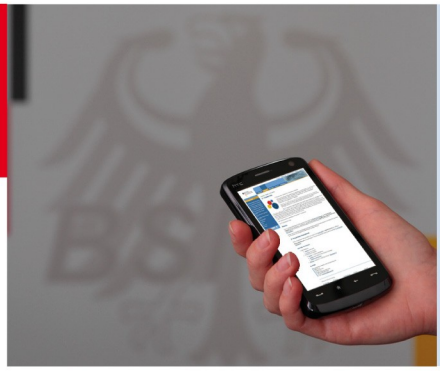
Bundesamt
für Sicherheit in der
Informationstechnik

Überblickspapier

Smartphones



IT-Grundschutz aktuell

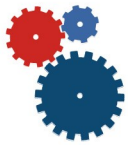
Was sind Smartphones und was können sie?

Smartphones sind Mobiltelefone mit zahlreichen Zusatzfunktionen. Nutzer können mit Smartphones im Internet surfen und Mediadateien wie Podcasts und Videos, beispielsweise von Youtube, abspielen. Smartphones besitzen einen vollständigen E-Mail-Client und können Termine und andere Daten zum Beispiel mit den Servern eines Firmennetzes synchronisieren. Dazu verfügen sie neben der Telefonnetzanbindung über weitere Schnittstellen wie etwa WLAN und Bluetooth. Außerdem sind bei vielen Smartphones bereits im Auslieferungszustand Clients für soziale Netzwerke und Blogdienste integriert. Anders als bei normalen Mobiltelefonen kann der Funktionsumfang von Smartphones nahezu unbegrenzt erweitert werden, da es bei Smartphones genauso einfach wie bei PCs oder Laptops ist, neue Programme zu installieren, die sogenannten Apps. Die Abgrenzung zu einem Laptop besteht hauptsächlich darin, dass ein Smartphone in der Regel mit einer Hand bedient werden kann, über eine kleinere Tastatur und einen kleineren Bildschirm verfügt, sowie weniger Rechenleistung aufweist. Die Speicherkapazitäten von Smartphones liegen aktuell bei 8 bis 16 Gigabyte, wobei viele Modelle mit SD-Cards auf derzeit 32 Gigabyte erweitert werden können. Mit zukünftigen Speicherkartengenerationen sind in absehbarer Zeit wahrscheinlich Kapazitäten bis zu 2 Terabyte möglich.

Gefährdungen

Smartphone-Anbieter müssen auf einem umkämpften Markt bestehen, der permanenten Änderungen unterworfen ist. Auf der Sicherheit der Smartphones oder der Applikationen liegt daher nicht immer die höchste Priorität. Auf der anderen Seite ermöglichen die ständigen wachsenden Funktionalitäten der Smartphones den Benutzern, permanent überall erreichbar zu sein und dabei nicht nur große Datenmengen verarbeiten zu können, sondern auch mobil auf Unternehmens- oder Behördennetze zugreifen zu können. Smartphones sind daher höchst attraktive Angriffsziele. Einige der typischen Gefährdungen sind im Folgenden aufgelistet:

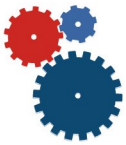
- Smartphones haben ein geringes Gewicht und kleine Abmessungen. Daher sind sie besonders durch physischen Verlust oder Diebstahl gefährdet. Ihr hoher Wiederverkaufswert macht Smartphones für Diebe sehr attraktiv. Es ist auch relativ unwahrscheinlich, verlorene Smartphones zurück zu bekommen.
- Neben dem physischen Verlust, ob Diebstahl oder nicht, ist der damit verbundene Datenverlust eine große Gefährdung. Auf acht Gigabyte lassen sich Projektdaten jeglicher Art (Ausschreibungen, Preiskalkulationen etc.) und E-Mails von vielen Jahren im vollen Umfang speichern. Zum Vergleich: Die gesamten Depeschen aus dem Wikileaks-Cablegate-Fall hätten auf einem Smartphone mehrfach Platz gefunden. Ebenso sind auf Smartphones häufig Zugangsdaten zum Firmennetz, zum privaten E-Mail-Konto, für das Online-Banking oder Ähnliches gespeichert.
- Smartphones besitzen meistens mehrere Schnittstellen wie USB, WLAN und Bluetooth für den Austausch von Daten. Sind diese Schnittstellen unzureichend abgesichert, können Daten darüber entwendet werden.
- Es gibt eine stetig zunehmende Anzahl von Schadsoftware, die auf Smartphones spezialisiert ist. Häufig stehen dahinter ähnliche Ziele wie bei Schadsoftware für den PC, es gibt aber auch einige andere Zielsetzungen dabei:
  - Das Ziel von Schadsoftware könnte sein, infizierte Smartphones zu veranlassen, im Hintergrund Telefonnummern anzuwählen, ohne dass dies der Benutzer sofort merkt. Wenn es sich bei der angerufenen Nummer um einen kostenpflichtigen Telefondienst handelt, kann wirtschaftlicher Schaden für den Besitzer entstehen.



Ferner gibt es Schadsoftware, die Smartphones dazu veranlasst, als Gesprächsvermittler zu arbeiten. Dies ist vergleichbar mit Bots bei PCs, die von einem Botmaster zum Versenden von Spam benutzt werden. Smartphones könnten so für Werbe- oder Betrugsanrufe missbraucht werden.

- Andere Schadsoftware versucht, infizierte Smartphones zu veranlassen, Kurzmitteilungen, beispielsweise mit Links zu verseuchten Internetseiten oder zu Werbung, an Rufnummern zu senden, die im internen Adressbuch gespeichert sind.
- Große Mengen infizierter Smartphones könnten für Überlast-Angriffe (Denial-of-Service) auf Telefonanschlüsse benutzt werden, um bestimmte Nummern, wie von Behörden, Polizei, Rettungsdiensten oder sonstigen Serviceeinrichtungen oder das gesamte Handynetz zu blockieren. Dass solche Angriffe grundsätzlich funktionieren könnten, zeigt sich, wenn zu Neujahr viele Nutzer gleichzeitig Neujahrswünsche über das Mobiltelefon ausrichten wollen.
- Die Liste der möglichen Kompromittierungen des Smartphones durch Schadsoftware ist im Prinzip so lang wie die Liste der möglichen Anwendungen für Smartphones. Schadsoftware könnte beliebige Anwendungen für eigene Zwecke missbrauchen. Eine App eines Sozialen Netzwerks könnte für die Verbreitung von Werbung und Schadsoftware benutzt werden, die App eines Buchladens für den Kauf nicht gewünschter teurer Produkte usw.

- Smartphones sind für Phishing-Angriffe attraktiv, weil sie als E-Mail-Client und zum Einkaufen von Waren und Dienstleistungen sowie zum Bezahlen und zur Identifikation bzw. Authentisierung genutzt werden. Beispielsweise könnten Angreifer versuchen, das beim Online-Banking genutzte mTAN-Verfahren zu unterlaufen.
- Durch allgemeine Programmschnittstellen (APIs) und auch durch die Fähigkeit vieler Smartphones zum Ausführen von Java sind dem Einsatz von Software auf Smartphones nur durch Speicher und Rechenleistung Grenzen gesetzt. Werden diese Programme oder Anwendungen nicht ausreichend geprüft, könnten diese die Sicherheit von Smartphones beeinträchtigen.

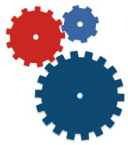


Die meisten Smartphone-Anbieter erlauben nur, zertifizierte Apps aus den eigenen App-Stores zu installieren und auszuführen. Dies wird allerdings immer wieder durch das sogenannte „Jailbreaking“ umgangen. Dadurch werden allerdings auch das Berechtigungsmanagement und andere Sicherheitsmaßnahmen außer Kraft gesetzt. Ein kompromittiertes Smartphone kann leicht zu verdeckten Tonaufnahmen, zum Beispiel von vertraulichen Gesprächen, benutzt werden. Die Mitschnitte können entweder sofort über die Telefonleitung nach außen geschickt oder als Datei gespeichert und später versendet werden.

- Durch die eingeschränkten Bedienungsoptionen von Smartphones gegenüber PCs ist es aufwändiger, URLs von Verkürzungsdiensten aus E-Mails oder Blogs vor dem Öffnen durch einen Webdienst prüfen zu lassen. Über Smartphones wird daher eher als über PCs unbeabsichtigt Schadsoftware aus Internetseiten heruntergeladen, die sich hinter den Kurz-URLs verstecken.
- Ein Angreifer könnte einem Smartphone-Benutzer vorschlagen, ihm ein „interessantes“ Video oder eine „coole App“ zu zeigen. Dazu müsste der Benutzer lediglich einer kurzzeitigen Verbindung mit dem anderen Gerät über Bluetooth zustimmen. Wenn das Video oder die App aber Schadsoftware enthält, wird so das Smartphone des Nutzers kompromittiert.
- Viele Smartphones besitzen einen GPS-Empfänger, über den automatisch Positionsdaten abgerufen, aber auch aufgezeichnet werden können. Diese Lokalisierung kann für ortsgebundene Dienste, aber auch für die Aufzeichnung von Bewegungsprofilen benutzt werden.Smartphones werden unter Umständen verkauft oder weitergegeben, zum Beispiel von einem ausscheidenden Mitarbeiter an dessen Nachfolger, bei einer Reparatur oder beim Wechsel auf ein neueres Modell. Dabei können zahlreiche persönliche Informationen, die auf dem Gerät gespeichert sind, in die Hände von Unbefugten geraten.

Sicherheitsmaßnahmen

Viele der Schadensszenarien aus den oben genannten Gefährdungen können weitreichende Auswirkungen haben, sowohl auf einzelne Personen als auch auf Institutionen, beispielsweise durch Datenabflüsse oder Missbrauch von Benutzerkennungen. Um Schäden vorzubeugen, müssen angemessene Sicherheitsmaßnahmen umgesetzt werden.



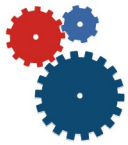
Bei dienstlich genutzten Smartphones sollten Sicherheitseinstellungen, soweit möglich, zentral vorgegeben werden. Trotzdem wird es immer Sicherheitsvorkehrungen geben, die die Benutzer selbst umsetzen müssen. Dabei sollten sich die Verantwortlichen in Unternehmen und Behörden immer darüber im Klaren sein, dass derzeit Smartphones nicht so gut abgesichert werden können wie etwa PCs oder Laptops.

Smartphones können und werden auch häufig außerhalb der Institution im privaten Bereich eingesetzt. Davon kann die Institution profitieren, weil Mitarbeiter jederzeit erreichbar sind. Auf der anderen Seite ergeben sich durch die private Nutzung von Smartphones spezifische Sicherheitsprobleme. Eine Lösung könnte es also sein, die private Nutzung zu untersagen. Dies ist aber in den meisten Fällen nicht praktikabel. Mehr noch: Es besteht die Gefahr, dass technisch versierte Nutzer versuchen, Sicherheitsmaßnahmen zu umgehen, um nicht freigegebene Anwendungen trotzdem zu nutzen. Eine Variante, Sicherheitsmaßnahmen zu umgehen, um beliebige Programme installieren zu können, ist das sogenannte Jailbreaking. Weil dabei praktisch alle Sicherheitsmaßnahmen des Herstellers ausgehebelt werden, muss dies einerseits den Mitarbeitern untersagt werden, aber andererseits sollte die Motivation, Jailbreaking zu nutzen, möglichst gering sein. Vor diesem Hintergrund stellt die Trennung von privater und dienstlicher Nutzung des Smartphones eine große Herausforderung dar.

Um eine angemessene Informationssicherheit beim Einsatz von Smartphones zu erreichen, müssen die Mitarbeiter noch mehr als in anderen Bereichen aktiv eingebunden werden. Daher werden im Folgenden die empfohlenen Sicherheitsmaßnahmen getrennt danach aufgezeigt, was von der Institution und was von den Mitarbeitern umzusetzen ist.

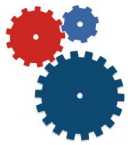
Umzusetzende Sicherheitsmaßnahmen der Institution

Für einen besseren Überblick über die verschiedenen Bereiche, in denen Sicherheitsmaßnahmen ergriffen werden sollten, wurden diese in die Bereiche Planung und Auswahl, Konfiguration und Betrieb kategorisiert.

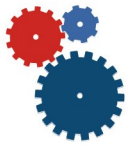


Planung und Auswahl

- Alle Rahmenbedingungen rund um die Smartphone-Nutzung sollten klar geregelt sein, inklusive der Sicherheitsvorgaben. Dazu gehört auch, dass der Einsatz von privaten Smartphones am Arbeitsplatz und im Netz der Institution eindeutig geregelt sein sollte. Umgekehrt sollte die private Nutzung von dienstlichen Smartphones eindeutig geregelt sein. Die Sicherheitsstrategie für Smartphones muss ein integraler Bestandteil der generellen Sicherheitsstrategie der Institution sein und in deren Sicherheitskonzept passen.
- Bereits bei der Entscheidung, welche Smartphones in einer Institution angeschafft und unter welchen Rahmenbedingungen sie eingesetzt werden, sollten Sicherheitsaspekte mit einbezogen werden. Wichtige Punkte, auf die bei der Auswahl geachtet werden sollte, sind:
  - Lassen sich die Smartphones in die existierenden Administrations- und Sicherheitsrichtlinien einbeziehen?
  - Lassen sich die Geräte zentral administrieren?
  - Lassen sich Updates einfach und möglichst zentral einspielen?
  - Lassen sich Datensicherungen zuverlässig und mit möglichst wenig Benutzerinteraktion durchführen?
  - Besitzen die Geräte geeignete Mechanismen zur Identifikation und Authentisierung der Benutzer?
  - Können mit den Smartphones Daten zu anderen Endgeräten verschlüsselt übertragen werden? Können die Geräte die darauf gespeicherten Daten verschlüsseln? Entsprechen die Kryptomechanismen dem Stand der Technik?
  - Können zusätzliche Sicherungsmechanismen genutzt werden?
  - Erlaubt die Produktarchitektur die nachträgliche Installation zusätzlicher Sicherheitsmechanismen (z. B. Verschlüsselungs- oder Virenschutzprogramme)?
- Nicht alle Smartphone-Typen bringen alle gewünschten Sicherheitsmechanismen mit, dann sollte geprüft werden, ob hierfür Zusatzsoftware verfügbar ist, die diese Anforderungen erfüllt.



- Aus Sicherheits- und Administrationssicht wäre es der Idealfall, wenn in der Institution nur ein Smartphone-Typ eingesetzt wird, das den erforderlichen Sicherheitsansprüchen genügt. In der Praxis ist es jedoch häufig so, dass es in einer Institution eine Vielzahl von verschiedenen Smartphone-Typen gibt. Diese weisen viele verschiedene Sicherheitsfunktionen und -möglichkeiten auf. Dann muss es eine komplette Übersicht über alle in der Institution verwendeten Smartphones, inklusive der darauf möglichen Sicherheitsfunktionen geben. Die Nutzung von Smartphones, die die vereinbarten Sicherheitsanforderungen nicht erfüllen, sollte verboten werden.
- Smartphones müssen in die vorhandene IT-Infrastruktur integriert werden. Es muss also geklärt werden, wie die Smartphones an die interne IT angebunden werden, also wie sie beispielsweise an E-Mail-Server gekoppelt und wie sie synchronisiert werden. Hierbei ist unter anderem zu klären, wie die Kommunikation abgesichert werden soll. Eine durchgängige E-Mail-Verschlüsselung ist nicht immer einfach herzustellen.
- Alle Nutzer von Smartphones müssen regelmäßig im geeigneten Umgang mit Smartphones geschult und auf Sicherheitsgefährdungen hin sensibilisiert werden.
- Die Bedienung von Smartphones findet in der Regel nicht unbeobachtet statt. Daher sollte die Institution geeignete Sichtschutzfolien für die Smartphones beschaffen und die Anwender auf deren Gebrauch verpflichten.
- Zum Schutz der Daten bei Verlust bieten viele Smartphones die Möglichkeit, die Nutzerdaten per Fernzugriff vollständig zu löschen. Einige Smartphones verfügen auch über die Möglichkeit, das Smartphone per Fernzugriff zu deaktivieren. Was hier möglich und sinnvoll ist, sollte vorab geklärt werden.
- Alle Verbindungen von Smartphones mit der Institution, um auf Daten wie E-Mails, Kalenderdaten und sonstige Dateien zuzugreifen, sollten verschlüsselt werden. Unverschlüsselte Verbindungen sollten zum Austausch geschäftsrelevanter Daten nicht zugelassen werden. Viele Smartphones unterstützen bereits die Benutzung von TSL/SSL, Public-Key-Infrastrukturen (PKIs) und Virtuellen Privaten Netzwerken (VPN). Falls herstellerseitig keine sichere Kommunikationsverschlüsselung vorgesehen ist, sollten entsprechende Sicherheitsprogramme installiert werden.

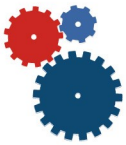


- Über GPS gewonnene Positionsdaten lassen sich zu vielen Zwecken ge- und missbrauchen. Bevor Anwendungen oder Funktionalitäten freigeschaltet werden, die GPS benutzen, sollten die Vor- und Nachteile gegeneinander abgewogen werden und der Umgang damit geklärt werden. Die Benutzer sollten über hieraus erwachsende Gefährdungen wie die Erstellung von Bewegungsprofilen informiert werden.
- Viele Smartphones offerieren auch die Möglichkeit, sie lokalisieren zu lassen. Diese Option ist reizvoll, z. B. zur schnellen Suche des Geräts oder auch des Benutzers. Dadurch könnten sie aber auch zur Überwachung von Personen eingesetzt werden. Die Nutzung solcher Funktionen muss in Deutschland mit der jeweiligen Personalvertretung und Datenschutzbeauftragten geklärt werden.
- Einfacher und erfreulich effektiv ist es, Hinweise zur Rückgabe an den ehrlichen Finder anzubringen, also z. B. über Aufkleber oder Display-Texte.

Eine Institution sollte nicht nur die Rahmenbedingungen abstecken, unter denen die Mitarbeiter Smartphones nutzen dürfen, es sollte auch geklärt werden, welche Regelungen bei Smartphones zu beachten sind, die Besucher mitbringen. Bei Gesprächen und Treffen mit vertraulichem Inhalt sollten Smartphones (und Mobiltelefone) am Besten draußen bleiben. Müssen Gesprächspartner zwingend erreichbar sein, sollten Smartphones im Sekretariat oder einer ähnlichen Stelle hinterlegt werden, die den Teilnehmer bei einem Anruf verständigt.

Konfiguration

- Bevor Smartphones in den Echtbetrieb genommen werden, also am Besten, bevor sie den Benutzer übergeben werden, sollten sie "gehärtet" werden, also auf bestmögliche Sicherheit hin eingerichtet werden. Wie im PC-Bereich sollten auch bei Smartphones alle nicht benötigten Schnittstellen deaktiviert und nicht benötigte Software entfernt werden.
- Smartphones sollten möglichst zentral administriert werden. Zentrale Managementsoftware kann in der Regel auch aus der Ferne Backups erstellen, Daten löschen und die Informationen auf einem Ersatzgerät wiederherstellen.
- Wie bei jedem Rechner sollte auch der Zugriff auf das Smartphone durch eine Authentisierung geschützt sein, beispielsweise über eine Passwort-Abfrage.

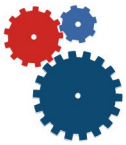


Auch wenn dies an Smartphones häufig umständlich erscheint, sollte die Authentisierung konsequent genutzt werden. Die genutzten Passwörter sollten den Vorgaben der zentralen Passwortrichtlinie entsprechen. Da die Eingabe des Passwortes am Smartphone selten unbeobachtet stattfindet, kann das Passwort leichter in fremde Hände geraten. Die Passwortrichtlinie sollte darum einen regelmäßigen Wechsel des Passwortes vorsehen. Bei längeren Phasen der Inaktivität sollte sich das Smartphone automatisch sperren und nur nach einer erneuten Authentisierung wieder benutzen lassen.

- Viele Smartphones besitzen ein umfangreiches Rechtemanagement, über das die Nutzung von Ressourcen des Smartphones geregelt werden kann. Wie überall, sollten auch hier die Rechte möglichst restriktiv vergeben werden. Nicht jede Anwendung erfordert den Zugang zu WLAN, Bluetooth oder Kamera.
  Die Rechte jeder Anwendung sollten möglichst zentral vergeben werden. Wenn technisch möglich, sollte unterbunden werden, dass die Benutzer diese Rechte selbstständig ändern können. Wo dies nicht möglich ist, müssen sie darauf hingewiesen werden, dass sie keine Einstellungen eigenständig ändern dürfen.

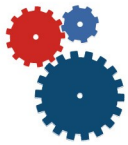
Betrieb

- Auf einem dienstlich genutzten Smartphone sollten nur freigegebene Anwendungen laufen. Dies können beispielsweise bestimmte, von einem App-Store geprüfte Anwendungen sein. Dabei ist zu beachten, dass die App-Stores unterschiedlicher Hersteller unterschiedlich stark die angebotenen Apps prüfen. Die Institution sollte eine Liste von erlaubten Anwendungen für Smartphones führen. Optimal ist der Betrieb eines eigenen App-Stores, da dies bequem für die Mitarbeiter und sicher für die Institution ist. Bei der Auswahl der zulässigen Anwendungen sollte die Institution nicht zu restriktiv sein. Auch wenn beispielsweise die Anwendungen „Wasserwaage“ oder „Sudoku“ nicht für die Arbeit gebraucht werden, kann die Erlaubnis, solche Apps (auf Privatkosten des Mitarbeiters) zu verwenden, zur besseren Annahme von Sicherheitsrichtlinien führen und so etwa die Motivation zum Jailbreaking verringern.
- Die Benutzer sollten wissen, welche Applikationen sie nutzen dürfen. Sie sollten auch die Kriterien kennen, warum bestimmte Applikationen nicht freigegeben werden. Die Einordnung in „dienstlich“ oder „privat“ ist allein kein ausreichendes Kriterium:



So gibt es beispielsweise Spiele für Smartphones, die Zugriff auf das Adressbuch verlangen und beim Start einem zentralen Spieleserver im Internet alle Kontaktdaten (eventuell auch die GPS-Positionsdaten) weitergeben. Hier gibt die Gefahr für die Informationssicherheit den Ausschlag, warum eine solche App nicht installiert werden sollte. Entsprechende Erläuterungen führen zu mehr Verständnis bei den Mitarbeitern und beugen der Umgehung des Verbots vor.

- Es dürfen keine unautorisierten Programme etwa über einen Jailbreak auf dem Smartphone installiert werden. Ob ein Jailbreak auf einem Smartphone durchgeführt wurde, kann (je nach Modell) über Tools, z. B. bei zentraler Administration, erkannt werden. Bei konkreten Vorfällen sollten die Gründe für das Jailbreaking ermittelt werden, ob es beispielsweise von Schadsoftware verursacht wurde oder vorsätzlich vom Benutzer durchgeführt wurde, und die entsprechenden Maßnahmen ergriffen werden.
- Das Betriebssystem der Smartphones sowie alle Anwendungen sind auf dem neuesten Stand zu halten und Sicherheitspatches zeitnah einzuspielen. Je nach Smartphone-Modell gibt es unterschiedliche Wege, um Updates einspielen, beispielsweise über Funk oder über Kabel nötig. Damit auch alle Smartphones zügig aktualisiert werden können, egal wo sie sich gerade befinden, sollten daher diese Randbedingungen beim Patch-Management berücksichtigt werden.
- Um Infektionen mit Schadsoftware, beispielsweise durch E-Mail-Anhänge oder Surfen im Internet („Drive-by-Infektionen“) vorzubeugen, sollte unbedingt ein aktueller Virenschutz installiert sein. Dieser sollte möglichst zentral administrierbar sein und auch Firewall-Funktionalitäten wie Schnittstellen-Filterung (z. B. WLAN, USB, Bluetooth) haben. Außerdem empfiehlt sich auch ein Spam-Filter, um unerwünschte E-Mails oder SMS zu blocken. Viele Anti-Viren-Apps können auch Webseiten auf Schadsoftware überprüft werden, bevor sie im Browser geladen werden.
- Wenn private Smartphones dienstlich genutzt werden dürfen, sollte die Institution vereinbaren, dass auch hierauf immer aktuelle Virenschutz-Software installiert wird.
- Um die auf Smartphones gespeicherten Daten zu schützen, sollten sensible Informationen nur bei ausreichender Verschlüsselung auf einem Smartphone gespeichert werden.

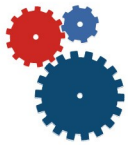


- Wichtige Daten auf den Smartphones der Anwender sollten regelmäßig, möglichst zentral, gesichert werden.
- Wird ein Smartphone weitergegeben, verkauft oder entsorgt, müssen vorher alle darauf gespeicherten sensiblen Informationen sicher gelöscht werden. Häufig gibt es dafür eine Funktion wie „Factory-Reset“ im Gerät, allerdings sollte danach kontrolliert werden, ob wirklich alle Daten gelöscht wurden. Auch zentrale Managementsoftware kann in der Regel alle Daten aus der Ferne löschen.
- Sicherheitsempfehlungen für den Nutzer

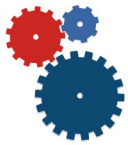
Sicherheitsmaßnahmen durch die Benutzer

Ohne die Mitarbeit der Benutzer kann keine Informationssicherheit bei Smartphones erreicht werden. Die Benutzer müssen die Smartphone-bedingten Risiken kennen, die festgelegten Sicherheitsvorgaben einhalten und für alle Sicherheitsmaßnahmen selbst Sorge tragen, die die Institution nicht zentral umsetzt. Im Einzelnen sind dies:

- Die Eingabe von Passwörtern und PINs am Smartphone sollte möglichst unbeobachtet geschehen. Bei der Auswahl und dem Umgang mit Passwörtern ist die generelle Passwortrichtlinie der Institution einzuhalten. Die Master-Passwörter sollten getrennt vom Smartphone an sicherer Stelle hinterlegt sein.
- Zum Schutz vor Verlust oder Diebstahl des Smartphones sollte es möglichst nicht ungeschützt herumliegen. Um Manipulationen oder Missbrauch vorzubeugen, sollte es auch nicht ausgeliehen werden. Wenn das Gerät doch an andere Personen vorübergehend weitergegeben wird, sollte das Smartphone möglichst nicht aus den Augen gelassen werden – ein Schadprogramm ist schnell aufgespielt. Wenn das nicht möglich ist, sollte hinterher überprüft werden, welche Aktivitäten durchgeführt wurden und ob Konfigurationen geändert oder Apps aufgespielt wurden.
- Wenn das Gerät dauerhaft weitergegeben wird, sind vorher alle sensiblen Daten sicher zu löschen.
- Im Falle eines Verlusts oder Diebstahls sollte das Smartphone möglichst zeitnah gesperrt und alle Daten aus der Ferne gelöscht werden. Wenn das Smartphone vollständig durch einen geeigneten Algorithmus verschlüsselt ist, reicht es, den Schlüssel zum Entschlüsseln aus der Ferne zu löschen, um unbefugten Zugriff zu verhindern. Besser ist aber, auch die Daten zu löschen.



- Zum Schutz vor unbefugter Nutzung sollten Bildschirmschoner oder ähnliche Zugriffssperren genutzt werden, die sich automatisch nach einer kurzen Zeitspanne der Inaktivität einschalten und nur durch eine erneute Authentikation wieder aufheben lassen.
- Benutzer sollten keine Dateien aus ungeprüften Quellen herunterladen. Alle Downloads sollten durch eine Antivirensoftware überprüft werden.
- Unerwartete E-Mail-Anhänge oder Anhänge von unbekannten Sendern sollten nicht geöffnet werden.
- Die Benutzer müssen dafür sensibilisiert sein, dass sie bei der Nutzung von Internet-Diensten, bei denen persönliche oder geschäftsrelevante Daten eingegeben werden, wie E-Mail, Online-Banking, Business-Kommunikationsplattformen, etc., auf eine verschlüsselte Verbindung (z. B. SSL-Symbol) und ein gültiges Zertifikat achten.
- Eine direkte Kopplung mit anderen Geräten zum Austausch von Daten, etwa über Bluetooth, darf nur bei vertrauenswürdigen Partnern geschehen, um zu vermeiden, dass das eigene Gerät manipuliert oder mit Schadsoftware infiziert wird.
- Nicht alle Sicherheitsmaßnahmen lassen sich zentral umsetzen. Dazu können das Aktualisieren des Betriebssystems, der Anwendungen und der Virensignaturen zählen. Wenn die Benutzer über solche anstehenden Maßnahmen informiert werden, müssen sie die erforderlichen Aktionen zeitnah umsetzen.
- Wenn Anwendungen installiert werden, sollten diesen nur die Rechte eingeräumt werden, die unbedingt erforderlich sind. Die Erfahrung zeigt, dass einige Anwendungen weitreichende Zugriffsrechte wie beispielsweise den Zugriff auf das GPS-Modul verlangen und Positionsdaten auslesen, speichern und an Dritte übermitteln, ohne dass dies erforderlich wäre. Solche Anwendungen sollten weder installiert noch ausgeführt werden, auch wenn sie der Smartphone-Anbieter zertifiziert hat.
- Nahezu alle Smartphone-Anbieter erlauben nur, dass von ihnen zugelassene und zertifizierte Programme auf dem Smartphone installiert werden können. Diese Vorkehrung kann mit Jailbreaking umgangen werden, also indem die Sperren der Anbieter ausgehebelt werden.



Da Jailbreaking allerdings auch zu Sicherheitsproblemen führen kann, darf es bei Smartphones, die sensible Daten enthalten, nicht durchgeführt werden.

Weitere BSI-Empfehlungen zu diesem Thema

- IT-Grundschutz-Kataloge, beispielsweise Bausteine B 3.404 Mobiltelefon und B 3.405 PDA https://www.bsi.bund.de/IT-Grundschutz-Kataloge
- Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen, BSI-Broschüre https://www.bsi.bund.de/DE/Publikationen/Broschueren/Mobile/mobileendgeraete.html
- Wie bewege ich mich sicher im mobilen Netz? https://www.bsi-fuer-buerger.de