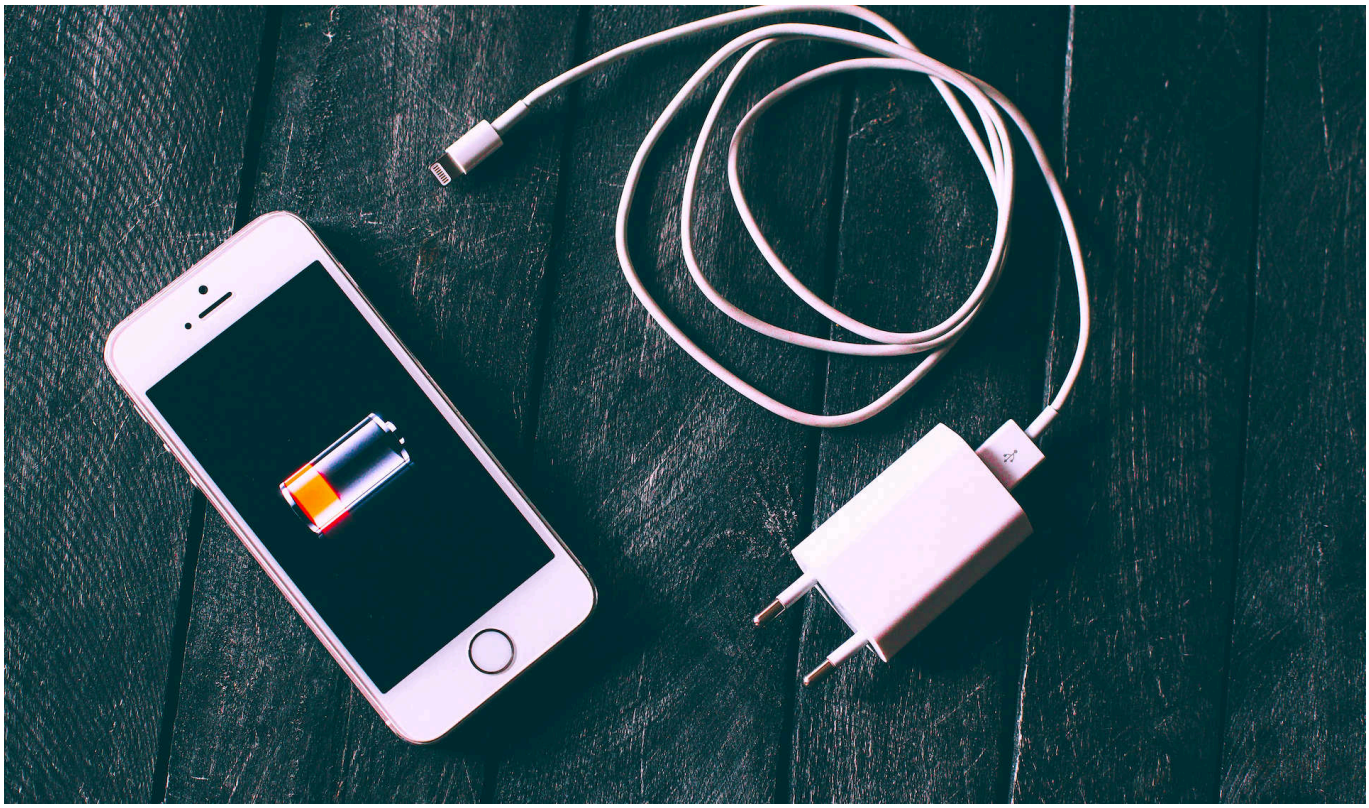
Schieb Report

Ausgabe 2021.07

Mehr Umweltschutz: Akkus sollen künftig austauschbar sein



Der Bundesrat will Hersteller verpflichten, mindestens fünf Jahre lang Akkus als Ersatzteile anzubieten. Außerdem sollen Verbraucher in der Lage sein, den Akku in ihren Geräten - vor allem in Smartphones - bei Bedarf selbst auszutauschen. Das soll den Lebenszyklus der Geräte verlängern und so die Umweltbelastung reduzieren.

Sind wir doch mal ehrlich: Wer macht sich schon Gedanken über all die Akkus, die wir heute wie selbstverständlich im Einsatz haben. Im Handy. In der Digitalkamera. Im Mikro. In der Action Cam. In der Power-Bank... Da kommen leicht und ohne Weiteres Dutzende, Hunderte Akkus in einem einzigen Haushalt zusammen.

Ein immenses Problem. Denn das Herstellen und vor allem auch das fachgerechte Entsorgen von Akkus ist ein immenses Umweltproblem, wie diese empfehlenswerte (und schockierende) ARTE-Dokumentation zeigt.

CO2-Ausstoß in Rechenzentren muss reduziert werden[/caption]

Festverbaute Akkus besonders problematisch

Besonders problematisch sind aber jene Akkus, die fest im Gerät verbaut sind. In der Smartwatch zum Beispiel. Oder in vielen Smartphones und Tablets. Prominentes Beispiel: das iPhone. Problematisch deshalb, weil bei fest verbauten Akkus der Austausch schwer fällt. Oder besser: Der Austausch ist sehr kostspielig wird und kann nur beim Hersteller durchgeführt werden.

Am Ende tauschen viele Menschen ihre Geräte aus, nur weil der Akku nicht mehr richtig will.

Schädlich für die Umwelt - das liegt auf der Hand. Deshalb fordert der Bundesrat jetzt - nachdem Umweltverbände das schon seit Jahren anregen -, dass Verbraucher den Akku jederzeit selbst(!) ersetzen können sollen. Außerdem sollen die Hersteller verpflichtet werden, mindestens fünf Jahre entsprechende Ersatzteile - insbesondere Akkus - anzubieten.

[caption id="attachment_772230" align="alignnone" width="1030"]

Hands of repairman using pentalob screwdriver when removing smartphone battery[/caption]

Festverbaute Akkus besonders problematisch

Das wäre schon eine Kehrtwende. Eine, die dringend nötig erscheint - und Hightech-Geräte nicht gleich "grün" macht, sondern lediglich den Umweltschaden etwas reduziert. Aber immerhin.

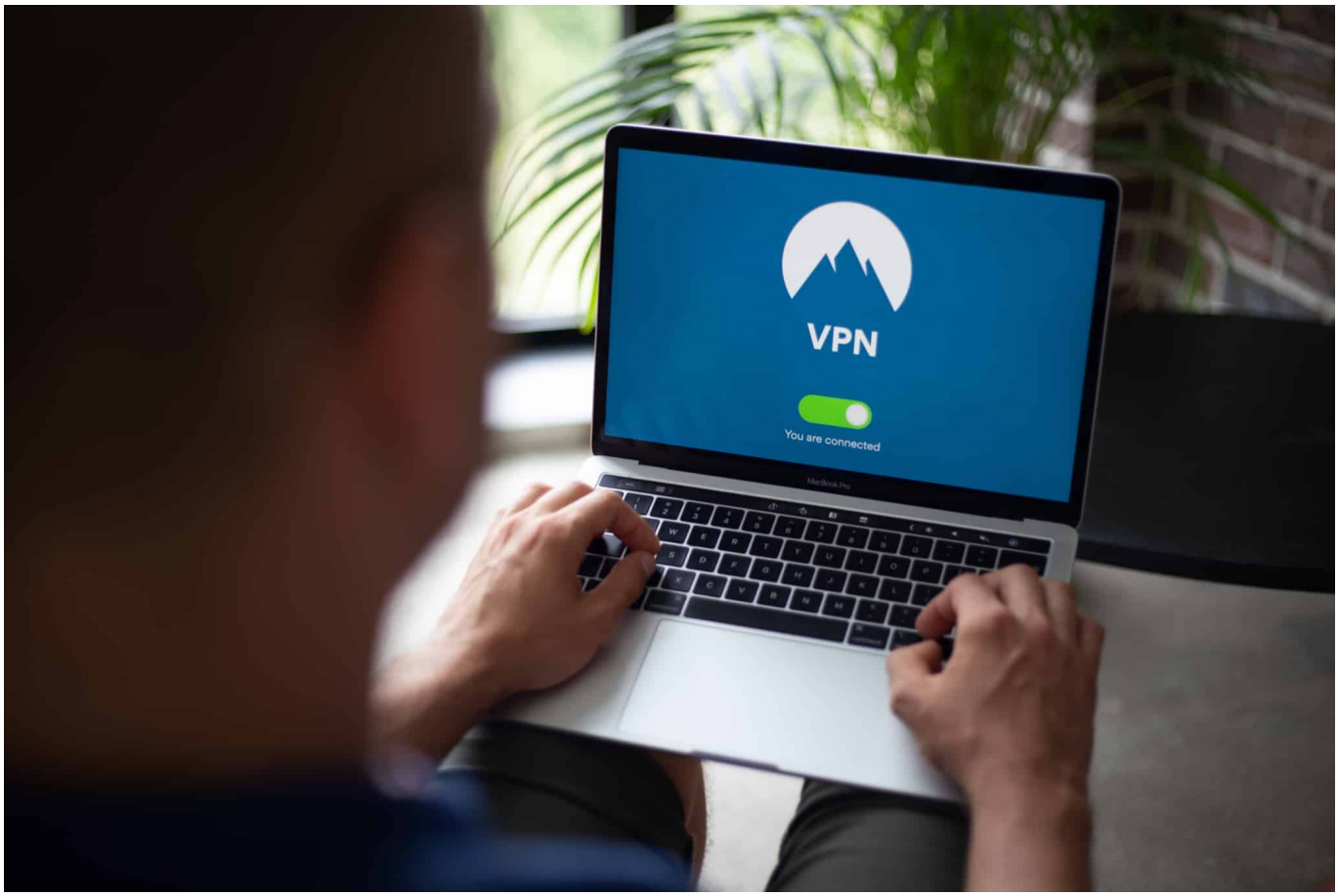
Das dürfte den Herstellern gar nicht gefallen. Sie müssen dann das Design ihrer Geräte ändern. Einige wären dann möglicherweise nicht mehr wasserdicht. Sie würden auch weniger verdienen, weil es definitiv viele Menschen gibt, die sich sagen: OK, der Akku gibt den Geist auf - dann wechsele sich zum aktuellen Modell.

Es ist noch deutlich mehr geplant. Etwa, dass die Hersteller Angaben über die Zusammensetzung des Akkus machen müssen (was ist drin?). Außerdem soll der Handel zur Rücknahme solcher Geräte verpflichtet werden. Eine höhere Rate an Wiederverwertung ist ein weiteres Ziel.

Alles richtig, alles gut. Hoffen wir, dass der Bundesrat sich damit durchsetzen kann.
[caption id="attachment_773552" align="alignnone" width="1030"]

Klick-Scham: Die Digitalisierung hinterlässt Spuren

Die besten Einsatzmöglichkeiten für ein VPN im Jahr 2021



Wer im Home Office arbeitet und mit Firmenrechnern kommuniziert, macht das in der Regel geschützt - durch ein "Virtual Private Network" (VPN). Es verschlüsselt die Kommunikation und macht den Datenstrom abhörsicher. So etwas lässt sich auch im privaten Bereich gewinnbringend einsetzen.

Viele fragen sich, was sie mit einem VPN (Virtual Private Network) eigentlich machen können - ob sie so etwas brauchen.

Einfach ausgedrückt funktioniert ein VPN, indem es all Ihre über das Internet ausgetauschte Informationen verschlüsselt und durch einen "Datentunnel" zum Zielort schickt (und von dort holt).

Das geschieht, indem es Ihre Internetverbindung von den Servern Ihres Internet Service Providers (ISP) auf seine eigenen umleitet. Die beeindruckendsten Online VPN haben Tausende von Servern auf der ganzen Welt. Das bedeutet, dass Sie nicht nur sicherstellen können, dass alle Ihre Daten verschlüsselt sind, sondern

Sie können im Internet surfen, als wären Sie in einem anderen Land.

Dies eignet sich hervorragend zum Streamen und zum Umgehen einer staatlicher Zensur. Wenn Sie sich damit begnügen, in Ihrem Heimatland zu bleiben, erlaubt Ihnen die sichere Verschlüsselung Ihres VPNs auch anonym zu surfen und generell ein privates Erlebnis im Internet zu haben und wer möchte das nicht.

Schützen Sie Ihre Identität

Wenn die meisten Menschen an ein VPN denken, denken sie in erster Linie an eine Lösung zum Schutz der Privatsphäre und das aus gutem Grund. Die ursprüngliche Hauptanwendung eines VPNs ist der Schutz des Benutzers und seiner Daten, um eine sichere Internetnutzung zu gewährleisten, egal bei welcher Aktivität.

Ein Kernelement eines VPNs ist eine starke Verschlüsselung - in der Regel AES-256 oder besser und das bedeutet, dass jedes einzelne Bit des durch das VPN gesendeten Datenverkehrs für jeden, der ihn abfängt, unlesbar ist. Dieser Abfangjäger könnte einfach Ihr ISP sein der versucht, die Nutzung Ihrer Verbindung einzuschränken oder es könnte eine böswillige Person oder ein Programm sein das versucht Ihre Daten zu stehlen.

Wer oder was auch immer sie sind, VPNs umgehen sie, indem sie einen "Tunnel" verwenden, der an Ihrem Gerät beginnt und an Ihrem Ziel endet - sei es Netflix, ein geo blockiertes soziales Netzwerk oder Ihr Online-Banking.

Streamen von geo blockierten Inhalten

Fernsehen über Streaming-Dienste ist heute die Norm und während es eine größere Auswahl als je zuvor gibt, kann ein VPN Ihre Optionen unermesslich erweitern. Diese VPN-Nutzung ist ideal für diejenigen, die im Urlaub oder auf Geschäftsreisen sind und für die abenteuerlustigen Couch-Potatoes.

Dienste wie Netflix haben unterschiedliche Bibliotheken mit Inhalten für Abonnenten in verschiedenen Regionen, was bedeutet, dass niemand wirklich alles sehen kann - es wird immer eine Serie oder einen Film geben, der in Ihrem Land blockiert ist. Mit einem Netflix-VPN können Sie sich jedoch mit einem Server in einem bestimmten Land verbinden und Netflix reagiert darauf, indem es Ihnen die Bibliothek dieser Region zur Verfügung stellt.

Zugriff auf Websites, wenn Sie im Ausland sind

Ähnlich wie Streaming-Dienste bieten auch viele andere Websites unterschiedliche Inhalte für Benutzer in verschiedenen Ländern an. Wenn Sie jedoch auf einer Reise sind, werden Sie auf Ihre reguläre Version zugreifen wollen, aber Sie werden mit einer Website konfrontiert, die möglicherweise völlig anders ist und sehr wahrscheinlich in einer Sprache, die Sie nicht sprechen. Wenn Sie ein VPN haben, müssen Sie einfach nur Ihre Verbindung verlagern, damit Sie wieder wie zu Hause aussehen, und schon können Sie wie von Zauberhand auf Ihre vertraute Seite zugreifen.

Dies ist auch für Online-Banking besonders nützlich. Wenn Sie einen Wochenendausflug gemacht und vergessen haben, Ihrer Bank Bescheid zu sagen, kann es passieren, dass Sie von Ihrem Konto ausgesperrt werden. In diesem Fall lohnt es sich, den VPN-Schalter einzuschalten und für einen Moment virtuell nach Hause zu fahren, um sicherzustellen, dass Ihr Konto nicht gesperrt wird und Sie im Ausland mittellos dastehen.

Mehr Live-Sport sehen

Wenn Sie ein Sportfanatiker sind, werden Sie wissen, dass das Anschauen von Live-Events ziemlich schnell teuer werden kann. Mit einem VPN und ein wenig Recherche können Sie jedoch eine Menge Geld sparen - und vielleicht ein Pay-per-View Event kostenlos finden.

GPS-Standort vortäuschen

Obwohl diese VPN-Nutzung nicht so bekannt ist wie andere und nicht für jeden nützlich sein wird, kann das Spoofing Ihres GPS-Standorts mit einem VPN besonders zuverlässig gemacht werden. Wenn Sie zum Beispiel einen gefälschten GPS-Standort für Pokemon GO erhalten möchten, müssen Sie entweder ein VPN mit einer GPS-Spoofing-App kombinieren.

Schützen Sie Ihre mobilen Geräte

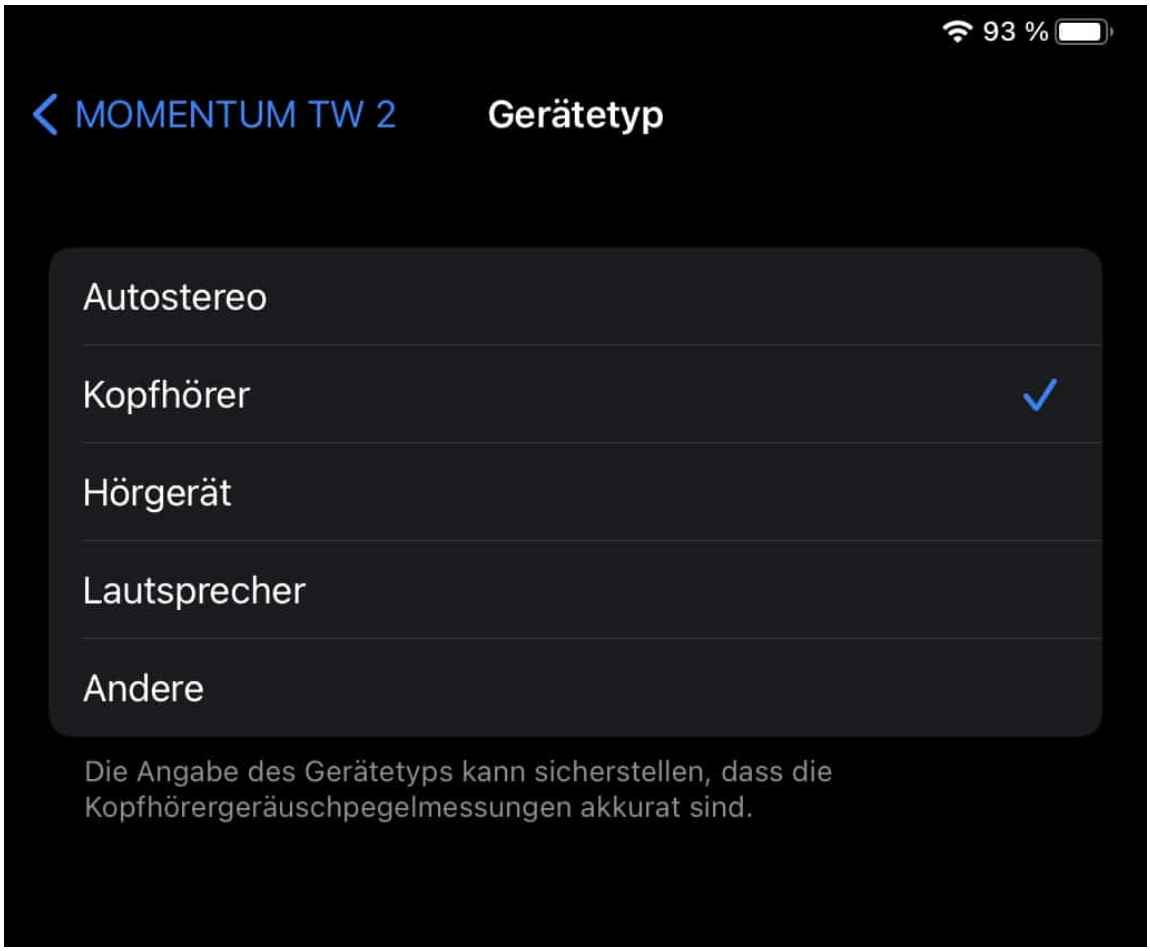
Wenn Sie sich bei einem guten Anbieter anmelden, erhalten Sie nicht nur ein Windows-VPN, sondern fast alle hochwertigen Dienste haben Apps für Android und iOS, und einige unterstützen sogar noch BlackBerry. Wenn Sie ein VPN auf Ihrem mobilen Gerät verwenden, können Sie sowohl zu Hause als auch unterwegs geschützt bleiben. Wenn man bedenkt, dass das Gerät, mit dem Sie

sich am häufigsten mit öffentlichem WLAN verbinden, wahrscheinlich Ihr Telefon ist, ist das eine vernünftige Entscheidung.

Automatische Lautstärkeeinstellungen bei iOS verhindern

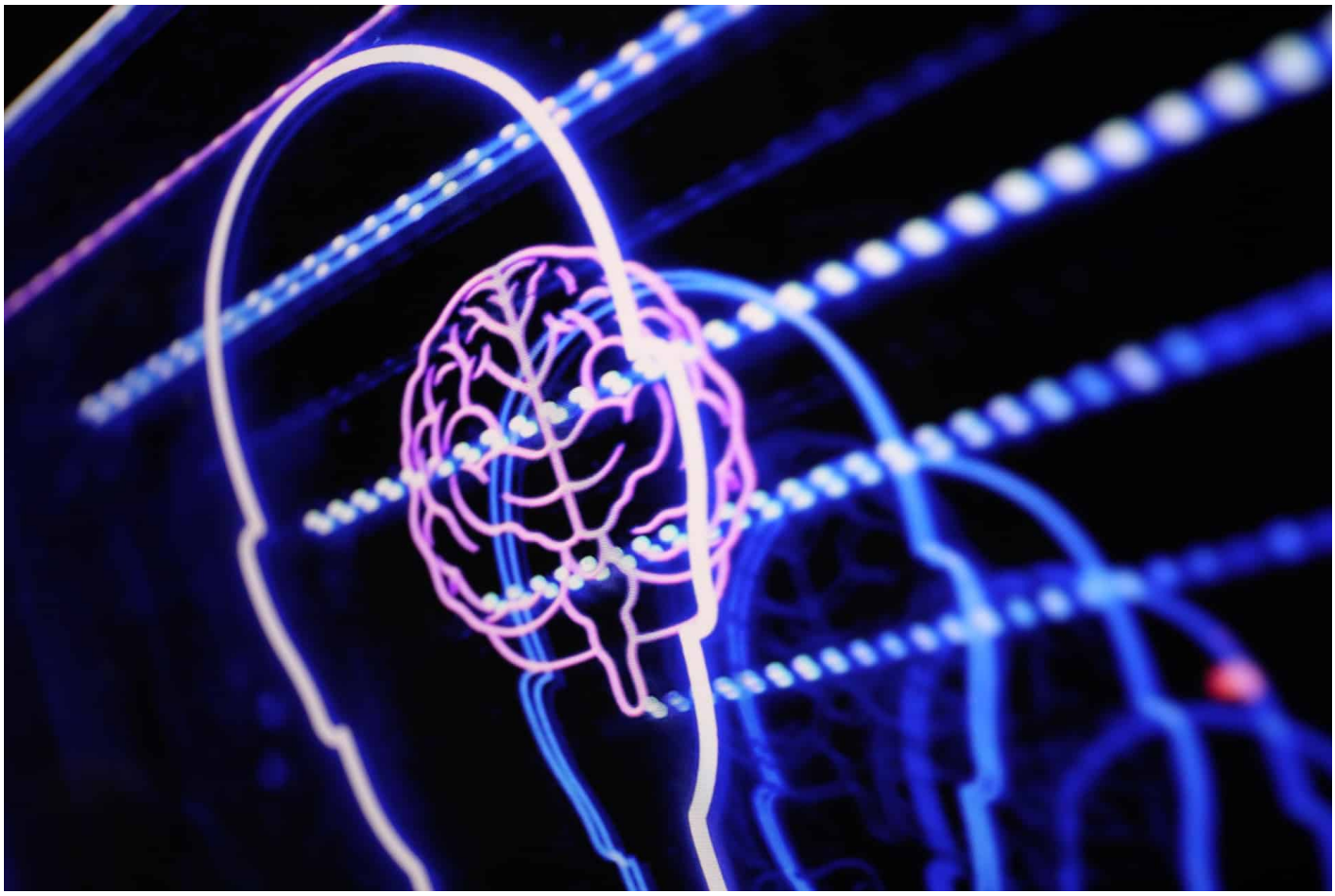
Apple versucht seine iOS-Nutzer zu schützen: Lautes Musikhören ist nicht gut für die Ohren, und so werden GEräte in ihrer Lautstärke automatisch begrenzt, wenn Sie über einen Zeitraum von 7 Tagen zu lange laut Musik gehört haben. Ärgerlich, wenn es sich dabei nicht um Kopfhörer, sondern beispielsweise um Bluetooth-Boxen handelt! iOS 14.4 erlaubt Ihnen hier mehr Freiheiten.

Keine Frage: Sie sollten nicht über lange Zeit laut Musik hören. Es gibt aber durchaus Situationen, wo die Lautstärke hoch sein muss: Musikdateien oder Klangquellen, die extrem leise abgemischt sind und bei denen die höchste Lautstärke-Einstellung gerade mal ausreichend ist. Lautsprecher, die einen großen Bereich beschallen müssen und laut sein müssen, damit sie auch die letzte Ecke erreichen. Mit iOS 14.4 können Sie die Lautstärkebegrenzung für alle Geräte ausser die Apple Airpods/Pro/Max umgehen.



In den Einstellungen von iOS/iPad OS tippen Sie auf **Bluetooth**, dann auf das **i** neben dem Bluetooth-Gerät. Hier finden Sie einen neuen Eintrag **Gerätetyp**, in dem Sie neben **Kopfhörer** (wo die Begrenzung aktiv wird) auch **Fahrzeugunterhaltung**, , **Lautsprecher** und **Hörhilfe** sowie **Sonstiges** auswählen können. Für die neuen Kategorien wirkt die Lautstärkekontrolle nicht.

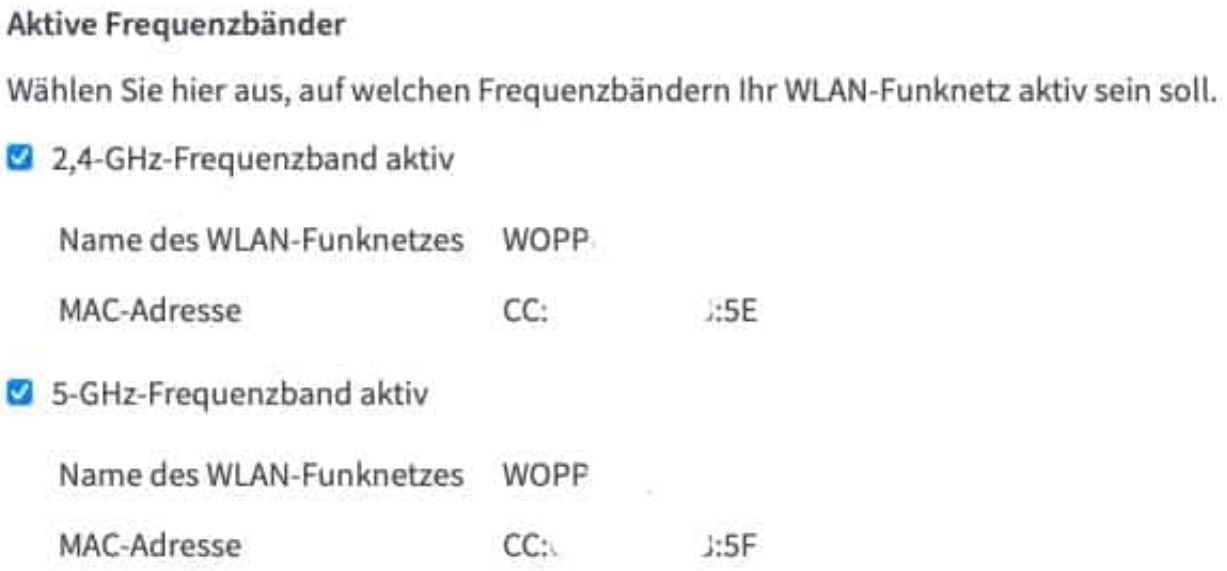
WLANs voneinander trennen per Repeater



Der Betrieb eines WLANs ist meist ein Selbstläufer. Sie konfigurieren es am Anfang einmal, dann greifen alle Ihre Geräte darauf zu und werden mit Internet und Daten von anderen Geräten versorgt. Sie können allerdings auch durch die Konfiguration eine Trennung von Geräten vornehmen. Wir zeigen Ihnen, wie das geht.

Die meisten modernen Router bieten die Möglichkeit, mehrere WLANs zu erzeugen. Zum einen durch die Trennung von 2.4GHz und 5GHz-Frequenzen, zum anderen durch die Möglichkeit, ein Gast-WLAN komplett getrennt von den anderen WLANs zu erzeugen.

In manchen Konstellationen macht es Sinn, bestimmte Geräte nur in das eine oder das andere WLAN zu lassen. Wenn Sie SmartHome-Komponenten im WLAN haben, dann sind die in dem 2.4GHz WLAN gut aufgehoben. Die meisten Smarthome-Geräte unterstützen kein 5GHz WLAN. Die normalen Geräte gehen dann in das 5GHz WLAN.



Über WLAN-Repeater können Sie nun selektiv WLANs verstärken: Wenn die normalen Geräte mit dem Router verbunden bleiben sollen, ein Smarthome-Gerät aber ein zu schwaches Netz bemängelt, dann lassen Sie über den Repeater nur das eine WLAN verstärken. Dazu wechseln Sie über den Router in die Konfigurationsoberfläche des Repeaters, klicken dort auf **WLAN** und entfernen den Haken neben dem WLAN, das nicht verstärkt werden soll.

Facebook lässt in Australien die Muskeln spielen - und blockiert seriöse Inhalte

Überall auf der Welt wird gestritten: Verlage beklagen die Übermacht von Google und Facebook im Netz - und hätten gerne ein Stück vom Werbekuchen. In Australien ist dieser Streit nun auf die Spitze getrieben worden. Google und Facebook sollen bezahlen. Nun hat Facebook als Reaktion australische Verlage und Sender gewissermaßen "ausgeknipst".

Am anderen Ende der Welt steht die Welt Kopf. Australische Verlagshäuser und Fernsehsender sind im Clinch mit US-Konzernen wie Google und vor allem mit Facebook. Es geht ums liebe Geld.

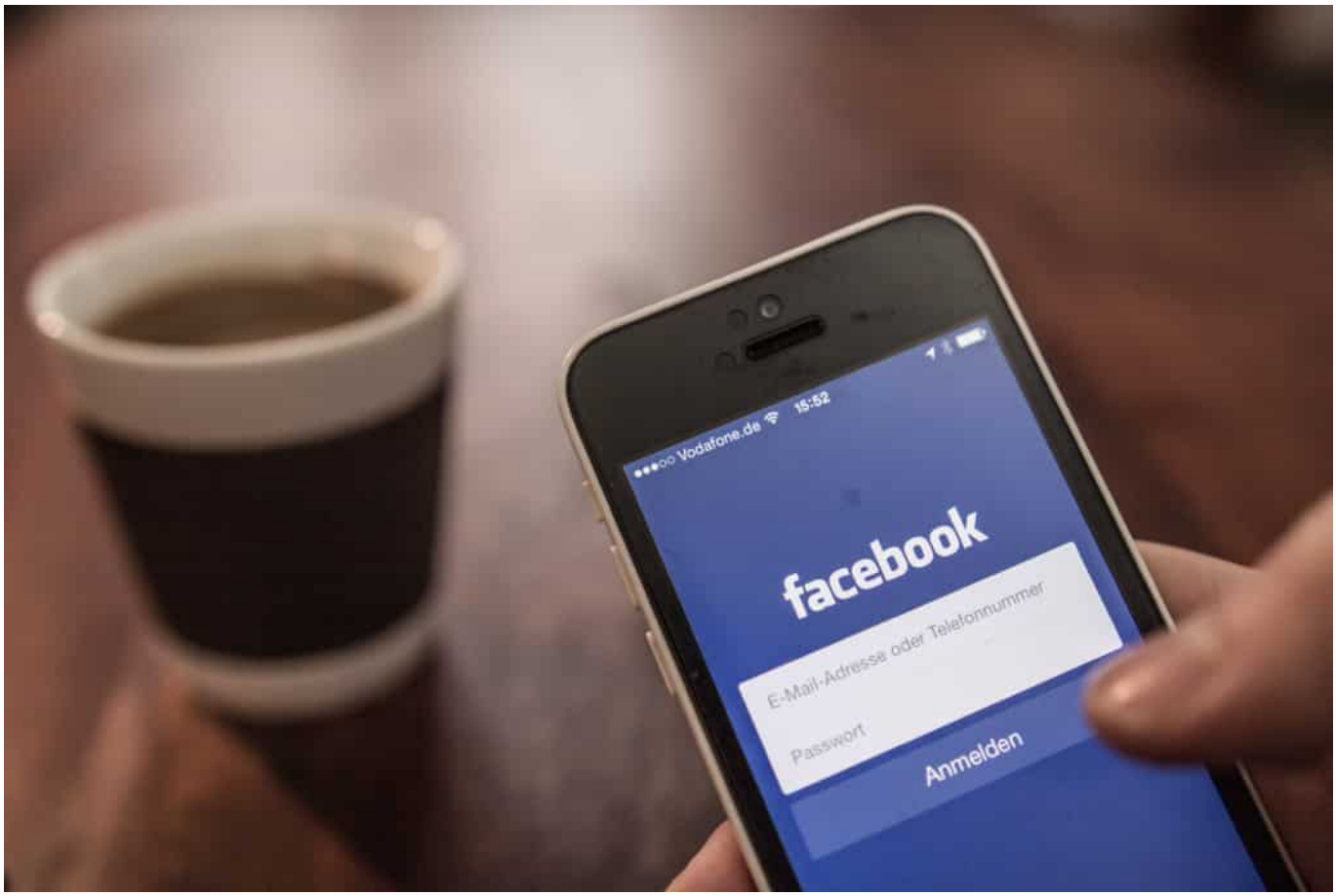
So ähnlich wie bei uns in Deutschland und Europa: Die alten Medien leiden unter der rasanten Entwicklung der neuen Medien, die Marktanteile kosten – und viel Geld verdienen, während Verlage zusehen müssen, wo sie bleiben. Vor allem im Netz. Die australische Regierung hat ein neues Gesetz in Planung, das die Verlage begünstigt. Google und Facebook sollen zahlen. Facebook reagiert ungewöhnlich massiv.

Der Streit ums Geld und den Werbekuchen

Aber worum geht es bei dem Streit in Australien zwischen australischer Regierung, Medienhäusern wie Verlagen sowie Google und Facebook eigentlich?

Es geht natürlich ums Geld. Wie überall auf der Welt haben Konzerne wie Google, Facebook und Co. die Werbemarkt nicht weniger als auf den Kopf gestellt. In Australien ist es so, dass von 100 Dollar Werbeeinnahmen im Netz rund 81 Dollar an Google und Facebook gehen. Das bleibt nicht viel für andere. Eigentlich würden die Verlage auch gerne im Netz verdienen – aber es bleibt nicht genug übrig.

Die australische Regierung will für mehr Gerechtigkeit sorgen und diskutiert im Parlament in Canberra einen Gesetzentwurf, der namentlich Google und Facebook verpflichten soll, Teile der Einnahmen an australische Verlage und Fernsehsender auszuschütten. Eine Art Umschichtung also. Es geht dabei nicht allein um das Zitieren von Texten und Headlines – wie das bei uns beim Leistungsschutzrecht der Fall war und ist –, sondern selbst das Verlinken soll Geld kosten. Klar, dass Google und Facebook da einen Hals kriegen.



Facebook blockiert redaktionelle Inhalte

Facebook hat nun seine Drohungen wahrgemacht und blockiert die Verbreitung von Medieninhalten.

Facebook greift wirklich zum äußersten Mittel: Nutzer können seit Mittwoch keine Medieninhalte mehr sehen oder teilen. Wer die Facebook-Seiten von Fernsehsendern wie ABC oder der Tageszeitung Sydney Morning Herald ansteuert, bekommt bestenfalls noch das Logo zu sehen – aber keine Inhalte. Und wer es versucht, Medieninhalte zu teilen, bekommt einen Warnhinweis präsentiert.

Von der Blockade sind nicht nur australische Medien betroffen, sondern auch ausländische Redaktionen. Sogar hier in Deutschland ist das zu merken: Wer Inhalte australischer Zeitungen verbreiten will, bekommt einen Warnhinweis. Die australischen Medienhäuser selbst können auch keine Inhalte mehr teilen. Facebook hat also vollständig den Stecker gezogen. Mit dem Argument: Wenn wir zahlen sollen, dann nutzen wir die Inhalte eben nicht mehr.

Empörung allerorten

Der Regierungschef schäumt vor Wut – und die Nutzer sind irritiert. Zu allem Überfluss sind nicht nur Inhalte von Medienhäuser von der Blockade betroffen, sondern auch Informationsdienste zum Thema Gesundheit und Notfalldienste. Facebook spricht hier von einem „Versehen“. Aber eins scheint klar: Facebook macht sich mit seinem Muskelspiel wenig Freunde.

Nicht nur in Australien, auch im Rest der Welt. Denn der Streit wird auch hier in Europa genau beobachtet, denn auch hier gibt’s Streit um Geld. Stichwort: Leistungsschutzrecht. Ähnliche Vorhaben, Google, Facebook und Co. ein Stück vom Werbekuchen abzunehmen, gibt es bei uns auch. Aber eine Plattform, die derart eklatant und die Meinungsbildung eingreift – und seriöse Medien einfach ausblendet. Das ist schon ein ungeheurer Vorgang.

Leistungsschutzrecht und Co.

Auch das Leistungsschutzrecht hier bei uns erhitzt die Gemüter. Es muss ein fairer Umgang herrschen. Natürlich würde es nicht gehen, komplette Artikel zu verwenden und dafür nichts zu zahlen. Aber schon Headlines und wenige Zeichen als Teasing berechnen zu wollen – wie bei uns in Deutschland – ist schon ziemlich verdreht.

Denn Google und sogar Facebook sorgen für ein hohes Maß an Sichtbarkeit für die Inhalte der Verlage. In Australien geht der Gesetzentwurf aber ja noch einen Schritt weiter: Sogar das Verlinken von Inhalten soll Geld kosten. Das ist schon einigermaßen verrückt – es widerspricht jedem Prinzip im Internet und lässt sich auch unabhängig davon nicht wirklich plausibel erklären. Die Reaktion von Facebook ist trotzdem krass. Google spricht mit den Verlagen und will sich einigen.

Facebook lässt sich Muskeln spielen und blendet Inhalte komplett aus. Das sollte auf keinen Fall zugelassen werden. Denn Google und Facebook sind Gatekeeper. Seriöse Inhalte auszublenden hat nicht nur wirtschaftliche Folgen, sondern auch gesellschaftliche. Wenn Menschen, die sich vor allem bei Facebook informieren nicht mal mehr seriöse Inhalte sehen können, so ist das eine Katastrophe.

Das kann sich eine Regierung auch auf keinen Fall bieten lassen. Die Welt schaut gerade aufmerksam nach Australien, denn hier wird ein Kampf ausgefochten, der auch überall sonst ausgefochten werden soll – auch hier bei uns in Europa.

Mein Gesicht gehört mir: Kommt ein Verbot für Gesichtserkennung?

Mehrere Verbände und Vereine - darunter auch der Chaos Computer Club - unterstützen eine Petition, die in der EU die Massenüberwachung mit Hilfe von biometrischen Daten wie Gesichtserkennung oder Fingerabdruck verbieten will. Wenn die Petition mehr als eine Million Unterschriften erhält, muss sich der EU-Rat damit beschäftigen.

Unser Gesicht ist wohl eins unserer eindeutigsten Erkennungsmerkmale: Jeder hat eins - und trägt es stets gut sichtbar mit sich herum.

Und es ist heute häufig öffentlich zu sehen: In Fotos, Postings und Videos. Das machen sich windige Unternehmen wie Clearview AI aus New York oder auch PimEyes aus Polen zunutze: Sie sammeln ungefragt im großen Stil öffentlich im Netz zugängliche Fotos und Videos ein, archivieren die enthaltenen Gesichter und erstellen biometrische Daten.

Iris Scan[/caption]

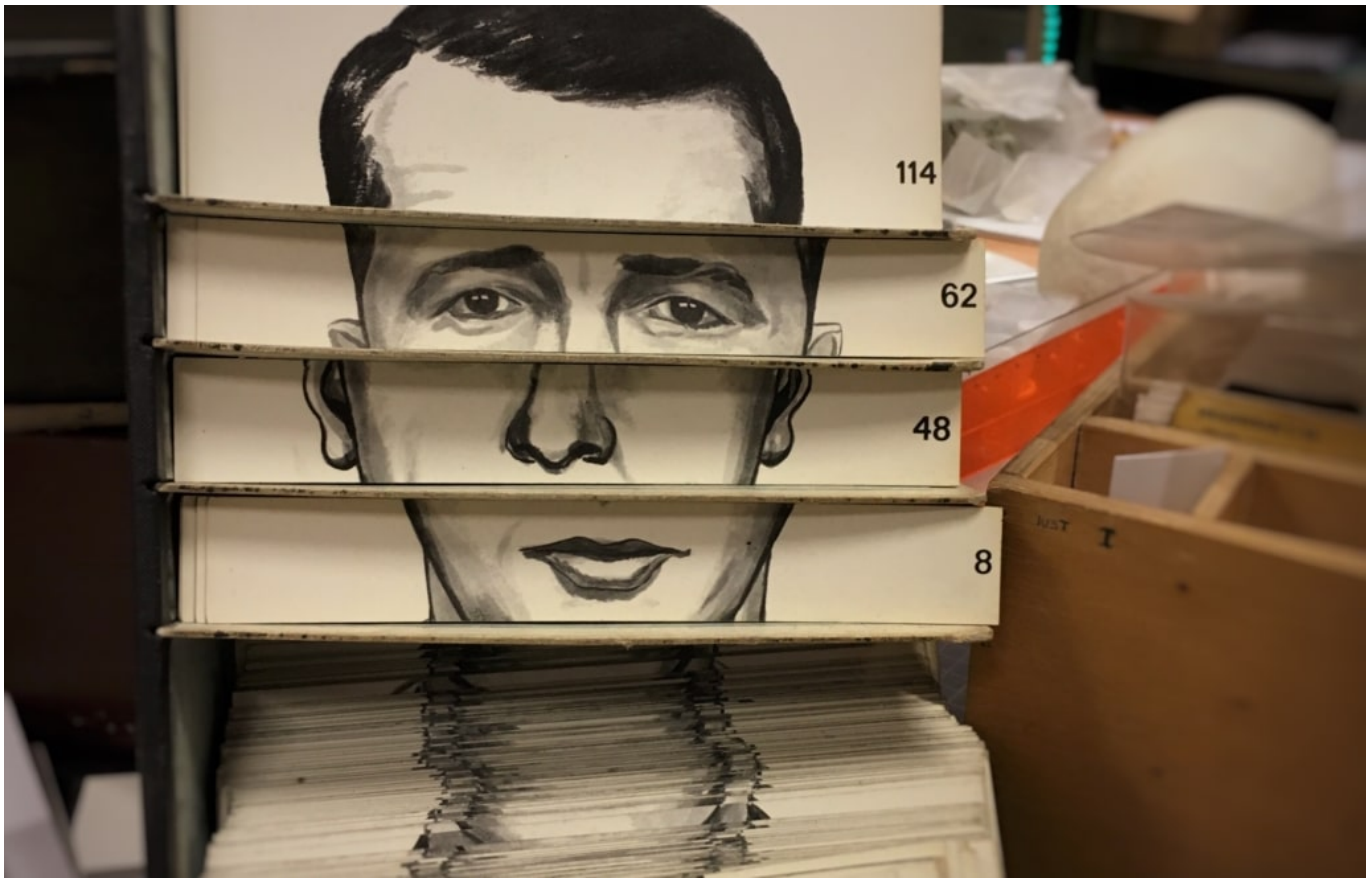
Biometrische Daten sind extrem sensibel - da unveränderlich

Die Folge: Wir sind ganz leicht anhand unseres Gesichts zu identifizieren. Es reicht ein Profilfoto bei Twitter oder Facebook - schon können mich entsprechend gefütterte Systeme mit einer erstaunlich hohen Trefferquote auf einem Foto erkennen. Für ein Sicherheitssystem noch OK - aber ganz sicher nicht, wenn Konzerne damit Geld machen und so jede Privatsphäre verloren geht. Auch noch ohne ausdrückliche Zustimmung der Betroffenen.

Das ist keine kleine Sache. Jeder von uns sollte es selbst in der Hand haben, ob seine biometrischen Daten in einer Datenbank landen - insbesondere in der eines kommerziellen Anbieters. Denn Gesichtserkennung ist ein weiteres, sehr potentes Mittel zur kommerziellen Totalüberwachung. Unsere biometrischen Merkmale sind nun mal unabänderlich. Eine Art "serienmäßig eingebaute Advertising-ID" - so dürfte es die Werbeindustrie sehen.

Wichtig zu wissen: Es ist heute technisch wirklich sehr einfach, Gesichtserkennung umzusetzen. Entsprechende Server sind bei Amazon oder Microsoft ohne weiteres buchbar. Und: Sie funktioniert erstaunlich gut.

[caption id="attachment_773558" align="alignnone" width="1030"]



Europäische Initiative strebt konsequentes Verbot an

Der Chaos Computer Club (CCC) hat sich jetzt deswegen einer europäischen Initiative angeschlossen, die sich Reclaim Your Face nennt und heute (17.02.2021) startet. Wörtlich: Wir sollen die Kontrolle über unser Gesicht zurückerlangen. Zentrale Forderung der Initiative: Das Sammeln von Gesichtern, aber auch anderer biometrischer Daten wie Fingerabdruck, Stimm- oder Gangmuster, Iris etc. als Mittel der Massenüberwachung per EU-Verordnung zu verbieten.

Eine mehr als sinnvolle Initiative, wie ich finde. Denn der unkontrollierten kommerziellen Nutzung gehört ein Riegel vorgeschoben. Es ist allerhöchste Zeit, denn das nächste Clearview AI wartet schon - da bin ich sicher. Und auch Facebook und Co. warten nur darauf, ein sich bietendes Regel-Vakuum zu nutzen.

Traurig genug, dass die Politik nicht von sich aus nach den bereits gemachten Erfahrungen mit Clearview AI, PimEyes und anderen entsprechende Schritte eingeleitet hat. Jetzt wird Druck gemacht - und das ist gut!

Gesichtserkennung: Kommerzielle Anbieter nutzen biometrische Daten ungefragt

Tracker: Sie wissen mehr als die Stasi

Manchmal könnte man doch den Eindruck haben, es müssen unglaublich ausgebuffte Geschäftsleute gewesen sein, die das Internet erfunden haben. Als hätten sie sich gefragt: Wie können wir bequem möglichst alle Menschen auf dem Planeten erreichen, ihnen rund um die Uhr Produkte verkaufen – und damit das alles perfekt klappt, auch noch unbemerkt total gläsern machen?

Dieses Ziel ist jedenfalls längst erreicht – auch wenn das zweifellos nicht die Intention der Leute gewesen ist, die das Vor-Kommerz-Internet aufgebaut haben. Da ging es um hehre Ziele: Unis vernetzen, Informationen austauschen, das Wissen der Welt verfügbar machen.

Der User ist das Produkt

Heute aber werden wir beobachtet, wo wir gehen, stehen, sitzen – oder uns (im Netz, aber auch sonst) bewegen. Wir wissen es. Und lassen es trotzdem einfach so geschehen. Vielleicht, weil man als einzelner sowieso nichts dagegen ausrichten kann? Vielleicht, weil wir unsere Seele verkauft haben. Der Deal: Kostenlose Dienste – dafür aber datentechnisch „nackig“ machen. Der User ist das Produkt

Das haben viele von uns akzeptiert. Aber vielleicht auch nur deswegen, weil sie keine Vorstellung davon haben, was die großen Player alles über die in Erfahrung bringen – und wie sie das machen. Bei der Nutzung von Facebook und Google weiß man natürlich: Wer die Dienste nutzt, hinterlässt eine ordentliche Datenspur.

Doch viel tückischer ist das, was sogenannte „Tracker“ über uns in Erfahrung bringen. So werden Systeme genannt, die uns weit über eine Anwendung oder eine App hinaus beobachten – und alles aufzeichnen, was relevant sein könnte. Ungefragt, in der Regel.

Tracker: Die Stasi der Werbeindustrie

Auf Webseiten bekommen wir einen Eindruck davon, dass es viele solcher Tracker geben muss. Denn ständig müssen wir Cookie-Fenster bestätigen, die immer länger und umfangreicher werden. Ein Indiz dafür, dass mit den Cookies nicht nur der Warenkorb realisiert wird – was ein guter Zweck von Cookies ist –, sondern viel mehr angestellt wird. Die sogenannten „Tracking“-Cookies sorgen dafür, dass wir überwacht und gläsern werden.

Tracker sind die Stasi die Werbeindustrie. Sie bringen früher oder später alles über uns in Erfahrung.

Besonders schwierig ist es bei Apps. Da gibt es keine Cookie-Fenster – aber trotzdem jede Menge Tracker. Laut aktuellen Studien befinden sich im Schnitt(!) in jeder App sechs verschiedene Tracker. Sechs! Fachleute haben jüngst 450 Android-Apps untersucht. Und in allen 450 Apps wurden die Ortungsdaten abgegriffen. In allen 450. Nicht, dass die Apps diese Daten auch nur ansatzweise benötigten.

Data Broker sammeln in unvorstellbarem Ausmaß

Sie werden trotzdem abgegriffen – und an **Data Broker** geschickt. Meist Werbenetzwerke (Google, Facebook, Amazom), die alle Daten gebrauchen können. Denn je mehr Daten, desto präziser das Profil jedes einzelnen. Desto passgenauere Werbung lässt sich präsentieren. Desto mehr Umsatz. Und nur darum geht es schließlich im Netz, oder?

Apple stört die Ausschlachtung der Nutzerdaten zunehmend. Apple hat nicht nur den Safari-Browser so programmiert, dass übereifrige Tracker gestört oder blockiert werden, sondern gerade erst auch eine Initiative angekündigt, die Trackern ganz klar den Kampf ansagt.

Schon bald sollen MacOS und iOS so programmiert sein, dass Nutzern jede Abfrage von Daten angekündigt wird – und eine Freigabe erfolgen muss. Dann kann die Foto-App nicht mehr einfach auf alle Fotos in der Bibliothek zugreifen, um die Standortdaten auszulesen. Oder unbemerkt auf Adressbücher zugreifen oder andere Daten vereinnahmen.

Apple startet Initiative gegen Tracker

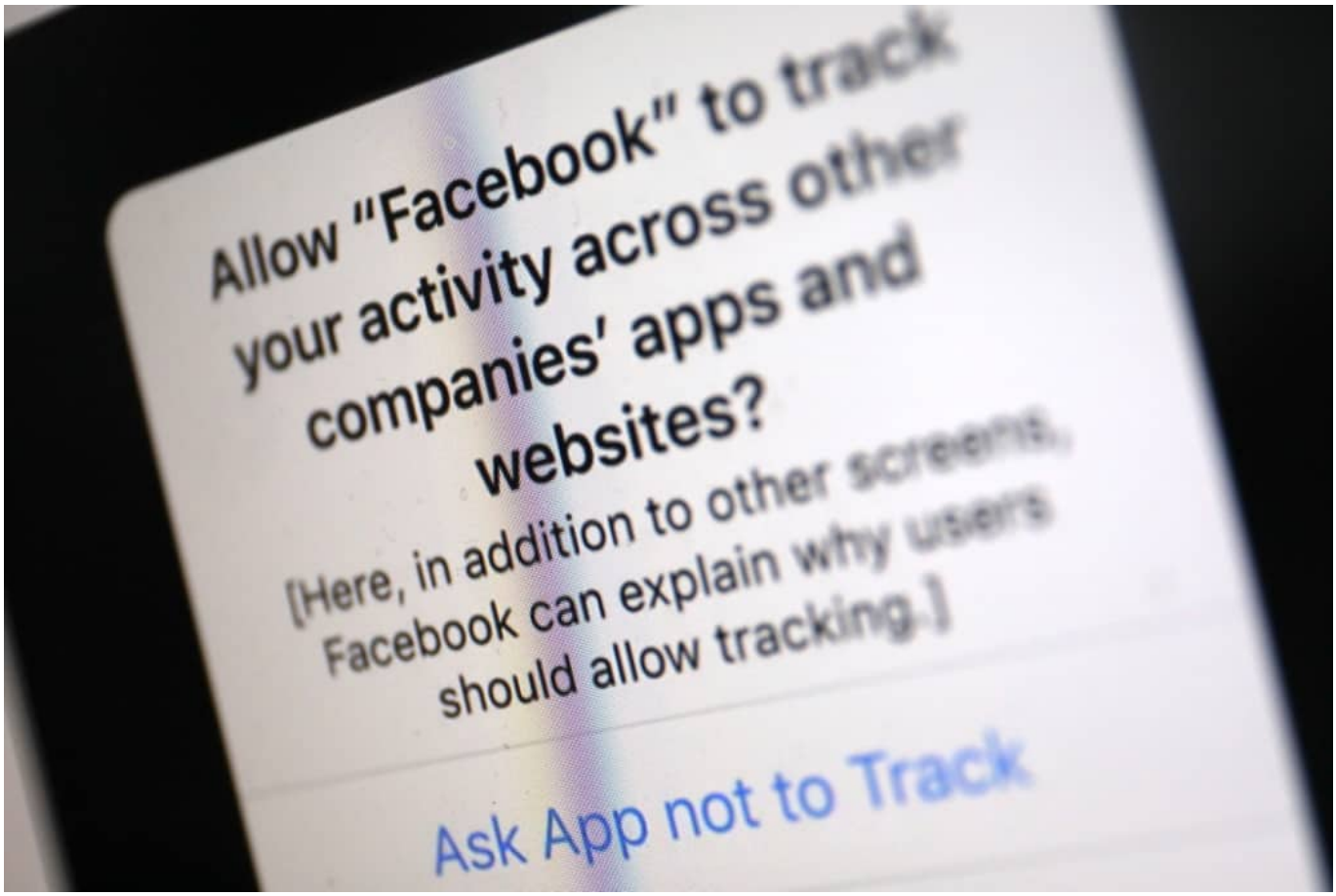
iPhones und Macs zeigen den Nutzern dann auf Wunsch jederzeit an, welche Tracker im Gerät aktiv sind – und in welchen Apps und Anwendungen genau. Es wird dann ein Leichtes sein, einzelne oder alle Tracker zu deaktivieren. Das bedeutet Transparenz und Kontrolle. Richtig so, Apple!

Das macht die Schnüffelsysteme also potenziell blind.

Facebook stört sich enorm an der Ankündigung und zieht regelrecht in den Krieg gegen Apple. Facebook hat bereits eine PR-Kampagne gestartet, weil Mark Zuckerbergs Unternehmen seine Felle davon schwimmen sieht. Denn natürlich wird es durch Apples Intervention in Zukunft deutlich schwieriger, die Nutzerinnen und Nutzer ungeniert auszuspionieren, wenn die das plötzlich merken – und zustimmen müssen.

Um beim Bild zu bleiben: Es macht einen Unterschied, ob man generell weiß, dass man bespitzelt wird – oder ob man weiß, dass auch der Nachbar spitzelt.

Es kommt also mächtig Bewegung in die Sache.



Richtige Richtung: Mehr Transparenz, mehr Kontrolle

Aber warum macht Apple das? Bislang scheint es doch ein unsichtbares Band zwischen allen Silicon-Valley-Konzernen zu geben, das niemand zerschneidet. Alle unterwerfen sich demselben Mantra: Es ist gut, so zu tun, als ob unsere Dienste kostenlos sind. Es ist gut, die Daten und Privatsphäre unserer Nutzer auszuschlachten. Es ist vollkommen in Ordnung, das wir das verdeckt tun und uns damit gesund stoßen.

Apple schert da aus. Aber Apple kann es sich auch leisten. Da Apple nicht davon lebt, Nutzerdaten auszuwerten. Apple kann bei Menschen, denen ihre Privatsphäre nicht völlig schnuppe ist, nun punkten: Seht hier, wie kümmern uns um Datenschutz und Privatsphäre.

Sehr löblich. In diese Richtung sollte es generell gehen. Eigentlich wäre es längst überfällig gewesen, dass die EU solche Regeln einführt und Transparenz und Kontrolle vorschreibt. Zwar sind erste Ansätze in der Politik erkennbar, aber es geht nicht schnell genug. Jetzt plötzlich regelt es der Markt.

Auch Google verspricht weniger Tracker

Selbst Google sieht sich gezwungen, zu reagieren. Nach Apples Vorstoß hat auch Google angekündigt, ähnliche – wenn auch nicht mal ansatzweise so weitgehende – Maßnahmen in Android vorzusehen. Klar: Google schneidet sich ins eigene Fleisch, wenn Tracker abgeschaltet werden. Google lebt von Werbeeinnahmen – und möchte sicher nicht, dass sich das ändert. Doch Facebook trifft es am härtesten. Denn Facebook ist der Weltmeister im Ausschlachten von Nutzerdaten.

Aber bleiben wir realistisch: Tracker und die damit verbundene Industrie dahinter, die Daten sammelt, zusammenführt, bewertet und ausschlachtet hat nur dann ein Ende zu befürchten, wenn wir akzeptieren, dass Dinge Geld kosten. Wenn wir bereit wären, für mehr Apps Geld zu bezahlen – anstatt uns Werbung gefallen zu lassen oder Tracking zu akzeptieren.

Prank-Videos: Youtuber beim Dreh erschossen

Ja: Filme über Streiche sind auch bei "Verstehen Sie Spaß?" oft alles andere als witzig. Aber was auf Youtube, Instagram, Tiktok und Co. als Streich (englisch: Prank) durchgehen soll, ist teilweise erschreckend. Auf die Opfer der teilweise schrecklichen Inszenierungen wird keine Rücksicht genommen - und dann tauchen sie auch noch in Videos auf. Prank Videos sind ein unappetetlicher Trend.

Was würden wir wohl tun, wenn plötzlich zwei junge Männer Anfang 20 wie aus dem Nichts auftauchen und mit langen Fleischermessern bewaffnet auf uns zukommen? Panische Angst wäre eine mehr als natürliche Reaktion. Und wer bei Verstand ist und keinen Fluchtweg entdeckt, macht sich bereit zum Widerstand.

Eine typische "Fight-or-Flight"-Situation: Flüchten oder Kämpfen. Unser Gehirn ist darauf programmiert.

Youtuber erschossen - weil er Menschen zu Tode erschreckt

In den USA hatte das jetzt schlimme Folgen: Ein junger Mann hat einen 20-Jährigen erschossen. Einen mit Fleischermesser in der Hand. Der meinte nämlich, es sei eine witzige Idee, gemeinsam mit einem Freund - ebenfalls mit einem Fleischermesser ausgerüstet - eine Gruppe junger Menschen zu "überraschen" und zu erschrecken - um das Ganze auf Video festzuhalten.

Weil man das halt so macht - auf Youtube und Co. "Prank"-Videos werden solche vollkommen kranken Inszenierungen verharmlosend genannt. "Prank" = Streich.

Jetzt ist der Youtuber tot. Weil in den USA nun mal viele Menschen Waffen tragen - und sich einer aus der angegriffenen Gruppe gewehrt hat. Wer will es einem Opfer eines derartigen Prank-Unsinns verdenken, dass es sich wehrt. Notwehr. Oder - weil keine tatsächliche Bedrohung bestand, diese aber nach vernünftigem Ermessen angenommen werden konnte und musste - Putativ-Notwehr.

Der Youtuber tot. Der junge Mann, der sich wehren musste, vermutlich traumatisiert. Ein toller Spaß, oder?

Prank: Menschen erschrecken soll lustig sein

Und das alles nur, weil es ein Youtuber unterhaltsam findet, Menschen grausame Streiche zu spielen.

Auf Youtube, Instagram, TikTok und Co. verbreitet sich der Trend schon länger. Damit die Videos auch geliked, geklickt, geteilt werden, am besten immer eine Nummer härter als im Video davor. Youtuber verdienen damit sogar Geld - Youtube selbst natürlich sowieso. Abartig.

Ich bin ganz ehrlich: Ich habe dafür nicht das geringste Verständnis. Empathielos, brutal, verrückt. Selbst gemeinhin als "harmlos" geltende Videos sind furchtbar. Was ist zum Beispiel lustig daran, Kleinkinder zu erschrecken, indem man sich in ein Gorilla-Kostüm begibt und sie traumatisiert? Die Kinder erleben einen Schockmoment - und dann werden die kleinen, bedauernswerten Opfer auch noch öffentlich bloß gestellt.

Es gibt kein harmlos - jeder Schrecken hat Folgen

Und wofür? Für Aufmerksamkeit. Schadenfreude. Fame. Für Geld.

Youtube verbietet solche Videos laut Richtlinien - aber nur "bei Streichen, bei denen die Opfer glauben, sie seien in ernsthafter Gefahr". Als Beispiel führt das Portal fingierte Einbrüche oder Schießereien an. Aber auch ein Mensch, der in eine Dose greift und ihm/ihr springt eine Vogelspinne entgegen oder ein zweijähriges Kind, das plötzlich von einem Plüschbären in Lebensgröße angegriffen wird, fühlt sich in Lebensgefahr. Solche Videos sind aber erlaubt und entsprechend zu sehen.

Die Beispiele zeigen: Harmlos gibt es nicht. Zum einen, weil Angst immer traumatisierend sein kann - erst recht, wenn diese Situation nicht selbst gewählt wurde (etwa, indem man ins Kino geht). Zum anderen, weil es genügend Verrückte in dieser Welt gibt, die meinen, in diesen überdrehten Medien alles toppen zu müssen.

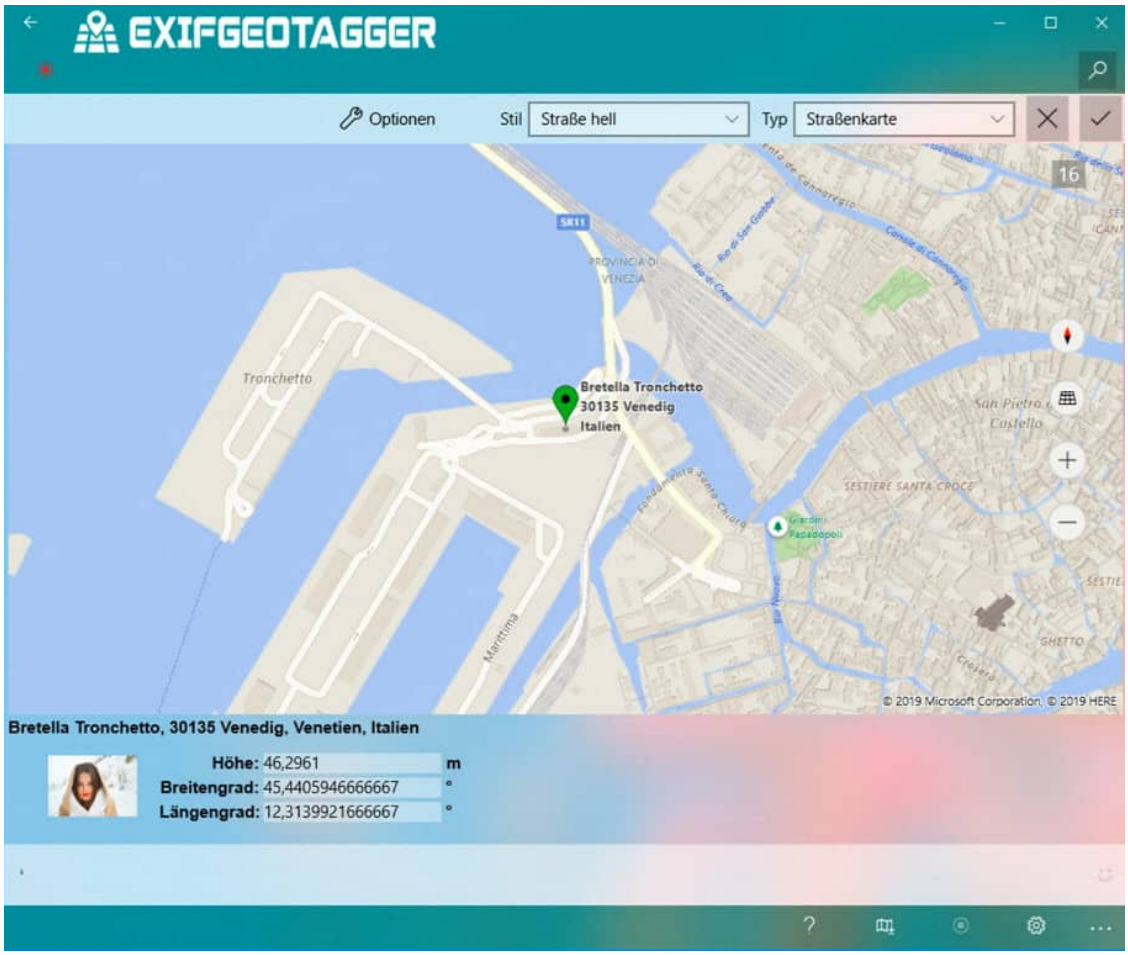
Prank ist nicht lustig. Prank ist krank.

Prank-Videos sind ein großer Trend - werden aber immer grausamer

Geodaten verändern: EXIFGeoTagger

Normalerweise sind sowohl die Smartphone-Kameras als auch die modernen System- und Spiegelreflex-Kameras in der Lage, die Position eines Fotos mit in die Datei zu schreiben. Die so genannten EXIF-Daten enthalten viele weitere Informationen. Diese sind auslesbar und geben Auskunft über die Umstände, unter denen das Foto gemacht wurde. Was aber, wenn Sie Bilder scannen, wo diese Informationen fehlen?

Viele Anwender gehen dazu über, Papierfotos und Dias einzuscannen, um sie digital zur Verfügung zu haben und vor Verfall zu bewahren. Bei diesen gescannten Bildern sind - so das überhaupt hinterlegt wird - das Aufnahmedatum und der -ort falsch. Die Informationen aus dem Fotoalbum, wo "Urlaub Venedig 1970" aufgedruckt steht, wird nicht übernommen.



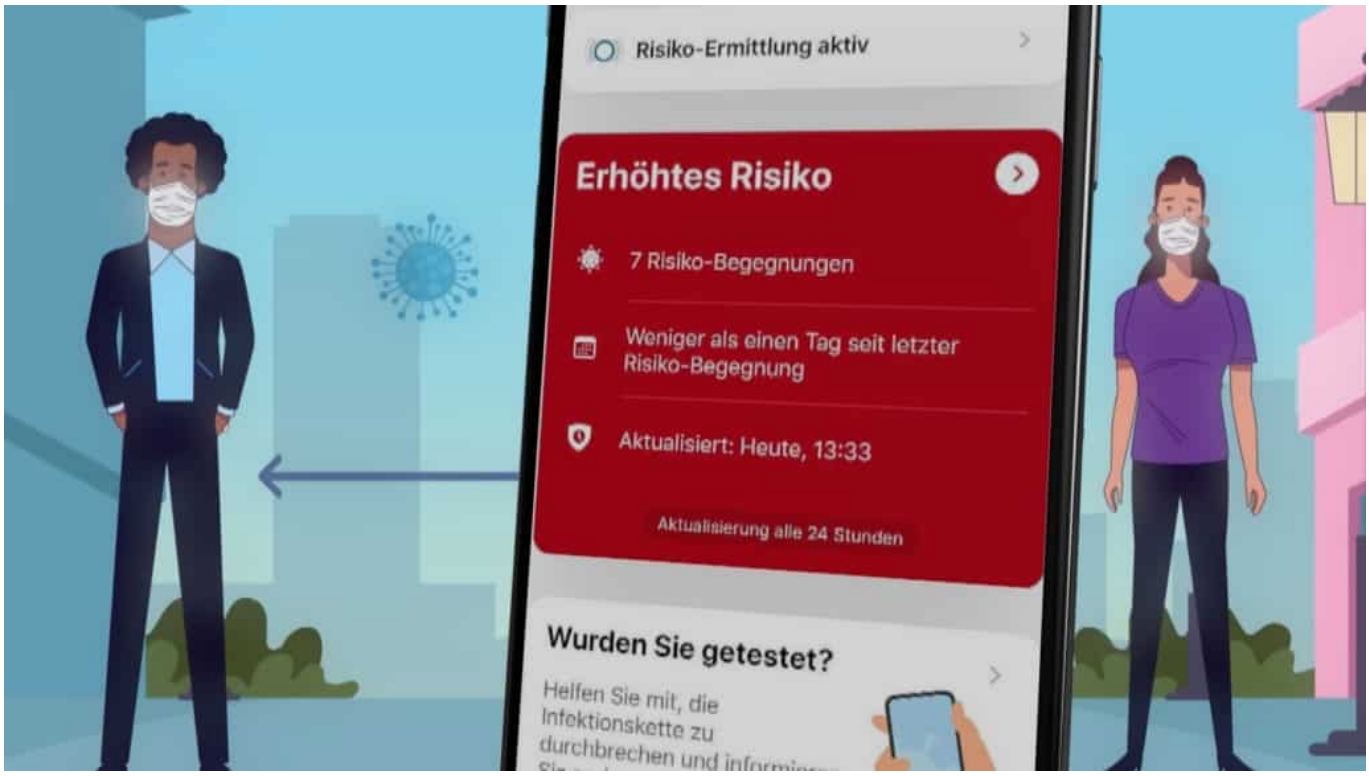
Die 2,49 EUR teure App EXIFGeoTagger für Windows 10 schafft hier komfortabel Abhilfe. Neben der manuellen Pflege der EXIF-Daten einzelner Bilddateien können Sie diese auch für mehrere Bilder übertragen lassen. Nehmen Sie einen ganzen Ordner von gescannten Bildern und weisen sie allen Bildern darin die selben Werte zu. Beispielsweise als Ort "Venedig" und als Datum den 1.7.1970. Natürlich können Sie auch für jedes einzelne Bild die Position ganz genau über eine Karte festlegen, wenn das für Sie sinn macht.

Corona Warn App Version 1.12.1: Das ist neu

Die neue Version der Corona Warn App funktioniert jetzt auch mit älteren iPhone-Modellen und informiert besser über stattgefundene Risikokontakte.

Inhalt:

- Was ist neu bei Version 1.12.1?
- Mit welchen älteren Modellen funktioniert die Warn-App jetzt?
- Was bringt die „Bewegungshistorie“?
- Wie komme ich an die neue Version heran?



Frage 1: Was ist neu bei Version 1.12.1?

Die Entwickler SAP und Telekom haben die Funktionen der Corona Warn App erheblich erweitert. Wichtigste Neuerung: Die Corona Warn App funktioniert jetzt auch auf einigen älteren iPhone-Modellen, auf denen die App bislang nicht funktionstüchtig war. Das lag allerdings weniger an den App-Entwicklern, als an Apple. Denn Apple musste erst sein mobiles Betriebssystem iOS 12.5 für die älteren iPhone-Modelle entsprechend erweitern. Das ist vor einigen Wochen geschehen – und jetzt macht die Corona Warn App von diesen neuen Möglichkeiten Gebrauch.

Neue ist aber auch eine „Begegnungshistorie“: Die App verrät nicht mehr – wie bisher – nur das Datum des letzten Risikokontakts, sondern alle ermittelten Risikokontakte. Das erlaubt es den Nutzern, sich ein besseres Bild vom individuellen Risiko zu machen.

Es sind weitere Updates in Planung.

Frage 2: Mit welchen älteren Modellen funktioniert die Corona Warn App jetzt?

Bislang hat die Corona Warn App auf iPhones wenigstens iOS 13.5 vorausgesetzt. Das kann allerdings erst ab dem iPhone 7 installiert werden. Ältere iPhone-Modelle arbeiten mit iOS 12. Erst vor kurzem hat Apple eine neue Version 12.5 für die älteren iPhone-Modelle herausgebracht, das die nötigen Funktionen zur Verfügung stellt, die den Einsatz der Corona Warn App ermöglichen.

Deshalb lässt sich die Corona Warn App jetzt auch auf allen iPhone-Modellen der 6er-Generation (iPhone 6 und iPhone 6 Plus) sowie auf dem iPhone 5s installieren und nutzen. Die Entwickler schätzen, dass dadurch rund 1,7 Millionen Geräte in Deutschland grundsätzlich dazu befähigt werden, nun die Corona Warn App zu nutzen.

Bei Android-Geräten hat sich nichts geändert.

Frage 3: Was bringt die „Begegnungshistorie“?

Bislang hat die Corona Warn App lediglich mitgeteilt, wie viele Risikobegegnungen es in den letzten 14 Tagen gegeben hat – und seit einer Weile auch, wann der letzte Kontakt gewesen ist. Viele Nutzerinnen und Nutzer haben sich aber detailliertere Informationen gewünscht. Insbesondere für den

Fall, dass es zu mehreren Risikobegegnungen gekommen ist, wann das jeweils war.

Die neue Version der Corona Warn App präsentiert in der „**Bewegungshistorie**“ nun alle erfolgten Risikokontakte. Die Begegnungshistorie wurde dem Kontakt-Tagebuch hinzugefügt. Nutzer der Corona Warn App können freiwillig auf ihrem Handy ein Tagebuch führen. Hier tragen sie ein, wann sie wen wo getroffen haben. Das Kontakttagebuch ist als Erinnerungsstütze gedacht: Im Falle einer Infektion lässt sich dann nachschlagen, zu welchen Begegnungen es gekommen ist. Die Einträge im Kontakttagebuch verbleiben im Smartphone und werden nicht geteilt oder übertragen.

Doch in der neuen Version der Corona Warn App erscheinen in diesen Kontakttagebuch nun auch mögliche Risikobegegnungen. Nicht der genaue Zeitpunkt, aber der Tag. Auf diese Weise kann jeder Nutzer individuell beurteilen, wie riskant die Begegnung möglicherweise tatsächlich gewesen ist. Eine erhebliche Verbesserung zu füheren Versionen, denn da wurde immer nur der jeweils letzte Risikokontakt erwähnt.

Frage 4: Wie bekomme ich die neue Version?

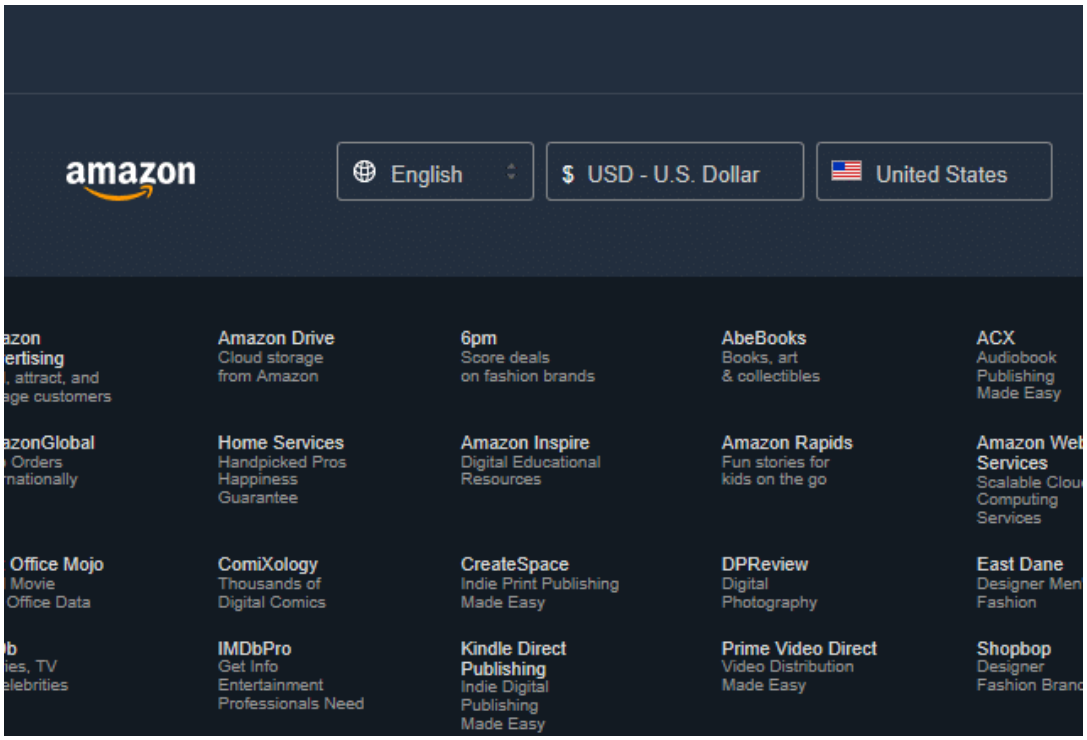
Die neue Version steht zum Download bereit. Sofern sie nicht automatisch installiert wurde, einfach im App-Store die Corona Warn App ansteuern – und den Button zur Aktualisierung antippen. Die App wird dann geladen und installiert.

Ob bereits die neueste Version vorliegt, lässt sich durch Antippen von „App-Informationen“ auf der Startseite herausfinden. Unter den Menüpunkten steht die Versionsnummer der verwendeten App. Sie sollte wenigstens 1.12.1 lauten.

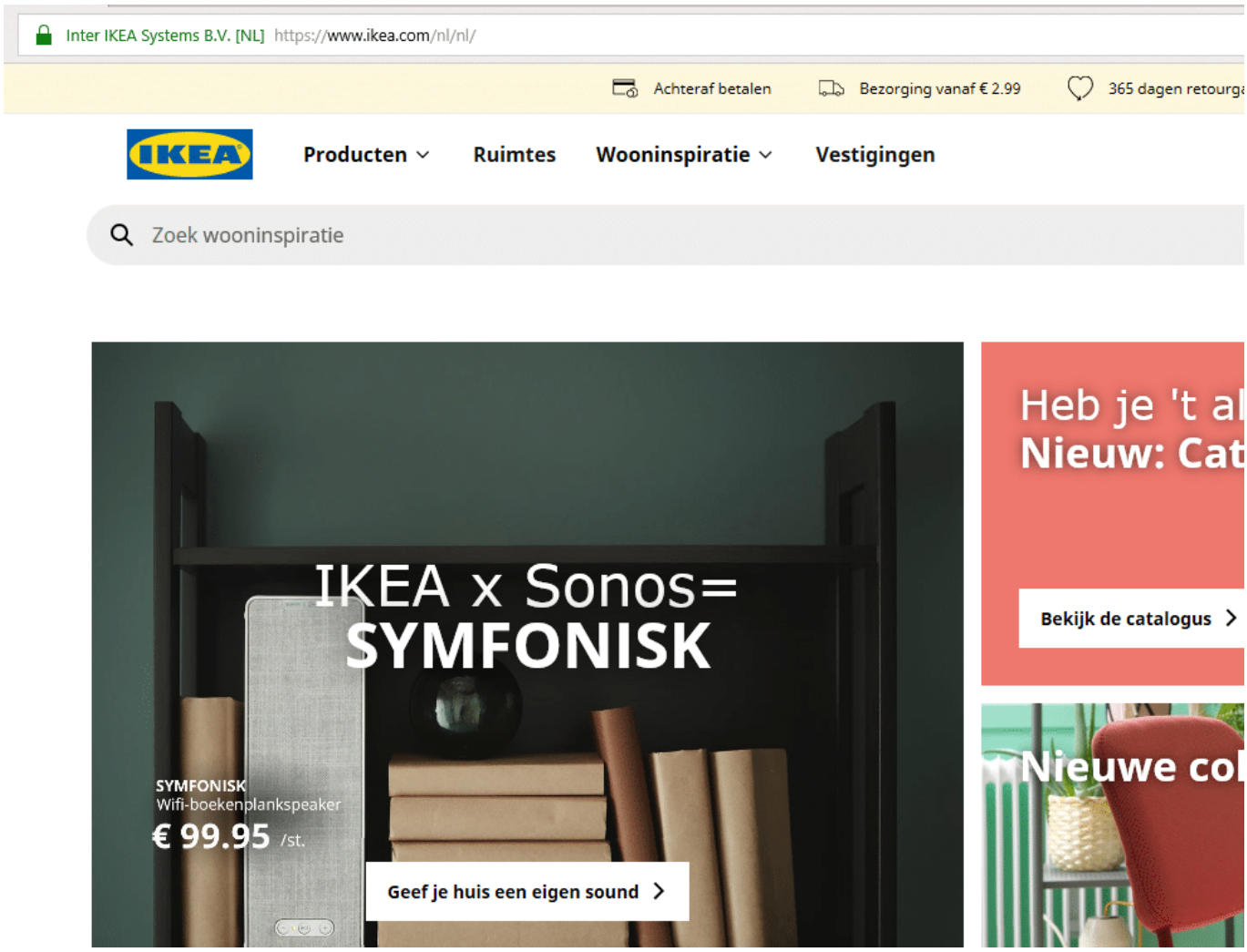
Ändern der Sprache einer Webseite

In vielen Fällen rufen Sie Webseiten nicht durch manuelles Eingeben der Adresse im Browser auf. Stattdessen nutzen Sie Links, die in einer E-Mail oder auf einer Webseite zu finden sind. Wenn die Seite dann nicht auf Deutsch, sondern in einer anderen Sprache angezeigt wird: Wir zeigen Ihnen, wie Sie die Sprache schnell umstellen können!

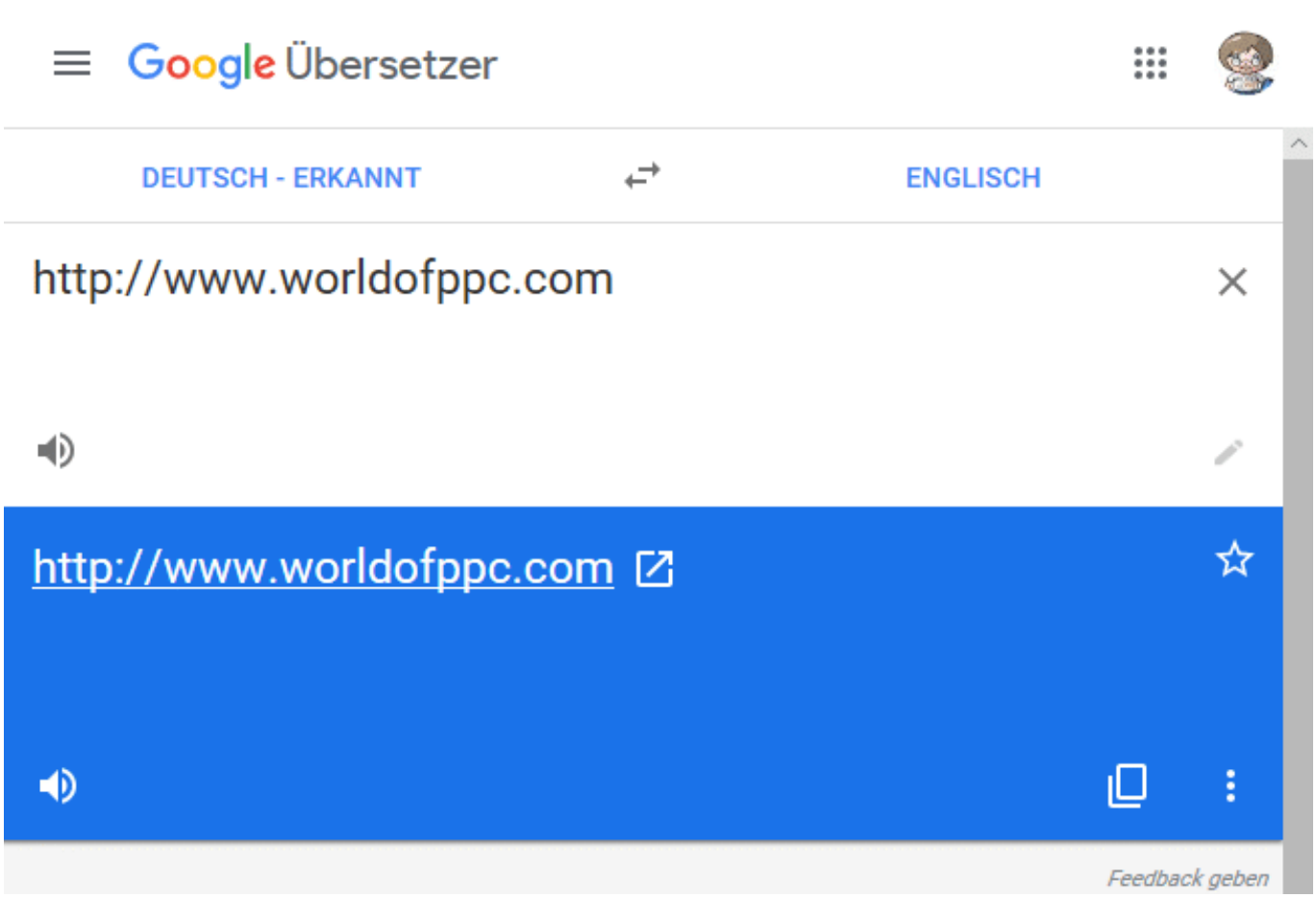
Viele Webseiten erkennen anhand der eingegebenen Adresse, welche Länderseiten Sie aufrufen wollen. Amazon.com beispielsweise führt zur US-Seite, amazon.de zur deutschen Seite. suchen Sie oben oder unten auf der Webseite nach einer Sprach- und Länderauswahl. Oft ist diese durch eine Länderflagge gekennzeichnet. Klicken Sie darauf und dann auf die deutsche Flagge, dann landen Sie auf der deutschen Länderseite. Diese ist dann natürlich gleich in der richtigen Sprache.



Haben sich die Entwickler weniger Mühe gemacht keine Länderauswahl vorgesehen, dann können Sie gegebenenfalls über die Adresszeile des Browsers Einfluß nehmen: Viele Webseiten springen nach Eingabe auf der Adresse automatisch auf eine andere, interne Adresse und zeigen diese auch an. Sie hat meist die Struktur //. Ändern Sie die beiden letzten Angaben einfach auf **/de/de**, also die deutsche Länderseite in deutscher Sprache.



Wenn das ales nichts hilft, dann bleiben Ihnen immer noch Übersetzer-Seiten. Rufen Sie beispielsweise Google Translate auf, und geben Sie die Adresse der zu übersetzenden Seite ein. Stellen Sie Quell- und Zielsprache ein, dann klicken Sie auf den Link in der Übersetzung. Schon wird die Webseite in der Zeilsprache angezeigt.


Google Übersetzer
DEUTSCH - ERKANNT
ENGLISCH
http://www.worldofppc.com
http://www.worldofppc.com
Feedback geben

Wenn das Mikrofon zu leise ist

Podcasts, VLOGs, Videotelefonie, überall benötigen Sie ein Mikrofon. Wenn Sie sich nicht auf meist eher dumpfe Headset-Mikrofone verlassen wollen oder sogar audiophile Ansprüche haben, dann werden Sie schnell auf ein professionelles Mikrofon wie das Shure SM7B oder das Rode NT2-A zurückgreifen. Eine lohnende Investition, aber was, wenn diese plötzlich zu leise sind?

Die meisten professionellen Mikrofone haben keinen USB-Anschluss, sondern einen so genannten XLR-Anschluss. Dafür gibt es keinen direkten Anschluss an den PC: Sie benötigen entweder eine Soundkarte, die das Mikrofon aufnehmen kann oder eine Digital Audio Workstation (DAW). Was diese aber meist nicht berücksichtigen: Viele der Mikrofone benötigen 48V Phantomspannung, die auch der USB-Port nicht liefern können.

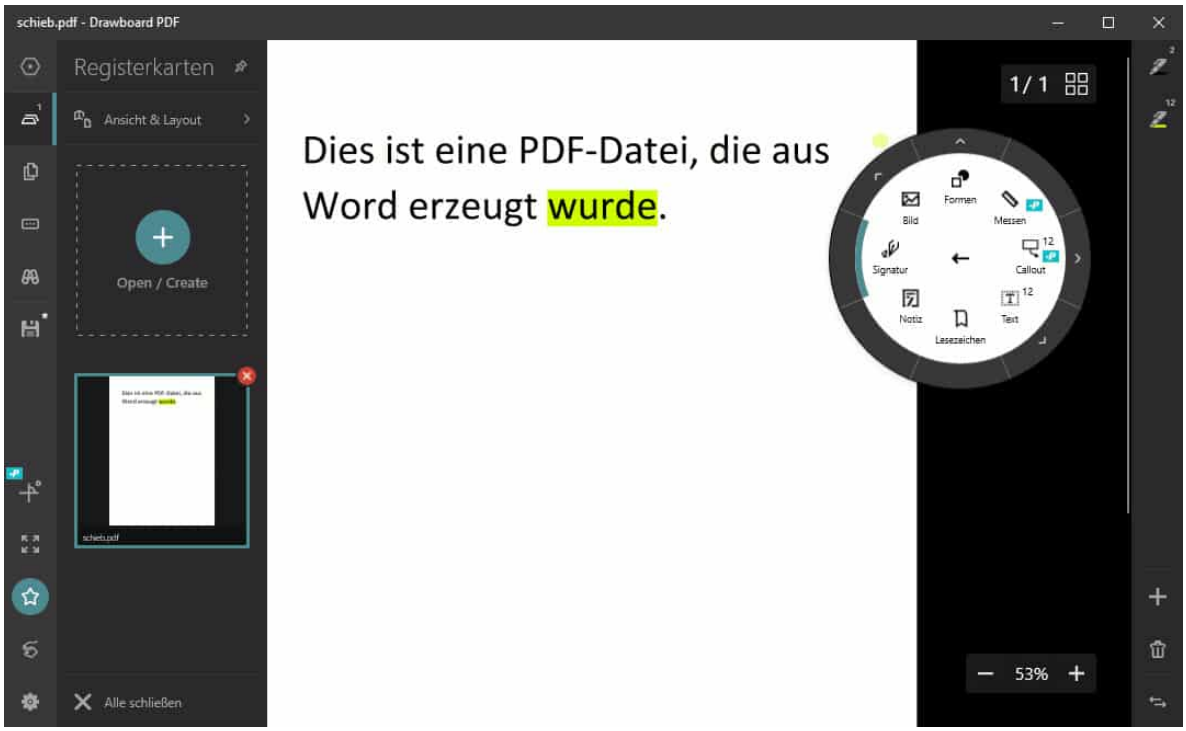
Eine komfortable Alternative sind Umsetzer von XLR zu USB wie das Shure X2U. Die wandeln die Spannung des USB-Ports entsprechend um und funktionieren gleichzeitig als Stromversorgung inklusive Phantomspannung und als Datenanschluss. Damit bekommen Sie auch den entsprechenden Pegel übertragen.

Wenn das Mikrofon zu leise ist, dann brauchen Sie einen Mikrofonverstärker, der das vom Mikrofon aufgenommene Signal möglichst rauschfrei so anhebt, dass Sie nicht scheinen müssen. Hier bietet sich das FetHead von Triton Audio an. Das ist ein kleiner Stecker, der zwischen Mikrofon und Kabel gesteckt wird. Der nimmt die Phantomspannung des DAW auf und nutzt Sie für die Verstärkung des Signals. Das hebt den Pegel deutlich an, ohne dass Sie im Mix die Lautstärke (und damit das Rauschen) stark erhöhen müssen.

Drawboard PDF – Mit Stift und virtuellem Papier

Das Erzeugen einer PDF-Datei ist der eine Schritt, die Bearbeitung ist der zeitaufwändigere und mindestens ebenso wichtige Schritt. Die Bearbeitungsfunktionen von Microsoft Edge und dem Acrobat Reader sind hier sehr rudimentär, hier ist die Windows-App Drawboard PDF, die Sie kostenlos im Windows Store herunterladen können.

Die kostenlose Version von Drawboard PDF erlaubt es Ihnen, mit einer Vielzahl von Stiften und Notiz-Funktionen die PDF-Datei mit Ihren Anmerkungen zu versehen. Wenn Sie ein Gerät mit einem Touchscreen und/oder einem Stift haben, dann können Sie diesen dafür nutzen. Das fühlt sich dann so an. Als hätten Sie ein Papierdokument und einen echten Stift vor sich. Um Ihnen weiteren Platz für Notizen zu geben, können Sie in die PDF-Datei leere Seiten einfügen und diese als Notizblatt nutzen.



Ein zusätzlicher Mehrwert ist die Favoritenleiste, die ihnen links von der aktuell bearbeiteten PDF-Datei die bisher im Programm geöffneten PDFs anzeigt. Über einen Klick auf das rote Kreuz oben rechts in einer der Miniaturansichten können Sie diese aus der Liste löschen. Über die Zeit können Sie sich so eine Favoritenliste pflegen, über die Sie ohne großen Suchaufwand Ihre wichtigsten PDFs direkt zur Verfügung haben, ohne den Speicherort kennen zu müssen oder eine umfangreiche Suche zu starten.

Die kostenpflichtige Version fügt dann noch einige weitere Funktionen wie digitales Briefpapier für die Notizseiten und Funktionen für das Zusammenfassen von PDF-Dateien zu einer einzelnen Datei hinzu. Wenn das für Sie interessant ist, dann können Sie dies im Monats- oder Jahres-Abonnement ab EUR 4,92 pro Monat direkt aus der App hinzubuchen.