Bundesministerium
Inneres

Mobile Sicherheit

Handlungsempfehlungen und präventive Maßnahmen für die sichere Nutzung von mobilen Endgeräten

Mobile Sicherheit

Handlungsempfehlungen und präventive Maßnahmen
für die sichere Nutzung von mobilen Endgeräten

Wien, 2023

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundesministerium für Inneres
Herrengasse 7, 1010 Wien
bmi.gv.at
Autor(en): Abteilung IV/S/2 – Netz- und Informationssystemsicherheit
Fachbereich Prävention
Coverbild: Adobe Stock
Druck: Digitalprintcenter des BMI

Vollständige Neuausgabe
Wien, November 2023

Rückmeldungen: Ihre Überlegungen zu vorliegender Publikation übermitteln Sie an praevention@nis.gv.at.

Vorwort

Mobile Endgeräte haben im Laufe der vergangenen beiden Jahrzehnte unser Leben verändert, sie sind unverzichtbarer Bestandteil unseres Alltags geworden. Für viele Menschen ist heute das Smartphone das zentrale, mitunter sogar einzige private IKT-Endgerät, das sie täglich nutzen. So wird ein modernes Smartphone heute nicht bloß zur Sprachkommunikation genutzt, sondern es sind ungleich mehr Dienste und Funktionen auf diesen Geräten vereint. Die Liste entsprechender Anwendungen ist scheinbar endlos und umfasst unter anderem:

- Kommunikationsdienste (z.B. SMS, MMS, E-Mail, Messenger)
- Internetdienste (z.B. Websurfing, Soziale Medien)
- Finanz-Anwendungen (z.B. Online-Banking, Zahlungsdienste, Online-Shopping)
- Verwaltungsdienste (z.B. Behördenwege, elektronische Ausweise)
- Standortbasierende Dienste (z.B. Ortungsdienste, Karten- oder Navigationsdienste)
- Multimedia-Anwendungen (Kamerafunktionen, Medienkonsum, Spiele)
- Büroanwendungen (z.B. Erstellung und Bearbeitung von Dokumenten)
- Neue Technologien (z.B. Bild- und Texterkennung, Übersetzungsdienste, Künstliche Intelligenz, Augmented Reality)

Dabei vergessen viele jedoch, dass all dies auch Gefahren birgt. Durch die enorme Konzentration von Funktionen, Diensten und vor allem Daten in den mobilen Endgeräten, stellen diese ein höchst attraktives Angriffsziel dar. Die Absichten und Motivationen von potenziellen Angreifern sind dabei ebenso vielfältig wie die von ihnen eingesetzten Angriffsvektoren. Unbestreitbar ist, dass erfolgreiche Angriffe auf Mobiltelefone heute tagtägliche Realität sind und die Schadensszenarien und -summen stetig zunehmen. Doch auch legaler Datenhunger mancher Anwendungen kann für Betroffene unangenehme Folgen haben.

Dabei kann schon die Beachtung einiger grundlegender Handlungsempfehlungen die Sicherheit Ihres mobilen Endgerätes und die Vertraulichkeit und Integrität Ihrer persönlichen Daten nachhaltig erhöhen. Wie so oft stehen aber auch in diesem Bereich Komfort und Sicherheit in einem permanenten Spannungsverhältnis. Ein Mehr an Sicherheit für Ihr Gerät und Ihre Daten kann auf der anderen Seite bedeuten, dass einige durchaus praktische Funktionen nur mehr eingeschränkt oder gar nicht mehr zur Verfügung stehen. Letztlich liegt es an Ihnen, den für Sie bestmöglichen Kompromiss zwischen Funktion, Komfort, Sicherheit und Privatsphäre zu finden.

Die vorliegende Broschüre möchte Ihnen dabei helfen.

Inhalt

1 Gerätesicherheit

Der erste Abschnitt beschreibt Maßnahmen zur Sicherstellung einer allgemeinen Gerätesicherheit. Der Fokus liegt hier auf dem Betriebssystem sowie auf grundlegenden Funktionalitäten des Endgeräts. Die folgenden Punkte bilden die Basis für ein umfassendes Sicherheitskonzept.

1.1 Betriebssystem

Ein **Betriebssystem** ist die grundlegende Software, die für die Nutzung der meisten heutigen elektronischen Geräte wie Desktop-, Notebook- und Tablet-Computer oder Smartphones zwingend erforderlich ist. Das Betriebssystem stellt dabei die Schnittstelle zwischen der verwendeten physischen Hardware und den Anwendungsprogrammen (Apps) dar. Es erfüllt wesentliche Aufgaben wie die Ansteuerung der Ein- und Ausgabegeräte oder die Verwaltung des Speichers. Die meisten Funktionen des Betriebssystems finden im Hintergrund statt und sind für Anwenderinnen und Anwender nicht unmittelbar sichtbar.

Der Teil des Betriebssystems, den Anwenderinnen und Anwender tatsächlich sehen und benutzen können, wird **Benutzeroberfläche** genannt. Diese ist erforderlich, um beispielsweise Anwendungsprogramme zu installieren und grundlegende Funktionen des elektronischen Gerätes zu steuern. Betriebssysteme können entweder eine grafische Oberfläche (Graphical User Interface – GUI) oder eine Kommandozeilen-Oberfläche aufweisen. Es gibt, abhängig vom verwendeten Gerät, eine Vielzahl von Betriebssystemen. Für Computer gehören Microsoft Windows, macOS oder Linux zu den bekanntesten Produkten, im Bereich der mobilen Kommunikation wären an erster Stelle Android oder iOS zu nennen.

Keine Software ist frei von Fehlern. Jedes Programm, sei es ein Betriebssystem oder eine App, weist aufgrund der hohen Komplexität heutiger Software Fehler auf. In der Regel führen solche Fehler dazu, dass verschiedene Funktionen zu inkorrekten Ergebnissen führen. Einige Programmfehler können jedoch von Angreifern dazu missbraucht werden, das Gerät mit Schad- oder Spionagesoftware (Malware) zu infizieren. Weist die Software derartige Fehler auf, so spricht man von **Sicherheitslücken (Vulnerabilities)**.

Erlangt ein Hersteller Kenntnis von Sicherheitslücken in seiner Software, so wird er in der Regel bestrebt sein, die zugrundeliegenden Fehler schnellstmöglich durch sein Team beheben zu lassen. In einem zweiten Schritt muss er die bereinigte Version der Software auf die Geräte der Anwenderinnen und Anwender übermitteln. Dies geschieht in Form

sogenannter **Sicherheits-Updates (Patches)**. Diese werden den Anwenderinnen und Anwendern der Software in der Regel möglichst zeitnah zur Verfügung gestellt.

Es liegt in der Verantwortung der Anwenderinnen und Anwender, zur Verfügung gestellte Sicherheits-Updates **zeitnah zu installieren**, im Bestfall unmittelbar nach einer entsprechenden Information, beispielsweise durch eine Nachricht in der Informationszeile des Mobilgerätes. Wird ein Sicherheits-Update installiert, wird die zugehörige Sicherheitslücke geschlossen und das Gerät ist durch Angriffe unter Ausnutzung dieser bestimmten Vulnerability nicht mehr gefährdet. Unterbleibt die Installation oder findet diese verzögert statt, steht das Gerät entsprechenden Angriffen weitgehend ungeschützt gegenüber.

Zuletzt muss beachtet werden, dass eine bestimmte **Hardware nicht für unbestimmte Zeit mit Betriebssystem-Updates unterstützt** wird. Sowohl bei Android als auch bei iOS behalten sich die Hersteller vor, Hardware ab einem bestimmten Alter nicht mehr mit Sicherheits-Updates zu versorgen. Wenn ein Gerät dieses Stadium erreicht hat, ist es empfehlenswert, die Anschaffung eines zeitgemäßen Gerätes zu überlegen. Dies erscheint insbesondere deshalb wichtig, da auf diesem Gerät bekannt gewordene Sicherheitslücken nicht mehr behoben werden und das Gerät entsprechenden Angriffen schutzlos gegenübersteht.

Wir empfehlen:
Sie sollten Sicherheits-Updates, die vom Hersteller Ihres Betriebssystems zur Verfügung gestellt werden, so zeitnah wie möglich auf Ihrem Mobilgerät installieren. Dies kann manuell oder durch die Nutzung einer automatischen Updatefunktion sichergestellt werden.

1.2 Rooten & Jailbreak

Wird ein Gerät mit Schadsoftware infiziert, verfügt diese in der Regel über dieselben Rechte wie die angemeldete Anwenderin bzw. der angemeldete Anwender. Je mehr Rechte für Menschen zur Verfügung stehen, desto mehr Rechte stehen auch der Schadsoftware zur Verfügung. Gängige Betriebssysteme für Mobilgeräte wie Android oder iOS schränken unter anderem auch aus diesem Grund die Funktionalität des Betriebssystems für Anwenderinnen und Anwender mehr (iOS) oder weniger (Android) ein. Die Idee hinter dieser Maßnahme ist, dass Menschen nur die Funktionen zur Verfügung stehen, die diese im Normalfall auch benötigen. Dies dient primär dem **Schutz des Mobilgeräts** vor potenziellem Schaden.

Es gibt jedoch Menschen, die sich aus verschiedenen Gründen nicht mit dieser zwangsweisen Einschränkung abfinden wollen. Sie streben an, alle Funktionen des Betriebssystems uneingeschränkt nutzen zu können. Da dies nicht mit regulären Mitteln zu erzielen ist, werden dafür von den Herstellern nicht freigegebene, unautorisierte Software-Werkzeuge benutzt. Im Fall von Android spricht man vom „**Rooten**“ des Mobilgeräts, bei iOS wird dafür ein Werkzeug namens „**Jailbreak**“ genutzt. Beiden Werkzeugen ist gemein, dass sie den Anwenderinnen und Anwendern uneingeschränkte Rechte auf dem betroffenen Gerät einräumen. Zu den Vorteilen zählt im Falle von iOS beispielsweise die Möglichkeit, vom Hersteller nicht freigegebene Apps zu installieren, die ansonsten nicht genutzt werden könnten.

All das erscheint jedoch nur im ersten Moment von Vorteil. Zwar haben Anwenderinnen und Anwender nun vollen Zugriff auf alle Funktionen, nur handelt es sich einerseits bei diesen Funktionen meist um solche, die man bei normaler Nutzung sowieso nicht benötigt, und andererseits hat nun auch etwaige Schadsoftware dieselben uneingeschränkten Rechte. Dies ermöglicht es der Schadsoftware im Anlassfall, einen **weitaus größeren Schaden** anzurichten, als dies im Normalfall der Fall wäre. Ein weiterer Aspekt ist, dass nach der Nutzung dieser unautorisierten Software-Werkzeuge etwaige Garantieansprüche gegen den Hersteller erlöschen.

Wir empfehlen:
Sie sollten auf eine Installation von nicht autorisierten Software-Werkzeugen zur Erlangung vollständiger Rechte auf Mobilgeräten („Rooten“ bei Android bzw. „Jailbreak“ bei iOS) unbedingt verzichten.

1.3 Vollverschlüsselung

Das Mobilgerät ist heute für viele Menschen die **digitale Manifestation ihrer Identität**. In vielen Fällen sind praktisch alle digitalen Daten einer Anwenderin oder eines Anwenders auf dem Mobilgerät gespeichert. Dabei handelt es sich in der Regel um Dokumente, Bilder, E-Mail-Nachrichten, Messenger-Daten, Kontaktdaten oder Zugänge zu sozialen Medien. Es ist daher erforderlich, diese Daten bestmöglich zu schützen. Um die auf einem Mobilgerät gespeicherten Daten umfassend zu schützen, genügt es nicht, einen starken Zugriffsschutz (PIN-Code, Passphrase, Biometrie) zu aktivieren.

Es ist zusätzlich empfehlenswert, den gesamten Datenspeicher im Gerät vollständig zu verschlüsseln. Man spricht hier von **Vollverschlüsselung**. In der Anfangszeit der mobilen Kommunikation stand diese Funktionalität gar nicht, nicht standardmäßig oder nur in

eingeschränktem Ausmaß zur Verfügung. Mittlerweile wenden die gängigen Betriebssysteme (Android und iOS) diese standardmäßig an.

Bei der Vollverschlüsselung wird der interne Datenspeicher **kryptographisch verschlüsselt**. Als Schlüssel zur Ver- und Entschlüsselung dienen dabei ein anzugebendes Kennwort oder biometrische Daten (z.B. Fingerabdruck, Gesichtsscan). Geht ein vollverschlüsseltes Gerät verloren oder wird ein solches gestohlen, hat der Finder bzw. Dieb im Regelfall keine Möglichkeit, die enthaltenen Daten zu lesen oder zu manipulieren.

Wir empfehlen:
Abhängig von Ihrem Betriebssystem sollten Sie sicherstellen, dass der interne Datenspeicher Ihres Mobilgerätes vollverschlüsselt und die enthaltenen Daten damit auch bei Verlust- oder Diebstahl vor unrechtmäßigem Zugriff geschützt sind.

1.4 Virenschutz und Firewall

Virenschutz-Programme schützen elektronische Geräte wie Desktop-, Notebook- und Tablet-Computer sowie Smartphones vor Schadsoftware. Entsprechende Programme überwachen dabei permanent das jeweilige Gerät und untersuchen potenziell gefährliche Dateien oder Aktivitäten. Wird eine Bedrohung erkannt, wird diese im Bestfall blockiert, bevor es zu einem Schaden am Gerät kommen kann. Darüber hinaus bieten manche Virenschutz-Programme sinnvolle Zusatzfunktionen, wie URL-Checker, die Links zu Webseiten vor der Ausführung auf etwaige Sicherheitsrisiken überprüfen, oder Konfigurations-Checker, welche die aktuellen Sicherheitseinstellungen auf dem Smartphone überprüfen.

Firewall-Programme überwachen den ein- und ausgehenden Datenverkehr eines elektronischen Geräts. Computer und Mobilgeräte kommunizieren mit der Außenwelt über eine Vielzahl an sogenannten Ports. Ein Firewall-Programm schließt in einem ersten Schritt alle Ports und öffnet diese in der Folge nur für Datenverkehr, der von Anwenderinnen und Anwendern oder deren legitimen Apps freigegeben wurde. Potenziell gefährliche Daten werden von der Firewall im Bestfall am Port abgewiesen und gelangen somit nicht auf das Gerät.

Virenschutz- und Firewall-Programme gehören inzwischen zur Standardausstattung jedes Computers. Ob diese Programme auf Mobiltelefonen sinnvoll oder überflüssig sind, ist Gegenstand kontrovers geführter Debatten. In diesem Zusammenhang müssen die beiden gängigen Betriebssysteme getrennt voneinander betrachtet werden.

Auf **iOS-Mobiltelefonen** ist kein dediziertes Programm für Virenschutz enthalten, es ist aber eine Firewall bereits ins Betriebssystem integriert. Darüber hinaus werden Maßnahmen gesetzt, die Anwenderinnen und Anwendern zusätzlichen Schutz bieten. Dazu gehört ein besonders strenges Prüfverfahren bei der Veröffentlichung von Apps (App Store Review).

In **Android-Mobiltelefonen** sind keine dedizierten Programme für Virenschutz- und Firewall-Funktionalitäten enthalten. Statt einer vollwertigen Firewall bietet Android allerdings Funktionen zur Steuerung des Internetzugriffs von Apps an. Zum Schutz der Anwenderinnen und Anwender wurde zusätzlich die Funktion Google Play Protect eingeführt, die Apps beim Herunterladen aus dem Google Play Store vor der Installation automatisch auf einen möglichen Befall mit Schadsoftware überprüft.

Beide Betriebssysteme verwenden darüber hinaus in ihren aktuellen Versionen das sogenannte **Sandboxing-Verfahren**, bei dem Apps jeweils in einem abgekapselten Speicherbereich ausgeführt werden, um eine etwaige Ausbreitung von Schadsoftware zu verhindern.

Bei der Auswahl geeigneter Virenschutz- und Firewall-Programme sollte unbedingt bedacht werden, dass diese Anwendungen auf allen Ebenen unter Umständen maximalen Zugriff auf das jeweilige Mobilgerät benötigen. Da auch diese Programme Fehler aufweisen können, bieten sie somit eine **besonders effektive Angriffsfläche** für potenzielle Angreifer. Daher ist es gerade in diesem Bereich entscheidend, bei der Auswahl des Produkts größtmögliche Sorgfalt walten zu lassen und das Programm nur von den herstellereigenen Plattformen zu beziehen sowie die Software permanent am aktuellen Stand zu halten.

Weiters muss beachtet werden, dass die Installation mancher Firewall-Programme nur auf Geräten möglich ist, auf denen zuvor nicht autorisierte Software-Werkzeuge zur Erlangung vollständiger Rechte („Rooten“ bei Android bzw. „Jailbreak“ bei iOS) ausgeführt wurden. Das Gefahrenpotenzial, das durch eine solche Vorgangsweise entsteht, ist größer als der erzielbare Mehrwert einer Firewall. Aus diesem Grund sollte auf den Einsatz solcher Programme generell verzichtet werden.

Wir empfehlen:

- Die Betriebssysteme Android und iOS haben in ihren aktuellen Versionen bereits konkrete Funktionen zum Schutz Ihres Mobilgerätes implementiert. Trotzdem sollten Sie zusätzlich geeignete Virenschutz- und Firewall-Programme auf Ihren Geräten installieren.

- Auf Programme, die zuvor den Einsatz nicht autorisierter Software-Werkzeuge zur Erlangung vollständiger Rechte („Rooten“ bei Android bzw. „Jailbreak“ bei iOS) erfordern, sollten Sie in jedem Fall verzichten.

1.5 Backups

Auch wenn sich Anwenderinnen und Anwender intensiv um den Schutz und den sicheren Betrieb ihrer elektronischen Geräte bemühen, kann **niemals ausgeschlossen werden, dass es zu einem Datenverlust kommt**. Dies kann einerseits durch eine Infektion mit Schadsoftware, aber andererseits auch durch physikalische Einflüsse wie Herunterfallen, Eindringen von Wasser oder Brand geschehen. Um wertvolle, möglicherweise nicht reproduzierbare Daten wie Bilder, Kontaktdaten oder persönliche Dokumente in solchen Situationen nicht zu verlieren, ist es entscheidend, regelmäßig Sicherheitskopien – sogenannte Backups – dieser Dateien zu erstellen.

Grundsätzlich stehen für die regelmäßige Herstellung von Sicherheitskopien mehrere Möglichkeiten zur Verfügung. Die komfortabelste Methode ist ein **automatisches Cloud-Backup**. Dabei werden vom Mobilgerät alle gewünschten Daten (zumeist in Kategorien wählbar) einmalig oder regelmäßig in einen Cloudspeicher kopiert bzw. mit diesem synchronisiert. Der entsprechende Speicherplatz im Internet (Cloud) wird dabei vom Hersteller des Mobiltelefons (z.B. Samsung) oder dem Anbieter des Betriebssystems (z.B. Google für Android, Apple für iOS) in der Regel kostenlos zur Verfügung gestellt.

Der **Vorteil eines automatischen Cloudbackups** liegt in der komfortablen Nutzung, die meist nur eine einmalige Aktivierung erfordert, und in der Nutzung von – für die Anwenderin und den Anwender – vollkommen wartungsfreiem Speicherplatz, der eine sehr hohe Datensicherheit aufweist und einen Zugriff von jedem beliebigen Ort aus ermöglicht. Der **Nachteil** ist, dass die gesamten Daten regelmäßig durch das Internet transportiert werden und an einem für die Anwenderin und den Anwender nicht bekannten Ort (oft auch außerhalb der Europäischen Union) gespeichert werden. Der mögliche Zugriff auf diese Daten durch Dritte (z.B. Nachrichtendienste) ist durch Gesetze des Speicherlandes geregelt. Zudem ist zu bedenken, dass – entgegen den Aussagen mancher Betreiber – Daten, sobald sie sich einmal in einer Cloud befinden, nur schwer bzw. in der Praxis möglicherweise gar nicht mehr vollständig aus dem Internet entfernt werden können. Aus diesen Gründen ist es empfehlenswert, die Speicherung von Daten in einer Cloud mit Bedacht durchzuführen.

Dem gegenüber steht ein **lokales Backup** ausgewählter Daten auf einen geeigneten Datenträger. Dabei wird das Mobiltelefon mit einem geeigneten Gerät (z.B. Notebook) verbunden und ausgewählte Daten werden auf ein externes Medium kopiert. Auch dieser

Vorgang kann entweder manuell oder mit Unterstützung geeigneter Apps automatisiert durchgeführt werden.

Der **Vorteil eines lokalen Backups** liegt darin, dass die Anwenderin und der Anwender zu jedem Zeitpunkt die volle Kontrolle über ihre Daten haben, da diese zu keinem Zeitpunkt in oder durch das Internet transportiert oder dort gespeichert werden. Der Nachteil ist, dass die Planung und Durchführung des Backups sowie eine empfohlene Vollverschlüsselung in der Verantwortung der Anwenderinnen und des Anwenders liegen. Auch die gesicherte Verwahrung des externen Datenträgers und der Schutz von zerstörerischen Umwelteinflüssen (z.B. Wasser, Feuer) verbleibt bei ihnen.

Wir empfehlen:
Um im Anlassfall eine Möglichkeit zur Wiederherstellung von verlorengegangenen oder zerstörten Daten zu haben, sollten Sie auf eine regelmäßige Herstellung von Backups achten, nach persönlicher Präferenz entweder in einem Cloudspeicher oder auf einem lokalen Datenträger.

2 Authentisierung und Authentifizierung

Gerade im Mobilbereich ist es von entscheidender Bedeutung, unbefugten Zugriff auf Daten, Dienste und Zugänge, die auf einem mobilen Endgerät gespeichert bzw. mit diesem genutzt werden, zu verhindern. Dieser Abschnitt beschreibt geeignete Möglichkeiten, legitimen Zugang zu einem System zu erlangen.

Dabei muss zwischen folgenden Begriffen unterschieden werden:

- **Authentisierung** bezeichnet das Nachweisen einer bestimmten Identität durch einen Benutzer oder eine Benutzerin.
- **Authentifizierung** bezeichnet die Prüfung der vom Benutzer oder der Benutzerin im Rahmen der Authentisierung behaupteten Identität.
- **Autorisierung** bezeichnet das Gewähren bestimmter Rechte (z.B. Zugang zu System) nach erfolgreich abgeschlossener Authentifizierung.

Zumeist wird in der Alltagssprache, aber vielfach auch in der Fachliteratur auf diese Differenzierung verzichtet und der gesamte **Vorgang aus Authentisierung, Authentifizierung und Autorisierung** vereinfacht als Authentifizierung bezeichnet. Zur leichteren Lesbarkeit wird in den nachfolgenden Ausführungen diese Sprachregelung übernommen.

2.1 Kennwortsicherheit

Die Verwendung eines **Kennwortes zur Authentifizierung** gegenüber einem System ist nach wie vor die am häufigsten angewandte Methode, um Zugang zu einem System zu erhalten. Auch im Mobilbereich sind Kennwörter – trotz des Siegeszuges biometrischer Authentifizierungsmethoden – noch immer sehr verbreitet. Aus diesem Grund ist es wichtig, sichere bzw. starke Kennwörter zu verwenden.

Starke Kennwörter zeichnen sich durch das geeignete Zusammenspiel von **Länge und Komplexität** aus. Während die Kennwortlänge die Anzahl der Zeichen eines Kennwortes beschreibt, bedeutet Komplexität in diesem Zusammenhang die Anzahl an möglichen unterschiedlichen Zeichen, aus denen sich das Kennwort zusammensetzen kann (Ziffern, Groß- und Kleinbuchstaben, Sonderzeichen).

Derzeit kann bei den folgenden Kennwortlängen von einer **in der Regel ausreichenden Sicherheit** ausgegangen werden (hundertprozentige Sicherheit kann jedoch auch in diesen Fällen nicht gewährleistet werden):

- Hohe Komplexität (d.h. Verwendung von Ziffern, Groß- und Kleinbuchstaben und Sonderzeichen): **12 Stellen** oder mehr
- Niedrige Komplexität: **16 Stellen** oder mehr

Darüber hinaus sollten im Rahmen der Kennwortsicherheit weitere Empfehlungen berücksichtigt werden:

- **Kennwortaufbewahrung:** Kennwörter sollten stets so aufbewahrt werden, dass unbefugte Dritte keine Möglichkeit haben, diese auszuspähen. Insbesondere das Aufschreiben von Kennwörtern an leicht zugänglichen Orten (z.B. Post-It am Monitor) sollte unbedingt unterbleiben. Eine geeignete Möglichkeit der Speicherung von Kennwörtern ist die Verwendung sogenannter Kennwortmanager (Passwort-Safes).
- **Kennwortweitergabe:** Persönliche Zugangsdaten sollten niemals an Dritte weitergegeben werden. Für bestimmte Situationen des Arbeitsalltags (z.B. Urlaubsvertretungen, IT-Support) ist eine Weitergabe persönlicher Zugangsdaten nicht erforderlich.
- **Unterschiedliche Kennwörter:** Es sollte nach Möglichkeit vermieden werden, gleiche Zugangsdaten für unterschiedliche Zugänge zu verwenden. Optimalerweise sollte jedes Kennwort nur genau für einen Zugang verwendet werden.
- **Berufliche und private Nutzung:** Zugangsdaten aus dem beruflichen Umfeld sollten niemals in einem privaten Konnex verwendet werden und umgekehrt. Auch sollte niemals eine dienstliche E-Mail-Adresse zur Registrierung eines privaten Dienstes genutzt werden und umgekehrt.

2.1.1 Authentifizierung mittels Passkey-Verfahren

Ein neues Konzept zur sicheren Authentifizierung ohne Verwendung klassischer Kennwörter stellt das sogenannte Passkey-Verfahren dar. Dieses wurde von der FIDO Alliance entwickelt, zu der Branchengrößen wie Google, Apple oder Microsoft gehören.

Das Passkey-Verfahren verzichtet auf die Nutzung von Kennwörtern und nutzt stattdessen ein asymmetrisches Verschlüsselungsverfahren. Bei der Registrierung eines Benutzerkontos bei einem Dienst wird ein sogenanntes Schlüsselpaar erstellt. Dieses besteht aus einem geheimen privaten Schlüssel, der ausschließlich dem Anwender bzw. der Anwenderin bekannt ist, und einem öffentlichen Schlüssel, der am Server des Diensteanbieters verbleibt.

Bei einem Anmeldevorgang mittels Passkey-Verfahren weist der Anwender bzw. die Anwenderin dem Diensteanbieter nach, dass er bzw. sie im Besitz des privaten Schlüssels ist und damit berechtigt ist, sich an dem Dienst anzumelden. Das zum Einsatz kommende technische Verfahren erlaubt es, den Besitz des privaten Schlüssels nachzuweisen, ohne diesen an den Diensteanbieter übermitteln zu müssen.

Das Passkey-Verfahren gilt gegenüber klassischen Kennwörtern als sichereres und komfortableres Anmeldeverfahren. Insbesondere besteht eine hohe Resilienz gegenüber typischen und verbreiteten Angriffsarten wie Phishing.

Wir empfehlen:

- Verwenden Sie ausschließlich starke Kennwörter. Je nach Komplexität empfehlen wir eine Länge zwischen 12 und 16 Stellen.
- Darüber hinaus sollten Sie Ihre Kennwörter stets sicher verwahren und niemals an Dritte weitergeben.
- Auch sollten Sie danach trachten, nach Möglichkeit für jeden Zugang ein individuelles Kennwort zu nutzen.
- Verwenden Sie statt klassischen Kennwörtern das Passkey-Verfahren, wenn der jeweilige Diensteanbieter dies anbietet.

2.2 Mehr-Faktor-Authentifizierung

Die Mehr-Faktor-Authentifizierung (oder auch Multi-Faktor-Authentifizierung) ist eine Möglichkeit, **die Sicherheit bei Anmeldevorgängen stark zu erhöhen**. Grundsätzlich kann eine Authentifizierung auf drei verschiedenen, sogenannten Faktoren beruhen:

- **Etwas, das ich weiß („Wissen“):** Die Identität des Benutzers oder der Benutzerin wird durch etwas nachgewiesen, das diese Person weiß (z.B. Kennwörter, Pin-Code)
- **Etwas, das ich habe („Besitz“):** Die Identität des Benutzers oder der Benutzerin wird durch einen physischen Gegenstand nachgewiesen, der sich im Besitz der Person befindet (z.B. registriertes Smartphone, Token-Generator, Keycard)
- **Etwas, das ich bin („Inhärenz“):** Die Identität des Benutzers oder der Benutzerin wird durch ein biometrisches Merkmal der Person nachgewiesen (z.B. Fingerabdruck, Gesichtserkennung, Iris-Scan)

In manchen Publikationen wird auch ein vierter Faktor angeführt, der jedoch im Cyber-Bereich von nachgeordneter Bedeutung ist:

- Der Ort, an dem ich mich aufhalte („Ort“): Die Identität des Benutzers oder der Benutzerin wird dadurch nachgewiesen, dass sich die Person an einem bestimmten Ort aufhält

Wenn für einen einzelnen Authentifizierungsvorgang **Daten aus zumindest zwei unterschiedlichen Faktoren** nachgewiesen werden müssen, spricht man von einer Mehr- (oder Multi-) Faktor-Authentifizierung. Ein sehr verbreitetes Beispiel für eine Mehr-Faktor-Authentifizierung ist die Behebung von Bargeld am Geldausgabeautomaten. Hier wird sowohl die physische Präsenz einer entsprechenden Bankkarte („Besitz“) als auch das Wissen um den zugehörigen Pin-Code („Wissen“) benötigt, um die Behebung durchzuführen.

Der einzig nennenswerte **Nachteil** der Mehr-Faktor-Authentifizierung ist der zusätzliche Aufwand für Benutzerinnen und Benutzer, wobei dieser im Hinblick auf die erhöhte Sicherheit unbedingt in Kauf genommen werden sollte.

2.2.1 mTAN/smsTAN-Verfahren

Eine nach wie vor weit verbreitete Methode der Mehr-Faktor-Authentifizierung ist das besonders im Bereich des Online-Bankings genutzte **mTAN-Verfahren**. Dabei ist es erforderlich, zuerst Zugangsdaten (Benutzername/Verfügernummer und Kennwort) einzugeben und danach eine Transaktion mit einem TAN-Code zu bestätigen. Dieser TAN-Code wird für jede Transaktion individuell mittels SMS auf ein zuvor registriertes Mobiltelefon übermittelt. Ohne das Vorhandensein des physischen Gegenstandes (Mobiltelefon mit passender SIM-Karte) wäre also die Durchführung einer Transaktion nicht möglich.

Lange Zeit galt dieses Verfahren als geeigneter Kompromiss aus Bedienungsfreundlichkeit und Sicherheit. Mittlerweile wurde jedoch eine Reihe von Fällen bekannt, in denen dieses Verfahren erfolgreich durch Angreifer umgangen werden konnte. Aus diesem Grund gilt das mTAN/smsTAN-Verfahren heute nicht mehr als ausreichend sicher und wird zunehmend durch verbesserte Verfahren ersetzt (z.B. Authenticator Apps).

Wir empfehlen:
Die Mehr-Faktor-Authentifizierung sollte immer angewandt werden, wenn seitens des jeweiligen Diensteanbieters diese Möglichkeit zur Verfügung gestellt wird. Dies ist bei einer großen Anzahl von Diensten möglich, es ist jedoch zu beachten, dass die Mehr-Faktor-Authentifizierung in der Regel bei jedem Dienst manuell aktiviert werden muss.

2.3 Biometrie

In den vergangenen Jahren hat im Mobilbereich die Nutzung der Biometrie zur Authentifizierung einen enormen Aufschwung genommen. Im Bereich der Biometrie werden unterschiedlichste Messungen am Benutzer oder der Benutzerin dazu verwendet, die Identität dieser Person gegenüber einem System nachzuweisen. Dabei kann grob zwischen folgenden Bereichen unterschieden werden:

- **Biologische Merkmale** (z.B. Fingerabdruck-Scan, Gesichtserkennung, Handvenen-Scan, Iris- oder Retina-Scan)
- **Verhaltensbiometrie** (z.B. Tipp-Dynamik, Touchscreen-Nutzung)

Aufgrund der jeweiligen **Einzigartigkeit biologischer und verhaltensbasierter Eigenschaften** kann mittels Biometrie im Rahmen eines Authentifizierungsvorganges der Nachweis einer Identität erbracht werden. Die Verwendung dieser Methode bietet für die Benutzerinnen und Benutzer ein Höchstmaß an Komfort, da eine schnelle und einfache Authentifizierung ermöglicht wird.

Durch die stetig besser werdenden Hard- und Softwarekomponenten wurde die **Sicherheit und Zuverlässigkeit** bei dieser Authentifizierungsmethode im Lauf der Zeit stark verbessert. Die erfassten biometrischen Merkmale werden durch Algorithmen in hochkomplexe Daten umgerechnet und gespeichert, die dann zur Authentifizierung verwendet werden. Durch diese hohe Komplexität und die scheinbare Zufälligkeit der Daten werden Angriffe durch Erraten nahezu unmöglich gemacht.

Trotzdem kann auch die Möglichkeit der Kompromittierung biometrischer Daten niemals ausgeschlossen werden. Ein **Nachteil** im Vergleich zur Verwendung von Kennwörtern be-steht darin, dass biometrische Merkmale des Benutzers oder der Benutzerin trotz einer etwaigen Kompromittierung nicht geändert werden können. Daher sollte diese Form der Authentifizierung stets mit Bedacht und ausschließlich bei vertrauenswürdigen Geräten und Diensten eingesetzt werden.

Bei den meisten mobilen Geräten können im Zusammenhang mit der biometrischen Authentifizierung **Daten mehrerer Personen** abgespeichert werden. Sollte ein Benutzer oder eine Benutzerin einem oder einer Dritten auf Basis biometrischer Daten (z.B. Fingerprint, Gesichtsscan) Zugriff zum Gerät gewähren, muss unbedingt beachtet werden, dass diese nicht bloß für die Entsperrung des Endgeräts verwendet werden können, sondern dass diese in der Regel auch Zugriff auf alle biometrisch gesicherten Funktionen und Dienste auf diesem Gerät ermöglichen (z.B. Online-Banking, Behördendienste).

Wir empfehlen:

- Verwenden Sie die Möglichkeit der biometrischen Authentifizierung ausschließlich bei vertrauenswürdigen Geräten und Diensten.
- Gewähren Sie niemals einem Dritten biometrischen Zugang auf Ihr Endgerät.

2.4 Kennwortmanager

Kennwortmanager (Password-Safes) bieten die Möglichkeit, **persönliche Zugangsdaten sicher zu verwahren**. Dabei handelt es sich um kleine Datenbanken, die es Benutzerinnen und Benutzern ermöglichen, die Zugangsdaten und URLs aller Nutzerkonten an einem Ort zentral abzuspeichern. Um die Sicherheit der Vertraulichkeit der Daten sicherzustellen, werden die Daten mit komplexen Algorithmen verschlüsselt und der Zugang mit einem sogenannten Master-Kennwort (oder geeigneten biometrischen Authentifizierungsmethoden) gesichert.

Benötigt eine Benutzerin oder ein Benutzer Zugangsdaten eines bestimmten Dienstes, kann er durch Eingabe des Master-Kennworts auf die Datenbank zugreifen und die benötigten Daten durch **Kopieren und Einfügen (copy/paste) in die jeweilige Eingabemaske** übertragen. Es besteht meist auch die Möglichkeit, die Datenbank so zu konfigurieren, dass dieser Vorgang nach Eingabe des Master-Kennworts automatisch durchgeführt wird.

Durch den Einsatz komplexer Verschlüsselungsalgorithmen ist es – ein ausreichend starkes Master-Kennwort vorausgesetzt – für Angreifer sehr schwierig bzw. praktisch nahezu unmöglich, an die gespeicherten Daten zu gelangen. Es ist jedoch zu bedenken, dass beim Einsatz von Kennwort-Managern der sogenannte **Schatztruhen-Effekt** zum Tragen kommt. Sollte das Master-Kennwort kompromittiert werden, erhält der Angreifer Zugriff zu den Zugangsdaten aller Konten der Benutzerin oder des Benutzers. Daher sollte besonderes Augenmerk auf die folgenden Punkte gelegt werden:

- **Verwendung eines sicheren und vertrauenswürdigen Passwort-Managers:** Es wird empfohlen, ausschließlich Kennwort-Manager zu verwenden, bei denen die Verschlüsselung direkt am eigenen Endgerät durchgeführt wird.
- **Einsatz eines ausreichend starken Master-Kennworts** (bzw. einer sicheren biometrischen Authentifizierungs-Methode): Von der Sicherheit des Master-Kennworts hängt die Sicherheit *aller* Zugangsdaten ab.

Neben einer Vielzahl von speziell für diesen Zweck hergestellten Apps, bieten die Betriebssysteme Android und iOS entsprechende Funktionalitäten an:

iOS-Geräte bieten die Möglichkeit, persönliche Zugangsdaten samt der zugehörigen URLs zu speichern. Werden solcherart gespeicherte Zugangsdaten benötigt, wird automatisch eine Schaltfläche eingeblendet, bei deren Betätigung die Zugangsdaten nach einer erfolgreichen biometrischen Authentifizierung automatisch ausgefüllt werden. Weiters überprüft iOS regelmäßig, ob gespeicherte Zugangsdaten (beispielsweise durch einen Kennwort-Leak) kompromittiert wurden oder einzelne Kennwörter bei zu vielen eigenen Konten verwendet werden.

Da **Android-Geräte** mit einem Google-Konto verknüpft sind, kann das eigene Google-Konto zur Speicherung beliebiger Zugangsdaten verwendet werden. Dazu ist es erforderlich, dass die Synchronisierung des Chrome-Browsers am Android-Endgerät mit dem eigenen Google-Konto aktiviert ist. Um auf die Zugangsdaten zuzugreifen, muss das Endgerät aktiv mit dem Google-Konto verbunden sein. Weiters besteht die Möglichkeit eines automatischen Anmeldens an beliebigen Diensten. Im Gegensatz zu iOS gibt es bei Android derzeit keine integrierte Funktion, um etwaige kompromittierte Zugangsdaten anzuzeigen.

Wir empfehlen:

- Verwenden Sie einen Kennwortmanager, um ihre persönlichen Zugangsdaten sicher und an einem einzigen Ort zu speichern.
- Achten Sie dabei unbedingt darauf, einen vertrauenswürdigen Kennwortmanager zu verwenden und nutzen Sie stets ein sicheres Master-Kennwort bzw. eine sichere biometrische Authentifizierungs-Methode.

3 Schutz vor unbefugter Nutzung

Mobilgeräte sind heute für viele Menschen der wichtigste, oft sogar einzige Speicherort für digitale Daten aller Art. Das bedeutet, dass praktisch alle digitalen Daten einer Anwenderin oder eines Anwenders, beispielsweise Dokumente, Bilder oder Kontaktdaten, auf dem Mobilgerät gespeichert sind.

Deshalb ist es wichtig, das Mobilgerät gegen unbefugte Nutzung durch Dritte zu schützen. Ebenso wichtig ist, die unbefugte Nutzung der mobilen Dienste eines Endgeräts (z.B. Telefonie, SMS, mobile Daten) durch Dritte zu verhindern. Entsprechende **Schutzmaßnahmen können auf mehreren Ebenen** aktiviert werden.

3.1 SIM-Sperre

Eine SIM-Sperre wirkt auf der **Ebene der SIM-Karte**. Mit dieser Maßnahme werden *nicht* das Mobilgerät und die darauf gespeicherten Daten gegen unbefugte Nutzung geschützt, sondern lediglich verhindert, dass Unbefugte die mobilen Dienste, die mit der SIM-Karte verknüpft sind (z.B. Telefonie, SMS, mobile Daten), nutzen können.

Eine Aktivierung schützt Anwenderinnen und Anwender daher vor **monetären Schäden** durch unberechtigte Nutzung der Telefonie- und Datendienste sowie vor einem möglichen **Identitätsdiebstahl** durch unrechtmäßige Nutzung der ausgehenden Rufnummer.

Diese Schutzmaßnahme ist **geräteunabhängig**. Wird die entsprechende SIM-Karte in ein Mobilgerät eingelegt und dieses eingeschaltet, erfolgt eine Abfrage des SIM-Codes (PIN). Wird dieser korrekt eingegeben, wird die Nutzung der mobilen Dienste auf diesem Gerät zugelassen. Hat eine Person keine Kenntnis über den SIM-Code, kann die betreffende SIM-Karte in *keinem* Mobiltelefon genutzt werden.

Eine SIM-Sperre arbeitet unabhängig von bzw. zusätzlich zu einer Anmeldung beim Betriebssystem (iOS oder Android) bzw. einer etwaigen aktivierten Bildschirmsperre.

Je nach Netzbetreiber ist die verpflichtende Eingabe eines SIM-Codes nach dem Einschalten des Mobilgerätes mit eingelegter SIM-Karte erforderlich oder auch nicht. Die Notwendigkeit der Eingabe kann durch den Anwender oder die Anwenderin **jederzeit aktiviert oder deaktiviert werden**.

Unabhängig von der Schutzwirkung einer aktivierten SIM-Sperre ist es sinnvoll, **im Fall von Verlust oder Diebstahl** des Mobilgeräts (mit eingelegter SIM-Karte), den jeweiligen Netzbetreiber zu kontaktieren und eine vollständige Sperre/Deaktivierung der SIM-Karte zu veranlassen.

Wir empfehlen:
Verwenden Sie bei ihren mobilen Endgeräten (mit eingelegter SIM-Karte) die Möglichkeit einer SIM-Sperre. Sofern diese bei ihrem Netzbetreiber nicht von vornherein aktiviert ist, aktivieren sie diese umgehend.

3.2 Bildschirmsperre

Die Verwendung einer angemessenen Bildschirmsperre ist ein einfacher Weg, ein mobiles Endgerät und die darauf gespeicherten Daten vor unbefugter Nutzung durch Dritte zu schützen. Im Unterschied zur SIM-Sperre wirkt die Bildschirmsperre auf **Ebene des Endgeräts**, ist also unabhängig von der eingelegten SIM-Karte wirksam.

Die Bildschirmsperre soll verhindern, dass

- unbefugte Personen, die physischen Zugriff auf das mobile Endgerät haben, Zugriff auf die gespeicherten Daten haben,
- unbefugte Personen, die physischen Zugriff auf die USB-Schnittstelle des mobilen Endgeräts haben, sich mit diesem verbinden können (z.B. zur Übertragung von Daten),
- unbefugte Personen, die physischen Zugriff auf das mobile Endgerät haben, die mobilen Dienste, die mit der eingelegten SIM-Karte verknüpft sind, *mit diesem Endgerät* nutzen können.

Es ist zu beachten, dass eine Bildschirmsperre nur dann vollständigen Schutz bietet, wenn das **Endgerät vollverschlüsselt** ist.

Eine Bildschirmsperre kann je nach verwendetem Endgerät und eingesetztem Betriebssystem bzw. installierter Betriebssystemversion durch verschiedene Entsperrmechanismen aufgehoben werden. Diese weisen unterschiedliche Sicherheitsniveaus auf:

- Wischgeste (keine Sicherheit)
- Entsperrmuster oder Klopfmuster (praktisch keine Sicherheit)
- PIN-Code (je nach Länge geringe bis mittlere Sicherheit)
- Passphrase (je nach Länge geringe bis hohe Sicherheit)

- Fingerabdruck (je nach Alter der Hardware geringe bis hohe Sicherheit)
- Gesichtserkennung (je nach Alter der Hardware geringe bis hohe Sicherheit)

Im Zusammenhang mit der Nutzung von Fingerabdruck- bzw. Gesichtserkennungs-Hardware ist zu beachten, dass das **Sicherheitsniveau stark vom Alter der eingesetzten Hardware** abhängig ist. Konnte beispielsweise Gesichtserkennungs-Hardware der ersten Generation problemlos mit einem Foto der betreffenden Person überlistet werden, weisen aktuelle Modelle eine sehr hohe Sicherheit auf.

Je nach eingesetztem Betriebssystem bzw. installierter Betriebssystemversion besteht die Möglichkeit, nach einer bestimmten **Anzahl an Fehlversuchen** automatisch den Zugriff auf das Endgerät vollständig zu unterbinden oder das Endgerät unwiderruflich zu löschen. Diese Funktionen sollten mit Vorsicht genutzt werden, auch legitime Anwender und Anwenderinnen können Daten im letzteren Fall nicht mehr wiederherstellen.

Wir empfehlen:
Verwenden Sie stets eine Bildschirmsperre mit hohem Sicherheitsniveau und achten Sie darauf, dass diese immer aktiv ist, wenn Sie das Endgerät nicht benutzen.

3.3 Sperrbildschirm-Benachrichtigungen

Sperrbildschirm-Benachrichtigungen sind eine Funktion, die es Anwenderinnen und Anwendern erlaubt, die Tatsache und/oder den Inhalt von Benachrichtigungen aller Art anzuzeigen, **ohne dass zuvor die Bildschirmsperre aufgehoben werden muss**. Dies steigert den Bedienungskomfort, ermöglicht es aber unter Umständen unbefugten Dritten, vertrauliche Informationen zu sehen, ohne dass sie Kenntnis über die Bildschirmsperre haben müssen.

Je nach eingesetztem Betriebssystem bzw. installierter Betriebssystemversion können diese sogenannten **Sperrbildschirm-Benachrichtigungen** aktiviert oder deaktiviert werden, oder es besteht die Möglichkeit, diese feingranular freizugeben bzw. zu verbieten. Beispielsweise kann:

- nur die Tatsache von Benachrichtigungen,
- die Tatsache und die erste Zeile des Inhalts von Benachrichtigungen,
- die Tatsache und der vollständige Inhalt von Benachrichtigungen bzw.
- die Tatsache und/oder der Inhalt von Benachrichtigungen nur bestimmter Apps

auf dem Sperrbildschirm angezeigt werden.

Es obliegt den Anwenderinnen und Anwendern im Einsatzfall, die Kritikalität von Benachrichtigungen zu bewerten und das Endgerät entsprechend zu konfigurieren. Dienstliche Endgeräte, die vertrauliche Daten des Arbeitgebers enthalten, sollten so konfiguriert werden, dass weder Tatsache noch Inhalt einer Benachrichtigung ohne Aufhebung der Bildschirmsperre sichtbar sind.

Wir empfehlen:
Deaktivieren Sie insbesondere auf dienstlichen Endgeräten die Anzeige sowohl von Tatsache als auch von Inhalt aller Benachrichtigungen auf dem Sperrbildschirm.

3.4 Sprachassistenten deaktivieren

Sprachassistenten sind Dialogsysteme, die **gesprochene Befehle von Anwenderinnen und Anwendern** entgegennehmen, um die Bedienung verschiedener Funktionen zu vereinfachen. Mit Hilfe von Natural Language Processing verarbeiten elektronische Assistenten die gesprochenen Anweisungen und führen diese aus.

Mit solchen Sprachbefehlen können verschiedene Funktionen bedient werden, es besteht aber auch die Möglichkeit, Inhalte von Nachrichten abzufragen. Durch die Verwendung von sogenannten Text-to-Speech-Technologien ist es auch möglich, sich Informationen vorlesen zu lassen. Somit können große Teile der Funktionalität eines Mobilgerätes durch Sprache genutzt werden.

Werden diese Sprachassistenten aktiviert, lauschen diese permanent, ob ein definiertes Signalwort (**„Hey Siri“** bei iOS bzw. **„Okay Google“** bei Android) ausgesprochen wird, interpretieren die von Anwenderinnen und Anwendern nachfolgend gesprochenen Worte als Befehl und versuchen diesen auszuführen.

Die Nutzung von Sprachassistenten erhöht zwar den Bedienungskomfort, birgt aber auch **erhebliche Risiken**:

- Die Nutzung von Sprachassistenten ist technisch nur möglich, wenn das Mikrofon permanent aktiviert ist. Das bedeutet, dass alle Gespräche im Umkreis des Mobilgerätes permanent mitgehört und entsprechend interpretiert werden.
- Die Auswertung der Sprachbefehle erfolgt nicht am Endgerät, sondern auf Servern des jeweiligen Anbieters (Apple bzw. Google). Das bedeutet, dass Sprach-

informationen über das Internet an den Anbieter übermittelt und dort gespeichert werden. Dies ist besonders in Anwendungsfällen kritisch, in denen sensible Informationen mittels Sprachbefehl eingegeben werden.

- Anbieter erklären, dass Sprachinformation erst nach der Erkennung des Signalworts an die jeweiligen Server übermittelt werden. Dies kann nicht unabhängig überprüft werden.
- Wie lange Sprachinformationen auf den Servern der Anbieter gespeichert und zu welchen anderen Zwecken diese verwendet werden (z.B. Marketingmaßnahmen), ist in der Datenschutzerklärung festgelegt, deren Inhalt den wenigsten Anwenderinnen und Anwendern bekannt ist.
- Laute und diffuse Umgebungsgeräusche können zu einer vermeintlichen Erkennung des Signalwortes führen. Da dies Anwenderinnen und Anwendern zu diesem Zeitpunkt nicht bewusst ist, können auch vertrauliche Gespräche unbeabsichtigt zum Anbieter übermittelt werden.

Insbesondere in Fällen, in denen die Konfiguration des Endgeräts die Möglichkeit bietet, **Sprachassistenten auch bei gesperrtem Bildschirm** verwenden zu können, besteht ein erhebliches Gefahrenpotential, da diese von Dritten ohne Authentifizierung genutzt werden können.

Wir empfehlen:
Deaktivieren Sie Sprachassistenten, wenn Sie diese nicht zwingend benötigen. Unterbinden Sie jedenfalls die Nutzung von Sprachassistenten bei gesperrtem Bildschirm.

4 App-Sicherheit

Das Betriebssystem ist nicht die einzige Softwarekomponente, die auf mobilen Endgeräten zu finden ist. Schon bei der Auslieferung eines Gerätes ist zusätzlich zum Betriebssystem eine Vielzahl weiterer Programme (hier Apps genannt) vorinstalliert. Darüber hinaus steht Anwenderinnen und Anwendern eine praktisch unbegrenzte Auswahl weiterer Apps zum Download zur Verfügung.

4.1 Sichere Quellen

Grundsätzlich stellt jedes lauffähige Programm, das auf einem Mobilgerät installiert wird, eine potenzielle Gefahr für die Sicherheit des Endgeräts dar, da Anwender und Anwenderinnen nicht wissen können, ob die jeweilige App frei von schädlichem oder bösartigem Code ist.

Um das Risiko für Anwenderinnen und Anwender so weit als möglich zu minimieren, haben die beiden großen Anbieter (Google bzw. Apple) für mobile Endgeräte, die ihr jeweils hauseigenes Betriebssystem (Android bzw. iOS) verwenden, **besonders geschützte Plattformen** aufgebaut, die sie ihren Nutzerinnen und Nutzern zur Verfügung stellen:

Google bietet für sein Betriebssystem Android alle verfügbaren Apps im Google Play Store an. Diese Plattform ist durch den Mechanismus Google Play Protect geschützt, der unbedingt aktiviert sein sollte. Google Play Protect arbeitet auf zwei Ebenen:

- Wird im Google Play Store eine App zum Download markiert, wird diese auf potenziell schädlichen Inhalt überprüft, bevor sie auf dem Endgerät installiert wird.
- Unabhängig davon prüft Google Play Protect regelmäßig die bereits auf dem Endgerät installierten Apps auf schädlichen Inhalt.

Je nach Konfiguration werden potenziell schädliche Apps automatisch deaktiviert bzw. deinstalliert oder die Nutzerinnen und Nutzer werden über die Gefahr lediglich informiert und zur Deinstallation aufgefordert.

Apple bietet für sein Betriebssystem iOS alle verfügbaren Apps im Apple App Store an. Auch Apple hat Schutzmechanismen auf mehreren Ebenen implementiert, um sicherzustellen, dass alle verfügbaren Apps frei von potenziell schädlichen Codes sind. Eine Besonderheit bei iOS ist, dass die Installation von Apps technisch ausschließlich über den Apple App Store möglich ist.

Wir empfehlen:

- Installieren Sie Apps ausschließlich über die Plattformen Google Play Store bzw. Apple App Store. Vermeiden Sie unbedingt die Installation von Apps aus anderen Quellen (.apk-Dateien bei Android).
- Stellen Sie sicher, dass alle zur Verfügung stehenden Schutzmechanismen (z.B. Google Play Protect) aktiviert sind.

4.2 Berechtigungen

Je nach eingesetztem Betriebssystem bzw. installierter Betriebssystemversion werden Anwenderinnen und Anwender entweder bei der Installation oder dem ersten Start einer neuen App um die **Genehmigung bestimmter Berechtigungen** gebeten. Dazu zählen unter anderem:

- Anrufe tätigen
- SMS versenden
- Standort verwenden
- Kamera verwenden
- Mikrofon verwenden

Nutzerinnen und Nutzer haben in diesen Fällen die Möglichkeit, die jeweilige Berechtigung **einmalig oder permanent** zu vergeben. Eine permanent vergebene Berechtigung bleibt für alle künftigen Aufrufe der jeweiligen App aufrecht.

Anwenderinnen und Anwender müssen davon ausgehen, dass eine App, die eine bestimmte Berechtigung einfordert, diese – sofern sie gewährt wird – auch nutzen wird. Die meisten nachgefragten Berechtigungen sind **für die ordnungsgemäße Funktion einer App auch erforderlich** (z.B. benötigt eine App, die Spracheingabe zulässt, zwingend die Be-rechtigung zur Nutzung des Mikrofons). Solche Berechtigungen müssen gewährt werden, sofern die entsprechende App genutzt werden soll.

Apps fordern auch immer wieder Berechtigungen ein, die **für die ordnungsgemäße Funktion der App nicht erforderlich** sind. Diese Berechtigungen werden zumeist dazu verwendet, Daten über die Nutzerinnen und Nutzer zu sammeln (z.B. Nutzungsverhalten, Bewegungsprofile) und diese zu Marketingzwecken zu verwenden oder an Dritte weiter zu verkaufen. Solche Berechtigungen sollten nach Möglichkeit verweigert werden.

Es obliegt den Anwenderinnen und Anwendern einzuschätzen, ob die angepriesenen Funktionalitäten einer App und die von ihr eingeforderten Berechtigungen in einem plau-

siblen Zusammenhang stehen. Ist ein solcher Zusammenhang nicht herstellbar, sollten die betreffenden Berechtigungen entweder verweigert oder die App deinstalliert werden.

Wir empfehlen:

- Vergeben Sie Berechtigungen mit Sorgfalt.
- Ist bei einer App ein sinnvoller Zusammenhang zwischen angepriesener Funktionalität und eingeforderten Berechtigungen nicht ersichtlich, verweigern Sie die entsprechenden Berechtigungen oder deinstallieren Sie die App.

4.3 Aktualisierungen

Keine Software ist frei von Fehlern. Dies gilt in besonderem Maße auch für Apps, die im Unterschied zu den großen Anbietern mitunter auch von kleinen, wenig professionellen Teams erstellt werden. Die Hersteller von Apps bieten in unregelmäßigen Abständen **Aktualisierungen für ihre jeweiligen Apps** an. Diese dienen in erster Linie dazu, entdeckte Fehler und daraus resultierende Sicherheitslücken zu beseitigen.

Aktualisierungen enthalten zumeist Sicherheits- und Stabilitätsverbesserungen, mitunter sind auch Funktionserweiterungen enthalten. Was genau durch eine bestimmte Aktualisierung geändert wird, ist in der Regel aus der Beschreibung in den Stores ersichtlich. Alternativ kann auch aus der jeweiligen Änderung der Versionsnummer auf die Art bzw. den Umfang der Aktualisierung rückgeschlossen werden.

Ausgangsversion	Aktualisierte Version	Änderungen
4.0.0	5.0.0	Wesentliche Funktionen und Fehlerbehebungen
5.0.0	5.1.0	Kleinere Funktionen und Fehlerbehebungen
5.1.0	5.1.1	Fehlerbehebungen

Um größtmögliche Sicherheit für Mobilgeräte sicherzustellen, sollten angebotene Sicherheitsupdates möglichst zeitnah installiert werden. Die Installation von Aktualisierungen für Apps sollte dabei aber **ausschließlich über die Plattformen Google Play Store bzw. App Store** erfolgen. Vermeintliche „Sicherheitsupdates“, wie sie immer wieder in sozialen Medien kursieren, stellen sich oft als Schadsoftware heraus.

Um alle Apps so zeitnah wie möglich mit Sicherheitsupdates zu versorgen, sollten **automatische Aktualisierungen** aktiviert werden. Diese Funktionalität kann direkt im Google Play Store bzw. im App Store aktiviert werden.

Wir empfehlen:

- Installieren Sie Aktualisierungen, die auf den Plattformen Google Play Store bzw. App Store angeboten werden, möglichst zeitnah.
- Um eine schnellstmögliche Versorgung mit Aktualisierungen sicherzustellen, sollten Sie automatische Aktualisierungen aktivieren.

5 Konnektivität

Mobile Endgeräte verfügen über eine hohe Konnektivität, was bedeutet, dass eine große Anzahl an Schnittstellen zur Verfügung steht, über die das Gerät mit seiner Umwelt kommunizieren kann. Während Schnittstellen ein **Mehr an Funktionalität** bieten, können sie jedoch auch für **Angriffe von außen** missbraucht werden.

5.1 Nutzung von Funkschnittstellen

Funkschnittstellen übertragen Daten mithilfe elektromagnetischer Wellen. Moderne mobile Endgeräte verfügen über eine Vielzahl solcher Schnittstellen. Dazu gehören unter anderem:

- Mobile Daten (z.B. EDGE, UMTS, HSPA, LTE, 5G)
- Wireless LAN (WLAN)
- Bluetooth
- Near Field Communication (NFC)

Grundsätzlich bietet jede aktivierte Funkschnittstelle eine **potenzielle Angriffsfläche**. Dies ist insbesondere dann der Fall, wenn die Schnittstelle zwar aktiviert ist, diese aber im Moment nicht benutzt wird. Es ist daher empfehlenswert, Funkschnittstellen **nur bei Bedarf bewusst zu aktivieren** und sie nach der Nutzung wieder zu deaktivieren.

Bei der Nutzung des Betriebssystems iOS ist zu beachten, dass eine Deaktivierung von WLAN über das Kontrollzentrum **nur unvollständig und temporär** möglich ist. Zum einen bleibt das WLAN im Hintergrund für bestimmte Funktionalitäten (z.B. Standortbestimmung) weiterhin aktiv und zum anderen wird die volle WLAN-Funktionalität um 5 Uhr des Folgetages automatisch wieder aktiviert. Wird eine dauerhafte Deaktivierung gewünscht, muss dies über das Einstellungsmenü durchgeführt werden. Dies gilt sinngemäß auch für Bluetooth.

Je nach eingesetztem Betriebssystem bzw. installierter Betriebssystemversion bleiben einmal genutzte **WLAN-Zugangsdaten und Verbindungsinformationen im Endgerät gespeichert**, auch wenn die Verbindung zum entsprechenden WLAN nicht mehr besteht.

Ist WLAN auf einem Endgerät aktiviert, besteht aber im Moment keine aufrechte Verbindung zu einer Gegenstelle, sucht das Gerät aktiv nach gespeicherten Gegenstellen und verbindet sich mit diesen automatisch.

Mit frei im Internet erhältlichen Geräten ist es leicht möglich, sich gegenüber dem Endgerät **als eine bekannte Gegenstelle auszugeben**, wodurch eine automatische Verbindung zwischen dem Mobilgerät und dem Gerät des Angreifers hergestellt wird. Ist dies der Fall, eröffnen sich für Angreifer neue Angriffsmöglichkeiten, beispielsweise kann der Datenverkehr von Nutzerinnen und Nutzer mitgelesen oder manipuliert werden.

Wir empfehlen:
Aktivieren Sie Funkschnittstellen auf Ihrem Mobilgerät (insbesondere WLAN, Bluetooth und NFC) nur bei Bedarf und deaktivieren Sie diese unmittelbar nach erfolgter Nutzung wieder.

5.2 Drahtlose Datenübertragungsdienste

Je nach eingesetztem Betriebssystem bzw. installierter Betriebssystemversion haben Anwenderinnen und Anwender die Möglichkeit, Fotos, Dokumente, Links oder ähnliches drahtlos mit Mobilgeräten in unmittelbarer Nähe zu teilen oder Daten von diesen zu empfangen. iOS bietet in diesem Zusammenhang den **Dienst AirDrop** an, Nutzerinnen und Nutzern von Android steht der **Dienst Nearby Share** zur Verfügung.

Bei den genannten Diensten werden die **Übertragungstechnologien Bluetooth und WLAN** technisch kombiniert. Der Verbindungsaufbau zwischen den Geräten erfolgt in einem ersten Schritt mittels Bluetooth, anschließend werden in einem zweiten Schritt die Daten unter Verwendung einer WLAN-Verbindung übertragen.

Generell gilt auch hier, dass **jede aktivierte Schnittstelle von Angreifern ausgenutzt werden kann**. Dienste können Sicherheitslücken beinhalten, die es Angreifern erlaubt, Daten während der Übermittlung oder auch aus dem Gerätespeicher auszuspähen oder zu exfiltrieren.

Wir empfehlen:
Aktivieren Sie drahtlose Datenübertragungsdienste auf Ihrem Mobilgerät (AirDrop, Nearby Share) nur bei Bedarf und deaktivieren Sie diese unmittelbar nach erfolgter Nutzung wieder.

5.3 Nutzung öffentlicher WLAN-Netzwerke

Es ist heute praktisch zu einer Selbstverständlichkeit geworden, dass Hotels, Restaurants, Flughäfen oder Einkaufszentren ihren Kundinnen und Kunden über **öffentliche WLAN-Netzwerke** Zugang zum Internet anbieten. In der Regel ist den Anbietern dieser Zugänge die individuelle Identität der Nutzerinnen oder Nutzer nicht bekannt. Je nach Konfiguration des Netzwerks erfolgt der drahtlose Zugang entweder

- unverschlüsselt oder
- zwar verschlüsselt, aber nach heutigen Maßstäben unsicher (z.B. WEP, WPA 1), oder
- verschlüsselt (z.B. WPA 2/3).

Verschlüsselte Zugänge sind daran erkennbar, dass für die Anmeldung im Netzwerk ein **Netzwerkschlüssel** erforderlich ist. Dabei kann es sich um einen gleichartigen Schlüssel für alle Kundinnen und Kunden oder (in seltenen Fällen) um individuell generierte Schlüssel handeln. Im Fall eines versuchten Aufbaus einer unverschlüsselten oder einer unsicher verschlüsselten Verbindung kann das mobile Endgerät (je nach Konfiguration) eine entsprechende Warnung ausgeben.

Dabei ist unbedingt zu berücksichtigen, dass die entsprechende **Verschlüsselung ausschließlich auf der Funkstrecke** (d.h. zwischen mobilem Endgerät und dem Zugangspunkt (Access Point, Hotspot) zum Tragen kommt, nicht jedoch entlang der gesamten restlichen Verbindung. Unabhängig davon, ob der Zugang zum WLAN unverschlüsselt oder verschlüsselt erfolgt, bestehen bei der Nutzung von öffentlichen WLAN-Netzwerken **erhebliche Sicherheitsrisiken**.

Da der Zugang zu öffentlichen WLAN-Netzwerken in der Regel anonym möglich ist, werden solche Netze oft zu Angriffen auf Nutzerinnen oder Nutzer verwendet. Befindet sich ein Angreifer im selben Netzwerk wie eine Anwenderin oder ein Anwender, stehen diesem **effektivere Angriffsmöglichkeiten** zur Verfügung. Bei einem sogenannten „Man-in-the-Middle"-Angriff klinkt sich beispielsweise ein Angreifer, der sich im selben WLAN-Netzwerk befindet, in den Datenstrom zwischen einem mobilen Endgerät und dessen beabsichtigter Gegenstelle ein und kann so den Datenverkehr (z.B. auch Kennwörter oder Kreditkartennummern) von Nutzerinnen und Nutzer mitlesen oder manipulieren.

Es ist daher empfehlenswert, bei der Nutzung von öffentlichen WLAN-Netzwerken **alle zur Verfügung stehenden Verschlüsselungsmöglichkeiten** zu nutzen. Dazu zählen unter anderem:

- **Verschlüsseltes Websurfing** durch Nutzung von SSL/TLS-Verbindungen (erkennbar an der Zeichenfolge https:// in der Adresszeile)
- **Verschlüsselter Mailabruf** (kann im jeweiligen E-Mail-Programm aktiviert werden)
- **Verschlüsselte Kommunikation** mit anderen Netzwerken (z.B. Firmennetzwerk) durch eine verschlüsselte VPN-Verbindung (Virtual Private Network)

Sollte zu einem beliebigen Zeitpunkt während des Verbindungsaufbaus zu einem öffentlichen WLAN-Netzwerk eine Warnmeldung erscheinen, die auf **Probleme mit einem Zertifikat** hinweist, so sollte zur Sicherheit der Verbindungsaufbau sofort abgebrochen werden und dieses WLAN bis auf weiteres nicht genutzt werden. Solche Warnmeldungen können zwar auch auf weitgehend harmlose Konfigurationsprobleme des Netzwerkes hinweisen, allerdings besteht eine hohe Wahrscheinlichkeit, dass ein **laufender Angriffsversuch** eine solche Warnmeldung hervorruft.

Wir empfehlen:
Vergegenwärtigen Sie sich, dass Sie bei der Nutzung öffentlicher WLAN-Netzwerke einem erheblichen Sicherheitsrisiko ausgesetzt sind und nutzen Sie solche nach Möglichkeit nicht für sensible Aktivitäten.

Ist eine Nutzung eines öffentlichen WLAN-Netzwerks unumgänglich, verwenden Sie alle zur Verfügung stehenden Verschlüsselungsmöglichkeiten.

Sollte während des Verbindungsaufbaus zu einem öffentlichen WLAN-Netzwerk eine Warnmeldung erscheinen, die auf Probleme mit einem Zertifikat hinweist, so sollte der Verbindungsaufbau sofort abgebrochen werden.

5.4 Nutzung eines VPN

Bei einem **Virtual Private Network (VPN)** handelt es sich um die Anbindung eines mobilen Endgeräts an ein entfernt liegendes Netzwerk (z.B. Firmennetzwerk). Für die Anbindung wird ein verschlüsselter Kanal („Tunnel“) durch ein bestehendes Kommunikationsnetz (z.B. öffentliches Internet) verwendet. Aufgrund des verschlüsselten Zugangs ist die Verbindung vor Spionage- oder Manipulationsangriffen geschützt.

Für den Anwender oder die Anwenderin am mobilen Endgerät verhält sich diese Konfiguration so, als wäre das Endgerät direkt an das Firmennetzwerk angebunden. Es ist beispielsweise möglich, die **Netzlaufwerke oder internen elektronischen Dienste des Unternehmens sicher zu nutzen**, obwohl man sich nicht physisch im Firmennetzwerk befindet. Die Einrichtung eines solchen VPN kann nicht durch den Anwender oder die

Anwenderin allein, sondern nur gemeinsam mit der IT-Fachabteilung des Unternehmens eingerichtet werden.

Diese Nutzungsart von Virtual Private Networks ist insbesondere im Zusammenhang mit **Homeoffice-Lösungen** von essenzieller Bedeutung. Die Nutzung eines Homeoffice-Arbeitsplatzes sollte stets nur auf Basis eines VPN-Zugangs erfolgen.

Ein weiterer Anwendungszweck eines Virtual Private Networks ist, den **Ursprung einer Internetverbindung zu verschleiern**. Surft ein Anwender oder eine Anwenderin im Internet, ist der Ursprung dieser Verbindung (IP-Adresse) in der Regel für das Ziel erkennbar. Gleichzeitig kann das Ziel den Ursprung einem Herkunftsland zuordnen und damit beispielsweise die angebotenen Inhalte oder Dienste aufgrund der geografischen Position der Anwender einschränken.

Um den eigenen Ursprung zu verschleiern, können Anwenderinnen und Anwender eine **VPN-Dienstleistung kommerzieller Anbieter** in Anspruch nehmen. Nutzt man einen diesbezüglichen Dienst, erscheint beim Ziel der Verbindung der Anbieter des VPN als Ursprung. Die IP-Adresse der Anwender und deren geografische Position bleibt gegenüber dem Ziel verborgen. Bei vielen Anbietern ist es sogar möglich, bei jeder Nutzung individuell festzulegen, welches Herkunftsland dem Ziel der Verbindung präsentiert wird. Damit wird es möglich, Dienste und Inhalte zu konsumieren, die auf bestimmte geografische Gebiete eingeschränkt sind.

Nachteil einer solchen Nutzung eines Virtual Private Networks ist einerseits eine in der Regel **reduzierte Verbindungsgeschwindigkeit**, andererseits darf nicht vergessen werden, dass der Ursprung der Verbindung (und damit die Anwenderin oder der Anwender) zwar gegenüber dem Ziel der Verbindung verschleiert wird, der Anbieter des VPN allerdings über alle diesbezüglichen Daten verfügt. Nutzerinnen und Nutzer sind daher gezwungen, auf die Seriosität und Vertrauenswürdigkeit des Anbieters zu vertrauen.

Kostenlose VPN-Anbieter finanzieren sich über Werbung, es werden jedoch oft auch die Daten der Nutzerinnen und Nutzer (im Rahmen der jeweiligen Datenschutzrichtlinie) **aufgezeichnet, ausgewertet und verkauft**. Unseriöse Anbieter tun dies mitunter auch ohne entsprechende Rechtsgrundlage, wodurch sensible oder personenbezogene Daten kompromittiert werden können. Sowohl bei kommerziellen als auch kostenlosen VPN-Anbietern kann **keine vollständige Anonymität** sichergestellt werden.

Virtual Private Networks sind beispielsweise für Personen essenziell, die in deren Heimatländern aus politischen oder anderen Gründen nicht (oder nur eingeschränkt) auf die Inhalte des World Wide Webs (WWW) zugreifen können. In vielen Diktaturen und autokratischen Jurisdiktionen ist die Nutzung eines VPN zur Umgehung solcher Einschränkungen unter Strafe gestellt.

Wir empfehlen:

- Verwenden Sie in Absprache mit der IT-Fachabteilung Ihres Unternehmens bei der Verbindung eines mobilen Endgeräts mit dem Unternehmens-Netzwerk stets einen VPN-Zugang.
- Achten Sie bei der Nutzung eines Virtual Private Networks zur Verschleierung Ihres Ursprungs stets auf die rechtlichen Rahmenbedingungen sowie auf die Seriosität und Vertrauenswürdigkeit des Anbieters.

5.5 Konnektivität bei USB

USB (Universal Serial Bus) ist eine **physische Schnittstelle**, die im Zusammenhang mit mobilen Endgeräten zur Datenübertragung oder zum Laden des Geräte-Akkus Verwendung findet. Die USB-Schnittstelle kommt in einer Reihe verschiedener Generationen und Bauformen zur Anwendung. Allen gemein ist die Tatsache, dass ein und derselbe physische Stecker gleichzeitig für eine Daten- und eine Stromverbindung genutzt werden kann. Dies kann zu Problemen führen.

Es ist heute üblich geworden, dass in öffentlichen Verkehrsmitteln, auf Flughäfen, in Einkaufszentren oder bei Großveranstaltungen **USB-Strom-Ladestationen** zur Verfügung gestellt werden. Oft ist es für Anwenderinnen und Anwender nicht ersichtlich, wer hinter diesem Angebot steckt und wie vertrauenswürdig der Anbieter ist. Wird die Ladestation genutzt, können die Anwender nicht sicherstellen, dass nicht zur selben Zeit über Datenleitungen ein Angriffsversuch auf das mobile Gerät durchgeführt wird.

Eine Möglichkeit, dieses Angriffsszenario auszuschließen, ist die Verwendung von sogenannten **„USB-Condoms“** (Datenblocker) bei der Nutzung von USB-Strom-Ladestationen. Dabei handelt es sich um kostengünstige, kleine Zwischenstecker, die zwischen das Mobilgerät und die Ladestation gesteckt werden. Im Inneren dieses Zwischensteckers sind die beiden Datenleitungen physikalisch durchtrennt, lediglich die Stromleitungen sind verbunden.

Wir empfehlen:

- Grundsätzlich sollte zum Laden eines mobilen Endgerätes stets ein eigenes Netzgerät verwendet werden. Vermeiden Sie für den Ladevorgang nach Möglichkeit die Nutzung fremder USB-Anschlüsse.
- Verwenden Sie bei Ladevorgängen an fremden USB-Anschlüssen oder öffentlichen USB-Strom-Ladestationen nach Möglichkeit immer ein „USB-Condom“.

6 Datenschutz

Sowohl bei persönlichen Daten als auch bei Daten des Arbeitgebers handelt es sich um ein wertvolles Gut, das bestmöglich vor dem Zugriff Dritter geschützt werden sollten, **unabhängig davon, ob dieser rechtlich zulässig ist oder nicht.**

6.1 Daten löschen

Wenn man sich von einem mobilen Endgerät endgültig trennt, ist es unumgänglich, alle Daten, die auf diesem Gerät gespeichert sind, zu löschen. Dabei muss beachtet werden, dass unter gewissen Rahmenbedingungen **Daten auch nach einer vermeintlichen Löschung noch am Gerät** erhalten bleiben können, obwohl es oberflächlich so aussieht, als wären diese vollständig gelöscht. Es besteht die Möglichkeit, unzureichend gelöschte Daten mit einfachen Mitteln wiederherzustellen.

Sowohl bei der Verwendung von Android als auch bei iOS muss das Mobilgerät zwar nicht zwingend mit einem entsprechenden Konto des Anbieters (Google bzw. Apple) verknüpft werden, widrigenfalls sind allerdings die Funktionen des Gerätes massiv eingeschränkt.

Die Nutzung eines Kontos ermöglicht in der Regel auch den Zugriff auf **persönlichen Speicherplatz in einem Clouddienst** des Anbieters. Je nach eingesetztem Betriebssystem bzw. installierter Betriebssystemversion wird dieser Speicherplatz mitunter automatisch zur Datensicherung des Endgeräts und/oder zur Speicherung sonstiger Daten verwendet. Es ist zu beachten, dass bei einer reinen Löschung der Daten am Endgerät (ohne Rücksetzung auf Werkseinstellungen), die **Verknüpfung des Geräts mit dem Konto erhalten bleibt** und künftige Besitzer des Gerätes somit Zugriff auf die Daten im Clouddienst erhalten können.

Bei einer endgültigen Weitergabe ist es daher empfehlenswert, das **Gerät vollständig zu löschen und auf die sogenannten Werkseinstellungen zurückzusetzen**. Dabei muss unbedingt berücksichtigt werden, dass ein Zurücksetzen auf Werkseinstellungen nur dann einen ausreichenden Schutz vor Wiederherstellung der Daten bietet, wenn das Gerät zuvor mit einem starken Kennwort oder einem biometrischen Schlüssel vollverschlüsselt war.

Zuletzt darf nicht vergessen werden, dass die Löschung oder Rücksetzung eines Mobilgerätes **nicht zwingend Einfluss auf Daten hat, die im Clouddienst gespeichert sind**. Jedes Endgerät, dass künftig mit einem bestehenden Konto verknüpft wird, kann damit Zugriff auf die dort gespeicherten Daten erlangen.

Wir empfehlen:

- Stellen Sie bei der Weitergabe eines mobilen Endgeräts sicher, dass alle gespeicherten Daten gelöscht werden und das Gerät auf die Werkseinstellungen zurückgesetzt wird.
- Beachten Sie, dass die Löschung bzw. Zurücksetzung eines Mobilgerätes per se keinen Einfluss auf die Daten in einem verknüpften Clouddienst hat und diese dort in der Regel erhalten bleiben.

6.2 Ad-Tracking

Ad-Tracking ist ein Verfahren, mit dem Werbetreibende und andere Unternehmen **das Online-Verhalten von Anwenderinnen und Anwendern aufzeichnen und analysieren**. Das Ziel solcher Unternehmen ist, diesen Anwenderinnen und Anwendern personalisierte, möglichst perfekt auf sie abgestimmte Werbebotschaften zu übermitteln oder möglichst passende Waren und Dienstleistungen anzubieten. Je besser Werbebotschaften und Angebote auf eine bestimmte Person abgestimmt sind, desto höher ist die Wahrscheinlichkeit, dass es zu einem erfolgreichen Geschäft kommt.

Ad-Tracking zeichnet eine **Vielzahl von unterschiedlichen Verhaltensweisen** auf. Diese reichen von der Analyse der Klick-Verhaltens oder des Scroll-Verhaltens bis hin zur Messung der Zeit, wie lange welches Werbevideo auf einer Streaming-Plattformen angesehen wurde. Die Hilfsmittel, die für die Aufzeichnung verwendet werden, umfassen unter anderem:

- (Werbe-)Cookies
- URL-Tracker
- Tracking-Pixel

Nutzerprofile, die durch Ad-Tracking entstehen, können **sehr umfangreich und detailliert** sein. Dazu kommt, dass auf diese Weise erhobene Daten auch zwischen Unternehmen und Dienstleistern gehandelt werden. Durch die Verknüpfung verschiedener Datenbestände steigt die Genauigkeit und Granularität des Nutzerprofils weiter an.

Je nach eingesetztem Betriebssystem bzw. installierter Betriebssystemversion besteht die Möglichkeit, entsprechende **Funktionalitäten auf dem mobilen Endgerät einzuschränken oder ganz zu deaktivieren**. Dazu ist anzumerken, dass durch die Deaktivierung dieser Funktionalitäten die Menge angezeigter Werbung nicht reduziert wird, sondern nur eine etwaige Individualisierung bzw. Personalisierung.

Wir empfehlen:

- Machen Sie sich bewusst, wie durch Ad-Tracking Ihr Nutzungsverhalten, Ihre Interessen und Ihre Vorlieben aufgezeichnet, analysiert und weiterverarbeitet werden und welche Intentionen dahinterstehen. Entscheiden Sie dann, ob Sie diese Art der Datensammlung wünschen oder nicht.
- Deaktivieren Sie gegebenenfalls die entsprechenden Funktionalitäten auf Ihrem mobilen Endgerät.

6.3 Cloud-Synchronisierung

Sowohl bei einer Verwendung von Android als auch bei iOS ermöglicht das jeweilige Benutzerkonto in der Regel auch einen Zugriff auf persönlichen Speicherplatz in einem Clouddienst des Anbieters. Je nach eingesetztem Betriebssystem bzw. installierter Betriebssystemversion besteht die Möglichkeit, bestimmte oder alle Daten, die auf dem lokalen Gerät gespeichert sind, **automatisch mit dem Clouddienst zu synchronisieren.**

Eine aktivierte Cloud-Synchronisierung bietet Anwenderinnen und Anwendern eine **Reihe von Vorteilen**:

- **Datensicherheit:** Die synchronisierten Daten im Clouddienst stehen auch bei Verlust, Diebstahl oder Defekt des Endgeräts weiterhin zur Verfügung. Bei einem Clouddienst handelt es sich um die Nutzung von für Anwenderinnen und Anwender wartungsfreiem Speicherplatz, der eine sehr hohe Datensicherheit aufweist.
- **Zugriff:** Der Zugriff auf die Daten ist nicht auf ein einzelnes Endgerät beschränkt. Vielmehr können Daten von jedem Ort bzw. von jedem Endgerät aus abgerufen werden, das mit dem entsprechenden Konto verknüpft ist.
- **Entlastung des Endgeräts:** Je nach eingesetztem Betriebssystem bzw. installierter Betriebssystemversion bestehen Möglichkeiten, automatisiert den Speicherplatz am Endgerät zu entlasten (z.B. synchronisierte Fotos werden am Endgerät in der Auflösung reduziert und erst, wenn ein Foto gezielt angewählt wird, wird es durch Download aus der Cloud wieder in hoher Auflösung angezeigt).

Als **Nachteile** müssen angeführt werden, dass die Cloud einen zusätzlichen Angriffsvektor für etwaige Angreifer darstellt, dass Anwenderinnen und Anwender dem Anbieter der Cloud hinsichtlich Datensicherheit bei Speicherung und Übermittlung und Datenschutz vertrauen müssen und dass durch die Synchronisierung erhebliches Datenvolumen beim Internetzugang generiert wird.

iOS (Apple) bietet für die sogenannte iCloud zwei unterschiedliche Sicherheitsniveaus an, einen standardmäßigen und einen erweiterten Datenschutz der Cloudanwendung.

Die Übermittlung von Daten zwischen Endgerät und Cloudspeicher erfolgt in jedem Fall verschlüsselt, der Zugriff auf den Cloudspeicher wird durch Zwei-Faktor-Authentifizierung geschützt. Beim standardmäßigen Datenschutz werden lediglich ausgewählte Dateien (z.B. Kennwörter) verschlüsselt abgespeichert, beim ab iOS 16.2 verfügbaren erweiterten Datenschutz erfolgt eine durchgängige Verschlüsselung aller Daten vom Endgerät über die Übermittlung bis hin zur Speicherung. Lediglich eigene Endgeräte sind in der Lage, in der Cloud abgespeicherte Dateien zu entschlüsseln, auch dem Cloudanbieter ist eine Entschlüsselung in diesem Fall nicht möglich.

Android (Google) bietet die Möglichkeit, die Daten am Endgerät mit dem Clouddienst **Google Drive** zu synchronisieren. Auch hier erfolgt die Übermittlung von Daten zwischen Endgerät und Cloudspeicher immer verschlüsselt, für den Zugriff auf den Cloudspeicher besteht die Möglichkeit einer Zwei-Faktor-Authentifizierung. In der Datenschutzerklärung und den Nutzungsbedingungen wird Google das Recht eingeräumt, mittels automatisierter Algorithmen und Systeme die **hochgeladenen bzw. synchronisierten Inhalte zu scannen**. Laut Google wird dies jedoch nur verwendet, um die Nutzerfreundlichkeit zu erhöhen, sowie Spam und illegale Aktivitäten zu erkennen.

Wir empfehlen:

- Wägen Sie die Vor- und Nachteile einer Cloud-Synchronisierung ab und konfigurieren Sie Ihr Endgerät entsprechend.
- Verwenden Sie für den Zugriff auf Ihren Cloudspeicher stets eine Zwei-Faktor-Authentifizierung.

6.4 Automatisches Ausfüllen

Die Funktion „Automatisches Ausfüllen“ ermöglicht es Anwenderinnen und Anwendern, mit einem Klick, **Web- oder App-Formulare automatisch mit zuvor hinterlegten Daten auszufüllen.** Dieses Verfahren wird oft beim Ausfüllen von Kontaktinformationen, Kreditkarteninformationen, Benutzernamen oder Kennwörtern verwendet.

Die Aktivierung dieser Funktionalität birgt das Risiko, dass Angreifer bei Verlust oder Diebstahl des mobilen Endgeräts leichter Zugriff auf die für das automatische Ausfüllen hinterlegten Daten erhalten können. Dadurch können diese beispielsweise Zugriff auf Kreditkarteninformationen oder Zugangsdaten erhalten und diese missbrauchen. Auch in Fällen, in denen das Endgerät durch Schadsoftware kompromittiert wurde, besteht ein diesbezüglich erhöhtes Risiko.

Eine gängige Angriffsart besteht auch darin, in scheinbar harmlosen Web- oder App-Formularen **versteckte Datenfelder** einzubauen. Diese sind beim Ausfüllen für Anwenderinnen und Anwender nicht sichtbar, ein aktiviertes automatisches Ausfüllen würde allerdings versuchen, diese mit hinterlegten Daten zu befüllen. Für den Fall, dass es sich bei den versteckten Feldern um sensible Datenfelder (z.B. Kreditkarteninformationen) handelt, würden die entsprechenden Daten über das Internet an den jeweiligen Server übermittelt. Somit könnten Angreifer in den Besitz von sensiblen Daten kommen, ohne dass dies den Nutzern bewusst ist.

Je nach eingesetztem Betriebssystem bzw. installierter Betriebssystemversion besteht die Möglichkeit, die Freigabe von hinterlegten Daten durch automatisches Ausfüllen vollständig zu unterbinden oder alternativ im Anlassfall durch einen **zusätzlichen Authentifizierungsvorgang** (z.B. Fingerabdruck) abzusichern.

Wir empfehlen:

- Sofern Sie die Funktionalität „Automatisches Ausfüllen“ nicht benötigen, sollten Sie diese deaktivieren.
- Wenn Sie nicht auf den Komfortgewinn verzichten wollen, aktivieren Sie unbedingt einen zusätzlichen Authentifizierungsvorgang zur Freigabe der hinterlegten Daten.

6.5 Ortungsdienste

Mobile Endgeräte weisen verschiedene Technologien auf, die eine mehr oder weniger genaue **Standortbestimmung (Lokalisierung) des Geräts** ermöglichen. Das Wissen um den momentanen Standort eines Mobilgeräts (und damit auch des jeweiligen Anwenders oder der Anwenderin) ist für die sinnvolle Funktion vieler Apps und Dienste unerlässlich.

Die Funktionalität, den Standort eines Endgeräts zu ermitteln, wird durch sogenannte **Ortungsdienste** erbracht. Diese Dienste nutzen dazu vor allem folgenden Technologien:

- **GNSS:** GNSS (Global Navigation Satellite System) ist der Sammelbegriff für satellitengestützte Systeme zur Positionsbestimmung eines mit dieser Technologie ausgestatteten Geräts (z.B. GPS, Galileo, GLONASS). Solche Systeme nutzen Satelliten, die mit Signalen permanent ihre aktuelle Position und die exakte Uhrzeit ausstrahlen. Aus den Signallaufzeiten können entsprechende Geräte ihre jeweils eigene Position und Geschwindigkeit errechnen. Praktisch alle mobilen Endgeräte weisen heute eine solche Funktionalität auf.

- **WLAN:** Eine weitere Methode zur Standortbestimmung ist WLAN-basierte Ortung. Dabei ermittelt ein mobiles Endgerät die Feldstärke von privaten und/oder kommerziellen WLAN-Signalen sowie die einmaligen (MAC-)Adressen der zugehörigen Zugangspunkte und gleicht diese mit einer Datenbank im Internet ab. Aus diesem Abgleich kann der eigene Standort bestimmt werden.
- **Mobilfunk:** Ortungsdienste können bestimmte Funktionen des Mobilfunknetzes nutzen, um die Standortbestimmung zu erleichtern (z.B. A-GPS).

Viele **Funktionen in Apps und Diensten sind von den Ortungsdiensten abhängig**. Beispielsweise erlauben aktivierte Ortungsdienste, dass die eigene Position in einer Karte eingezeichnet wird, dass basierend auf dem eigenen Standort bestimmte Informationen angezeigt werden oder dass bei der Aufnahme von Fotos die entsprechende Ortsinformation in das Foto eingebettet wird. Eine besondere Funktionalität ist auch das Auffinden eines verlorenen oder gestohlenen Mobilgeräts anhand seiner aktuellen Standortdaten.

Als wesentlicher Nachteil der permanenten Aktivierung von Ortungsdiensten ist anzuführen, dass es Dritten möglich wird, Bewegungsprofile zu erstellen, wodurch Rückschlüsse auf Gewohnheiten, Vorlieben und Beziehungen gezogen werden können. Dies gilt sowohl für berechtigte Dritte (Anbieter), als auch unberechtigte Dritte (Angreifer).

Wir empfehlen:
Aktivieren Sie Ortungsdienste auf Ihrem Mobilgerät nur, wenn Sie Dienste nutzen, die Standortinformationen unbedingt benötigen.

Bundesministerium für Inneres
Herrengasse 7, 1010 Wien
praevention@nis.gv.at
bmi.gv.at