SYS.3.2: Tablet/Phablet/Smartphone

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

1.1 Einleitung

Smartphones und Tablets sind heutzutage ständige Begleiter in der Informationsgesellschaft. Sie sind ständig online, das heißt mit dem Internet oder den internen Ressourcen einer Institution verbunden, und bieten hierdurch jederzeit Zugriff auf digitale Informationen. Aufgrund von modernen, einfachen Bedienkonzepten sowie hoher Leistungsfähigkeit sind Smartphones und Tablets der Firma Apple weit verbreitet im beruflichen Umfeld. 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 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" 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 vertraulich klassifiziert.

Benutzergruppe 2

- Die Benutzer nutzen die zur Verfügung gestellten Smartphones und Tablets zur Telefonie, zum Versenden von E-Mails und zum Bearbeiten geschäftlicher Dokumente.
- 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, zum Versenden von E-Mails und zum Bearbeiten geschäftlicher Dokumente.
- Die Benutzer haben des Weiteren Zugriff auf interne Kollaboration und Dokumentenmanagementsysteme, Finanzdaten oder kritische Systeme der Institution.
- Teilweise sind die Informationen als vertraulich klassifiziert.

1.2 Lebenszyklus

Planung und Konzeption

In der Planungs- und Konzeptionsphase sollen alle eventuellen Nutzungsszenarien, z. B. Einbindung in eine Kollaborations-Lösung, Zugriff auf Warenwirtschaftssysteme sowie der maximal umzusetzende Schutzbedarf, in die Auswahl der zentralen Managementlösung einfließen. Ist eine strikte Trennung zwischen privaten und geschäftlichen Bereichen gewünscht, empfiehlt sich die Überprüfung, ob mittels Managed Apps und Managed Open-in eine Trennung von geschäftlichen und privaten Informationen erreichbar ist. Auch Container-Lösungen sollten in Erwägung gezogen werden. Ebenso sollte in dieser Phase die Überprüfung der Anforderungen an eine benutzerbezogene Integration der Smartphones und Tablets in die Infrastruktur erfolgen. Entsprechend dem Überprüfungsergebnis können Anforderungen an die bisherigen Sicherheitsgateways und deren Funktionen z. B. die automatische Freischaltung von Filter-Regeln für den Benutzer und dessen Geräte oder der automatische Entzug von Zugriffsrechten bei Verletzung aktiver Sicherheitsrichtlinien sein.

In der Planungsphase ist die Vereinbarkeit der allgemeinen Geschäftsbedingungen der Firma Apple mit den geschäftlichen, sicherheitstechnischen und datenschutzrechtlichen Regelungen der Institution zu überprüfen. Ein auf jeden Fall zu betrachtender Punkt ist die Überprüfung der iCloud-Nutzung. Aktuell ist z. B. die Nutzung des iCloud-Accounts nur für den privaten Gebrauch vorgesehen. Eine Übersicht relevanter AGBs ist in Kapitel 3.2 Literatur aufgeführt.

Beschaffung

Bei der Beschaffung von Smartphones und Tablets sowie bei der Auswahl des Mobilfunkproviders sollten neben den wirtschaftlichen Aspekten die sicherheitstechnischen Aspekte einfließen. Beispiele: Wird für eine vereinfachte Grundfilterung der erlaubten IP-Adressen der Geräte ein institutionsspezifischer Access-Point-Name (APN) vom Mobilfunkprovider benötigt? Soll die Authentisierung am VPN-Gateway oder dem Institutions-WLAN auf Basis von EAP-SIM erfolgen? Stellt die Nutzung des Programm zur Geräteregistrierung (DEP) eine flexiblere Alternative dar?

Umsetzung

Es gibt verschiedenste Sicherheitsmechanismen und Herangehensweisen an die Umsetzung zur Erzielung des gewünschten Schutzniveaus bei Smartphones und Tablets. In Kapitel 3 werden Empfehlungen zur Absicherung der Smartphones und Tablets anhand der drei einleitend definierten Benutzergruppen aufgezeigt. Bei der Implementierung der Umsetzungsempfehlungen werden auf die verwalteten Geräte sogenannte Konfigurationsprofile ausgerollt. Das Ausrollen kann mittels Apple Push oder EAS erfolgen. Unabhängig davon, auf Basis welcher Methode die Konfigurationsprofile auf die verwalteten Geräte ausgerollt werden, muss sichergestellt sein, dass Benutzer nicht in der Lage sind, ohne Autorisierung die Konfigurationsprofile zu löschen.

Betrieb

Damit Smartphones und Tablets geordnet und zuverlässig genutzt werden können, müssen technische und organisatorische Maßnahmen umgesetzt werden. Einige der Maßnahmen können nicht zentral und einheitlich über alle Geräte ausgerollt werden und benötigen die Unterstützung durch den

Benutzer. Wird die gleiche Härtungsmaßnahme durch die Verantwortlichen in mehr als einem Konfigurationsprofil auf dem Gerät implementiert, wird durch eine Summierung aller Konfigurationsprofile die jeweils strengere Einstellung auf dem Zielgerät angewendet.

Apple kann bei Vorliegen eines entsprechenden Gerichtsbeschlusses für einen behördlichen Zugriff auf persönliche Benutzerinformationen aus 16 Datengruppen des jeweiligen iCloud-Benutzerkontos sorgen. Die 16 Gruppen werden im Dokument „Legal Process Guidelines“ detailliert beschrieben (siehe Kapitel 3.2). So würden die Strafverfolgungsbehörden z. B. die Informationen über die aktuellen Geo-Daten des Geräts erhalten, Apple-Store-Einkäufe und -Transaktionen, iCloud-Inhalte wie Dokumente sowie die Aktivierungsinformationen, Registrierungsdaten und Game-Center-Verknüpfungen in Augenschein nehmen können.

Aussonderung

Klassischerweise wird für das sichere Löschen von Festplatten ein mehrfaches Überschreiben der Daten empfohlen. Bei Flashspeicher, wie er in iOS-basierten Smartphones und Tablets verbaut ist, können die internen Speicherblöcke bauartbedingt nicht direkt adressiert werden. Dies bedeutet, dass zum Löschen der Daten die Funktionen zum Zurücksetzen des Betriebssystems genutzt werden müssen. Ein Zurücksetzen in den Werkszustand stellt für Informationen mit normalen Schutzbedarf eine ausreichende Methode des Löschens dar. Sollten auf dem Gerät Informationen mit hohem Schutzbedarf verarbeitet oder gespeichert worden sein, ist die Zerstörung des Geräts nach DIN 66399 die sichere Methode.

Notfallvorsorge

Im Zuge der Notfallvorsorge sollten mit Vertragspartnern Vereinbarungen bzgl. des MDM und der Bereitstellung einer ausreichenden Anzahl an Endgeräten getroffen sein. Es sollte außerdem geplant sein, wie etwa mit Verlusten von Endgeräten oder der darauf gespeicherten Daten umgegangen werden soll.

2 Maßnahmen

Im Folgenden sind spezifische Umsetzungshinweise für iOS-basierte Smartphones und Tablets aufgeführt.

2.1 Basis-Maßnahmen

Die folgenden Maßnahmen müssen vorrangig umgesetzt werden:

SYS.3.2.3.M1 Strategie für die iOS-Nutzung

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 BSI IT-Grundschutz zertifizierten Rechenzentrumsdienstleister betrieben werden sollte.

Für eine einfachere Erstinbetriebnahme kann auf die Möglichkeit der Geräteregistrierung über das Apple DEP zurückgegriffen werden. Vertiefende Informationen werden über den in Kapitel 3.2 zur Verfügung gestellten Web-Link bereitgestellt.

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 Backup-Strategie der

Institution.

Abhängig vom geplanten Einsatzzweck muss eine geeignete Endgeräte-Auswahl 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

Bei der Nutzung von Online-Speicher-Diensten (z. B. Microsoft-Cloud, Google Drive, Dropbox, iCloud) 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 des §3 Absatz 1 Bundesdatenschutzgesetz (BDSG) übergeben werden. Eine solche Auftragsdatenverarbeitung ist, in Abhängigkeit vom tatsächlichen Speicherort der Daten, laut §11 BDSG 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.

SYS.3.2.3.M3 Verwendung des Gerätecodes (Passcode)

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 zum Zwecke der Grundabsicherung des Zuganges 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 1: Verwendung des Gerätecodes (Passcode)

SYS.3.2.3.M4 Verwendung der Konfigurationsoption "Automatische Sperre"

Die Konfigurationsoption "Automatische Sperre" ist gleichbedeutend mit der Bildschirmsperre an einem PC. Dies bedeutet, dass bei Nichtbenutzung ein interner Zähler gestartet und nach Erreichen der 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 2: Verwendung der Konfigurationsoption „automatische Sperre“

SYS.3.2.3.M5 Verwendung der Konfigurationsoption „Gerätesperrung“

Da nicht ausgeschlossen werden kann, dass das Gerät nur kurzfristig, z. B. weniger als drei Minuten, unbeobachtet Dritten zugänglich ist, werden die folgenden Empfehlungen für die Umsetzung der oben genannten Maßnahmen unter Beachtung der Kriterien der drei fiktiven Benutzergruppen vorgeschlagen.

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

Tabelle 3: 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 der Telefonfunktion erlauben.

SYS.3.2.3.M6 Verwendung der Konfigurationsoption "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 4: Verwendung der Konfigurationsoption "Maximale Anzahl von Fehlversuchen"

SYS.3.2.3.M7 Verhinderung des unautorisierten Löschens von Konfigurationsprofilen

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 die Integration des Gerätes in die MDM-Infrastruktur mittels des Programm zur Geräteregistrierung (Device Enrollment Program, DEP) durchgeführt, ist der Benutzer automatisch nicht in der Lage, unautorisiert Veränderungen an den Konfigurationsprofilen vorzunehmen.

SYS.3.2.3.M8 Zeitnahe Aktualisierung des Betriebssystems

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" sowie auf dem Home-Screen in der App "Einstellungen" angezeigt. Die Verantwortlichen müssen zeitnah einen Test auf Kompatibilität mit den aktuell eingesetzten Apps und eingebundenen Infrastrukturkomponenten durchführen. Können im Ergebnis 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.

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 5: Etablierung zeitnaher Aktualisierungen des Betriebssystems

Seit der Einführung von iOS 9 ist es möglich, über die Mobile Device Management Systeme eine Aktualisierung des Betriebssystems anzustoßen.

2.2 Standard-Maßnahmen

Gemeinsam mit den Basismaßnahmen entsprechen die folgenden Maßnahmen dem Stand der Technik im Bereich iOS (for Enterprise).

SYS.3.2.3.M9 Verwendung eines komplexen Gerätecodes (Passcode)

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 6: Verwendung eines komplexen Gerätecodes (Passcode)

SYS.3.2.3.M10 Verwendung des Fingerabdrucksensors (Touch ID)

Zur besseren Akzeptanz eines komplexen Passcodes und der hiermit einhergehenden besseren Verschlüsselung der Informationen auf dem Gerät kann auf den Einsatz des Fingerabdrucksensors zurückgegriffen werden. Bei der Nutzung von biometrischen Merkmalen (Fingerabdruck) zum Entsperren ist es einem potentiellen Angreifer möglich, auf der Oberfläche des Gerätes oder von Gegenständen mit glatter Oberfläche die Fingerabdrücke abzunehmen und nachzubauen. 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 Touch ID nach Ablauf von 48 Stunden 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
Touch-ID für das Entsperren des Geräts erlauben	ja	ja	nein
Ändern der Touch-ID-Fingerabdrücke erlauben	ja	nein	nein
Touch-ID verwenden für iTunes und App Store	nein	nein	nein

Tabelle 7: Verwendung des Fingerabdrucksensors (Touch-ID)

SYS.3.2.3.M11 Verwendung nicht personalisierter Gerätenamen

Über den Gerätenamen kann ein Angreifer meist Rückschlüsse auf den Benutzer oder die Institution erlangen. So wird der Gerätename z. B. nach dem Bluetooth-Pairing mit integrierten Multimedia-Systemen oder Freisprecheinrichtungen in modernen Fahrzeugen in diesen 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 der 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

SYS.3.2.3.A12 Verwendung institutionsbezogener Apple IDs

Beim Einsatz einer Apple ID sollte diese mit niemandem geteilt werden, da sie in etwa dem Windows-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, Fotos 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, iBook-Store und bei iTunes einher, sofern diese nicht für geschäftliche Zwecke zuvor über das Programm für Volumenlizenz (VPP) erworben wurden. Ein Vorteil des Einsatzes des VPP ist, dass keine institutionsbezogene Apple ID seitens des Benutzers benötigt wird. Erfolgte die Geräteregistrierung mittels DEP, ist für die dienstliche Nutzung des Gerätes ebenfalls keine institutionsbezogene Apple ID notwendig. Kann auf die geschäftliche Nutzung der iCloud verzichtet werden, sollte durch die Verwendung verwalteter Apps die iCloud-Nutzung auf das Benötigte reduziert oder komplett ausgeschlossen werden. In diesem Fall ist eine institutionsbezogene Apple ID ebenfalls nicht notwendig.

Sollte die Geräteregistrierung nicht mittels DEP erfolgt sein und nicht das VPP genutzt werden, sollte zum Zwecke der Vorsorge vor Verlust geschäftlicher Daten, die auf dem Gerät selbst oder in der iCloud

gespeichert sind, durch den Mitarbeiter eine institutionsbezogene 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 für "Einschränkungen unter iOS"

Zum Zwecke der Sicherstellung der Vertraulichkeit und Integrität der verarbeiteten bzw. auf dem iOS-basierten Gerät gespeicherten Daten sollten alle nicht erlaubten Funktionen oder Dienste deaktiviert sein. Welche empfohlenen Funktionalitäten 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 Netzen, 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 8: Verwendung der Konfigurationsoption für "Einschränkungen unter iOS" - Hintergrundbild

Sperrbildschirm

Über den Sperrbildschirm stehen den Anwendern mannigfaltige Möglichkeiten zur Anzeige von Informationen der werksseitig installierten Apps, wie z. B. die Kalenderübersicht für heute und morgen, die Erinnerungen, die Verkehrslage, das Wetter sowie via Widgets die Informationen der aus dem App-Store installierten und mittels Push-Notification angezeigten Kurznachrichten zur Verfügung. Über das Kontrollzentrum besteht die Möglichkeit, sehr schnell und einfach das Gerät in den Flugmodus zu setzen, aber auch AirPlay für das gesamte Gerät zu aktivieren.

	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 9: Verwendung der Konfigurationsoption für "Einschränkungen unter iOS" - Sperrbildschirm

Die Absicherung von AirPlay wird in der Maßnahme SYS.3.2.3.M16 thematisch vertieft. Einhergehend mit der Freigabe der Mitteilungszentrale und der Ansicht "heute" sollte eine Sensibilisierung der Anwender bzgl. der Nutzung der aneignenbaren Informationen erfolgen und eine Empfehlung ausgesprochen werden, welche Widgets mit welchem Inhalt nicht zu aktivieren sind.

Siri

Siri dient der Erkennung und Verarbeitung der Sprache des Benutzers und ermöglicht hierdurch, die Funktionen eines persönlichen Assistenten umzusetzen. Bei einer bestehenden Internetverbindung werden alle Sprachdaten über eine kryptographisch abgesicherte Verbindung an Server unter der Hoheit von Apple übertragen, auf den Servern verarbeitet, das ermittelte Ergebnis an das Gerät zurückgesandt und zur Weiterverarbeitung angeboten. 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 10: 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 Marketing-Begriff Unified Communication (UC) werden alle Konfigurationsempfehlungen für die von Apple fest integrierten Apps wie FaceTime und iMessage für Video und Nachrichten-Chats zusammengefasst.

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

Tabelle 11: 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 12: 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 dieser 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 13: 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 14: Verwendung der Konfigurationsoption für "Einschränkungen unter iOS" - übergreifend

SYS.3.2.3.M14 Verwendung der iCloud-Infrastruktur

In SYS.3.2.3.M1 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 (siehe SYS.3.2.3.M1), 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“ über den in Kapitel 3.2 hinterlegten Link 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 15: Verwendung der iCloud-Infrastruktur

SYS.3.2.3.M15 Verwendung der Continuity-Funktionen

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 sowie 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, dessen RSS-Abos, 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 behandeln[1]	ja	nein	-
Handoff erlauben	ja	nein	nein

Tabelle 16: Verwendung der "Continuity-Funktionen"

SYS.3.2.3.M16 Verwendung der Konfigurationsoption für AirPlay

Mit AirPlay wird es den Benutzern 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 17: 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, wird für diese Anwender ein vertretbarer Kompromiss zwischen Benutzbarkeit der Geräte und Sicherheit der Informationen der Institution realisiert.

SYS.3.2.3.M17 Verwendung der Gerätecode-Historie

Für die drei fiktiven Benutzergruppen werden Empfehlungen zum Zwecke der Wahrung der Vertraulichkeit des verwendeten Passcodes und zur Verhinderung der zu schnellen Wiederholung desselben durch den Benutzer in der nachfolgenden Tabelle benannt. Bei der Festlegung des Werts können zur besseren Akzeptanz auch die etablierten Regelungen innerhalb der Windows-Domäne oder ähnlichen herangezogen werden.

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

Tabelle 18: Verwendung der Gerätecode-Historie

Für die Benutzergruppe 1 wurde die Wiederholung des ersten ursprünglichen Passwortes bereits nach

1 Wenn diese Option deaktiviert ist, wird AirDrop in einer verwalteten App den Anwendern nicht als Option angeboten.

dem fünften Wechsel ermöglicht. Unter Berücksichtigung der maximalen Passcodegültigkeit (siehe SYS.3.2.3.M3) ist die Wiederholung des ersten Passcode des Benutzers somit nach 600 Tagen möglich.

SYS.3.2.3.M18 Verwendung der Konfigurationsoption für den Browser Safari

Mit dem Betriebssystem iOS liefert Apple den vorinstallierten Browser Safari mit der Möglichkeit der Anpassung durch Konfigurationsprofile mit. 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 19: Verwendung der Konfigurationsoption für den Browser Safari

SYS.3.2.3.M19 Verwendung der Filteroption für Webseiten

Unabhängig von der permanenten Einbindung in die Proxy- und Reputation-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 der externen 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 20: Verwendung der Filteroption für Webseiten - allgemein

Wird durch die Verantwortlichen in der IT bereits ein Reputations-Service oder eine Proxy-Infrastruktur angeboten, lassen sich die iOS-basierten Geräte durch die Hinterlegung eines globalen

HTTP-Proxies für alle installierten Browser integrieren. Für die Verwendung eines globalen Proxies müssen die Apps einen NSURL Aufruf initiieren. 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 21: 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.3.2.3.M20 Einbindung der Geräte in die interne Infrastruktur via VPN

Zum Zwecke der Wahrung der Vertraulichkeit und Integrität der Informationen der Institution sollen die iOS-basierten Geräte 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“ des BSI werden Empfehlungen ausgesprochen für die Verwendung von IPSec und SSL/TLS (siehe Kapitel 3.2). 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 Standardnetzwerk-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

Der Mehrwert iOS-basierter Geräte entsteht meist erst, wenn ein Smartphone oder Tablet integraler Bestandteil der Infrastruktur der Institution ist und im Ergebnis den Anwendern einen umfänglichen Zugang zu den Informationen ermöglicht. Dies bedeutet, dass interne Daten (meist Daten mit einer Vertraulichkeitsklassifizierung) außerhalb der Institutionsinfrastruktur den Anwendern auf deren 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. Im Rahmen des Freigabeprozesses sollten mindestens die folgenden Kriterien geprüft und als Basis für eine Ablehnung oder Freigabe dienen:

- Wird durch die App unberechtigt auf Informationen des Anwenders zugegriffen?
    - Versucht die App, unberechtigt auf die Geo-Daten 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 nicht werbefreie Apps die Gefahr des Anwender-Profiling?
- 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 des Volumenlizenzenprogramms (VPP) für Unternehmen können mittels der nachfolgenden Konfigurationsoptionen und deren Verwendung die Wahrung der Sicherheitsziele 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 22: Einbindung des App-Store und Freigabe von Apps

2.3 Maßnahmen für erhöhten Schutzbedarf

Im Folgenden sind Maßnahmenvorschläge aufgeführt, die über das dem Stand der Technik entsprechende Schutzniveau hinausgehen und bei erhöhtem Schutzbedarf in Betracht gezogen werden sollten. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Maßnahme vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

SYS.3.2.3.M22 Durchsetzung von Compliance-Anforderungen (CI)

Die Erkennung einer Manipulation des Betriebssystems ist über die Abfrage einer von Apple freigegebenen Schnittstelle nicht vollumfänglich möglich. Die Erkennung von Verstößen gegen interne Regelungen der Institution sollte durch das MDM-Framework des jeweiligen Anbieters sichergestellt werden. In Abhängigkeit der Güte der Jailbreak-Verschleierung kann dieser erkannt werden, es ist jedoch von einer geringen Erkennungsrate auszugehen. Bei Verdacht auf Verstoß gegen Regelungen oder 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.

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

Durch die Hinterlegung eines speziellen Ablaufdatums oder eines Ablaufintervalls (Tage und Stunden)

können auf dem Gerät hinterlegte Konfigurationsprofile ohne sonst benötigte Internetverbindung automatisch gelöscht und so sichergestellt werden, 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 Verwendung standortbasierter Policies (CI)

Ein Beispiel für eine Geofencing-Anforderung könnte sein, dass die eingesetzten Geräte das Gelände der Institution nicht verlassen dürfen und beim Verlassen ein Warnhinweis an den Anwender, die verantwortlichen Administratoren und das Sicherheitsmanagement gesendet wird. Durch die zeitliche Verzögerung hat der Anwender die Chance, mit dem Gerät wieder zurück auf das Gelände der Institution zu gehen und so eine Löschung der Informationen oder des Geräts zu verhindern. Durch die aktive Benachrichtigung des Sicherheitsmanagements kann dieses den Sicherheitsvorfall erkennen, durch Sensibilisierungsmaßnahmen die eigenen Anwender schulen und bei einem Diebstahl sicherstellen, dass relevante Informationen das Gelände der Institution nicht verlassen. Diese Art der Absicherung der Informationen mit hohem Schutzbedarf könnte auch auf gesetzliche Territorien z. B. den Bereich des Bundesdatenschutzgesetzes oder des Europäischen Datenschutzraums, angewendet werden. Der Einsatz von Geofencing-Richtlinien darf jedoch nicht gegen interne und gesetzliche Anforderungen verstoßen. Eine mögliche institutionsinterne Auswertung von standortbasierten Daten ist organisatorisch auszuschließen bzw. mit der Personalvertretung abzustimmen.

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

Seitens der Firma Apple wurde die AirPrint-Funktionalität fest in das Betriebssystem eingebaut. Diese Funktion lässt sich nicht grundsätzlich einschalten oder abschalten. Die verantwortlichen Administratoren sollten die in der Institution freigegebenen AirPrint-Drucker durch ein Konfigurationsprofil dem Benutzer 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 (CI)

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 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 Verwendung der Konfigurationsoption für APN

Diese Konfigurationsoption bestimmt, wie iOS-basierte Gerät die Verbindung zum Mobilfunknetz herstellen. Dies bedeutet, dass bei falschen Einstellungen keine Möglichkeit zur Etablierung einer Datenverbindung besteht. Aktuell können APN-Benutzernamen und -Passwörter mit bis zu 64 Zeichen im Konfigurationsprofil definiert werden. 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.

3 Weiterführende Informationen

3.1 Wissenswertes

Derzeit liegen keine über das bereits beschriebene Maß hinausgehenden Informationen vor. Sachdienliche Hinweise nimmt die IT-Grundschutz-Hotline gerne entgegen (grundschutz@bsi.bund.de).

3.2 Literatur

Weiterführende Informationen finden sich unter anderem in folgenden Veröffentlichungen:

- BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html
- Apple-Support-Webseite, https://www.apple.com/de/support/
- Support für Unternehmen und Bildungseinrichtungen, https://www.apple.com/de/support/business-education/
- Programm zur Geräteregistrierung (DEP), https://www.apple.com/de/support/business-education/dep/
- Programm für Volumenlizenzen (VPP), https://www.apple.com/de/support/business-education/vpp/
- Netzwerke und Sicherheit, https://www.apple.com/de/support/business-education/security/
- Apple Configurator, https://www.apple.com/de/support/business-education/apple-configurator/
- Abgekündigte und Vintage-Produkte der Firma Apple, https://support.apple.com/de-de/HT201624
- iOS Sicherheit (iOS9.0 oder neuer), http://images.apple.com/de/business/docs/iOS_Security_Guide.pdf
- Apple-Sicherheitsupdates, https://support.apple.com/de-de/HT201222
- Two-factor authentication for Apple ID, https://support.apple.com/en-us/HT204915
- AGB für iTunes, http://www.apple.com/legal/internet-services/itunes/de/terms.html
- AGB für iCloud, http://www.apple.com/legal/internet-services/icloud/de/terms.html
- AGB für Game-Center, http://www.apple.com/legal/internet-services/itunes/gamecenter/de/terms.html
- Datenschutzrichtlinie von Apple, http://www.apple.com/legal/privacy/de-ww/
- Übersicht der Vereinbarungen rund um die Rubrik Sales und Support, http://www.apple.com/legal/sales-support/
- Access-Point-Name (APN), https://de.wikipedia.org/wiki/Access_Point_Name
- Dokument „Legal Process Guidelines“, https://ssl.apple.com/privacy/docs/legal-process-guidelines-us.pdf
- Anleitung Gerätewiederherstellung, https://support.apple.com/de-de/HT204306?&cid=acs::fm-itunes_HT204306
- Apple-ID, https://appleid.apple.com/de/
- Freigabe von Diagnose- und Nutzungsdaten an Apple, https://support.apple.com/de-de/HT202100
- iCloud Webservice, https://icloud.com
- Übersicht über iCloud-Speicher und iCloud-Backup, https://support.apple.com/kb/PH12519?locale=de_DE&viewlocale=de_DE
- Backups in iCloud und iTunes, https://support.apple.com/de-de/HT204136

- Häufig gestellte Fragen zur „iCloud-Fotomediathek“, https://support.apple.com/de-de/HT204264
- Häufig gestellte Fragen zu „Mein Fotostream", https://support.apple.com/de-de/HT201317
- Häufig gestellte Fragen zur „iCloud-Fotofreigabe“, https://support.apple.com/de-de/HT202786