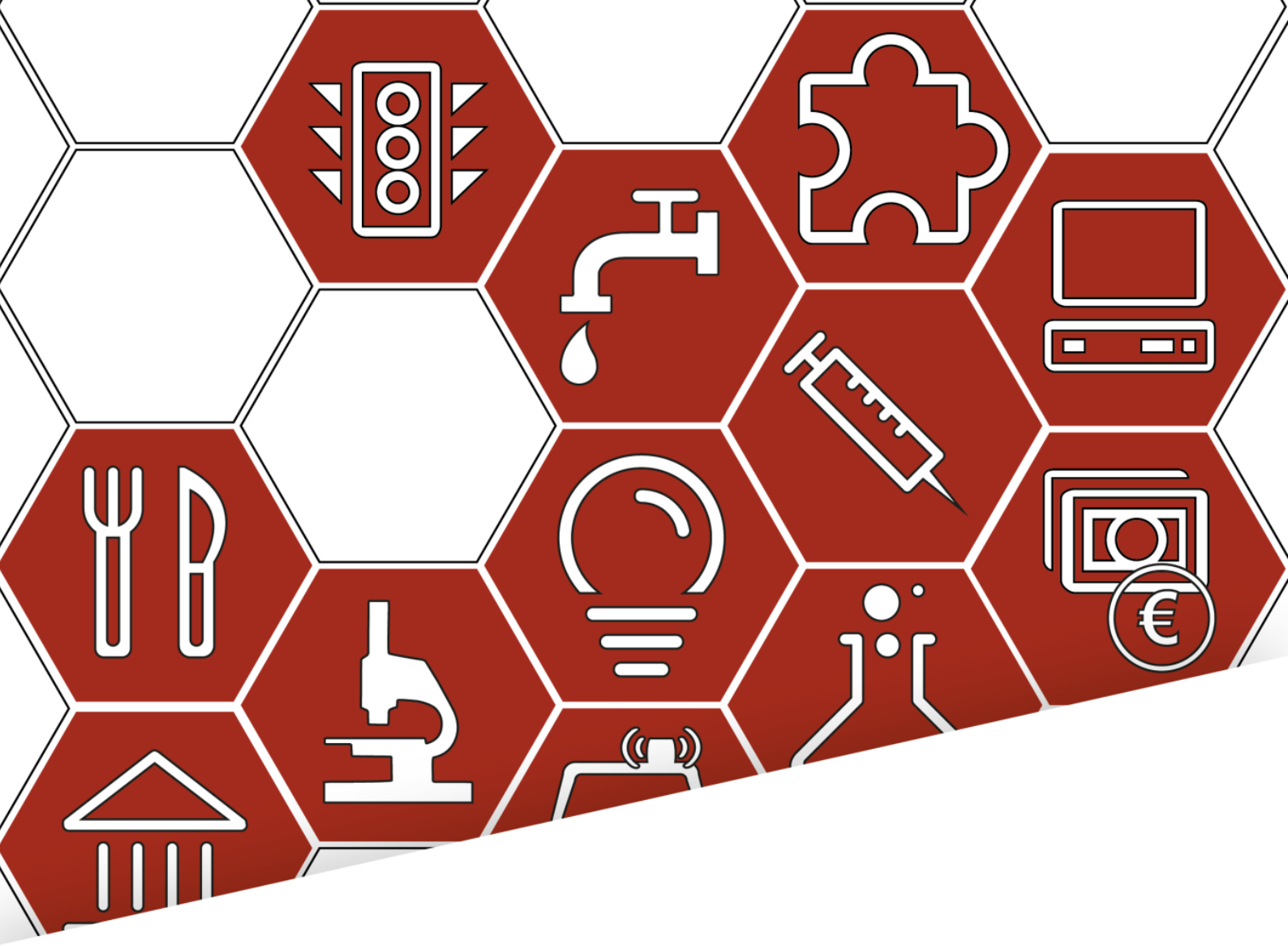

März 2017

Sicherheitsratschläge

zu iPhone & Co

20 Empfehlungen und präventive Maßnahmen

BM.I
REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR INNERES
BUNDESAMT FÜR VERFASSUNGSSCHUTZ UND TERRORISMUSBEKÄMPFUNG

IMPRESSUM

Medieninhaber/Herausgeber:
Bundesamt für Verfassungsschutz und Terrorismusbekämpfung,
Herrengasse 7, 1010 Wien

Herstellung:
Digitalprintcenter des BMI

CYBER SECURITY .BVT
Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert.

Inhalt

Ihr iPhone oder iPad - genau wie auch alle anderen modernen Smartphones - **kommuniziert permanent mit dem Internet**, sofern die entsprechende Verbindung eingerichtet und aktiv ist. Selbst wenn Sie Ihr iPhone gerade nicht aktiv verwenden oder es in Ihrer Hosentasche „schlummert“, werden Informationen aktiv an das Internet übermittelt oder aus dem Gerät ausgelesen. Vielen Benutzerinnen und Benutzern ist nicht bewusst, wie viele Daten Ihr Gerät dabei an Dritte weitergibt. Persönliche Nachrichten, Fotos und Zugangsdaten, aber auch Finanzinformationen werden im Hintergrund mit anderen Diensten synchronisiert und laufen dabei Gefahr, von Dritten mitgelesen oder von Angreifern gezielt ausspioniert zu werden.

Doch schon die Beachtung einiger grundlegender Empfehlungen kann die Sicherheit Ihres Gerätes und Ihrer Daten nachhaltig erhöhen. Leider stehen aber **Sicherheit und Komfort oftmals in einem Spannungsverhältnis**. Wenn Sie die folgenden Sicherheitsempfehlungen befolgen, kann es unter Umständen dazu kommen, dass einige (teilweise durchaus hilfreiche) Funktionen eingeschränkt werden oder nicht mehr zur Verfügung stehen. Gleichzeitig stellen Sie damit aber sicher, dass ihre **Daten besser geschützt sind und Ihre Privatsphäre signifikant erhöht** wird.

Natürlich müssen Sie nicht alle Empfehlungen befolgen. Wählen Sie für sich einfach jene aus, von denen Sie denken, dass Sie am geringsten beeinträchtigt werden oder deren Funktionen Sie ohnedies gar nicht oder nur selten nutzen - **es ist Ihre freie Wahl**! Und selbst wenn Sie unmittelbar keine der Sicherheitsempfehlungen anwenden, erhalten Sie mit diesem Dokument dennoch einen umfassenden Überblick über die wichtigsten Sicherheitsmaßnahmen bei der Handhabung Ihres iPhones und somit ein Gefühl für mögliche Bedrohungen.

1. Firmware-Updates

Jede Software enthält Fehler und Sicherheitslücken, auch die Firmware (Betriebssystemsoftware) in Ihrem iPhone oder iPad. Diese Sicherheitslücken werden vom Hersteller in mehr oder weniger kurzen Abständen durch Updates behoben. Doch Updates dienen neben der Bereinigung von Schwachstellen auch dazu, mehr oder weniger nützliche Funktionalitäten auf Ihr Gerät nachzuliefern. Viele Benutzerinnen und Benutzer fühlen sich durch häufige Updates gestört und führen diese in der Folge nicht mehr zeitnah aus oder verzichten gleich generell darauf.

Sicherheitslücken sind oft sehr gut im Internet dokumentiert und laden Nachahmungstäter dazu ein, diese für eigene Angriffe auszunützen. Daher ist es besonders wichtig, **Sicherheitsupdates jeweils zeitnah nach ihrem Erscheinen zu installieren**. Gleiches gilt sinngemäß natürlich auch für Ihre installierten Apps. Zur Installation rufen Sie in den Einstellungen den Eintrag Softwareaktualisierung auf. Das Smartphone sucht dann automatisch auf den Servern der Firma Apple, ob eine neuere Version für Ihr iPhone verfügbar ist.

„Einstellungen“ ► *„Allgemein“* ► *„Softwareupdate“*

2. Schutz gegen unbefugte Nutzung

Um die Daten auf Ihrem iPhone oder iPad auch nach einem Verlust oder Diebstahl zu schützen, ist es sehr wichtig, das Gerät gegen unbefugte Nutzung zu sperren. In der Regel wird dazu ein PIN-Code verwendet. Dieser bietet aber aufgrund der eingeschränkten Länge und der Beschränkung auf Ziffern einen vergleichsweise geringen Schutz. Sofern Ihr iPhone dies unterstützt, empfehlen wir zum Schutz ihrer Daten **statt des PIN-Codes ein starkes Kennwort („alphanumerischer Code“) zur Entsperrung** Ihres Gerätes zu verwenden.

„Einstellungen“ ► „Touch ID & Code“ ► „Code ändern“ ► „Codeoptionen“

Die Stärke eines Kennworts wird einerseits durch die Länge, andererseits durch den verwendeten Zeichenvorrat bestimmt. Eine **ausreichend lange Kombination aus Buchstaben, Zahlen und Sonderzeichen bietet dabei den bestmöglichen Schutz**. In den Codeoptionen haben Sie die Möglichkeit, zwischen drei verschiedenen Kennwortarten („Codes“) zu wählen:

- *Eigener alphanumerischer Code*
- *Eigener numerischer Code*
- *Vierstelliger numerischer Code*

Auch hier gilt natürlich wieder, dass Sicherheit und Komfort in einem Spannungsverhältnis stehen. Ob Ihnen eine deutlich erhöhte Sicherheit den zusätzlichen Aufwand für die Eingabe eines starken Kennworts wert ist, müssen aber letztlich Sie selbst entscheiden.

Darüber hinaus empfehlen wir, dass Ihr iPhone so eingestellt wird, dass die **Kennwortabfrage immer unmittelbar, also ohne Verzögerung nach dem Aktivieren des Sperrbildschirms** erforderlich wird. So ist sichergestellt, dass das Gerät auch unmittelbar nach dem Sperren bereits geschützt ist.

„Einstellungen“ ► „Touch ID & Code“ ► „Pass Code verlangen: sofort“

Zusätzlich bietet Ihr iPhone für den Fall des Verlusts oder Diebstahls eine weitere Sicherheitsfunktion, die „**Datenlöschfunktion**“. Ist diese aktiviert, so wird der gesamte Gerätespeicher gelöscht, wenn der Pass Code zehnmal falsch eingegeben wird.

„Einstellungen“ ► „Touch ID & Code“ ► „Daten löschen: ein“

Doch hier ist Vorsicht geboten! Denken Sie daran, dass die Daten nach erfolgter Löschung auch von Ihnen nicht wieder hergestellt werden können (ausgenommen natürlich, Sie haben zuvor ein lokales Backup mit iTunes durchgeführt ► *siehe Punkt 20*).

Anmerkung: Abhängig von der verwendeten Gerätegeneration steht Ihnen der Fingerabdrucksensor („Touch ID“) zur Verfügung. Dieser ersetzt über weite Bereiche das Erfordernis, Kennwörter einzugeben. Mittlerweile ist mehrfach nachgewiesen, dass auch **Touch ID keinen absoluten Schutz bietet**. Inwieweit Sie Touch ID als Zugangsschutz nützen möchten, obliegt dabei Ihnen.

3. Deaktivieren von Sperrbildschirm-Benachrichtigungen

Egal, wie komplex Ihr Kennwort auch ist, es verhindert nicht, dass vertrauliche Daten von Dritten gelesen werden können, wenn diese auf dem Sperrbildschirm angezeigt werden. E-Mail-, Messenger- und WhatsApp Nachrichten, sowie viele weitere Informationen Ihrer installierten Apps können bei Ihrem iPhone auch auf dem Sperrbildschirm angezeigt werden. Dadurch können solche Informationen **ohne Eingabe des PIN-Codes oder Kennworts gelesen werden**.

Vorsicht ist vor allem bei SMS-TANs oder privaten Terminen angebracht. Diese werden auf diese Art und Weise oft ungewollt angezeigt und geben Dritten unerwünschte **Einblicke in Ihre Privatsphäre**. Je weniger Informationen Ihr iPhone auf dem Sperrbildschirm präsentiert, desto sicherer sind Ihre Informationen vor fremden Blicken.

1. *„Einstellungen“ ► „Touch ID & Code“ ► „Zugriff bei Sperrung erlauben“*
2. *Home-Steuerung: aus*

Wenn „Home-Steuerung“ nicht deaktiviert ist, müssen Sie für jede App einzeln entscheiden, ob Sperrbildschirm-Benachrichtigungen zulässig sein sollen.

4. Zwei-Faktor-Authentifizierung

Zwei Schlösser sind besser als eines! Wir empfehlen daher überall dort, wo es möglich ist, die Zwei-Faktor-Authentifizierung zu nutzen. Dies gilt insbesondere für Apple-ID und iCloud. Die **Zwei-Faktor-Authentifizierung bietet zusätzliche Sicherheit** für Ihre Apple-ID. Sie wurde entwickelt um sicherzustellen, dass nur Sie selber auf Ihren Account zugreifen können, selbst wenn jemand anderer Ihr Kennwort kennt. Das Verfahren ist vergleichbar mit dem mTAN-Verfahren beim Online-Banking.

Wenn Sie die Zwei-Faktor-Authentifizierung einrichten, können Sie ein oder mehrere vertrauenswürdige Geräte registrieren, die dann vierstellige Authentifizierungscodes empfangen können (entweder per SMS oder über den „Find-my-iPhone“-Service). Wenn Sie sich künftig anmelden, um Ihre Apple ID zu verwalten, die iCloud zu nutzen oder einen Einkauf in iTunes, iBooks oder dem App-Store zu tätigen, müssen Sie Ihre Identität bestätigen, indem Sie **sowohl Ihr Kennwort, als auch den vierstelligen Code eingeben**, der für genau diese eine Anmeldung auf das registrierte Endgerät übermittelt wurde.

Die Aktivierung der Zwei-Faktor-Authentifizierung erfordert zwei separate Schritte.

Schritt 1 (auf Website):

https://appleid.apple.com ► „Verwalten Ihrer Apple ID“ ► „Sicherheit“ ► „Zwei-Faktor-Authentifizierung“

Schritt 2 (auf iPhone oder iPad mit iOS 9 oder neuer):

1. *„Einstellungen“ ► „iCloud“*
2. *Wenn notwendig, melden Sie sich an und tippen Sie auf Ihre Apple-ID*
3. *„Passwort & Sicherheit“ ► „Zwei-Faktor-Authentifizierung: ein“*

5. Deaktivieren von Siri auf dem Sperrbildschirm

Siri (Speech Interpretation and Recognition Interface) dient der Erkennung gesprochener Sprache und dient auf iPhones und iPads als persönlicher Assistent. Wichtig dabei ist, dass **Siri mit jedem kommunizieren kann und wird**, nicht nur mit dem rechtmäßigen Besitzer des Geräts.

Ihr iPhone bietet die Möglichkeit, **Siri ohne Entsperrung direkt am Sperrbildschirm zu verwenden**. In der Praxis bedeutet das aber, dass jeder Siri nutzen kann, wenn er physischen Zugriff auf Ihr Gerät hat. In diesem Fall kann Siri natürlich auch Ihre persönlichen Informationen preisgeben.

Zur Sicherheit Ihrer vertraulichen Daten empfehlen wir daher, die **Nutzung von Siri am Sperrbildschirm zu verbieten**.

„Einstellungen“ ►„Siri“ ► „Zugriff im Sperrzustand: aus“ und

„Einstellungen“ ►„Siri“ ►„Hey Siri erlauben: aus“

6. Deaktivieren der Synchronisierung mit der iCloud

Alle Daten, die Sie auf Ihrem iPhone oder iPad speichern, werden automatisch mit der iCloud synchronisiert. Das bedeutet, dass unter anderem **Nachrichten, Notizen, Kontaktinformationen oder Dokumente im Hintergrund in die Cloud** kopiert werden und dort bestehen bleiben (unter Umständen auch dann, wenn Sie sie am Smartphone längst gelöscht und vergessen haben).

Eine Synchronisierung Ihrer Daten mit der iCloud kann natürlich auch sinnvoll sein, insbesondere wenn Sie **mehrere Geräte nutzen, die permanent und automatisch am selben Stand** bleiben sollen. Ob Sie also dieses Service deaktivieren oder nicht, hängt primär von Ihren eigenen Nutzungsgewohnheiten ab.

1. *„Einstellungen“ ► „iCloud“*
2. *Deaktivieren Sie die Synchronisation überall dort, wo sie nicht benötigt wird*

7. Verhindern automatischer WLAN-Verbindungen

Hat sich Ihr iPhone oder iPad einmal mit einem WLAN-Hotspot verbunden, so speichert Ihr Gerät diese Informationen. Kommt Ihr Gerät (nach dem Verlassen dieses WLAN-Hotspotbereichs) zu einem späteren Zeitpunkt wieder in den Empfangsbereich dieses WLANs, wird es sich **automatisch wieder mit diesem Netz verbinden**. Dies geschieht ohne weitere Rückfrage oder Bestätigung automatisch im Hintergrund.

Diese an sich nützliche Funktion kann jedoch von frei im Internet erhältlichen Geräten („bad hotspots“) ausgenützt werden, um Ihr iPhone anzugreifen. Diese **Geräte sind in der Lage, jeden beliebigen WLAN-Hotspot nachzuahmen** und ihrem Telefon vorzutäuschen, ein bereits gespeicherter, vertrauenswürdiger Hotspot zu sein. Während also Ihr iPhone glaubt, mit einem bekannten WLAN verbunden zu sein, hat es sich in

Wirklichkeit mit dem Netz des Angreifers verbunden. Das bietet dem Angreifer zum einen die Möglichkeit, problemlos Ihren **Netzwerkverkehr mitzulesen**, zum anderen befindet sich ihr Endgerät währenddessen im Netz des Angreifers. Dieser Umstand eröffnet dem Angreifer **weitaus effektivere Angriffsmöglichkeiten**.

Wir empfehlen daher grundsätzlich, das **WLAN ihres iPhones oder iPads nur bei Bedarf zu aktivieren** und sofort nach der Benutzung wieder zu deaktivieren. Positiver Nebeneffekt ist eine deutlich verlängerte Akkulaufzeit. Es ist durchaus verständlich, dass diese Maßnahme eine Verringerung des Benutzungskomforts bedeutet, allerdings ist das Risiko gerade bei diesem Punkt nicht zu unterschätzen. „Bad hotspots“ sind im Internet für wenig Geld für jedermann erhältlich.

8. Verwendung eines VPN

Wenn Sie von unterwegs mit Ihrem Firmennetzwerk kommunizieren, sollte diese Verbindung als **virtuelles privates Netzwerk (VPN)** konfiguriert werden. Dies gilt umso mehr, wenn sie öfters unsichere, öffentliche WLAN-Hotspots (Flughäfen, Restaurants, Hotels, öffentliche Plätze) verwenden müssen.

Grundsätzlich handelt es sich bei einem VPN um ein in sich geschlossenes, verschlüsseltes Kommunikationsnetz. Dieses verfügt allerdings nicht über eigene physikalische Verbindungen zwischen den Endstellen, sondern es benutzt in der Regel das öffentliche Internet als Transportmedium.

Die Sicherheit wird dadurch erzeugt, dass sie zwischen den Endpunkten temporär einen verschlüsselten Kanal aufbauen, der wie ein **sicherer Tunnel durch das Internet** wirkt. Dadurch kann bei entsprechender Konfiguration eine abhör- und manipulationssichere Kommunikation zwischen den Endpunkten sichergestellt werden.

„*Einstellungen*“ ► „*Allgemein*“ ► „*VPN*“ ► „*VPN hinzufügen*“

Es würde den Rahmen dieses Dokuments sprengen, detailliert auf die Einrichtung und die Nutzung von VPNs einzugehen, weswegen wir uns an dieser Stelle auf den bloßen Hinweis beschränken müssen. Zu beachten ist jedenfalls, dass die Nutzung von verschlüsselten VPN einerseits in manchen Ländern aus politischen Gründen problematisch ist und dass es andererseits Apps gibt, die bei der Verwendung über ein VPN in ihrer Funktion eingeschränkt sind.

9. AirDrop deaktivieren

AirDrop ermöglicht es Ihnen, **Dateien zwischen iOS-Geräten, wie iPhone und iPad ohne externe LAN- oder WLAN-Verbindungen auszutauschen**. Die Konfiguration und die Verbindung zwischen den Geräten erfolgen dabei automatisch, somit müssen von Ihnen keine weiteren Einstellungen getätigt werden.

AirDrop funktioniert laut Hersteller in einem Umkreis von bis zu neun Metern. Der Datenaustausch per AirDrop ist bequem, sollte aber unseres Erachtens **nur bei Bedarf kurz aktiviert werden**. Jeder nach außen sichtbare Dienst stellt für Angreifer eine

potenzielle Einbruchsmöglichkeit dar. Wenn Sie AirDrop unmittelbar nach jedem Gebrauch wieder deaktivieren, reduzieren Sie diese Gefahr erheblich.

Ein durchaus erfreulicher Nebeneffekt ist, dass Ihr iPhone oder iPad bei deaktiviertem AirDrop erheblich weniger Strom verbraucht und dadurch die Akkulaufzeit erhöht wird.

„Einstellungen“ ► „Allgemein“ ► „Einschränkungen“ ►„AirDrop: aus“

10. WLAN und Bluetooth sicher nutzen

Ähnliches wie für AirDrop gilt auch für andere Schnittstellen Ihres iPhones oder iPads, wie WLAN oder Bluetooth. Keine Schnittstelle ist gegen mögliche Angriffe besser geschützt, als eine deaktivierte Schnittstelle.

Sie sollten es sich zur Gewohnheit machen, Schnittstellen Ihres Gerätes (wie WLAN oder Bluetooth) **immer zu deaktivieren, wenn diese nicht benötigt werden**. Nicht nur die bereits beschriebene automatische Anmeldung an WLAN-Netze, sondern auch die gemeinsame Nutzung von WLANs (Flughäfen, Restaurants, Hotels, öffentliche Plätze) sind Gefahrenquellen. Meist „sieht jeder jeden“, nur selten sind qualitativ hochwertige WLAN-Access-Points im Einsatz, die den Datenverkehr aller Teilnehmer auch sauber trennen können.

Übrigens gilt natürlich auch hier, dass Ihr iPhone oder iPad bei deaktivierten Schnittstellen durchaus weniger Strom verbraucht und dadurch die Akkulaufzeit erhöht wird.

11. Deaktivieren der Auto-Ausfüllen-Funktion in Safari

Wird Ihr iPhone oder iPad gestohlen oder bekommt ein unbefugter Dritter aus einem anderen Grund die Möglichkeit des physischen Zugriffs auf das Gerät, besteht die Möglichkeit, dass diese Person Daten, die Sie irgendwann zuvor einmal eingegeben haben, **mit Hilfe der Auto-Ausfüllen-Funktion lesen und benutzen kann**. Das kann sogar so weit gehen, dass sich jemand, der Ihr Gerät unbefugt benutzen kann, sich auf verschiedenen Webseiten für Sie ausgibt.

Auch hier kommt das bereits angesprochene Spannungsverhältnis zwischen Sicherheit und Komfort deutlich zum Vorschein. Trotzdem empfehlen wir zum Schutz Ihrer kritischen Daten (zumindest Namen, Kennwörter und Kreditkarteninformationen), **die Auto-Ausfüllen-Funktion in Safari zu deaktivieren** und somit diese Gefahr zu reduzieren.

„Einstellungen“ ► „Safari“ ► „Namen und Passwörter: aus“ und

„Einstellungen“ ► „Safari“ ► „Kreditkarten: aus“

Dadurch wird sichergestellt, dass solche Daten nicht gespeichert und missbraucht werden können.

12. Zugriffe von Apps auf private Daten verhindern

Viele Apps können problemlos auf Ihre privaten Daten zugreifen. Es gibt in Ihrem iPhone oder iPad eine Menge **Funktionen und Datentypen, auf die fast jede App zugreifen kann**. Das beginnt bei Bildern und Kontakten und endet bei Ihrem Standort oder Ihren Nachrichten.

Jede App fragt einmalig nach, ob sie Zugriff auf bestimmte Informationen erhalten darf. Erlaubt man den Zugriff, so merkt sich die App dies für das nächste Mal und fragt nicht mehr erneut nach. So erlangen Ihre Apps im Laufe der Zeit eine Vielzahl von Berechtigungen. Und mit der Zeit **vergisst der Benutzer vollkommen, welche Informationen von welchen Apps verwendet werden dürfen**.

Das muss nicht so sein! Erfreulicherweise finden sich auf Ihrem iPhone und iPad Möglichkeiten, mit denen Sie Ihre Privatsphäre besser schützen können. Sie können in den Datenschutzeinstellungen den **Zugriff auf Kontakte, Bilder oder Nachrichten selektiv einschränken**. Bei einer zu restriktiven Handhabung ist es jedoch möglich, dass auch legitime Funktionen eingeschränkt werden. Auf jeden Fall erscheint es sinnvoll, die **Zugriffsrechte Ihrer Apps regelmäßig zu überprüfen** und gegebenenfalls anzupassen.

„Einstellungen“ ► „Datenschutz“ ► „Kontakte“ bzw. „Fotos“ bzw. „Kalender“ u.s.w.

13. E-Mail Sicherheit

Wenn Sie eine unverschlüsselte E-Mail von A nach B senden, verhält es sich genauso, wie wenn Sie eine Ansichtskarte mit der Post versenden. Jede Person, die die Karte entlang des Weges in die Hand bekommt, **kann Inhalte hinzufügen, löschen oder verändern**. Und sie kann dies in Ihrem Namen tun! Aus diesem Grund sollte eine **E-Mail-Übermittlung eigentlich immer verschlüsselt** sein.

Grundsätzlich kann man zwischen zwei verschiedenen Arten von Verschlüsselung unterscheiden:

- **End-to-End-Verschlüsselung**
- **Transportverschlüsselung**

Vereinfacht gesagt, verschlüsseln Sie Ihre Daten bei einer **End-to-End-Verschlüsselung** bereits in Ihrem Gerät und schicken die verschlüsselten Daten in Richtung Ziel. Ob die Übertraungsstrecke zwischen Ihnen und dem Ziel zusätzlich verschlüsselt ist, ist für Sie nicht relevant. Die Entschlüsselung kann erst durch den Empfänger erfolgen.

Der Vorteil ist, dass niemand entlang der Übertragungsstrecke (unverschlüsselten) Zugriff auf Ihre Daten hat. Der Nachteil hingegen ist, dass die Einrichtung und Nutzung dieser Funktionalität mit einigem Aufwand für Sie und Ihre Kommunikationspartner (Austausch und Einrichtung von Zertifikaten) verbunden ist. Details zu dieser Verschlüsselungsart würden den Rahmen dieses Dokuments jedoch sprengen.

Bei der **Transportverschlüsselung** werden nicht die Daten an sich, sondern die Übertragungsstrecke (oder Teile davon) verschlüsselt. Das bedeutet, dass Sie Ihre Daten unverschlüsselt in Richtung Ziel absenden können. Entscheidend dabei ist aber, dass die Übertragungsstrecke(n) richtig konfiguriert ist/sind.

Als Endbenutzer haben Sie im Bereich der Transportverschlüsselung **lediglich Einfluss auf die Übertragungsstrecke zwischen Ihrem Endgerät und Ihrem E-Mail-Provider**. Auf die Übertragungsstrecken zwischen Ihrem Provider und dem Provider des Empfängers, sowie auf die Übertragungsstrecke zwischen dem Empfänger und seinem Provider haben Sie keinerlei Einfluss; diese Strecken könnten gegebenenfalls auch unverschlüsselt sein.

In einem beruflichen Umfeld (d.h. bei dienstlichen Mobilgeräten) wird die Kommunikation zwischen Ihrem iPhone oder iPad und dem E-Mail Provider in der Regel durch den unternehmensinternen IT-Bereich konfiguriert. In einem privaten Umfeld hingegen müssen Sie diesen Teil der **Übertragungsstrecke selbst konfigurieren. Nutzen Sie SSL/TLS**!

Bei den allermeisten Providern kann die Kommunikation zwischen Ihrem Endgerät und dem Provider sowohl unverschlüsselt, als auch verschlüsselt konfiguriert werden. Sollte Ihr Provider eine verschlüsselte Nutzung nicht unterstützen, sollten Sie überlegen, ob Sie den Provider nicht besser wechseln sollten.

1. *„Einstellungen“ ► „Mail“ ► „Accounts“*
2. *E-Mail Konto auswählen► „Account“ ► „Erweitert“ ►„SSL verwenden: ein“*

Anmerkung: Alle Daten, die Sie zur Konfiguration Ihres Accounts benötigen, erhalten Sie von Ihrem Provider. Das sind im Wesentlichen die Servernamen für sendenden und empfangenden Betrieb, sowie die entsprechenden Portnummern.

14. Bilder in E-Mails

Wenn Sie auf Ihrem iPhone oder iPad E-Mails empfangen und diese öffnen, werden darin enthaltene Bilder automatisch angezeigt. Das gilt in der Standardkonfiguration sowohl für in die E-Mail eingebettete Bilder, als auch für lediglich verlinkte Bilder. Doch gerade **das automatische Nachladen von verlinkten Bildern birgt in der Praxis erhebliche Risiken**.

Das automatische Nachladen von verlinkten Bildern wird insbesondere von den Versendern von Spam genutzt, um die Validität der verwendeten E-Mail-Adressen zu verifizieren. Das wird dadurch möglich, dass sich Ihr E-Mail Programm in diesem Fall beim Webserver, auf dem das verlinkte Bild physisch liegt, aktiv melden muss. Diese Kontaktaufnahme kann vom Angreifer registriert werden. Somit weiß der Angreifer, dass die E-Mail-Adresse auf einen validen Empfänger gezeigt hat. Darüber hinaus kann dieses Feature auch das Einschleusen von Schadsoftware erleichtern.

Wir empfehlen, die im Auslieferungszustand aktivierte Funktionalität „Bilder von Web-Servern laden“ **in den Mail-Einstellungen auszuschalten**. Ist in einer E-Mail, deren

Ursprung Sie vertrauen, ein verlinktes Bild enthalten, können Sie dieses bei Bedarf ohne großen Aufwand manuell nachladen.

„Einstellungen“ ► „Mail“ ► „Bilder von Web-Servern laden: aus“

15. Mein iPhone suchen

Wir hoffen, dass Sie nie in diese Situation kommen: iPhone verlegt, verloren oder gar gestohlen. Eine Möglichkeit, für diese Situation vorzusorgen, ist die **Einrichtung der App „Mein iPhone suchen“**. Diese Anwendung zeigt auf einer Karte den momentanen Aufenthaltsort des mobilen Gerätes. Dabei wird GPS zur Ortung genutzt.

Nach einer erfolgreichen Ortung haben Sie mit Ihrer Apple-ID auf der Seite *https://icloud.com/find* mehrere Möglichkeiten:

- Sie können am Gerät einen **Ton abspielen**. Damit beginnt das Gerät, einen lauten Ton auszusenden, um Sie nochmals bei der Suche zu unterstützen.
- Sie können in den **Modus „Verloren“** wechseln. Mit dieser Funktion senden Sie eine Telefonnummer an das verlorene Gerät, unter der Sie ein etwaiger Finder kontaktieren kann.
- Sie können das **Gerät löschen**. Dabei werden alle Inhalte und Einstellungen gelöscht. Gleichzeitig wird mit dieser Funktion auch die **Aktivierungssperre** eingeschaltet, die das Zurücksetzen auf Werkseinstellungen verhindert und das Gerät bei einem Diebstahl mehr oder weniger wertlos macht. Ihr iPhone oder iPad kann in diesem Fall nur mehr von Apple - unter Vorlage eines Eigentumsnachweises - reaktiviert werden.

Diese an sich sinnvolle Funktionalität hat jedoch den Nachteil, dass die App **nur im Rahmen der iCloud** funktioniert und Ihr iPhone oder iPad Ihr **Bewegungsprofil permanent an Apple** übermittelt.

„Einstellungen“ ► „Datenschutz“ ► Ortungsdienste ► „Ortungsdienste: ein“ und

„Einstellungen“ ► „Datenschutz“ ► Ortungsdienste ► „Systemdienste“ ► „Mein iPhone suchen: ein“

16. Ortungsdienste

Ihr iPhone oder iPad verwaltet in den Einstellungen, welche Apps oder Systemdienste **Zugriff auf die Daten des Ortungsdienstes** haben. Viele Apps und Systemdienste machen regen Gebrauch von der Positionsbestimmung, ohne dass dies für den Anwender einen signifikanten Nutzen bringt. Wir empfehlen daher, dass Sie diese Einstellungen regelmäßig kontrollieren.

„Einstellungen“ ► „Datenschutz“ ► Ortungsdienste ► „Ortungsdienste“ bzw.

„Einstellungen“ ► „Datenschutz“ ► Ortungsdienste ► „Systemdienste“

Bei den Systemdiensten erscheinen zum Beispiel die ortsabhängigen „iAds“, sowie „Hinweise“, „häufige Orte“ und „beliebte Orte in der Nähe“ praktisch überflüssig. Sie werden kaum von Apps unterstützt, ermöglichen aber die Erstellung **detaillierter Bewegungsprofile**. Positiver Nebeneffekt ist auch hier eine deutlich verlängerte Akkulaufzeit, da die GPS-Funktion signifikant weniger genutzt wird.

17. Jailbreak or not?

„Jailbreaking“ bedeutet die **Umgehung einer Schutzfunktion**. Normalerweise können Sie nur jene Funktionen auf Ihrem iPhone oder iPad nutzen, die Ihnen Apple über die Benutzeroberfläche zur Verfügung stellt. Ein „Jailbreak“ ermöglicht den direkten Zugriff auf das darunterliegende Betriebssystem („Kernel-Zugriff“). Das Umgehen der vom Hersteller bewusst implementierten Einschränkungen bietet neben einigen unbestreitbaren Vorteilen aber auch **erhebliche Nachteile und Gefahren**.

Mit einem „Jailbreak“ erlischt einerseits die Herstellergarantie Ihres iPhones, wesentlich schwerwiegender ist andererseits jedoch der Sicherheitsaspekt. Nicht nur Sie erhalten bei einem derart manipulierten Gerät direkten Zugriff auf das Betriebssystem, sondern auch jegliche Schadsoftware. Bedenken Sie, dass Sie durch einen „Jailbreak“ bewusst **vom Hersteller gesetzte Sicherheitsmaßnahmen außer Kraft** setzen. So können beispielsweise problemlos selbst signierte Anwendungen ausgeführt werden, was eine erhöhte Gefahr für Malware-Aktivitäten bedeutet.

Wir empfehlen daher dringend, von einem „Jailbreak“ Abstand zu nehmen. Hacken Sie nicht Ihr eigenes Gerät! Vertrauen Sie gerade in diesem Fall nicht irgendwelchen fragwürdigen Anleitungen aus dem Internet.

18. WLAN-Passwort

Der folgende Punkt behandelt ausnahmsweise nicht direkt eine Funktion Ihres iPhone oder iPads, ist aber nichtsdestotrotz für die Sicherheit Ihres Gerätes von großer Bedeutung. Oft verwenden Nutzer an Orten, an denen Sie sich bevorzugt aufhalten (Wohnung), ein WLAN, das über einen festen Zugangspunkt ans Internet angebunden ist. Die Kommunikation zwischen Ihrem Mobiltelefon und dem WLAN-Hotspot sollte dabei bestmöglich gesichert sein.

Wir empfehlen daher, auf dem WLAN-Hotspot eine **Verschlüsselung nach dem WPA2-Standard** mit einem sicheren, starken **Kennwort von mindestens fünfzehn Zeichen** einzurichten. Das Kennwort sollte dabei sowohl Groß- als auch Kleinbuchstaben, sowie Ziffern und/oder Sonderzeichen enthalten. Dabei muss nicht darauf geachtet werden, ob man sich das Kennwort leicht merken kann. Das WLAN-Kennwort wird nur ein einziges Mal eingegeben und dann dauerhaft gespeichert.

Das WLAN-Kennwort kann danach notiert und **an sicherer Stelle (z.B. Safe) abgelegt werden**. Geht die Verbindung einmal verloren oder wird sie irrtümlich gelöscht, so kann man das WLAN-Kennwort nachlesen und wieder neu eingeben.

Gleiches gilt natürlich auch für den Fall, in dem Sie Ihr **iPhone oder iPad als Hotspot** einrichten. In diesem Fall müssen Verschlüsselungsart und starkes Kennwort analog zu oben auf Ihrem Mobiltelefon eingerichtet werden.

19. Schutz Ihrer Privatsphäre

Viele Websites und Onlineshops legen Profile mit detaillierten Daten an, um Kunden zu erkennen, zu bewerten und ihnen (im Bestfall) **maßgeschneiderte Angebote** zu präsentieren. Oft werden diese Daten allerdings auch weiterverkauft und von Dritten mit anderen Daten über Sie verknüpft. So entstehen sehr rasch Datensammlungen, die **Ihre Privatsphäre nachhaltig untergraben**. Glücklicherweise bietet Ihr iPhone oder iPad Möglichkeiten, diese „Sammelwut" ein wenig einzuschränken.

„Einstellungen" ► *„Datenschutz"* ► *„Werbung"* ► *„Kein Ad-Tracking: ein" und*

„Einstellungen" ► *„Safari"* ► *„Kein Tracking: ein"*

Durch Aktivieren von „Kein Ad-Tracking" wird zwar möglicherweise genauso viel Werbung wie bisher angezeigt und es kann sein, dass die angezeigte Werbung für Sie weniger relevant ist; der Vorteil dieser Vorgangsweise besteht aber darin, dass **weniger Daten über Sie gespeichert** werden.

Darüber hinaus empfehlen wir, dass Sie ab und zu **Ihre Ad-ID zurücksetzen**. Die Ad-ID ist die Kennung, die Sie als Werbeempfänger eindeutig identifiziert und unter der die Daten zu Ihrer Person gespeichert werden. Wenn Sie die mit Ihrer Ad-ID verknüpften Informationen löschen möchten, können Sie diese einfach zurücksetzen.

„Einstellungen" ► *„Datenschutz"* ► *„Werbung"* ► *„Ad-ID zurücksetzen"*

Ihr iPhone oder iPad überträgt darüber hinaus eine Vielzahl an Informationen über die Art und Weise, wie Sie Ihr Gerät nutzen bzw. über mögliche Probleme an Apple. Wenn Sie dies nicht wünschen, können Sie die **Übertragung von Benutzerdaten an Apple vollständig ausschalten**.

„Einstellungen" ► *„Datenschutz"* ► *„Diagnose & Nutzung"*

Nicht unmittelbar damit in Zusammenhang steht die **Funktionalität „Betrugswarnung"**. Trotzdem empfehlen wir an dieser Stelle, dieses Feature zu aktivieren. Nach einer Aktivierung wird Safari Sie mit hoher Wahrscheinlichkeit warnen, wenn Sie eine Phishing-Website angesteuert haben. In diesem Fall sollen Sie auf keinen Fall persönliche Daten eingeben.

„Einstellungen" ► *„Safari"* ► *„Betrugswarnung: ein"*

20. Regelmäßiges Backup

Zu guter Letzt gehört zur Sicherheit Ihres Mobiltelefons - wie bei jedem Computer - ein **regelmäßiges Backup der Nutzerdaten** auf Ihrem iPhone oder iPad. Dazu zählen unter anderem Ihre Dokumente, aber auch Ihre Einstellungen.

Der Trend zur Nutzung einer **cloudbasierten Lösung** ist auch hier nicht mehr zu stoppen. Ihr iPhone oder iPad sieht dafür die iCloud vor. Diese Möglichkeit steht dabei im Widerspruch zum oben Gesagten (► *siehe Punkt 6*). Wenn Sie sich für diese Möglichkeit entscheiden, muss Ihnen bewusst sein, dass Ihre gesamten persönlichen Daten auf Servern von Apple gespeichert werden. Dies erfordert durchaus ein **erhebliches Maß an Vertrauen**. Einerseits müssen Sie darauf vertrauen, dass die Datensicherheit auf diesen Servern Ihren diesbezüglichen Anforderungen genügt, andererseits müssen Sie aber auch darauf vertrauen, dass Apple (und seine Partner) diese Daten nur in dem von Ihnen erlaubten Ausmaß für eigene Zwecke nutzen.

Auf der Habenseite besteht allerdings der Vorteil, dass Sie - wann auch immer, von wo auch immer - schnell auf Ihre Daten zugreifen können. Nutzen Sie mehr als ein iOS-Gerät, wird Ihr kostenloser iCloud-Speicher vermutlich zu klein werden. In diesem Fall sollten Sie überlegen, ob nicht eine (kostenpflichtige) Erweiterung Ihres Speichers sinnvoll ist.

„Einstellungen“ ► „iCloud“ ► „Backup“ ► „iCloud-Backup: ein“

Sollten Sie sich jedoch entschlossen haben, die iCloud nicht zu aktivieren, kann alternativ auch ein **lokales Backup mit iTunes** durchgeführt werden. Welche Variante Sie wählen, ist letztendlich Ihre persönliche Entscheidung.

Bundesamt für Verfassungsschutz und Terrorismusbekämpfung
Cyber Security Center