Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

iOS

Konfigurationsempfehlung auf Basis betriebssystemeigener Mittel für eine Nutzung mit erhöhter Sicherheit

1 Einleitung

Smartphones und Tablet-Computer werden heute zunehmend im Arbeitsumfeld eingesetzt und sind vielfach zum wichtigsten Arbeitsgerät für Mitarbeiter geworden. Mittlerweile gibt es eine nicht mehr zu überschauende Anzahl an Geräten mit unterschiedlichen Betriebssystemen. Smartphones und Tablet-Computer mit iOS, Android oder Windows Phone sind mit modernen, einfachen Bedienkonzepten eher auf den Consumer-Markt ausgerichtet und weniger für den geschäftlichen Einsatz mit hohem Schutzbedarf. Damit unterscheiden sie sich grundlegend von anderen Konzepten mobiler Endgeräte, die speziell für den Unternehmenseinsatz konzipiert wurde. Trotzdem finden Geräte mit iOS und Android zunehmend in der Geschäftswelt Verwendung und verdrängen etablierte Lösungen.

Die Innovation bei mobilen Endgeräten hat in den letzten Jahren viele Neuerungen hervorgebracht und viele Funktionen explizit für den Unternehmenseinsatz und insbesondere die Verwaltung der Endgeräte integriert. Zur Nutzung dieser Funktionen werden vergleichbar zum Desktop Einsatz zentrale Management Dienste benötigt. Diese unterstützen im Gegensatz zu klassischen PCs die Verwaltung der mobilen Endgeräte, auch wenn diese „im Feld“ unterwegs sind. Hierdurch werden speziell die Anforderungen für den Unternehmenseinsatz angesprochen.

In diesen Konfigurationsempfehlungen für iOS, die in Zusammenarbeit mit dem Hersteller Apple erstellt wurden, soll gezeigt werden, welche betriebssystemeigenen Mittel zur Verfügung stehen und wie diese zur Erhöhung der Datensicherheit beitragen. Aufgrund der Herkunft der Geräte aus dem Consumer-Bereich reichen die Konfigurationseinstellungen jedoch nicht aus, um Geschäftsprozesse abzusichern, sodass weitere Maßnahmen erforderlich sind. Zusätzlich soll daher aufgezeigt werden mit welchen Mitteln einer Geräteverwaltung erhöhte Sicherheit umgesetzt werden kann.

In der aktuellen Version von iOS wurden maßgebliche Erweiterungen für den Datenschutz und die Verwaltung in Unternehmen eingeführt, welche in diesem Dokument einbezogen wurden.

In den Empfehlungen wird im Folgenden als mobiles Endgerät immer "iPhone" genannt. Dies ist beispielhaft zu sehen. Gemeint sind die iOS-basierten Geräte iPhone, iPad und iPod touch, jeweils in den Versionen, für die die Empfehlungen zutreffen.

Ebenso werden vom Leser gewisse Vorkenntnisse bezüglich der verwendeten Begriffe erwartet. Beispiele sind hier "App", "Safari" oder "App Store".

2 Einsatzszenarien

Bei der Verwendung von Smartphones und Tablets für berufliche Zwecke können grundsätzlich drei Einsatzszenarien unterschieden werden. Das erste Szenario ist ein rein dienstlicher Gebrauch, bei dem keinerlei private Daten und Zugriffe existieren, das Gerät durch sein Passwort und die verwendete Verschlüsselung geschützt ist und nur definierte Apps verwendet werden können. Das zweite Szenario behandelt eine gemischte Verwendung von dienstlich und privat. Dabei können durch eine Systemkonfiguration private Daten von dienstlichen Daten getrennt werden. Im dritten Fall werden sämtliche beruflichen Belange in einer abgeschlossen, gesicherten Einheit bearbeitet, dem sogenannten "Secure Container". Das Smartphone kann außerhalb dieses Containers normal, das heißt ohne spezielle, restriktive Konfiguration verwendet werden. Mit dem Secure Container können weitere besondere technische Anforderung implementieren werden, wie beispielsweise Mehrfaktorauthentifizierung. Hiermit können besonders schützenswerte Daten zusätzlich abgesichert werden.

In iOS wurden zuletzt Verwaltungsfunktionen zur Trennung von privaten und dienstlichen Daten eingeführt. Ein Beispiel hierfür ist die Funktion „Managed Open-In". Hierdurch wird eine Trennung der Daten möglich, obwohl dem Nutzer in einigen Anwendungen diese gleichzeitig konsolidiert dargestellt werden können.

Für die bestmögliche Verwaltung und Prüfung der Compliance ist der Einsatz einer Mobile Device Management- Lösung (MDM) in Verbindung mit dem Device Enrollment Program (DEP) vorgesehen.

Je nach Schutzbedarf ist abzuwägen, wie die mobilen Endgeräte eingesetzt und verwaltete werden. Für einen niedrigen bis normalen Schutzbedarf reicht der Einsatz der nativen Programme. Für einen erhöhten bis hohen Schutzbedarf sollte eine MDM-Lösung, eventuell in Verbindung mit einem DEP eingesetzt werden. Bei hohem Schutzbedarf und in der Bundesverwaltung empfiehlt das BSI den Einsatz des Secure Containers, weil nur damit eine Wechselwirkung zwischen privater und beruflicher Verwendung des mobilen Endgerätes weitestgehend vermieden werden kann und dienstlichen Daten sicher gespeichert werden können. Siehe dazu auch die Empfehlungen zur Cyber-Sicherheit "Mobile Device Management"[1] der Allianz für Cyber-Sicherheit.

3 Sicherheitsrichtlinien

Bevor mobile Endgeräte in eine Unternehmensstruktur eingebunden werden können, müssen klare Regeln für die Integration festgelegt werden. Mit diesen Sicherheitsrichtlinien, den sogenannten Security Policies, werden
u. a. die Rahmenbedingungen bezüglich Auswahl der Geräte, Auswahl der Daten, die auf den Geräten verarbeitet werden dürfen, Einschränkungen der Benutzer und Limitierung der Möglichkeiten der Geräte (Hardware wie Software) festgelegt.

Neben den Sicherheitsrichtlinien ist auch eine Dienstvereinbarung mit einer klaren Darstellung der Rahmenbedingungen für die Verwendung der mobilen Endgeräte notwendig.

Die Durchsetzung der technischen Anforderungen der Sicherheitsrichtlinien ist bei der steigenden Vielzahl der mobilen Endgeräte nur noch mit entsprechenden Tools erreichbar. Dazu wird eine MDM-Lösung verwendet. Mit dieser können sowohl die Einstellungen auf den Geräten vorgenommen und geprüft, als auch ein Lizenzmanagement institutionell erworbener Apps durchgeführt werden.

Apple hat zusätzlich das Programm "Apple Configurator"[2] veröffentlicht, das für die initiale Konfiguration von iOS-Geräten verwendet werden kann und das weitere Einstellungsmöglichkeiten bietet.

1 https://www.allianz-fuer-cybersicherheit.de/ACS/DE/_/downloads/BSI-CS_052.html
2 https://itunes.apple.com/de/app/apple-configurator/id434433123?mt=12

4 Restrisiken

Selbst bei der Verwendung von sicheren Einstellungen auf dem mobilen Endgerät, die sowohl den Benutzer als auch die Apps weitgehend in ihren Freiheiten einschränken, bleibt ein Restrisiko. Dieses Restrisiko beruht in erster Linie darauf, dass die Geräte außerhalb einer gesicherten Umgebung eingesetzt werden, oft auch in Umgebungen, in denen man einen Laptop nicht einsetzen würde. Es besteht immer die Gefahr, dass die Geräte (und damit die darauf befindlichen Daten) abhandenkommen. In einem solchen Fall kann man nur darauf vertrauen, dass die eingesetzten Mechanismen zum Schutz der Daten noch wirksam greifen und nachträglich initiierte Aktionen (beispielsweise Remote Wipe) funktionieren.

Sogar beim Einsatz eines Secure Containers verbleiben Restrisiken, denen nicht ohne weiteres begegnet werden kann. Als Beispiel sei die unerlaubte Verwendung des Gerätemikrofons zum Abhören genannt.

Grundsätzlich muss Herstellern proprietärer Lösungen ein hohes Maß an Vertrauen entgegengebracht werden. Auch iOS ist ein solches proprietäres mobiles Betriebssystem, dessen Sourcecode nicht offengelegt und nicht überprüfbar ist. Das gesamte "iOS-Ökosystem", inklusive nativen Apps, App-Store, Push-Mechanismen und Clouddiensten unterliegt vollständig der Kontrolle des Herstellers.

Außerdem muss beachtet werden, dass sichere Konfigurationen immer auch Beschränkungen für den Benutzer bedeuten. Dies führt nicht nur zu Akzeptanzproblemen, sondern fördert auch die Fantasie der Benutzer, Grenzen und Beschränkungen zu überwinden.

5 Allgemeine Empfehlungen

5.1 Hardware

Bei der Neuanschaffung von iPhones sollte auf aktuelle Hardware geachtet werden. Geräte, die vom Betriebssystemhersteller nicht mehr unterstützt werden, sollten durch neue ersetzt werden.

Beim Übergang vom iPhone 4S auf das iPhone 5 hat Apple einen Wechsel beim Kabelanschluss vom 30-poligen Dock Connector auf den sogenannten "Lightning Connector" vollzogen. Ältere Hardwareerweiterungen (einschließlich Sicherheitsprodukte, wie beispielsweise Smartcard-Reader) können ab dem iPhone 5 nicht mehr ohne spezielle Adapter verwendet werden.

5.2 Aktualisierungen

Apple stellt in unregelmäßigen Abständen Aktualisierungen beziehungsweise neue Versionen des iOS-Betriebssystems zur Verfügung. Vor dem Umstieg auf eine neue Version von iOS sollte geprüft werden, ob die vorhandenen Geräte noch unterstützt werden und die verwendeten Apps auch mit dem Update einwandfrei funktionieren. Aktualisierungen des installierten Betriebssystems sollten in jedem Fall zeitnah auf die Geräte ausgerollt werden, um bekannte Sicherheitslücken zu schließen.

Informationen zum Sicherheitsinhalt einer iOS-Version sowie Informationen, welche Apple-Geräte durch ein Update unterstützt werden, liefert die Apple-Datenbank[3]. Die Datenbank enthält Updateinformationen zu allen Apple-Produkten, u.a. auch zu iOS. IOS Betaversionen können durch ein kostenpflichtiges Entwicklerprogramm für iOS[4] heruntergeladen und getestet werden. Grundsätzlich ist es empfehlenswert für den Test von Beta Versionen keine Produktivgeräte zu verwenden. Für den Test müssen dediziert iPhones im Apple-Entwicklerprogramm registriert werden. In der Regel ist ein Downgrade von der Betaversion nur auf die aktuelle Version möglich.

3 http://support.apple.com/kb/HT1222?viewlocale=de_DE&locale=de_DE
4 https://developer.apple.com/programs/ios/

Nach einer Aktualisierung sollte überprüft werden, dass die Einstellungen nach der Installation weiterhin unverändert vorliegen und den Anforderungen entsprechen. Durch Updates werden gegebenenfalls neue Funktionen integriert oder aktiviert, welche in der Vorgängerversion nicht enthalten waren. Damit können Konfigurationsänderungen auftreten. Beispiel: Aktivierung der Bluetooth-Funktion mit Einführung von Continuity.

5.3 Synchronisation

Die Synchronisation von Inhalten findet in den meisten Fällen zwischen einem iPhone und einem Desktop-Computer oder mit zentralen Diensten statt. Zentrales Hilfsmittel für den Abgleich mit einem Computer ist das Programm iTunes. Es hält alle Daten vor, die mit dem mobilen Endgerät abgeglichen werden. Synchronisiert werden können Programme, Medieninhalte, Lesezeichen, Bücher, Kontakte, Kalender, Fotos, Notizen, Dokumente und Klingeltöne. Eine Synchronisation kann mittels USB oder im selben WLAN stattfinden. Zusätzliche Informationen finden Sie im Apple-Supportartikel[5].

Wenn Sie in iTunes die Option "Automatisch synchronisieren, wenn dieses iPhone verbunden ist" aktivieren, findet eine Synchronisation statt, sobald das iPhone an den Computer angeschlossen wird. Um das zu verhindern, muss diese Option deaktiviert werden. Zu beachten ist, dass es sich hierbei um keine globale Einstellung in iTunes handelt, die für jedes zu synchronisierende iPhone einzeln vorgenommen werden muss.

Standardmäßig wird jedes iPhone, das an einen Mac oder PC angeschlossen wird, in die dortige iTunes-Bibliothek aufgenommen. Das heißt, dass beispielsweise ein beruflich genutztes Gerät mit einem privaten iTunes-Computer synchronisiert werden kann. Um dies zu verhindern, muss das iPhone in den sogenannten "Supervised Mode" versetzt werden. In diesem Modus geht das Gerät nur mit einem bestimmten Mac eine Synchronisations-Beziehung ein. Näheres dazu siehe Kapitel "Supervised Mode".

5.4 Backup

Damit die Daten des iPhones im Bedarfsfall wiederhergestellt werden können, sollten Sie regelmäßige Backups anlegen. Diese Backups können lokal über iTunes oder in der iCloud angelegt und wiederhergestellt werden. Für das iCloud-Backup benötigen Sie keinen lokalen iTunes-Computer und auch keine Kabelverbindung mehr, sondern nur eine WLAN-Verbindung und eine Apple-ID. Eine Sicherung wird automatisch erstellt, wenn das Gerät gesperrt, mit einem WLAN-Netzwerk sowie einer Stromverbindung verbunden ist. Die Übertragung der Daten, wie auch das Backup selbst auf den iCloud-Servern, ist verschlüsselt. Die Daten werden nach ihrer Verschlüsselungsklasse im verschlüsselten Zustand vom Gerät übertragen und nochmals auf den iCloud-Servern verschlüsselt. Der Verschlüsselungs-Schlüssel dazu wird nicht vom Benutzer, sondern von Apple vergeben. Daten mit der Klasse „No Protection“ werden lediglich für den Transport verschlüsselt und liegen auch im Backup unverschlüsselt vor. Keychain-Inhalte (Passwörter, E-Mail-Accounts, WLAN-Accounts, usw.) werden mithilfe eines Hardwareschlüssels (UID) des Gerätes verschlüsselt und können somit immer nur auf dem Original-Gerät wiederhergestellt werden.

Apple stellt den iCloud-Backup-Dienst unter Vorbehalt zur Verfügung. Hierbei wird weder eine dauerhafte Speicherung der Backup-Daten gewährleistet noch ,dass die Daten "...NICHT VERSEHENTLICH BESCHÄDIGT ODER VERFÄLSCHT WERDEN, VERLOREN GEHEN ODER ENTFERNT WERDEN". Lesen Sie dazu Kapitel "iCloud" und folgen Sie dem Link zu den Nutzungsbedingungen für die iCloud.

Sollten Sie sich dennoch für ein iCloud-Backup entscheiden, können Sie festlegen, welche Daten in der iCloud gesichert werden sollen (Einstellung - iCloud). Wie bei anderen Lösungen

5 http://support.apple.com/kb/HT1386?viewlocale=de_DE&locale=de_DE

auch müssen Sie sich aber bewusst sein, dass Sie keinen Einfluss auf den Schutz der Backup-Daten haben. Der einzige "Schutz"-Mechanismus, der in Ihrem Einflussbereich liegt, ist das Kennwort für die verwendete Apple-ID. Verwenden Sie für die iCloud eine andere Apple-ID als beispielsweise für den Apple Store und verwenden Sie ein ausreichend langes und komplexes Kennwort. Siehe dazu auch Kapitel "Zwei-Faktor-Authentifizierung für Apple-ID" unten.

Das BSI empfiehlt, lokale Backups auf einem externen Datenträger (beispielsweise einer externen Festplatte) in regelmäßigen Zeitintervallen. Sichern Sie diese Backups mit einem Kennwort. In diesem Fall werden die Backups mit dem Passwort verschlüsselt. Bei der Verwendung einer MDM- Lösung oder des „Apple Configurator“ kann die Eingabe eines Kennworts erzwungen werden.

Werden Apps durch ein MDM auf dem iPhone installiert, kann das Backup für die Daten der App deaktiviert werden, insofern das MDM System diese Funktion unterstützt. Das heißt, dass die Einstellungen für eine App, die über ein MDM installiert wird, dahingehend verändert werden, dass die Inhalte der App nicht in ein Backup übernommen werden. Vergleichen Sie hierzu auch den Abschnitt „Managed Open-In”.

5.5 iCloud

Über Apples iCloud können Daten zwischen verschiedenen Apple-Geräten automatisch synchronisiert werden. Damit stehen die Daten automatisch auf allen angemeldeten Geräten zur Verfügung. Es handelt sich um E-Mails, Kontakte, Kalenderdaten, Erinnerungen, Lesezeichen, Notizen, Passbook-Daten, Fotos und Schlüsselbund-Daten, mit denen Zugangsdaten synchronisiert werden. Außerdem können Backups und Dokumente in der iCloud abgelegt werden. Daneben gibt es Apps, welche die Daten vollständig in der iCloud ablegen. Weitere Dienste wie "Mein iPhone suchen" werden auch über die iCloud realisiert.

Bei der Verwendung der iCloud-Dienste wissen Sie nicht, wo Ihre Dokumente, Backups und sonstigen Daten gespeichert werden und ob ihre Daten auf den Servern wieder gelöscht werden, wenn Sie die entsprechenden Optionen auf allen iPhones deaktivieren. Lesen Sie auch die Nutzungsbedingungen[6] für die iCloud.

Trotz der Annehmlichkeiten, die die iCloud mitbringt, empfiehlt das BSI für die berufliche Verwendung von iPhones auf Synchronisierungsdienste über die iCloud zu verzichten. Ebenso empfiehlt das BSI keine dienstlichen Dokumente und Backups in der iCloud zu speichern. Auch sollte kein iCloud-E-Mail-Account verwendet werden.

5.6 Geräteverschlüsselung / Code-Sperre

Mit der Aktivierung der Code-Sperre wird das iPhone automatisch verschlüsselt (Data Protection). Das Schlüsselmaterial wird aus einer Kombination von geräteeigenen Daten (UID - Unique Identification Key) und dem Sperr- Code selbst erzeugt. Die UID ist fest in das iPhone eingebrannt und kann nicht verändert werden. Angreifer, die die Code-Sperre knacken wollen, brauchen demnach zur Entschlüsselung der Daten das Gerät selbst, weil auf einem baugleichen Gerät eine andere UID eingebrannt ist.

Benutzer können nur über die Qualität der Code-Sperre das Schutzniveau der Verschlüsselung beeinflussen. Bei Geräten, die abhandenkommen, braucht ein Angreifer, der im Besitz des Gerätes ist, zurzeit etwa 15 Minuten, um einen 4-stelligen nummerischen Code zu knacken. Bei einem 6-stelligen alphanumerischen Code würden laut Hersteller dagegen fünfeinhalb Jahre benötigt[7].

6 http://www.apple.com/legal/internet-services/icloud/de/terms.html
7 http://images.apple.com/privacy/docs/iOS_Security_Guide.pdf

Aktivieren Sie die Code-Sperre unter *Einstellungen - Allgemein - Code-Sperre* und verwenden Sie einen mindestens 6-stelligen alphanumerischen Code. Stellen Sie den Wert für „Automatische Sperre“ auf einen möglichst niedrigen Wert ein. Mit iOS 9 wird auf einem iOS Gerät mit integrierter „Touch ID“ automatisch ein mindestens 6-stelliger numerischen Code verlangt.

Lesen Sie in diesem Zusammenhang auch den Absatz "Application Data Encryption".

5.7 Zwei-Faktor-Authentifizierung für Apple-ID

Die Apple-ID ist der zentrale Zugang zu den Apple-Diensten iTunes, App Store, iCloud, iMessage, FaceTime usw. Die Account-Daten sind in der Vergangenheit öfter Ziel von Angriffen gewesen. In dem entsprechenden Account werden u. a. auch die Kreditkartendaten gespeichert.

Als neue Sicherheitsfunktion hat Apple die Zwei-Faktor-Authentifizierung für die Verwaltung des Apple-ID-Accounts und für den Einkauf mit einem neuen Gerät im iTunes Store, App Store oder iBookstore sowie iMessage und FaceTime eingeführt. Sie wird über die Internet-Seite zur Apple-ID[8] eingerichtet.

Bei dem Zwei-Faktor-Authentifizierungsverfahren muss neben dem Kennwort eine zusätzliche PIN eingegeben werden. Diese PIN erhält der Benutzer über einen alternativen Weg auf ein registriertes Gerät - entweder als SMS oder über ein anderes iPhone, welches über dieselbe iCloud-ID angemeldet wurde. Diese Geräte werden automatisch als vertrauenswürdige Geräte hinterlegt. Bei der Anmeldung wählt der Nutzer aus, auf welches registrierte Gerät oder welche Telefonnummer der Code gesendet werden soll.

Bei der Wiederherstellung eines Geräts aus einem iCloud-Backups werden alle Apps wieder aus dem App Store geladen und neu installiert. Mit der Einführung von iOS 9 wird dazu für jede dabei verwendete Apple-ID der zweite Faktor abgefragt.

5.8 Wi-Fi (WLAN)

Smartphones, wie das iPhone, sind nur sinnvoll einsetzbar, wenn sie Zugang zum Internet haben. Die hauptsächlichen Kommunikationskanäle sind dabei das Mobilfunknetz über die SIM-Karte des Providers sowie im Nahbereich Wi-Fi (WLAN). Problematisch sind unverschlüsselte WLANs, etwa an öffentlichen Orten. In diesen Netzen kann potentiell jeder den Netzwerkverkehr mitlesen.

In solchen Netzen werden Ihre Daten durch den Einsatz eines Virtual Private Networks[9] (VPN) im sonst unverschlüsselten Netzwerkverkehr verschlüsselt, sodass ein Angreifer die Daten zwar noch mitlesen kann, sie aber nicht mehr versteht. Die Verwendung von VPN ist jedoch mit Aufwand verbunden, da die Gegenseite der Kommunikationsstrecke ebenso VPN unterstützen muss. Im dienstlichen Umfeld ist dieser Aufwand aber in jedem Fall gerechtfertigt.

Obwohl für den Nutzer ein Komfortfaktor, kann es aus Sicherheitssicht kritisch sein, dass sich ein iPhone die WLANs, in die es einmal eingebucht war, anhand des WLAN-Namens (SSID) merkt. Kommt das Gerät zu einem späteren Zeitpunkt wieder in den Funkbereich eines solchen WLANs, verbindet sich das iPhone automatisch. Um diese Komforteinrichtung auszunutzen, muss ein Angreifer nur wissen, dass Ihr iPhone einmal in einem bestimmten unverschlüsselten öffentlichen WLAN eingebucht war und kann dem iPhone dann ein eigenes WLAN mit der gleichen SSID präsentieren. Das iPhone verbindet sich automatisch. Dies ist besonders an öffentlichen Plätzen wie Flughäfen kritisch.

8 https://appleid.apple.com/
9 http://de.wikipedia.org/wiki/Virtual_Private_Network

Um ein WLAN aus der Merkliste des iPhones zu entfernen, klickt man in Einstellungen - WLAN bei dem entsprechenden WLAN auf "Dieses Netzwerk ignorieren". Das geht aber nur, wenn das iPhone momentan in dem Netzwerk eingebucht ist. Alternativ kann man in Einstellungen - Allgemein - Zurücksetzen - alle Netzwerkeinstellungen zurücksetzen. Damit werden alle gespeicherten WLANs gelöscht. Anschließend verbindet man sich erneut mit den bekannten und gesicherten WLANs.

Generell sollten Sie die WLAN-Funktion in unsicheren Umgebungen nur bei gleichzeitiger Verwendung eines VPN aktivieren oder komplett deaktivieren (Einstellungen – WLAN). Gleiches gilt, wenn sie überhaupt nicht gebraucht wird.

WLAN-Unterstützung
Mit iOS 9 wurde die neue Funktion WLAN-Unterstützung oder im englischen „Wi-Fi Assist“ integriert. Mit dieser wird es ermöglicht, bei einer schlechten WLAN-Verbindung anstatt des WLANs - automatisch - das Mobilfunknetz zur Datenverbindung verwendet wird. Diese Funktion belastet allerdings den genutzten Datentarif, teilweise können hohe Kosten entstehen. Die Funktion wird nicht verwendet, wenn sich das iPhone im Roaming befindet.

WLAN-Unterstützung kann man in *Einstellungen - Mobiles Netz* deaktivieren. In diesem Fall verhält sich das iPhone wie unter iOS 8 und früher.

Weitere Informationen zu den Einstellungen und zur Nutzung von mobilen Daten auf iPhone und iPad (Cellular-Modell) entnehmen Sie dem Apple Support Artikel[10].

5.9 Persönlicher Hotspot

Eine weitere Verbindungsart per WLAN ist die Einstellung "Persönlicher Hotspot" (*Einstellungen - Persönlicher Hotspot*). Bei Aktivierung auf Ihrem Gerät stellen Sie anderen Nutzern Ihren Internetzugang (UMTS/LTE über die SIM-Karte) zur Verfügung. Die Verbindung selbst ist sowohl passwortgeschützt als auch verschlüsselt (WPA2) und sicherheitstechnisch eher unkritisch; die Daten werden im iPhone einfach durchgereicht. Für Sie fallen höchstens zusätzliche Verbindungskosten an. Als zusätzliche Sicherheitsmaßnahme sollten Sie das voreingestellte Kennwort durch ein eigenes, komplexes ersetzen.

Anders herum gesehen können Sie Ihr iPhone aber auch mit einem Ihnen angebotenen Hotspot verbinden. Hier ist Vorsicht geboten. Ihr iPhone "sieht" nur einen WLAN-Zugang. Theoretisch muss die Verbindung dazu nicht verschlüsselt sein, was zur Problematik des oben genannten öffentlichen WLANs führt. Auch wissen Sie nicht, was auf dem anderen mobilen Endgerät passiert. Werden Ihre Daten dort auch nur durchgereicht oder sind eventuell "Zwischenschichten" eingebaut, die Ihre Daten mitlesen?

Verzichten Sie daher weitgehend auf die Verbindung zu "Persönlichen Hotspots" beziehungsweise akzeptieren Sie diese im Ausnahmefall nur von vertrauenswürdigen Personen.

Der Persönliche Hotspot kann auch durch die neue Funktion Continuity im Hintergrund aktiviert und verwendet werden. Siehe dazu auch das Kapitel "Continuity".

Hinweis: Die Verbindung zu einem persönlichen Hotspot funktioniert nicht nur über WLAN, sondern auch per Bluetooth und USB-Kabel. Bei der Verbindung über Bluetooth ist zu beachten, dass bei Deaktivierung des persönlichen Hotspots die Kopplung (Pairing) der Bluetooth-Verbindung nicht immer automatisch beendet wird. Dieses Phänomen ist geräteabhängig. Prüfen Sie daher nach der Deaktivierung des persönlichen Hotspots die Bluetooth-Verbindung.

10 https://support.apple.com/en-us/HT201299

5.10 Bluetooth

Die im Abschnitt Wi-Fi erwähnte Merkliste für bekannte WLANs existiert in ähnlicher Form auch bei Bluetooth. Zu beachten ist, dass der Mechanismus zum allgemeinen Löschen der Merkliste von Netzverbindungen (*Einstellungen - Allgemein - Zurücksetzen - Netzwerkeinstellungen*) für Bluetooth nicht wirkt. Erst wenn man in *Einstellungen - Bluetooth - Devices* auf *"Dieses Gerät ignorieren"* klickt, wird das spezielle Gerät entkoppelt und aus der Merkliste entfernt.

Die Bluetooth-Schnittstelle ist immer wieder Ziel von Angriffsversuchen. Deaktivieren Sie die Bluetooth-Funktion, wenn Sie sie nicht benötigen. Sollte Ihr iPhone oder ein gekoppeltes Bluetooth-Gerät verloren gehen, denken Sie daran, die Verbindungsschlüssel in den verbleibenden Geräten zu löschen.

5.11 Schutzprogramme

Aus Sicht des BSI ist ein gesondertes Virenschutzprogramm auf mobilen Endgeräten zurzeit nicht erforderlich.

Betriebssysteme, wie iOS, sind über die Rechtestruktur für Apps verhältnismäßig gut abgesichert. Das Sandbox- Prinzip verhindert den Zugriff auf Daten außerhalb der Ablaufumgebung, den Zugriff von außen auf App-Daten sowie zwischen Apps. Bei den verschiedenen mobilen Plattformen ist der Grad der Abschottung insgesamt jedoch durchaus unterschiedlich. iOS gibt sich innerhalb des Apple-Ökosystems geschlossener als andere mobile Betriebssysteme, die Programmierern mehr Freiheiten lassen und teilweise auch alternative App-Stores zulassen.

Wegen der genannten Abschottung durch die Sandbox können Schutzprogramm-Apps weder auf andere Apps, noch auf das Betriebssystem zugreifen. Die verbleibenden Datenbestände reichen jedoch nicht für eine umfassende Schutzwirkung wie sie auf Desktop-Computer stattfindet.

Schutzprogramme (AV-Apps) bieten neben der Erkennung von Malware oft weitere Funktionen, wie zum Beispiel Diebstahlschutz, "Parental Control", Verschlüsselung, "Safe Browsing", usw. Im Unternehmensumfeld werden diese Funktionen überwiegend durch die sowieso notwendige Mobile Device Management-Lösung erbracht und können dort durch den Administrator zentral gesteuert werden. Für den Bereich „Safe Browsing“ und Phishing-Schutz lesen Sie bitte das Kapitel "Internet-Browser".

Wichtig ist aus Sicht des BSI, dass die Anwender auf die Risiken hingewiesen werden, die durch sogenanntes "Jailbreaken" bzw. "unsichere" App-Stores entstehen. Beim Jailbreak werden die durch die Rechtestruktur des Betriebssystems gegebenen Sicherheitsmechanismen außer Kraft gesetzt. Programme können mit Root-Berechtigung ablaufen und sind nicht mehr kontrollierbar. Sie könnten sich im System auch jenseits einer Erkennungsmöglichkeit von AV-Apps festsetzen.

Die Anzahl schadhafter Apps in "sicheren" App-Stores ist gering. Taucht im App-Store ein Malware-Paket auf, ist der Anbieter des Stores, d. h. im Falle von iOS Apple gefordert, um betroffene Anwender zu warnen. Der Anbieter könnte sogar eine schadhafte App wieder von den Geräten deinstallieren.

5.12 Supervised Mode / Betreuung

Der "Supervised Mode" bietet erweiterte Verwaltungsmöglichkeiten über eine MDM-Lösung auf einem iPhone, welche im Normalfall nicht verfügbar sind. Der Modus kann ausschließlich bei Aktivierung des iPhones aktiviert bzw. deaktiviert werden. Erweiterte Möglichkeiten sind zum Beispiel die Unterbindung der Kopplung mit Host Systemen, Deaktivierung des Menüs

Einschränkungen und der Möglichkeit ein iPhone über *Alle Inhalte und Einstellungen löschen* zurückzusetzen und einige mehr.

Der „Supervised Mode“ kann entweder über das Programm "Apple Configurator" oder das DEP (vgl. Device Enrollment Program) aktiviert werden. Der „Apple Configurator“ kann in kleineren Unternehmen auch als Konfigurations-Tool und für die Grundeinstellung neuer Geräte eingesetzt werden und iPhones weitgehend über die USB Schnittstelle konfigurieren. Das Tool kann sowohl Konfigurationsprofile als auch Apps installieren. Es ist kostenlos, setzt aber einen Mac-Rechner voraus.

Wie oben beschrieben, bietet der „Supervised Mode“ auch den Vorteil, dass iPhones gefahrlos an fremde Ladestationen angeschlossen werden können.

Hinweis 1: Beim Einstellen des "Supervised Mode" über den „Apple Configurator“ wird das iPhone vollständig gelöscht. Vorhandene Daten sollten erst gesichert werden, bevor der Supervised Mode eingeschaltet wird.

Hinweis 2: Bei Mac-Rechner mit deutscher Spracheinstellung wird der „Apple Configurator“ auch in deutschsprachiger Übersetzung installiert. Im Programm heißt der Reiter "Supervise" dann "Betreuen".

5.13 AirDrop

Über AirDrop können Daten zwischen Apple-Geräten ausgetauscht werden. Die Kommunikation geschieht über ein temporäres ad-hoc Netzwerk (WLAN und Bluetooth) von Gerät zu Gerät. Für die Zeit der Datenübertragung wird eine verschlüsselte Datenverbindung, unabhängig von den bestehenden Verbindungen, aufgebaut. Mit Beendigung der Übertragung wird die Verbindung automatisch wieder abgebaut.

Mit iOS 9 wurde eine neue Einschränkung eingeführt, welche AirDrop als nicht verwalteten Zielort behandelt. Diese Einschränkung muss als Profil bei verwalteten Geräten installiert werden. Wenn diese Einschränkung aktiviert wurde und zusätzlich die Funktion „Managed Open-In“ verwendet wird, können Dokumente aus verwalteten Apps nicht mehr über AirDrop verteilt werden.

Wie auch bei anderen Schnittstellen sollte auch AirDrop abgeschaltet werden, wenn es nicht benötigt wird.

5.14 Vertrauenswürdige Verbindung

Zum Schutz vor unautorisiertem Zugriff über die USB-Schnittstelle auf ein iPhone hat Apple ein Kopplungsmodell eingeführt, welches den Zugriff von einem Hostrechner auf ein iPhone steuert. In der Vergangenheit war es möglich, dass, solange das iPhone entsperrt war, Hostsysteme über USB ungehindert auf ein iPhone zugreifen konnten. Seit iOS 7 überprüft das iPhone die Verbindung zum Host, ob dieser vom Nutzer als vertrauenswürdig definiert wurde. Handelt es sich beim Verbindungsaufbau um einen unbekannten Host, wird der Nutzer explizit darauf hingewiesen. Der Nutzer muss dem Zugriff auf sein iPhone zustimmen. Durch diese Funktion wird der Zugriff auf das iPhone durch beispielsweise ein manipuliertes Ladegerät unterbunden und die Sicherheit maßgeblich erhöht.

Bei Supervised-Geräten bestand hier bereits die Möglichkeit diese Kopplung komplett zu unterbinden und den Datenaustausch zu einem Host zu verbieten.

Benutzer sollten dahingehend geschult werden, dass sie keine vertrauenswürdige Verbindung mit einem fremden, nicht autorisierten Host eingehen.

5.15 Continuity

Mit Continuity besteht die Möglichkeit, dass alle Geräte, die mit derselben iCloud-ID konfiguriert wurden, Inhalte direkt miteinander austauschen können, sofern sie sich im selben WLAN und in unmittelbarer Entfernung befinden. Hierbei kommt neben WLAN auch Bluetooth zum tragen. Unterstützt werden hierbei die Übertragung von Dokumenten innerhalb unterstützter Apps, wie zum Beispiel Mails, welche Sie auf dem iPhone begonnen haben und auf dem Mac fortführen wollen, als auch umgekehrt. Auch können Telefonate am Mac oder einem anderen iOS Gerät angenommen, bzw. initiiert werden. Zudem kann auch der „Personal Hotspot“ des iPhones automatisch verwendet werden, auch wenn dieser in *Einstellungen - Persönlicher Hotspot* deaktiviert ist. Diese Funktionalität wird als "Instant Hotspot" bezeichnet.
Steht ein entsprechendes Dokument zur Fortführung bereit, wird dies entweder mit einem entsprechendem Icon im iOS Lock Screen (oder im OS X Dock) angezeigt. Bei Verwendung des Icons wird das entsprechende Dokument auf das andere Gerät übertragen.

Wie auch bei anderen Schnittstellen sollte auch Continuity abgeschaltet werden, wenn es nicht benötigt wird. Die Funktion kann über *Einstellungen - Allgemein - Handoff & App-Vorschläge - Handoff* deaktiviert werden.

5.16 Per App-VPN

„Per App VPN“ steht für verwaltete Apps zur Verfügung, vgl. auch „Managed Open-In”. Mit dieser Option kann einer verwalteten App ein dedizierter VPN-Tunnel zugewiesen werden, welcher automatisch bei Verwendung der App initiiert und nach Inaktivität beendet wird. Im Gegensatz zu einer klassischen VPN-Konfiguration terminiert nicht das gesamte iPhone den Tunnel, welcher allen darauf installiert Apps Zugriff auf das Intranet des Unternehmens bietet, sondern nur die definierten Apps. Hierdurch wird ein verbesserter Schutz des Unternehmensnetzwerkes gegenüber unautorisierten Zugriffen bei privater Verwendung des iPhones geboten.

Neben den verwalteten Apps kann „Per App VPN“ auch für Safari-Domänen konfiguriert werden. Wird in Safari eine entsprechende Domäne geöffnet, wird automatisch der VPN-Tunnel aufgebaut und der Browser kann die Intranet Dienste des Unternehmens nutzen. Da Safari auf der Sandboxing-Technologie beruht, kann nur der aktive Tab des Browsers auf das Unternehmens-Intranet zugreifen.

Da die VPN Verbindung nicht auf Geräteebene sondern auf App Ebene aufgebaut wird, wird im Unternehmen hierfür eine SSL/TLS-VPN oder seit iOS 9 eine IKEv2 VPN-Infrastruktur mit Unterstützung von „Per App VPN“ benötigt. Gegebenenfalls ist die Installation eines entsprechenden Clients auf dem iPhone notwendig. Weitere Informationen dazu im Support-Artikel des Herstellers[11].

5.17 VPN Always-on

Soll sämtlicher Datenverkehr eines iPhones über das unternehmenseigene Netzwerk laufen, bietet sich die Funktion *„VPN* always-on“ in Verbindung mit dem Protokoll IKEv2[12] an. Diese Funktion bietet die Tunnelung sämtlichen Datenverkehrs des Gerätes, unabhängig von WLAN oder Mobilfunknetz, über das VPN-Gateway des Unternehmens.

Weitere Informationen dazu im entsprechenden Apple-Dokument[13].

11 https://help.apple.com/deployment/ios/#/apdfbf6f529b
12 Internet Key Exchange: siehe: http://en.wikipedia.org/wiki/Internet_Key_Exchange
13 https://help.apple.com/deployment/ios/#/iore8b083096

5.18 Auto-Updates

Apps und ihre Updates können bei iOS automatisch installiert werden. Diese Funktion muss explizit für die verwendete „Apple ID“ aktiviert werden. Damit sind die Programmversionen nicht mehr unter der Kontrolle des Unternehmens oder Benutzers. Dieses Feature sollte abgeschaltet werden (*Einstellungen - iTunes und App* Store - *Automatische Downloads*). Updates sollten vor der Verteilung durch den Administrator getestet werden.

Zusätzlich besteht für Apps die Möglichkeit, ihre Inhalte automatisch im Hintergrund über das Mobilfunknetz oder WLAN zu aktualisieren, um dem Nutzer bei der nächsten Nutzung aktuelle Informationen anbieten zu können (*Einstellungen - Allgemein - Hintergrundaktualisierung*). Auch diese Funktion sollte nur im begründeten Bedarfsfall aktiviert werden.

5.19 iOS Update durch die IT-Administration

Mit iOS 9 und einem MDM kann seitens der IT-Administration ein Update für iOS für die verwalteten iPhones angestoßen werden. Dieser Prozess gewährleistet, dass alle iPhones denselben Versionsstand haben, beziehungsweise kritische Sicherheitsupdates installiert werden.

Die aktuelle Implementierung erfordert für eine automatische Installation des Updates, dass das iPhone über keinen PIN-Code verfügt. Wurde es mit einem PIN-Code versehen, wird der Nutzer zur Installation aufgefordert und anschließend nach dem PIN-Code gefragt, um die Installation durchführen zu können.

Mit dieser neuen Funktion ist eine Aktualisierung der iPhones durch die IT-Administration möglich, die nicht verhindert werden kann.

Für eine automatische Installation ohne Nutzeraktion wäre ein Gerät ohne PIN-Sperre notwendig. Diese Installationsart sollte in keinem Falle verwendet werden, da damit eine elementare Sicherheitsfunktion außer Kraft gesetzt wird.

5.20 Activation Lock

Die Aktivierungssperre greift für die Aktivierung eines iPhones für die Ersteinrichtung. Ein Gerät, bei dem die Aktivierungssperre eingerichtet ist, kann nur mit Hilfe der genutzten iCloud-Anmeldedaten reaktiviert und damit genutzt werden.

Hat der Nutzer ein iCloud Konto auf dem iPhone konfiguriert und die Funktion “Mein iPhone suchen” aktiviert, wird automatisch die Aktivierungssperre für das Gerät aktiviert. Wird ein iPhone auf den Auslieferungszustand zurückgesetzt (*Allgemein - Zurücksetzen sowie Remote-Funktion*), ist für die Neu-Aktivierung des Gerätes sowohl der Accountname als auch das Passwort der iCloud ID notwendig, um die Aktivierung durchzuführen. Gestohlene iPhones ab iOS 7 sind damit für den Dieb im Prinzip wertlos.

Die Aktivierungssperre wird durch Deaktivierung der Funktion “Mein iPhone suchen” ebenfalls deaktiviert. Außerdem wird die Funktion deaktiviert, wenn das Gerät durch “*Alle Dokumente und Einstellungen löschen*” in den Auslieferungszustand versetzt wird.

Bei der Rücknahme eines dienstlichen iPhones sollte daher darauf geachtet werden, dass das iPhone nicht durch die Funktion „Remote Wipe” gelöscht wird, sondern in den Auslieferungszustand zurückgesetzt wird. Im Zweifelsfall kann dies auch über das iCloud-Konto[14] geschehen.

Weitere Information zur Aktivierungssperre im entsprechenden Apple-Dokument[15].

14 http://icloud.com/
15 http://support.apple.com/kb/PH13695?viewlocale=de_DE

5.21 Enterprise Single Sign-On

Gerade bei Smartphones mit relativ kleinen Tastaturen ist die Eingabe von komplexen Kennwörtern schwierig. Bei mehreren Enterprise-Apps, die alle passwortgeschützt sind, führt dies dazu, dass der Benutzer kurze, einfache Zugangscodes verwendet. Bei Single Sign-On authentifiziert sich der Benutzer nur einmal gegenüber den Unternehmensservern. Das Betriebssystem übernimmt dann für alle "registrierten" Apps die weitere Anmeldung. Durch den Wegfall der lästigen Mehrfacheingabe steigt auch die Akzeptanz für ein komplexes Kennwort. Neben der Verwendung von Passwörtern können auch Zertifikate genutzt werden.

Weitere Information zur Aktivierungssperre im entsprechenden Apple-Dokument[16].

5.22 Notification Sync

Bei „Notification Sync“ handelt es sich um einen iCloud-Dienst, der dafür sorgt, dass Mitteilungen (Notifications) auf die verschiedenen iPhones des Benutzers synchronisiert werden. Auf allen Geräten erscheint die gleiche Mitteilung und verschwindet auch wieder von allen Geräten, wenn der Benutzer sie auf seinem aktuellen Gerät löscht. Da es sich um einen Cloud-Dienst handelt, sollten Sie genau abwägen, ob Sie einen solchen Dienst in Anspruch nehmen.

5.23 SMS Weiterleitung

Verwenden mehrere iOS Geräte und Macs dieselbe „Apple ID“ für den iMessage-Dienst, kann unter iOS 8 die Weiterleitung von SMS dediziert für weitere Geräte aktiviert werden. In diesem Falls werden am iPhone eingehende SMS auf allen aktivierten Geräten angezeigt. (*Einstellungen - Nachrichten - Weiterleiten von SMS*)

Diese Einstellung sollte nur im Bedarfsfall aktiviert werden.

5.24 Managed Open-In

Eine App kann sich in iOS als Kandidat für die Bearbeitung bestimmter Dateitypen (beispielsweise zur Anzeige von PDF-Dokumenten) registrieren. Wählt der Benutzer in einer anderen App - etwa im Browser - bei einem solchen Dokument die Option "Öffnen in", wird die registrierte App in einem Auswahlmenü aufgelistet. Dies kann zu einem Sicherheitsproblem führen, wenn sensible Daten unbedacht mit ungeeigneten Apps (beispielsweise soziale Netzwerke oder Clouddienste) geöffnet werden.

Unter iOS werden Apps, welche über ein MDM installiert wurden, automatisch als verwaltete Apps gekennzeichnet. Hierzu stehen Enterprise-Apps oder über das sogenannte Volume Purchase Program[17], kurz VPP, bezogene Apps zur Verfügung. Dem gegenüber werden die durch den Nutzer installierten Apps als nicht verwaltet gehandhabt. Innerhalb einer MDM-Lösung bietet sich die Möglichkeit, dass das Öffnen von Dokumenten aus verwalteten Apps in nicht verwaltete Apps und das Öffnen von Dokumenten aus nicht verwalteten Apps in verwaltete Apps, unterbunden werden kann. Der “Öffnen in” Dialog bietet in diesem Fall nur die entsprechend konfigurierten Apps an.

Hierdurch wird eine Trennung von dienstlichen und privaten Daten erreicht und eine Abwanderung von einem Bereich in den anderen unterbunden. Wurde ein E-Mail-Account über das MDM konfiguriert gelten dieselben Regeln und E-Mailanhänge können nur in verwalteten Apps geöffnet werden.

Neben den verwalteten Apps werden verwaltete Bücher, Document Provider, Tastaturen und Domänen unterstützt.

16 https://help.apple.com/deployment/ios/#/apdf5b35aad2Sync
17 https://www.apple.com/de/business/programs/

Hinweis 1: Mit iOS 9 können Apps und deren Updates über MDM mittels VPP auch installiert werden, wenn der App-Store auf dem iPhone deaktiviert wurde.

Hinweis 2: Mit iOS 9 besteht die Möglichkeit, über ein MDM nicht verwaltete Apps in verwaltete Apps zu migrieren. Da es sich um vom Nutzer installierte Apps handelt, ist dieser über diese Änderung zu informieren, da seine privaten Daten nicht mehr mit seinen eigenen Apps ausgetauscht werden können.

Weitere Information zur „Managed Open-In“ siehe hier[18].

5.25 Application Data Encryption

Grundsätzlich sind alle Daten eines iPhones verschlüsselt gespeichert. Das hierfür benötigte Schlüsselmaterial ist in einem Hardwarebaustein fest eingebrannt. Die Frage ist, in welchem Zustand des Geräts auf die Daten zugegriffen werden kann, das heißt, wann das Schlüsselmaterial für die Entschlüsselung der Daten zur Verfügung steht. Apple definiert verschiedene Klassen, denen die Daten zugeordnet werden.

Complete Protection
Das Schlüsselmaterial steht zur Verfügung, wenn das Gerät entsperrt ist. Nach dem Sperren des Geräts wird das Schlüsselmaterial wieder vernichtet.

Protected Unless Open
Solange eine Datei geöffnet ist, steht ein individueller Dateischlüssel zur Verfügung. Wird die Datei geschlossen, wird auch der Schlüssel vernichtet. Diese Klasse wird beispielsweise für Downloads im Hintergrund verwendet.

Protected Until First User Authentication
Nach einem Reboot sind die Daten dieser Klasse bis zum ersten Entsperren nicht zugreifbar. Nach der ersten Benutzer-Authentisierung (über die Code-Sperre) bleibt das Schlüsselmaterial bis zum Herunterfahren im Speicher.

No Protection
Das Schlüsselmaterial steht bei eingeschaltetem Gerät ständig zur Verfügung. Sinn dieser Klasse ist im Prinzip nur die Funktion "Remote Wipe", bei der die Schlüssel im Bedarfsfall einfach gelöscht werden. Damit sind die Daten nicht mehr zugreifbar.

In iOS sind die Daten von Drittanbieter-Apps - bei Verwendung der Code-Sperre - bis zum ersten Unlock nicht zugreifbar. Das heißt, dass der Benutzer sich am Gerät mit der PIN erst authentifizieren muss, bevor die Daten zugreifbar sind.

Unabhängig davon haben Programmierer die Möglichkeit, Daten mithilfe dieser Schutzklassen zu sichern. Je nach Schutzbedarf sollte bei eigen-entwickelten Apps auf die Verwendung der geeigneten Schutzklasse geachtet werden.

5.26 Sicheres Löschen

Eine wichtige Frage im Rahmen des Life Cycle Management von iOS Geräten ist das sichere Löschen eines Endgerätes im Falle einer Außerbetriebsetzung oder eines Reparaturfalles. Grundsätzlich ist in beiden Fällen anzuraten zuvor ein Backup des Gerätes vorzunehmen, um die Daten auf einem neuen Gerät wieder herstellen zu können. Nähere Informationen hierzu liefert ein Artikel des Herstellers[19].

18 https://help.apple.com/deployment/ios/#/iorf4d72eded
19 http://support.apple.com/de-de/ht4946

Vor Außerbetriebnahme ist das iPhone sicher zu löschen. Gehen Sie hierzu in die *Einstellungen* des iOS und wählen Sie unter *Allgemein* die Option *Zurücksetzen*. Mit *Alle Inhalte und Einstellungen löschen* werden sämtliche Inhalte gelöscht. Da die Daten des Dateisystems verschlüsselt sind, reicht zum Löschen der Daten, das Schlüsselmaterial zu entfernen.

5.27 Device Enrollment Program / DEP

Das „Device Enrollment Program[20]", kurz DEP, bietet für Unternehmen die Möglichkeit, dass neue iPhones einem MDM Servern zugewiesen und somit automatisch verwaltet werden können, ohne das eine Interaktion mit der IT-Administration oder durch den Nutzer notwendig ist.

Dazu muss sich ein Unternehmen für das DEP-Programm registrieren[21] und autorisierte Handelspartner, über welche die Geräte bezogen werden, benennen. Der Handelspartner wird über eine sogenannte DEP-Reseller-ID identifiziert. Das Unternehmen benötigt eine DEP-Customer-ID.

Durch das DEP wird eine erhöhte Sicherheit für die Anwendung im Unternehmen erreicht. Einstellungen werden automatisch auf das iPhone ausgerollt und entsprechend der Compliance-Regeln umgesetzt. Ein Abweichen von diesem Prozess ist dem Nutzer nicht möglich, da selbst bei Zurücksetzen des iPhones der Prozess wieder von vorne beginnt. In diesem Sinne wird ähnlich der Aktivierungssperre auch ein erhöhter Diebstahlschutz erreicht, da das iPhone ohne Nutzerauthentifizierung nicht verwendet werden kann.

Weitere Information zu „Device Enrollment Program" im Support-Artikel des Herstellers[22].

Hinweis 1: Werden iPhones über das DEP entsprechend verwaltet, ist es nicht möglich, das iPhone über den Apple Configurator oder iTunes zu aktivieren.

Hinweis 2: Mit iOS 9 ist das iPhone erst betriebsbereit, wenn alle Konfigurationen auf das Gerät aufgespielt wurden. Zwischenzeitlich verweilt das iPhone im Setup Assistenten.

5.28 S/MIME

iOS verfügt über eine integrierte Unterstützung von S/MIME in iOS auf Basis von Zertifikaten. Unter iOS 7 werden sämtliche Mails des Postfaches verschlüsselt, sobald S/MIME aktiviert wurde. Ab iOS 8 hat der Nutzer die Möglichkeit bei jeder einzelnen Mail zu entscheiden, ob diese verschlüsselt werden soll oder nicht.

5.29 Touch ID

Alle aktuellen iOS Geräte verfügen über eine „Touch ID". Diese ermöglicht es dem Nutzer anstatt des Passwortes seinen Fingerabdruck für das Entsperren des Gerätes, Einkäufe in den Apple Stores oder, insofern vom App Entwickler integriert, die Öffnung von Apps, zu verwenden. Hierbei wird nicht der Fingerabdruck des Nutzers als Passwort verwendet. Der Nutzer muss ein Passwort hinterlegt haben um „Touch ID" aktivieren zu können.

Zur Erhöhung der Sicherheit wird vom iPhone dennoch das Passwort verlangt, wenn das iPhone neu eingeschaltet, das Gerät seit mehr als 48 Stunden nicht mehr verwendet, per Fernzugriff gesperrt, fünfmal kein autorisierter Fingerabdruck erkannt wurde, oder aber ein neuer Fingerabdruck hinterlegt werden soll. Insgesamt können bis zu 5 Fingerabdrücke hinterlegt werden.

20 https://www.apple.com/de/business/programs/
21 http://deploy.apple.com/
22 https://www.apple.com/de/business/docs/VPP_Business_Guide_DE_Aug14.pdf

Biometrische Sensoren können grundsätzlich getäuscht werden, wie dies bei „Touch ID“ schon der Fall war. Der Aufwand einer qualifizierten Täuschung ist dennoch sehr hoch und ein entsprechend hochwertiger Fingerabdruck muss vorhanden sein. Dennoch bietet die Verwendung von „Touch ID“ eine höhere Akzeptanz komplexere Passwörter oder überhaupt einen PIN-Code zu verwenden. Außerdem kann durch Verwendung von „Touch-ID“ in öffentlichen Bereichen kein PIN-Code mitgelesen werden.

Grundsätzlich sollte von einem Unternehmen geprüft werden, ob das Restrisiko bei Verwendung von solchem Mechanismen getragen werden kann. Die Verwendung von „Touch ID“ kann unterbunden werden.

5.30 Siri

Apples Sprachassistent Siri ist zentraler Bestandteil von iOS. Bereits bei der initialen Konfiguration wird der Nutzer gefragt, ob diese Funktion aktiviert werden soll. Mittels langem Drücken des Home Buttons kann Siri aufgerufen werden, um beispielsweise Textnachrichten zu erstellen oder aktuelle Termine abzufragen. Siri erhält dabei weitreichenden Zugriff auf zentrale Daten, wie Mail, Nachrichten, Kontakte, Kalender und weitere. Siri ist zudem in der Standardkonfiguration im Sperrbildschirm verfügbar.

Zur Erkennung der Sprache werden Teile der Kommandos an Apple-Server zur Analyse geschickt, um diese auf dem iPhone ausführen zu können. Hierbei werden laut Apple jedoch keine Nutzerdaten vom iPhone selbst übertragen.

In der aktuellen iPhone Generation iPhone 6s und iPhone 6s plus kann Siri auch mittels des Kommandos „Hey Siri“ ohne Betätigung des Home-Buttons aktiviert werden. Das iPhone reagiert auf das Kommando und aktiviert Siri zur Kommandoeingabe. Diese Komfortfunktion kann aus Sicherheitssicht kritisch sein. Bei älteren iPhone Modellen ist ein analoges Verhalten möglich, wenn das iPhone am Strom angeschlossen wird. In beiden Fällen muss die Funktion explizit aktiviert werden.

Trotz der Annehmlichkeiten, die Siri mitbringt, empfiehlt das BSI für die berufliche Verwendung von iPhones auf Siri zu verzichten oder zumindest Siri für den Sperrbildschirm und die Funktion „Hey Siri“ zu deaktivieren. Die Einstellungen zu Siri finden sich unter *Einstellungen - Allgemein - Siri*.

5.31 TLS 1.2

iOS 9 setzt durchgehend auf die empfohlene Version von TLS 1.2 zur Datenverschlüsselung. Zur Erhöhung der Datensicherheit fordert Apple ab iOS 9 TLS 1.2 als Mindeststandard. Das kann zur Folge haben, dass Safari oder App Store Apps in Verbindung mit einer älteren Version von TLS einen Dienst nicht mehr erwartungsgemäß aufrufen.

Entwickler, die in den Apps weiterhin TLS 1.1 verwenden wollen, können dazu Ausnahmen definieren.

5.32 Suche / Spotlight-Suche

Apple bietet unter iOS verschiedene Möglichkeiten an, Inhalte zu suchen. Dabei handelt es sich um die sogenannte Schnellsuche (Spotlight), Vorschläge von Siri und Siri selbst. (Unabhängig davon kann mit Safari über eine klassische Suchmaschine gesucht werden.)

Das generelle Suchverhalten von Spotlight kann unter *Einstellungen - Allgemein - Spotlight-Suche* beeinflusst werden. Hier können Sie die Vorschläge von Siri deaktivieren sowie auswählen, welche Apps in die Suchen einbezogen werden sollen. Die Verwendung von Spotlight sollte

auf eine lokale Suche beschränkt sein. Schalten Sie dazu in *Einstellungen - Allgemein - Spotlight-Suche* Bing-Suchergebnisse sowie Spotlight-Vorschläge ab.

Zudem können Suchanfragen über Spotlight und Safari auch ortsbezogene Ergebnisse liefern. Um dies zu verhindern, müssen Safari- & Spotlight-Vorschläge unter *Einstellungen - Datenschutz - Ortungsdienste - Systemdienste* deaktiviert werden.

Weitere Informationen dazu finden Sie im Apple-Supportartikel[23].

6 Apps

Parallel zu den allgemeinen Einstellungen des Betriebssystems müssen natürlich auch die Apps in sicherheitstechnischer Hinsicht betrachtet werden. Primär geht es dabei um die "nativen" Apps, die in die iOS-Versionen integriert sind.

6.1 Mail

iOS bietet Assistenten für die Einrichtung von E-Mail-Konten für Postfächer in der iCloud, in Microsoft Exchange, Gmail, Yahoo, AOL und Outlook an. Darin sind verschiedene Felder, beispielsweise die Servernamen, bereits vorbelegt. Daneben gibt es einen allgemeinen Einrichtungs-Assistenten für andere E-Mail-Serverdienste.

Die Einrichtungs-Assistenten für die vordefinierten Serverdienste richten automatisch verschlüsselte Übertragungsprotokolle ein. Achten Sie bei dem Assistenten für sonstige E-Mail-Server selbst auf die Verwendung der verschlüsselten Protokolle (POP3S, IMAPS, SMTPS).

Über Profile kann eingeschränkt werden, dass Mails von Unternehmensaccounts nicht über einen anderen Account weitergeleitet werden können, um die Datenabwanderung zu unterbinden.

6.2 Internet-Browser

Der Internet-Browser ist sicherlich auch bei mobilen Endgeräten eine der am meisten verwendeten Apps. Verwenden Sie einen sicheren Internet-Browser, der innerhalb der Browser-Tabs nach dem Sandbox-Prinzip arbeitet. Dazu können Sie den in iOS integrierten Browser "Mobile Safari" verwenden. Achten Sie bei der Verwendung von sonstigen Browsern auch auf das Sandbox-Verfahren.

Der Browser verfügt über einen "Privatmodus", in dem die aufgerufenen Webseiten nicht zum "Verlauf" (Historie) hinzugefügt werden. Cookies, Lesezeichen sowie Leselisten werden nicht gespeichert, usw. Beim Chrome Browser heißt dieser Modus "Incognito-Tab", bei Mobile Safari "Privates Surfen".

Verwenden Sie diese Modi, wenn Sie keine Spuren ihres Surf-Verhaltens hinterlassen wollen und Ihre Eingaben und Downloads nicht temporär gespeichert werden sollen.

Internet-Browser auf mobilen Endgeräten haben im Vergleich zu Browsern auf Desktop Computern keinen effektiven Schutz vor Phishing-Seiten. Dies liegt hauptsächlich an dem großen Update-Bedarf der Phishing-Seiten-Datenbank. Eine Schutzmöglichkeit besteht darin, einen zentralen Proxy-Server einzurichten, über den der Internetverkehr geleitet wird. Auf dem Proxy wird dann ein Phishing-Filter eingerichtet.

Dennoch hat der Browser von iOS einen einfachen Phishing-Filter, der eingeschaltet werden sollte (Einstellungen - Safari - Betrugswarnungen).

23 https://support.apple.com/de-de/HT201285

6.3 3rd-Party-Apps / Drittanbieter-Apps

Apps von Drittanbietern werden bei Apple ausschließlich über den „App Store" vertrieben. Einzige Ausnahme sind die eigen-entwickelten sogenannten Enterprise-Apps, die auch über einen „Enterprise App Store" (in Verbindung mit einer MDM-Lösung) verteilt werden können.

Wählen Sie 3rd-Party-Apps für berufliche Belange mit Bedacht aus. Wenn mit diesen Apps dienstliche Daten verarbeitet werden sollen, sollten die Kommunikationskanäle verschlüsselt sein. Außerdem dürfen die verarbeiteten Daten nur auf dem Firmenserver, oder direkt in der App, also durch die Sandbox geschützt, gespeichert werden. Achten Sie daher darauf, dass keine Daten in der Cloud (iCloud oder auch andere Clouddienste) gespeichert werden.

6.4 Enterprise-Apps

Nicht alle Anforderungen einer Organisation können durch „App Store"- Apps abgedeckt werden. Dabei kann es sich um spezielle Prozesse oder sensible Daten handeln. Zu diesem Zweck bietet Apple das sogenannte „iOS Developer Enterprise Programm", kurz iDEP an. Hiermit kann eine Organisation Apps entwickeln und mit einem iDEP Zertifikat signieren, um diese unter iOS ausführbar zu machen. Die Apps können den betrieblichen Bedingungen entsprechend entwickelt werden und werden unabhängig vom „App Store" bereitgestellt. Dies kann entweder durch ein MDM oder aber über eine Portalseite geschehen. Die Bereitstellung der Enterprise- oder auch In-house- Apps darf nur an Organisationsmitglieder erfolgen. Beachten Sie daher die aktuell gültigen Lizenzbedingungen zum Programm.

Insofern ein Nutzer die entsprechenden Zertifikate noch nicht auf seinem iPhone hinterlegt hat, muss er das Zertifikat zunächst als vertrauenswürdig akzeptieren. Erst dann ist die App lauffähig. Der Nutzer erhält bei erstmaligem Start der App einen Warndialog, den er bestätigen kann. Alternativ kann dies unter *Einstellungen - Allgemein - Profile* vorgenommen werden. Wurde ein Zertifikat als vertrauenswürdig akzeptiert, sind alle weiteren Apps, welche mit demselben Zertifikat signiert wurden, automatisch lauffähig.

Da eine „Enterprise App" ohne den „App Store" auf jedem iPhone installiert werden kann, können manipulierte - mit einem iDEP Zertifikat signierte - Apps auch über unsichere Quellen verteilt werden. Mit iOS 9 kann die Installation von organisationsfremden „Enterprise Apps" auf Basis ihrer Zertifikate verhindert werden. Deaktivieren Sie hierzu die Einschränkung *Einstufen neuer Entwickler firmenweiter Apps als vertrauenswürdig erlauben*. Anschließend hat der Nutzer nicht mehr die Möglichkeit, die Zertifikate fremder Enterprise-Entwickler zu akzeptieren und nur die hausinternen Apps sind lauffähig.

7 iOS Einstellungen / Settings

In den vorangegangenen Kapiteln wurden bereits mehrfach Konfigurations-Menüs von iOS genannt. Diese befinden sich alle in der "Einstellungen"-App. Bis auf einige Ausnahmen besteht die Möglichkeit, die Konfigurationen lokal in der "Einstellungen"-App zu machen, den bereits beschriebenen „Apple Configurator" zu verwenden sowie eine „Mobile Device Management"-Lösungen ein zusetzen.

Viele Einstellmöglichkeiten sind in der "Einstellungen-App" einfach zu finden und selbsterklärend, wie beispielsweise das Menü Einstellungen - WLAN. Andere Menüs sind mitunter komplexer und liegen teilweise in Untermenüs versteckt. An dieser Stelle sollen die zentralen Menüs Einstellungen - *Datenschutz* und Einstellungen - *Allgemein - Einschränkungen* sowie die Einstellungen zur Mitteilungszentrale beschrieben werden.

7.1 Datenschutz

Über das Menü *Einstellungen - Datenschutz* können Sie steuern, welche Apps auf Ihre persönlichen Daten (Kontakte, Kalender, Fotos, usw.) zugreifen dürfen. Sie sind in verschiedene Kategorien unterteilt. Beispiel: Ortungsdienste. In diesem Menüpunkt werden alle installierten Apps aufgelistet, die auf die Ortungsdienste (GPS und Netzwerkstandort) zugreifen wollen. Sie können für jede App entscheiden, ob sie dieses Recht bekommen soll oder nicht.

In der Vergangenheit kam es immer wieder vor, das Apps den Zugriff auf persönliche Daten missbraucht haben, um beispielsweise an Kontaktdaten zu gelangen. Gehen Sie nach dem Minimalprinzip vor und stellen Sie sich bei jeder Kategorie kritisch die Frage, ob die angezeigten Apps tatsächlich das entsprechende Recht zum Zugriff auf diese persönlichen Daten bekommen sollen. Im Zweifel sollten Sie das Recht verweigern. Apps für iOS müssen so programmiert sein, dass sie bei einem verweigerten Recht im Funktionsumfang zwar eingeschränkt sind, aber weiterhin funktionieren, also nicht abstürzen.

Zugriffsberechtigungen zu den personenbezogenen Daten werden bei der Installation von neuen Apps abgefragt. Kontrollieren Sie nach der Installation neuer Apps, ob Ihre Entscheidung zum Zugriff richtig konfiguriert wurde.

7.2 Einschränkungen

Das Menü E*instellungen - Allgemein - Einschränkungen* wird durch einen vierstelligen nummerischen PIN-Code geschützt. Administratoren sollten hier einen PIN-Code verwenden, der nicht oder nur bei Bedarf an den Benutzer weitergegeben wird. Alternativ lässt sich ab iOS 8 die manuelle Konfiguration der Einschränkungen auf „Supervised Devices“ pro Profile deaktivieren.

Im Bereich *Erlauben* können bestimmte - von Apple vorgegebene - Apps beziehungsweise Dienste erlaubt oder verboten werden; voreingestellt ist alles erlaubt. Legen Sie hier insbesondere fest, ob der Benutzer den App Store benutzen, Apps löschen, aber auch, ob er den iCloud-basierten Spracherkennungsdienst "Siri" verwenden darf.

Im Bereich *Zulässiger Inhalt* werden zunächst die Altersbeschränkungen für Medieninhalte und Apps konfiguriert. Hier wird aber auch festgelegt, ob der Benutzer sogenannte In-App-Käufe tätigen darf. Apps von Drittanbietern werden häufig in einer Basisversion kostenlos angeboten, interessante Funktionen soll der Benutzer dann zusätzlich erwerben. Bei Geräten, die ein Administrator vorkonfiguriert, wird diese Funktion nicht benötigt und sollte deaktiviert werden.

In dem Menü findet sich auch das Menü Datenschutz (s.o.) wieder, so dass die dort gemachten Einstellungen gesperrt werden können. Das bedeutet, dass der Benutzer die gewählten Einstellungen nicht verändern kann und neue Apps die gesperrten Funktionen nicht nutzen können. Bei der Installation wird dann eine Warnmeldung ausgegeben. Dies führt allerdings häufig zu Unverständnis bei den Benutzern und Nachfragen beim Support, insbesondere dann, wenn Sie dem Benutzer den „App Store” erlauben - Apps aufgrund der hier gemachten Einschränkungen aber nicht vollständig funktionieren. Legen Sie in den eingangs genannten Security Policies fest, welche Funktionalitäten gesperrt werden und kommunizieren Sie diese deutlich an die Benutzer.

Hinweis: Bei den unterschiedlichen iOS-Versionen sind die Inhalte in dem Menü Allgemein - Einschränkungen durchaus unterschiedlich. Bei neueren Versionen kommen neue Einträge hinzu, teilweise sind die Einträge aber auch umsortiert. Außerdem können Einträge in Menüs unveränderlich ausgegraut sein, wenn eine MDM-Lösung eingesetzt wird.

7.3 Mitteilungszentrale / In der Zentrale / Notification Center

Ein weiterer Menüpunkt in der "Einstellungen"-App ist Mitteilungen ("In der Zentrale", "Notification Center"). Mitteilungen werden in der Mitteilungszentrale - den Touch-Screen von oben nach unten streichen - angezeigt. Sie können aber auch im Sperrbildschirm dargestellt werden. In dem Menüpunkt können Sie konfigurieren, welche Apps Mitteilungen anzeigen. In den Untermenüs der einzelnen Apps legen Sie dann fest, ob Mitteilungen im Sperrbildschirm angezeigt werden sollen. Schalten Sie diese Funktion für solche Apps ab, die berufliche Daten mitteilen könnten.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an info@cyber-allianz.de gesendet werden.