Sicherheit mit iPhone und iPad

Eine Frage der Konfiguration

Dass mobile Geräte im Geschäftsleben eine bedeutende Rolle spielen, steht außer Frage. Sollten bei dieser Nutzung auch sensible Daten bearbeitet beziehungsweise gespeichert werden, ist es von maßgeblicher Bedeutung, dass diese Geräte entsprechend gegen unbefugten Zugriff gesichert werden. Man spricht hier von einer Härtung. Dieser Artikel beschreibt für iOS-Geräte, mit welchen Schritten diese Härtung mit Bordmitteln, die das Betriebssystem mitbringt, erreicht werden kann. Apple hat in den neueren Versionen einiges vorgesehen …

Apple hat in den letzten Jahren das Thema IT-Sicherheit deutlich nach vorne getrieben. Angefangen von Themen wie dem ständigen Ausbau der integrierten System-Sicherheit und des zugrundeliegenden kryptographischen Konzepts von iOS, sind es im Alltag vor allem die Einführung von Touch- beziehungsweise Face-ID, welche die Umsetzung von IT-Sicherheitsmaßnahmen unterstützen beziehungsweise erleichtern können.

Dieser Artikel hat das Ziel, einem interessierten iOS-Anwender (und mit iOS sind hier iPhone und iPad gemeint) in verständlicher Art und Weise Möglichkeiten aufzuzeigen, wie er die vorhandenen Bordmittel von Apple nutzen kann, um sein Gerät sicherer zu machen. Daher werden die grundlegenden Sicherheitskonzepte von Apple (wie beispielsweise die „Secure Enclave") hier nicht weiter vertieft. Zum besseren Verständnis soll aber kurz auf die Punkte Touch- beziehungsweise Face-ID eingegangen werden, da sie für das behandelte Thema von grundlegender Bedeutung sind. Es wird weiterhin auch keine Third-Party-Software betrachtet. Es geht nur um die Funktionen, die das Apple-Betriebssystem mitbringt.

Touch-ID und Face-ID

Mit Touch- beziehungsweise Face-ID hat Apple biometrische Verfahren eingeführt, um die Bestätigung der Identität einer berechtigen Person zu erlangen. Bei Touch-ID wird dabei die Fingerabdruck-Struktur und bei Face-ID die Gesichts-Struktur als Merkmal herangezogen.

Es ist hierbei wichtig zu wissen, dass diese biometrischen Verfahren als zusätzliche Funktionen zum Passcode zu verstehen sind. Dieser ist nach wie vor die Grundlage zur Entschlüsselung der Daten des iOS-Geräts. Der Passcode kann nun allerdings komplexer gestaltet werden (einen vierstelligen Passcode verwendet ja wohl hoffentlich niemand mehr zur Absicherung seines Geräts), da die Entsperrung des Geräts ja nun durch Touch- beziehungsweise Face-ID erfolgt. Es gibt aber Ausnahmen, bei denen ein Passcode nach wie vor notwendig ist. Diese sind in der Tabelle 1 aufgeführt.

Tabelle 1: Situationen, in denen ein Passcode zwingend benötigt wird

- Aktualisierung des Geräts
- Löschen des Geräts
- Änderung des Passcodes
- Installieren von iOS-Konfigurations-Profilen
- Nach dem Einschalten oder Neustart des Geräts
- Das Gerät wurde für 48 Stunden nicht entsperrt
- Das Passwort wurde in den letzten 156 Stunden (sechseinhalb Tage) nicht zum Entsperren des
- Geräts verwendet und das Gerät wurde in den letzten 4 Stunden nicht durch Biometrie entsperrt
- Das Gerät wurde remote gesperrt
- Es gab fünf erfolglose biometrische Anmeldeversuche
- Nach einem SOS Ruf

Wie sicher möchte ich sein?

Bevor es darum geht, wie ein iOS-Gerät gehärtet wird, ist es ratsam, dass der Benutzer sich Gedanken darüber macht, wie wichtig ihm persönlich IT-Sicherheit ist. Die folgenden Beispiele sollen als Anregungen dienen, wie eigene Überlegungen aussehen könnten, insbesondere in der Abwägung zwischen „Härtung" (Grad der Sicherheitskonfiguration) und dem sogenannten „Ease of Use" (der einfachen Benutzbarkeit):

- Ist mir bewusst, welche Vielzahl an persönlichen Daten auf dem Gerät gespeichert werden? Als Beispiele hierfür werden E-Mails, Zahlungsdaten, Kontaktdaten, Website-Accounts und -Passwörter, Termine, Gesundheitsdaten, Daten von Ortungsdiensten genannt.
- Es können Funktionen und Informationen auch bei einem gesperrten Gerät verfügbar sein (iMessage, E-Mail, Siri). Möchte ich das einschränken?
- Was mache ich, wenn das Gerät verloren geht oder gestohlen wird?
- Wie sehr möchte ich mich und meine Daten im Internet exponieren?
- Wie weit vertraue ich Firmen, die ihren Sitz außerhalb der Europäischen Union haben (z.B. der iCloud von Apple)?

Auf Basis dieser eigenen Überlegungen, können dann Entscheidungen getroffen werden, in welcher Form und „Schärfe" die nun folgenden Absicherungsmaßnahmen tatsächlich umgesetzt werden. Funktionen und Einstellungen, die eine solche Abwägung erfordern, werden in den Empfehlungen mit „prüfen", gefolgt von einer Empfehlung, gekennzeichnet.

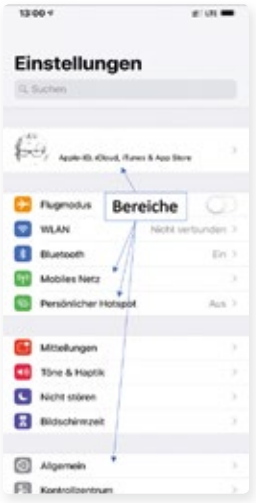
Basis-Sicherheit: der Passcode, Updates und Back-up

Zu den grundlegenden Bestandteilen eines Sicherheitskonzepts gehört der Passcode. Wie schon erwähnt, stellt ein vierstelliger numerischer Code heute keine angemessene Absicherung mehr dar. Also ist hier die Empfehlung, dass Benutzer von Touch-/Face-ID einen komplexen Passcode aus Sonderzeichen, alphanumerischen Zeichen in Klein- und Großschreibung und mit einer Länge von 8 bis 13 Zeichen verwenden. Es bietet sich an, die Zeichen aus den Anfangsbuchstaben eines leicht merkbaren Satzes zu verwenden. Sonderzeichen lassen sich am besten über eine einfache Regel generieren, beispielsweise ein „!" für ein „I". Der Passcode sollte schriftlich fixiert und an einem sicheren Ort aufbewahrt werden.

Von nicht weniger Bedeutung ist es, die Geräte auf dem neuesten Versionsstand (am besten mit automatischen Updates, siehe unten) zu halten sowie regelmäßig ein aktuelles Back-up zu erstellen. Wer Apple vertraut, kann hier Cloud-Back-up nutzen. Dieses Variante ist aber nicht so umfangreich und sichert vor allem nicht die Passwörter von Apps, wie es das verschlüsselte iTunes-Back-up tut.

Konfigurationsempfehlungen

Alle hier dargestellten Konfigurationsempfehlungen beziehen sich auf iOS 12.x und stellen eine Auswahl dar. Es wird also nicht jeder mögliche Parameter bewertet. Der einfacheren Lesbarkeit halber wurde die Tabellenform gewählt und bedarfsweise ein kurzer Kommentar hinzugefügt. Die erste Ebene (also ganz links) entspricht den Bereichen in der App „Einstellungen".



Die Bereiche der App „Einstellungen"

App „Einstellungen"

Apple-ID

Dieser Bereich befindet sich in der App ganz oben.

- Passwort & Sicherheit → Zwei-Faktor-Authentifizierung → aktivieren
  → Erhöht die Sicherheit der Apple-ID durch Abfrage eines weiteren Faktors (Code).
- iCloud → Mein iPhone suchen → aktivieren
- iCloud → iCloud Back-up → optional aktivieren
- Standort teilen→ optional aktivieren
  → Je nach persönlicher Einschätzung aktivieren, dann aber Mitglieder regelmäßig in der „Freunde"-App prüfen.

Mobiles Netz

- WLAN-Anrufe → aktivieren
  → WLAN-Anrufe haben in der Regel eine höhere Abhörsicherheit
- SIM-PIN prüfen, deaktivieren
  → setzt eine aktive Touch-/Face-ID beziehungsweise einen starken Passcode voraus. Nur so ist die Funktion „Mein

iPhone suchen" nach einem Neustart funktionsfähig.

Persönlicher Hotspot

- Persönlicher Hotspot → prüfen, deaktivieren
  → Wenn ein persönlicher Hotspot benötigt wird, sollte er nur für die Dauer des Einsatzes aktiviert sein und mit einem angemessenen WLAN-Passwort (> 8 alphanumerische Zeichen) versehen sein.

Mitteilungen

- Vorschauen zeigen (wenn entsperrt)
  → Erlaubt, dass Vorschauen von Mitteilungen aus Apps, wie Nachrichten, Mail, Kalender, Erinnerungen oder FaceTime, erst angezeigt werden, wenn das Gerät entsperrt ist.

Allgemein

- Softwareupdate → Automatische Updates → aktivieren
- AirDrop → nur für Kontakte
  → AirDrop lässt den Austausch von Daten zwischen iOS-Geräten in der Nähe zu. Diese Funktion sollte nur beschränkt und kontrolliert verfügbar sein.
- Handoff → prüfen, deaktivieren
  → Mit Handoff kann auf einem Gerät eine Aktivität anfangen und nahtlos auf einem weiteren iOS-Gerät mit gleicher Apple ID fortgesetzt werden.
- Hintergrundaktualisierung → prüfen, deaktivieren
  → Bei der Hintergrundaktualisierung werden unter Umständen auch Daten (wie der Standort) an Dritte übertragen.
- Tastatur → Diktierfunktion aktivieren → prüfen, deaktivieren
  → Ist die Diktierfunktion aktiviert, wird alles Gesagte an Apple gesendet. Ebenso die Standortdaten, wenn die Ortungsdienste aktiviert sind. Nach eigener Aussage verknüpft Apple diese Daten nicht mit Daten, die aus anderen Apple-Diensten stammen.
- Profile & Geräteeinstellungen → nur notwendige Profile
  → Profile bieten weitreichende Möglichkeiten, iOS-Geräte zu beeinflussen und sind deshalb mit Sorgfalt regelmäßig zu prüfen.

Kontrollzentrum

- Steuerelemente anpassen → prüfen, anpassen
  → Die im Kontrollzentrum verfügbaren Elemente sollten auf die wirklich notwendigen Funktionen beschränkt werden, insbesondere dann, wenn das Kontrollzentrum im Sperrbildschirm verfügbar ist (siehe auch „Touch/Face-ID & Code").

Anzeige & Helligkeit

- Automatische Sperre → aktivieren
  → Empfohlen wird eine Zeitspanne nicht größer als zwei Minuten, bei Verwendung von Touch/Face-ID nicht größer als 30 Sekunden.

Siri & Suchen

- Siri im Sperrzustand erlauben → prüfen, deaktivieren
  → Wie bei der Diktierfunktion werden Daten an Apple gesendet.

Mit Siri können im gesperrten Zustand die folgenden Funktionen ausgelöst werden:

- Telefonanrufe tätigen, SMS versenden, E-Mails versenden
- Anruferliste ansehen
- Voicemails anhören
- Apps aufrufen
- Bluetooth ein- und ausschalten, Flugmodus einschalten
- Details von bestimmten, namentlich bekannten Kontakten ansehen
- Details von Kontakten mit einfach zu erratenden Namen ansehen
- Einträge auf Twitter und Facebook machen
- In Apple Maps gespeicherte Adressen ansehen

Touch/Face-ID & Code

- Touch/Face-ID verwenden für: → alles aktivieren (iPhone entsperren, iTunes & App-Store, Passwort automatisch auffüllen
- Aufmerksamkeitsprüfung (nur Face-ID) → aktivieren
  → Hierbei wird geprüft, ob der Anwender aktiv ist (also zum Beispiel nicht schläft).
- Code anfordern → aktivieren
  → Geräte mit Touch/Face-ID „sofort", andere nach 1 Minute
- Im Sperrzustand Zugriff erlauben:
  1. Ansicht heute → deaktivieren
  2. Mitteilungszentrale → prüfen, deaktivieren
     → Wenn die Mitteilungszentrale aktiv bleiben soll, den Stil der Benachrichtigungen pro App individuell anpassen
     → zumindest bei Mail und Nachrichten „Vorschauen zeigen" deaktivieren.
  3. Kontrollzentrum → prüfen, deaktivieren
     → siehe auch „Kontrollzentrum"
  4. Siri → prüfen
     → siehe „Siri & Suchen"
  5. Mit Nachricht antworten → prüfen, deaktivieren
  6. Wallet → prüfen, deaktivieren
     → bei aktivierter Touch/Face-ID aktivieren
  7. verpasste Anrufer zurückrufen → prüfen, deaktivieren
  8. USB-Zubehör → deaktivieren
     → Wenn die Option deaktiviert ist, muss das iPhone, wenn es länger als eine Stunde gesperrt war, entsperrt werden, damit USB-Zubehör eine Verbindung herstellen kann.
  9. Daten löschen → aktivieren
     → Regelmäßig verschlüsselte Backups erstellen, damit im Fall einer Löschung – durch die Versuche Unbefugter – das Gerät wiederhergestellt werden kann.

Datenschutz

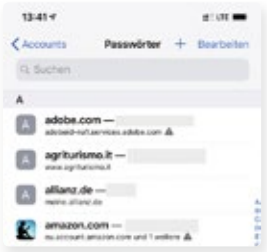
- Apps und Apps in Ortungsdienste → prüfen, selektiv setzen
  → Die Berechtigungen der Apps sollten sinnvoll und möglichst restriktiv gesetzt werden. Unnötige Berechtigungen sollten vermieden werden.
- Analyse → nicht senden
  → die hier lokal aufgezeichneten Daten können auch persönliche Informationen enthalten!
- Werbung → Kein Ad-Tracking aktiv
  → Hiermit wird den Werbeanbietern mitgeteilt, dass keine zielgerichtete Werbung gewünscht ist.

- Ortungsdienste → Systemdienste → prüfen, deaktivieren
  → Bei der Weitergabe von Standort und Bewegungsdaten ist Sparsamkeit anzuraten.
  → Folgende Ausnahmen sollten aktiviert bleiben: Kompasskalibrierung, Mein iPhone suchen, Mobilfunknetzsuche, Notruf & SOS, WLAN-Anrufe, WLAN Netzwerke und Zeitzone einstellen.
- Ortungsdienste → Systemdienste → Produktverbesserungen → deaktivieren

Passwörter & Accounts

- Website & App-Passwörter → regelmäßig prüfen
  → Hier werden Passwörter von Webseiten und Apps angezeigt, die iOS speichert. Mehrfach vorkommende Passwörter werden durch das Symbol Dreieck mit Ausrufezeichen dargestellt. Diese sollten genauer überprüft werden. Es empfiehlt sich, bei der Generierung solcher Passwörter die automatische iOS-Funktion zu nutzen.

Bild: © depositphotos.com/GaudiLab



Website & App-Passwörter mit Hinweis-Symbol

Safari

- Allgemein → Pop-Ups blockieren R aktivieren
- Datenschutz & Sicherheit R aktivieren
  → alle aktivieren, bis auf „alle Cookies blockieren"

Fotos

- iCloud-Fotos, Mein Fotostream → prüfen, deaktivieren
  → Diese Funktionen laden Ihre Fotos automatisch in die iCloud. Wer das nicht will, sollte diese Funktionen deaktivieren.

Diese Empfehlungen verstehen sich als Vorschläge. Schlussendlich entscheidet der Benutzer auf der Basis eigener Überlegungen (siehe Abschnitt „Wie sicher möchte ich sein?") über sein persönliches Sicherheitsniveau. Einer individuellen Härtung des eigenen iOS-Geräts steht nun aber nichts mehr im Weg. ■

ANDREAS JAGERSBERGER,
Principal Security Consultant bei CORPORATE TRUST Business Risk & Crisis Management