Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

Android

Konfigurationsempfehlung auf Basis betriebssystem-eigener Mittel für eine Nutzung mit erhöhter Sicherheit

1 Einleitung

Android ist ein weitgehend quelloffenes Betriebssystem für mobile Geräte, wie Smartphones und Tablet-Computer, das von der "Open Handset Alliance"[1] unter der freien Apache-Lizenz sowie der GNU General Public License (GPL) entwickelt wird. Federführend ist dabei die Firma Google. Basis ist ein Linux-Kernel, auf dem das Betriebssystem Android als Mittelschicht läuft. Darauf werden in einer kontrollierten Ablaufumgebung Applikationen (Apps) von Drittanbietern installiert und ausgeführt. Das Betriebssystem verfolgt dabei mit dem sogenannten *Sandbox-Prinzip* den Ansatz der kontrollierten Trennung von Apps vom Betriebssystem und auch von App zu App.

Aufgrund der Quelloffenheit haben Gerätehersteller die Möglichkeit, die Android-Mittelschicht an eigene Bedürfnisse anzupassen und sie um – z. T. proprietäre – Komponenten zu erweitern. Einige Hersteller unterstützen so Besonderheiten der verwendeten Hardware, andere Hersteller ändern beispielsweise die komplette Bedienoberfläche in ihren Geräten. Diese Veränderungen beziehungsweise Ergänzungen führen in der "Android-Landschaft" zu einer mittlerweile unüberschaubaren Vielzahl von angepassten Android-Versionen (Android-Fragmentierung), die durch den Einsatz von Android auf verschiedenartigen Geräteklassen über klassische Smartphones hinaus, z. B. Uhren, Unterhaltungssysteme und insbesondere Tablets, enorm an Komplexität gewinnt. Die Pflege dieser angepassten Versionen sowie die Versorgung der Geräte mit Betriebssystem-Updates wird von den Herstellern allein schon in dem schnelllebigen Smartphone-Markt nur unzureichend geleistet. Neue Betriebssystem-Versionen, die von Google herausgegeben werden, müssen dann durch die Gerätehersteller, wiederum an die eigenen Bedürfnisse angepasst werden. Aufgrund der sehr schnellen Produktzyklen im Bereich mobiler Endgeräte kann man oft beobachten, dass ein neues Android-Gerät, früher auf dem Markt erscheint, als dass es neue und angepasste Betriebssystem-Updates für die etablierten Geräte gibt.

Durch den hohen Grad der Fragmentierung der Android-Landschaft ist es unmöglich, Konfigurationsempfehlungen für alle möglichen Android-basierten Geräte zu geben. Die vorliegende Empfehlungen beschränken sich daher auf die von Google herausgegebene Grundversion von Android. Es soll gezeigt werden, welche betriebssystemeigenen Mechanismen zur Verfügung stehen und wie diese mit geeigneten Maßnahmen zur Erhöhung der Datensicherheit beitragen. Viele Empfehlungen sind jedoch allgemeingültig auch auf angepassten Android-Versionen anderer Hersteller sowie weitere Geräteklassen anwendbar.

1 http://www.openhandsetalliance.com/

Gefährdungen durch konzeptionelle Schwächen, systembedingte Mängel oder ausgenutzte Schwachstellen im Betriebssystem können mit den empfohlenen Konfigurationen und Maßnahmen höchstens gemildert, jedoch nicht vollständig beseitigt werden. Solchen Gefährdungen kann im PC-Bereich z. B. unter Microsoft Windows mit zusätzlichen Schutzprogrammen begegnet werden, die Angriffe tief im Betriebssystem auf Kernel- und Prozessebene abwehren. Im Betriebssystem Android unterliegen Schutzprogramme jedoch den gleichen Einschränkungen wie "normale" Apps von Drittanbietern und sind demzufolge nicht in der Lage, Verteidigungslinien „vor der Schadsoftware“ aufzubauen und so ein vergleichbares Schutzniveau zu gewährleisten. Mehr dazu im Kapitel "Schutzprogramme".

Für einen sicheren Einsatz im Unternehmensumfeld mit einem hohen und sehr hohen Schutzbedarf reichen die empfohlenen Konfigurationen alleine nicht aus. Ohne weitere Maßnahmen sollten auf Android-Geräten **keine vertraulichen Daten verarbeitet werden**. Solche Maßnahmen werden im nächsten Kapitel "Einsatzszenarien" beschrieben.

2 Einsatzszenarien

Bei der Verwendung von Smartphones und Tablets für berufliche Zwecke sind grundsätzlich drei Einsatzszenarien denkbar:

1. Der Gebrauch der im Betriebssystem integrierten Apps (Kontakte, Kalender, E-Mail-Client, Webbrowser) und/oder vergleichbaren Apps von Drittanbietern. Dabei kommt es oft zu einer Vermischung von geschäftlicher und privater Benutzung.
2. Sämtliche geschäftlichen Belange werden in einer abgeschlossen, gesicherten Einheit bearbeitet, dem sogenannten "Secure Container". Es handelt sich dabei um Drittanbieter-Apps. Das Smartphone kann außerhalb dieses Containers normal, das heißt ohne spezielle, restriktive Konfiguration verwendet werden.
3. Private und geschäftliche Bereiche werden als unterschiedliche virtuelle Maschinen auf einem Gerät betrieben. Hierbei werden der private und geschäftliche Bereich nicht auf Anwendungsebene, sondern auf Betriebssystemebene getrennt. Ein Datenaustausch zwischen beiden virtuellen Maschinen ist nur über die tiefer liegende Virtualisierungsschicht in Form des Hypervisors (auch Virtual Machine Monitor, VMM genannt) möglich.

Das BSI empfiehlt, sofern aus wirtschaftlichen oder organisatorischen Gründen keine umfassende Lösung verwendet werden kann, die eine Trennung geschäftlicher und privater Bereiche mittels Virtualisierungstechniken umsetzt, mindestens den Einsatz des Secure Containers, weil damit Wechselwirkungen zwischen privater und geschäftlicher Verwendung des mobilen Endgerätes verhindert werden und alle geschäftlichen Daten sicher gespeichert werden können. Eine ungeregelte Nutzung der im Betriebssystem integrierten Apps sowie die Vermischung geschäftlicher und privater Daten ist in jedem Fall zu vermeiden. Siehe dazu auch die Empfehlungen zur Cyber-Sicherheit "Mobile Device Management"[2] der Allianz für Cyber-Sicherheit.

Für den Fall, dass dieser Empfehlung nicht gefolgt werden kann, werden in diesem Dokument Konfigurationsempfehlungen für den Gebrauch der "nativen" Apps (Szenario 1) gegeben.

3 Sicherheitsrichtlinien

Bevor mobile Endgeräte in eine Unternehmensstruktur eingebunden werden können, müssen klare Regeln für die Integration festgelegt werden. Mit diesen Sicherheitsrichtlinien, den sogenannten Security Policies, werden u. a. die Rahmenbedingungen bezüglich Auswahl der Geräte, Auswahl der Daten, die auf den Geräten verarbeitet werden dürfen, Einschränkungen der Benutzer, Limitierung der Möglichkeiten der Geräte (Hardware wie Software), festgelegt. Die BSI

2 https://www.allianz-fuer-cybersicherheit.de/dok/6649766

Publikation „Überblickspapier Smartphone“[3] liefert dazu weitere Aspekte.

Neben den Sicherheitsrichtlinien ist auch eine Betriebsvereinbarung mit einer klaren Darstellung der Rahmenbedingungen für die Verwendung der mobilen Endgeräte notwendig.

Die Durchsetzung der technischen Anforderungen der Sicherheitsrichtlinien ist bei der steigenden Anzahl der mobilen Endgeräte nur noch mit entsprechenden Tools erreichbar. Dazu wird eine Mobile Device Management-Lösung (MDM) verwendet.

4 Aktualisierungen

Durch die Popularität des Betriebssystems Android und den damit verbundenen Marktanteilen ist die Wahrscheinlichkeit relativ hoch, dass Schwachstellen gefunden und aktiv ausgenutzt werden. Daher ist die zeitnahe Verfügbarkeit sowie das Einspielen von Updates beim Auftreten von Schwachstellen wichtig. Es sollten nur Geräte von solchen Herstellern verwendet werden, die eine nachvollziehbare und schnelle Updatepolitik haben und ihre Geräte langfristig mit Aktualisierungen versorgen[4]. Geräte, die keine Betriebssystem-Updates mehr erhalten, sollten ausgesondert werden. Das Restrisiko für die Ausnutzung gegebenenfalls bestehender Sicherheitslücken wird entsprechend größer.

Neue Versionen von Apps sollten vor der Installation auf neue oder veränderte Funktionalitäten geprüft werden. Man kann sich über neue Versionen von Apps benachrichtigen lassen. Die Einstellungen dazu werden in der *Google Play* App im Menü Einstellungen vorgenommen. Neuen Versionen können auch Veränderungen in den Berechtigungen (Permissions) aufweisen. Lesen Sie dazu auch das Kapitel "Permissions".

Automatische App-Updates sollten deaktiviert werden (Google *Play Store* App - Einstellungen - 'Keine automatischen App-Updates').

5 Bluetooth und NFC

Nicht benötigte Schnittstellen sollten grundsätzlich abgeschaltet werden. Beispiele hierfür könnten sein: Bluetooth oder NFC.

6 WLAN und Mobilfunknetze

Smartphones sind nur sinnvoll einsetzbar, wenn sie Zugang zum Internet haben. Die derzeit hauptsächlichen Kommunikationskanäle sind dabei das Mobilfunknetz des Providers sowie im Nahbereich WLAN. Problematisch sind unverschlüsselte WLANs, etwa in öffentlichen Plätzen, in Hotel-WLANs oder großen Handelsketten. Hier kann praktisch jeder den Netzwerkverkehr mitlesen.

Generell sollte die WLAN-Funktion in unsicheren – das heißt unverschlüsselten sowie fremd kontrollierten – Umgebungen deaktiviert werden. Ebenso, wenn sie überhaupt nicht gebraucht wird.

Die Kommunikation außerhalb eines WLAN geschieht über das Mobilfunknetz des Providers mittels der Standardprotokolle GSM, UMTS (3G) und LTE (4G). GSM gilt als unsicher und kann mit wenig Aufwand abgehört werden[5]. Mit UMTS wurden verbesserte Authentifizierungs-Mechanismen eingeführt, Sicherheitsprobleme sind aber auch bei dieser Technik nicht ausgeschlossen[6]. Demgegenüber verkürzt der neuste Standard (LTE) die Akkulaufzeit etwas mehr. Dieser Nachteil sollte jedoch aufgrund der besseren Absicherung der Kommunikation in Kauf genommen werden. LTE basiert vollständig auf einem IP-Übertragungssystem. Die Datenübertragung erfolgt also (wie schon im Internet allgemein üblich) datenpaketorientiert auf Basis

3 https://www.bsi.bund.de/dok/6604784
4 The state of Android updates: http://arstechnica.com/gadgets/2014/08/the-state-of-android-updates-whos-fast-whos-slow-and-why/
5 BSI Dokument "Öffentliche Mobilfunknetze und ihre Sicherheitsaspekte": https://www.bsi.bund.de/dok/6604038
6 Lücke im SS7 bei UMTS: http://heise.de/-2503376

des IP-Protokolls. Für alle Verbindungen wird AES als Verschlüsselung eingesetzt.

Bei einigen Android-basierten Geräten kann der unsichere Standard GSM sogar deaktiviert werden, was irreguläre Abhörmaßnahmen auf der Luftschnittstelle erschwert.

In allen ungesicherten Netzen sollten die Daten durch den Einsatz eines Virtual Private Networks[7] (VPN) verschlüsselt werden. Die Verwendung von VPNs ist jedoch mit Aufwand verbunden, da die Gegenseite der Kommunikationsstrecke ebenso das VPN unterstützen muss. Im geschäftlichen Bereich ist dieser Aufwand aber in jedem Fall gerechtfertigt.

7 Rooten

Beim sogenannten Rooten wird das Sicherheits-Konzept von Android außer Kraft gesetzt. Apps können mit Root-Berechtigung ablaufen und haben so alle Möglichkeiten, das Betriebssystem zu kontrollieren.

Im Unternehmenseinsatz sollten Android-basierte Geräte nicht "gerootet" sein.

Daneben gibt es für eine Vielzahl von Android-basierten Geräten alternative Android-Versionen, sogenannte Custom ROMs, die nicht vom Hersteller selbst stammen. Als Beispiel sei das weit verbreitete LineageOS[8] – früher CyanogenMod – genannt. Mit diesen Custom-ROMs erhält der Benutzer in der Regel mehr Möglichkeiten der Einflussnahme auf das Betriebssystem. Zu beachten ist, dass durch die Manipulation des originalen Betriebssystems die Herstellergarantie möglicherweise verloren geht. In jedem Fall wird der Nachweis, dass ein aufgetretener Schaden nicht durch die Betriebssystemmanipulation hervorgerufen wurde, schwierig. Custom-ROMs sollten für geschäftliche Zwecke nicht eingesetzt werden.

8 App-Stores

Im Auslieferungszustand ist üblicherweise nur Googles eigener App-Store über die App *Google Play* erreichbar. Apps aus anderen Quellen können nicht installiert werden. Dies verhindert eine Systemeinstellung (*Einstellungen - Sicherheit - Unbekannte Herkunft*). Wird diese Einstellung deaktiviert, können Apps aus beliebigen Quellen installiert werden. Dies können alternative App-Stores sein, Internet-Seiten, auf denen ein Installationspaket einer App verlinkt ist, aber beispielsweise auch ein solches Paket im Anhang einer E-Mail. Grundsätzlich gilt, dass Apps nicht ohne Nutzerinteraktion, nämlich durch Bestätigung der App-Berechtigungen, installiert werden können.

Wie im Kapitel "Schutzprogramme" erläutert wird, bestehen schädliche Apps (Malware) bei Android technisch gesehen aus vollkommen normalen Programmen, d. h. Apps, die der Benutzer selbst installiert. Diese maliziösen Apps kommen fast ausschließlich aus "unsicheren Quellen", App-Stores, die keine ausreichende Sicherheitskontrolle haben oder Installationspakete aus sonstigen Quellen. Im Gegensatz dazu wird der Play Store von Google überwacht, gegenüber den sonstigen Quellen sind hier bisher kaum Fälle bekannt geworden.

Das BSI empfiehlt, keine Apps aus unsicheren und nicht vertrauenswürdigen Quellen zu installieren. Ob und welche Apps installiert werden dürfen, sollte durch eine spezifische Unternehmens-Richtlinie geregelt werden.

Mit der Systemeinstellung *Einstellungen - Sicherheit - Unbekannte Herkunft* werden aber auch alternative, seriöse App-Stores deaktiviert. Als ein Beispiel für eine ebenfalls professionell betreute Alternative zu Google Play sei der Amazon-App-Store genannt. Bei diesem werden, wie auch bei Google Play, die von der ENISA empfohlenen Maßnahmen zur Absicherung von App-Stores[9] umgesetzt.

7 http://de.wikipedia.org/wiki/Virtual_Private_Network
8 https://www.lineageos.org/
9 http://www.enisa.europa.eu/media/press-releases/app-store-security2013-the-five-lines-of-defence-new-report-by-eu-cyber-security-agency-enisa

Das BSI empfiehlt, die Option abzuschalten und für Apps aus solchen App-Stores nur im Bedarfsfall kurzfristig einzuschalten.

9 Apps verifizieren

Google bietet mit der Option *Einstellungen - Sicherheit - Apps verifizieren* die Möglichkeit, Apps vor der Installation mithilfe einer Reputationsdatenbank auf schädliche Apps zu prüfen. Dies betrifft Apps aus unbekannten Quellen. Zudem sucht der Google-Dienst dann regelmäßig auf dem Gerät nach schädlichen Apps. Werden Apps als schädlich erkannt, wird eine entsprechende Warnung angezeigt und die Installation abgebrochen.

Zu beachten ist, dass *Apps verifizieren* ein Cloud-Dienst ist und Daten über die Apps sowie über das Gerät an Google gesendet werden[10].

Im Unternehmens-Einsatz ist es empfehlenswert, die zu verwendenden Apps vorab von einem unabhängigen Prüfinstitut tiefgehend auf mögliche schädliche Funktionalitäten untersuchen zu lassen.

Die Option *Apps verifizieren* ist eine der effektivsten Schutzmaßnahmen gegen schädliche Apps – Das BSI empfiehlt die Nutzung daher.

10 Schutzprogramme

Schädliche Apps im Android-Umfeld sind Apps, die neben gewollten, sinnvollen auch ungewollte, bösartige Funktionen enthalten. Es handelt sich dabei meist nicht um Programme, die sich tief im Betriebssystem einnisten, wie z. B bei Standard Desktop-Computer, sondern um Apps, die der Benutzer (oder das Unternehmen) selbst installiert. Meist handelt es sich bei 'infizierten' Apps um Programme aus unsicheren Quellen.

Betriebssysteme, wie Android, sind über die Rechtestruktur für Apps verhältnismäßig gut abgeschottet. Das Sandbox-Prinzip verhindert sowohl den unkontrollierten Zugriff auf Daten außerhalb der Ablaufumgebung als auch den Zugriff von außen auf die App.

Derzeitige Schutzprogramme für mobile Endgeräte erkennen Malware-Apps anhand von statischen Signaturen. Eine auf Desktop-Systemen eingesetzte echte Hintergrundüberwachung der laufenden Prozesse, die für eine gute Schutzwirkung notwendig ist, ist auf mobilen Betriebssystemen, wie Android und iOS, für Drittanbieter-Apps nicht möglich. Beim Virentest findet demnach eine Prüfung statt, ob eine App in einer Malware-Datenbank enthalten ist – Auch hierbei, wie bei Google, als Cloud-Dienst. Dieser Vorgang geschieht vor der Installation der App automatisch, kann aber auch auf alle bereits installierten Drittanbieter-Apps angewendet werden.

Schutzprogramme (AV-Apps) bieten oft neben der Erkennung von Malware weitere Funktionen, wie zum Beispiel Diebstahlschutz, "Parental Control" (Kinderschutz), Verschlüsselung, "Safe Browsing" (Blockieren von unsicheren Websites), usw.

Aus Sicht des BSI ist Virenschutz auf mobilen Endgeräten aus grundsätzlichen Erwägungen zurzeit nicht erforderlich. Die von Google im offiziellen Play Store umgesetzten Mechanismen sowie die ohnehin vor einer Verteilung über MDM vorzunehmenden Prüfungen sind in der Lage, ein hinreichendes Schutzniveau zur Abwehr von Schadprogramm zu gewährleisten. Zudem sind am Markt verfügbare Virenschutzlösungen mit technischen Einschränkungen verbunden, insbesondere erfolgt wie oben beschrieben keine Überwachung im Hintergrund. Lediglich für Nutzer, die Apps auch aus alternativen Quellen beziehen oder die die oben genannten Zusatzfunktionen nutzen wollen, können AV-Apps neben dem Google-Dienst *Apps verifizieren* eine sinnvolle Ergänzung darstellen. Eine Übersicht über Android-Sicherheits-Apps liefern die einschlägigen Testinstitute, wie beispielsweise AV-TEST.

10 https://support.google.com/accounts/answer/2812853?hl=de

Bei der ausschließlichen Nutzung von Apps aus vertrauenswürdigen, sicheren App-Stores sowie geprüften Apps, kann zurzeit auf zusätzliche AV-Programme verzichtet werden.

11 Datenschutz und Privatsphäre

Der Verlust von Daten und der Privatsphäre stellt ein großes Problem für den Benutzer dar. Die Erfassung und Auswertung von Nutzerdaten (Kontakte, Geopositionen, Surfverhalten, E-Mail-Inhalte usw.) ist häufig intransparent und nur schwer nachvollziehbar.

11.1 Permissions

Permissions sind die Berechtigungen, die eine App im Android-Betriebssystem hat. Mit Berechtigungen kann eine App auf Objekte außerhalb der eigenen Sandbox zugreifen. Beispiele sind *Kontakte lesen oder Zugriff auf Mikrofon, Kamera oder Geopositionsdaten.* Es gibt Einzel- und Gruppenberechtigungen, unterteilt in kritische, unkritische und systemrelevante Berechtigungen.

Die Berechtigungen werden dem Benutzer vor der Installation einer App angezeigt und er muss sie explizit bestätigen. Er kann nur alle Berechtigungen gleichzeitig bestätigen. Verweigert er das, wird die App nicht installiert.

App-Berechtigungen sollten kritisch geprüft werden. Dies ist die einzige Einflussmöglichkeit, die ein Anwender hat. Im Zweifelsfall sollte er eine App nicht installieren.

Weitere Informationen zu Android-Berechtigungen findet man auf BSI-FUER-BUERGER[11].

11.2 Cloud-Dienste

Aus Sicht des Datenschutzes sollte sorgfältig abgewogen werden, welche (persönlichen oder geschäftlichen) Daten wo verarbeitet und gespeichert werden. Eine Vielzahl von Apps verwenden externe Dienste und Speicherkapazitäten für diese Aktionen. Insbesondere die Speicherkapazitäten und die Möglichkeit der Synchronisation der Daten über mehrere Geräte sind bei den Benutzern beliebt. Oft werden solche Dienste verwendet, ohne dass den Benutzern klar ist, dass es sich dabei um Cloud-Technik handelt und wichtige Daten extern gespeichert werden. Nutzer sollten bei der Auswahl von Apps darauf achten, ob die Daten der App lokal oder in der Cloud gespeichert werden.

11.3 Backups

Backups sind Sicherheitskopien, aus denen die Nutzerdaten im Bedarfsfall wieder hergestellt werden können. Diese Daten sollten nur lokal gespeichert werden und zusätzlich verschlüsselt sein. Die Ablage von Nutzerdaten in Cloud-Speichern oder die automatische Synchronisation zwischen Mobilgerät und Cloud-Speicher stellt keine ausreichende Sicherung der Daten dar. Nutzer müssen bei solchen Diensten damit rechnen, dass diese Daten unverschlüsselt vorliegen und die Anbieter diese Daten ggf. für ihre Zwecke nutzen. In Google Play gibt es Apps, die Backups auch von nicht-gerooteten Geräten anfertigen können[12].

11.4 Widgets

Widgets sind kleine Programme, die im Homescreen des Smartphones ablaufen. Sie sind im Betriebssystem schon teilweise vorhanden, können aber auch aus dem App Store nachinstalliert werden. Typische Widgets sind Kalender, Notizen, E-Mail oder Wetter.

Diese Widgets können auch im Sperrbildschirm angezeigt werden.

Es ist darauf zu achten, dass im Sperrbildschirm durch Widgets keine sensitiven Daten angezeigt werden, beispielsweise SMS (die z. B. mTANs für Bank-Transaktionen enthalten können), E-Mail-Nachrichten oder Kalendereinträge.

11

12 Beispiel: MyPhoneExplorer (Desktop-Programm) und zugehörige MyPhoneExplorer Client (Android App)

11.5 Google Apps und Google Dienste

Es gibt eine Vielzahl von Apps und Diensten von Google; dazu gehören Apps, die bereits mit dem Android-Gerät ausgeliefert werden sowie Apps, die man nachträglich installieren kann. Beispiele sind:

- Gmail
- Chrome
- Hangout
- Google Kalender
- Google Drive
- YouTube
- Picasa
- Google Play
- Google+
- Google Now

Alle Google-Apps und Google-Dienste sind u. a. auch über Google Now miteinander verzahnt und bilden ein Ökosystem, das die Verwendung von Android-Geräten bequem macht. So wird beispielsweise bei Google Maps die aktuelle Position in der Karte angezeigt, wenn man sich orientieren will, oder tageszeit- oder ortsabhängige Ereignisse werden automatisch im Bildschirm eingeblendet. Seit der Android-Version 4.4 enthält Google Now die Sprachsteuerungsfunktion 'always-listening'. Ist diese Funktion aktiviert, reagiert das Mobilgerät auf die Worte 'OK Google' und führt den gesprochenen Befehl aus oder beantwortet die gesprochene Anfrage. Dabei ist das Mikrofon des Gerätes immer aktiviert, wenn sich das Gerät im eingeschalteten Zustand befindet.

Nutzer erkaufen sich diese Bequemlichkeit jedoch mit der Übertragung ihrer Daten an Google, die Google gemäß der Nutzungsvereinbarung zur Bereitstellung des Dienstes weiter auswerten und nutzen kann. Anwender sollten daher überlegen, welche Apps beziehungsweise Dienste sie verwenden wollen. Über die App *Google Einstellungen* hat der Benutzer Möglichkeiten, den Abfluss von Daten durch Google-Dienste zu steuern. Zudem kann man im Menü *Einstellung - Apps* nicht benötigte System-Apps deaktivieren[13]. Mit weitergehenden Maßnahmen ist es sogar möglich, ein Android-basiertes Mobilgerät weitgehend auch ohne Google-Apps und Google-Dienste zu betreiben.

An dieser Stelle sei deutlich darauf hingewiesen, dass Google zwar eine umfassende Integration seiner Apps und Dienste in Android vorgenommen hat, Anbieter anderer Apps deren Nutzerdaten aber ebenso erfassen, speichern und (oft für Werbezwecke) auswerten.

12 E-Mail

Bei E-Mail-Programmen ist bei der Einrichtung des Accounts darauf zu achten, dass die Übertragung von empfangenen und gesendeten E-Mails verschlüsselt geschieht). Bei der Verwendung von Web-Mailern muss das HTTPS-Protokoll verwendet werden.

13 Internet-Browser

Der Internet-Browser ist sicherlich auch bei mobilen Endgeräten eine der am meisten verwendeten Apps. Es ist ein Internet-Browser zu verwenden, der nach dem Sandbox-Prinzip arbeitet.

Der Standardbrowser in Google Nexus-Geräten ist der Chrome-Browser. Der Browser verfügt über einen "Inkognito-Modus", in dem die aufgerufenen Webseiten nicht zum "Verlauf" (Historie) hinzugefügt werden. Cookies, Lesezeichen, Leselisten, usw. werden nicht gespeichert. Dieser Modus ist zu verwenden, wenn man keine Spuren des Surf-Verhaltens auf dem Endgerät hinterlassen will und Eingaben und Downloads nicht registriert werden sollen. Der Inkognito-Modus kann jedoch prinzipiell nicht einer ggf. Server-seitig implementierten Überwachung entgegenwirken. Insofern ist die Bezeichnung "Inkognito" irreführend, da gegenüber dem Anbieter der Webseite keine Anonymisierung erfolgt.

Enthält der verwendete Browser einen Phishing-Filter, sollte dieser auch verwendet werden.

13 https://support.google.com/googleplay/answer/3123922?hl=de

14 Android Debugging Bridge

Android-basierte Mobilgeräte verfügen mit der sogenannten Android Debugging Bridge (ADB, auch USB-Debugging) über eine Schnittstelle, die weitgehenden Zugriff auf das Gerät erlaubt. Diese Schnittstelle besteht standardmäßig aus einer Kabelverbindung zwischen Mobilgerät und Desktop-Computer, es gibt aber auch Erweiterungen, die eine Verbindung über WLAN erlauben. Die Schnittstelle ist primär für den Entwicklungsprozess von Apps gedacht, wird aber auch für diverse andere Datenzugriffe auf dem Gerät verwendet. Die Schnittstelle ist standardmäßig deaktiviert, kann aber durch den Benutzer aktiviert werden (bei einigen Geräten durch versteckte Kommandos im Menü *Einstellungen).*

Diese Schnittstelle ist für den normalen Gebrauch von Android-basierten Geräten nicht notwendig und sollte in jedem Fall deaktiviert werden.

15 Display-Sperre

Im Menü *Einstellung - Sicherheit - Display-Sperre* kann man wählen, ob das Gerät über eine Display-Sperre verfügen und mit welcher Methode die Entsperrung erfolgen soll. Zur Wahl stehen:

- keine
- Finger bewegen
- PIN
- Passwort
- Muster
- Face Unlock

Die Wahlmöglichkeit *keine* und *Finger bewegen* bieten keinerlei Schutz vor unberechtigtem Zugriff. Eine *PIN* kann aus mindestens 4 und maximal 16 Ziffern bestehen. Das Gleiche gilt für ein *Passwort* aus alphanumerischen Zeichen. Ein mit dem Finger abzufahrendes *Muster* hat Werte zwischen 4 und 9 Punkte. *Face Unlock* ist als Zugangsschutz ungeeignet, da Personen, die sich ähnlich sehen, das Smartphone entsperren können. Teilweise reicht schon ein ausgedrucktes Foto zur Entsperrung.

Der beste Zugangsschutz bietet ein ausreichend langer PIN-Code beziehungsweise ein entsprechend komplexes alphanumerisches Passwort.

Über das Menü *Einstellung – Display -Ruhezustand* kann die Zeit bis zur automatischen Aktivierung einer Displaysperre zwischen 15 Sekunden und 30 Minuten eingestellt werden. Es wird empfohlen, dort keine Zeiten über fünf Minuten zu wählen.

16 Geräteverschlüsselung

Mit dem Menü *Einstellung - Sicherheit - Telefon verschlüsseln* kann man die Daten des Smartphones verschlüsseln. Es handelt sich um eine Verschlüsselung der Datenpartition des Benutzers. Dazu ist die Eingabe einer PIN oder eines Passworts beim Gerätestart notwendig, die beliebte Wischgeste (Finger bewegen) funktioniert damit nicht.

Zu beachten ist, dass bisher nur der interne Gerätespeicher verschlüsselt wird, Daten auf einer eventuell vorhandenen externen Speicherkarte oder Daten die in der Cloud gespeichert werden jedoch nicht. Ist dies der Fall, kann zur Verschlüsselung der Daten der SD-Karte oder Daten in der Cloud auf Drittanbieter-Apps aus dem App Store zurückgegriffen werden.

Weiterhin ist zu beachten, dass gegebenenfalls eine Verschlüsselung nur durch das Zurücksetzen des Geräts auf Werkseinstellung rückgängig gemacht werden kann. Dabei gehen alle Daten auf dem internen Speicher des Geräts verloren. Zur Datenwiederherstellung muss vor dem Zurücksetzen ein Backup erstellt werden.

17 Geräteadministrator-Apps

Als "Geräteadministratoren"werden in Android Apps bezeichnet, die Sicherheitsrichtlinien durchsetzen. Die Apps tragen sich im Menü *Einstellungen - Sicherheit - Geräteadministratoren* ein und müssen vom Nutzer dort auch aktiviert werden.

Die Richtlinien betreffen:

- Passwortregeln
- Aufforderung für ein neues Passwort
- Automatische Bildschirmsperrung
- Datenlöschung (Werkseinstellung) aus der Ferne
- Geräteverschlüsselung
- Abschalten der Kamera

Sie können in der jeweiligen App fest enthalten sein oder von einem entfernten Server gesendet werden[14]. Oft werden solche Apps mit einer entsprechenden Infrastruktur angeboten.

Da es sich um normale Apps handelt, sollten Nutzer während der Installation auf die Berechtigungen achten, die solche Apps fordern. Bei bereits installierten Geräteadministrator-Apps kann über das Menü *Einstellungen - Sicherheit - Geräteadministratoren* die Administrator-Funktionalität abgeschaltet werden.

18 Restrisiken

Selbst bei der Verwendung von sicheren Einstellungen auf dem mobilen Endgerät, die sowohl den Benutzer als auch die Apps weitgehend in ihren Freiheiten einschränken, bleibt ein Restrisiko. Dieses Restrisiko beruht in erster Linie darauf, dass die Geräte außerhalb einer gesicherten Umgebung eingesetzt werden, oft auch in Umgebungen, in denen man einen Laptop nicht einsetzen würde. Es besteht immer die Gefahr, dass die Geräte (und damit die darauf befindlichen Daten) durch Verlust oder Diebstahl abhandenkommen. In einem solchen Fall kann man nur darauf vertrauen, dass die eingesetzten Mechanismen zur Datenabsicherung wirksam greifen und nachträglich initiierte Aktionen (beispielsweise eine Fernlöschung) funktionieren. Hierbei ist aber auch abzuwägen, ob Fernlöschmechanismen oder Geräteortung nicht anderen Datenschutzaspekten widersprechen.

Bei allen Varianten des Einsatzes von Android verbleiben Restrisiken unterschiedlicher Tragweite, denen nicht ohne Weiteres begegnet werden kann. Als Beispiel seien die unerlaubte Verwendung des Gerätemikrofons zum Abhören oder die unerlaubte Nutzung der GPS-Funktion zum systematischen Tracking des Benutzers genannt.

Darüber hinaus liegen weitere Restrisiken in der Sprach-, SMS- und Datenkommunikation über das Internet, die ohne zusätzliche Maßnahmen nicht Ende-zu-Ende gesichert sind.

Zu beachten ist auch, dass sichere Konfigurationen immer auch Beschränkungen für den Benutzer bedeuten. Dies führt nicht nur zu Akzeptanzproblemen, sondern fördert auch die Fantasie der Benutzer, Grenzen und Beschränkungen zu überwinden.

14 Supportartikel zu Device Administrator API (englisch): http://developer.android.com/guide/topics/admin/device-admin.html

19 Fazit

Mobile Geräte mit dem Betriebssystem Android sind sowohl im Privat- wie im Geschäftsbereich weit verbreitet. Diese Verbreitung liegt im Wesentlichen an der Offenheit des Systems, an vergleichsweise günstiger Hardware und an der Vielzahl kostenfreier Apps. Diese Offenheit führt jedoch einerseits zu einer komplexen Betriebssystem-Struktur, andererseits aber auch zu einer unüberschaubaren Vielzahl von Geräten mit unterschiedlichen Android-Versionen. Dadurch ergeben sich ebenso heterogene wie komplexe Anforderungen beim Versuch einer abgesicherten Nutzung der Geräte.

Für den beruflichen Einsatz von Android-basierten Geräten sind mindestens die oben empfohlen Konfigurationen durchzuführen. Beim Einsatz dieser Geräte in größeren Umgebungen und Stückzahlen ist die Verwaltung mittels einer Mobile Device Management-Lösung[15] unumgänglich.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an **info@cyber-allianz.de** gesendet werden.

15 https://www.allianz-fuer-cybersicherheit.de/dok/6649766