Schieb Report

Ausgabe 2021.05

WLAN-Status per App messen

Verschiedene Faktoren können die Qualität der WLAN-Verbindung beeinflussen: Beispielsweise ein Rechner, der Updates herunterlädt und dann im Netzwerk verteilt, ein Familienmitglied, das gerade ein riesiges Update für ein XBOX-Spiel herunterlädt oder eine umfangreiche Datensicherung durchführt. Für solche regelmäßigen Analysen des WLANs empfiehlt sich die routerspezifische App, die die meisten Hersteller anbieten. Wir zeigen Ihnen, wie Sie schnell eine Bewertung Ihres WLAN vornehmen können.

Bei AVM und deren Fritz!Boxen gibt es die App Fritz!WLAN für iOS und Android, die Sie kostenlos herunterladen können. Bei anderen Herstellern gibt es meist ebenfalls entsprechende Apps im App Store beziehungsweise dem Play Store. Nach dem Start zeigt diese Ihnen einen Überblick über Ihr WLAN an. Wenn Sie Mesh-Geräte einsetzen (dazu später mehr), dann bekommen Sie automatisch angezeigt, mit welchem der Repeater Sie verbunden sind. Idealerweise führen Sie die Messung wiederholt an verschiedenen Stellen des Hauses (und damit auch verbunden mit verschiedenen Repeatern) durch.

Um die Messung zu starten, tippen Sie auf WLAN messen. Die App überträgt nun Daten vom Router ans Endgerät und zeigt Ihnen den aktuellen Datendurchsatz an. Auch hier gilt wie bei der manuellen Messung: Der Balken sollte möglichst gerade sein. Zeigen sich dort stärkere Schwankungen, dann ist das WLAN instabil. Das kann verschiedene Ursachen haben.

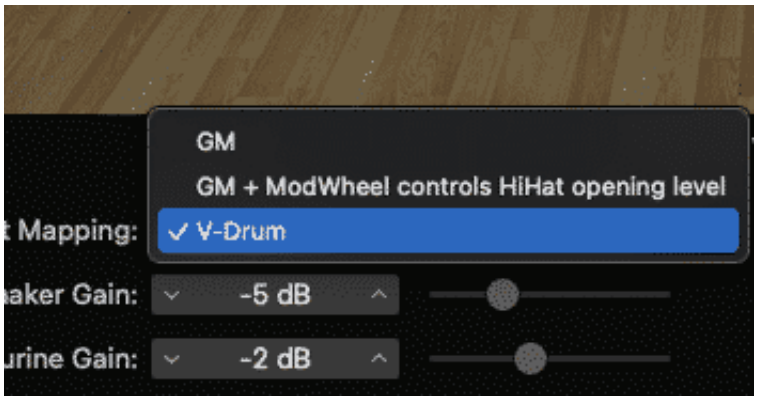
Ein instabiles WLAN hat nicht nur Auswirkungen auf die Geschwindigkeit: Sie haben eher selten das Hauptaugenmerk auf die Übertragung größerer Datenmengen gerichtet, bei der Sie die Geschwindigkeitseinbußen bemerken. Je nach Ursache für die Instabilität brechen Datenübertragungen allerdings nicht selten einfach ab, was Sie eine Menge Zeit kosten kann, wenn Sie nicht direkt vor dem Rechner sitzen und diese neu starten können!

HiHats bei Logic Pro richtig einrichten

Logic Pro ist das Programm, mit denen Einsteiger wie Profis mit wenig Aufwand und einer steilen Lernkurve Musik aufnehmen können. Ob Sie nun nur mit einem Mikrofon oder mit MIDI-Instrumenten arbeiten, Logic Pro führt alles zusammen. Bei einem elektronischen Schlagzeug aber kann es ein kleines Problem mit dem Hi-Hat geben, denn das verhält sich anders als die anderen Teile. Wir zeigen Ihnen, wo Sie die richtige Einstellung vornehmen!

Das Hi-Hat hat zwei Becken, die aufeinander schlagen. Das steuern Sie durch einen Fußschalter. Allerdings klingt das angeschlagene Hi-Hat anders, wenn es geschlossen ist, als wenn es offen ist. Logic Pro muss also unterscheiden, ob der Fußschalter getreten ist oder nicht. Im Standard passiert das nicht: Das Hi-Hat klingt offen wie geschlossen gleich. Um das zu ändern, klicken Sie in die Drumspur, dann links auf **DrumKit**.

Logic Pro zeigt Ihnen jetzt das Kit mit all seinen Elementen an. Klicken Sie dann auf das Hi-Hat und öffnen Sie das Einstellungsmenü unter dem Drumkit durch einen Klick auf den Pfeil. Unter Mapping stellen Sie das Kit von **GM** auf **V-Drum** um.



Das Hi-Hat macht nun beim Anschlag in geschlossenem Zustand den klassischen Hi-Hat-Sound und klingt offen wie bisher.

Medikamente, Masken, Tests und Impfstoffe: Hunderte von Anzeigen für Anti-Covid-Produkte im Darknet gefunden

Data Scientists der City University of London betonen die Wichtigkeit einer kontinuierlichen Überwachung von Darknet, insbesondere angesichts der aktuellen Knappheit an Anti-Covid-19-Impfstoffen.

Neue Forschungen von Dr. Andrea Baronchelli von der **City, University of London** über den Handel mit Anti-Covid-Gesundheitsprodukten im Dark Web haben gezeigt, dass eine kontinuierliche Überwachung des Netzwerks notwendig ist, insbesondere im Hinblick auf die aktuelle Impfstoffknappheit.

In der Studie "Dark Web Marketplaces and COVID-19: before the vaccine", die in der Fachzeitschrift *EPJ Data Science* veröffentlicht wurde, haben Baronchelli und Kollegen zwischen dem 1. Januar und dem 16. November 2020
30 Darknet-Websites überwacht und dort 851.199 Angebote gefunden.

Davon bezogen sich insgesamt **788 Anzeigen direkt auf Covid-19-Produkte**.

Persönliche Schutzausrüstung (PSA), wie z. B. Masken, ist mit 355 eindeutigen Auflistungen (45,1 % der Covid-19-spezifischen Auflistungen) die am **häufigsten vertretene Kategorie. Die am zweithäufigsten vertretene Kategorie sind Pharmazeutika** mit 228 (28,9 %) eindeutigen Einträgen. Eine weitere signifikant vertretene Kategorie sind Scams (medizinischer Betrug) mit 99 (12,6 %) beobachteten eindeutigen Einträgen.

Die Forscher verfolgten die Entwicklung verschiedener Produktkategorien, Medikamente (z. B. Hydroxychloroquin) und gefälschter Gesundheitsprodukte im Laufe der Zeit und verglichen die Trends mit Veränderungen der öffentlichen Aufmerksamkeit, gemessen an Tweets und den meistbesuchten Wikipedia-Seiten.

Sie betonten auch die Wichtigkeit von bestimmten Standorten wie **Dark Bay/DBay**:

> "In unserem Datensatz hat DarkBay eine dominante Präsenz unter den Seiten, die Covid-spezifische Produktlistings anbieten. DBay gehört zu den Top-100-Sites im gesamten Darknet und gilt als das e-Bay von

> Darknet, da es mehr Anzeigenkategorien als andere bietet. Er war im untersuchten Zeitraum zu 80 % der Zeit zugänglich, mehr als 77 % im Falle von Empire, dem zum Zeitpunkt der Studie größten globalen Darknet-Markt."

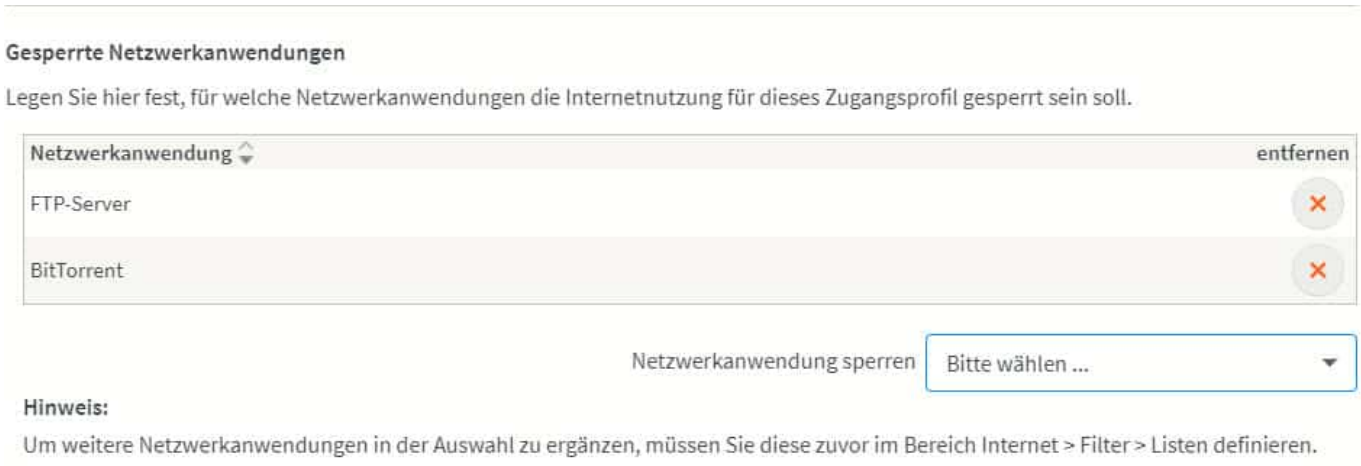
Nach den Autoren ist es wichtig das Darknet kontinuierlich zu überwachen, insbesondere in dieser Zeit, in der es in verschiedenen Regionen der Welt an Anti-Covid-Impfstoffen mangelt:

> "Fehlinformierte Bürger oder Opfer von Fake News können durch Einkäufe im Darknet in Versuchung geführt werden und sich so ernsthaften Gesundheitsrisiken aussetzen. Darüber hinaus untergräbt die begrenzte Verfügbarkeit von Produkten in der Mainstream-Wirtschaft die Vorschriften gegen Spekulation und die Unternehmen, die dieselben Produkte legal verkaufen."

Zugriffsfilterungen unter Windows in der Familie

Wenn Sie für ein Familienmitglied Zugriffe auf Webseiten filtern wollen, dann hat Windows 10 dafür eine integrierte Funktion. Suchen Sie in der Windows-Suchleiste nach **Familienoptionen**, klicken Sie die gefundene Option an und dann auf **Familieneinstellungen anzeigen**. Sie können hier Familienmitglieder verwalten und neue hinzufügen.

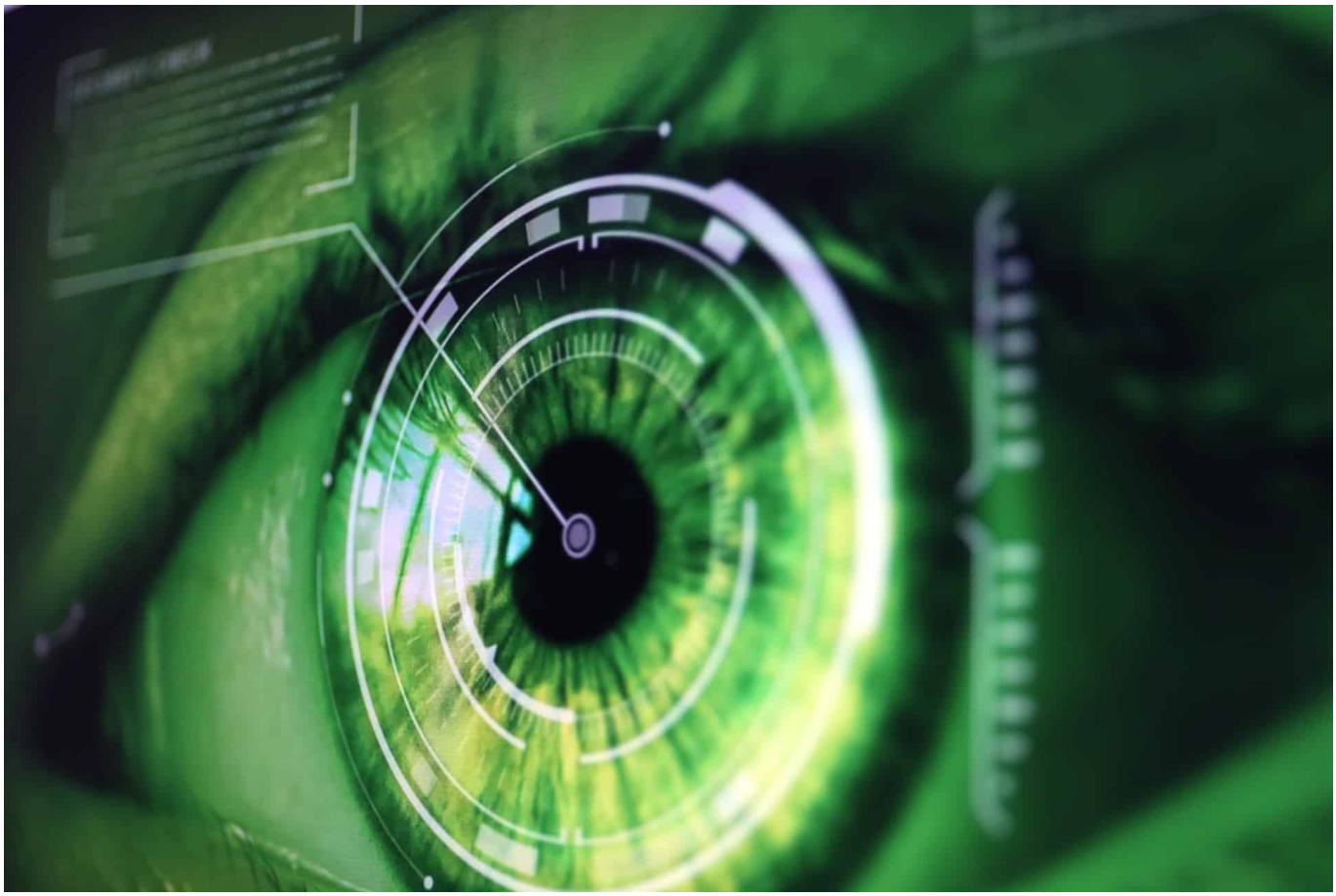
Wenn Sie die Rechte eines Benutzers verwalten wollen, dann legen Sie diesen als **Mitglied** an. Danach können Sie verschiedene Nutzungseinschränkungen vornehmen. So beispielsweise die Zeit, die pro Tag an den angemeldeten Geräten verbracht werden darf, Apps und Spiele, die genutzt werden dürfen und Kosten, die anfallen dürfen.



Für Online-Aktivitäten gibt es unter **Inhaltsbeschränkungen** einen eigenen Bereich. Hier können Sie festlegen, dass nicht jugendfreie Webseiten blockiert werden. Noch interessanter aber: Sie können bestimmte Webseiten blockieren (das so genannte „Blacklisting“) oder aber nur explizit freigegebene Webseiten zulassen („Whitelisting“).

Mit der Familienverwaltung können Sie unter Windows also relativ genau festlegen, was ein Benutzer machen darf. Allerdings richtet sich diese Funktion mehr an eine echte Familie (mit Kindern, denen Berechtigungen erteilt werden), und die Anwender müssen dem Beitritt in die Familie zustimmen.

Vorsicht vor Facebook-Video "Schau mal, was ich gefunden habe!"

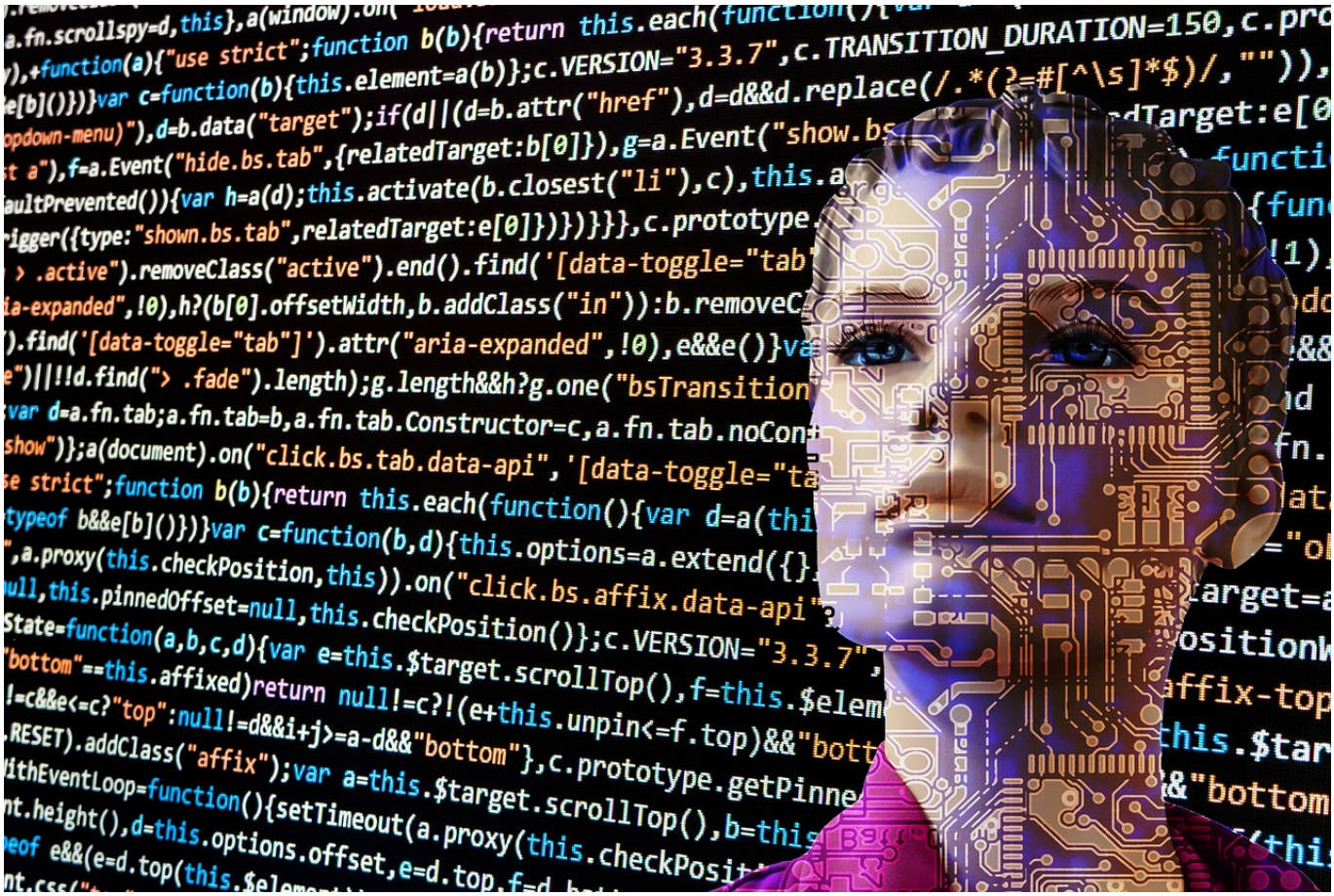


Die Nutzung von sozialen Netzwerken wie Facebook und Twitter bringt automatisch mit sich, dass Sie persönliche Informationen mit der Welt teilen. Da bleibt die Unsicherheit, ob diese manchmal kritischen Informationen an die richtigen Adressaten gehen. Wenn Sie dann von einem vermeintlichen Freund eine erschrockene Nachricht bekommen, ob Sie das in einem Video sind, dann reagieren Sie schnell panisch. Besser nicht!

Genau diese Situation ist bei Facebook sehr verbreitet: Sie bekommen von einem Ihrer Freunde über den Messenger eine Nachricht mit dem Titel "Du bist es??" oder "Schau mal. was ich gefunden habe" und einem vermeintlichen Video. Die Tatsache, dass Ihr Name zusätzlich im Titel steht, vermittelt den Eindruck der Echtheit.

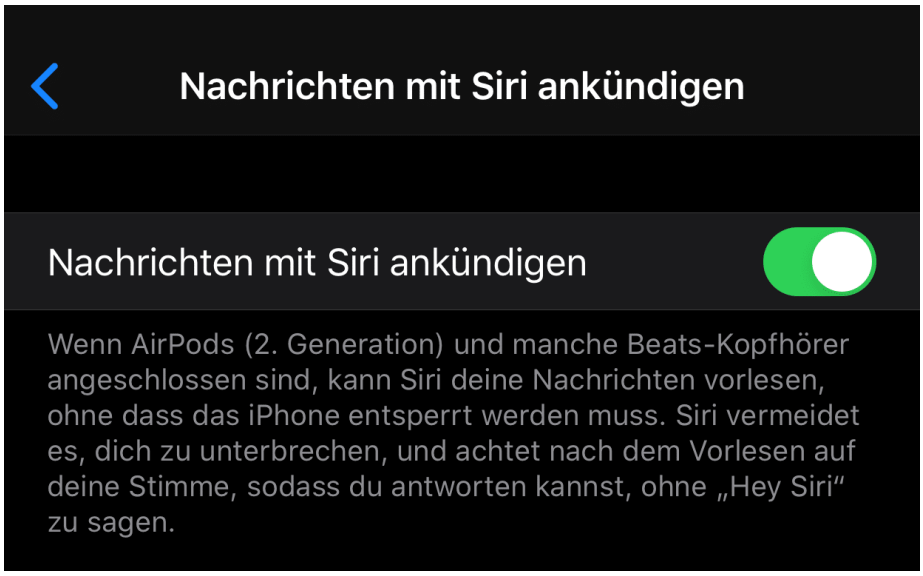
Tatsächlich verbirgt sich hinter dieser Nachricht ein perfider Phishing-Angriff. Wenn Sie auf den Link klicken, dann werden Sie auf eine gefälschte Facebook-Anmeldeseite geleitet. Melden Sie sich an dieser Seite an, dann ist Ihr Facebook-Konto gekapert! Ignorieren Sie die diese Nachrichten und klicken Sie nicht auf die Links darin. Allerdings sollten Sie den Absender informieren, denn dessen Facebook-Konto gehört schon zu den gekaperten!

Automatisches Vorlesen von iMessages auf den AirPods Pro/Max aktivieren

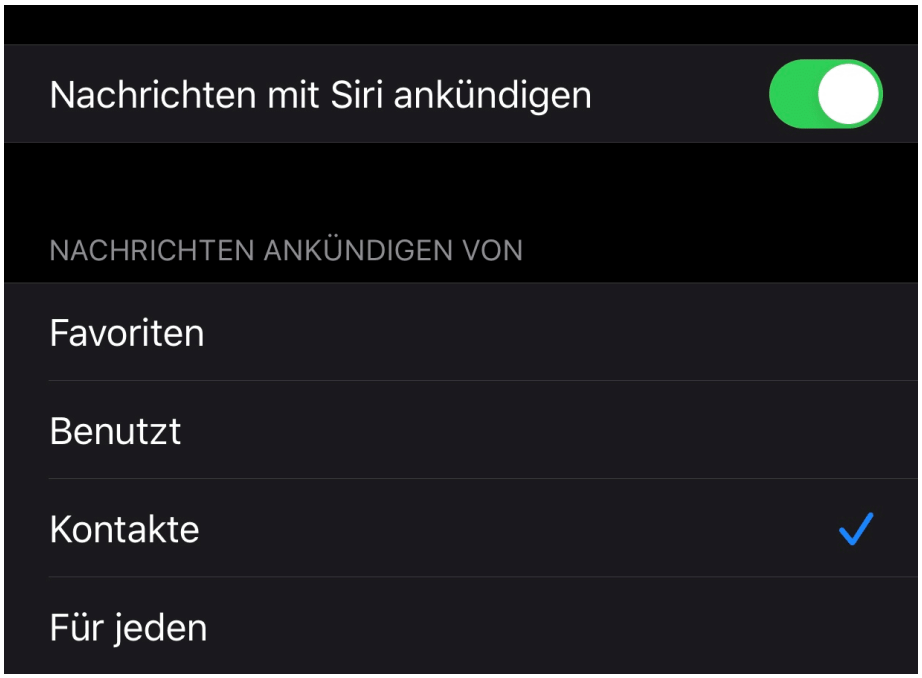


Kopfhörer können nicht nur zum Musikhören verwendet werden, sondern auch zu anderen Dingen. Je ausgeklügelter sie sind, desto mehr Funktionen haben sie. Das gilt auch für die AirPod Pro/Max von Apple. Die haben sogar so viele Funktionen, dass manche sich in iOS gut verstecken. Unter anderem die lange angekündigte Funktion "Nachrichten vorlesen": Wir zeigen Ihnen, wo Sie diese finden.

Auch die AirPods nutzen Siri als Sprachassistenten. Sie aktivieren sie wie gewohnt, indem Sie "Hey Siri" sagen und dann einen Sprachbefehl eingeben. Und genau das ist essentieller Bestandteil der Vorlesefunktion. Tippen Sie in den Einstellungen auf **Siri & Suchen**. In der Liste der Funktionen recht weit unten finden Sie die Option **Nachrichten Vorlesen**. Aktivieren Sie sie.



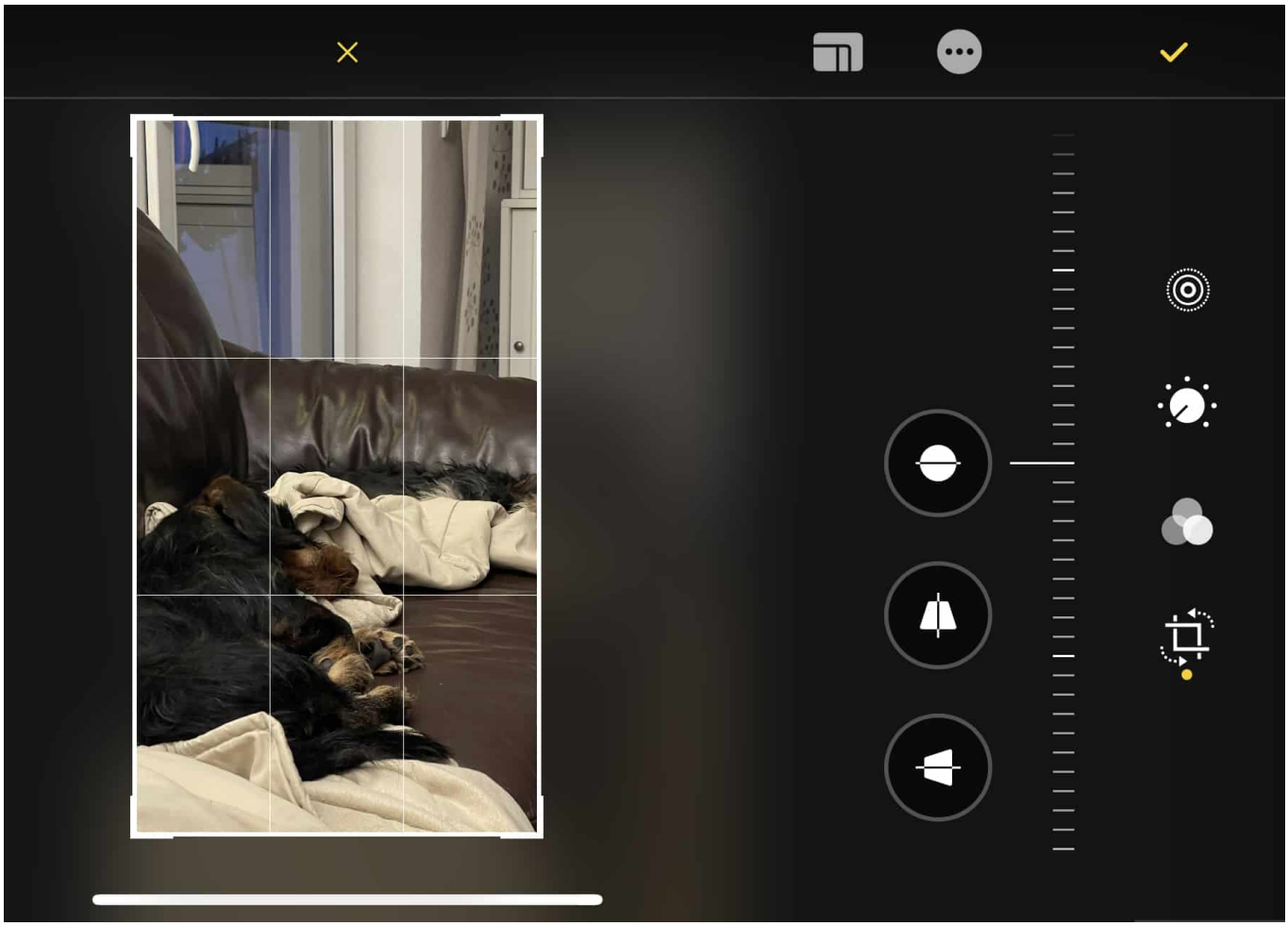
Damit aktivieren Sie für die AirPods Pro und die Airpods der zweiten Generation das Vorlesen der Nachrichten. Je nach der Menge der eingehenden Nachrichten kann das aber durchaus störend sein: Nicht jede Nachricht rechtfertigt das Unterbrechen Ihres Musikgenusses. Auch hier können Sie aber einschreiten: Tippen Sie auch Nachrichten, dann können Sie aus verschiedenen Varianten wählen: Entweder lassen Sie sich alle Nachrichten vorlesen, oder nur die von Kontakten oder Favoriten. Wenn Sie eine Konversation verfolgen wollen, weil Sie auf eine Antwort warten, dann aktivieren Sie **Benutzt**. Damit werden nur die Nachrichten vorgelesen, deren Absender schon im Posteingang vorhanden sind.



Bilder bei iOS frei zuschneiden

Kennen Sie das? Sie haben bisher immer bei iOS Bilder frei zuschneiden können, um störende Randbereiche zu entfernen. Dann kommt ein Update, und schon geht das nicht mehr. Zweifeln Sie nicht an sich selbst, Apple hat hier tatsächlich etwas geändert. Wir zeigen Ihnen, wo Sie die neuen Einstellungen finden!

Statt direkt die freie Anpassung des Rahmens, der den zu beschneidenden Bereich festlegt, nutzen zu können, will iOS nun im ersten Schritt nur noch Beschneiden im Seitenverhältnis des Fotos zulassen. Schieben Sie den Bildausschnitt schmaler, dann wird dieser automatisch auch flacher. Ein freies Bestimmen des Seitenverhältnisses geht erst einmal nicht.



Dafür finden Sie am oberen Bildschirmrand ein neues Symbol links neben dem mit den frei Punkten. Tippen Sie mit dem Finger darauf, dann aktivieren Sie den Freiformrahmen. Diesen können Sie an den Ecken wieder wie gewohnt entweder schmaler oder breiter (oder auch beides gleichzeitig) machen, um den optimalen Bildausschnitt zu erreichen. Es kostet sie eben nur ein Tippen mehr.

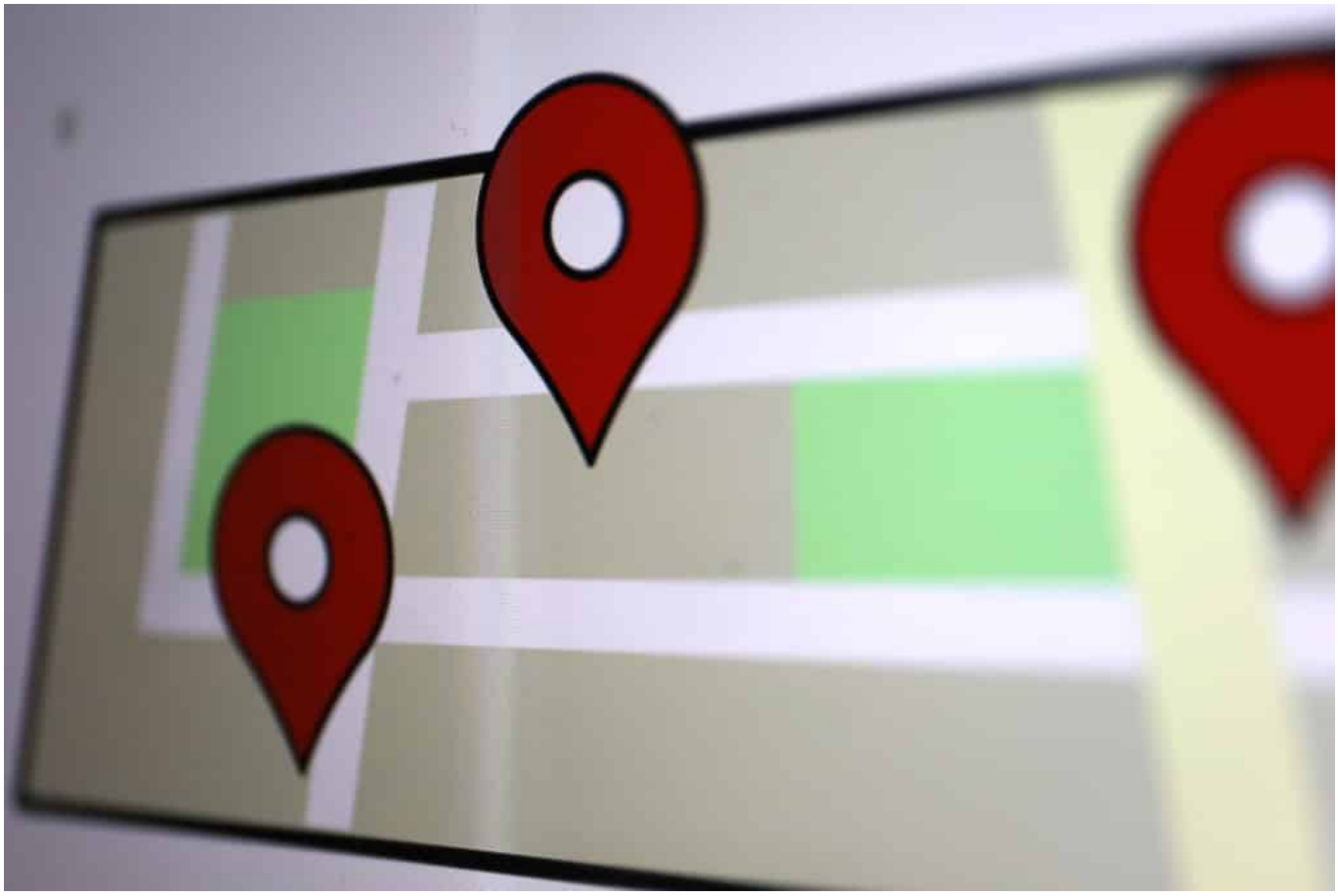
Netzwelt: Apple erhöht die Sicherheit in Apps

Im Web sind die meisten vorsichtig: Jede Webseite präsentiert beim ersten Besuch umfangreiche Übersichten darüber, welche Cookies hinterlegt werden. Nutzer haben die Möglichkeit, dem zuzustimmen – oder eben nicht. Dann dürfen die Cookies auch nicht gespeichert werden. Und das bedeutet in der Regel wenigstens ein bisschen mehr Privatsphäre und Datenschutz. Doch bei Apps gibt es so etwas nicht. Sind die also sicher?

Webseiten müssen uns informieren, wenn Cookies angelegt werden. Bei Apps gibt es so etwas nicht. Bedeutet das, dass es dort auch keine Cookies gibt?

Das ist leider ein Trugschluss. Auch Apps spionieren Nutzer aus – das machen viele Apps sogar sehr intensiv. Jede App enthält laut aktuellen Studien im Durchschnitt sechs sogenannte „Tracker“. Methoden also, die Nutzer der Apps auszukundschaften – in der Regel für die Werbeindustrie. Wo und wann gehen die User online, welche Apps verwenden sie, wofür interessieren sie sich – das lässt sich mit Trackern herausfinden.

Unbemerkt, denn das passiert alles im Hintergrund. Diese Daten sind sehr wertvoll und lassen sich von der Werbeindustrie auf dem Smartphone ausschlachten. Bei jeder App, die wir benutzen, füttern wir im Schnitt sechs Tracking-Systeme mit Daten.



Kostenlose Apps tracken häufiger

Wir sollten uns öfter mal fragen: Wieso gibt es eine App kostenlos? Klar, bei der ARD Audiothek zum Beispiel liegt es auf der Hand. Die App ist von Gebührengeldern finanziert. Aber die meisten müssen die nicht unerheblichen Entwicklungskosten für eine App wieder reinbekommen. Wenn sie kein Geld dafür nehmen von den Nutzern, finden sie einen anderen Weg. Manche zeigen innerhalb der Apps – etwa Spielen – Werbung.

Dann sehen wir zumindest, wie die App refinanziert wird. Bei manchen Apps erscheint aber keine Werbung, und sie spionieren uns trotzdem aus. Das machen „Tracker“ im Hintergrund. Sechs davon im Durchschnitt pro App. Das bedeutet: Manche Apps deutlich weniger oder gar keine, andere aber auch 12 oder mehr Tracker. Und wir merken es nicht einmal.

Tracker ablehnen - das geht normalerweise kaum

Auf Webseiten kann ich die Cookies ablehnen. In der Welt der Apps gibt es etwas Vergleichbares noch nicht. Doch Apple arbeitet daran: Seit einigen Wochen erfahren Nutzer von iOS und MacOS in den entsprechenden App-Stores, welche Angaben die Entwickler der Apps über die erhobenen Daten machen. Sie müssen genau angeben, welche Daten aus dem Gerät gelesen und verarbeitet werden, etwa Kontaktdaten oder Kalenderdaten. Das ist schon mal ein Fortschritt.

Doch jetzt hat Apple angekündigt, in den nächsten Versionen seiner Betriebssysteme – die alle im Frühjahr erscheinen sollen – deutlich mehr Funktionen anzubieten, die auch Tracker betreffen. Die Nutzer sollen die Möglichkeit haben zu sehen, welche Tracker im Gerät aktiv sind – und bei welcher App. Und: Die Nutzer können die Tracker auch jederzeit bequem abschalten. Das führt dann dazu, dass die Apps keine Daten mehr erheben und weitergeben können, wenn die Nutzer das nicht wollen. Also deutlich mehr Privatsphäre und Datenschutz für die User.

Apple kann das, Google kaum

Das klingt doch nach einer begrüßenswerten Entwicklung. Warum nur bei Apple?

Der große Vorteil von Apple ist, dass das Unternehmen sein Geld nicht mit dem Auswerten von Nutzerdaten verdient. Deshalb hat Apple kein Interesse daran – und unterstützt tatsächlich aktiv den Datenschutz. Die Werbenetzwerke freut das nun nicht gerade.

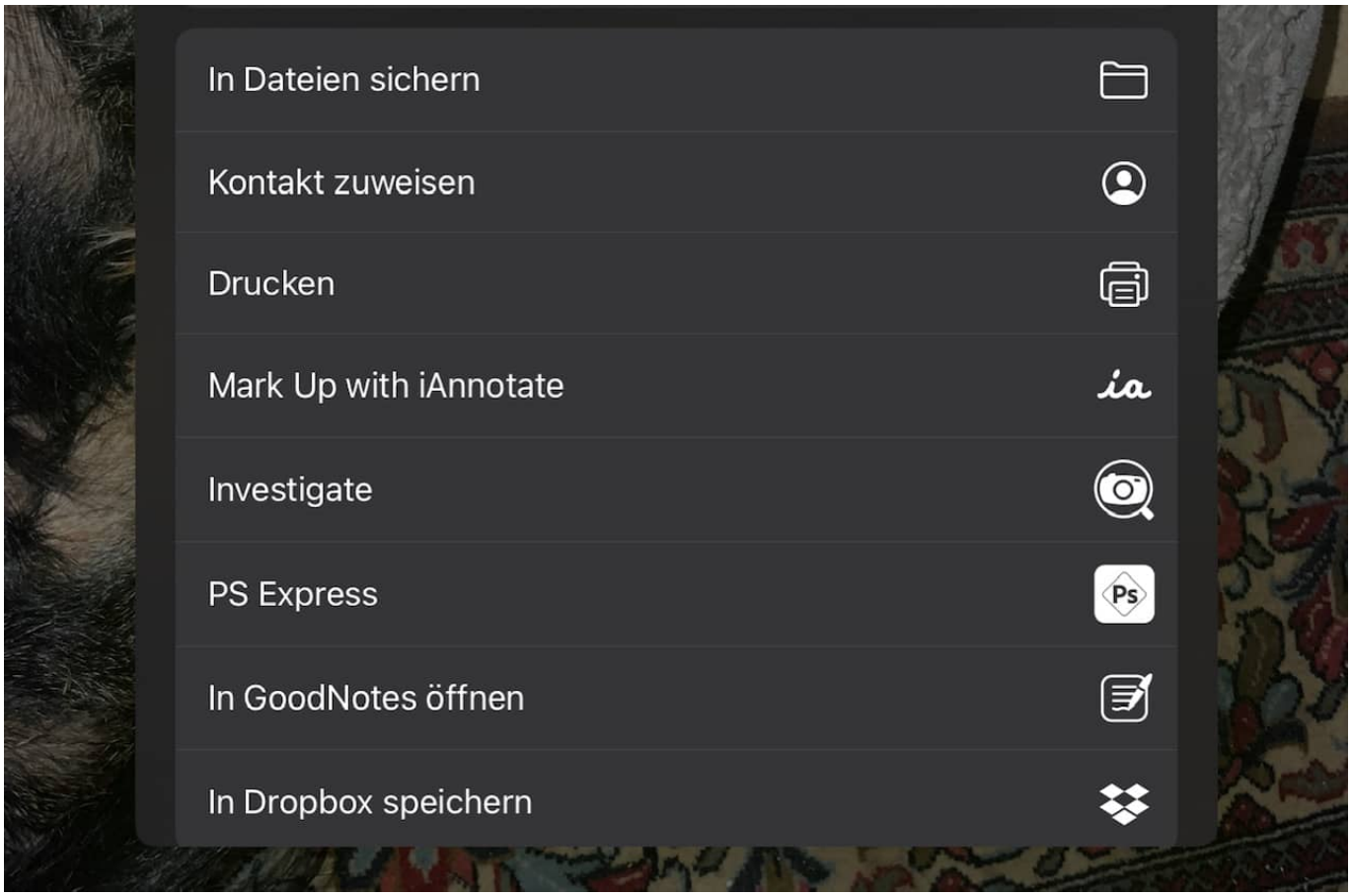
Für Facebook ist das ein riesiges Problem. Mark Zuckerberg erklärt Apple deshalb aktuell auch zum größten Rivalen. Auch Google dürfte sich darüber nicht freuen – Google betreibt ein sehr großes Werbenetzwerk. Google wird eine ähnliche Transparenz wohl kaum in Android einbauen, denn dann würde sich Google ins eigene Fleisch schneiden.

Die jüngsten Vorschläge und Entwicklungen bei Apple taugen eigentlich fast als Blaupause für entsprechende Vorschriften. Die EU sollte eine Transparenz und Gestaltungsmöglichkeit vorschreiben, wie sie Apple nun anbietet.

Fotos direkt als PDF versenden auf iOS

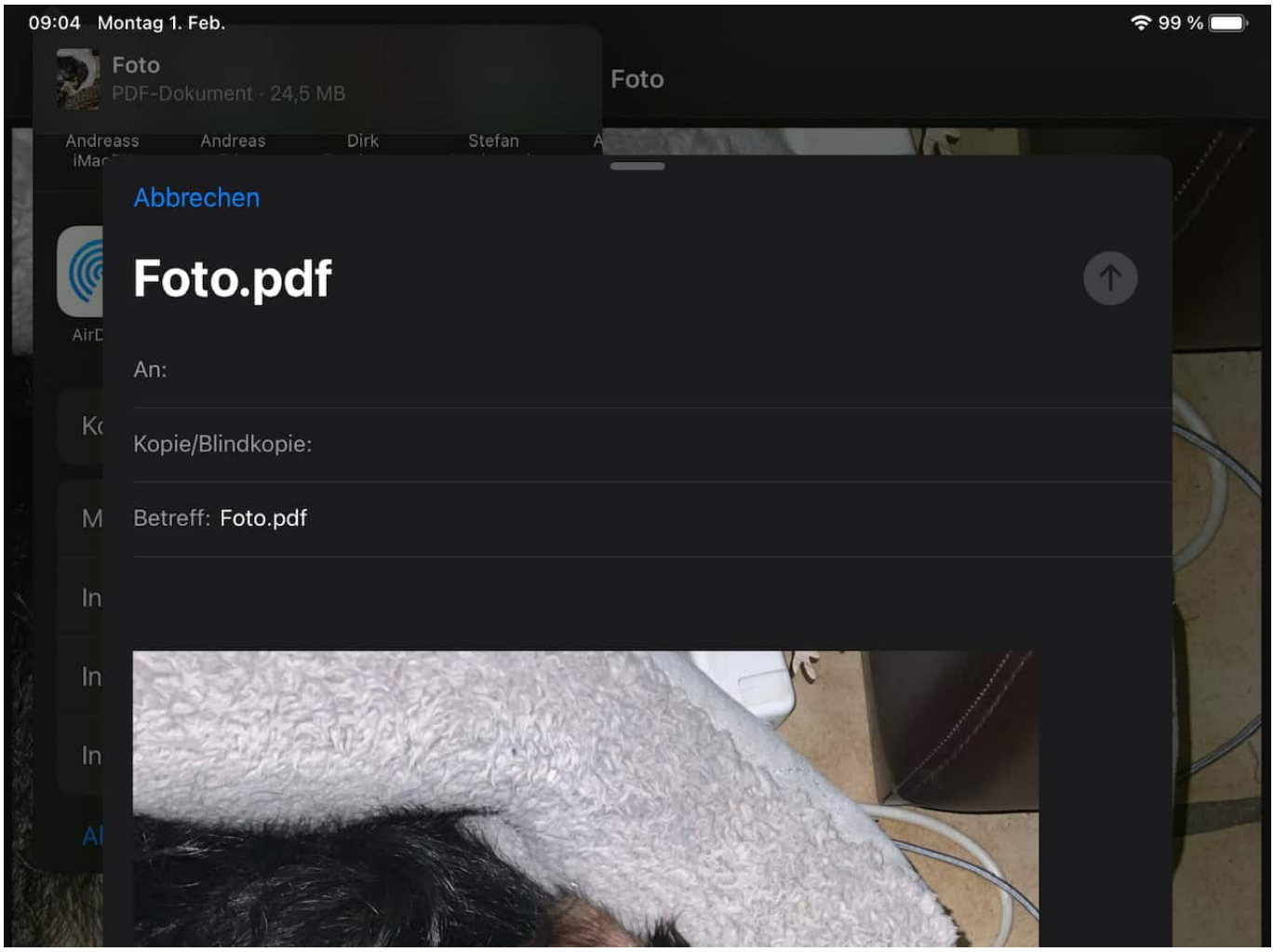
Die Schnittstelle der analogen zur digitalen Welt ist frei schwebend. Auch wenn Sie bestimmte Dokumente immer noch in Handarbeit und auf Papier erstellen, müssen diese doch elektronisch auf die Reise geschickt werden. Wenn der Scanner nicht in der Nähe ist, dann hilft hier auch das Smartphone. Wir zeigen Ihnen, wie das geht!

Viele Anwender können mit einem einzelnen Foto nicht viel anfangen: Ob es nun eine Baustellenbegehung, eine Fotodokumentation oder die Kunst-Hausaufgabe im Homeschooling ist, der Empfänger erwartet eine PDF-Datei. Bevor Sie nun Mühe in die Installation einer App und deren Bedienung investieren, können Sie auf einem iOS-Gerät mit aktueller Betriebssystemversion eine integrierte Funktion nutzen.



Wenn Sie ein Papierdokument haben, dann fotografieren Sie es mit der integrierten Kamera Ihres Gerätes. Wechseln Sie nun in die Fotos-App. Markieren Sie durch ein Tippen auf **Auswählen** und Antippen der Bilder alle Bilder, die in die PDF eingehen sollen.

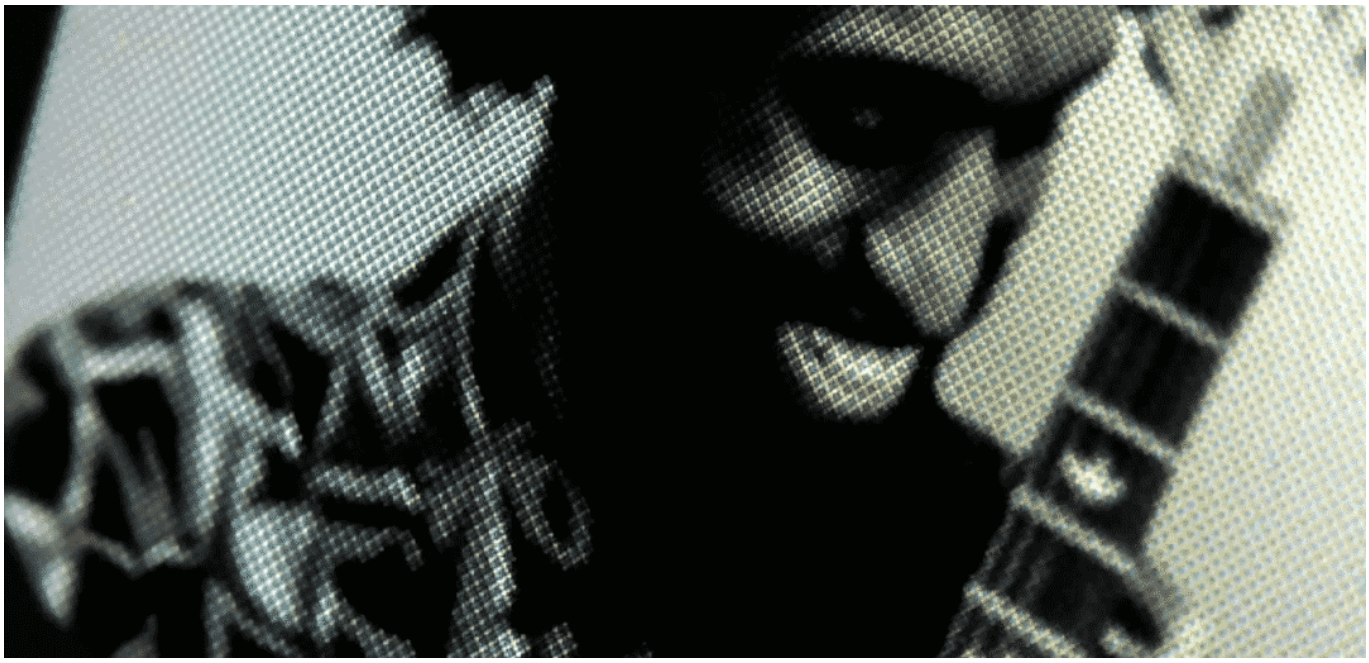
Zum Erstellen der PDF-Datei müssen Sie jetzt einen kleinen Umweg gehen: Tippen Sie auf das **Teilen**-Symbol und auf **Drucken**. Statt einen Drucker auszuwählen, wischen Sie in der Voransicht mit zwei Fingern auf dem Bildschirm auseinander, als wollten Sie das Bild vergrößern. Dieses wird dann auf dem kompletten Bildschirm dargestellt.



Auch wenn das auf den ersten Blick nicht zu erkennen ist: Jetzt haben Sie bereits eine PDF-Datei in den virtuellen Händen. Tippen Sie wieder auf das **Teilen**-Symbol, um diese Datei per OneDrive, Dropbox oder einem anderen Programm zu teilen.

Wenn Sie diese noch bearbeiten möchten: Sie finden Sie über die **Dateien-App** von iOS unter **Downloads** mit dem Namen **Neueste Fotos anzeigen**!

Clubhouse und die DSGVO



Die Datenschutzgrundverordnung (DSGVO) schreibt klipp und klar einige Dinge vor, etwa deutschsprachige Nutzungsbedingungen - und sorgsamen Umgang mit persönlichen Daten. Die derzeit so populäre Clubhouse-App verstößt gleich gegen mehrere Aspekte der DSGVO - ist aber trotzdem nach wie vor im App-Store von Apple.

Die Audio-App Clubhouse erlebt bei uns in Deutschland aktuell einen regelrechten Hype. Zumindest bei Branchen-Insidern, Journalisten und einigen Politikern. In virtuellen Räumen mit anderen sprechen zu können – tatsächlich sprechen, mit der eigenen Stimme! –, das ist durchaus eine charmante Idee und ein interessantes neues Konzept.

Clubhouse wirkt auf viele wie ein neues Spielzeug auf Kinder: Alle wollen damit mal spielen.

Es gibt reichlich Kritik an Clubhouse [illegible] Kritik!

Kritik am mangelnden Datenschutz - und Verstoß gegen DSGVO

Doch die Verbraucherzentrale Bundesverband (VZBV) hat die Clubhouse-Anbieter schon wegen gravierender rechtlicher Mängel abgemahnt. Unter anderem wegen des fehlenden Impressums und weil es keine deutschsprachigen Datenschutzbestimmungen gibt. Das teilte VZBV-Vorstand Klaus Müller jetzt auf Twitter mit.

Datenschützer kritisieren zum Beispiel die Praxis von Clubhouse, alle geführten Gespräche intern aufzuzeichnen – und vor allem, dass Nutzer ihr komplettes Adressbuch bei Clubhouse hochladen müssen. Mittlerweile weiß man: Es werden nur die Nummern hochgeladen, nicht die Namen. Aber eben alle Nummern.

Nummern werden mehrfach übertragen

Mehr noch - Experten haben herausgefunden: Die App überträgt sogar jedes Mal die Nummern im Adressbuch, sobald ein Clubhouse-User jemanden einladen möchte. Auf diese Weise bekommt Clubhouse mit, welche Nutzerin wann wen kennengelernt hat. Das traut sich nicht einmal WhatsApp. (Mal abgesehen von der Tatsache, dass es keine Nutzungsbedingungen in deutscher Sprache gibt.)

Das wirft die Frage auf, wieso eine App, die eindeutig gegen die DSGVO verstößt, in der EU überhaupt im App-Store von Apple auftaucht?

https://soundcloud.com/user-999041145/hype-um-clubhouse-app-wdr-5-tone-texte-bilder-interviews-23012021

App-Stores sollten Verantwortung übernehmen

Nutzer vertrauen zu Recht darauf, dass Apps im App-Store gewissen Mindeststandards genügen. Apple unternimmt gerade eine Menge, um die Transparenz bei Apps zu erhöhen. Meine Forderung wäre, dass die App-Stores aktiv einen DSGVO-Check machen müssen. Apps, die nicht DSGVO-konform

sind, gehören entweder überhaupt nicht in einen Store – oder sollten zumindest mit einem dicken, fetten Warnhinweis versehen sein. Oder wieder aus dem Store verschwinden.

Der auf Internetrecht spezialisierte Anwalt Christian Solmecke meint nämlich dazu: "Nach Kenntnis der Rechtsverstöße sind App-Stores möglicherweise verpflichtet, die Angebote abzuschalten." So, wie Facebook Hasskommentare löschen muss. Oder ein Provider eine rechtsradikale Webseite.

Das scheint mir ein interessanter Aspekt zu sein: App-Stores sollten mehr Verantwortung übernehmen.

Das Home Office absichern: Cyberkriminelle haben Hochkonjunktur

Cyberkriminelle versuchen verstärkt, durch gezielte Angriffe in die Rechner von Home-Office-Nutzern zu kommen – um dort zu spionieren oder Schaden anzurichten. Deshalb sollte jeder sein Home Office gut absichern.

Zu Hause zu arbeiten, das ist in vielerlei Hinsicht etwas völlig anderes als im Büro zu arbeiten. Experten warnen: Die persönliche Umgebung lenkt ab – und lässt Mitarbeiter unvorsichtig werden. Hinzu kommt, dass das Heimnetzwerk in der Regel längst nicht so gut abgesichert ist wie ein Firmennetzwerk. In der Firma sorgen zahlreiche Sicherheitsstandards und Tools dafür, dass Angriffe abgewehrt und auffälliges Verhalten erkannt wird.

Zu Hause im Home Office mangelt es an solchen Sicherheitsmechanismen meist völlig. Um so wichtiger, das eigene Heimnetzwerk und das Home Office abzusichern. Schon Kleinigkeiten helfen. Wer einfache Regeln beachtet, macht sein Home Office deutlich sicherer.

1. Updates einspielen

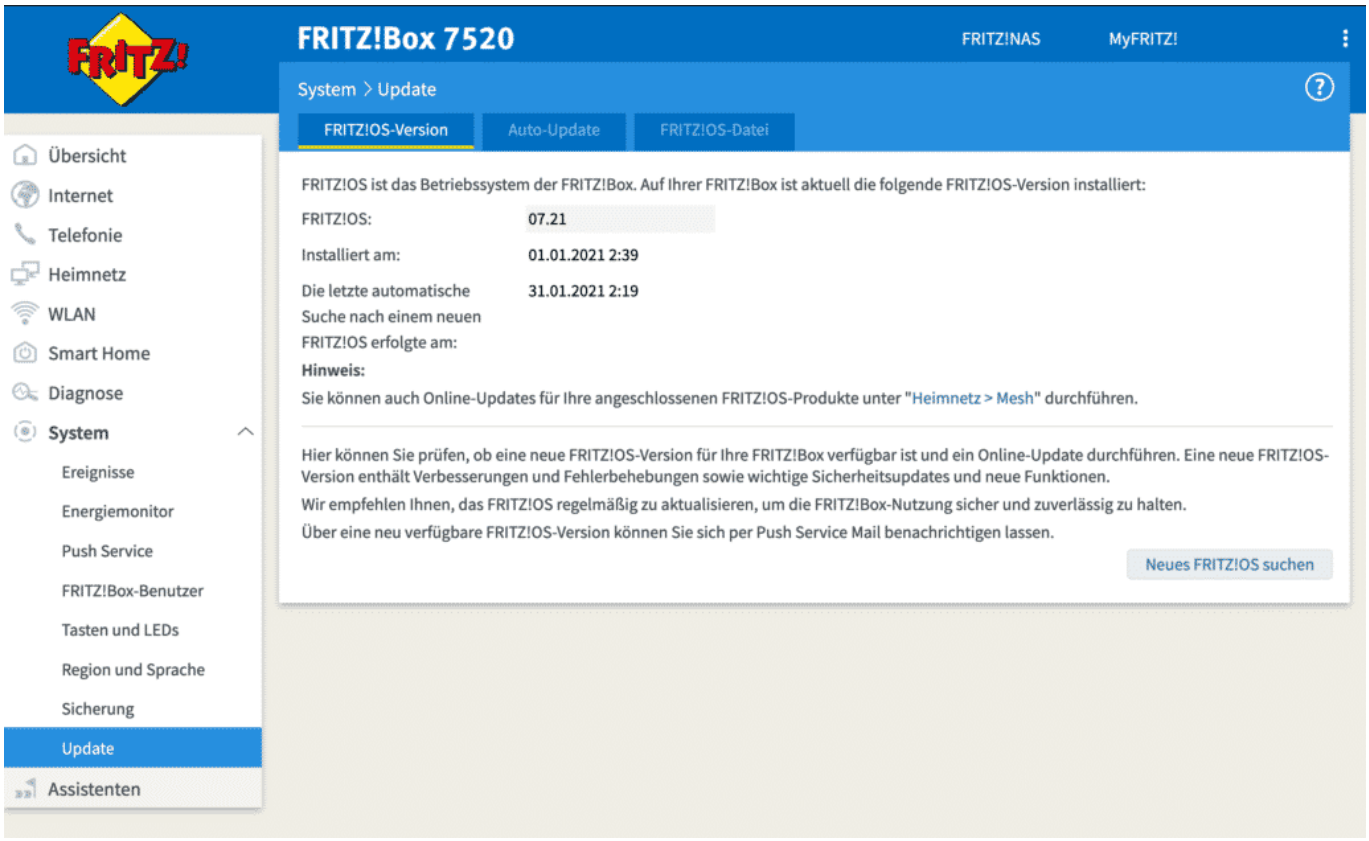
Das Wichtigste überhaupt: Updates einspielen, sobald sie verfügbar sind. Das gilt nicht nur für das Betriebssystem, sondern auch für alle regelmäßig eingesetzten Programme und Apps, insbesondere für Office-Anwendungen, PDF-Software, E-Mail-Programm, Kommunikations-Software (Zoom, Skype, Teams) und alle anderen regelmäßig im Einsatz befindlichen Programme.

2. Onlinekonten absichern

Für jeden Onlinedienst ein anderes, einmaliges und komplexes Passwort verwenden. Gängige Passwort-Manager helfen bei der Verwaltung. Außerdem: Wo immer möglich, die Zwei-Faktor-Authentifizierung (2FA) aktivieren. Das geht heute bei allen großen Onlinediensten. Beim Login muss dann neben Benutzername und Passwort noch ein weiterer Code eingegeben werden, die im eigenen Smartphone erzeugt wird. Das wehrt Hacker wirkungsvoll ab.

3. Schad-Software abwehren

Besonders wichtig ist, Schad-Software zu erkennen und abzuwehren. Dabei helfen spezielle Programme. Sofern möglich, auf Windows-Rechnern den serienmäßig mitgelieferten „Defender“ aktivieren, der Schadprogramme abwehrt. Noch besser ist es, geeignete Schutzprogramme zu installieren. Es gibt kostenlose wie Avira Free Antivirus, aber auch zahlreiche kostenpflichtige Programme. Sie erkennen mitunter auch, wenn Daten aus dem eigenen Rechner abgegriffen werden – und verhindern das.



4. Router und WLAN absichern

Auch der Router kann ein Einfallstor für Angriffe sein, die dann das gesamte Netzwerk betreffen. Deshalb unbedingt auch den Router aktuell halten. Dazu in die Bedienoberfläche des Router gehen (Handbuch!) und dort nach Updates suchen. Hier ist auch zu sehen, ob sich möglicherweise nicht legitimierte Geräte im Netzwerk befinden. Wichtig;: Das WLAN mit einem Passwort absichern.

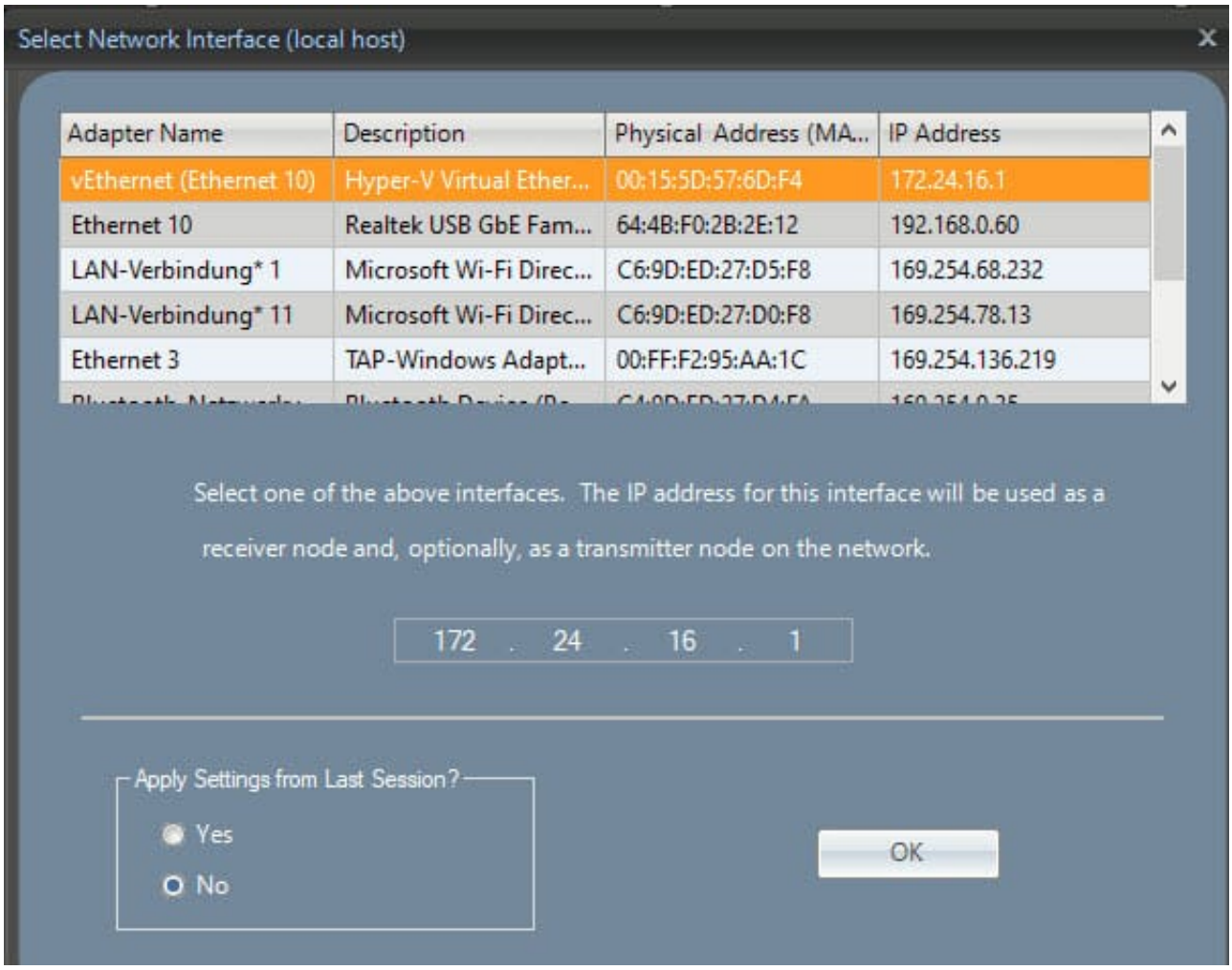
5. Anhänge und Links kritisch beobachten

Besonders heikel sind Mail-Anhänge (Dokumente) und Links in E-Mails. Sie könnten gefälscht oder manipuliert sein. Daher immer den Absender überprüfen und kritisch beobachten, was passiert. Verdächtige Dokumente nicht öffnen. Beim Anklicken von Links überprüfen, ob die geöffnete Webseite korrekt ist. Im Zweifel Webseiten bevorzugt über Favoriten-Liste aufrufen.

Netstress: Netzwerkgeschwindigkeit am PC messen

Die Netzwerkgeschwindigkeit zu messen ist kein Luxus: Störungen im Netzwerk können Ihre Arbeit deutlich verlangsamen. Wenn Sie Ihren manuellen Messungen nicht trauen oder die Messung ein wenig professioneller durchführen wollen, dann ist Netstress eine gute kostenlose Alternative.

Das Programm setzt ebenfalls darauf, dass zwei Geräte Daten untereinander über das Netzwerk austauschen. Statt aber alleine die Geschwindigkeitsangaben des Netzwerkes zu benutzen, wird Netstress auf beiden Rechnern installiert und sorgt für die strukturierte Messung der Netzwerkleistung. Dabei können Sie dann nicht nur verschiedene Übertragungsarten und Paketgrößen, sondern auch die dafür genutzten Netzwerkadapter auf den Rechnern bestimmen.



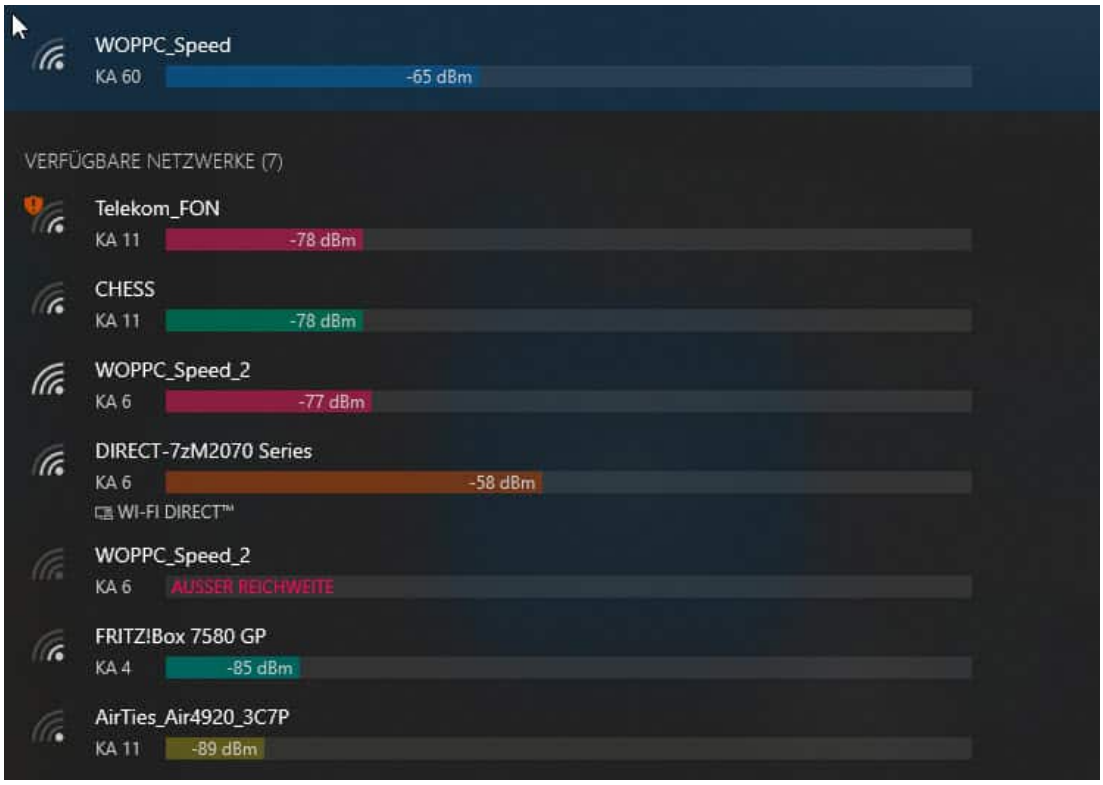
Das erlaubt Ihnen, mit wenig Aufwand ein Problem mit zu langsamer Netzwerkgeschwindigkeit einzugrenzen. Beispielsweise dann, wenn es sich um ein Treiber- oder Hardwareproblem handelt: Das tritt dann nur bei einem der Netzwerkadapter Adapter auf, sodass Sie hier konkret in eine Lösungsfindung einsteigen können.

Auch bei Netstress müssen Sie den einen Teilnehmer an der Messung per Kabel möglichst nah am Router angeschlossen haben. Für den anderen entscheiden Sie dann, ob sie in für eine WLAN-Messung oder eine Messung des verkabelten Teils des Netzwerkes einsetzen möchten.

WLAN-Analyse in Windows: WiFi Analyzer

Ihr WLAN wird gefühlt immer langsamer, Verbindungen brechen ab? Dann sollten Sie einmal strukturiert analysieren, was die Ursache ist. Während professionelle Netzwerk-Analyse-Tools meist sehr teuer sind haben Sie unter Windows 10 Glück: Der Wifi Analyzer ist eine in der Basisversion kostenlose Software, die Ihnen viele Informationen auf einen Blick anbietet.

Nach der Installation können Sie sie sich durch einen Klick auf das WLAN-Symbol oben links in der Symbolleiste eine Übersicht der empfangbaren WLANs und der Dämpfungswerte an. Der Dämpfungswert gibt Aufschluss darüber, wie stark der Empfang ist beziehungsweise wie beeinflusst das WLAN-Signal durch Ihre Empfangsposition ist, beispielsweise durch Wände. Ein niedrigerer Dämpfungswert ist also positiv!



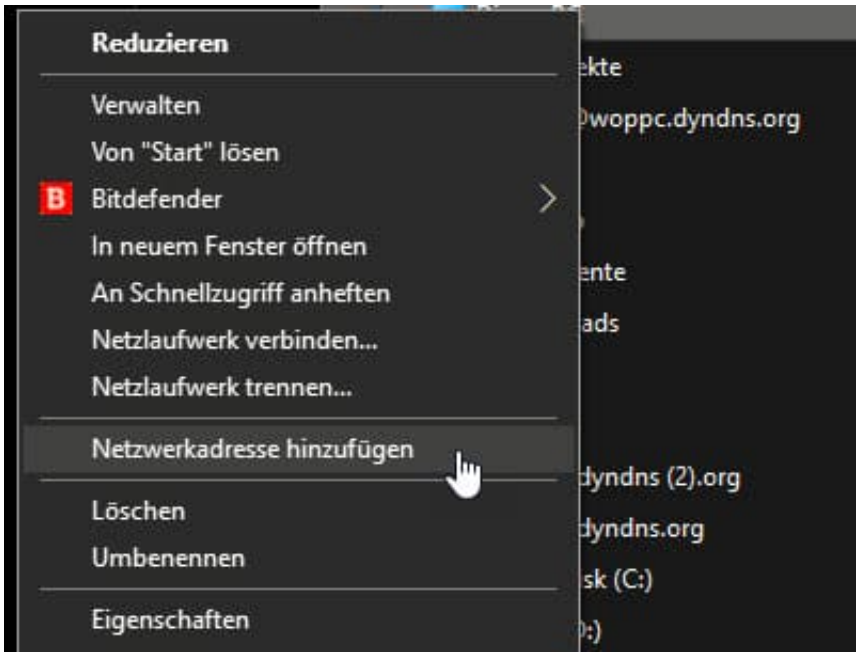
So gut wie jeder Haushalt hat ein oder gar mehrere WLANs. Besonders in eng bebauten Gegenden sorgt das dafür, dass sich mehrere WLANs um die Funkkanäle streiten. Normalerweise sollte Ihr Router hier eigenständig den optimalen Kanal herausfinden und einstellen, manchmal funktioniert das aber nicht.

Der WiFi Analyzer zeigt Ihnen unter Analyse eine Übersicht der WLAN-Kanäle und deren Belegung an. Anhand der aktuell empfangenen WLANs und den Kanälen die diese verwenden, zeigt die App Ihnen eine Empfehlung an, welcher Kanal optimal wäre. Die Empfehlung wird mit einer Sterne-Empfehlung versehen: Je mehr Sterne blau sind, desto weniger „Fremdverkehr“ befindet sich auf dem Kanal. Je weniger Sterne die Empfehlung bekommt (die ja schon den besten verfügbaren Kanal enthält), desto beeinträchtigter ist Ihr Netzwerk.

Verbinden eines FTP-Servers unter Windows 10

Die Cloud mag das Sinnbild des Datenspeichers sein, über den Sie von überall her zugreifen können. Weiter verbreitet sind trotzdem immer FTP-Server. Vor allem zum Herunterladen von Updates und Zusatzsoftware werden die von Firmen betrieben. Auch Netzwerkfestplatten und sogar Router lassen sich als FTP-Server nutzen. Wir zeigen Ihnen, wie Sie unter Windows eine Verbindung zu einem FTP einrichten.

Natürlich können Sie eine der vielen FTP-Apps wie zum Beispiel SmartFTP nehmen, es geht aber auch einfacher: Ein FTP-Server ist nichts anderes als ein Datenspeicher wie eine Festplatte. Der Windows Explorer ist das Standardprogramm für den Umgang mit Dateien. Dieser bietet die Möglichkeit, FTP-Server als Speicher hinzuzufügen.



Klicken Sie im Explorer mit der rechten Maustaste auf **Dieser PC**, dann auf Netzwerkadresse hinzufügen. Wählen Sie dann **Eine benutzerdefinierte Adresse** und geben Sie die externe Adresse des FTP-Servers ein. Diese muss mit **ftp://** beginnen.

Im Normalfall wird der Server die Anmeldung mit Benutzernamen und Kennwort fordern. In diesem Fall entfernen Sie den Haken bei **Anonym anmelden** und geben Sie den Benutzernamen ein. Nach Abschluss der Konfiguration können Sie die Verbindung zum FTP aufbauen. Sie werden dann zur Eingabe des Kennwortes aufgefordert. Dieses können Sie auf Wunsch auch für weitere Verbindungen speichern.