Datenschutz bei Smartphones. Was muss ich dazu wissen?

Smartphones sind unsere ständigen Begleiter. Das nicht nur im Privatleben, sondern auch im beruflichen Umfeld. Dabei wird allzu oft vergessen, dass auf diesen Smartphones eine Vielzahl von sensiblen Daten gespeichert und verarbeitet werden. Das geht von E-Mails über Fotos bis hin zu GPS-Daten und Bewegungsprofilen. Mit Ihrem Smartphone können Sie über Cloud-Services eventuell auch direkt auf sensible Unternehmensdaten, wie z.B. Kundendaten aus dem zentralen CRM-System zugreifen. Im privaten Umfeld werden Sie in der Regel auch Ihre Bankgeschäfte mit dem Smartphone erledigen, was die Sensibilität der Daten wiederum erhöht. So können Kriminelle dann auch Geld von Ihren Bankkonten stehlen.

Datenschutzverletzungen am Smartphone. Welche Risiken muss ich kennen?

Die meisten Datenschutzverletzungen auf Mobilgeräten sind auf die folgenden grundlegenden Sicherheitsversagen zurückzuführen:

- Benutzer verwenden unsichere oder gar keine Kennwörter / Codes.
- Benutzer speichern unverschlüsselte Daten.
- Benutzer fallen auf Phishing oder andere Social Engineering-Tricks herein.
- Benutzer installieren Apps aus unzuverlässigen Quellen.
- Das Smartphone Betriebssystem (Android, iOS) und die Apps werden nicht auf dem aktuellen Stand gehalten, wodurch die Anfälligkeit für Hackerangriffe steigt.

Leitfaden sicherer Einsatz von Smartphones. Was muss ich konkret tun?

Mit den nachfolgenden Basis-Sicherheitsmaßnahmen können Sie sensible Daten auf dem Smartphone wirksam vor Angreifern schützen. Wenn Sie die nachfolgende Checkliste durchgehen, kennen Sie Ihren aktuellen Sicherheitsstatus, denn alle Maßnahmen sollten umgesetzt sein oder sollten bei der Nutzung beachtet werden.

Checkliste Sicherheit bei Smartphones.

Sicherheitsmaßnahme	Umgesetzt / Beachtet  (Ja/Nein)
Sie haben eine Gerätesperre mit mindestens 6-stelligen Code aktiviert? (Mit dem Code wird auch die Verschlüsselung auf aktuellen Smartphones aktiviert.)	
Sie haben die Einstellungen aktiviert, dass nach einer fünfmaligen Fehleingabe alle Daten gelöscht werden?	
Sie halten Betriebssystem und Apps stets auf dem aktuellen Stand und spielen Updates regelmäßig und zeitnah ein?	
Sie geben Passwörter und PINs am Smartphone stets unbeobachtet ein?	
Sie rufen unbekannte Nummern nicht zurück? (Insbesondere ist Vorsicht geboten bei SMS oder Anrufnummern aus dem Ausland. Mit solchen Nummern wird oft Gebührenbetrug begangen. Das kann sehr schnell teuer werden.)	
Sie lassen das Smartphone zum Schutz vor Verlust oder Diebstahl nicht aus den Augen?	
Sie wenden sich im Falle eines Verlusts oder Diebstahls des Smartphones unverzüglich an Ihren IT-Support und lassen das Gerät sperren sowie alle Daten aus der Ferne löschen?	
Sie führen eine direkte Kopplung mit anderen Geräten zum Austausch von Daten - etwa über Bluetooth oder USB- nur bei vertrauenswürdigen Partnern durch? (So vermeiden Sie, dass Ihr eigenes Gerät manipuliert oder mit Schadsoftware infiziert wird. Dies gilt auch für das Laden Ihres Smartphones an einer öffentlichen Ladestation.)	
Sie installieren nur Apps aus vertrauenswürdigen Quellen? (App-Stores der Hersteller, Google Playstore, Apple App-Store).	
Sie lassen Verbindungen zu Ihrem Smartphone nur mittels eines starken Kennwortes zu? (Persönlicher Hotspot, Bluetooth).	
Sie nutzen unterwegs stets Hotspots, die eine verschlüsselte Verbindung anbieten? Andernfalls greifen Sie auf keine sensiblen Daten zu oder übertragen keine solche Daten? (Passwörter können z.B. bei solchen offenen WLANs leicht abgefangen werden.)	
Sie löschen alle Daten auf Ihrem Smartphone (Reset) bevor Sie dieses in Reparatur geben?	

Sie speichern keine Unternehmensdaten incl. Fotos auf privaten Cloudspeichern? (Google Drive, DropBox, OneDrive, iCloud usw.).	

Drei Goldene Datenschutzregeln für Smartphones. Was muss ich dazu wissen?

Über die Basis-Sicherheitsmaßnahmen hinaus sind die nachfolgenden 3 goldenen Regeln für mehr Datenschutz im Umgang mit Smartphones zu beachten.

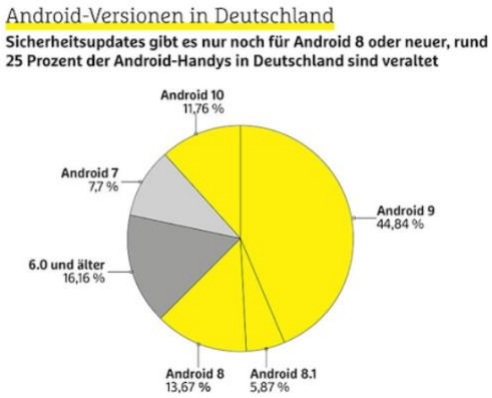
1.) Wenn Sie das Gerät ausnahmsweise an andere Personen vorübergehend weitergeben, lassen Sie das Smartphone möglichst nicht aus den Augen. Ein Schadprogramm ist schnell aufgespielt.
2.) Wenn Sie Anwendungen installieren, sollten Sie diesen nur die Rechte einräumen, die unbedingt erforderlich sind. Die 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 Sie weder installieren noch ausführen.
3.) Geschäftliche und private Daten müssen möglichst getrennt gespeichert werden. Nutzen Sie getrennte E-Mail-Postfächer (privat und dienstlich) und getrennte Datenverzeichnisse. Am einfachsten können Sie sich an dieser Stelle schützen, wenn Sie die private Nutzung auf ein notwendiges Maß reduzieren und so wenig persönliche Daten speichern wie möglich.

Fazit

Die Nutzung des Smartphones bietet Ihnen die Chance auch mobil flexibel und effektiv zu arbeiten. Diese Flexibilität hat Ihren Preis. Nur wenn Sie die Risiken kennen, können Sie diese minimieren. Mit dem vorliegenden Leitfaden haben Sie die wesentlichen Informationen zum sicheren Einsatz Ihres Smartphones zur Hand und können diesen auch regelmäßig kontrollieren. So sind Sie auch mobil stets auf der sicheren Seite.

Das müssen Sie konkret bei Android Smartphones beachten.

Beim Neukauf eines Handys ist auch die Betriebssystem-Version ein Kaufargument. Das gilt gerade beim Kauf sehr günstiger Modelle aus Altbeständen oder gar von Gebrauchthandys. Ein paar gesparte Euros können Sie teuer zu stehen kommen. Und: Falls das Betriebssystem eines neuen Handys (noch) nicht aktuell ist, erkundigen Sie sich, ob und bis wann der Hersteller ein Update geplant hat.



Werden Sie als Anwender selbst aktiv.

Die verschiedenen Sicherheits-Maßnahmen von Google sind zwar alle in Ordnung. Doch am Ende des Tages zählt nicht, was auf dem Papier steht, sondern was auf den einzelnen Handys wirklich eingestellt ist. Das prüfen und verbessern Sie in drei großen Schritten:

1.) Android-Version prüfen

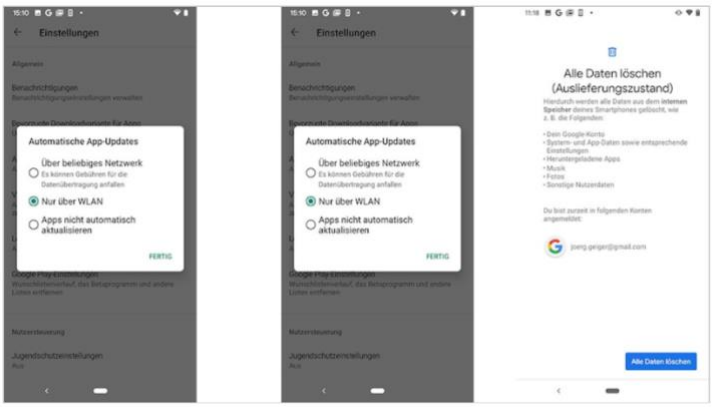
Nicht jeder Nutzer hat stets die Hand am Android-Puls, im Gegenteil, es ist eher selten, dass man die genaue Android-Version parat hat. Doch die kann man einfach prüfen: Öffnen Sie dazu auf dem Smartphone die App »Einstellungen» und tippen Sie unten - je nach Version - auf »System« oder »Mein Gerät«. Über »Erweitert« und/oder »Systemupdate« können Sie die Android-Version und den Stand der Sicherheitsupdates ablesen. Mit Android 8 oder höher sind Sie derzeit noch halbwegs auf der sicheren Seite, denn dann liefert Google noch regelmäßig Updates. Doch Vorsicht, vielleicht bremst ja auch Ihr Hersteller. Das Datum bei »Stand der Sicherheitsupdates« sollte nicht weiter als einige Wochen zurückliegen. Sollte es eine neue Android-Version oder ein Sicherheitsupdate für Ihr Handy geben, können Sie von dieser Stelle aus das Update anstoßen.

2.) Sicherheitsupdates einspielen

Sicherheitsupdates sollten eigentlich immer automatisch eingespielt werden, das erfolgt aber nicht zwingend. Ist Ihr Handy nicht auf dem aktuellsten Stand, können Sie in den »Einstellungen« unter »Sicherheit« beziehungsweise »Sicherheitsstatus« oder »Updates für System-Apps« nachsehen, ob Updates verfügbar sind. Auf manchen Geräten wird hier zwischen Sicherheitsupdates und Google-Play-Systemupdates unterschieden. Folgen Sie beiden Wegen und spielen Sie entsprechend verfügbare Updates ein. Wichtig: Trotz aktueller Android-Version ist es nicht gesagt, dass die Hersteller alle Patches weiterreichen. Ein Motorola Moto G5 mit Android 8.1 ist zum Beispiel im Januar 2020 auf dem Patch-Level von Februar 2019. Beim Thema Update sind Sie leider generell weitgehend abhängig vom Hersteller Ihres Smartphones. Wie schon gesagt, sollte man schon deshalb vor dem Kauf nach den Updatepläne des Herstellers für ein bestimmtes Modell fragen.

3.) Verschlüsselung prüfen

Smartphones sind kleine, leichte Geräte, die leicht gestohlen werden können oder auch mal verloren gehen. Für diesen Fall sollten Sie vorsorgen. Eine Geräteverschlüsselung macht Ihre Handydaten für Dritte unlesbar. Sie prüfen die Geräteverschlüsselung in den »Einstellungen« unter »Sicherheit«, bei manchen Android-Versionen heißt der entsprechende Punkt auch »Sicherheit & Standort« oder liegt unter »Google« im Bereich »Sicherheit« versteckt. Unter »Verschlüsselung & Anmeldedaten« sehen Sie, ob der interne Speicher verschlüsselt ist. Falls nicht, können Sie die Verschlüsselung dort aktivieren.



Die App "Einstellungen" ist die Anlaufstelle für wichtige Sicherheitsoptionen. Hier können Sie Displaysperren definieren (links), Updateoptionen festlegen (Mitte) oder Handydaten löschen (rechts).

Auch die Apps sollten Sie im Auge behalten.

Bisher haben wir nur Android selbst ins Visier genommen. Doch eine Vielzahl an Bedrohungen geht auch von Apps aus. Diese vier Maßnahmen beugen möglichen Gefahren vor:

1.) App-Updates automatisch einspielen

App-Updates können zwar in Ausnahmefällen auch Probleme machen, in der Regel verbessern sie aber die bereits installierten Apps auf Ihrem Smartphone. Gefixt werden dabei Bugs und es gibt ganz nebenbei oft auch noch neue Funktionen. Sämtliche App-Updates laufen über den Play Store, wenn Sie keine alternative App-Quelle nutzen. Dementsprechend finden Sie in der Play-Store-App auf dem Handy auch die Einstellungsmöglichkeiten. Tippen Sie in der App auf das Dreistrich-Menü oben links und dann auf »Einstellungen«. Dort aktivieren Sie »Automatische App-Updates«. Wenn Sie Ihre mobile Datenflat schonen wollen, wählen Sie »Nur über WLAN« aus.

2.) Unnötige Apps entfernen

Auf manchen Handys stapeln sich die Apps bis unter die Decke. Gegen das Ausprobieren von Apps spricht erst mal nichts, doch jede App bietet im Grunde eine gewisse Angriffsfläche, ganz abgesehen vom belegten Speicherplatz und der mangelnden Übersicht. Wenn Sie also bestimmte Apps nicht (mehr) nutzen, ist es keine schlechte Idee, sie zu löschen. Das geht ebenfalls über die Play-Store-App und das Dreistrich-Menü. Tippen Sie dort auf »Meine Apps und Spiele«. Schauen Sie die Liste der installierten Apps (unter dem Reiter »Installiert«) alle paar Wochen durch, und wenn Sie einen Löschkandidaten gefunden haben, tippen Sie auf die App und danach auf »Deinstallieren«.

3.) Tracker vor der Installation aufspüren

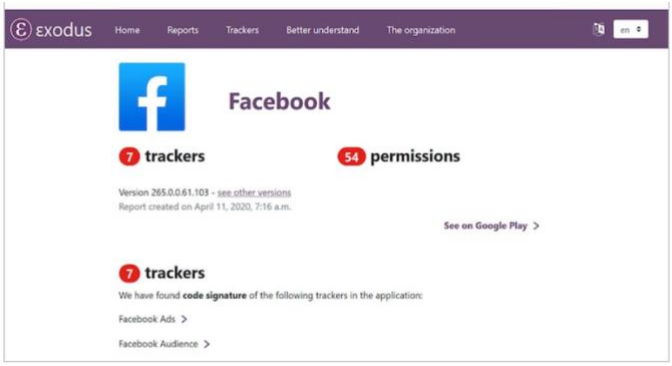
Ein Problem ist, dass man neuen Apps vor der Installation nicht ansieht, ob sie womöglich schädlichen Code enthalten. Trotzdem kann und sollte man die Berechtigungen vor der Installation prüfen. Da gibt es zwei gute Möglichkeiten:

Wählen Sie auf der Play-Store-Seite der fraglichen App »Über diese App«. Dann ganz nach unten scrollen und auf »App-Berechtigungen« tippen.

Über die Webseite von Exodus Privacy, einer Non Profit Organisation können Sie Apps vorab und kostenlos auf eingebaute Tracker prüfen lassen. Dazu genügt es, die URL der

Play-Store-Seite ins Suchfeld zu kopieren und auf »Perform Analysis» zu klicken. Im Ergebnisbericht sind potenziell gefährliche Einstellungen mit Ausrufezeichen markiert, also auch ohne große Fremdsprachen- und IT-Kenntnisse zu identifizieren.

4.) Berechtigungen installierter Apps ändern



Exodus Privacy analysiert Apps bevor Sie selbst sie installieren und liefert detaillierte Informationen. Die Facebook-App unterstützt sieben externe Tracker und hat an 54 Stellen Zugriff auf das Android-System.

Welche Berechtigungen sich bereits installierte Apps herausnehmen, können Sie wieder leicht über die »Einstellungen« Ihres Handys prüfen. Tippen Sie auf »Apps & Benachrichtigungen«. Wählen Sie die App aus, die Sie prüfen wollen, und tippen Sie auf »Berechtigungen«. Sie können in der Übersicht festlegen, welche Berechtigungen die App haben soll, zum Beispiel könnten Sie Chrome den Standortzugriff erlauben oder verbieten.

An diesen Stellschrauben können Sie noch drehen - 10 schnelle Tipps.

Die mobile Sicherheit hängt nicht nur von der verwendeten Android-Version ab oder davon, ob die richtigen Security-Tools im Einsatz sind. Genauso wichtig ist, wie Sie den Zugang zu Ihrem Mobilgerät sichern, auf welchen Wegen die Kommunikation läuft und manchmal kommt es einfach darauf an, wie der Handy-Nutzer sich im Alltag verhält.

1. Zugriffsschutz verstärken: Verschärfen Sie die Displaysperre auf Ihrem Handy

Zugriff auf Ihr Handy sollte nur eine Person haben, Sie selbst. Besonders gilt das, wenn Ihr Handy gestohlen wird. Zwischen Ihren persönlichen Daten und dem Dieb steht dann nur eine PIN. Sie sollten diesen Schutz verschärfen: Zunächst sollten Sie Kombinationen wie »1234« oder »0000« nicht verwenden. In den Einstellungen unter »Sicherheit« beziehungsweise »Sicherheit & Standort« in früheren Android-Versionen können Sie die PIN für die Displaysperre auch auf acht statt vier Stellen verlängern. Noch sicherer sind alphanumerische Passwörter. Wichtig auch: Unbedingt auf das Zahnrad daneben tippen und die »Automatische Sperre« aktivieren.

2. Sicher am Hotspot: Nutzen Sie ein VPN

Anders als in vielen Werbebotschaften präsentiert, macht Sie ein VPN (Virtual Personal Network) nicht unsichtbar. Doch das sollte auch nicht der Grund für seinen Einsatz sein. Sie können mit einem VPN auch ein unsicheres Netz wie einen Hotspot sicher nutzen. Der Einstieg könnte das kostenlose ProtonVPN sein. Der Nachteil: Es bietet nicht die volle Geschwindigkeit. Wer häufig einen VPN-Dienst nutzt, sollte zum Bezahl-Abo greifen. Für zwei Geräte verlangt ProtonVPN ca. 4 Euro pro Monat.

3. Passwörter im Griff mit Passwort-Manager

Eine Basis-App auf jedem Handy sollte ein Passwortmanager sein. Der merkt sich alle Passwörter für Sie, speichert alles in einem verschlüsselten Datensafe und erlaubt den Zugang nur über ein Masterpasswort. In Zukunft müssen Sie sich also nur noch ein einziges Passwort merken und der Rest kommt vom Passwortmanager. Zwei Optionen gibt es dafür: Entweder Sie nutzen einen Passwortdienst wie LastPass oder Sie verwenden einen lokalen Passwortmanager. KeePass ist unter Windows eine gute Lösung, das Android-Pendant dazu ist Keepass2Android.

ProtonVPN schützt Sie vor unerlaubten Systemzugriffen durch Dritte. Für die uneingeschränkte Nutzung der App wird allerdings ein Monatsbeitrag fällig.

4. Vorausschauend handeln: Handy orten lassen.

Falls das Handy verschwunden ist, wäre eine Ortungsfunktion schön. Daran müssen Sie aber auf jeden Fall vorher denken: In den Einstellungen steuern Sie dafür den Punkt »Sicherheit« beziehungsweise »Sicherheit & Standort« an und schalten »Mein Gerät finden« ein. Orten können Sie ein abhandengekommenes Handy auf verschiedenen Wegen. Sind Sie in Chrome mit Ihrem Google-Konto angemeldet, reicht eine Google-Abfrage mit »Handy suchen«. Google bietet Ihnen dann die Smartphone-Ortung als ersten Treffer an. Alternativ steuern Sie im Browser einfach android.com/find an. Auf diesem Weg können Sie Ihr Handy auch klingeln lassen, fernsperren und sogar ganz einfach löschen.

5. Seriennummer des Geräts notieren

Findet man ein verlorenes Handy weder per Ortung noch durch ehrliche Finder wieder, bleibt der Gang zu Polizei. Doch bei einer Anzeige reicht es nicht aus, nur das Handymodell anzugeben. Hier müssen Sie die IMEI parat haben, die International Mobile Station Equipment Identity. Das ist eine 15-stellige Seriennummer, die jedes Handy eindeutig identifiziert. Geben Sie "*#06#" statt einer Telefonnummer in Ihre Handy-App, erscheint die IMEI. Die Polizei Nordrhein-Westfalen bietet auf ihrer Webseite auch einen Handypass zum Download oder Ausdrucken an. Dort können Sie zusätzlich weitere nützliche Daten dokumentieren.

6. Schnittstellen abschalten: WLAN und Bluetooth nur bei Bedarf

WLAN und Bluetooth dürften die meisten Nutzer regelmäßig verwenden. Da ist es natürlich komfortabel, diese Schnittstellen immer eingeschaltet zu lassen. Sicherer ist es aber, sie nur bei Bedarf zu aktivieren. Über die Schnelleinstellungen von Android klappt das auch ganz einfach. Wischen Sie vom oberen Displayrand nach unten und tippen Sie die Symbole für WLAN und Bluetooth an, um sie zu deaktivieren.

7. Kontakt vermeiden: Handy nicht an fremde PCs anschließen

Es ist gar keine so schlechte Idee, das Handy ab und zu an den eigenen Computer anzuschließen, etwa für schnelle Backups. Doch an einem fremden Rechner hat Ihr Smartphone nichts verloren. Ein infizierter PC könnte zur Bedrohung für ein angeschlossenes Smartphone werden.

8. Daten sparen: Mobile Webseiten statt Apps

Es gibt heute für so ziemlich alles eine App, die braucht man aber nicht für jeden Kram. Besonders bei Diensten, die man nicht so häufig nutzt, sind auch mobile Webseiten eine Option. Der Vorteil: Die Möglichkeiten für Tracking sind begrenzt. Probieren Sie also mal statt einer App einfach die mobile Webseite des Anbieters aus. Damit sind Sie beim ersten Zugriff sogar schneller.

9 Virenscanner ja oder nein?

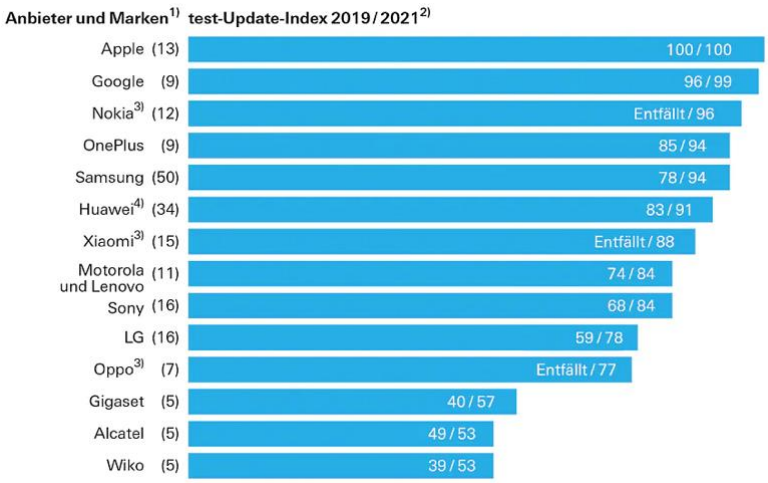
Ein Muss wie unter Windows ist ein Virenscanner unter Android nicht. Mit Play Protect werden die Apps im Play Store ohnehin von einer Automatik auf Schädlinge gecheckt. Wer nur Standard-Apps verwendet, braucht keinen Extraschutz. Trotzdem ist die Bedrohung für Android real und wer gerne Apps aus verschiedenen Quellen ausprobiert, sollte über einen Zusatzschutz nachdenken. Trend Micro Mobile Security ist der derzeitige Testsieger bei Android-Virenscannern.

10. Vor dem Wechsel: Handy-Daten sicher löschen

Es kommt der Tag, an dem selbst das treueste Handy ausgemustert wird. Doch nachdem Sie das neue Smartphone erfolgreich in Betrieb genommen haben, sollten Sie die Daten auf dem alten löschen. Ist das Smartphone verschlüsselt, reicht ein System-Reset über die »Einstellungen«. Trennen Sie aber vorher die Verknüpfung zum Google-Konto unter »Konten«.

Updateversorgung von Smartphones. Das sollten Sie wissen.

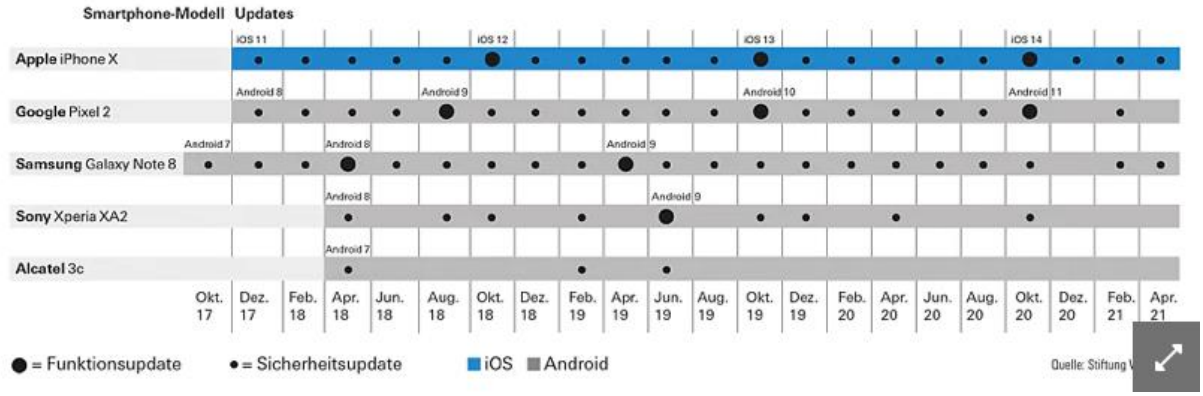
Apple versorgt seine Handys nach wie vor am zuver-lässigsten mit Updates. Die Anbieter von Android-Handys haben sich gegen-über dem Test von 2019 verbessert, doch es gibt weiter große Unterschiede: Google liegt vorn, gefolgt von Nokia, das bei den meisten Modellen die System-Variante „Android One“ nutzt.



In Klammern: Anzahl der in die Unter-suchung 2021 einbezogenen Modelle des jeweiligen Anbieters. Der Index bewertet, wie oft, wie lange und mit welcher Art von Updates die Anbieter ihre Geräte versorgen

Smartphone-Updates im Vergleich.

Während Apple sein iPhone X wie alle iPhones regelmäßig aktualisiert, sieht der Update-Verlauf für verschiedene Android-Handys sehr unterschiedlich aus. Googles Pixel 2 bekam seit Ende 2017 drei neue Android-Versionen und regel-mäßige Sicherheitsupdates, das Alcatel 3c kein großes Funktions- und nur drei kleine Sicherheits-updates.



Aktuelle Sicherheitslücke bei Android. Das müssen Sie prüfen.

Eine schwere Sicherheitslücke bei Bluetooth auf Android-Smartphones haben Sicherheitsforscher der Firma ERNW entdeckt. Betroffen von der Schwachstelle sind die Android-Versionen 9.0 bis 8.0 sowie möglicherweise älter. Das berichtet unter anderem "Inside Digital". Die wichtigste Nachricht vorab: Wer sein Android-Gerät auf die neueste Systemversion 10.0 updatet, kann die Schwachstelle schließen und ist vor Angriffen sicher. Alle anderen Nutzer mit älteren Android-Versionen sollten hingegen dringend das neueste Update vom Februar 2020 installieren.

Bei der entdeckten Sicherheitslücke können Kriminelle und Hacker laut den Sicherheitsforschern von ERNW Schadcode theoretisch auf Millionen Smartphones spielen, wenn Bluetooth aktiviert ist. Dafür ist kein Datenaustausch nötig. Hacker müssten nur das Bluetooth-Zielgerät ausfindig machen. Für einen potenziellen Angriff muss lediglich die Bluetooth-Mac-Adresse des Geräts bekannt sein.

Persönliche Daten von Android-Nutzern abgreifbar

Diese Sicherheitslücke kann anschließend eine Malware – also ein Virus – ins System einschleusen und so persönliche Daten abgreifen oder die VPN konfigurieren beziehungsweise nutzen, wie "Inside Digital" berichtet. Wie beschrieben wurde die Schwachstelle in Android 8.0 bis 9.0 entdeckt. **Alle Nutzer sollten daher dringend das am 3. Februar 2021 veröffentlichte Sicherheitsupdate für Android installieren, um die Schwachstelle zu schließen. Das gilt auch für Nutzer mit noch älteren Systemversionen als 8.0.**

Was Android-Nutzer sonst tun können:

Sie sollten Bluetooth nur aktivieren, wenn dies unbedingt erforderlich ist. Beachten Sie, dass die meisten Bluetooth-fähigen Kopfhörer auch kabelgebundenes analoges Audio unterstützen, man die Bluetooth-Verbindung also auch deaktivieren kann.

Lassen Sie Ihr Gerät nicht auffindbar für andere Bluetooth-Geräte. Die meisten Handys sind nur erkennbar, wenn man das Bluetooth-Scan-Menü aufruft. Einige ältere Telefone sind jedoch möglicherweise dauerhaft erkennbar.

Fazit:

Android Smartphones, die eine Android Version älter als 8 haben und von Seiten des Herstellers nicht mehr mit Sicherheitspatches versorgt werden, sind angreifbar. Solche Smartphones tragen für den Nutzer ein hohes Sicherheitsrisiko. Sie sollten auf solchen Smartphones keine sensiblen Daten speichern und auch kein Onlinebanking nutzen. Wenn Sie dennoch den vollen Funktionsumfang dieser Smartphones nutzen möchten, sollten Sie unbedingt ein Antivirenprogramm nutzen und sehr vorsichtig mit der Installation von Apps sein. Installieren Sie ausschließlich Apps, die Sie tatsächlich benötigen und schränken Sie deren Rechte auf das notwendige Maß ein.

Mit Apple Geräten sind Sie in der Regel stets auf dem neuesten Stand, wenn Sie die bereitgestellten Sicherheitsupdates tatsächlich installieren. Prüfen Sie regelmäßig in den Einstellungen, ob es Sicherheitsupdates gibt und installieren Sie diese zeitnah. Stellen Sie automatische Updates ein.

Wählen Sie bei Ihrem nächsten Kauf eines Smartphones einen Hersteller aus, der einen langen Updatezeitraum zusichert. Hier sind mindestens 4 Jahre zu fordern.

Sicherheit gibt es nicht zum Nulltarif. Das gilt auch für Smartphones. Denn billige Smartphones werden eben nicht mit Updates versorgt und gebrauchte Smartphones sind oftmals zu alt, um noch Updates zu erhalten.

Mit Apple Geräten sind Sie was das Thema Sicherheit angeht stets auf der „sicheren Seite“. Das schlägt sich jedoch auch im Preis nieder.