-Infrastruktur nicht grundsätzlich durch das Sicherheitsmanagement der Institution untersagt, SOLLTE die Vereinbarkeit der Continuity-Funktionen mit den internen Richtlinien unter Berücksichtigung der Aspekte Vertraulichkeit und Integrität bewertet werden. Auf Basis der Bewertungsergebnisse SOLLTE geregelt werden, inwieweit diese Funktionen technisch bzw. organisatorisch eingeschränkt werden.

SYS.3.2.3.A16 ENTFALLEN (S)
Diese Anforderung ist entfallen.

SYS.3.2.3.A17 Verwendung der Gerätecode-Historie (S)
Im Konfigurationsprofil SOLLTE die Anzahl der eindeutigen Codes bis zur ersten Wiederholung auf einen angemessenen Wert festgelegt sein.

SYS.3.2.3.A18 Verwendung der Konfigurationsoption für den Browser Safari (S)
Die bereits in der Institution etablierten Browserrichtlinien SOLLTEN entsprechend auch für Safari durch technische und organisatorische Maßnahmen umgesetzt werden. Dabei SOLLTEN die bereits etablierten Anforderungen für Browser auf stationären und tragbaren PCs als Grundlage für die Absicherung der iOS-basierten Geräte dienen sowie die Einsatzszenarien. Das Einsatzumfeld der Geräte SOLLTE beachtet werden.

SYS.3.2.3.A19 ENTFALLEN (S)
Diese Anforderung ist entfallen.

SYS.3.2.3.A20 ENTFALLEN (S)
Diese Anforderung ist entfallen.

SYS.3.2.3.A21 Installation von Apps und Einbindung des Apple App Stores (S)
Um sicherzustellen, dass den autorisierten Benutzern die benötigten Apps zum notwendigen Zeitpunkt ausreichend zur Verfügung stehen, SOLLTE überlegt werden, den Apple Business Manager in die MDM-

Infrastruktur zu integrieren. Zahlungen im App Store SOLLTE NICHT über biometrische Verfahren bestätigt werden.

3.3 Anforderungen bei erhöhtem Schutzbedarf

Im Folgenden sind für den Baustein SYS.3.2.3 *iOS (for Enterprise)* 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.

SYS.3.2.3.A22 ENTFALLEN (H)
Diese Anforderung ist entfallen.

SYS.3.2.3.A23 Verwendung der automatischen Konfigurationsprofillöschung (H)
Geräte, die über einen klar definierten Zeitraum durchgängig offline sind, SOLLTEN ihren Zugang zur internen Infrastruktur verlieren. Nach Ablauf des definierten Zeitraums oder an einem bestimmten Tag, SOLLTE das Konfigurationsprofil ohne Zutun der IT-Zuständigen gelöscht werden. Falls der Benutzer des Geräts vor Ablauf der Frist auf das interne Netz zugreift, SOLLTE der Zeitraum bis zur automatischen Löschung des Konfigurationsprofils erneuert werden. Falls sicherzustellen ist, ob der Benutzer noch im Besitz des Gerätes ist, SOLLTE der Benutzer aktiv zum Zugriff innerhalb einer Frist aufgefordert werden. Falls die Frist ohne Zugriff verstricht, sollte das Konfigurationsprofil dieses Benutzers automatisch gelöscht werden.

SYS.3.2.3.A24 ENTFALLEN (H)
Diese Anforderung ist entfallen.

SYS.3.2.3.A25 Verwendung der Konfigurationsoption für AirPrint (H)
Freigegebene AirPrint-Drucker SOLLTEN dem Benutzer durch ein Konfigurationsprofil bereitgestellt werden. Um zu vermeiden, dass Informationen auf nicht vertrauenswürdigen Druckern von Benutzern ausgedruckt werden können, SOLLTEN stets alle Kommunikationsverbindungen über die Infrastruktursysteme der Institution geführt werden.

SYS.3.2.3.A26 Keine Verbindung mit Host-Systemen (H)
Um zu vermeiden, dass iOS-basierte Geräte unautorisiert mit anderen IT-Systemen verbunden werden, SOLLTEN die Benutzer iOS-basierte Geräte ausschließlich mit dem MDM verbinden können.

SYS.3.2.3.A27 ENTFALLEN (H)
Diese Anforderung ist entfallen.

4 Weiterführende Informationen

4.1 Wissenswertes

Das BSI hat in den „BSI-Veröffentlichungen zur Cyber-Sicherheit“ das Dokument BSI-CS 074: „iOS-Konfigurationsempfehlung auf Basis betriebssystemeigener Mittel für eine Nutzung mit erhöhter Sicherheit“ (Stand 2015) veröffentlicht.

Die Firma Apple stellt im Kontext der Themen dieses Bausteins unter anderem folgende weiterführende Informationen bereit:

- Apple Configurator: https://support.apple.com/de-de/apple-configurator
- Apple Security Updates: https://support.apple.com/en-us/HT1222
- Abgekündigte und Vintage-Produkte: https://support.apple.com/de-de/HT201624
- Apple Business Manager: https://business.apple.com
- Support für Unternehmen und Bildungseinrichtungen:

https://www.apple.com/de/support/business-education/

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 SYS.3.2.3 *iOS (for Enterprise)* von Bedeutung.

G 0.9 Ausfall oder Störung von Kommunikationsnetzen

G 0.11 Ausfall oder Störung von Dienstleistern

G 0.14 Ausspähen von Informationen (Spionage)

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

G 0.19 Offenlegung schützenswerter Informationen

G 0.21 Manipulation von Hard- oder Software

G 0.22 Manipulation von Informationen

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 0.27 Ressourcenmangel

G 0.28 Software-Schwachstellen oder -Fehler

G 0.29 Verstoß gegen Gesetze oder Regelungen

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

G 0.32 Missbrauch von Berechtigungen

G 0.35 Nötigung, Erpressung oder Korruption

G 0.36 Identitätsdiebstahl

G 0.37 Abstreiten von Handlungen

G 0.38 Missbrauch personenbezogener Daten

G 0.39 Schadprogramme

G 0.41 Sabotage

G 0.42 Social Engineering

G 0.46 Integritätsverlust schützenswerter Informationen