Sicherheitseinstellungen für Tablets

Android

Co-financed by the European Union
Connecting Europe Facility

Saferinternet.at
Das Internet sicher nutzen!

ispa
Internet Service Providers Austria

Inhaltsverzeichnis

Schutz gegen unbefugte Nutzung	3
System-Updates des Geräteherstellers	7
Synchronisierung & regelmäßige Sicherungskopien (Backups)	8
Datenschutzeinstellungen für Apps einrichten	9
Jailbreak, Root und gesperrte Tablets	16
Kostenfalle In-App-Käufe	17
WLAN und Bluetooth	18
Datenverschlüsselung	19
Verkaufen, Verschenken & Verborgen	20
Tablet-Finder: finden oder sperren	21
Das kindersichere Tablet	22

Hinweis: Je nach Hersteller Ihres Android-Geräts können die genauen Bezeichnungen für einzelne Einstellungen bzw. deren Position im Menü unter Umständen von der Darstellung in diesem Leitfaden abweichen. Die Funktionen sind allerdings bei den meisten Geräten vorhanden. Konsultieren Sie im Zweifelsfall die Dokumentation des Herstellers.

Impressum:

ISPA – Internet Service Providers Austria, Währinger Straße 3/18, 1090 Wien
Dachverband der österreichischen Internetwirtschaft

5. aktualisierte Auflage.
Wien, September 2017
Redaktion: Barbara Piller, Moritz F. Fürst
Endgerät: Samsung Galaxy Tab S3
Betriebssystem: Android 7.0

Android und Google Play sind eingetragene Marken von Google Inc., USA. Samsung Galaxy und Samsung Galaxy Tab S3 sind eingetragene Marken von Samsung Electronics Co., Ltd, Südkorea.

Gefördert durch die Europäische Union – Safer Internet Projekt. Alle Angaben erfolgen ohne Gewähr. Eine Haftung der Autorinnen und Autoren, durch die ISPA, das Projekt Saferinternet.at oder die Europäische Union ist ausgeschlossen.

Schutz gegen unbefugte Nutzung

Wie das Smartphone ist auch das Tablet für die meisten Menschen zu einem sehr personalisierten Gerät mit hoch sensiblen Informationen geworden. Persönliche Daten wie z. B. das Adressbuch mit allen Kontakten, Fotos, Social Media Apps oder private und geschäftliche E-Mail-Accounts sind ein „best of" all jener Daten, die unser Leben bestimmen. Eine wichtige Sicherheitsvorkehrung zum Schutz dieser Informationen besteht darin, durch Einrichtung einer Passwortabfrage (Bildschirmsperre) unbefugten Zugriff auf das Gerät und die darauf gespeicherten Informationen zu unterbinden.

Es ist ratsam, eine Bildschirmsperre zu verwenden – es erscheint zwar zeitaufwendig jedes Mal aufs Neue den Code einzugeben, trägt aber beachtlich zum Schutz des Tablets bzw. der darauf gespeicherten Daten bei. Je nach Nutzungsgewohnheiten kann die Sperrzeit individuell festgelegt werden – von einer automatischen Bildschirmsperre nach 10 Sekunden bis hin zu mehreren Minuten.

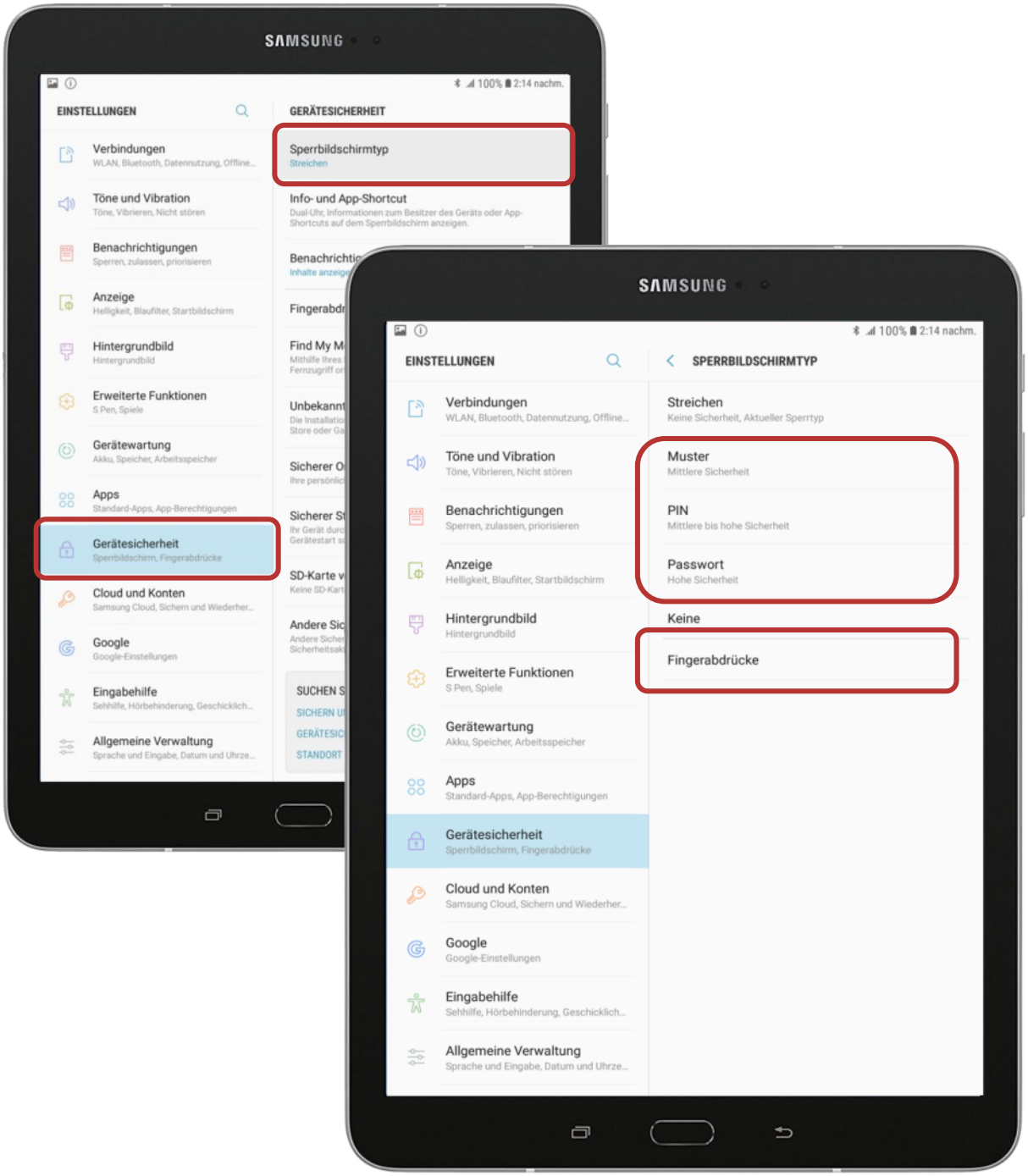
Bei der Bildschirmsperre von Android-Tablets gibt es für gewöhnlich mehrere Möglichkeiten:

- Musterentsperrung
- PIN-Eingabe
- Passwort-Eingabe
- Fingerabdruckscanner
- Gesichtserkennung (Face Unlock)

Egal für welche Methode man sich entscheidet: Es sollte darauf Acht gegeben werden, dass die Eingabe des Entsperrmusters oder –codes unauffällig erfolgt. Viele Sicherheitsangriffe sind überraschend trivial, eine weit verbreitete Methode ist etwa das Abschauen oder Abfotografieren von Zugangsdaten und Passwörtern oder deren Eingabe. Besonders auf öffentlichen Plätzen, in dicht gedrängten Verkehrsmitteln oder bei neugierigen Sitznachbarn im Flugzeug sollten Nutzerinnen und Nutzer vorsorglich achtsam sein.

Display-Sperre bei Android-Tablets einrichten

Einstellungen – Gerätesicherheit – Sperrbildschirmtyp



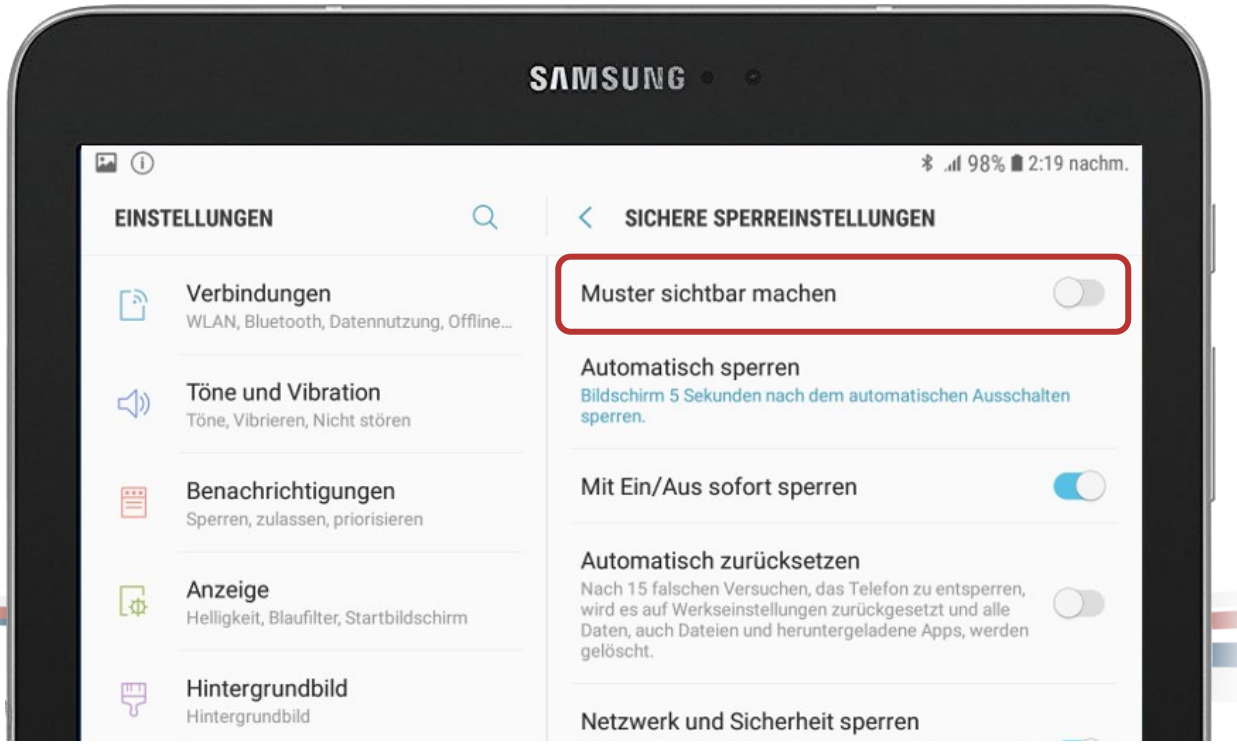
Die PIN-Eingabe ist der Klassiker beim Passwortschutz. Je nach Schwierigkeitsgrad der Zahlenkombination bietet sie mittlere bis hohe Sicherheit. Die Pin sollte aus mindestens 4 Stellen und nicht mehr als 17 Stellen bestehen. Geburtstage oder 1234 als Zahlenkombination sollten vermieden werden, da diese zu

leicht zu erraten sind. Die Passworteingabe weist die höchste Sicherheitsstufe auf, besonders wenn eine Zahlen-, Buchstaben- und Sonderzeichenkombination verwendet wird. Um „komplizierte" Passwörter nicht zu vergessen, bieten sich die Anfangsbuchstaben eines einprägsamen Merksatzes an. Beispielsweise ergäbe sich das Passwort „ImÄ&b1970g" aus dem Merksatz „Ich mag Äpfel & bin 1970 geboren". Wichtig: Das gleiche Passwort sollte bei anderen Diensten nicht nochmals verwendet werden, da man es so potentiellen Angreifern einfach macht, mit nur einem Passwort auf mehrere Konten zuzugreifen.

Die Musterentsperrung ist eine sehr beliebte Methode zum Schutz des Endgerätes. Die Musterentsperrung bewegt sich als Sicherheitsvorkehrung im mittleren Bereich, da diese leicht beobachtet oder nachvollzogen werden kann. Das Muster wird meistens auf einer 4 x 4-Punkte-Matrix als Verbindungslinie von mindestens vier Punkten festgelegt. Zum Entsperren muss auf dem Touch-Display die vorher festgelegte Linie nachgefahren werden. Einige Tablets bieten zusätzlich die Möglichkeit, das Muster beim Entsperren des Geräts nicht sichtbar zu machen (die Verbindungslinien nicht anzuzeigen). Diese Einstellung sollte unbedingt gewählt werden, da sie es für Fremde erschwert, das Muster zu erkennen.

Muster bei Mustersperre unsichtbar machen

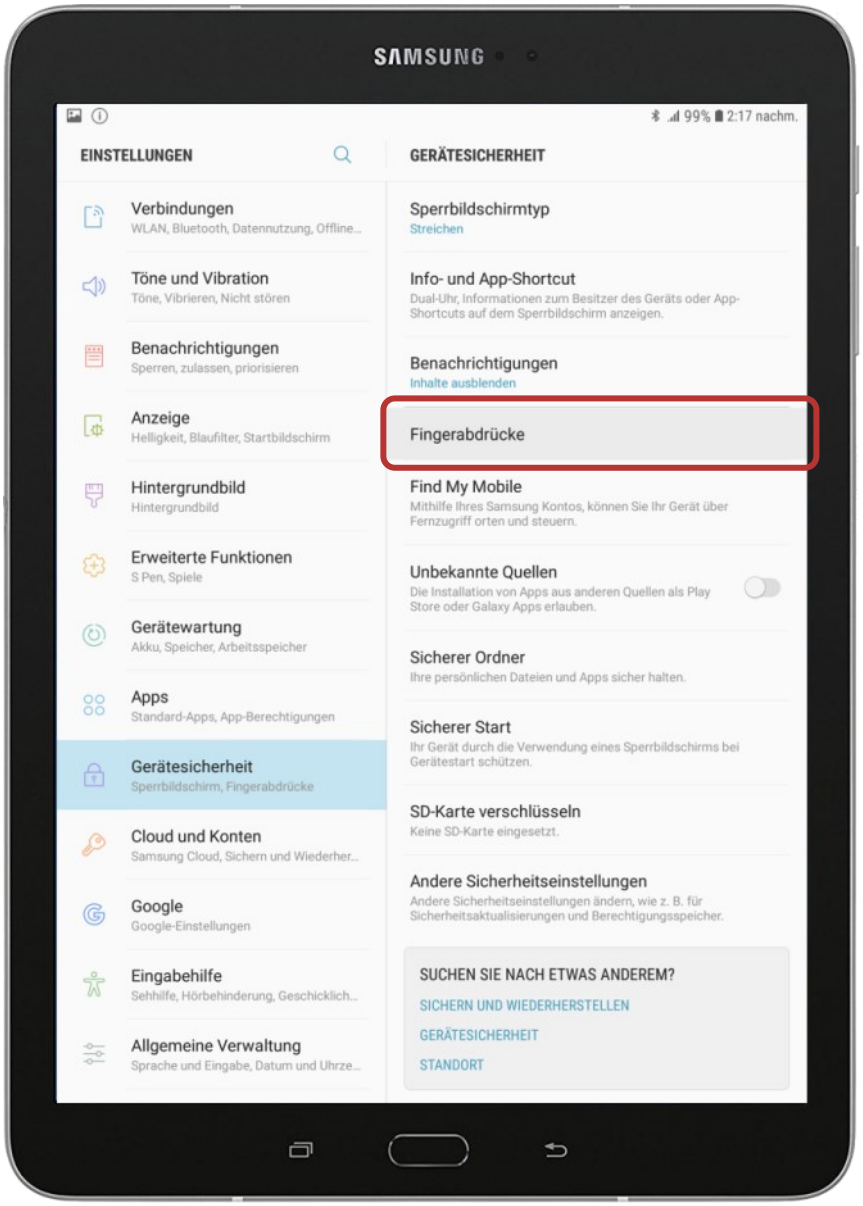
Einstellungen – Gerätesicherheit – Sichere Sperreinstellungen – „Muster sichtbar machen" deaktivieren



Fingerabdruckscanner einrichten

Manche Tablets bieten einen Fingerabdruck-Scanner an, der allerdings auch keinen absoluten Schutz bietet. Um diese Art der Entsperrung nutzen zu können, muss vorab eine andere Display-Sperre eingerichtet werden. Dies ist notwendig, sollte der Fingerabdruck einmal nicht erkannt werden.

Einstellungen – Gerätesicherheit – Fingerabdrücke

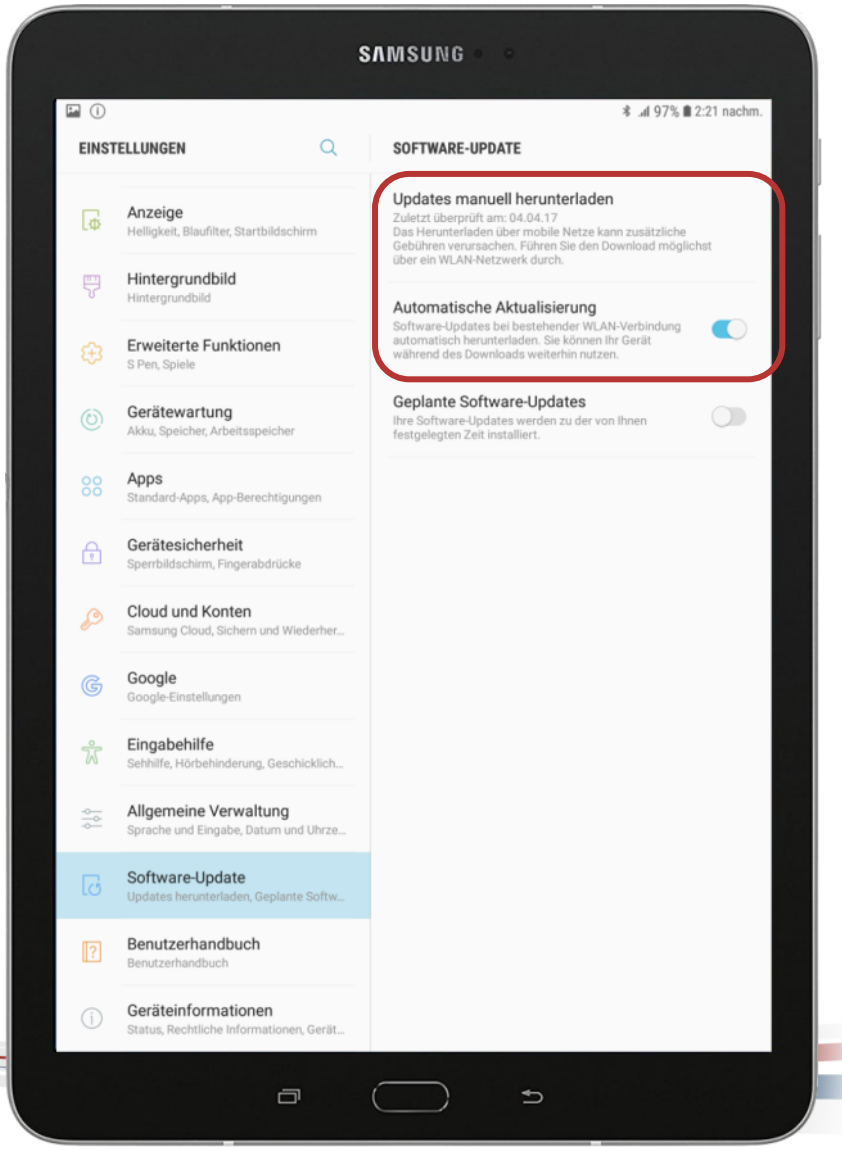


System-Updates des Geräteherstellers

Die vom Hersteller empfohlenen System-Updates sollten unbedingt durchgeführt werden, denn Updates enthalten kleine Systemverbesserungen: Sie reparieren Fehler oder schließen eventuelle Sicherheitslücken. Die Hersteller haben, sobald sie Kenntnis über ein (Sicherheits-) Problem bei einem ihrer Produkte erlangen, großes Interesse, umgehend zu reagieren und versuchen schnell eine Lösung des Problems zu erarbeiten. Die meisten Tablets haben eine Funktion, die automatisch auf System-Aktualisierungen überprüft. Sollte keine automatische Aktualisierung eingerichtet sein, sollte das Sicherheits-Update möglichst zeitnah nach der Veröffentlichung installiert werden. (Sicherheitslücken sind sehr gut dokumentiert und können von unbefugten Personen für eigene Angriffe schnell ausgenützt werden).

Software-Updates

Einstellungen – Software-Update



Synchronisierung & regelmäßige Sicherungskopien (Backups)

Genau wie bei einem PC ist es auch bei einem Tablet notwendig, regelmäßig Sicherungskopien durchzuführen. Im Falle eines Daten- oder Geräteverlusts kann so auf das Backup zugegriffen werden und zumindest der letzte Stand der gesicherten Daten ist verfügbar.

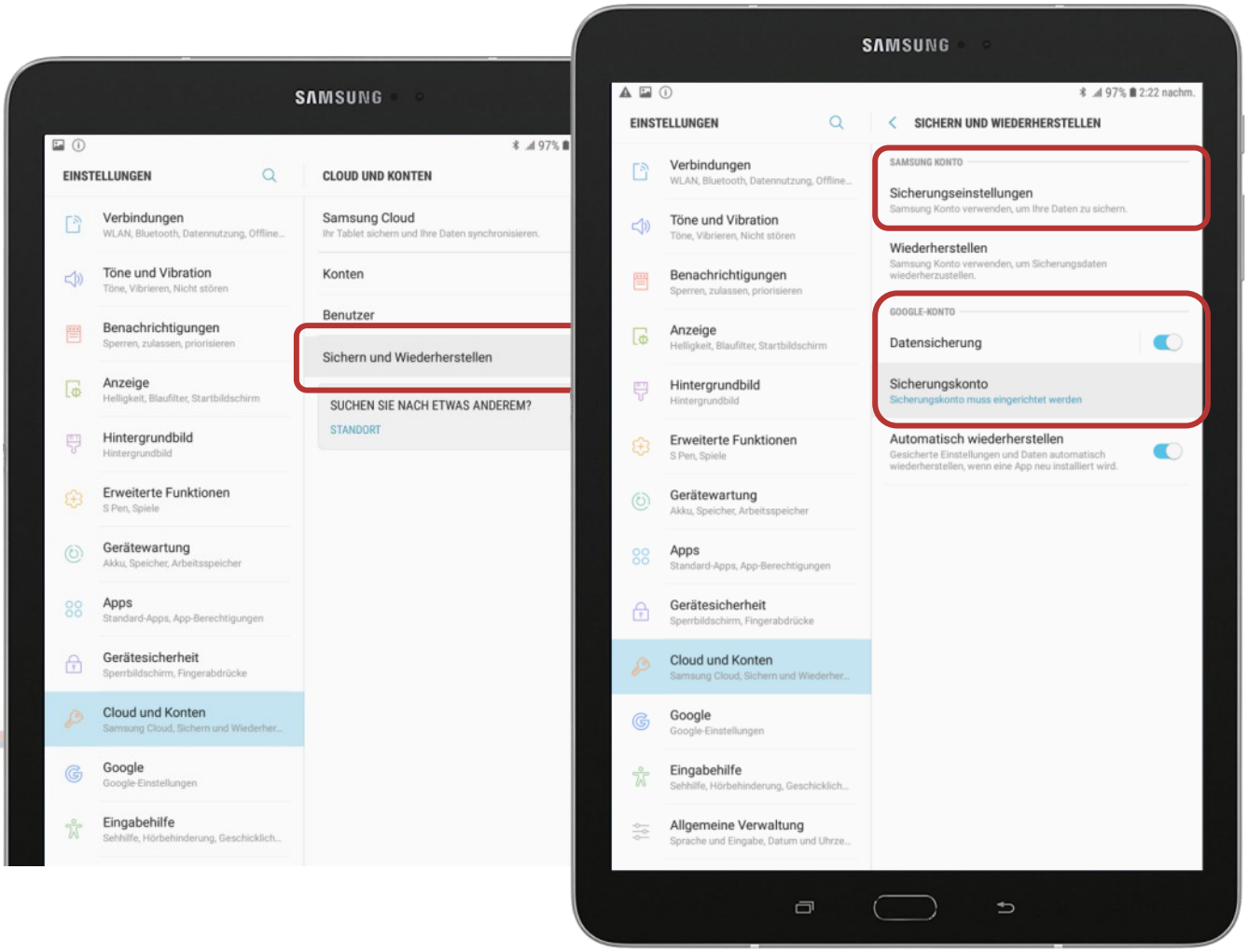
Hierfür können beispielsweise die Daten per USB-Kabel auf den PC übertragen werden. Ebenso gibt es die Möglichkeit, der Synchronisation und Datensicherung mittels eines Cloud-Dienstes. Dabei sollten allerdings Datenschutz und -sicherheit bedacht werden.

Daten vom Tablet auf PC übertragen

Das Tablet per USB-Kabel mit dem PC verbinden. Das Gerät erscheint als Wechseldatenträger im Dateimanager (Explorer).

Datensicherung mittels Cloud-Diensten von Samsung oder Google

Einstellungen – Cloud und Konten – Sichern und Wiederherstellen – Sicherungseinstellungen bzw. Sicherungskonto



Datenschutzeinstellungen für Apps einrichten

Moderne Tablets verfügen über zahlreiche Sensoren (z. B. Mikrofon, Kamera, GPS-Empfänger), sind häufig mit dem Internet verbunden und speichern jede Menge persönliche Daten - diese Informationen können nicht nur mittels gezielter Angriffe bzw. durch physischen Zugriff auf das Tablet, sondern auch durch auf dem Gerät installierte Software in unbefugte Hände gelangen. Wenn beim Kauf und Download von Apps ein paar wenige Punkte beachtet werden, kann jedoch das Sicherheitsrisiko minimiert werden.

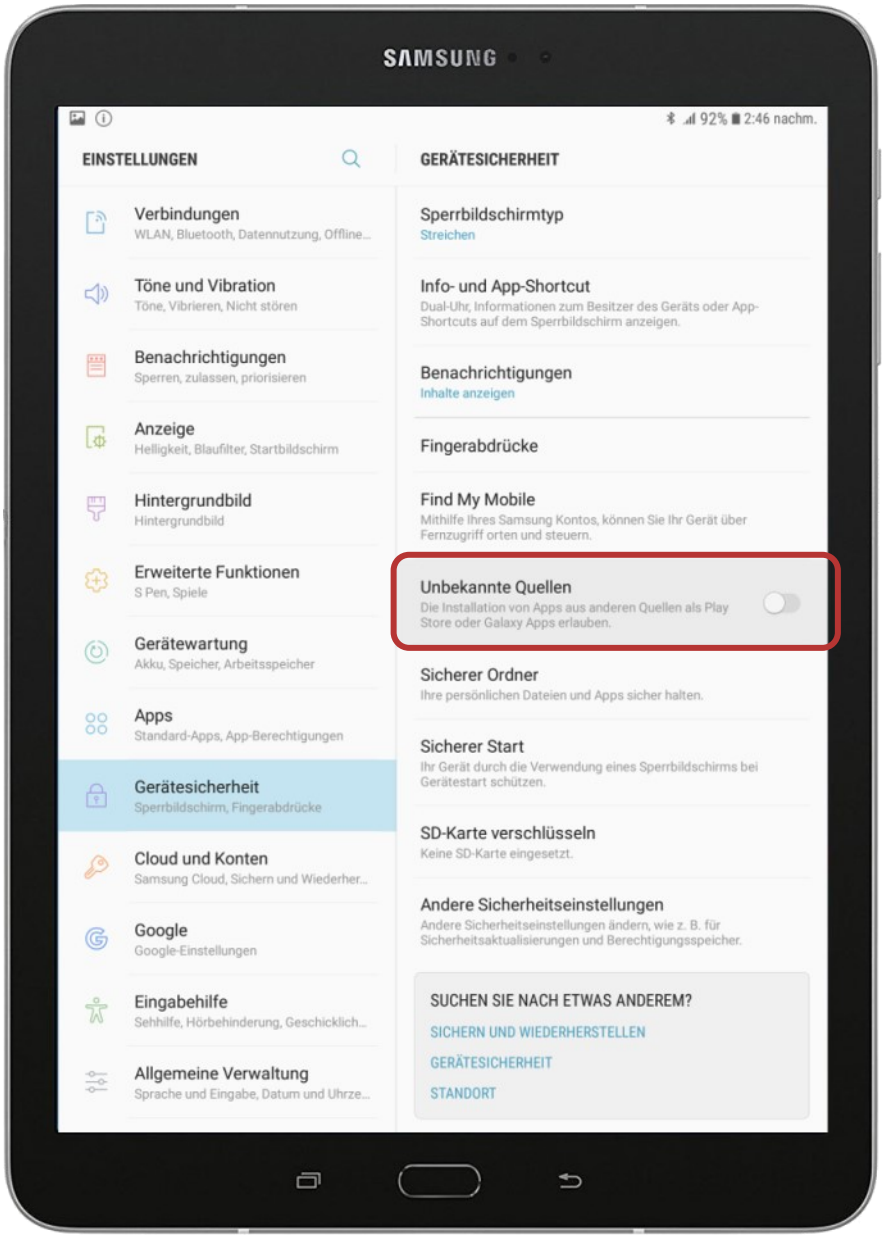
Apps nur aus den offiziellen App-Stores beziehen

Um sich vor Schadsoftware zu schützen, sollten Apps von Drittanbietern nur aus dem Google Play Store bzw. dem „Galaxy Apps"-Verzeichnis von Samsung geladen werden. Diese müssen nämlich ein Testverfahren durchlaufen, bevor sie zum Download verfügbar sind und auf dem Gerät installiert werden können. Auch dieses Verfahren kann naturgemäß keinen absoluten Schutz garantieren, solange aber nur Apps aus offiziellen Stores geladen werden und Nutzerinnen und Nutzer grundlegende Sicherheitsregeln beachten (Vorsicht bei E-Mail-Anhängen etc.), ist das Tablet vor der unachtsamen Installation von Schadsoftware relativ sicher. Die Möglichkeit der Installation von Apps aus anderen Quellen als dem Play Store lässt sich vollständig deaktivieren.

Beim Google Play Store kann zudem in den Einstellungen der „Filter für Inhalte" aktiviert werden. Hier wird über eine Inhaltsfilterung der Zugriff auf Apps beschränkt, die heruntergeladen werden können (z. B. Apps, welche Standortdaten der Nutzerinnen und Nutzer sammeln).

Sperre von Apps aus anderen Quellen als Play Store oder Galaxy Apps

Einstellungen – Gerätesicherheit – „Unbekannte Quellen" abwählen



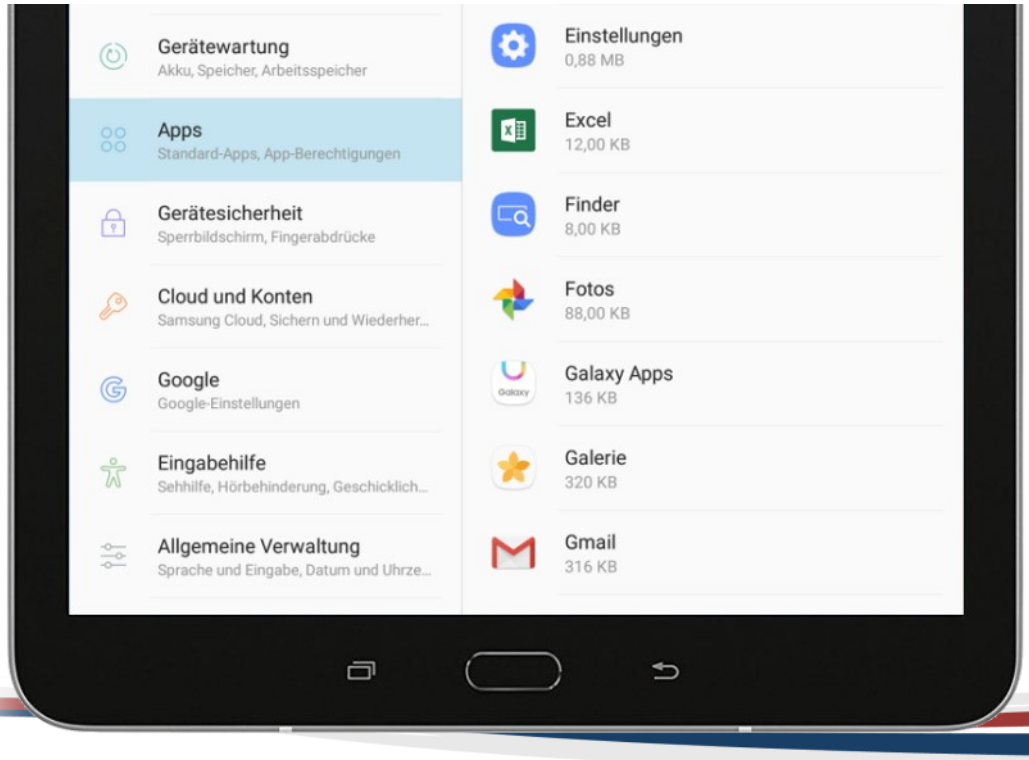
Nicht allen App-Zugriffsberechtigungen zustimmen

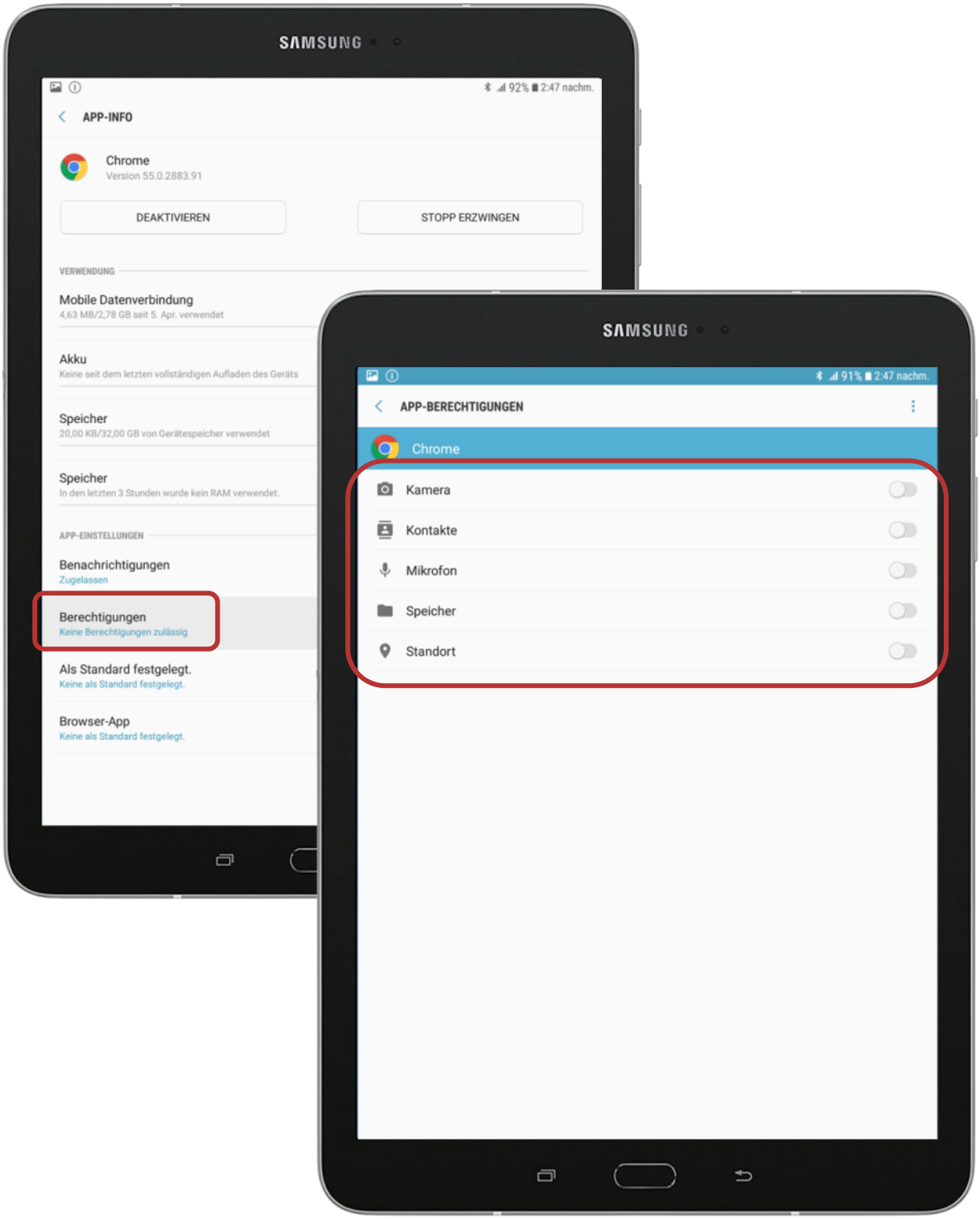
Vor der endgültigen Installation einer App muss deren Zugriffsberechtigungen zugestimmt werden. Hier sollten Nutzerinnen und Nutzer vorsichtig sein und nur dann zustimmen, wenn diese Zugriffsrechte notwendig erscheinen. Bösartige Apps machen sich hier die Unachtsamkeit der Userinnen und User zu Nutze und fordern Berechtigungen, die einerseits nicht notwendig sind und andererseits das Tablet und die Daten angreifbar machen.

Nutzerinnen und Nutzer sollten bewusst auswählen, welche Daten sie welcher App zur Verfügung stellen wollen. Handelt es sich zum Beispiel um eine Spiele-App, braucht diese eher keinen Zugriff auf das Telefonbuch; dass eine Navigations-App Zugriff auf die GPS-Daten benötigt, macht wiederum Sinn. Nutzerinnen und Nutzer sollten sich hier die Frage stellen, warum sie einer App Zugriff zu Daten gestatten sollten, wofür staatliche Einrichtungen in der Regel eine richterliche Anordnung brauchen.

App-Berechtigungen verwalten

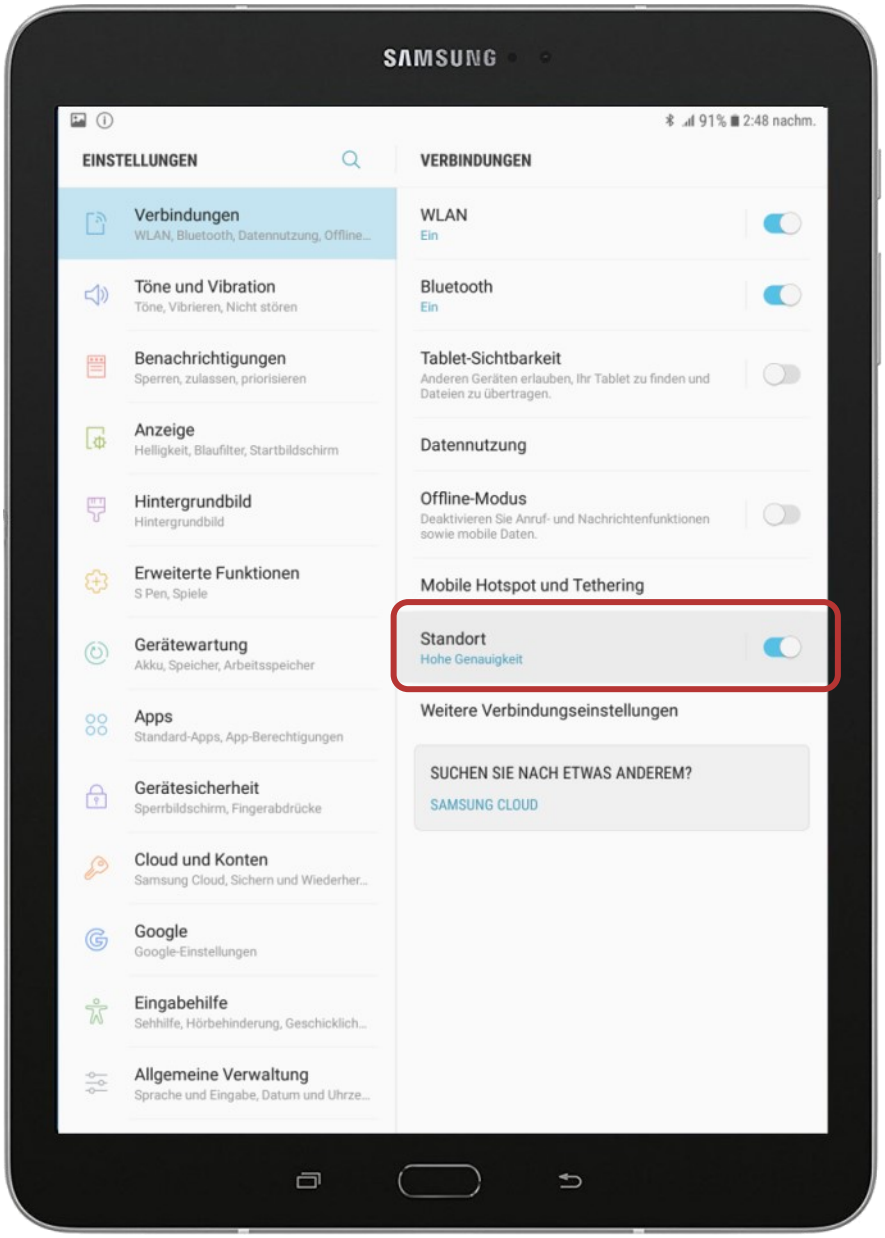
Einstellungen – Apps – die jeweilige App auswählen – Berechtigungen – nicht benötigte Berechtigung abwählen




SAMSUNG
92% 2:47 nachm.
APP-INFO
Chrome
Version 55.0.2883.91
DEAKTIVIEREN
STOPP ERZWINGEN
VERWENDUNG
Mobile Datenverbindung
4,63 MB/2,78 GB seit 5. Apr. verwendet
Akku
Keine seit dem letzten vollständigen Aufladen des Geräts
Speicher
20,00 KB/32,00 GB von Gerätespeicher verwendet
Speicher
In den letzten 3 Stunden wurde kein RAM verwendet.
APP-EINSTELLUNGEN
Benachrichtigungen
Zugelassen
Berechtigungen
Keine Berechtigungen zulässig
Als Standard festgelegt.
Keine als Standard festgelegt.
Browser-App
Keine als Standard festgelegt.
SAMSUNG
91% 2:47 nachm.
APP-BERECHTIGUNGEN
Chrome
Kamera
Kontakte
Mikrofon
Speicher
Standort

Deaktivierung von GPS-Daten-Übermittlung

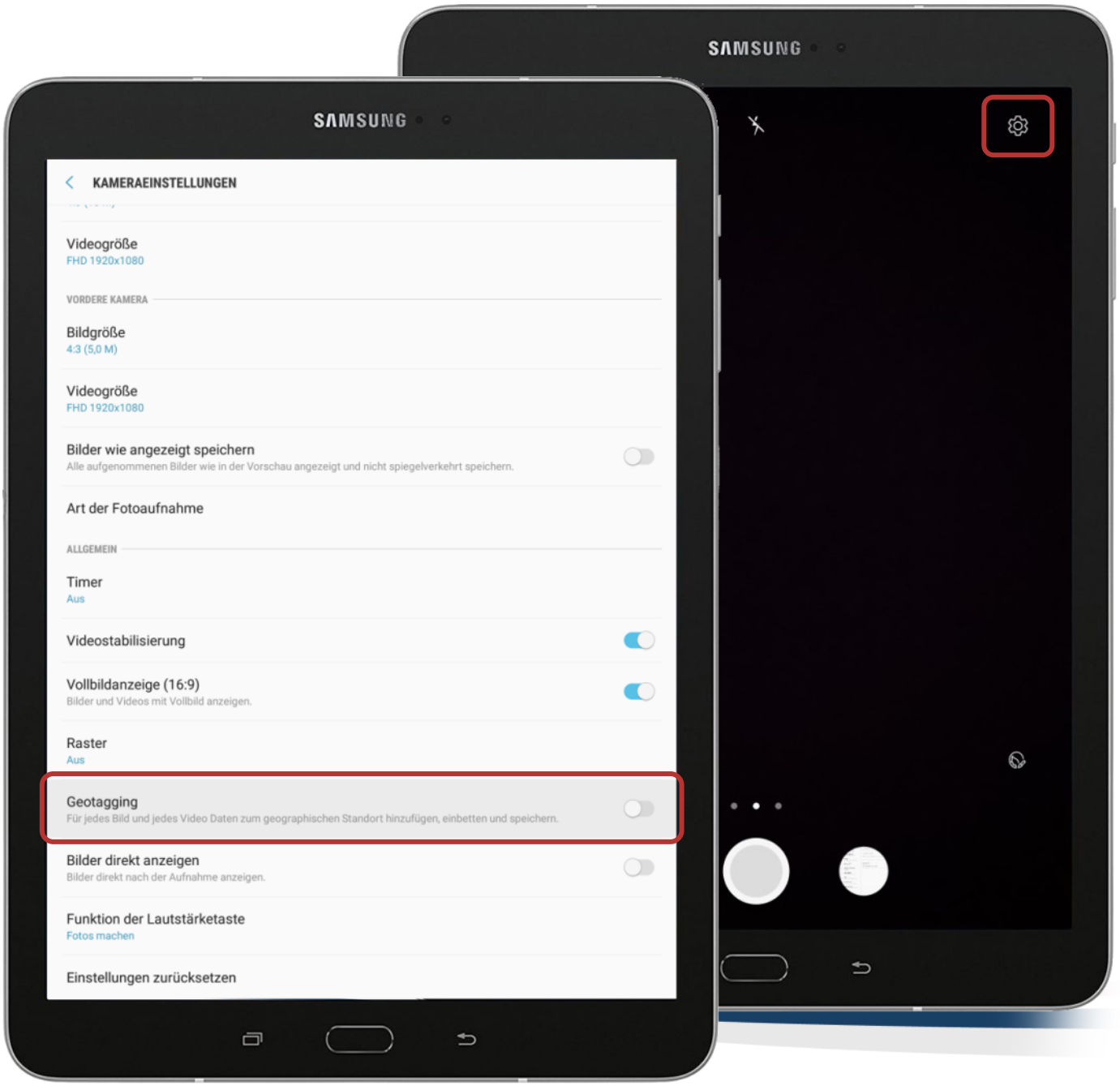
Einstellungen – Verbindungen – Standort



Deaktivierung des Geo-Taggings bei Fotos

Achtung: Bei einigen Tablets reicht es aber nicht, lediglich die allgemeine Positionsdatenübermittlung zu deaktivieren. Auch wenn diese abgedreht ist, kann es dennoch sein, dass weiterhin der eigene Aufenthaltsort bekannt gegeben wird: und zwar beim Aufnehmen und Versenden von Fotos („Geo-Tagging"). Ein Geo-Tag ist das automatische Einbetten des Standorts zum Zeitpunkt der Aufnahme in die Fotodatei.

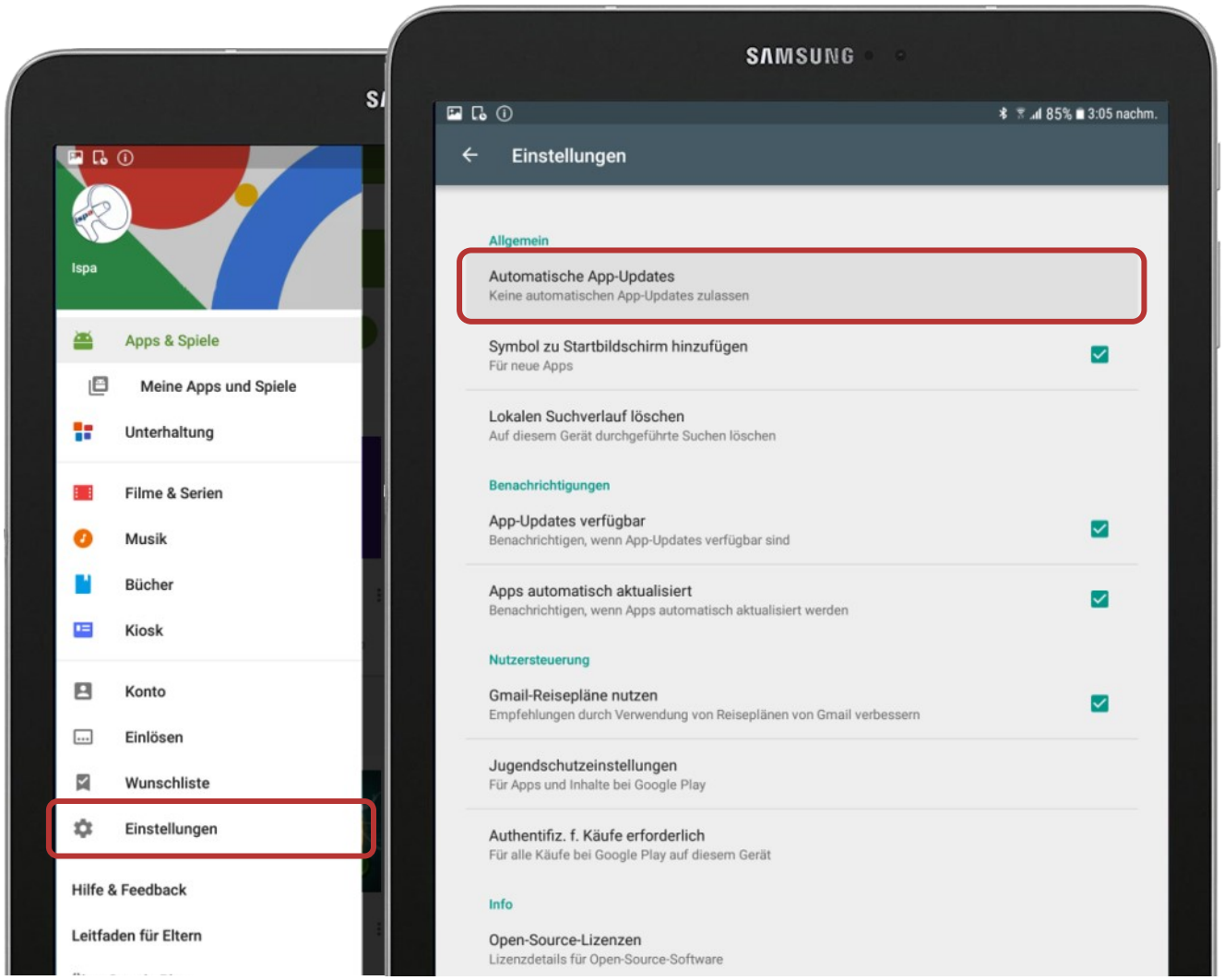
Die Kamera öffnen – Einstellungen (rechts oben) – „Geotagging" abwählen



Keine automatischen App-Aktualisierungen & nur WLAN für Aktualisierungen

Die automatische App-Aktualisierung sollte deaktiviert werden. Werden App-Updates ausgerollt, kann es durchaus sein, dass beispielsweise weitere oder neue Nutzungsrechte von der App verlangt werden. Es empfiehlt sich, zumindest überblicksartig die Updates im Blick zu haben. Möchten Nutzerinnen und Nutzer das tun, gleichzeitig aber nicht manuell nach neuen App-Updates suchen müssen, sollte die „Benachrichtigungsfunktion" aktiviert werden. Diese informiert, wenn ein neues Update bereitsteht. Entscheiden sich Nutzerinnen und Nutzer trotzdem für die automatische Aktualisierung, sollte die Funktion „nur über WLAN" aktiviert werden, ansonsten können solche Hintergrundaktualisierungen das eigene Datenvolumen strapazieren und im schlimmsten Fall Zusatzkosten verursachen.

Google Playstore – nach rechts swipen – Einstellungen – „Automatische App-Updates" abwählen



Jailbreak, Root und gesperrte Tablets

„Jailbreaking" oder „Rooten" ist das inoffizielle Entsperren von Software und Hardware, meint in den meisten Fällen aber das Entsperren von Smartphones und Tablets. „Root" ist vergleichbar mit einem Administratorkonto, welches volle Zugriffs- und Schreibrechte hat und über welches somit das gesamte System verändert werden kann. Das birgt potentielle Sicherheitsrisiken. Für die meisten Nutzerinnen und Nutzer ist es daher ratsam, auf solche Maßnahmen zu verzichten.

Achtung: Durch den Jailbreak und das Rooten können die Betriebssysteme der Tablets beeinträchtigt oder sogar beschädigt werden. Ebenso können nach dem Jailbreak oder dem Rooten Software-Updates des Geräteherstellers nicht mehr so einfach eingespielt werden. Ungeübte Nutzerinnen und Nutzer können auch Opfer von falschen Jailbreak-Programmen oder von Schadsoftware werden. Zudem fällt das Jailbreaking und Rooten in eine rechtliche Grauzone und kann unter Umständen die Garantie des Geräts beeinträchtigen!

Beim „Rooten" überwiegen daher für die meisten Nutzerinnen und Nutzer die Risiken einen etwaigen Nutzen. Es ist für gewöhnlich sinnvoller, darauf zu verzichten.

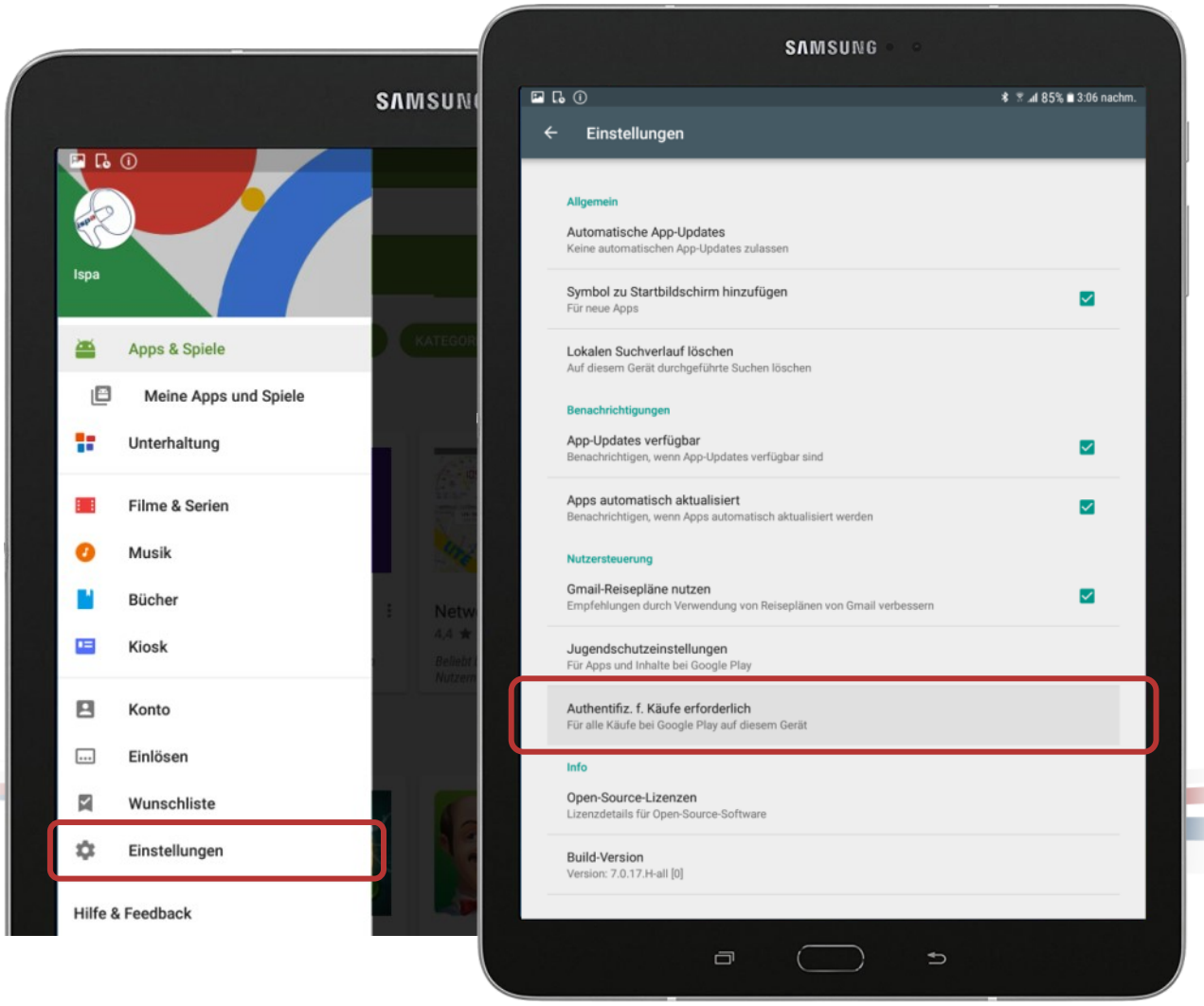
Kostenfalle In-App-Käufe

Bei manchen Apps (z. B. Spielen) besteht die Möglichkeit, in den Anwendungen Guthaben oder Punkte zu kaufen, ohne den klassischen Bestellvorgang zu durchlaufen („In-App-Käufe"), wodurch die Gefahr, unbeabsichtigt Geld auszugeben, steigt. In-App-Käufe können zu einer unvorhergesehenen Kostenfalle werden: Besonders Kindern und Jugendlichen ist es oft nicht bewusst, dass sie auf ein kostenpflichtiges Angebot klicken, wenn sie zum Beispiel zusätzliches Spielguthaben erwerben, um in einem Spiel schneller voranzukommen.

Bei Android gibt es hier die Funktion der „Authentifizierung für Käufe". Ist diese aktiviert, müssen Nutzerinnen und Nutzer bei jedem Kaufvorgang den entsprechenden Code zur Bestätigung eingeben.

Authentifizierung für App-Käufe

Google Playstore – nach rechts swipen – Einstellungen – „Authentifizierung für Käufe erforderlich"



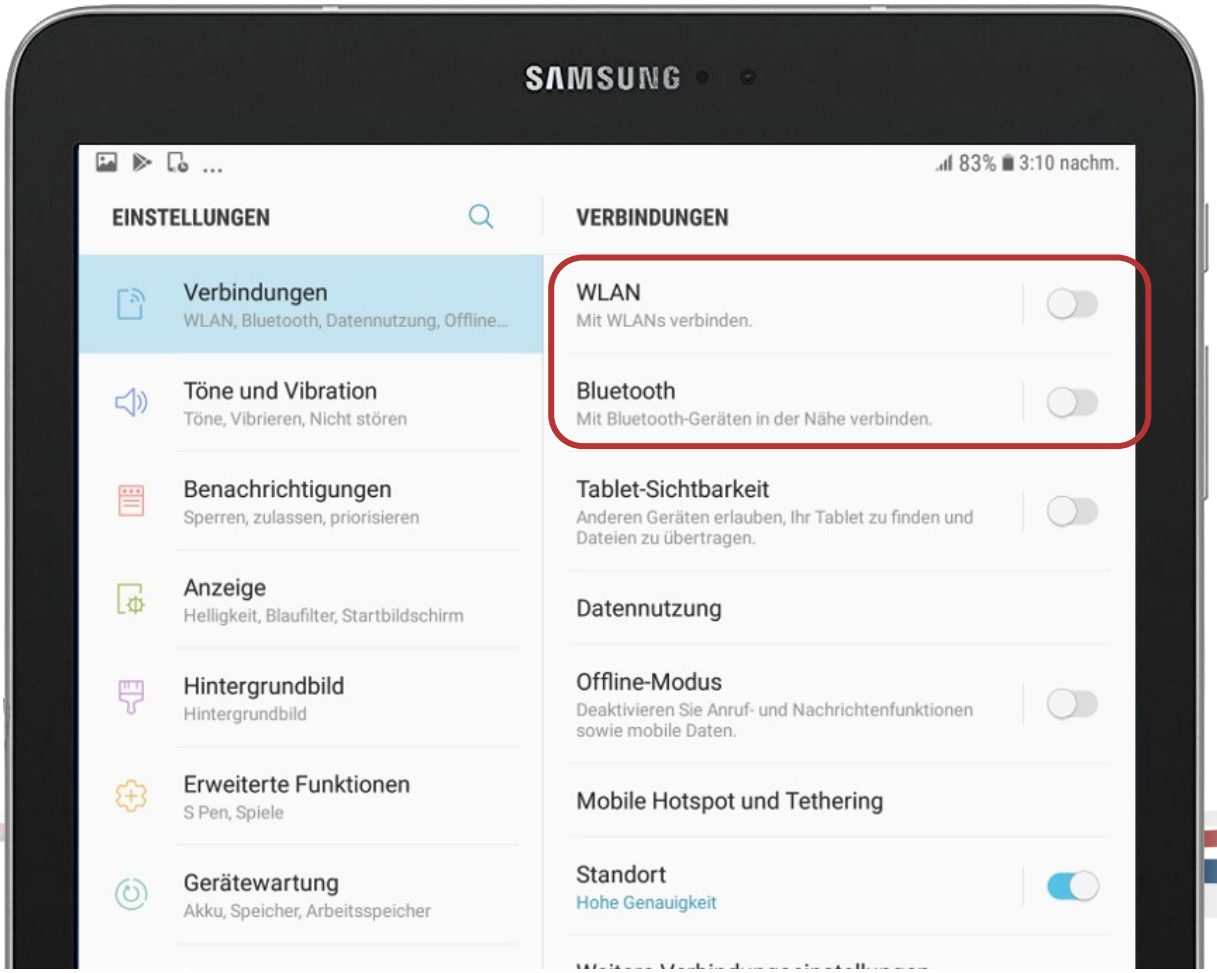
WLAN und Bluetooth

„Home is where your wifi connects automatically."

Wenn sich das Tablet selbstständig im Büro oder daheim mit dem WLAN verbindet, ist das praktisch und bequem, aber auf Dauer ein Sicherheitsrisiko. Der Datenaustausch über WLAN oder Bluetooth ist oft nur mangelhaft gesichert und kann relativ leicht ausspioniert werden. Die WLAN- und Bluetooth-Funktion sollte nur dann eingeschalten werden, wenn auf ein lokales WLAN-Netzwerk zugegriffen werden soll oder die Bluetooth-Funktion unmittelbar benötigt wird. Ein angenehmer Nebeneffekt dieser einfachen Sicherheitsvorkehrung ist außerdem ein stark reduzierter Stromverbrauch.

WLAN und Bluetooth deaktivieren

Einstellungen – Verbindungen – WLAN bzw. Bluetooth. Alternativ ist durch eine Swipe-Geste vom oberen Bildschirmrand der Schnellzugriff auf diese Einstellungen über das Notification Center möglich.



Datenverschlüsselung

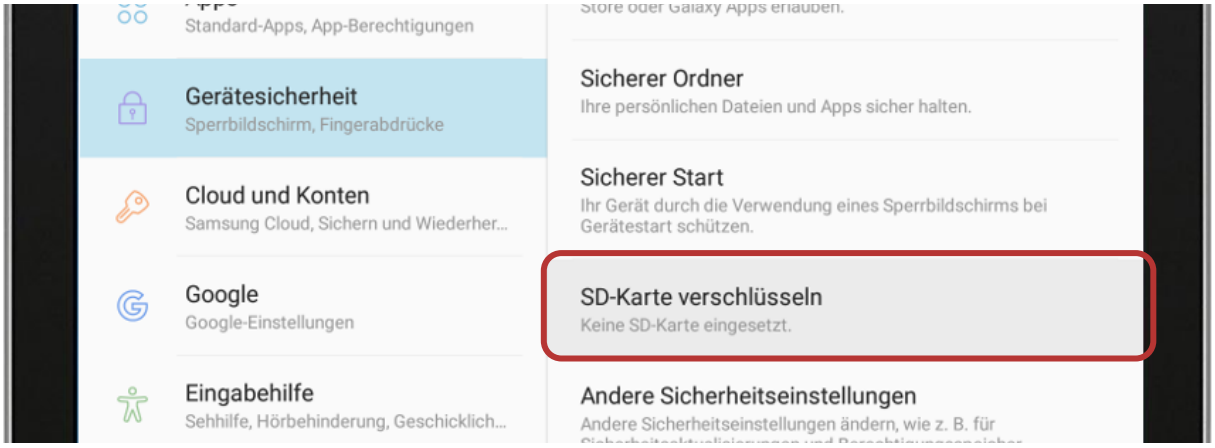
Viele Android-Tablets bieten die Funktion der Datenverschlüsselung für die Micro-SD-Karte – wenn eine im Gerät eingesetzt und in Verwendung ist. Damit können Daten, welche extern – also auf der Micro-SD-Karte – gespeichert sind, zusätzlich geschützt werden. Hier gibt es oftmals die Möglichkeit, die gesamte Speicherkarte oder auch nur einzelne Inhalte zu verschlüsseln.

Sollen die Daten noch besser vor Missbrauch geschützt werden, kann eine Datenverschlüsselung für alle Tablet-Inhalte angedacht werden. Diese Option wird jedoch nicht von allen Geräten unterstützt. Wird das Tablet gestohlen oder geht verloren, sind Konten, Einstellungen, Apps, Musik und Videos nur mit einem vorher festgelegten PIN-Code einsehbar. Die Passwortabfrage zur Entschlüsselung erfolgt bei jedem Einschalten des Gerätes zusätzlich zur SIM-Codesperre.

Achtung: Die Verschlüsselung kann nicht rückgängig gemacht werden. Die Verschlüsselung kann nur aufgehoben werden, wenn das Gerät auf den Werkzustand zurückgesetzt wird, wodurch die Daten gelöscht werden.

Verschlüsselung der SD-Karte

Einstellungen – Gerätesicherheit – SD-Karte verschlüsseln



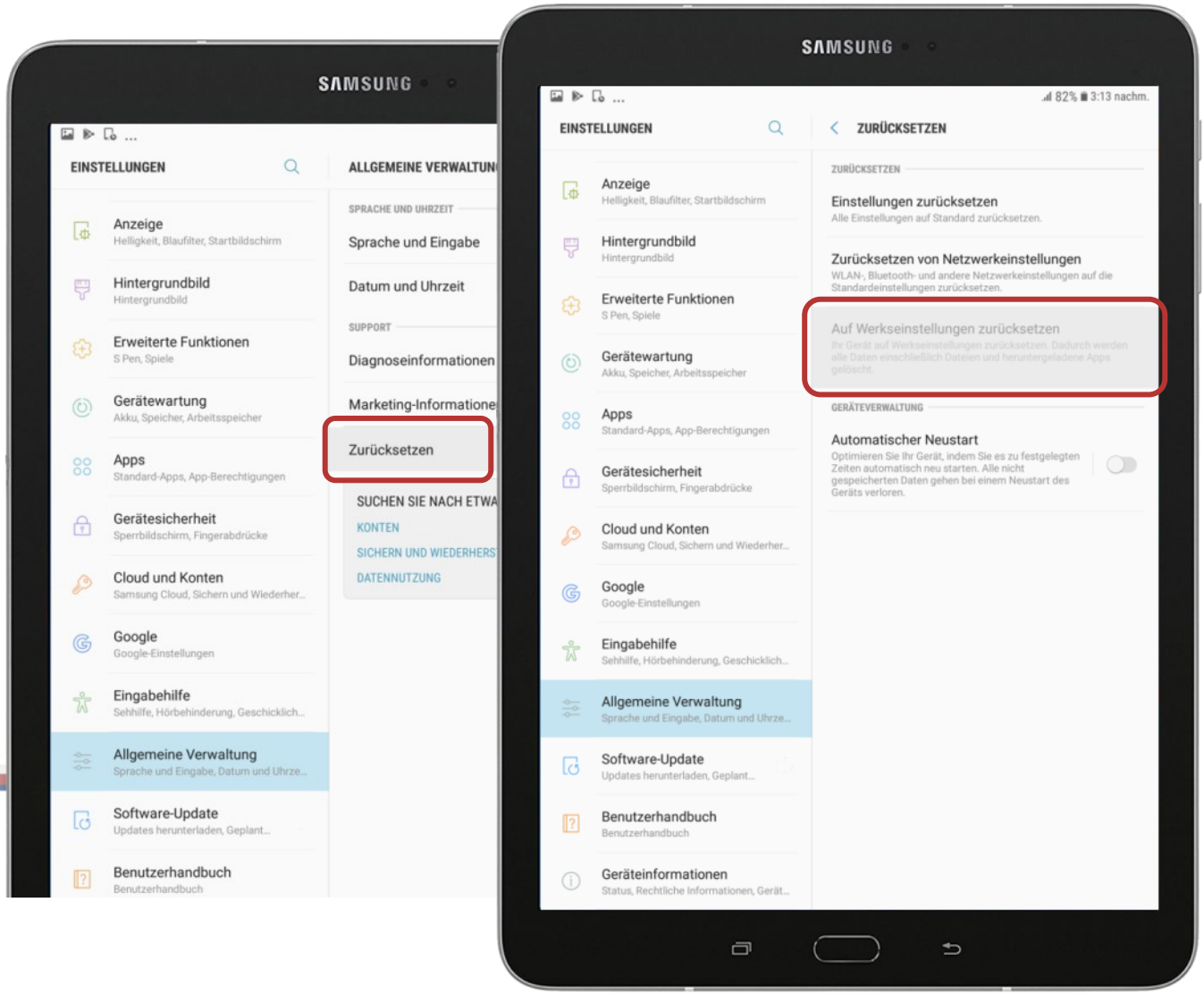
Verkaufen, Verschenken & Verborgen

E-Mails, Urlaubsfotos, Login-Daten für Facebook & Co: Auf dem Tablet sind sehr viele persönliche Daten gesammelt. Soll das Gerät weitergegeben oder verkauft werden, sollte es unbedingt auf den Werkzustand zurückgesetzt und alle Daten gelöscht werden.

Um die Weitergabe persönlicher Daten zu verhindern, sollten der Speicher des Tablets sowie die SD-Karte nach Möglichkeit vollständig zurückgesetzt werden. Hierfür reicht es nicht, diese einfach nur zu löschen, da gelöschte Daten unter Umständen wiederhergestellt werden können. Um Daten vollständig und sicher vom Gerät zu entfernen, gibt es speziellen Löschsoftware, die den Speicher mehrmals mit „Unsinn" überschreibt. Auf jeden Fall sollte das Gerät aber auf den Werkzustand zurückgesetzt werden.

Auf Werkzustand zurücksetzen

Einstellungen – Allgemeine Verwaltung – Zurücksetzen – Auf Werkseinstellungen zurücksetzen



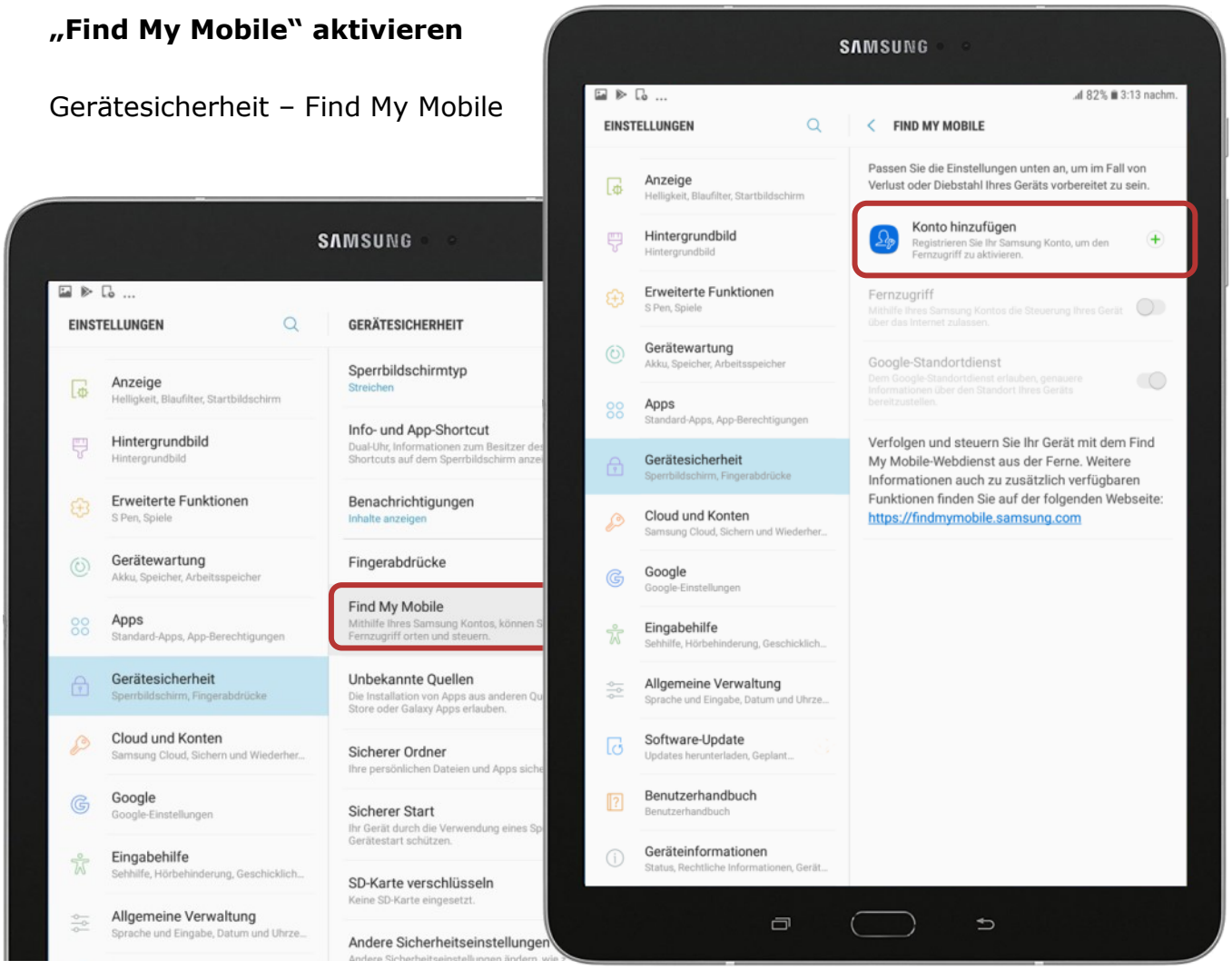
Tablet-Finder: finden oder sperren

Die meisten Tablets bieten die Möglichkeit, es bei Verlust oder Diebstahl zu orten, es sperren zu lassen oder sogar die Daten aus der Ferne zu löschen. Android unterstützt diese Funktion im Rahmen des Android Geräte-Managers bzw. über „Find My Mobile".

Ist diese Funktion aktiviert, kann das Gerät über das Konto beim Hersteller des Tablets oder das Google-Konto geortet, gesperrt oder die Daten können aus der Ferne gelöscht werden. Damit dieser Fernzugriff-Service funktioniert, muss der Standortzugriff in den Einstellungen erlaubt werden. Ebenso muss der Standortzugriff beim Google-Konto aktiviert werden. Um das Tablet im Fall des Falles zu orten, müssen sich Nutzerinnen und Nutzer in der Web-App des Android Geräte-Managers mit den Zugangsdaten ihres Google-Kontos einloggen (google.com/android/devicemanager). Bietet das eigene Tablet keine solche Funktion, kann alternativ auf Sicherheits-Apps von Drittanbietern (die GPS-Lokalisierung anbieten) zurückgegriffen werden.

„Find My Mobile" aktivieren

Gerätesicherheit – Find My Mobile



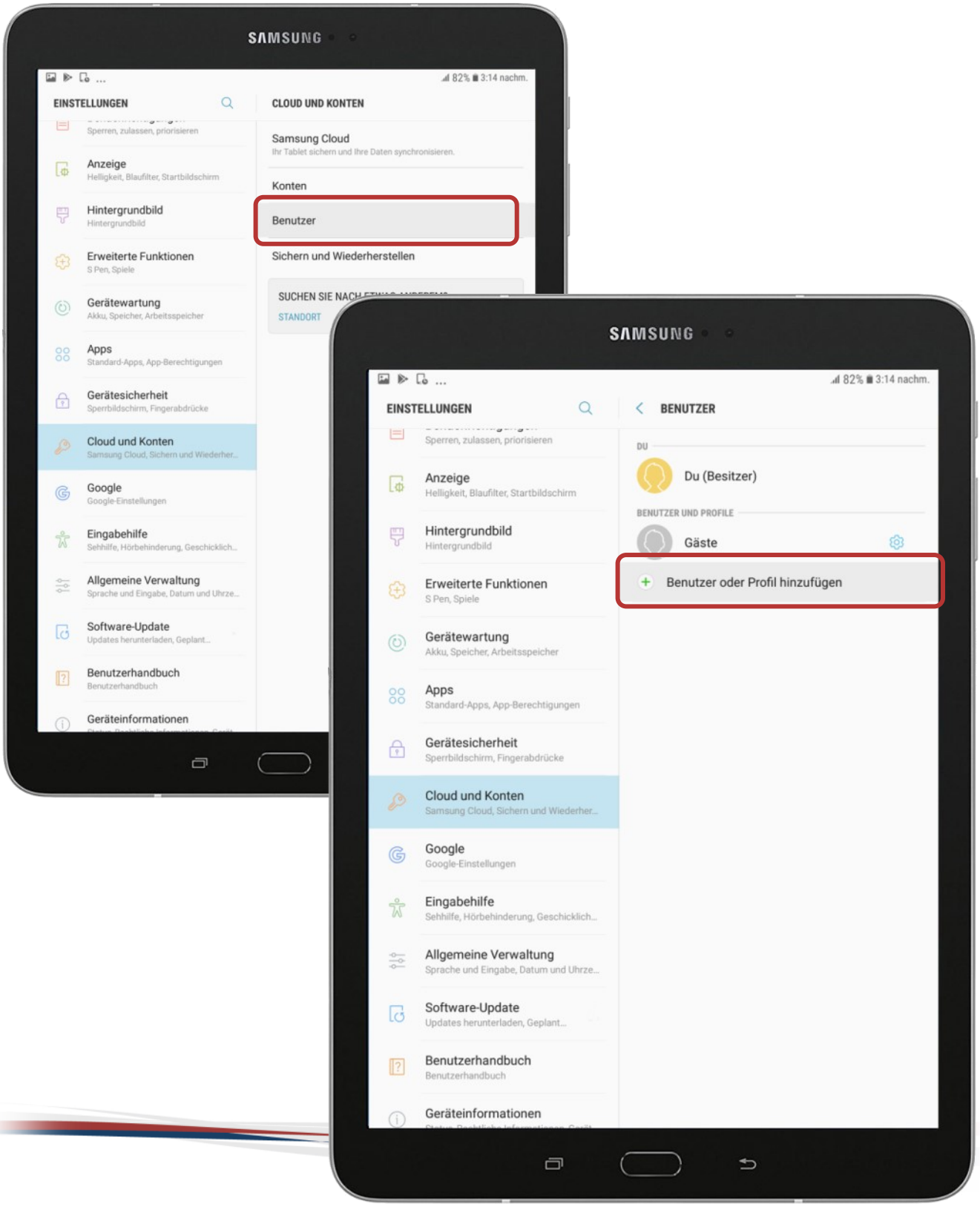
Das kindersichere Tablet

Um ein Tablet bei Bedarf kindersicher zu machen, sollten das Roaming deaktiviert, die Authentifizierung für App-Käufe eingeschalten, der App-Filter auf jugendfrei gestellt und ebenso Mehrwertdienste gesperrt werden. Falls diese Funktion vom Gerät unterstützt wird, kann ein Limit für den mobilen Datenverbrauch gesetzt werden. Für eine Nutzung durch jüngere Kinder kann überhaupt das Internet deaktiviert werden (in den Flugmodus wechseln).

Eine weitere Möglichkeit ist es, ein eigenes – kindgerechtes - Nutzerprofil auf dem Tablet anzulegen. Hier ist die Hauptnutzerin oder der Hauptnutzer gleichzeitig Administratorin oder Administrator und kann für jedes weitere angelegte Profil individuelle Einstellungen vornehmen, beispielsweise festlegen, auf welche Apps zugegriffen werden kann oder nicht.

Mittlerweile gibt es zahlreiche Apps, die sich dem Thema Kindersicherheit widmen. Diese sind aber Endgerät-basiert und funktionieren primär über Sperren und Filter. Zusätzlich sollten Erziehungsberechtigte bedenken, dass Medienerziehung nicht an Programme delegiert werden kann. Wichtig ist es, mit Kindern über das Internet, ungeeignete Inhalte und Online-Gefahren zu sprechen und ganz generell die Medienkompetenz der jüngsten Userinnen und User zu fördern. Ebenso sollten Eltern – und ältere Geschwister – bedenken, dass sie eine Vorbildfunktion haben, Kinder ahmen gerne das Verhalten von Älteren nach.

Tipps, Hilfestellungen und Info-Materialien für Eltern und Erziehungsberechtigte gibt es unter www.saferinternet.at/fuer-eltern. Pädagoginnen und Pädagogen finden unter www.saferinternet.at/fuer-lehrende auch Materialien und Übungen für den Einsatz im Unterricht.

Neues Nutzerprofil anlegen

Einstellungen – Cloud und Konten – Benutzer