Bundesamt
für Sicherheit in der
Informationstechnik

Ihre Meinung ist gefragt:
Überarbeitete Struktur der Umsetzungshinweise

Zu vielen Bausteinen des IT-Grundschutz-Kompendiums gibt es detaillierte Umsetzungshinweise. Diese beschreiben, wie die Anforderungen der Bausteine umgesetzt werden können und erläutern im Detail geeignete Sicherheitsmaßnahmen. Damit sind sie ein wichtiges Alleinstellungsmerkmal des IT-Grundschutzes, der nicht nur Sicherheitsanforderungen vorgibt, sondern die Anwender auch bei der konkreten Umsetzung unterstützt.

Im Rahmen der kontinuierlichen Überarbeitung des IT-Grundschutzes sollen die Umsetzungshinweise neu strukturiert werden. Dies soll die Anwendung erleichtern, Redundanzen vermeiden und ermöglichen, auch themenübergreifende Vorschläge für geeignete Maßnahmen zu definieren.

Ein erster Entwurf dieser neuen Struktur steht mit dem vorliegenden überarbeiteten Umsetzungshinweis zum Baustein SYS.3.2.3 iOS (for Enterprise) zur Kommentierung bereit.

Dieser Umsetzungshinweis ist auf dem Stand der Edition 2020 des IT-Grundschutz-Kompendiums. Gerne nehmen wir hierzu inhaltliche Anmerkungen entgegen, möchten aber insbesondere um die Kommentierung der Struktur bitten, z. B.: Ist die Aufteilung verständlich? Fehlen Aspekte?

Die wesentlichen Änderungen in der Struktur der Umsetzungshinweise sind folgende:

- **Der Lebenszyklus wurde entfernt.** Je nach Ausprägung enthielt dieser bisher nur allgemeine Informationen oder eine exemplarische Zuordnung einzelner Anforderungen zu den Lebenszyklus-Phasen. Zudem ist die Abbildung der drei Anforderungskategorien Basis, Standard und Erhöhter Schutzbedarf auf feste Phasen in vielen Fällen nicht sinnvoll möglich.
- **Ein Umsetzungshinweis kann nun Maßnahmen für mehrere Bausteine enthalten.** In der Regel werden viele Sicherheitsanforderungen bereits durch übergreifende Bausteine abgedeckt. Beispielsweise stellt der Baustein SYS.3.2.1 *Allgemeine Smartphones und Tablets* eine Anforderung für die Verwendung eines Zugriffsschutzes auf. Diese gilt gleichermaßen für alle Smartphones und Tablets unabhängig vom Betriebssystem. Der Umsetzungshinweis zu SYS.3.2.3 *iOS (for Enterprise)* beschreibt nun konkrete Maßnahmen für iOS, um diese allgemeingültige Anforderung zu erfüllen. So können Redundanzen in den Bausteinen vermieden werden.
- **Maßnahmen sind aufsteigend sortiert.** Zur leichteren Auffindbarkeit sind die Maßnahmen aufsteigend nummeriert, wobei weiterhin eine eindeutige Zuordnung zwischen den Maßnahmen (gekennzeichnet mit M) und den Anforderungen (gekennzeichnet mit A) besteht. Im Umsetzungshinweis wird nicht nach Anforderungskategorie unterschieden.

Bitte senden Sie Ihre Anmerkungen und Kommentare an: grundschutz@bsi.bund.de

Bundesamt
für Sicherheit in der
Informationstechnik

Umsetzungshinweise zum Baustein: SYS.3.2.3 iOS (for Enterprise)

1. Einleitung

Mobilgeräte sind ständige Begleiter in der heutigen Informationsgesellschaft. Sie sind fast ununterbrochen online, das heißt mit dem Internet oder dem internen Institutionsnetz (Intranet) verbunden, und ermöglichen damit jederzeit den Zugriff auf digitale Informationen. Die Geräte können über diverse Schnittstellen kommunizieren, zum Beispiel über Mobilfunk, WLAN oder Bluetooth. Aufgrund von modernen, einfachen Bedienkonzepten sowie hoher Leistungsfähigkeit sind Smartphones und Tablets der Firma Apple im beruflichen Umfeld weit verbreitet.

Um die Anforderungen an die Benutzbarkeit und Flexibilität mit der Erfüllung der Sicherheitsstrategie und der Konzepte der Institution vereinbaren zu können, müssen zu verwaltende Geräte in eine Mobile-Device-Management-Infrastruktur (MDM) integriert sein. Eine begründete Ausnahme unter Betrachtung von wirtschaftlichen Aspekten kann die Verwaltung einer kleineren, einstelligen Anzahl von Geräten ohne Einsatz eines MDM sein. So sind fast alle nachfolgend aufgezeigten Beispiele auch mit dem "Apple Configurator" [AppleConf] der Firma Apple für kleinere Gerätezahlen umsetzbar. Bei Einsatz des "Apple Configurator" sollten durch das Sicherheitsmanagement alternative Reaktions- und Informationswege für eine zeitnahe Reaktion auf Sicherheitsvorfälle etabliert sein.

Für die Abbildung der unterschiedlichen Umsetzungsempfehlungen in Abhängigkeit vom Einsatzzweck des Geräts, von der Benutzergruppe sowie vom Zugriff auf Informationen der Institution wird innerhalb dieses Dokuments auf die folgenden drei fiktiven Benutzergruppen zurückgegriffen.

Benutzergruppe 1

- Die Benutzer nutzen die zur Verfügung gestellten Smartphones primär zur Telefonie und zum Versenden von E-Mails.

- Die Benutzer haben keinen weiteren Zugriff auf interne Kollaboration und Dokumentenmanagementsysteme.
- Die Informationen sind nicht als sensibel, geschäftskritisch oder vertraulich klassifiziert.

Benutzergruppe 2

- Die Benutzer nutzen die zur Verfügung gestellten Smartphones und Tablets zur Telefonie, um E-Mails zu versenden und um dienstliche Dokumente zu bearbeiten.
- Die Benutzer haben des Weiteren Zugriff auf interne Kollaboration und Dokumentenmanagementsysteme.
- Teilweise sind die Informationen als sensibel bzw. geschäftskritisch klassifiziert.

Benutzergruppe 3

- Die Benutzer nutzen die zur Verfügung gestellten Smartphones und Tablets zur Telefonie, um E-Mails zu versenden und um dienstliche Dokumente zu bearbeiten.
- Die Benutzer haben des Weiteren Zugriff auf interne Kollaboration und Dokumentenmanagementsysteme, Finanzdaten oder kritische Systeme der Institution.
- Teilweise sind die Informationen als vertraulich klassifiziert.

2. Maßnahmen

Im Folgenden sind spezifische Maßnahmen für die Anforderungen des Bausteins SYS.3.2.3 *iOS (for Enterprise)* sowie für weitere Bausteinen aufgeführt, die hiermit im Zusammenhang stehen:

SYS.3.2.1 *Allgemeine Smartphones und Tablets* und SYS.3.2.2 *Mobile Device Management (MDM)*.

Diese zusätzlichen Maßnahmen sollten bei der Umsetzung der genannten Bausteine berücksichtigt werden. Alle Maßnahmen (gekennzeichnet mit M) sind aufsteigend nummeriert und korrespondieren mit den entsprechenden Anforderungen (gekennzeichnet mit A).

2.1 Maßnahmen zum Baustein SYS.3.2.3 iOS (for Enterprise)

SYS.3.2.3.M1 Strategie für die iOS-Nutzung (B)

Grundsätzlich setzen alle MDM-Anbieter auf den von der Firma Apple freigegebenen Schnittstellen auf und unterstützen meist kurze Zeit nach Freigabe einer neuen iOS-Version neu hinzugekommene Funktionen. Dies bedeutet, dass das MDM mindestens die benötigten Absicherungsmaßnahmen unterstützen und sich in die bereits vorhandene Infrastruktur integrieren lassen muss. Durch den Betrieb des MDM und der verwalteten Geräte darf kein Verlust der Vertraulichkeit, Integrität und Verfügbarkeit der Informationen und verknüpften Systeme verursacht werden. So ist abzuwägen, ob das MDM in der Cloud, vor Ort in den eigenen Rechenzentren oder bei einem nach ISO 27001 auf der Basis von IT-Grundschutz zertifizierten Rechenzentrumsdienstleister betrieben werden sollte.

Werden iOS-Geräte genutzt, ist es zunächst notwendig, bestimmte strategische Punkte zu klären, die bei der Nutzung relevant sein könnten, z. T. abhängig von der eigenen IT-Infrastruktur. So sollten Daten nach Möglichkeit nicht ausschließlich auf den mobilen Endgeräten gespeichert sein, so dass diese im Verlustfall nicht ebenfalls verloren gehen. Dies berührt auch die allgemeine Strategie für Datensicherungen der Institution.

Abhängig vom geplanten Einsatzzweck muss eine geeignete Auswahl der Endgeräte getroffen werden. Außerdem ist frühzeitig zu klären, ob Apps von Drittanbietern auf den iOS-Geräten eingesetzt werden sollen.

SYS.3.2.3.M2 Planung des Einsatzes von Cloud-Diensten (B)

Bei der Nutzung von Online-Speicher-Diensten (z. B. iCloud, Google Drive, Dropbox) kann zwischen verschiedenen Varianten unterschieden werden. Das Online-Backup, bei dem Daten einmalig oder in regelmäßigen Abständen über das Internet gespeichert werden, um nach einem Datenverlust wieder abgerufen werden zu können, stellt dabei die einfachste Form der Nutzung dar. Bei der sogenannten Online-Festplatte stehen je nach Dienstleister neben der reinen Datenspeicherung auch zusätzliche Funktionen zur Verfügung, wie

das Teilen von Daten mit Mitarbeitern, Freunden oder Geschäftspartnern, die gemeinsame Arbeit an Dokumenten sowie die Synchronisation verschiedener Endgeräte.

Ist der Zugriff auf die Daten der Institution nicht möglich, da der Online-Speicher-Dienst aufgrund eines Ausfalls des Dienstleisters oder der Verbindung zum Dienst nicht zur Verfügung steht, kann dies die Geschäftsprozesse stören oder komplett zum Erliegen bringen. Wichtig sind in diesem Zusammenhang insbesondere die Schutzbedarfsanforderungen an die betroffenen Informationen. Sofern eine hohe Verfügbarkeit Grundlage der Prozesse ist, drohen bei längeren Ausfallzeiten des Online-Dienstes finanzielle Verluste meist einhergehend mit Imageschädigungen. Neben der Verfügbarkeit des Online-Speichers und der darin abgelegten Informationen hat vor allem die Vertraulichkeit der Informationen einen hohen Stellenwert. Gelingt es Angreifern, Zugang zu vertraulichen Informationen der Institution zu erlangen und diese z. B. einem breiteren Personenkreis zugänglich zu machen, drohen Imageverlust sowie rechtliche Konsequenzen und finanzielle Einbußen.

Bei der Übertragung von Informationen, deren Bearbeitung über das Netz oder deren abschließender Speicherung können Integritätsprobleme auftreten, die bis hin zum Totalverlust führen können. Dies gilt auch für verschlüsselte Daten. Die Auswirkungen für die Institution sind ähnlich wie beim Verlust der Vertraulichkeit.

Rechtliche Aspekte beim Einsatz von Cloud-Diensten spielen immer dann eine Rolle, wenn personenbezogene Daten im Sinne der DSGVO übergeben werden. Eine Auftragsdatenverarbeitung ist, in Abhängigkeit vom tatsächlichen Speicherort der Daten, nur unter bestimmten Voraussetzungen möglich und zudem an die Erteilung eines schriftlichen Auftrages gebunden. Bei einer Zuwiderhandlung gehen Institutionen das Risiko ein, gegen bestehendes Recht zu verstoßen und hierdurch nicht nur ihren Ruf zu schädigen, sondern sich auch Schadenersatzansprüchen oder Bußgeldern gegenüberzusehen.

Werden bei Vertragsende die Informationen der Institution durch den Anbieter des Online-Speichers nicht ordnungsgemäß gelöscht, besteht die Gefahr, dass Unbefugte weiterhin Zugriff auf diese Informationen erhalten.

Weiterführende Informationen zu diesen Themen finden sich zusätzlich in den entsprechenden Bausteinen.

iOS-basierte Geräte bieten grundsätzlich eine enge Verzahnung mit den iCloud-Diensten des Herstellers Apple an. Über den App Store können zusätzliche Apps zur vereinfachten Einbindung von weiteren Cloud-Dienstleister auf dem Gerät installiert werden. Im Vorfeld des Einsatzes von Smartphones und Tablets müssen an die Verantwortlichen für das Provider-Management, den Betrieb und Einkauf die zu erfüllenden betrieblichen, sicherheitstechnischen sowie datenschutzrechtlichen Anforderungen im Einklang mit den internen Richtlinien übergeben werden.

Für eine einfachere Erstinbetriebnahme kann auf die Möglichkeit der Geräteregistrierung über den Apple Business Manager [AppleBM] zurückgegriffen werden. Vertiefende Informationen hierzu sind auf den Websites von Apple verfügbar.

SYS.3.2.3.M3 ENTFALLEN

Die zugehörige Anforderung im Baustein ist entfallen.

SYS.3.2.3.M4 ENTFALLEN

Die zugehörige Anforderung im Baustein ist entfallen.

SYS.3.2.3.M5 ENTFALLEN

Die zugehörige Anforderung im Baustein ist entfallen.

SYS.3.2.3.M6 ENTFALLEN

Die zugehörige Anforderung im Baustein ist entfallen.

SYS.3.2.3.M7 Verhinderung des unautorisierten Löschens von Konfigurationsprofilen (B)

In Abhängigkeit von dem eingesetzten MDM-Anbieter besteht die Möglichkeit, Einschränkungen hinsichtlich der Löschung von Konfigurationsprofilen zu hinterlegen. So kann die Möglichkeit bestehen, dass das Konfigurationsprofil niemals oder aber passwortbasiert und somit autorisiert gelöscht werden kann. Bei der passwortbasierten Autorisierung sollen die in der Institution etablierten Vorgaben für Passwörter eingehalten werden. Grundsätzlich sollen die Benutzer nicht dazu befähigt werden, die Konfigurationsprofile unbemerkt löschen zu können. Des Weiteren empfehlen sich mindestens pro Benutzer- bzw. Profilgruppe unterschiedliche

Passwörter zur Absicherung der Konfigurationsprofile zu verwenden. Wird das Gerät mittels des Apple Business Managers in die MDM-Infrastruktur integriert, ist der Benutzer automatisch nicht in der Lage, unautorisiert Veränderungen an den Konfigurationsprofilen vorzunehmen.

SYS.3.2.3.M8 ENTFALLEN

Die zugehörige Anforderung im Baustein ist entfallen.

SYS.3.2.3.M9 ENTFALLEN

Die zugehörige Anforderung im Baustein ist entfallen.

SYS.3.2.3.M10 Verwendung biometrischer Authentisierung (S)

Zur besseren Akzeptanz eines komplexen Passcodes und der hiermit einhergehenden besseren Verschlüsselung der Informationen auf dem Gerät können biometrischen Verfahren zur Authentisierung verwendet werden. Bei der Nutzung von biometrischen Merkmalen (Fingerabdruck über Touch ID oder Gesicht über Face ID) zum Entsperren ist es einem potentiellen Angreifer unter Umständen möglich, diese nachzuahmen. So kann er auf der Oberfläche des Gerätes oder von Gegenständen mit glatter Oberfläche die Fingerabdrücke abnehmen und nachbauen, auch Angriffe über nachgebaute Gesichter in Form von Masken sind denkbar. Bei der Abwägung der Risikoakzeptanz der Kompromittierung des Fingerabdruckes gegenüber der besseren Verschlüsselung und der Durchsetzung von komplexen Passwörtern innerhalb der Institution sollte mit einfließen, dass bei aktiver biometrischer Authentisierung 48 Stunden nach der letzten erfolgreichen Nutzung eine Verifizierung des rechtmäßigen Besitzers durch die Eingabe des Passcodes erfolgt. Aus diesem Grunde ist es äußerst wichtig, den Passcode nicht an Dritte weiterzugeben. Welche empfohlenen Funktionalitäten unter Berücksichtigung der drei fiktiven Benutzergruppen genutzt werden könnten, wird in der nachfolgenden Tabelle aufgezeigt.

	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
Biometrie für das Entsperren des Geräts erlauben	ja	ja	nein
Ändern der Touch ID- / Face ID-Merkmale erlauben	ja	nein	nein
Biometrie verwenden für iTunes und App Store	nein	nein	nein

Tabelle 1: Verwendung biometrischer Authentisierung (Touch ID und Face ID)

SYS.3.2.3.M11 Verwendung nicht personalisierter Gerätenamen (S)

Über den Gerätenamen kann ein Angreifer oft Rückschlüsse auf den Benutzer oder die Institution erlangen. So wird der Gerätename z. B. nach dem Bluetooth-Pairing in integrierten Multimedia-Systemen oder Freisprecheinrichtungen moderner Fahrzeuge hinterlegt. Ebenfalls kann nach dem Verbinden mit Hotspots der Name des Geräts gesehen werden. Aus diesem Grunde sollten keine Gerätenamen mit Bezug zu der Institution und dem Benutzer konfiguriert werden, um so der personalisierten Profilbildung und Erratbarkeit typischer Passwörter vorzubeugen. Für eine leichte Identifikation innerhalb der Institution empfiehlt sich die Verwendung einer Asset-Nummer. Zur Vermeidung einer versehentlichen Änderung des Gerätenamens sollte zusätzlich die in der Tabelle aufgeführte Konfigurationseinstellung umgesetzt sein.

	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
Ändern des Gerätenamens erlauben	nein	nein	nein

Tabelle 2: Verwendung nicht personalisierter Gerätenamen

SYS.3.2.3.M12 Verwendung von Apple IDs (S)

Beim Einsatz einer Apple ID sollte diese mit niemandem geteilt werden, da sie prinzipiell einem Benutzerkonto gleichgestellt ist. Sollte jemand Drittes in den Besitz des Passworts der Apple ID gelangen, kann dieser auf die persönlichen und geschäftlichen Daten zugreifen, einschließlich der Kontakte sowie Geräte-Backups in der iCloud. In den AGB für die iCloud schließt die Firma Apple die Möglichkeit der Übertragung der Apple ID an eine andere Person komplett aus.

Zudem gehen mit der Apple ID verknüpfte Zahlungsmittel für alle Einkäufe im App Store oder bei iTunes einher, sofern diese nicht für geschäftliche Zwecke zuvor über den Apple Business Manager für Volumenlizenzen erworben wurden. Ein Vorteil des Einsatzes des ist, dass keine institutionsbezogene Apple ID seitens des Benutzers benötigt wird. Erfolgte die Geräteregistrierung mittels des Apple Business Managers, ist für die dienstliche Nutzung des Gerätes ebenfalls keine institutionsbezogene Apple ID notwendig. Kann auf die dienstliche Nutzung der iCloud verzichtet werden, sollte durch die Verwendung verwalteter Apps die iCloud-Nutzung auf das notwendige Maß reduziert oder komplett ausgeschlossen werden. In diesem Fall ist eine institutionsbezogene Apple ID ebenfalls nicht notwendig.

Sollte die Geräteregistrierung und Verwendung von Volumenlizenzen nicht mittels Apple Business Manager erfolgen oder werden Dienste verwendet, für die eine Apple ID unbedingt erforderlich ist, so sollte statt einer persönlichen Apple ID des Benutzers eine anonymisierte Apple ID verwendet werden. Wird in der Institution bereits ein Namenskonzept z. B. für das Windows-Benutzerkonto, basierend auf Organisationseinheiten sowie Rollen und Funktionen des Mitarbeiters, umgesetzt, empfiehlt sich dessen Erweiterung um die Erstellung der Apple ID. Über die zu hinterlegende E-Mail-Adresse versendet Apple Hinweise zur Benutzung der iCloud, Rechnungen der zur Verfügung stehenden Stores sowie Anfragen an das Benutzerkonto oder nach einem Passwort-Reset der Apple ID. Es empfiehlt sich die Hinterlegung einer gesonderten E-Mail-Adresse für die Apple ID und die Auswertung der Nutzung und des Zwecks der Nutzung.

SYS.3.2.3.M13 Verwendung der Konfigurationsoption "Einschränkungen unter iOS" (S)

Um die Vertraulichkeit und Integrität der verarbeiteten bzw. auf dem iOS-basierten Gerät gespeicherten Daten sicherzustellen, sollten alle nicht erlaubten Funktionen oder Dienste deaktiviert sein. Welche empfohlenen Funktionen und Dienste unter Berücksichtigung der drei fiktiven Benutzergruppen mittels Konfigurationsprofilen und organisatorischen Anweisungen gesteuert werden sollten, wird in den folgenden Themengruppen definiert und erläutert.

Hintergrundbild

Durch die Verwendung von Gesichtserkennungssoftware besteht heutzutage die Möglichkeit, Personen auf dem Bild im Sperrbildschirm z. B. mit Bildern aus sozialen Netzwerken, öffentlich zugänglichen Bildergalerien sowie den Ergebnissen von Suchmaschinen abzugleichen und so den Benutzer zu ermitteln, darauf aufbauend potentielle Passwörter abzuleiten und weitere Ansätze für Social-Engineering-Angriffe zu entwickeln. Nachfolgend die entsprechenden Konfigurationsempfehlungen zur Reduzierung der Angriffsfläche für Social Engineering basierend auf dem Beispiel eines persönlichen Hintergrundbilds, welches beispielsweise den Benutzer oder Teile seiner Familie darstellt.

	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
Ändern des Hintergrundbilds erlauben	ja	ja	nein

Tabelle 3: Verwendung der Konfigurationsoption für "Einschränkungen unter iOS" - Hintergrundbild

Sperrbildschirm

Über den Sperrbildschirm stehen den Anwendern viele Möglichkeiten zur Anzeige von Informationen zur Verfügung. Dazu gehören werksseitig installierte Apps, wie z. B. Kalenderübersicht, Erinnerungen oder Verkehrslage, via Widgets Informationen von Apps aus dem App Store sowie verschiedene Arten von Benachrichtigungen. Über das Kontrollzentrum besteht zudem die Möglichkeit, auch ein gesperrtes Gerät sehr schnell und einfach in den Flugmodus zu versetzen, womit es z. B. für ein MDM nicht mehr erreichbar ist.

	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
Wallet-Mitteilungen im Sperrbildschirm anzeigen	ja	ja	nein
Kontrollzentrum im Sperrbildschirm anzeigen	ja	ja	nein
Mitteilungszentrale im Sperrbildschirm anzeigen	ja	nein	nein
Ansicht „heute“ im Sperrbildschirm anzeigen	ja	nein	nein

Tabelle 4: Verwendung der Konfigurationsoption für "Einschränkungen unter iOS" - Sperrbildschirm

Einhergehend mit der Freigabe der Mitteilungszentrale und der Ansicht "heute" sollte eine Sensibilisierung der Anwender bzgl. der Nutzung der dort angezeigten Informationen erfolgen und eine Empfehlung ausgesprochen werden, welche Widgets mit welchem Inhalt deaktiviert werden sollten.

Siri

Siri dient als persönlicher Assistent und setzt hierfür auf Sprachein- und ausgabe. Bei einer bestehenden Internetverbindung werden alle Sprachdaten über eine kryptographisch abgesicherte Verbindung an Server von Apple übertragen und auf diesen Servern verarbeitet. Die nachfolgende Tabelle zeigt beispielhaft, mittels welcher Konfigurationseinstellungen ein pragmatischer Umgang mit Siri möglich ist.

	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
Siri erlauben	ja	ja	nein
Siri erlauben, während das Gerät gesperrt ist	nein	nein	-
Siri-Obszönitätenfilter aktivieren	ja	ja	-
Benutzergenerierten Inhalt in Siri erlauben	ja	nein	-

Tabelle 5: Verwendung der Konfigurationsoption für "Einschränkungen unter iOS" - Siri

Sollten sich in der Anwendergruppe blinde und sehbehinderte Menschen befinden, wird die Bedienung des Geräts durch Siri massiv vereinfacht bzw. die umfängliche Nutzung von Smartphones und Tablets erst ermöglicht. Die Möglichkeiten der Verwendung des Gerätes durch Siri dürfen jedoch nicht mit den Funktionen von VoiceOver verwechselt werden. Dies muss in die Bewertung möglicher Risiken hinsichtlich Verletzung der Vertraulichkeit und Integrität einfließen.

Unified Communication

Unter dem Begriff Unified Communication (UC) werden alle Konfigurationsempfehlungen für die von Apple fest integrierten Apps wie FaceTime und iMessage für Videotelefonie und textbasierten Chats zusammengefasst.

	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
FaceTime erlauben	ja	ja	nein
iMessage erlauben	ja	ja	nein

Tabelle 6: Verwendung der Konfigurationsoption für "Einschränkungen unter iOS" - Unified Communication

Sollten durch das Sicherheitsmanagement bereits Empfehlungen zum Umgang mit Chat- und Videotelefonie-Anwendungen definiert sein, sollten diese Empfehlungen auch für die Nutzung von FaceTime und iMessage gelten. Bei der Verwendung von FaceTime und iMessage werden alle Informationen auf allen mit der Apple ID verknüpften Geräte simultan in der Anwendung selbst und in der Mitteilungszentrale angezeigt.

Diagnose- und Nutzungsdaten

Basierend auf den Hinweisen der Firma Apple können zu den Diagnose- und Nutzungsdaten auch Details zu Hardware- und Betriebssystemspezifikationen und Leistungsstatistiken sowie Informationen über die Art der Nutzung des Geräts und der Apps gehören. Persönliche Daten der Anwender werden entweder gar nicht aufgezeichnet oder aus den Berichten gelöscht, bevor diese an Apple gesendet werden. Wenn der Anwender zugestimmt hat, dass Apple diese Informationen zur Verfügung gestellt werden, und gleichzeitig die Ortungsdienste aktiviert sind, wird zusätzlich die aktuelle Position des Geräts versendet. Es werden die in der Tabelle aufgeführten Einstellungswerte für den Umgang mit Diagnose- und Nutzungs- sowie den Ortungsdaten empfohlen.

	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
Diagnose- und Nutzungsdaten an Apple senden	nein	nein	nein

Tabelle 7: Verwendung der Konfigurationsoption für "Einschränkungen unter iOS" - Diagnose- und Nutzungsdaten

Sollte diese Empfehlung von den etablierten Vorgaben der Institution z. B. für Windows-Systeme abweichen, empfiehlt sich eine übergreifende Bewertung des Umgangs mit Diagnose- und Nutzungsdaten und eine einheitliche Umsetzung.

Apple Watch

Durch die Verknüpfung der Smartwatch von Apple mit einem iOS-basierten Gerät besteht die Möglichkeit, z. B. Nachrichten oder E-Mails auf der Apple Watch zu erhalten und direkt darauf zu reagieren. Für die Integration und Absicherung werden die beiden folgenden Konfigurationsoptionen angeboten.

	Benutzergruppe 1	**Benutzergruppe 2**	**Benutzergruppe 3**
Apple-Watch-Handgelenkerkennung aktivieren	ja	ja	ja
Koppeln mit der Apple Watch erlauben	ja	ja	ja

Tabelle 8: Verwendung der Konfigurationsoption für "Einschränkungen unter iOS" - Apple Watch

Übergreifend

An dieser Stelle werden einzelne übergreifende Empfehlungen aufgeführt, die sich nicht direkt thematisch gruppieren lassen.

	Benutzergruppe 1	**Benutzergruppe 2**	**Benutzergruppe 3**
Verwendung der Kamera entsprechend der allgemeinen Institutionsrichtlinien erlauben	ja	ja	ja
Bildschirmfoto oder Bildschirmaufnahme erlauben	ja	nein	nein
Sprachwahl erlauben, während das Gerät gesperrt ist	ja	nein	nein
iBooks Store erlauben	ja	ja	ja
Backup unternehmenseigener Bücher erlauben	nein	ja	ja
Automatisches Synchronisieren erlauben	nein	nein	nein
Verschlüsselte Backups erzwingen	ja	ja	ja
Beschränktes Ad-Tracking erzwingen	ja	ja	ja
Löschen aller Inhalte und Einstellungen erlauben	ja	ja	nein
Benutzer dürfen nicht vertrauenswürdige TLS-Zertifikate annehmen	ja	nein	nein
Automatische Updates für Trust-Zertifikate erlauben	ja	ja	ja
Einstufen neuer Entwickler firmenweiter Apps als vertrauenswürdig erlauben	ja	nein	nein
Ändern der Beschränkungen erlauben (Wenn diese Option deaktiviert wurde, können Benutzer keine eigenen zusätzlichen Einschränkungen auf dem Gerät definieren.)	ja	ja	ja
Dokumente von verwalteten Quellen in nicht verwalteten Zielen erlauben	ja	nein	nein
Dokumente von nicht verwalteten Quellen in verwalteten Zielen erlauben	ja	nein	nein

Tabelle 9: Verwendung der Konfigurationsoption für "Einschränkungen unter iOS" - übergreifend

SYS.3.2.3.M14 Verwendung der iCloud-Infrastruktur (S)

In SYS.3.2.3.M2 wurde die Strategie des Einsatzes von Cloud-Diensten und den hiermit einhergehenden betrieblichen, sicherheitstechnischen und datenschutzrechtlichen Anforderungen definiert. Welche Möglichkeiten der zentralen Verwaltung von Funktionen für den Einsatz der iCloud bestehen, wird nachfolgend beschrieben. Ist die Nutzung der iCloud-Infrastruktur nicht grundsätzlich durch das Sicherheitsmanagement der Institution verboten worden, sollte eine Prüfung erfolgen, inwieweit die Nutzung der folgenden Funktionen mit den internen Vorgaben vereinbar ist. Bei der Prüfung muss auch der Umgang seitens der Firma Apple mit behördlichen Anfragen einfließen. Detaillierte Informationen sind im Dokument „Legal Process Guidelines“ auf der Apple-Website einsehbar.

Wird iCloud genutzt, sollte die von Apple angebotene Zwei-Faktor-Authentisierung für den iCloud-Zugriff geprüft und aktiviert werden.

Welche Funktionalitäten der iCloud ohne Sicherheitsverlust unter Berücksichtigung der drei fiktiven Benutzergruppen mittels Konfigurationsprofilen gesteuert werden sollten, wird in der nachfolgenden Tabelle dargestellt.

	Benutzergruppe 1	**Benutzergruppe 2**	**Benutzergruppe 3**
iCloud-Backup erlauben	ja	nein	nein
iCloud-Dokumente und -Daten erlauben	ja	nein	nein
iCloud-Schlüsselbund erlauben	nein	nein	nein
Verwalteten Apps das Sichern von Daten in iCloud erlauben	ja	nein	nein
Synchronisierung von Notizen und Anmerkungen für unternehmenseigene Bücher erlauben	ja	ja	nein
iCloud-Fotofreigabe erlauben	ja	ja	ja
„Mein Fotostream“ erlauben	ja	ja	ja
Ändern der Einstellungen von „Freunde suchen“ erlauben	nein	nein	nein

Tabelle 10: Verwendung der iCloud-Infrastruktur

SYS.3.2.3.M15 Verwendung der Continuity-Funktionen (S)

Mit der Funktion AirDrop können die Anwender mit anderen Anwendern in der Nähe z. B. Fotos, Videos oder Standortinformationen austauschen. Voraussetzung hierfür ist, dass beide Anwender ein Gerät der Firma Apple verwenden. Mit der Funktion Handoff wird den Anwendern die Möglichkeit zur Verfügung gestellt, ein Dokument, eine E-Mail oder eine Nachricht auf einem Gerät zu beginnen und auf einem anderen Gerät in der näheren Reichweite an der Stelle fortzufahren, wo sie aufgehört haben. Handoff funktioniert mit Apps von Apple wie E-Mail, Safari, Karten, Nachrichten, Erinnerungen, Kalender, Kontakte, Pages, Numbers und Keynote, mit der Zwischenablage auf Apple-Geräten sowie mit einigen Drittanbieter-Apps. Zu diesem Zwecke werden unter Einbeziehung der iCloud-Infrastruktur z. B. Suchanfragen und Favoriten in der Maps-App, neu erlernte Wörterbucheinträge, die Anruf-Historie, Playback-Positionen der Podcast-App, Tabs des Browsers Safari, Lesezeichen der iBooks-App, die VIP-Liste in der Mail-App sowie HomeKit-Einstellungen geräteübergreifend synchronisiert.

Beide Funktionen benötigen hierfür eine aktive Apple ID. Bei der Funktion Handoff müssen die verwendeten Geräte mit der selben Apple ID verknüpft sein. Dies bedeutet, dass die hier vorgeschlagenen Einstellungen mit den Einstellungen für die iCloud korrespondieren müssen.

	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
AirDrop erlauben	ja	ja	nein
AirDrop als nicht verwalteten Zielort behandeln1	ja	nein	-
Handoff erlauben	ja	nein	nein

Tabelle 11: Verwendung der "Continuity-Funktionen"

SYS.3.2.3.M16 ENTFALLEN

Die zugehörige Anforderung im Baustein ist entfallen.

SYS.3.2.3.M17 Verwendung der Gerätecode-Historie (S)

Für die drei fiktiven Benutzergruppen werden Empfehlungen genannt, um die Vertraulichkeit des verwendeten Passcodes zu wahren und um zu verhindern, dass dieser zu häufig durch den Benutzer wiederholt wird. In der Regel sollten bei der Festlegung des Werts die etablierten Regelungen basierend auf dem allgemeinen Passwortkonzept der Institution verwendet werden.

	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
Passcode-Verlauf	5	10	10

Tabelle 12: Verwendung der Gerätecode-Historie

SYS.3.2.3.M18 Verwendung der Konfigurationsoption für den Browser Safari (S)

Mit dem Betriebssystem iOS liefert Apple den vorinstallierten Browser Safari aus, der durch Konfigurationsprofile angepasst werden kann. Durch die tiefgreifende Implementierung der Browser-App besteht die Möglichkeit, das Verhalten des Browsers an die internen Vorgaben der Institution anzupassen. In der nachfolgenden Tabelle werden Empfehlungen für die Anpassung unter Berücksichtigung der drei fiktiven Benutzergruppen benannt.

	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
Verwendung von Safari erlauben	ja	ja	ja
Automatisches Ausfüllen aktivieren	ja	nein	nein
Betrugswarnung erzwingen	ja	ja	ja
JavaScript aktivieren	ja	ja	ja
Pop-Ups unterdrücken	nein	ja	ja
Cookies akzeptieren	immer erlauben	von besuchten Webseiten erlauben	von aktueller Webseite erlauben

Tabelle 13: Verwendung der Konfigurationsoption für den Browser Safari

SYS.3.2.3.M19 ENTFALLEN

Die zugehörige Anforderung im Baustein ist entfallen.

SYS.3.2.3.M20 Einbindung der Geräte in die interne Infrastruktur via VPN (S)

iOS-basierte Geräte sollten mittels VPN in die Infrastruktur der Institution eingebunden und integriert werden. Für die Konfiguration der VPN-Verbindungen zu den Servern von Aruba VIA, Check Point Mobile VPN, Cisco AnyConnect, F5 SSL, Juniper SSL, SonicWALL Mobile Connect, NCP, genua oder SINA können die MDM-Anbieter auf von Apple mit den VPN-Herstellern abgestimmte Einstellungen zurückgreifen. Jedoch müssen neben dem Konfigurationsprofil teilweise noch zusätzlich die Apps der VPN-Server-Hersteller, z. B. die App "F5 BIG-IP Edge

Client", "Junos Pulse", "Cisco AnyConnect" und "Aruba Network VIA", aus dem App Store installiert sein. Im Dokument „Technische Richtlinie TR-02102“ [BSI-TR-02102] des BSI werden Empfehlungen ausgesprochen für die Verwendung von IPSec und SSL/TLS. Bei der Implementierung des VPN besteht unabhängig vom genutzten Algorithmus und Protokoll die Möglichkeit, ein VPN permanent, nur bei Bedarf oder für einzelne verwaltete Apps zu konfigurieren.

Permanentes VPN

Ein permanentes VPN ermöglicht die volle Kontrolle über alle Kommunikationsverbindungen. Die Verantwortlichen in der Institution können so den Datenverkehr zu und von iOS-basierten Geräten vollständig überwachen und bei Bedarf filtern und somit die Informationen der Institution schützen und den Zugriff der Geräte auf das Internet entsprechend den internen Anforderungen regulieren.

VPN On-Demand

Mit VPN On-Demand können iOS-basierte Geräte bei Bedarf automatisch eine VPN-Verbindung in die Institution herstellen. VPN On-Demand erfordert eine Authentisierung unabhängig vom verwendeten Protokoll auf Zertifikatsbasis. Das VPN On-Demand-Konfigurationsprofil muss mit dem Schlüssel "OnDemandRules" in einer VPN-Payload konfiguriert werden. Die Regeln für das Erkennen des Bedarfs erfolgt in zwei Etappen, der Netzwerkerkennung und der Verbindungsevaluierung.

VPN auf App-Basis

Ein VPN auf App-Basis ermöglicht jeder über das MDM verwalteten App, mittels eines Tunnels mit den Systemen in der Institution zu kommunizieren. Allen nicht verwalteten Apps wird die Nutzung des Tunnels in die Institution untersagt. Ein weiteres Merkmal für verwaltete Apps ist, dass unterschiedliche VPN-Verbindungen konfiguriert werden, um Informationen noch differenzierter zu schützen. Für die Realisierung eines VPN auf App-Basis muss die verwaltete App über Standard-Netz-APIs angesprochen werden können.

Eine generelle Empfehlung kann an dieser Stelle nicht getroffen werden, da der Schutzbedarf, die genutzten Algorithmen und Authentisierungsmethoden sowie die vorhandene DNS-Struktur bei der Entscheidung für oder gegen eine Variante einfließen müssen.

SYS.3.2.3.M21 Freigabe von Apps und Einbindung des Apple App Stores (S)

Der dienstliche Mehrwert eines iOS-basierten Smartphones oder Tablets hängt häufig davon ab, ob es einen umfänglichen Zugang zu den Informationen der Institution ermöglicht. Dies bedeutet, dass interne Daten (oftmals mit einer Vertraulichkeitsklassifizierung) den Anwendern außerhalb der Institutionsinfrastruktur auf den Geräten zur Verfügung gestellt werden müssen. Die iOS-Plattform ist an sich geschlossen und die Firma Apple kontrolliert alle Programme (Apps) vor der Freigabe im App Store. Trotz dieser Kontrolle ist nicht ausgeschlossen, dass durch die Apps vertrauliche oder interne Informationen abfließen können. Im Rahmen eines Freigabeprozesses innerhalb der eigenen Institution sollten mindestens die folgenden Kriterien geprüft und als Basis für eine Ablehnung oder Freigabe von Apps dienen:

- Wird durch die App unberechtigt auf Informationen des Anwenders zugegriffen?
- Versucht die App, unberechtigt auf die Standortdaten des Geräts zuzugreifen?
- Versucht die App, unberechtigt auf das Adressbuch zuzugreifen?
- Versucht die App, unberechtigt auf die Zwischenablage des Geräts zuzugreifen?
- Versucht die App, unberechtigt zu erkennen, welche Apps auf dem Gerät noch installiert sind?
- Versucht die App, unberechtigt die Kommunikationsverbindungen umzuleiten?
- Erfolgt die Speicherung von App-Anwendungsdaten außerhalb des deutschen bzw. europäischen Datenschutzraums?
- Erfolgt die Speicherung von App-Anwendungsdaten automatisiert oder ungefragt auf Servern außerhalb der Hoheit der Institution?
- Besteht durch Apps die Gefahr des Anwender-Profiling, etwa durch Werbung oder andere Tracker?

- Werden die Daten innerhalb der App automatisch beim Entsperren des Geräts entschlüsselt oder muss der Anwender zusätzlich ein Passwort zum Entschlüsseln eingeben?
- Werden durch die App eigene Sharing-Dienste oder Netzwerkschnittstellen angeboten?
- Werden regelmäßig Aktualisierungen des App-Entwicklers zur Verfügung gestellt?
- Setzt der App-Entwickler die aktuellsten Schnittstellen und Richtlinien von Apple um?

Unter Berücksichtigung der Ergebnisse des Freigabeprozesses und unabhängig von der Verwendung von Volumenlizenzen für Unternehmen können mittels der nachfolgenden Konfigurationsoptionen und deren Verwendung die Sicherheitsziele der Institution je Benutzergruppe unterstützt werden.

	Benutzergruppe 1	**Benutzergruppe 2**	**Benutzergruppe 3**
Installation von Apps über den App Store erlauben	ja	ja	nein
Automatische App-Downloads erlauben	ja	nein	nein
Entfernen von Apps erlauben	ja	ja	nein
In-App-Käufe erlauben	ja	ja	nein
iTunes-Passwort für alle Einkäufe erforderlich	ja	ja	ja

Tabelle 14: Einbindung des App-Store und Freigabe von Apps

SYS.3.2.3.M22 ENTFALLEN

Die zugehörige Anforderung im Baustein ist entfallen.

SYS.3.2.3.M23 Verwendung der automatischen Konfigurationsprofillöschung (H)

Durch die Hinterlegung eines speziellen Ablaufdatums oder eines Ablaufintervalls (Tage und Stunden) können auf dem Gerät hinterlegte Konfigurationsprofile ohne sonst benötigte Internetverbindung automatisch gelöscht werden. So wird sichergestellt, dass zum Beispiel keine VPN-Verbindung in die Institution mehr möglich ist. Dieses Verfahren sollte jedoch nur eingesetzt werden, wenn der Anwender grundsätzlich nur einen zeitlich begrenzten Zugang zu Informationen mit erhöhtem Schutzbedarf benötigt. Sind auf dem Gerät Informationen mit hohem Schutzbedarf gespeichert, kann diese Methodik auch als präventive Maßnahme zur Verifizierung und Sicherstellung des rechtmäßigen Anwenders/Besitzers dienen.

SYS.3.2.3.M24 ENTFALLEN

Die zugehörige Anforderung im Baustein ist entfallen.

SYS.3.2.3.M25 Verwendung der Konfigurationsoption für AirPrint (H)

Die AirPrint-Funktion wurde durch Apple fest in das Betriebssystem eingebaut, sie lässt sich nicht grundsätzlich einschalten oder abschalten. Die verantwortlichen Administratoren sollten die in der Institution freigegebenen AirPrint-Drucker durch ein Konfigurationsprofil den Benutzern bereitstellen. Des Weiteren empfiehlt es sich bei der Bewertung und Freigabe von AirPrint-Druckern in der Institution, diese in ein eigenes Netzsegment zu integrieren. Nur durch ein eigenes Netzsegment ist es einfach möglich, für diese eine angepasste Firewall-Regel über den Freigabeprozess zu beantragen, die Multicast-Kommunikation auf Port 5353 (Bonjour, mDNS) innerhalb des Netzsegments zu verwalten und das Internet Printing Protocol (IPP) auf die benötigten IP-Adressen oder Netzsegmente zu begrenzen. Hierfür muss sichergestellt sein, dass stets alle Kommunikationsverbindungen über die Infrastruktursysteme der Institution geführt sind.

SYS.3.2.3.M26 Keine Verbindung mit Host-Systemen (H)

Für die Erstellung eines lokalen Backups muss das Gerät mit iTunes via USB-Kabel oder WLAN verbunden sein. Bei der Verwendung von WLAN kann ein Angreifer versuchen, unbemerkt einen Man-in-the-Middle-Angriff durchzuführen und die Kontrolle über die Informationen auf dem Gerät zu erlangen. Bei einem lokalen Backup, ob verschlüsselt oder unverschlüsselt, kann jeder mit Host-Zugriff von diesen Dateien nahezu unbemerkt eine Kopie anfertigen, im Nachgang diese angefertigte Kopie unter Umständen entschlüsseln und die vorhandenen

Informationen, insbesondere das Benutzerverhalten, analysieren. Ein weiteres Risiko in der Verknüpfung des iOS-basierten Geräts mit einem Host (PC oder Notebook) besteht in der lokalen Ablage eines gültigen Pairing-Keys auf dem Host. Ein Angreifer kann unter Verwendung des Pairing-Keys für einen bestimmten Zeitraum ohne Kenntnis des Passcodes vertrauliche Informationen vom iOS-basierten Gerät extrahieren. Um den benannten Angriffsszenarien und dem Verlust vertraulicher Informationen vorzubeugen, sollte die Verbindung mit Host-Systemen durch die verantwortlichen Administratoren verhindert worden sein.

SYS.3.2.3.M27 ENTFALLEN

Die zugehörige Anforderung im Baustein ist entfallen.

2.2 Maßnahmen zum Baustein SYS.3.2.1 Allgemeine Smartphones und Tablets

SYS.3.2.1.M4 Verwendung eines Zugriffsschutzes (B)

Ein wirksamer Zugriffsschutz für iOS-basierte Geräte wird durch die Betrachtung verschiedener Aspekte erreicht.

Gerätecode

Mit der Aktivierung des Passcodes soll unberechtigten Dritten der Zugriff auf die Informationen im Smartphone oder Tablet verwehrt werden. Für die drei fiktiven Benutzergruppen sind die folgenden in der Tabelle aufgeführten Konfigurationen basierend auf dem Einsatzzweck und dem Schutzbedarf der Informationen empfehlenswert.

	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
Einfache Werte erlauben	nein	nein	nein
Mindestlänge des Passcodes	6	8	8
Maximale Passcodegültigkeit	120	90	90
Ändern des Codes erlauben	ja	ja	ja

Tabelle 15: Verwendung des Gerätecodes (Passcode)

Automatische Sperre

Die Konfigurationsoption "Automatische Sperre" ist gleichbedeutend mit der Bildschirmsperre an einem PC. Dies bedeutet, dass bei Nichtbenutzung nach Erreichen einer festgelegten Zeitspanne der Bildschirm gesperrt wird. Durch einen niedrigen Wert kann somit sichergestellt werden, dass ein nicht benutztes oder kurzfristig unbeaufsichtigtes Gerät von einem Unberechtigten nicht ohne Authentisierung genutzt werden kann. Bei der Festlegung der Zeitspanne sollten nicht die Werte für einen stationären PC zugrunde gelegt werden, sondern der Einsatzzweck, der Einsatzort, der ermittelte Schutzbedarf, die Anforderungen an die Benutzbarkeit sowie die vereinbarte Komplexität des Passcodes. Für die drei fiktiven Benutzergruppen wird die in der Tabelle aufgeführte Zeitspanne empfohlen.

	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
Automatische Sperre (maximal)	5 Minuten	3 Minuten	2 Minuten

Tabelle 16: Verwendung der Konfigurationsoption „automatische Sperre“

Gerätesperrung

Mit dieser Option wird die Zeitspanne angegeben, innerhalb der die Sperrung des Geräts aufgehoben werden kann, ohne dass der Passcode eingegeben werden muss. Für die drei fiktiven Benutzergruppen wird die in der Tabelle aufgeführte Zeitspanne empfohlen.

	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
Maximale Zeitgrenze für Gerätesperrung	1 Minute	sofort	sofort

Tabelle 17: Verwendung der Konfigurationsoption „Gerätesperrung“

Die sofortige Abfrage des Passcodes bei den Benutzergruppen 2 und 3 liegt darin begründet, dass sich auf dem Gerät vertrauliche Informationen befinden könnten. Für die Benutzergruppe 1 wurde in diesem Beispiel die Benutzbarkeit ein wenig stärker gewichtet und würde so die Möglichkeit der kurzfristigen unautorisierten Benutzung erlauben.

Maximale Anzahl von Fehlversuchen

Mit dieser Option wird festgelegt, nach wie vielen fehlerhaften Passcode-Eingaben alle Daten vom Gerät gelöscht werden. Sollten keine Veränderungen an den werksseitigen Einstellungen vorgenommen worden sein, erzwingt das Gerät nach sechs gescheiterten Versuchen eine Sperrfrist. Erst nach Ablauf der Sperrfrist kann der Passcode erneut eingegeben werden. Diese Sperrfrist verlängert sich automatisch mit jedem weiteren Fehlversuch. Wird die maximale Anzahl an Fehlversuchen gleich oder kleiner als 6 gewählt, wird keine Sperrfrist erzwungen. Beim Erreichen der festgelegten maximalen Anzahl an Fehlversuchen wird sofort das Löschen der Daten vom Gerät ausgelöst. Bisherige teilautomatisierte Angriffe auf den Passcode gingen davon aus, dass gar kein Wert zur Reduzierung der maximal erlaubten Fehleingaben gesetzt ist oder ein Wert von zehn Versuchen und nur ein einfacher Passcode aus vier Nummern genutzt wird. Hierdurch erhalten professionelle Angreifer genügend Spielraum für ein systematisches Ausspionieren des Passcodes. Für die drei fiktiven Benutzergruppen werden die folgenden maximalen Werte empfohlen.

	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
Maximale Anzahl an Fehlversuchen	8	6	3

Tabelle 18: Verwendung der Konfigurationsoption "Maximale Anzahl von Fehlversuchen"

Komplexer Geräte-Code

Mit der Aktivierung des Passcodes wird unberechtigten Dritten der Zugriff auf die Informationen im Smartphone bzw. Tablet verwehrt. Durch Verwendung eines komplexen Passworts wird zusätzlich eine verbesserte Entropie für bestimmte Verschlüsselungscodes zur Verfügung gestellt. Für die drei fiktiven Benutzergruppen werden die folgenden in der Tabelle aufgeführten Werte empfohlen.

Da sich die Verwendung von Sonderzeichen in Passcodes stark auf die Benutzbarkeit auswirkt, sollte ihr Einsatz sorgfältig abgewogen werden. Die Komplexität lässt sich ebenfalls durch eine signifikante Erhöhung der Passwortlänge steigern.

	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
Alphanumerische Werte erforderlich	nein	ja	ja
Sonderzeichen erforderlich	nein	nein	ja (alternativ: Passwortlänge erhöhen)

Tabelle 19: Verwendung eines komplexen Gerätecodes (Passcode)

SYS.3.2.1.M5 Updates von Betriebssystem und Apps (B)

Die Firma Apple stellt in unregelmäßigen Abständen neue bzw. aktualisierte Versionen des Betriebssystems iOS kostenlos für aktuell unterstützte Geräte zur Verfügung. Die Verfügbarkeit einer Aktualisierung wird dem Benutzer über die App "Einstellungen" im Bereich "Allgemein / Softwareaktualisierungen" angezeigt. Die Verantwortlichen müssen zeitnah einen Test auf Kompatibilität mit den aktuell eingesetzten Apps und eingebundenen Infrastrukturkomponenten durchführen. Können keine gravierenden Fehler hinsichtlich Benutzbarkeit, Sicherheit und Zuverlässigkeit festgestellt werden, müssen alle Benutzer darüber informiert und aufgefordert werden, die Geräte innerhalb eines definierten Zeitfensters zu aktualisieren. Die nachfolgende Tabelle benennt Empfehlungen für den Aktualisierungszeitraum und unterstützende Maßnahmen.

Unter aktuellen Versionen von iOS ist es möglich, über MDM-Systeme eine Aktualisierung des Betriebssystems anzustoßen.

Ältere Geräte, für die keine aktuellen iOS-Versionen mehr bereitgestellt werden, müssen im Rahmen des Life-Cycle-Managements rechtzeitig ausgesondert und durch unterstützte Geräte ersetzt werden. Es muss verhindert werden, dass nicht mehr vom Hersteller unterstützte und mit Updates versorgt Geräte im Einsatz sind.

	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
Aktualisierungszeitraum	14 Tage	7 Tage	7 Tage
Unterstützende technische Maßnahmen	keine	nach Ablauf des Zeitraums wird der Zugang zu internen Informationen und Systemen für nicht aktualisierte Geräte gesperrt	nach Ablauf des Zeitraums wird der Zugang zu internen Informationen und Systemen für nicht aktualisierte Geräte gesperrt

Tabelle 20: Etablierung zeitnaher Aktualisierungen des Betriebssystems

SYS.3.2.1.M13 Regelungen zum Screensharing und Casting (S)

Mit AirPlay wird es den Benutzern von iOS-basierten Geräten ermöglicht, ihre Musik, Fotos und Videos an einen AirPlay-Empfänger wie das Apple TV zu streamen. Ein weiterer Einsatzzweck für AirPlay ist die Bildschirmsynchronisation zwischen einem iOS-basierten Gerät und dem Apple TV. Durch die Bildschirmsynchronisation über AirPlay kann in Konferenzräumen der Institution sehr leicht eine Integration der Anwender- und Gastgeräte erfolgen. Die nachfolgend aufgeführten Konfigurationsbeispiele bieten einen optimalen Kompromiss zwischen den Benutzeranforderungen hinsichtlich Flexibilität und den internen Sicherheitsvorgaben der Institution für die drei fiktiven Benutzergruppen.

	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
Code-Eingabe bei erster AirPlay-Verbindung anfordern	ja	ja *)	ja *)

Tabelle 21: Verwendung der Konfigurationsoption für AirPlay

*) Durch das Hinzufügen von Konfigurationsprofilen für die Benutzergruppen 2 und 3, die durch eine Whitelist und Hinterlegung von Passwörtern die erlaubten AirPlay-Ziele beschränken, kann für diese Anwender ein vertretbarer Kompromiss zwischen Benutzbarkeit der Geräte und Sicherheit der Informationen der Institution realisiert werden.

SYS.3.2.1.M28 Verwendung der Filteroption für Webseiten (S)

Unabhängig von der permanenten Einbindung in die Proxy- und Reputationsdienst-Infrastruktur der Institution bietet Apple die Möglichkeit der Erstellung von Filterlisten für erlaubte URLs (diese sind eine Ergänzung der bereits durch Apple vorselektierten URL-Gruppen), Whitelist-URLs, Blacklist-URLs und die externe Einbindung von Inhaltsfiltern von Drittanbietern. An dieser Stelle kann abweichend zu den vorherigen Maßnahmen keine generelle Empfehlung ausgesprochen werden, vielmehr wird die Verwendung der einzelnen Möglichkeiten pro Benutzergruppe aufgezeigt.

	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
Erlaubte URLs	ja	nein	nein
Blacklist-URLs	ja	ja	nein
Nur bestimmte Websites	nein	nein	ja
Plug-in	ja	ja	ja

Tabelle 22: Verwendung der Filteroption für Webseiten - allgemein

Wird durch die Verantwortlichen in der IT bereits ein Reputationsdienst oder eine Proxy-Infrastruktur angeboten, lassen sich die iOS-basierten Geräte durch die Hinterlegung eines globalen HTTP-Proxies für alle installierten Browser darin integrieren. Eine Integration der Geräte in die interne Proxy-Infrastruktur muss mittels einer VPN-Verbindung wahlweise permanent oder basierend auf den verwendeten Apps in die Infrastrukturen erfolgen. Die folgenden HTTP-Proxy-Konfigurationsoptionen können für die Hinterlegung eines globalen Proxy genutzt werden.

	Benutzergruppe 1	Benutzergruppe 2	Benutzergruppe 3
Proxy-Typ	automatisch	automatisch / manuell	manuell
Proxy-Server und -Port	-	Werte bei manueller Proxy-Konfiguration hinterlegen	Werte hinterlegen
Authentifizierung	-	Werte bei manueller Proxy-Konfiguration hinterlegen	Werte hinterlegen
Passwort	-	Werte bei manueller Proxy-Konfiguration hinterlegen	Werte hinterlegen
Proxy-Server-URL	Werte hinterlegen	Werte bei automatischer Proxy-Konfiguration hinterlegen	-
Direkte Verbindung erlauben, wenn PAC nicht erreichbar ist	ja; bei automatischer Proxy-Konfiguration hinterlegen	nein; bei automatischer Proxy-Konfiguration hinterlegen	-
Umgehen des Proxy erlauben, um auf firmeneigene Netzwerke zuzugreifen	ja	ja	ja

Tabelle 23: Verwendung der Filteroption für Webseiten - Proxy-Konfigurationsoptionen

Die Konfigurationsoptionen für die Einbindung der Geräte über eine VPN-Einwahl werden in der Maßnahme SYS.3.2.3.M20 benannt.

SYS.3.2.1.M29 Verwendung eines institutionsbezogenen APN (H)

Diese Konfigurationsoption bestimmt, wie iOS-basierte Geräte die Verbindung zum Mobilfunknetz herstellen. Dies bedeutet, dass bei falschen Einstellungen keine Möglichkeit zur Etablierung einer Datenverbindung besteht. Durch die Verwendung eines institutionsbezogenen APN besteht die Möglichkeit, den möglichen IP-Adressbereich einzuschränken und diesen eingeschränkten IP-Adressenbereich in die Firewall-Regelprozesse und -Freischaltungen aufzunehmen.

2.3 Maßnahmen zum Baustein SYS.3.2.2 Mobile Device Management (MDM)

SYS.3.2.2.M23 Durchsetzung von Compliance-Anforderungen (H)

Die Erkennung von Verstößen gegen interne Regelungen der Institution sollte durch das MDM-Framework des jeweiligen Anbieters sichergestellt werden.

Die Erkennung einer Manipulation des Betriebssystems ist über die Abfrage einer von Apple freigegebenen Schnittstelle nicht vollumfänglich möglich. In Abhängigkeit der Qualität der Verschleierung eines Jailbreaks kann dieser erkannt werden, es ist jedoch von einer geringen Erkennungsrate auszugehen. Bei Verdacht auf Verstoß gegen Regelungen oder auf Manipulation des Betriebssystems sollen die zuvor von den verantwortlichen Administratoren konfigurierten Aktionen selbstständig ausgeführt werden. Aufgrund der unterschiedlichen Implementierungsvarianten der einzelnen MDM-Anbieter besteht keine Möglichkeit, eine allgemeingültige Konfigurationsempfehlung auszusprechen.

3. Weiterführende Informationen

3.1 Wissenswertes

Hier werden ergänzende Informationen aufgeführt, die im Rahmen der Maßnahmen keinen Platz finden, aber dennoch beachtenswert sind. Derzeit liegen für diesen Baustein keine entsprechenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne unter grundschutz@bsi.bund.de entgegen.

3.2 Quellenverweise

[AppleBM] Apple Business Manager: https://support.apple.com/de-de/guide/apple-business-manager/

[AppleConf] Apple Configurator: https://support.apple.com/de-de/apple-configurator

[BSI-TR-02102] BSI TR-02102 "Kryptographische Verfahren: Empfehlungen und Schlüssellängen": https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html