Filtereinstellungen beim ersten Smartphone – So schützen Sie ihr Kind

Smartphones sind heute wahre Alleskönner. Sie vereinigen u.a. Telefon, Kamera, MP3-Player, aber auch Taschenlampe, Stoppuhr, Berggipfelerkennung, Thermometer und Navigationsgerät in einem einzigen Gerät. Möglich machen dies Applikationen – kurz Apps genannt. Diese Multifunktionalität ist zunächst eine wirklich feine Sache. Die Einfachheit der Bedienung befördert die rasante Verbreitung in alle gesellschaftlichen Schichten. Über 90% der BürgerInnen in Deutschland im Alter zwischen 14 und 59 Jahren besitzen diese Alleskönner.

Auch bei Kindern unter 14 Jahren hat die Verbreitung in den vergangenen Jahren massiv zugenommen. Aktuelle Daten zeigen, dass in der Altersgruppe der **Grundschulkinder bereits mehr als die Hälfte im Besitz eines Smartphones** sind.

So schön die Welt der Smartphones und ihrer Apps auch ist, so sollte die Kehrseite nicht außer Acht gelassen werden. Zwar muss für die beliebten Apps, gerade im Social Media Bereich, kein Geld an die Unternehmen entrichtet werden, dennoch bezahlt der Kunde einen nicht zu unterschätzenden Preis. **Die Apps gelten als ausgemachte Datenkraken**. Sie sammeln offiziell oder auch verborgen Daten über ihre Nutzer. Diese Daten wiederum werden zu **Persönlichkeits- und Bewegungsprofilen** zusammengefügt und an Werbepartner und andere – auch staatliche Behörden - weiterverkauft bzw. weitergereicht. Hier entstehen die Summen, die beispielsweise Facebook 2019 einen Börsenwert von an die 500 Milliarden US-Dollar verschaffte. Um diese Zahl einzuordnen, im Vergleich dazu hat der VW-Konzern einen Marktwert von etwa 101 Milliarden US-Dollar. Zudem bieten die **Apps aufgrund von Sicherheitsmängeln zahlreiche Einfallstore für Hackerangriffe**.

Dabei gehen die Apps bei der Datensammlung recht geschickt vor. Neben notwendigen Daten zur besseren Darstellung der Inhalte, werden gezielt Daten aus anderen Apps abgegriffen. Haben Sie sich schon einmal die Frage gestellt, weshalb beispielsweise eine einfache Taschenlampen-App den Zugriff auf Ihre Kontakt-, Bild- oder Standortdaten benötigt? Sicherlich nicht, um die Taschenlampe heller zu machen.

Aber auch der Zugriff von Social Media Apps, wie Facebook, Snapchat oder TikTok auf persönliche Bereiche im Smartphone ist zu hinterfragen. Wenn Sie in der Fußgängerzone von einer freundlichen, aber Ihnen völlig unbekannten Person angesprochen werden, ob Sie ihr die Kontaktdaten aller Freunde, ihren privaten und dienstlichen Kalender, sowie all ihre Fotos übergeben würden, ist die Antwort eindeutig. Wenn Sie zudem dem Unbekannten auch noch mitteilen müssten, wann sie sich, wo in den letzten Tagen, Wochen und Monaten aufgehalten haben, werden Sie einsilbig.

Nun soll die schöne Welt der Smartphones und Apps nicht verteufelt werden. Sie gehört zu uns wie viele andere Annehmlichkeiten auch. Doch wir sollten Vorkehrungen treffen. Gerade bei unseren Kindern, denen freilich der Hintergrund dieser scheinbar kostenfreien Welt noch wenig einleuchtet, müssen wir Vorsicht walten lassen. *„In der Vergangenheit wurden gravierende Sicherheitsmängel festgestellt. Der Umstand ist umso besorgniserregender, weil dadurch Daten von Kindern und Jugendlichen gefährdet sind.“ (*https://futurezone.at/apps/wie-gefaehrlich-ist-tiktok/400976654)

Die folgenden Tipps sollen Ihnen helfen das erste Smartphone Ihres Kindes so einzustellen, dass ungerechtfertigte Zugriffe auf die persönlichen Daten möglichst minimiert werden.

Tipp 1: Zugangssperre zum Smartphone
Versehen Sie das Smartphone ihres Kindes mit einer Zugangssperre. Diese kann über einen Code, über ein Muster oder über einen Finger-, bzw. Gesichtserkennungssensor erfolgen. Die Art der Sperrfunktionen ist von Gerätetyp und Alter abhängig. Bei Verlust oder Diebstahl des Gerätes muss der „neue“ Besitzer schon über tiefergehende Kenntnisse verfügen, um an ihre Daten gelangen zu können. Auch bei Ihrem eigenen Smartphone sollten Sie nicht auf die Zugangssperre verzichten.

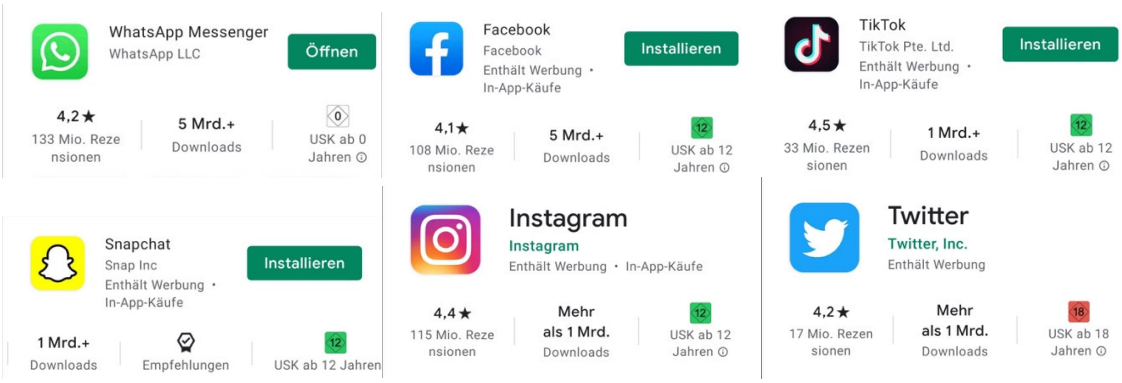
Schließt nämlich Ihr Kind bei einem Streamingdienst über Ihr Gerät ein kostenpflichtiges Abo ab, ist der Vertrag gültig. Man spricht hier von einer sogenannten Anscheinsvollmacht.

Tipp 2: Keine Speicherung von Zugangsdaten in Browser oder App
Es ist durchaus lästig immer wieder seine Zugangsdaten bei den verschiedenen Diensten eingeben zu müssen. Wie bequem und verlockend ist die Speicherung dieser Daten in der App oder im Browser. Das sollten Sie auf gar keinen Fall machen. Sie übergeben einem Autodieb ja auch nicht die Wagenschlüssel und halten ihm auch noch die Türe auf. Bringen Sie Ihrem Kind frühzeitig den sorgfältigen Umgang mit Zugangsdaten bei. Dazu gehört auch, sich von einer App abzumelden, wenn man sie aktuell nicht mehr benötigt.

Tipp 3: Installation einer App
Nehmen Sie die Installation einer neuen App selbst vor. Übergeben Sie das nicht in die Hand Ihres Kindes, da mit der Installation auch eine vertragliche Verpflichtung eingegangen wird. Eventuell entstehen auch direkte Abo-Kosten für die Nutzung der Applikation. Zur Installation ist meist ein entsprechendes Konto bei dem jeweiligen App-Store notwendig. Auch hier werden vertragliche Vereinbarungen getroffen, die Sie als Eltern vornehmen sollten.

Tipp 4: Verzicht bei Unsicherheit
Seien Sie bereit auf eine App zu verzichten, wenn Sie kein sicheres Gefühl haben. Bei der Installation einer neuen App kontrollieren Sie, auf welche Daten diese Zugriff haben möchte. Ist Ihnen dieser Zugriff nicht schlüssig und ist die Installation an den Datenzugriff gekoppelt, lassen Sie die Finger davon. Die Unternehmen sichern zu, dass die Regelungen der Datenschutzgrundverordnung (DSGVO) eingehalten werden. Da es sich um amerikanische oder chinesische Unternehmen handelt, sind sie aber auch den Regelungen der Heimatländer als Gesamtkonzern verpflichtet. Eine Weiterreichung von personenbezogenen Daten kann damit nicht ausgeschlossen werden (Urteil Europäischer Gerichtshof, Juli 2020).

Tipp 5: Mindestalter beachten
Achten Sie bei der Neuinstallation einer App darauf, für welches Mindestalter dieses Programm empfohlen wird. Aktuell ist WhatsApp ab 0 Jahren freigegeben, Facebook, Snapchat, TikTok und Instagram ab 12, Twitter erst ab 18 Jahren. Bedenken Sie, dass diese Apps Daten zu personalisierten Werbezwecken sammeln. Dabei spielt das Alter eine wesentliche Rolle.



Tipp 6: Einstellungen vornehmen
Wenn Sie sich für die Installation einer App entschieden haben, nehmen Sie Einstellungen in dieser vor, um die Daten Ihres Kindes vor unzulässigen Zugriffen zu schützen. Bei Kindern und Jugendlichen sind aktuell die Apps von TikTok, Instagram, Facebook, Snapchat, Whatsapp sowie Youtube sehr

gefragt. Die Vorlieben ändern sich allerdings, daher müssen Sie am Puls der Zeit bleiben. Im Anhang finden Sie Tipps für TikTok, Instagram, Facebook und Snapchat exemplarisch als Hilfestellung.

Autor: Matthias Dossenbach, Fachberater Informatik – Datenschutzbeauftrager im Schulamtsbezirk Bamberg

Quellen:
Statistische Daten: https://de.statista.com/statistik/daten/studie/459963/umfrage/anteil-der-smartphone-nutzer-in-deutschland-nach-altersgruppe/
Icons: https://www.iconfinder.com
TikTok: https://www.connect.de/ratgeber/tiktok-privatsphaere-videos-filter-clips-optionen-challenges-tipps-3201189.html
https://futurezone.at/apps/wie-gefaehrlich-ist-tiktok/400976654

Inhalte zu anderen Social-Media-Apps beruhen auf eigenen Recherchen.
Weiterführende Links:
https://mobilsicher.de/ratgeber/handy-fuer-kinder-einrichten-android
https://www.sicheres-netz-hilft.de/wissen/iphone-kindersicher-er-machen/
https://www.saferinternet.at/privatsphaere-leitfaeden/
https://www.klicksafe.de/themen/kommunizieren/
https://families.google.com/intl/de/familylink/privacy/notice/

Die Kampagne zum kritischen Medienkonsum wurde entwickelt von der Projektgruppe „Digitale Sucht“ der Gesundheitsregion^{plus}. Die Gesundheitsregion^{plus} ist ein vom Staatsministerium für Gesundheit und Pflege gefördertes Projekt mit einer Laufzeit von fünf Jahren. Weitere Auskünfte dazu erhalten Sie von Frau Bärbel Matiaske unter der Telefonnummer: 09191/86-3510.