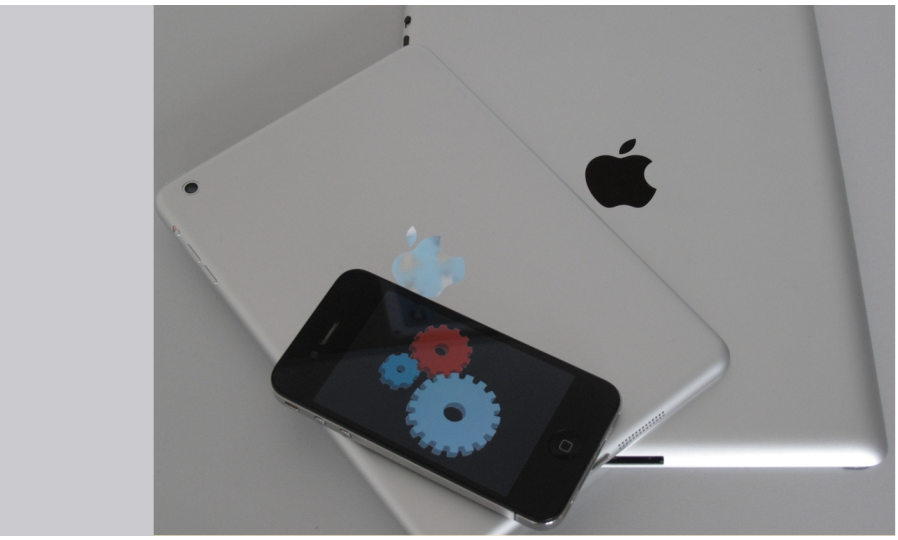
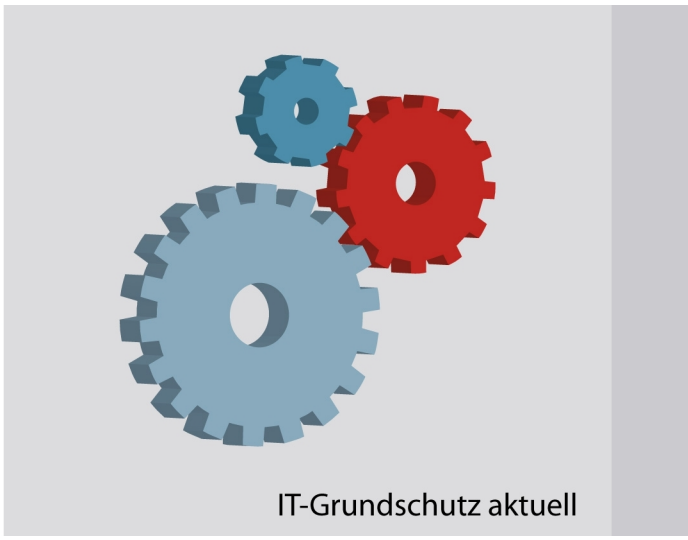
Bundesamt
für Sicherheit in der
Informationstechnik

Überblickspapier Apple iOS





Was ist Apple iOS?

iOS ist ein Betriebssystem des amerikanischen Herstellers Apple für verschiedene Produkte, darunter das iPhone, iPad, iPod touch und einige Versionen von Apple TV.

Die Software hieß zunächst "iPhone OS" und wurde 2010 in "iOS" umbenannt. Basis des Betriebssystems ist ein, an ARM-Prozessoren angepasstes, OS X, das wiederum auf Unix basiert. Die erste Version von iOS wurde im Januar 2007 zusammen mit dem iPhone vorgestellt. Zusätzlich zum Betriebssystem enthält iOS verschiedene Anwendungen wie den Internet-Browser Safari und das E-Mail-Programm Apple Mail. Zahlreiche weitere Programme, kurz "Apps" genannt, können über den Apple App Store installiert werden.

Unter den iOS-basierten Geräten, den so genannten "iDevices", nimmt Apple TV eine Sonderstellung ein, da es kein mobiles Gerät ist und nicht über einen Touchscreen, sondern eine Fernbedienung gesteuert wird. Trotzdem finden sich Apple TV Geräte in einigen Institutionen, zum Beispiel in Konferenzräumen. Einige der nachfolgend angesprochenen Gefährdungen und Maßnahmen zur Abhilfe treffen auch auf Apple TV-Geräte zu. In erster Linie beschreibt das folgende Überblickspapier aber die mobilen iDevices.

Überblickspapier Apple iOS

Welche Sicherheitsstrategie verfolgt Apple?

Apple setzt, verglichen mit anderen Herstellern, auf eine restriktive Politik, was die Erweiterbarkeit der Hardware und die Verfügbarkeit von Software angeht. So dürfen Apps erst über den App Store vertrieben werden, nachdem sie verschiedene Tests durch Apple bestanden haben. Dieses Konzept führte bislang dazu, dass es, verglichen mit anderen Plattformen, nur wenig Schadsoftware und kaum erfolgreiche Attacken auf iOS-Geräte gibt. Trotzdem sind auch iDevices Angriffen ausgesetzt und müssen dementsprechend geschützt werden, durch korrektes Verhalten und durch technische Abwehrmaßnahmen.

Apple nutzt in iOS ein mehrstufiges Sicherheitskonzept. Es versucht schon während der Initialisierung der Hardware zu verhindern, dass Schadsoftware in das System eingeschleust wird. So sind an jedem Schritt des Start-up Prozesses kryptografisch signierte Komponenten beteiligt, darunter der Bootloader, Kernel und die Kernelerweiterungen. Passen die Signaturen nicht zu den hinterlegten Werten, stoppt der Startprozess und das iDevice muss entweder über die Verwaltungssoftware iTunes oder den Device Firmware Upgrade-Mode in den Ursprungszustand versetzt werden.

Updates beheben unter anderem Sicherheitslücken in älteren Softwareversionen. Damit Angreifer kein iDevice auf einen älteren Versionsstand zurücksetzen können, um eine solche Lücke auszunutzen, verwendet Apple System Software Personalization. Während eines Upgrades findet ein kontinuierlicher Informationsaustausch zwischen dem Endgerät und Apples Installation Authorization Servern statt. Jeder Teil des Installationspakets wird mit einem Anti-Replay-Wert und der eindeutigen Kennung des iDevice (ECID) gekennzeichnet. So kann keine ältere iOS-Version eines anderen Gerätes auf das Zielobjekt aufgespielt werden, um deren Schwachstellen auszunutzen.

Sobald der Kernel gestartet wurde, kontrolliert er, welche Benutzerprozesse und Apps ausgeführt werden dürfen. Um sicherzustellen, dass alle Apps von einer bekannten und sicheren Quelle stammen und nicht manipuliert wurden, verlangt iOS, dass jede ausführbare Software mit einem durch Apple ausgestellten, gültigen Zertifikat signiert ist. Das gilt für Software, die mit dem Endgerät ausgeliefert wird genauso, wie für Apps von Drittanbietern. Institutionen, die Anwendungen selbst entwickeln und verteilen wollen, müssen sich im Apple iOS Developer Enterprise Programm (iDEP) anmelden. Nach der erfolgreichen Aufnahme im Programm erhalten die Institutionen ein Verteilungsprofil, mit dem sie interne Apps signieren und auf ihren Endgeräten installieren können.

Sicherheitsvorkehrungen müssen so transparent wie möglich sein, um die Produktivität der Anwender nicht unnötig einzuschränken. Viele Sicherheitsfunktionen von iOS sind von Apple in der Standardeinstellung bereits aktiviert und müssen von den Administratoren nicht mehr konfiguriert werden, bevor die Geräte an die Benutzer verteilt werden. Andere Sicherheitsmaßnahmen, wie die Geräteverschlüsselung, lassen sich nicht abschalten, weder durch den Anwender noch durch den Administrator.

Welchen Fokus hat das Überblickspapier?

Zahlreiche der Gefährdungen und Maßnahmen, die iPhones und iPads betreffen, sind allgemeiner Natur und werden bereits im vorhandenen Überblickspapier "Smartphones" des Bundesamt für Sicherheit in der Informationstechnik (BSI) umfassend behandelt. So sollte es selbstverständlich sein, wo immer möglich Daten in Transit und Storage zu verschlüsseln und nur die Rechte zu vergeben, die unbedingt notwendig sind, um Aufgaben zu erfüllen. Auch sollten so wenige Apps wie möglich genutzt werden, damit das Risiko von Schwachstellen gering bleibt. In diesem Überblickspapier "Apple iOS" werden generische Gefährdungen und Maßnahmen nur bei wesentlichen Abweichungen von iOS angesprochen. Bei einigen Angriffsvektoren spielt die verwendete iOS-Version eine große Rolle. So verbleiben in den Modellen iPhone 3G und älter, die nur bis zu iOS 4.2 aktualisiert werden können, einige Schwachstellen, die in aktuellen Modellen mit einer neueren iOS-Version behoben sind.

Die aufgezählten Gefährdungen gelten für alle Einsatzfälle, allerdings muss eine Institution die Risiken abwägen und als Resultat die zutreffenden Maßnahmen treffen. Bei Anwendern mit höheren Sicherheitsanforderungen, zum Beispiel bei Wirtschaftsvorständen, sollten weitergehende Maßnahmen getroffen und umgesetzt werden, auch wenn diese unter Umständen Nutzerfreundlichkeit und Produktivität in Mitleidenschaft ziehen können.

Gefährdungsübersicht

Ein iOS-Gerät ist wie jedes mobile Endgerät zahlreichen potenziellen Gefährdungen ausgesetzt. Zum Teil unterscheiden sich die Gefährdungen nicht von denen, die auch auf IT-Systeme wie einen PC wirken. So können wichtige Informationen verloren gehen, wenn eine aktuelle und vollständige Datensicherung fehlt. Andere Gefährdungen sind typisch für ein mobiles Endgerät, beispielsweise der Verlust durch Diebstahl. Generische Gefährdungen, die auf jedes Smartphone oder Tablet wirken, sind bereits umfassend im Überblickspapier "Smartphones" des BSI beschrieben. Wichtige spezifische Angriffsvektoren für iOS werden nachfolgend erläutert.

Jailbreak

Bei einem Jailbreak werden Nutzungsbeschränkungen von iOS-Geräten, die Apple bewusst vorgenommen hat, rückgängig gemacht. Dafür werden spezielle Programme oder Web-Dienste verwendet, die Schwachstellen in iOS ausnutzen. Alle "iDevices" lassen sich theoretisch jailbreaken, einschließlich Apple TV und iPod touch, auch wenn Jailbreaks manchmal nur temporär oder mit großen Verzögerungen verfügbar sind und immer schwerer durchgeführt werden können. Im Jahr 2010 waren schätzungsweise 10 % aller iOS-Geräte jailbroken. Laut den Nutzungsbedingungen von Apple erlischt durch den Jailbreak die Herstellergarantie. Darüber hinaus entstehen zahlreiche Angriffspunkte, weil viele Sicherheitsmechanismen von Apple ausgeschaltet werden und Anwendungen und Anwender vollen Zugriff auf das Betriebssystem erhalten. Auch Live-Images vom Speicherinhalt des iOS-Geräts lassen sich sehr leicht vom ungeschützten iOS-Gerät erstellen. Besonders bedenklich ist, dass nach dem Jailbreak Apps aus ungeprüften Quellen installiert werden können, die möglicherweise Schadsoftware enthalten. Viele Benutzer versäumen es auch, ein neues Root-Passwort zu vergeben, es wird durch den Jailbreak auf einen allgemein bekannten Standardwert gesetzt. Wenn der Jailbreak den sogenannten SIM-Lock aufheben soll, beeinträchtigt das die GPS-Funktion einiger Geräte. Das kann nachträglich bei verschiedenen iPhone 3GS-Modellen nicht mehr rückgängig gemacht werden.

Schwachstellen in iOS

Sowohl in iOS als auch in Apps werden immer wieder Schwachstellen entdeckt, die verschiedene Sicherheitsprobleme nach sich ziehen können. Schwachstellen, mit denen sich der Passcode umgehen lässt, gibt es beispielsweise in den iOS-Versionen vor 4.1 und in 5.0.1. Der bekannte Fehler des Smart Cover–Unlock, bei dem die Abdeckung des iPad (Smart Cover) zusammen mit einer bestimmten Vorgehensweise den Passcode aufhebt, tritt hingegen nur in v5.0 auf und ist in Version 5.0.1 abgestellt. Mit iOS 6 hat Apple insgesamt 197 Sicherheitslücken gegenüber der Vorgängerversion behoben.

Sicherheitslücken durch Dienste und Apps

Geräte mit iOS-Betriebssystem können zahlreiche Anwendungen ausführen, sie sind mit Diensten und Funktionen ausgestattet, die für den dedizierten Firmeneinsatz oft nicht notwendig sind. Ein Beispiel sind Geolocation-Dienste, bei denen der Standort des Benutzers erfasst und mit einem Dienst verknüpft wird. Mit solchen Diensten lassen sich unter Umständen Zugangsbeschränkungen umgehen oder persönliche Informationen abgreifen. Ein Beispiel ist der Beschleunigungssensor, dessen Daten missbraucht werden können, um Eingaben über den Touchscreen auszuspähen.

Ungewollter Datenabfluss durch Apps und iOS

Wenn der Benutzer bei der Installation des iOS 6 nicht widerspricht, sendet das iPhone im Hintergrund Diagnosedaten, wie beispielsweise Log-Dateien oder Details von App-Abstürzen und Ähnliches an Apple. Diese Daten könnten persönliche oder vertrauliche Informationen enthalten. Zudem können legitim installierte Apps solche Daten ohne Wissen des Anwenders an Dritte weitergeben.

Ungewollte Datenablage

Wenn iOS-Geräte mit iTunes synchronisiert werden, legen sie automatisch eine Datensicherung von verschiedenen Informationen auf dem iTunes-Host an (im Verzeichnis /Users/<your user name>/Library/Application Support/MobileSync/Backup/). Weil diese Datensicherungen in der Standardeinstellung nicht verschlüsselt sind, besteht die Gefahr, dass persönliche Daten auf dem Host eingesehen werden können. Ein Beispiel dafür sind bekannte Fehler in Apps, bei dem Daten, die auf dem iOS-Gerät geschützt gespeichert waren, unverschlüsselt auf dem Host gesichert wurden

Sicherheitslücken durch Siri

Die Sprachsteuerung Siri kann auch bei gesperrtem Gerät verschiedene Aktionen auslösen. So lassen sich durch Unbefugte SMS-Nachrichten verschicken, einige Kontaktdaten anzeigen oder Rückrufe vornehmen.

Kein oder zu schwacher Passcode

Das Passwort oder Passcode ist entscheidend für die Sicherheit eines mobilen Endgeräts verantwortlich und wird hier explizit erwähnt, obwohl es zu den grundlegenden Sicherheitsmaßnahmen gehört. Ein zu schwaches oder kein Passwort erleichtert Angreifern den Zugang zum Endgerät und den Zugriff auf die darauf gespeicherten Informationen.

Apps verstoßen gegen Sicherheitsvorgaben

Smartphones und Tablets sind auch deshalb so beliebt und universell einsetzbar, weil eine große Zahl von Apps dafür existieren. Diese Apps können aber zu Sicherheitsproblemen führen, beispielsweise, wenn die Software Schwachstellen enthält. Öffentlich zugängliche Datenbanken listen zahlreiche Schwachstellen und bereits existierende Programme auf, die diese Schwachstellen ausnutzen. Darüber hinaus sind weitere Aspekte bei Apps problematisch. Einige Apps verhalten sich selbst ohne bekannte Schwachstellen so, dass sie gegen die Sicherheitsvorgaben von Institutionen verstoßen könnten.

- Einige Apps nutzen beispielsweise ein automatisches Login, was die Gefahr von Datenverlust erhöht.
- Andere Apps öffnen verdeckt Netz-Ports, sodass das Endgerät anfällig für Netzattacken wird.
- Viele Apps legen Log- und Hilfs-Dateien an, aus denen sich relevante Informationen extrahieren lassen. Ein Beispiel ist der Keyboard-Cache. Für Textfelder, in die Passwörter eingegeben werden, ist er abgeschaltet, nicht jedoch bei Kontonummern, Steuernummern, etc.
- Apps, die Online-Speicher (Cloud-Storage) nutzen, können die Datenschutz- und Vertraulichkeitsbestimmungen der Institution verletzen.
- Trotz der Kontrollen durch Apple ist nicht auszuschließen, dass sich Schadcode in offiziell über den Apple AppStore verteilte Anwendungen einschleicht.

Fehlende Schutzsoftware

Zurzeit bieten noch sehr wenige Hersteller Schutzsoftware gegen Viren, Trojaner und andere Schadsoftware für iOS-Geräte an. Bislang haben sich diese Programme auch kaum bei den Benutzern von iOS-Geräten durchgesetzt. Dadurch besteht das Risiko einer Infektion, auch wenn es bislang nur wenig Schadsoftware für iOS gibt.

Umgehen von Sandboxing

Apps werden bei iOS-Geräten in einer geschützten Umgebung ausgeführt, die den direkten Zugriff auf iOS nicht erlaubt (Sandboxing). Dieser Schutz wirkt jedoch nicht oder nur eingeschränkt, wenn ein kompromittiertes Betriebssystem anderen Apps den Zugriff erlaubt oder selbst unerlaubt auf Daten zugreift.

Mobile Device Management

Es gibt zahlreiche Anwendungen, mit denen mobile iOS-Geräte verwaltet werden können. Diese Mobile Device Management-Lösungen (MDM) werden unter anderem dafür genutzt, Konfigurationsprofile und Richtlinien auf die Endgeräte auszubringen, zu verwalten und wieder zu entfernen. Im Zusammenhang mit Mobile Device Management können verschiedene Gefährdungen entstehen.

- Apple ändert die verfügbaren Richtlinien und deren Funktionsumfang bei Upgrades. Nicht jedes MDM-Programm unterstützt alle möglichen Apple iOS-Richtlinien oder deren aktuellste Version.
- Manuell über iPCU (iPhone Configuration Utility) hinzugefügte Richtlinien können von MDM-Software nicht entfernt werden.
- Benutzer können Richtlinien mit Sicherheitseinstellungen manuell löschen, wenn sich das iDevice nicht im Supervised-Modus befindet.
- Werden die Richtlinien über ungesicherte Wege wie E-Mail oder SMS-Link verteilt, sind vertrauliche User-Informationen in den Richtlinien während der Übertragung ungeschützt.

iMessage-Bug

Bei iOS-Versionen vor iOS 6 ist es möglich, dass nach dem Verlust oder Diebstahl eines iPhones weiterhin Nachrichten von dem Gerät gesendet und empfangen werden, obwohl die Passwörter geändert, die SIM-Karte deaktiviert und das iPhone zurückgesetzt wurde (iMessage-Bug).

Ungewollte Vertrauensstellung zu iTunes

Ein entsperrtes iOS-Gerät kann sich mit jedem Host-Computer verbinden, auf dem iTunes läuft. Dabei wird eine Vertrauensstellung zwischen Host und iOS-Gerät etabliert, über die ungewollt persönliche Daten auf den Host übertragen werden könnten. Ein Beispiel dafür wäre, wenn der Benutzer sein iOS-Gerät mit einem Host verbindet, um lediglich dessen USB-Port zum Laden zu nutzen.

Vertraulichkeitsverlust durch Mail

Bei einer unzureichend konfigurierten Mail-Anwendung könnten sich Anhänge aus verschlüsselten E-Mails in andere Anwendungen verschieben lassen, wenn die Anwendungen mit dem passenden Dateityp registriert wurden. Dadurch kann es zum Vertraulichkeitsverlust dieser Inhalte kommen.

Missbrauch von QR-Codes

Für iOS- und andere mobile Endgeräte sind zahlreiche Apps erhältlich, mit denen QR-Codes (Quick Response Codes) gescannt und verarbeitet werden können. Meist sind in den QR-Codes Links zu Webseiten hinterlegt. Vereinzelt haben Angreifer die QR-Codes bereits genutzt, um Benutzer auf Webseiten mit Phishing-Absichten oder mit Schadsoftware umzuleiten.

Sicherheitsgateway blockiert APNS

Viele Anwendungen und Dienste von iOS nutzen den Apple Push Notification Service (APNS). Über APNS können Anwendungen Benachrichtigungen erhalten, zum Beispiel die Aufforderung ein Icon zu verändern oder einen Signalton abzuspielen, etwa wenn eine neue E-Mail eingegangen ist. Auch Mobile Device Management-Server nutzen APNS zur Verwaltung der iOS-Geräte. Wenn ein nicht korrekt konfiguriertes Sicherheitsgateway (Firewall) der Institution APNS blockiert, können Informationen verloren gehen und Anwendungen unter Umständen nur eingeschränkt arbeiten.

Zero-Day-Angriff über Netzverbindung

Geräte mit iOS-Betriebssystem weisen architekturbedingt kein Sicherheitsgateway (Firewall) auf. Nach Einschätzung von Apple ist kein Sicherheitsgateway nötig, weil das Sandboxing der Apps Angriffe über diesen Weg verhindert. Es ist trotzdem denkbar, dass Angreifer versuchen, über eine Netzverbindung Pakete in das Betriebssystem einzuschleusen, die eine bis dato unentdeckte Schwachstelle ausnutzen könnten.

Kein "always-on" für VPN

Das Betriebssystem iOS enthält einen eigenen Client für Virtual Private Networks (VPN). Netzverbindungen sollten immer über das VPN aufgebaut und aufrechterhalten werden, allerdings verfügt iOS nicht über eine "always-on" Einstellung für die VPN-Funktionalität. Anwender könnten versehentlich ungesicherte Netzverbindungen aufbauen und so vertrauliche Informationen im Klartext übertragen.

Vertraulichkeits- und Datenverlust durch iCloud

Seit Mitte 2011 bietet Apple eine Online-Plattform mit dem Namen "iCloud" (früher iTools/.Mac/MobileMe) an. Mit ihr lassen sich zahlreiche Informationen und Inhalte über den Online-Speicher auf bis zu zehn Apple-Geräten und Windows-Rechnern synchronisieren (ab iOS 5 und Mac OS X 10.7 bzw. Windows Vista). Die Daten werden auf den Servern verschlüsselt abgelegt, allerdings hat Apple dazu einen Generalschlüssel und kann auf die Daten zugreifen. Apple kann nach eigenen Aussagen bei "Anfragen von Strafverfolgungsbehörden, anderen Behörden und/oder sonstigen Dritten" von dieser Möglichkeit Gebrauch machen. Dadurch könnte die Vertraulichkeit wichtiger Informationen verloren gehen. Wer unberechtigten Zugriff zu iCloud erhält, kann die dort abgelegten Daten einsehen und löschen, was den Datenverlust auf allen damit verknüpften Endgeräten zur Folge hat.

Datenverlust bei Weitergabe

Wird versäumt die persönlichen Daten des Vorbesitzers eines iOS-Geräts rückstandslos zu löschen, wenn das Gerät weitergegeben, verkauft oder vernichtet wird, können schützenswerte Informationen in falsche Hände geraten. Gleiches gilt für jegliche Art von mobilen Endgeräten, unabhängig vom Hersteller oder Betriebssystem.

Unabsichtlicher Datenverlust

Wenn Benutzer die Möglichkeit haben, das iOS-Gerät auf eigene Initiative hin komplett zu löschen (Wipe/Remote Wipe), kann es, wie bei allen mobilen Endgeräten, zu ungewolltem Datenverlust kommen.

Datensicherung nicht verschlüsselt

Alle iOS-Geräte bieten die Möglichkeit, automatisch Datensicherungen von wichtigen Daten zu erstellen. In der Standardeinstellung werden die Backups durch iTunes nicht verschlüsselt, was einem Angreifer volle Kontrolle über die wichtigsten Informationen des Users gibt, wenn er Zugang zum iTunes-Host gewinnt.

Wie kann diesen Risiken von iOS begegnet werden?

Vollständige IT-Sicherheit kann es nicht geben, weder bei stationären Endgeräten noch bei mobilen iDevices. Wenn alle, auch nur entfernt infrage kommenden Angriffsvektoren, mit entsprechenden Maßnahmen verringert werden, bleibt die Benutzbarkeit auf der Strecke. Schlimmer noch, die Mitarbeiter werden versuchen, die Maßnahmen zu umgehen und wirken damit dem Ziel der IT-Sicherheit entgegen. Diese Gefahr besteht umso mehr bei Endgeräten wie iDevices, die gerade für ihre hohe Bedienerfreundlichkeit bekannt sind. Der Trend hin zu "Bring-your-own-Device" wird nicht zuletzt dadurch verursacht, dass Anwender die Vorteile ihrer Endgeräte aus dem privaten Lebensbereich in der Institution nicht missen möchten. Sicherheitsbeauftragte und IT-Administratoren müssen aus dem Spektrum der möglichen Maßnahmen gegen generische und iOS-spezifische Gefährdungen sorgfältig auswählen und die Balance zwischen Sicherheit und Benutzbarkeit finden. Während schon der gesunde Menschenverstand grundlegende Maßnahmen wie Datensicherung, Verschlüsselung und Datensparsamkeit nahelegt, sind gerade weitergehende technische Restriktionen vor allem vom Risikoprofil der Institution abhängig. Ein Softwarekonzern muss in der Regel anderen Ansprüchen an die Datensicherheit genügen als ein kleiner produzierender Betrieb. Das sollte sich auch in den umgesetzten Maßnahmen widerspiegeln.

Zentraler Einkauf

In einer Institution genutzte iOS-Geräte sollten zentral beschafft und aktiviert werden. Damit kann die Institution generelle Nutzungseinschränkungen wie den Supervised-Modus vorgeben oder Richtlinien für die Datensicherung, App-Installation und die Verbindung mit drahtlosen Netzen festlegen.

Whitelist-Ansatz für Apps

Die Flexibilität von Smartphones und Tablets mit iOS-Betriebssystem basiert unter anderem auf der großen Menge verfügbarer Apps. Trotzdem sollten Institutionen die Zahl der Apps auf den Endgeräten möglichst gering halten, weil Software immer fehlerbehaftet ist und Schwachstellen aufweisen kann. Lässt sich vorgeben, welche Apps die Benutzer installieren dürfen, kommen viele potenzielle Gefährdungen gar nicht erst zum Tragen. Bei einem klar definierten Einsatzgebiet ist es empfehlenswert, nur die von der Institution freigegebenen Apps auf dem iOS-Gerät zu erlauben und zu verhindern, dass zusätzliche Apps installiert werden (Whitelist-Ansatz). Das kann über Richtlinien des Mobile Device Management (MDM) und durch den Supervised-Modus von iOS ab Version 6 geschehen.

Jailbreaks erkennen

Bei einem Jailbreak werden Nutzungsbeschränkungen von iOS-Geräten, die Apple bewusst vorgenommen hat, rückgängig gemacht. Alle "iDevices" lassen sich jailbreaken, einschließlich Apple TV und iPod touch, auch wenn Jailbreaks manchmal nur temporär oder mit großen Verzögerungen verfügbar sind. Ein Grund für Jailbreaks ist es, Apps zu installieren, die nicht über den offiziellen Kanal des Apple App-Store bezogen werden können. Allerdings erleichtert ein Jailbreak Angriffe durch Schadsoftware auf iOS. Unter anderem kann ein derart manipuliertes iOS die korrekte Signatur von Software nicht mehr kontrollieren. Institutionen sollten Jailbreaks verbieten. Technisch lassen sich Jailbreaks durch restriktive Richtlinien und den Supervised-Modus erschweren. Eine eingesetzte Mobile Device Management-Software (MDM) sollte trotzdem durchgeführte Jailbreaks erkennen können. Weil sich die Software, die den Jailbreak durchführt, in der Regel vor der Erkennung tarnt und das Betriebssystem entsprechend verändert, kann der Jailbreak nicht immer eindeutig erkannt werden. Eine relativ sichere Variante um Jailbreaks trotzdem zu entdecken, sind durch die Institution entwickelte Apps, die Veränderungen am Betriebssystem registrieren.

Keine PIN für automatische Aktivierung

Alle iOS-Geräte müssen aktiviert werden, bevor sie sich benutzen lassen. iPhones benötigen eine eingelegte SIM-Karte, um aktiviert zu werden. iPads, die auch über eine Mobilfunkeinheit verfügen können, können auch ohne SIM-Karte genutzt werden, für die Aktivierung wird diese nicht zwingend benötigt.. Damit die Aktivierung automatisch durchgeführt werden kann, zum Beispiel durch Apple Configurator, darf zu diesem Zeitpunkt noch kein PIN-Code auf der SIM vergeben sein.

iTunes lock-down

Ab iOS 5 ist iTunes nicht mehr zwingend für die Verwaltung der iOS-Geräte notwendig. Werden die Funktionen von iTunes nicht unbedingt benötigt, sollte die Software nicht verwendet oder administrativ gesperrt (locked-down) werden. Allerdings kann die eingebaute lokale Datensicherungsfunktion von iTunes im Unternehmenseinsatz sinnvoll sein. Falls iTunes im Unternehmen genutzt werden soll, ist es empfehlenswert, die Freigabe von Musik- und anderen Dateien abzuschalten. Wenn das iOS-Gerät zusätzlich privat genutzt wird, können die Daten online über das Internet oder auf dem privaten IT-System des Benutzers gesichert werden. Allerdings ist vorab zu klären, wie sich Firmendaten auf einem privaten IT-System rechtlich auswirken. Das BSI hat zum Themenbereich Bring-you-own-device (BYOD) ein eigenes Überblickspapier verfasst, dass weitergehende Informationen zu dieser Situation enthält. Wird iTunes zur Datensicherung eingesetzt, sollte unbedingt die Verschlüsselung aktiviert werden, die in der Standardeinstellung abgeschaltet ist. Die Datensicherung über Apples Online-Dienst iCloud erfolgt standardmäßig verschlüsselt, der Dienst ist jedoch in erster Linie für Privatanwender konzipiert. Institutionen sollten die möglichen Implikationen durch den Speicherort außerhalb Deutschlands berücksichtigen und bedenken, dass Apple theoretisch Zugriff auf die Daten hat. Unternehmenswichtige Daten einer Institution sollten nicht mit iCloud gesichert werden.

Aufladen nur per Ladegerät

Um iOS-Geräte aufzuladen, sollten ausschließlich Ladegeräte, Netzteile oder autorisierte IT-Systeme verwendet werden. Durch die Verbindung über das USB-Kabel könnten sonst ungewollt Daten mit iTunes auf dem fremden IT-System synchronisiert werden oder Schadsoftware auf das iOS-Gerät gelangen.

Ungewollten Datentransfer unterbinden

Wenn Benutzer diese Funktion bei der Installation von iOS 6 nicht explizit ablehnen, sendet das iPhone im Hintergrund Diagnosedaten an Apple. Dazu gehören Log-Dateien und Details über abgestürzte Apps. Apple versichert, dass diese Daten anonymisiert übertragen werden. Wenn Institutionen diesen Datentransfer unterbinden wollen, kann dieser im Untermenü "Diagnose & Nutzung" abgeschalten werden.

Falls möglich keine persönlichen E-Mail Accounts

Institutionen sollten keine persönlichen E-Mail Accounts auf betrieblich genutzten iOS-Geräten erlauben, falls das mit der Verteilungsstrategie für Endgeräte (kein BYOD) vereinbar ist.

Ohne Zusatzsoftware nur S/MIME möglich

Wenn E-Mails signiert und verschlüsselt werden müssen, ist zu berücksichtigen, dass iOS ohne zusätzliche Erweiterungen nur S/MIME unterstützt.

Datensparsamkeit bei Apps beachten

Die aktuelle Version 6 von iOS enthält im Bereich "Einstellungen" einen Menüpunkt "Datenschutz". Darin lässt sich festlegen, auf welche Weise Apps auf persönliche Daten wie Geoposition, Kalender, Fotos und Ähnliches zugreifen dürfen. Auch Social Media-Accounts wie Facebook oder Twitter können hier für den Zugriff durch Anwendungen freigegeben oder gesperrt werden. Generell sollten Apps persönliche Daten so sparsam wie möglich nutzen.

Updates zeitnah einspielen

Apple veröffentlicht Updates und Patches für iOS. In den neuen Versionen werden in der Regel viele potenzielle Sicherheitslücken behoben. Weil die Schwachstellen danach allgemein bekannt sind, sollten Anwender oder Institutionen so schnell wie möglich upgraden. In der Regel wirkt sich das nicht negativ auf unterstützte Software von Drittanbietern aus. Fabrikneue Geräte verfügen bei der Auslieferung über die aktuellste iOS-Version, viele ältere Geräte können aktualisiert werden. Die derzeit ausgelieferte Version 6 von iOS ist beispielsweise neben dem iPhone 5 ebenso auf iPhone 3GS, 4, und 4S lauffähig. In Einsatzbereichen mit erhöhten Sicherheitsanforderungen sollten keine iOS-Geräte benutzt werden, die nicht die aktuellste iOS-Version ausführen können.

Zentrales MDM nutzen

Alle Einstellungen sollten, soweit möglich, über ein Mobile Device Management-Programm (MDM) zentral vorgenommen und die Benutzer dahin gehend geschult werden, an den Richtlinien keine Änderungen vorzunehmen. Das lässt sich unter anderem erreichen, indem restriktive Einstellungen in einer Richtlinie mit, für die Arbeit unerlässlichen, Einstellungen, beispielsweise für den E-Mail Account, verbunden werden. Möglich ist auch, eine Einstellung pro Richtlinie zu nutzen und sie mit einem Passwort zu versehen. Sie können dann, mit Ausnahme der Basis-Richtlinie ("Enrollment Profile"), nicht mehr gelöscht werden. Entfernt ein Benutzer die Basis-Richlinie, werden auch alle hierarchisch darunter liegenden Einstellungen gelöscht. Das iDevice ist dann nicht mehr im Netz der Institution funktionsfähig.

Funktionsumfang der MDM-Software

Mobile Device Management-Software zur Verwaltung von iOS-Geräten wird von zahlreichen Herstellern angeboten. Damit lassen sich unterschiedliche iOS-Geräte einstellen und aus der Ferne konfigurieren. Die MDM-Software muss alle konfigurierbaren Richtlinien der Apple iOS-Geräte unterstützen und sollte eine Möglichkeit bieten, Geräte mit Jailbreak im Netz und unautorisierte Software auf den Endgeräten zu erkennen und zu melden.

Supervised-Modus

Alle iOS-Geräte mit iOS 6 beherrschen den Supervised-Modus (vorher nur iPad). Im Supervised-Modus kann die Institution mehr Kontrolle über das Gerät ausüben und zahlreiche sicherheitsrelevante Einstellungen vornehmen. So lässt sich beispielsweise der Zugriff zu Game Center, Bookstore und erotischen Büchern verbieten und ein globaler Proxy einrichten, über den sämtlicher HTTP-Verkehr geleitet wird. Außerdem erlaubt der Supervised-Modus eine Kiosk-Betriebsart (App-Lock), in der das Gerät nach dem Start nur eine definierte Anwendung ausführt, die der Benutzer nicht wechseln kann. Aus Sicherheitssicht ist besonders wichtig, dass Benutzer bei iOS-Geräten im Supervised-Modus MDM-Richtlinien nicht mehr entfernen können. Allerdings erfordert der Supervised-Modus eine Neuinstallation von iOS 6. Wurde bereits mit dem Endgerät gearbeitet, müssen persönliche Daten und Apps vorher gesichert und wiederhergestellt werden, nachdem das Gerät im Supervised-Modus arbeitet.

Alle iOS-Geräte gehen eine Host-Verbindung mit jedem aktiven iTunes ein. Dadurch könnten ungewollt Daten mit iTunes auf einem unautorisierten IT-System ausgetauscht werden. Der "Supervised-Modus" verhindert das, da sich ein iOS-Gerät im "Supervised-Modus" nur noch an den Host koppelt, der den Supervised-Modus initiiert hat.

Guided Access

Guided Access ist ein Bestandteil von iOS 6, mit dem sich Restriktionen in Apps festlegen lassen. Bei einer App im Guided Access-Modus kann der Administrator bestimmte Teile des Bildschirms abdunkeln, den Touchscreen abschalten und den Beschleunigungssensor stilllegen. Benutzer dürfen die aktive App nicht verlassen oder zu einer anderen App wechseln, ohne den Guided Access-Code zu kennen. Wenn iOS-Geräte allgemein zugänglich sind, zum Beispiel als Audio- und Video-Guide in einem Museum, können sie durch Guided-Access in ihrer Funktion stark eingeschränkt und Sicherheitsrisiken minimiert werden.

Copy&Paste abschalten

In Einsatzgebieten mit sehr hohen Sicherheitsanforderungen kann es sinnvoll sein, Kopieren und Einfügen (Copy&Paste) abzuschalten oder zu reglementieren, um zu verhindern, dass Daten aus geschützten in offene Anwendungen wie Web-Mail kopiert werden. Diese Maßnahme lässt sich mit MDM-Programmen umsetzen, Apples iOS selbst bietet diese Möglichkeit nicht.

Thin-Client-Wall

Durch den Einsatz von Thin-Client Technik können Benutzer von iOS-Geräten mit Anwendungen der Institution arbeiten, ohne dass die Daten das Unternehmensnetz verlassen (Thin-Client-Wall). Dadurch kann auch vermieden werden, dass beispielsweise der Exchange-Account des Benutzers über potenziell unsichere WAN-Verbindungen synchronisiert wird.

Kein "Simple Passcode"

Der Passcode schützt iOS-Geräte vor unbefugtem Zugriff und sollte immer aktiviert sein. Bei Geräten mit iOS-Version 4 und höher lässt sich anstelle der einfachen PIN aus vier Zahlen auch ein komplexerer Passcode eingeben. Dazu muss die Einstellung "Einfacher Code" deaktiviert werden. Auch wenn der längere Passcode weniger benutzerfreundlich ist, sollten Institutionen davon Gebrauch machen. Apple bietet bei iOS im Zusammenhang mit dem Passcode einige weitere Schutzmaßnahmen an. Nach einer bestimmten Zahl von Fehleingaben wird das iOS-Gerät temporär gesperrt, um so zu verhindern, dass viele Kombinationen durchprobiert werden. Falls eine höhere Sicherheitsstufe gewünscht wird, lässt sich das iOS-Gerät nach mehr als zehn Fehleingaben löschen.

Schutzsoftware

IT-Systeme von Apple waren bislang sehr selten Ziel von Schadsoftware. Für iOS-Geräte ist ebenfalls kaum Schadsoftware bekannt. Trotzdem kann es sinnvoll sein, Schutzsoftware zu installieren, weil damit auch Spam- und Phishing-Mails abgefangen werden können. Generell sollte auf den beteiligten Servern, wie E-Mail- oder Proxy-Servern, entsprechende Schutzsoftware installiert werden, damit Schadsoftware nicht zum iOS-Gerät übertragen werden kann.

Profiles sicher verteilen

Richtlinien (Profiles) müssen auf einem sicheren Weg an die iOS-Geräte verteilt werden, da sie vertrauliche Benutzerinformationen enthalten können. Das kann manuell mit dem iPhone Configuration Utility (iPCU) oder dem Apple Configurator über eine USB-Verbindung erfolgen oder, wenn vorhanden, mittels einer Certificate Authority mit LDAP-Directory, Simple Certificate Enrollment Protocol (SCEP) und einem Webserver.

APNS-Ports in Sicherheitsgateways

Damit Nachrichten des Apple Push Notification Service (APNS) korrekt von den iOS-Geräten empfangen werden, müssen die Sicherheitsgateways (Firewalls) in der Institution korrekt konfiguriert und verschiedene Ports geöffnet sein (TCP 2195/2196/5223). Es ist zu klären, ob durch APNS ein Sicherheitsrisiko entstehen kann, allerdings erfordern auch Dienste anderer Hersteller wie Microsofts Windows Server Update Services (WSUS) geöffnete Ports.

Apple ID

Die Apple ID ist für den Einkauf von Apps notwendig. Sie dient auch dazu, Benutzer gegenüber verschiedenen Diensten zu identifizieren. Je nach Art der Beschaffung muss die Apple ID unterschiedlich verwaltet werden. Bei einem BYOD-Modell wird dem Benutzer in der Regel Vertrauen entgegengebracht, sodass er seine private Apple ID bei der Institution hinterlegen und für den Betrieb des iOS-Geräts verwenden kann. Werden Apps im Auftrag der Institution gekauft, sollte eine Erstattung der Kosten möglich sein. Dürfen Benutzer keine eigenen

Apps installieren, sollte die Apple ID für jedes Endgerät durch die Institution generiert werden, ohne sie mit einer Zahlungsmethode zu verknüpfen. In diesem Fall kennen die Benutzer die Apple ID nicht. Allerdings muss das Support-Personal die Apps installieren und auf dem neuesten Stand halten, was erheblichen Aufwand nach sich ziehen kann.

Siri konfigurieren

Siri ist eine Spracherkennungssoftware innerhalb von iOS , die verschiedene Aktionen auslösen kann. Konvertiert wird die Spracheingabe nicht auf dem iOS-Gerät selbst, sondern auf weltweit verteilten Servern. Zudem kann Siri auch Aktionen bei gesperrtem iOS-Gerät durchführen, wenn die Benutzer oder die Institution diese Funktion nicht explizit abgeschaltet haben. Je nach Sicherheitsanforderung der Institution sollte überlegt werden, Siri gänzlich abzuschalten oder mit entsprechenden Profilen bei einer aktiven Bildschirmsperre zu deaktivieren.

Automatische SMS-Antwort

In der Version 6 von iOS lässt sich bei abgewiesenen Anrufen eine passende SMS an den Anrufer senden. Es sind verschiedene Mustertexte vordefiniert aber auch eigene Texte möglich. Diese Funktion ist in der Grundeinstellung auch bei gesperrtem Gerät möglich, kann aber mit einem Passwort versehen werden.

Physische Kontrolle über iDevice

Wenn Benutzer die physische Kontrolle über das iDevice abgeben müssen, beispielsweise am Flughafen bei einer Sicherheitsüberprüfung des Endgeräts, müssen die darauf gespeicherten Daten, das Betriebssystem und die Anwendungen vor unberechtigtem Zugriff geschützt werden. Ein iDevice muss dazu auf alle Fälle mit einem ausreichend sicheren Passcode versehen sein und gesperrt werden, bevor es aus der Hand gegeben wird. Falls der Verdacht besteht, dass das iOS-Gerät manipuliert oder unberechtigt benutzt wurde, sollte der Sicherheitsbeauftragte der Institution informiert und die auf dem Gerät abgespeicherten Informationen gelöscht werden.

Vorgehen bei Verlust oder Diebstahl

Institutionen sollten im Vorfeld Prozesse etablieren, wie und unter welchen Voraussetzungen iOS-Geräte gelöscht werden können. Wird ein iOS-Gerät gestohlen oder verloren, muss es aus der Ferne deaktiviert werden, um unbefugten Zugang zu verhindern. Welche Methode dafür genutzt wird, hängt auch davon ab, ob die Institution oder ein Benutzer Eigentümer des Geräts ist. Wenn eine Netzverbindung zum iOS-Gerät besteht, kann der Administrator die Sperrung über Exchange ActiveSync oder MDM-Software aus der Ferne einleiten. Ohne MDM-Software lässt sich ab iOS 5 iCloud für diese Aufgabe nutzen. Ältere iOS-Versionen verwendeten dafür MobileMe. Der Online-Dienst iCloud erfordert die Apple ID des Benutzers zur Authentisierung und kann Nachrichten auf das Gerät schicken, den Standort des iDevice auf einer Karte anzeigen, einen neuen Passcode setzen oder das Gerät komplett löschen.

Sicheres Löschen

Mit dem Device Firmware Upgrade-Modus (DFU) oder über die Systemeinstellung "Einstellungen und Inhalte löschen" lassen sich iOS-Geräte komplett löschen, zum Beispiel bevor sie ein neuer Mitarbeiter erhält. Der DFU-Modus kann über iTunes ausgelöst werden, dazu muss iTunes keine vorherige Host-Verbindung mit dem iOS-Gerät etabliert haben. Bei einer Erstverbindung mit dem Host muss für den Zugriff durch iTunes auf das Gerät der PIN Code eingegeben werden. Alternativ lässt sich der DFU-Modus durch eine Tastenkombination am iOS-Gerät starten. In der Regel enthalten auch Mobile Device Management-Programme eine entsprechende Funktionalität.

Domains und Ports für die Kommunikation

Damit iOS-Geräte reibungslos kommunizieren können, müssen Regeln für das Sicherheitsgateway (Firewall) konfiguriert werden. Welche Domainnamen und Ports aktuell freigeschaltet werden müssen, dokumentiert Apple online in Support-Dokumenten.

Fazit

Apple hat vor einigen Jahren mit dem iPhone und dem iPad den Grundstein für den heutigen Boom bei Tablets und Smartphones gelegt. Die Geräte des Konzerns aus Cupertino gelten als Designobjekte und haben im Markt eine hohe Begehrlichkeit. Weil die iDevices im privaten Umfeld so beliebt sind, war abzusehen, dass sie auch in Unternehmen und Behörden Einzug halten werden. Heute nutzen zahlreiche Institutionen neben anderen Smartphones und Tablets zahlreiche iDevices.

Es ist legitim, das Mitarbeiter die Vorteile wie einfache Benutzbarkeit und hohe Funktionalität im beruflichen Umfeld nutzen wollen. Doch hier müssen andere Sicherheitsmaßstäbe gelten, als im Privatbereich. Wenn beruflich verwendete Daten missbraucht werden oder verloren gehen, können hohe Schäden entstehen. Die Empfehlungen in diesem Überblickspapier sollen den Blick für potenzielle Gefahrenpunkte schärfen und helfen, diese Gefahren einzudämmen. Zusammen mit dem Überblickspapier "Smartphones" des BSI steht umfassendes Ratgebermaterial zur Verfügung, mit dem Smartphones allgemein und iDevices im Besonderen geschützt werden können.

An das BSI werden häufig Wünsche für IT-Grundschutz-Bausteine herangetragen, die aus verschiedenen Gründen nicht zeitnah realisierbar sind. Meist werden zu aktuellen neuen Vorgehensweisen, Technologien oder Anwendungen spezifische Sicherheitsempfehlungen benötigt, mit denen auf IT-Grundschutz basierende Sicherheitskonzepte schnell und flexibel erweitert werden können. Mit den Überblickspapieren sollen zeitnah zu aktuellen Themen Lösungsansätze präsentiert werden. Kommentare und Hinweise richten Sie bitte an: grundschutz@bsi.bund.de