iOS

Apple versteht es seit jeher, die Vorstellung des großen iOS-Updates rund um die hauseigene Entwicklerkonferenz medienwirksam zu inszenieren. Die Änderungen in iOS sind oft weniger spektakulär. Beim Wechsel von der 12er-Generation auf iOS 13 fallen die Neuerungen überraschend üppig aus: Akkuoptimierungen, von Grund auf neu entworfene Karten-App, überarbeitete Produktivitätsfunktionen und das iPad als Zweitbildschirm sind gerade im Business-Einsatz nützlich.

iOS 13, Catalina & Co.

Das bieten Apples neue Betriebssysteme

Die hohen Erwartungen der Besucher im Vorfeld der Entwicklerkonferenz WWDC wurden bereits bei der Eröffnungsrede, der Keynote, noch übertroffen. Mit einem unglaublich schnellen Tempo und gut geplanten Übergängen zwischen Feature-Updates, Demos und Videos führten die Protagonisten durch Apples neue Betriebssystem-Linien aus tvOS, watchOS, iOS, iPadOS und macOS. Hier eine Übersicht.

Beginnen wir mit **tvOS**. Dieses bietet nun einen Multi-User-Support und kann direkt mit den Game-Controllern der Xbox One und der Playstation 4 zusammenarbeiten. Mit Blick auf das bereits angekündigten All-You-Can-Play-Abo (Apple Arcade) ein gewiss sehr vorteilhafter Schritt.

› Obwohl schon häufig gefordert, kam das iPadOS für die meisten Besucher der WWDC ziemlich überraschend. (Foto: Apple)

Mit **watchOS 6** geht die Apple Watch große Schritte in Richtung Unabhängigkeit. So erhält diese einen eigenen AppStore und watchOS Apps lassen sich nun auch ohne iPhone-Gegenstück installieren und betreiben. Abgerundet wird die Eigenständigkeit mit neuen Netzwerk- und Audio-Streaming-APIs. Auch sind neue Apps wie Sprachmemo und Taschenrechner genauso enthalten wie neue Watch Faces.

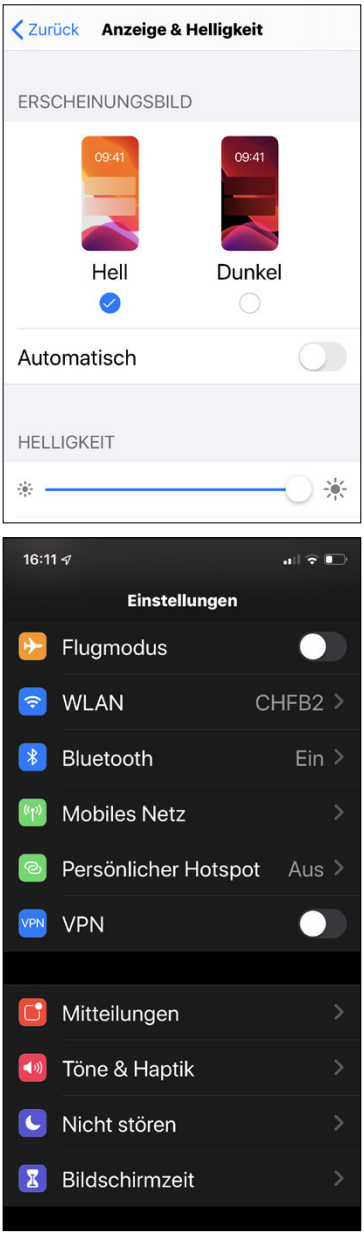
› watchOS erhält einen eigenen AppStore. (Foto: Apple)

iOS 13: Mehr Leistung, Sicherheit und Privatsphäre

Mit **iOS 13** legt Apple auch weiterhin großen Wert auf Leistung und Performance – und dies nicht nur auf Neugeräten. Von der erhöhten Download- und Startgeschwindigkeit von Apps und einer allgemeinen Verbesserung der System-Performance dürften alle Geräte ab iPhone 6S (ab iPad Air 2) profitieren. Dies gilt auch für die schneller werdende Gesichtserkennung. Memoji lassen sich nun noch mehr anpassen und können als personalisiertes Emoji über die Tastatur in jeglicher App eingebunden werden.

Der neu einführte **Dark Mode** sieht großartig aus und ist maßgeschneidert für die OLED-Displays der iPhone-X-Generation. Da ein schwarzes OLED-Pixel keinen Strom verbraucht, dürfte das Feature auch beim Energiehaushalt eine Verbesserung bedeuten. Außerdem wurden Systembestandteile von iOS wie das Share Sheet mit neuen Designs und Funktionen ausgestattet.

Doch damit nicht genug: Die neue Privatsphäre-wahrende Single-Sign-On-Funktion **„Sign in with Apple"** (mehr ab › Seite 112) ist der Angriff aus Cupertino auf die datenhungrigen Anmeldedienste aus dem Hause Facebook und Google. Apple verspricht, keine Profildaten bei der Nutzung zu erheben und ermöglicht es, die persönlichen Daten wie die Mail Adresse vor den Diensteanbietern zu maskieren. Die Funktion kann nicht nur auf iOS und macOS genutzt werden. Windows und Android werden ebenfalls unterstützt.



› Mit iOS 13 bekommt das iPhone-Betriebssystem ein Dark Mode.

Wer als App-Entwickler in seiner App zukünftig eine Login-Variante von Google oder Facebook implementiert hat, wird zusätzlich verpflichtet, ab Herbst 2019 auch den Login über „Sign in with Apple" anbieten.

Der digitale Assistent **Siri** bekommt mit iOS 13 eine neue, vollständig algorithmisch generierte Stimme. Zumindest im Englischen wurde das Ergebnis bereits präsentiert, inwieweit dies auch in deutscher Sprache umgesetzt wird, muss sich zeigen. Im Umgang mit den AirPods wurde die Interaktion ebenfalls optimiert. Eingehende Nachrichten können sofort vorgelesen und direkt beantwortet werden, ohne dass der Anwender dies mit „Hey Siri" einfordert. Auch die **Bedienungshilfen** erlauben nun eine komplett sprachgesteuerte Nutzung von iOS. Sämtliche Funktionen von iOS und der installierten Apps lassen sich so ohne händische Eingriffe bedienen, was beispielsweise Autofahrern zugute kommt.

Das Thema **Augmented Reality** geht mit ARKit 3.0 in die nächste Runde (mehr dazu ab › **Seite 38**). Die neue People Occlusion-Funktion ermöglicht es, echte Menschen nahtlos in eine Augmented-Reality-Welt einzufügen. Menschen können hinter sich liegende virtuelle Objekte damit verdecken oder vor ihnen physikalisch korrekt herlaufen. Damit wirkt ARKit wirklich räumlich. Mithilfe des Reality Composer Editor, der für macOS und iOS verfügbar ist, können Entwickler ihre 3D-Landschaften jetzt einfach gestalten und mit Effekten und Animationen aufwerten.

iPadOS: Angepasstes Betriebssystem für das iPad

Eines hatten die vielen Gerüchte nicht zum Thema: das iPad bekommt mit **iPadOS 13** ein eigenes Betriebssystem (mehr dazu ab › **Seite 12**). Dieses nimmt zwar Anleihen an iOS 13, erweitert dieses (augenscheinlich) jedoch um einige dringend benötigten Anpassungen. So bietet der Home-Bildschirm mehr Platz für Apps. Auch das Multitasking wurde erweitert. So können mehrere Dokumente auf verschiedenen App-Screens (Spaces) geöffnet werden.

Mit dem Apple **Pencil** kann der iPad Anwender von überall einen Screenshot einfordern und auf diesem Markierungen vornehmen. Das dahinter liegenden PencilKit-Framework steht nun auch allen anderen App-Entwicklern ebenfalls zur Verfügung. Funktionen wie „Cut, Copy, Paste" oder auch „Undo" haben neue Drei-Finger-Gesten auf dem iPad bekommen. Das Markieren von Text mit dem Finger wurde ebenfalls vereinfacht. Zudem wurde die „**Dateien**"-App sehr stark überarbeitet. Die aktuelle Überarbeitung bietet zum Beispiel die Möglichkeit, nicht nur einzelne Dateien, sondern auch ganze Ordner mit Freunden zu teilen. Der Anschluss von USB-Sticks, SD-Karten (per Adapter) und anderer Massenspeicher (HDD, SSD) ist möglich. Das iPad wird so zu einem vollwertigen Arbeitsplatz.

macOS: Abschied von iTunes

Auch für **macOS** gab es ein Update. Unter dem Namen Catalina steht eine neue Version in den Startlöchern. Dabei nimmt Apple Abschied von iTunes und verteilt die Funktionen auf mehrere „neue" macOS-Apps (Musik, TV, Podcasts). Die Interaktionen mit kabelgebundenen iOS Geräten erfolgt nun über den Finder, um z.B. Backups von Geräten zu erstellen oder zurück zu spielen. Die Funktion mit dem Namen **SideCar** (mehr dazu ab › **Seite 17**) macht das iPad sowohl zu einem zweiten Display für den Mac, als auch zu einem Zeichentablett.

Wie bereits im letzten Jahr angekündigt, kann macOS Catalina nun auch mit iPad-Apps arbeiten. Damit diese über die als „Catalyst" bezeichnete Technologie – damals sprach Apple noch von „Marzipan" – möglich ist, müssen Entwickler beim Erstellen einer so nutzbaren App dies speziell bestätigen. Ein Klick in der Entwicklungsumgebung soll hierfür ausreichen.

Mit dem neuen **SwiftUI**-Framework schafft Apple die notwendigen Voraussetzungen für die nächste Generation von Entwicklerwerkzeugen auf allen seinen Plattformen. Doch auch hardwareseitig gab es eine Überraschung: Nachdem professionelle Anwender von Apple seit langem ein professionelles modularer erweiterbares macOS Rechnersystem verlangten, wird dies nun mit dem neuen Mac Pro geliefert.

› Mit macOS Catalina nimmt Apple Abschied von iTunes und verteilt diese Funktionen nun auf „neue" Apps für Musik, TV und Podcasts. (Foto: Apple)

Fazit

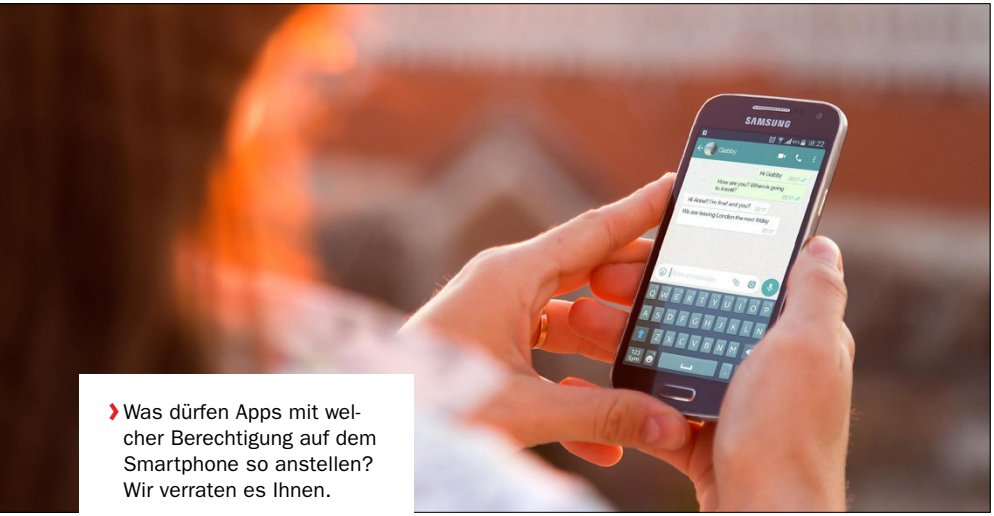
Entwickler haben lange nicht mehr so eine umfangreiche Show an Neuigkeiten und Ankündigungen erlebt. Man darf gespannt sein, ob Apple gegen Ende des Jahres alle versprochenen Funktionen fristgerecht abliefern kann. Ein genaues Datum für das Release der einzelnen Versionen steht noch aus. Eingetragene interessierte Nutzer können aber schon an Beta-Tests teilnehmen.

Mark Zimmermann

Rechte verstehen und einschränken

App-Berechtigungen unter Android

Vor der Installation oder spätestens bei der ersten Verwendung einer App müssen Sie deren Zugriffsrechte bestätigen. Doch viele Programme fordern deutlich mehr Rechte, als sie eigentlich benötigen. Wir zeigen auf, was hinter den einzelnen App-Berechtigungen steckt und was bei alledem zu beachten ist.



› Was dürfen Apps mit welcher Berechtigung auf dem Smartphone so anstellen? Wir verraten es Ihnen.

Auf Ihrem Android-Gerät sind in der Regel diverse Apps installiert: von Facebook und WhatsApp über Wettervorhersage, Nachrichten und Fahrplanauskunft bis hin zu diversen Spielen und Dienstprogrammen. Manche Apps tun aber nicht nur das, was sie sollen und was der Benutzer von ihnen erwartet. Wenn eine Taschenrechner-App zum Beispiel auf Ihre Standortdaten zugreifen will, die Taschenlampe einen Zugriff auf Ihr Adressbuch verlangt oder die Puzzle-App Einblick in Ihre privaten Nachrichten fordert, ist Vorsicht angebracht. Denn viele Apps verlangen Zugriffsrechte, die für ihren Anwendungszweck gänzlich unnötig sind.

In diesem Ratgeber erklären wir, was die einzelnen App-Berechtigungen genau bedeuten und worauf Sie achten sollten. Darüber hinaus geben wir Ihnen Anleitungen an die Hand, wie das Prüfen und auch das Verwalten der Berechtigungen bei der Neuinstallation sowie bei bereits installierten Apps funktioniert.

App-Berechtigungen und ihre Bedeutung

Die möglichen App-Zugriffsrechte sind in folgende Gruppen unterteilt:

In-App-Käufe, Geräte-und App-Verlauf, Einstellungen für Mobilfunkdaten, Identität, Kontakte, Kalender, Standort, SMS, Telefon, Fotos/Medien/Dateien, Kamera, Mikrofon, WLAN-Verbindungsinformationen, Informationen zur Bluetooth-Verbindung, Wearable-Sensordaten/-Aktivitätsdaten, Geräte-ID & Anruferinformationen sowie *Sonstiges*. Google will so die App-Verwaltung einfacher gestalten.

Bei diesen App-Berechtigungen sollten Sie vorsichtig sein

Welche Berechtigungen Sie einer App erteilen, sollten Sie davon abhängig machen, ob Sie der App vertrauen und um welche verlangten Zugriffsrechte es sich handelt. Denn manche Berechtigungen sind eher harmlos, wobei andere durchaus gefährlich werden können. So werden die Berechtigungsgruppen *Fotos/Medien/Daten, In-App-Käufe, Kalender, Kamera, Kontakte, Mikrofon, SMS, Standort, Telefon* sowie *Wearable-Sensorendaten/-Aktivitätsdaten* als potenziell gefährlich eingestuft. Aber warum sind gerade diese Berechtigungen kritisch und welchen Apps können Sie den Zugriff dennoch gewähren?

- **Fotos/Medien/Daten:** Wenn Sie einer App den Zugriff auf Ihre Fotos, Medien und Daten gestatten, müssen Sie im schlimmsten Fall damit rechnen, dass diese Ihre privaten Dateien ausspäht, verändert oder sogar löscht. Einen berechtigten Anspruch auf diesen Zugriff haben dennoch beispielsweise Dateimanager-Apps, Social-Media-Apps oder Bildbearbeitungsprogramme.
- **Kalender:** Diese Berechtigung kann vor allem für diejenigen gefährlich werden, die aktiv den Kalender auf dem Smartphone nutzen. So könnte eine bösartige App nicht nur Ihre Tagesabläufe ausspähen, sie könnte auch Ihre Termine ändern oder sogar löschen. Die Berechtigung ist aber etwa für Gmail sinnvoll, um wichtige Termine aus Ihren Mails in Ihrem Kalender zu speichern.
- **Kamera:** Nicht nur Kamera-Apps, auch Taschenlampen-Anwendungen benötigen den Zugriff, um den LED-Blitz zu verwenden. Allerdings könnten Malware-Apps die Möglichkeit, jederzeit Videos und Fotos aufzunehmen, auch dazu nutzen, Sie auszuspionieren.
- **Kontakte:** Hier sollten Sie beachten, dass eine schädliche App alle Kontaktdaten Ihrer Familie, Freunden und Geschäftspartnern speichern und schlimmstenfalls verkaufen könnte. Chat-Apps wie Whatsapp benötigen den Zugriff, um Ihnen alle verfügbaren Kontakte anzeigen zu können.

- **Mikrofon:** Das Recht, auf das Mikrofon Ihres Smartphones zuzugreifen und dadurch Audiomitschnitte erstellen zu können, macht Ihr Mobilgerät für Malware-Apps zu einem perfekten Abhörgerät. Naturgemäß aber benötigen Apps zum Diktieren, für Videochats und dergleichen diese Zugriffsrechte.
- **SMS:** Im schlimmsten Fall kann eine schädliche App auf Ihre Kosten Nachrichten versenden und sogar per SMS gebührenpflichtige Dienste abonnieren. Sie sollten also sicherheitshalber das Bezahlen per SMS bei Ihrem Provider deaktivieren. Einige Anwendungen wie Whatsapp nutzen diese Berechtigung, um Verifizierungscodes zu lesen. Doch auch dieser Einsatzzweck lässt sich umgehen, indem Sie manuell den Code auf Ihrem Smartphone eintippen.
- **Standort:** Ihre Standortdaten benötigen Apps, um Sie gezielt zu orten und vielleicht sogar, um Bewegungsprofile zu erstellen. Bei Navigationsanwendungen wie Google Maps oder auch Sport-Tracking-Apps wie Runtastic sind solche Daten allerdings notwendig. Auch von Empfehlungsanwendungen wie Yelp oder Tripadvisor werden sie gefordert.
- **Telefon:** Auch der Zugriff auf Ihr Telefon kann bei einer betrügerischen App gefährlich werden. So könnte die App ohne Ihr Wissen und Ihre Erlaubnis kostenpflichtige Nummern anrufen und enorme Kosten verursachen. Bei Anwendungen wie etwa Skype ist der Zugriff jedoch wiederum notwendig, um aus der App direkt Ihre Kontakte anrufen zu können.
- **Wearable-Sensorendaten/-Aktivitätsdaten:** Diverse Fitness-Programme wie Google Fit oder Fitbit benötigen Zugriff auf die Aktivitäts- oder Wearable-Sensorendaten, um Ihnen nützliche Ergebnisse zu präsentieren. Anderen Anwendungen sollten Sie den Zugriff auf keinen Fall gewähren, denn sie könnten Ihre körperliche Verfassung ausspionieren.

› Überlegen Sie, ob der Zugriff für die jeweilige App benötigt wird. Im Bild handelt es sich um eine Navigations-App, die Standortfreigabe wird also benötigt.