Schieb Report

Ausgabe 2022.10

Geräte nach IP-Adresse finden bei der Fritz!Box

Irgendein Gerät treibt Unsinn im Netzwerk. Ihr habt die IP-Adresse, aber damit immer noch nicht das Gerät. Die AVM Fritz!Box und andere Router helfen hier!

Als Anwender ist man von den dauernden Hiobsbotschaften rund um Viren, Hacks und Datenlöcher sensibilisiert. Manchmal sogar übersensibilisiert: JEde kleine Fehlermeldung über eine vermeintlich unnormale Aktivität am eigenen PC, Mac oder im Netzwerk sorgt für einen Schreck und ein unwohles Gefühl.

IP-Adressen: Eindeutig, aber nicht sprechend

Ein Netzwerk ist vollkommen einfach strukturiert. Das heißt wie so oft leider aber auch: Nicht wirklich sprechend und komfortabel! Geräte identifizieren sich nicht mit ihrem Namen, sondern mit der Netzwerkadresse, IP-Adresse genannt. Die ist eine Kombination aus mehreren Ziffernkolonnen, die quasi eine Wegbeschreibung der Datenpakete ermöglichen. Meist hat der Router im heimischen Netzwerk die IP-Adresse 192.168.0.1, ein Gerät die Adresse 192.168.0.151. Jede IP-Adresse

ist zu einem Zeitpunkt nur einmal vergeben, gibt aber in ihrer ursprünglichen Form keine Auskunft darüber, welches Gerät Sie gerade verwendet.

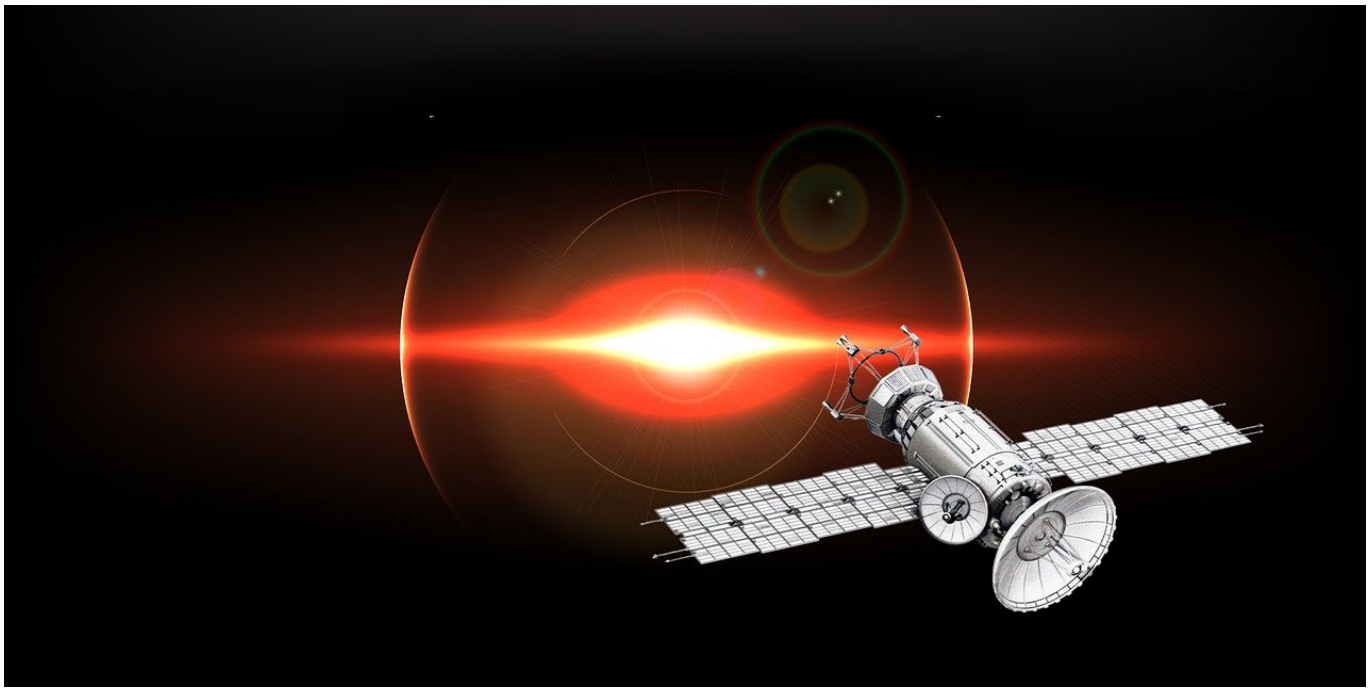
Der Router als Telefonbuch

Viele Geräte identifizieren sich auch mit ihrem Namen im Netzwerk, die Zuordnung zwischen IP und Namen kann nur der Router herstellen. Bei eine Meldung "192.168.0.151 betrachtet gerade Ihren Bildschirm" ist erst einmal keine Panik nötig.

XBOX	LAN 4 mit 1 Gbit/s	192.168.0.158	
PC-192-168-0-156	WLAN verbunden mit Buero	192.168.0.156	5 GHz, 43 / 72 Mbit/s
iPhone-von-Andreas	WLAN verbunden mit Buero	192.168.0.155	5 GHz, 780 / 144 Mbit/s
Andreass-iPadPro129	WLAN verbunden mit Buero	192.168.0.154	5 GHz, 650 / 78 Mbit/s
MBP-M1Pro	WLAN	192.168.0.151	5 GHz, 650 / 526 Mbit/s
dda5852c-6a45-408d-8e8b-df70f5e15399	WLAN verbunden mit Buero	192.168.0.143	5 GHz, 520 / 234 Mbit/s
Lukas-iPad-Kindle	WLAN verbunden mit Buero	192.168.0.141	5 GHz, 780 / 468 Mbit/s
none-22	WLAN	192.168.0.140	2,4 GHz, 52 / 65 Mbit/s
iPad-Niklas-neu	WLAN verbunden mit Buero	192.168.0.136	5 GHz, 780 / 585 Mbit/s

Ruft die Konfigurationsoberfläche des Router auf und wechselt dort in die Netzwerkeinstellungen/die Netzwerkübersicht. Da steht in der einen Spalte die IP-Adresse, in einer anderen aber auch gleich der Name des Gerätes. Der muss nicht immer sprechend sein. Im vorliegenden Fall zeigt sich aber schnell, dass es sich um ein Macbook Pro handelt. Mit der Information lässt sich schnell identifizieren, ob das Gerät ein Recht hat, den eigenen Bildschirm zu beobachten oder nicht.

Berechtigungen auf die Position vergeben bei iOS



Viele Apps unter iOS verlangen Zugriff auf die Position. Dazu darf der Benutzer einmal eine Entscheidung treffen und muss dann damit leben. Dumm, wenn die Wahl versehentlich falsch war. Keine Sorge, das lässt sich im Nachgang ändern!

Das Dümmste, was bei der ersten Abfrage einer App nach der Berechtigung für die Position passieren kann, ist ein Tippen auf **Beim Verwenden der App**. Dann nämlich, wenn die App auch im Hintergrund laufen können soll. Aus Datenschutzsicht ist die Einstellung natürlich sinnvoll, denn der Zugriff auf die Position ist dann nur möglich, wenn der Benutzer die App aktiv benutzt und nicht heimlich. Es gibt aber Apps, die die Position auch im Hintergrund verwenden müssen, um zu funktionieren. Beispielsweise die Sony Imaging Edge App. Die überträgt die aktuelle Position an eine externe Digitalkamera, sobald diese eingeschaltet wird. Im Hintergrund, denn der Anwender wird im Vordergrund etwas anderes machen.

Um die GPS-Zugriffseinstellungen anzupassen, führt der Weg in den Einstellungen von iOS über **Datenschutz** > **Ortungsdienste**. Während iOS im oberen Teil allgemeine Einstellungen vornehmen lässt, findet sich darunter eine Liste aller Apps, die die Position verwenden könnten/wollen. Ein Tip auf eine App bringt ein Menü zum Vorschein, in dem zwischen den zur Verfügung stehenden Berechtigungen gewählt werden kann. Bei einer solchen App macht hier die Einstellung **Immer** Sinn.

Mehr Nachhaltigkeit: Apple und die Umwelt

Apple hat eine Reihe neuer Modelle seiner erfolgreichsten Produkte vorgestellt: iPhones 13 in Grün, ein neues iPhone SE, ein neues iPaid Air und einiges mehr. Bei allen Geräten weist Apple explizit darauf hin, dass sehr viel recyceltes Material verbaut und verwendet wird.

Es wird aus meiner Sicht immer wichtiger, bei der Herstellung von Hightech-Produkten darauf zu achten, dass sie "umweltfreundlich" produziert werden. Umweltfreundlich im strengen Sinne geht gar nicht. Aber es ist wichtig, darauf zu achten, Umwelt und Klima möglichst so wenig zu belasten wie möglich.

Das ist am Ende immer eine Frage der Balance. Wer Elektrogeräte herstellt und vertreibt, belastet natürlich Klima und Umwelt. Aber wie viel - und was wird unternommen, diese Belastung maximal zu reduzieren?

Nachhaltige Produktion

Apple ist ein Hersteller, der zumindest versucht, nachhaltiger zu produzieren.

Die iPhone 13 Pro- und iPhone 13-Modelle, das iPhone SE, aber auch das neue iPaid Air sind für eine möglichst geringe Umweltbelastung entwickelt worden. Die Geräte werden größtenteils aus recycelten Materialien hergestellt, darunter 100 Prozent recycelte Seltene-Erden-Metalle in der Taptic Engine und den Audiomagneten, 100 Prozent recyceltes Wolfram in der Taptic Engine und 100 Prozent recyceltes Zinn im Lötmittel der Hauptplatine.

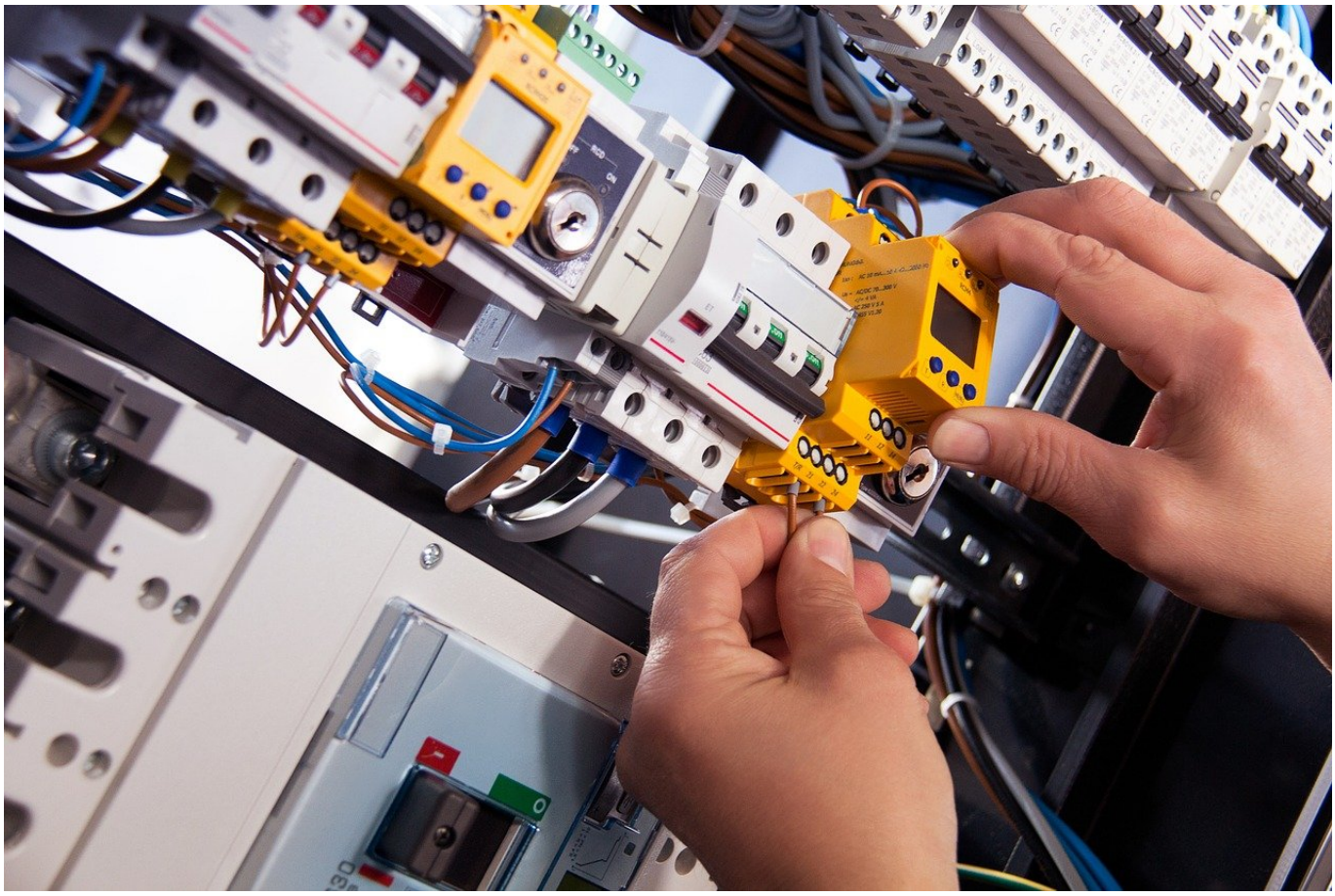
Beim iPhone 13 kommen 100 Prozent recyceltes Gold in der Plattierung der Hauptplatine und der Verdrahtung der Front- und Rückkameras zum Einsatz und auch das Zinn im Lötmittel der Hauptplatine und erstmals im Lötmittel der Batteriemanagementeinheit ist zu 100 Prozent recycelt. iPhone 13 und iPhone 13 mini verfügen außerdem über Antennenleitungen, die aus **wiederverwerteten Plastikwasserflaschen** bestehen, die chemisch in ein stärkeres, leistungsfähigeres Material umgewandelt worden sind — erstmals in der Industrie.

Weniger Verpackung spart 600 Tonnen Kunststoff

Durch die neu designte Verpackung ist keine Umverpackung aus Kunststoff mehr nötig. Dadurch werden 600 Tonnen Kunststoff eingespart und Apple kommt seinem Ziel näher, bis 2025 vollständig auf Kunststoff in seinen Verpackungen zu verzichten. Die iPhone 13 Pro- und iPhone 13-Modelle zum Beispiel erfüllen hohe Standards für Energieeffizienz und sind frei von zahlreichen Schadstoffen.

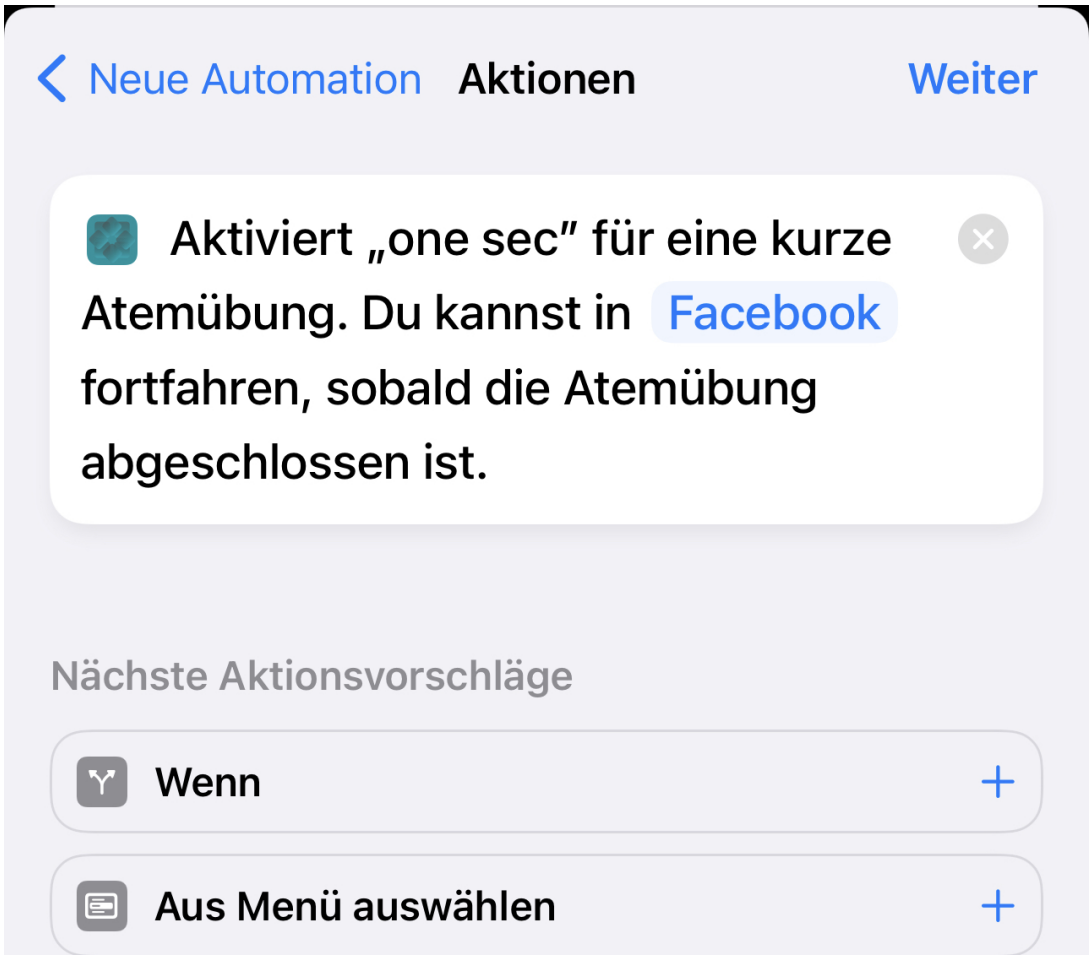
Apple ist bereits heute bei allen weltweiten Unternehmensaktivitäten klimaneutral und plant bis 2030 über alle Tätigkeitsbereiche des Unternehmens, die Zuliefererkette und den Produktlebenszyklus hinweg klimaneutral zu werden. Das bedeutet, dass jedes verkaufte Apple Gerät von der Komponentenherstellung, Montage, dem Transport, der Nutzung durch die Kund:innen, dem Aufladen bis hin zum Recycling und zur Materialrückgewinnung keinerlei Auswirkungen auf das Klima haben wird

Stress vermindern und Zeit sparen: One Sec



Facebook, Instagram, der Newsreader: Apps, die täglich unzählige Male aufgerufen werden. Einfach nur aus Reflex. Das stresst unnötig, lässt sich aber schnell verhindern und in etwas Positives umwandeln!

Ihr kennt das garantiert: Kaum ist die Konzentration kurz unterbrochen, wandert erst der Blick, dann der Griff zum Handy. Mal eben Facebook Timeline checken, neueste Nachrichten lesen. Vollkommen egal, ob das letzte Mal gerade erst zwei Minuten her ist. Dieser Reflex kostet Zeit, die Ihr besser nutzen könntet. Die kostenlose App One Sec (von "One Second", eine Sekunde) für iOS hilft dabei, statt Stress Entspannung zu schaffen. Nicht ganz so extrem wie Digital Detox, aber ähnlich effektiv.

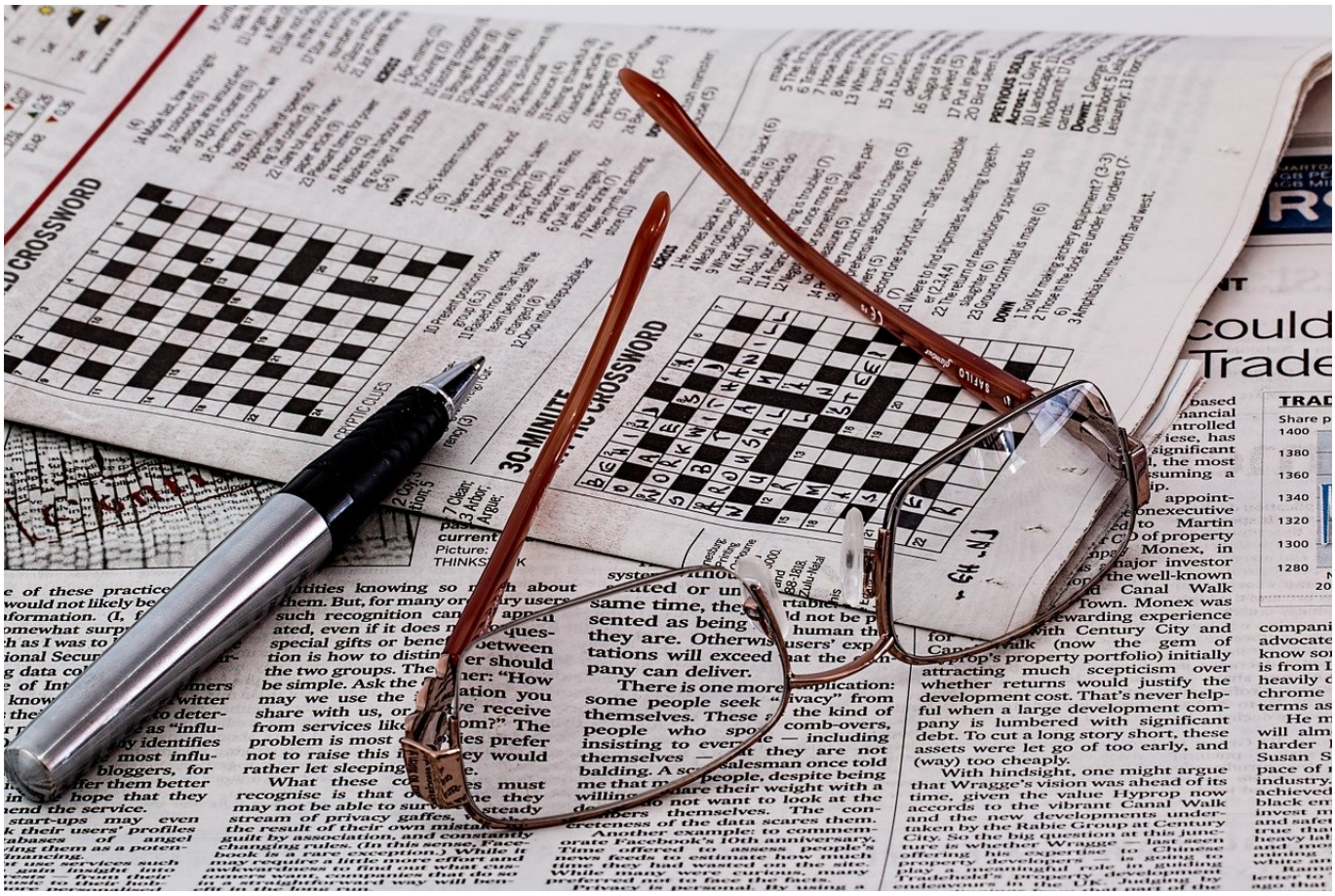


One Sec setzt sich zwischen das Tippen zum Start und die zu startende App. Bevor diese für den Anwender bedienbar wird, zeigt sie einen Zyklus von zwei Atemzügen an. Die Idee: Atmet einmal lang ein und wieder aus, dann entscheidet aktiv, ob die App gestartet werden soll, oder ob der Start abgebrochen werden soll.

Klingt auf den ersten Blick unsinnig, ist aber einen Versuch wert: Die Zwangspause ist zum einen beruhigend und entspannend, auf der anderen Seite lässt sie das drängende Zwangsgefühl, die Inhalte der app anzusehen, abklingen. In der Summe tippen die meisten Anwender häufiger auf "Nicht starten" als auf "Starten".

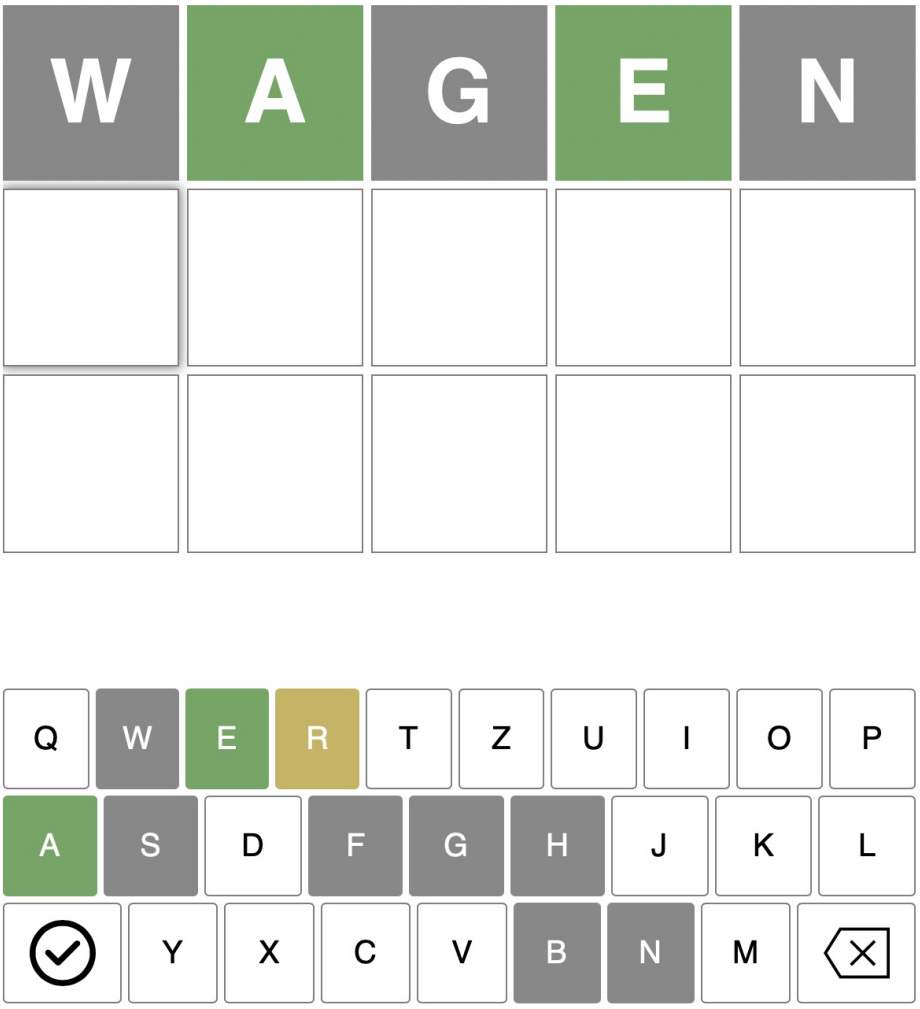
Die Einrichtung der App funktioniert über die Automatisierungsfunktionen von iOS. In der App wird jeder Schritt beschrieben, der Prozess muss für jede App, deren Start verzögert werden soll, einzeln durchgeführt werden.

Wordle auf dem iPhone/iPad spielen ohne Werbung

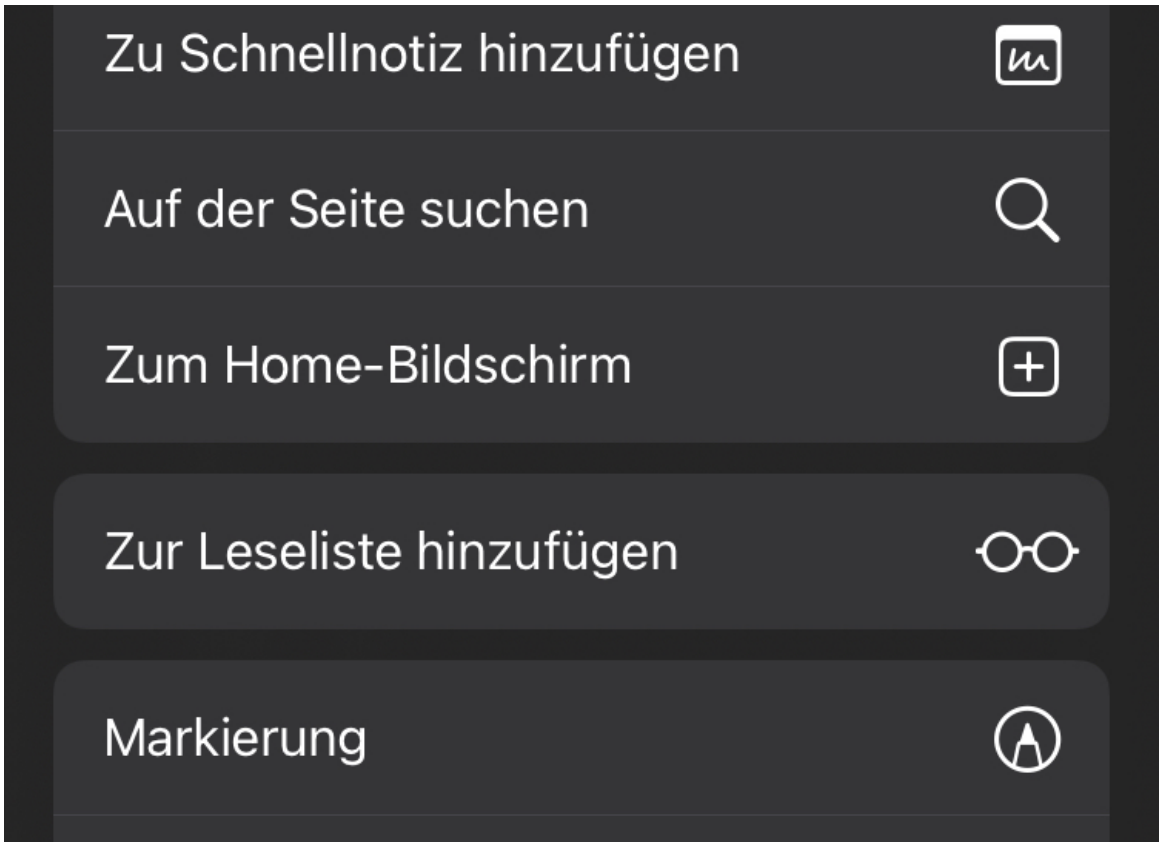


Wordle ist ein Ratespiel, das sich riesiger Beliebtheit erfreut. Eigentlich als Webseite implementiert bieten viele Anbieter auch Apps an. Die sind aber nicht offiziell und mit Werbung. Baut Euch sich einfach selbst eine App!

Die New York Times als ursprünglicher Anbieter des Spiels hatte Wordle als Webseite konzipiert, und dabei sicherlich auch die Werbeeinnahmen durch die Zugriff einkalkuliert. Die App-Anbieter müssen ein wenig anders vorgehen, darum finden sich in den diversen inoffiziellen Apps im App-Store nervige Werbebanner. iOS bietet die Möglichkeit, aus einer Webseite eine App zu bauen, und das ohne Programmierkenntnisse.



Als erstes muss die Webseite von Wordle (z.B. http://www.wordle.at für das deutsche Wordle) in Safari geöffnet werden. Ein Tippen auf das Teilen-Symbol oben in der Safari-Leiste öffnet ein neues Menü. In dem tippt auf **Zum Home-Bildschirm**.



iOS legt nun eine neue Verknüpfung im Home-Bildschirm an. Die angegebene URL und der Name der Verknüpfung lassen sich frei verändern. Das geht unter macOS übrigens genauso!

Diese Verknüpfung im Home Screen ist allerdings nicht nur ein Favorit im Browser, sondern kann noch mehr: iOS kapselt das Safari-Fenster und lässt die Webseite wie eine App laufen. Einziger Nachteil beim ersten Start: Wenn Sie schon eine Partie im Browser laufen haben, dann nimmt dieser die bisher eingetragenen Buchstaben nicht mit.

Das BSI warnt vor Cyberangriffen: Diese Tipps helfen

Das Risiko, Opfer von Cyberangriffen zu werden (etwa durch russische Hackers oder Bots), ist aktuell erhöht - warnt das BSI. Ein paar eher simple Tipps und Grundregeln helfen, nicht so leicht zum Opfer zu werden.

Laut „Bundesamt für Sicherheit in der Informationstechnik“ (BSI) sind zeitnah Hack-Angriffe auf westliche Ziele zu erwarten. Wer nun glaubt, solche Angriffe würden sich auf Banken, Politiker oder Behörden beschränken, der täuscht sich: Wir alle sollten unsere digitale Arbeitsumgebung unbedingt besser absichern.

Unsere Haustüre schließen wir routinemäßig ab. Unser Auto ebenso. Auch das Fahrrad. Eigentlich alles, was uns lieb und teuer ist, wird vor ungewünschten Zugriffen Fremder bewahrt. Das liegt in unserer Natur und ist ein persönliches Schutzbedürfnis. Nur bei Computer, Cloud und Smartphone sind überraschend viele Menschen nachlässig, was Sicherheit und aktiven Schutz anbelangt. Am ehesten wohl, weil sie die wahren Gefahren nicht abschätzen können – und auch nicht wissen, wie „abschließen“ hier eigentlich funktioniert.

BSI warnt ausdrücklich vor erhöhter Bedrohungslage

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt laut Medienberichten vor drohenden Angriffen auf „Hochwertziele“. Wer nun denkt, das ginge ihn nichts an, könnte sich täuschen. Denn viele von uns arbeiten heute wie selbstverständlich im Home Office oder nutzen Smartphone und Computer dazu, um auf Cloud-Dienste des Arbeitgebers zuzugreifen – oder kennen jemanden, der in der kritischen Infrastruktur arbeitet.

Es ist grundsätzlich wichtig, sich und seine Daten zu schützen – aktuell erst recht. Aber wie vorgehen? Die gute Nachricht: Dazu ist kein Informatik-Diplom notwendig. Das Befolgen einiger Regeln reicht schon.

1. Software aktuell halten

Die mit weitem Abstand wichtigste Maßnahme ist: Software aktuell halten. Das gilt insbesondere für das verwendete Betriebssystem (auch auf Smartphones und Tablets!), aber natürlich insbesondere für PC oder Notebook. Ob Windows, MacOS oder Linux: Sollte das Betriebssystem eine neue Version ankündigen, sollte das so schnell wie möglich installiert werden – auch wenn es manchmal lästig ist. Sofern keine Hinweise erscheinen (das ist Einstellungssache), bitte regelmäßig nach Updates schauen und sie installieren.

Das gilt ebenso für jede Software, die benutzt wird. Ob Office, Word, PDF-Reader, E-Mail-Software oder das Lieblingsspiel: Software muss immer aktuell sein. Denn Sicherheitslücken sind die liebsten Einfallstore für Hacker und bieten die größte Angriffsfläche. Wer alles aktuell hält, reduziert das Risiko!

2. Zwei Faktor Authentifizierung verwenden

Wo immer möglich, die Zwei-Faktor-Authentifizierung aktivieren. Das mit Abstand beste Mittel, um unerwünschten Zugriff auf Onlinekonten und Geräte zu schützen. Neben Benutzername und Passwort muss dann noch eine weitere Information beim Anmelden eingegeben werden. Meist ein Code, der im eigenen Handy erzeugt wird – in der Regel in einer Authentifizierungs-App wie Google oder Microsoft Authenticator. Angreifer müssten Zugang zum Handy erlangen, um sich dann irgendwo anzumelden. Das ist nicht völlig undenkbar, aber ungeheuer

schwierig.

Diese Sicherheitsmaßnahme überall aktivieren, wo es geht: Facebook, Instagram, Twitter, Mail-Postfach, Paypal, Google, LinkedIn. Auf diese Weise wird auch verhindert, dass sich Fremde als jemand anders ausgeben können, zum Beispiel, indem sie im Namen eines Journalisten oder Politikers Aussagen posten. Es ist beim ersten Mal etwas mühsamer, spielt sich aber schnell ein – und erhöht die Sicherheit enorm.

3. Router, WLAN und Smartphone sichern

Nicht zu vernachlässigen sind auch die kleineren Hardware-Geräte zu Hause: Ob Router, WLAN oder Smarthome – auch diese Systeme sind potenzielle Ziele. Auch wenn es nicht weit verbreitet ist, aber wer möchte schon, dass Fremde über ein Smart-TV Gespräche abhören können oder sich Zugang zum Haus verschaffen? Deshalb müssen auch Router und andere Geräte gesichert werden.

Auch hier lassen sich oft Updates einspielen. Wer dabei Hilfe braucht, sollte sich die besorgen. Auch sollten die Zugangspasswörter zu diesen Geräten nicht in der Standardeinstellung belassen werden.

4. Nicht blauäugig sein: Phishing-Angriffe

Last not least: Immer vorsichtig sein. Wer eine SMS, eine WhatsApp-Nachricht oder eine E-Mail erhält, die dringend dazu auffordert, sich irgendwo anzumelden, könnte Opfer einer gezielten „Phishing-Attacke“ sein. Betrüger versuchen die Menschen dazu zu motivieren, ihre Zugangsdaten auf einer manipulierten, aber echt aussehenden Webseite einzugeben. Das lässt sich nur vermeiden, indem man auf gar keinen Fall einen Link anklickt oder verwendet, der vorgegeben wird – immer die Adressen selbst eingeben oder aus der eigenen Favoritenleiste auswählen.

Facebook-Anmeldungen an Apps und Websites löschen

Melden Sie sich mit Facebook an Apps und Webseiten an, um Zeit zu sparen? Dann kontrollieren und löschen Sie diese Anmeldungen regelmäßig. Oft nutzen Sie diese nur einmal. Warum also ein Risiko eingehen?

Viele Webseiten und Apps wollen Sie kennen und Ihre Informationen speichern. Dazu können Sie ein eigenes Konto anlegen. Einfacher ist es aber, wenn Sie Ihr Facebook-Konto dazu nutzen. Kein neues Passwort, keinen Benutzername, den Sie sich merken müssen, Ihre Facebook-Zugangsdaten kennen Sie.

Übersicht über die Anmeldungen

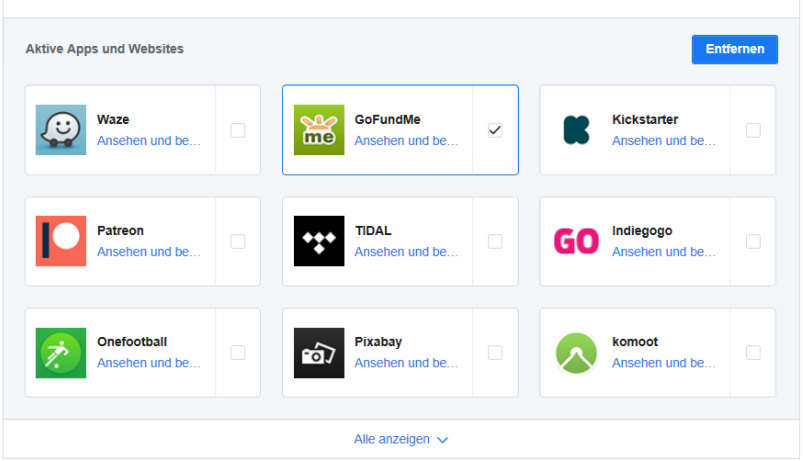
Wenn Sie das erste Mal die Anmeldung per Facebook bei einer neuen App oder Webseite vorgenommen haben, informiert Sie Facebook darüber. Per Push-

Nachricht, E-Mail und Benachrichtigung auf der Webseite. Ein Klick auf diese Benachrichtigung führt Sie dann direkt zur Übersicht der aktiven Apps und Webseiten.

Alternativ klicken Sie auf **Einstellungen** > **Apps und Websites** um in die Übersicht derjenigen zu kommen, die mit Ihrem Facebook-Konto gekoppelt sind. Wenn Sie auf eines der Symbole klicken, dann zeigt Ihnen Facebook alle Berechtigungen, die die App/die Webseite hat.

Löschen der Anmeldung per Facebook

Im Normalfall verwenden Sie die Anmeldung per Facebook für Dienste und Seiten, die Sie nur selten nutzen und wo der Aufwand des Anlegens eines eigenen Benutzerkontos übertrieben scheint. Da macht es Sinn, die Zugriffsrechte auch wieder zu löschen! In der Übersicht der Apps und Websites bei Facebook können Sie für jedes Element, auf die Zugriff besteht, ein- oder ausschalten. Das Ausschalten kann natürlich dazu führen, dass bestimmte Funktionen nicht mehr funktionieren.



Markieren Sie in der Übersicht einen Eintrag und klicken Sie dann auf **Entfernen**, um den Zugriff der App/Webseite zu löschen. Besonders bei nur einmal verwendeten Anmeldungen sollten Sie dies direkt machen, dann vergessen Sie es später nicht mehr.

Passwort vs. PIN vs. biometrische Authentifizierung – was ist für Windows 11 am sichersten?

Seine eigenen Geräte, Dokumente und Daten abzusichern wird immer wichtiger. Das fängt schon beim Zugriff auf Rechner oder Mobilgerät an. Welche Methode ist die Beste unter Windows 11: PIN, Gesichtserkennung oder Passwort? Wir haben mal genauer hingeschaut...

Unter Windows 11 können sich Benutzer mit ***Hello PIN*** anmelden. Dabei handelt es sich um eine von Microsoft empfohlene Methode, mit der Nutzer schnell und sicher Zugriff auf das Gerät erhalten. Die **Anmelde-PIN** besteht unter Windows 11 in der Regel aus vier Ziffern (in Unternehmen kann dies manchmal abweichen und längere Kombinationen sind möglich) - kennt man ja von Bank- und Kreditkarten.

Passwort, Pin & Co. – was ist wirklich sicher?

Dieses *Hello Pin* Anmeldeverfahren birgt einen großen Sicherheitsnachteil, denn es gibt wenig Möglichkeiten, eine besonders komplexes und individuelle PIN zu erstellen. Um zu vermeiden, dass Unbefugte die PIN erraten, vermeide, Zahlenfolgen zu verwenden, die einen persönlichen Bezug zu dir haben, wie etwa

dein Geburtstag oder deine Hausnummer.

Hello PIN ist bisher wohl die beliebteste Anmeldemöglichkeit. Ist das Gerät jedoch mit den notwendigen technischen Voraussetzungen ausgestattet, setzen viele Nutzer auch auf die Gesichtserkennung oder ihren Fingerabdruck als Authentifizierungsmöglichkeit. Diese Form der Anmeldung ist praktisch, da sie schneller durchzuführen ist.

Außerdem bietet sie den Vorteil, dass du dir kein Passwort merken musst (du musst dir jedoch eines für den Fall festlegen, dass die Erkennung nicht funktioniert oder um die **Gesichtserkennung** zu (de-)aktivieren).

Stärken und Schwächen der unterschiedlichen Authentifizierungsmöglichkeiten

Leider ist die Methode der Gesichtserkennung nicht immer sicher, weil die Frontkamera eines Tablets oder eines Laptops Schwächen aufweisen kann. So

konnten Experten schon häufiger nachweisen, dass, wenn ein Raum zu dunkel ist, die Person eine Sonnenbrille aufhat oder wenn Haare ins Gesicht wehen, die Systeme und die Kamera schnell überfordert sind. Auch ein Foto des Nutzers kann die Kamera austricksen.

Sicherer ist es, den **Fingerabdrucksensor** zu verwenden, da hierbei nicht so schnell eine Manipulationsgefahr bestehen oder eine Schwachstelle des Systems auftreten kann. Auch hierbei gilt, dass du zusätzlich ein Passwort festlegen musst.

Sichere Passwörter

Achte bei **Passwörtern** darauf, dass sie individuell und komplex sind. Nutze bei Windows 11 nicht dasselbe Passwort, das du bereits bei zehn anderen Online-Konten verwendest. Ein Passwort-Manager kann dir helfen, für jedes deiner Konten, inklusive deines PCs, sichere Passwörter zu erstellen und diese in einem virtuellen Tresor abzuspeichern. Somit kannst du geräteübergreifend über den Passwort-Manager auf all deine Zugangsdaten zugreifen.

Seit Windows 8 kannst du für das Entsperren darüber hinaus das sogenannte *Picture Password* verwenden. Das heißt, für den gesperrten Bildschirm legst du ein Foto fest. Auf diesem musst du dann bestimmte Punkte in der richtigen Reihenfolge anklicken, um dein Gerät freizuschalten.

Zu guter Letzt gibt es noch den **Sicherheitsschlüssel**. Das ist eine kennwortfreie Anmeldemethode, die vorwiegend von Organisationen verwenden. Es erfordert, dass du über ein physisches Gerät verfügst, das nur du nutzt. Allgemein ist diese Art der Anmeldung am sichersten, aber bei Privatpersonen eher unüblich.

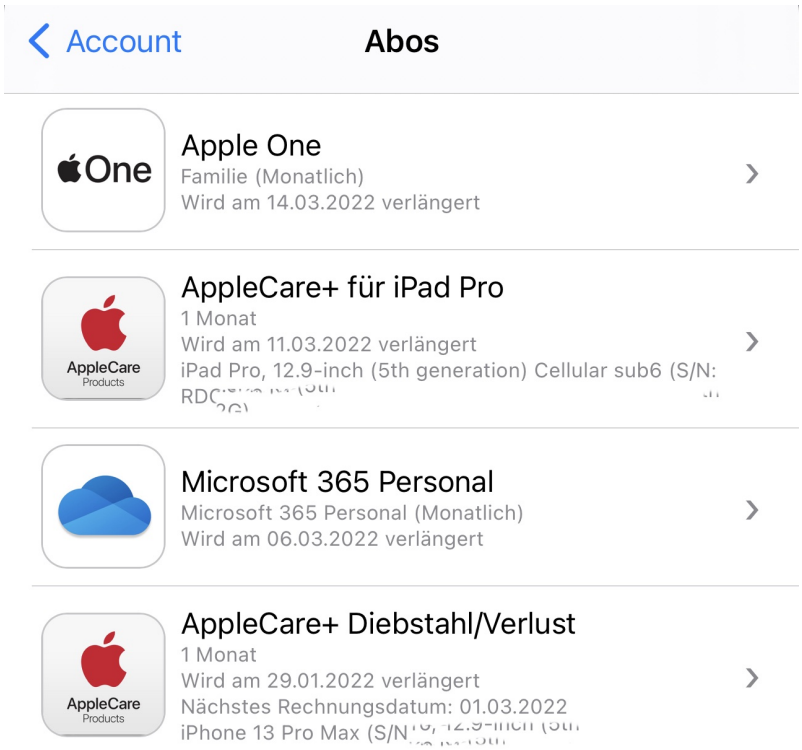
Abonnements bei iOS beenden

Anbieter sind gerne bereit, für einen neuen Dienst einen Testzugang bereits zu stellen. Der kostet dann nichts - bis er sich verlängert. Wir zeigen, wo iOS die Übersicht der Abos und die Kündigungsmöglichkeiten versteckt.

Kostenlose Abos sind toll. Erstmal. Denn im mehr oder minder Kleingedruckten steht dann oft, dass sich das Abo automatisch verlängert, wenn der Monat abgelaufen ist. Leider sind die Abonnements recht gut versteckt und nicht so einfach zu finden. Das führt meist dazu, dass Ihr sie vergesst, bis es zu spät ist.

Apple Arcade ist eines der Beispiele, wo ein kostenloser Testmonat nutzbar ist. Während dieses Monats lassen sich alle Apps des Spiele-Dienstes kostenlos herunterladen. Nach diesem Monat ist eine Kündigung nötig, damit sich das Abo nicht automatisch verlängert. Die geht so:

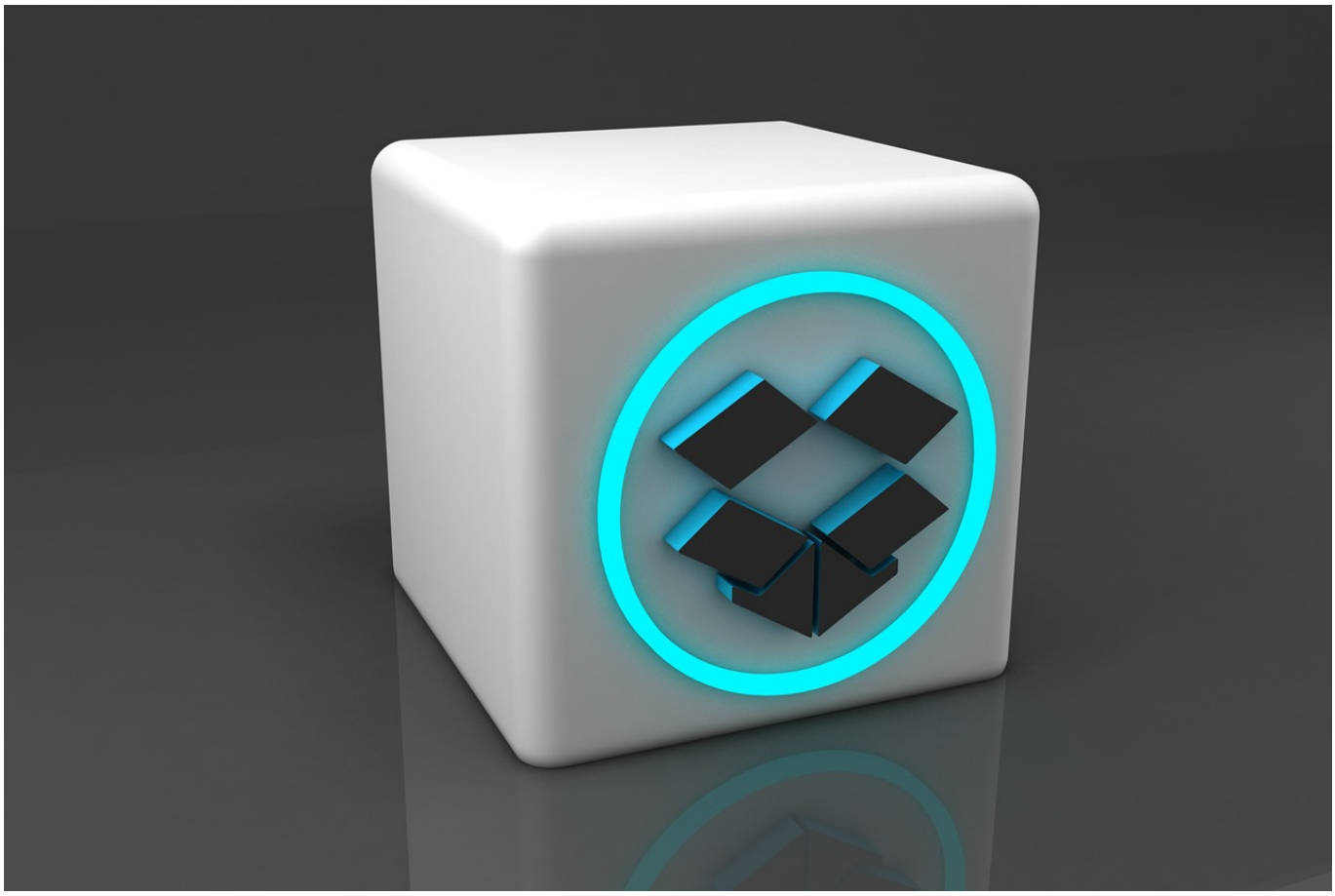
Startet den App Store auf dem iOS-Gerät, und tippt auf das Kontobild.



Tippt nun auf **Abonnements**. iOS zeigt alle Abonnements, die über den App Store abgeschlossen wurden. Tippt das entsprechende Abo an, dann kann dieses durch **Abonnement kündigen** zum nächst möglichen Zeitpunkt gekündigt werden.

Es ist allerdings genau zu überlegen, was vor der Kündigung gegebenenfalls noch nötig ist: Eine App nicht mehr nutzen zu können ist die eine Geschichte. Teilweise gehören dazu aber auch Dateien, die mit dem Programm erzeugt wurden. Diese sind dann gegebenenfalls nicht mehr nutzbar. Eine Datensicherung macht Sinn! Die möglichen Kündigungstermine sind natürlich abhängig von dem Vertrag, der mit dem Anbieter geschlossen wurde.

Bandbreite sparen bei Dropbox



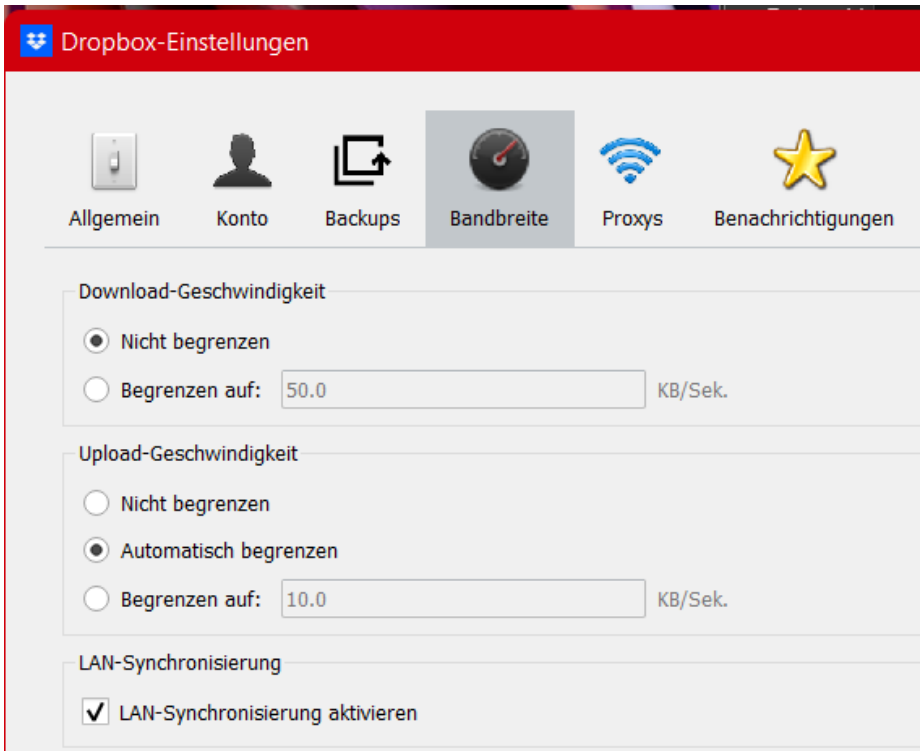
Nicht jeder Anwender hat das Glück, eine schnelle Internetleitung zu haben. Ist diese langsam, dann können Upload und Synchronisation in die Cloud schnell zu Wartezeiten führen. Bei Dropbox gibt es ein Mittel dagegen!

Das Internet ist mittlerweile so etwas wie ein intellektuelles Grundnahrungsmittel. Ohne Informationen sind wir aufgeschmissen und schnell unleidlich. Jetzt haben Informationen verschiedenes Gewicht: Die Webseite, die gerade von Interesse ist, soll schnell da sein. Ob eine Datei, die lokal auf der Festplatte liegt, rasend schnell oder nur schnell auf der Dropbox ankommt, dagegen eher nachgeordnet.

Einstellen der Bandbreite für Dropbox

Im Standard verwenden alle Anwendungen einfach die Internet-Bandbreite, die gerade zur Verfügung steht. Die variiert je nach Leitung, nach Teilnehmern, die am eigenen Anschluss Datenverbrauchen und oft auch nach der Internethungrigkeit der Nachbarn, die am selben Knoten hängen. Zwischen den

Anwendungen gibt es keine vorgegebene Priorität. Wer zuerst kommt, mahlt zuerst!



Dropbox lässt aber in der App zu, deren Datenhunger einzubremsen. Durch Klick mit der rechten Maustastet auf das App-Symbol im Tray, das Kontobild und dann **Einstellungen** > **Bandbreite** lassen sich separat für Upload und Download separate Bandbreite vergeben. Im Standard ist der Download nicht begrenzt, der Upload automatisch (nach verfügbarer Bandbreite). Das macht Sinn, denn das Herunterladen einer geänderten oder neuen Datei aus der Cloud auf den PC ist nötig, um sie bearbeiten zu können. Das Hochladen ist ohne Frage auch wichtig, da die Datei aber lokal vorliegt, kann es problemlos länger dauern.

Durch einen Klick auf **Begrenzen auf** kann die maximale Bandbreite in kb/s eingegeben werden. Bei 50kb/s dauert das Verarbeiten eine 1MB-Datei also 20 Sekunden, immer noch schnell genug für die allermeisten Ansprüche.

Apple präsentiert M1 Ultra und "Mac Studio" Desktop

Apple baut seinen M1-Prozessor weiter aus: Neben M1 Pro und M1 Max gibt es jetzt auch noch einen M1 Ultra (zwei M1 Max in einem). So viel Leistung in einem Desktop-Computer gab es wohl noch nie.

Apple hat den **M1 Ultra** vorgestellt, den nächsten großen Schritt bei Apple Chips und dem Mac.

Dank einer Technologie namens "UltraFusion" verbindet Apple zwei M1-Max-Prozessoren miteinander - und macht daraus einen neuen M1-Ultra. Die neue Architektur verbindet zwei Prozessoren auf einem Chip mit nie dagewesener Rechenleistung und Fähigkeiten.

Neues "Mac Studio"

Das ist kein Prozessor für Web-Surfer und Office-Benutzer, sondern für Menschen, die ihrem Rechner einiges abverlangen. Zum Beispiel, weil sie aufwändiges 3D-Rendering betreiben, 3D-Modelle erstellen und bearbeiten, Trickeffekte in Videos berechnen oder aufwändiges "Compositing" betreiben. Ich persönlich gehöre zur letzten Gruppe: Ich verlange meinem Rechner auch gelegentlich eine Menge ab, wenn ich - teilweise sehr aufwändige - Blenden und

Effekte rechnen lasse.

Überhaupt ist der Video-Schnitt eine rechenaufwändige Sache heutzutage. Vor allem dann, wenn man mit Material in 4K- oder sogar 8K-Auflösung arbeitet.

Deshalb verspreche ich mir vom M1 Ultra einiges. Der ist im ebenfalls neuen Mac Studio verbaut und soll eine atemberaubende Rechenleistung bei gleichzeitig branchenführender Leistung pro Watt sorgen. Denn anders als andere Prozessoren sind die CPUs aus der M1-Serie nicht nur schnell, sondern verbrauchen auch noch weniger Energie. Im Notebook sorgt das für längere Akkuzeiten - im Desktop für weniger Stromverbrauch.

M1 Ultra: 114 Milliarden Transistoren

Das neue Prozessor besteht laut Apple aus 114 Milliarden Transistoren, den meisten, die jemals in einem Chip in einem Personal Computer verbaut worden sind. Der M1 Ultra kann mit bis zu 128 GB gemeinsamen Arbeitsspeicher mit hoher Bandbreite und geringer Latenz konfiguriert werden, auf den die 20-Core CPU, die 64-Core GPU und die 32-Core Neural Engine zugreifen können. Dies bietet Entwicklern, die Code kompilieren, Künstlern, die in großen 3D Umgebungen arbeiten, die so groß sind, dass sie bisher nicht gerendert werden konnten, und Videoprofis, die Videos bis zu 5,6-mal schneller in ProRes umwandeln können als mit einem 28-Core Mac Pro mit Afterburner, eine unfassbare Leistung.

Bahnbrechende UltraFusion Architektur

Die Grundlage für den M1 Ultra ist der extrem leistungsstarke und energieeffiziente M1 Max. Um den M1 Ultra zu bauen, werden zwei M1 Max Chips mithilfe von UltraFusion, der von Apple entwickelten Architektur, zusammengefügt. Die gängigste Methode zur Leistungssteigerung besteht darin, zwei Chips über eine Hauptplatine miteinander zu verbinden, was in der Regel mit erheblichen Nachteilen verbunden ist, beispielsweise einer erhöhten Latenzzeit, einer geringeren Bandbreite und einem höheren Stromverbrauch.

Die innovative UltraFusion von Apple verwendet jedoch einen Silizium-Interposer, der die Chips über mehr als 10.000 Signale miteinander verbindet und eine enorme Bandbreite von 2,5 TB/s mit geringer Latenz zwischen den Prozessoren

ermöglicht — mehr als das Vierfache der Bandbreite der führenden Multi-Chip Interconnect Technologie. Dadurch verhält sich der M1 Ultra wie ein einzelner Chip und wird von der Software als solcher erkannt, sodass Entwickler:innen ihren Code nicht umschreiben müssen, um von seiner Leistung zu profitieren. So etwas hat es bislang noch nicht gegeben.

Unerreichte Leistung und Energieeffizienz

Der M1 Ultra verfügt über eine außerordentlich leistungsstarke 20-Core CPU mit 16 Kernen für hohe Leistung und vier Kernen für hohe Effizienz. Er liefert eine 90 Prozent höhere multithreaded Leistung als der schnellste verfügbare 16-Core Chip eines Desktop-PCs mit demselben Leistungsumfang. Darüber hinaus erreicht der M1 Ultra die Spitzenleistung des PC-Chips mit 100 Watt weniger.[2] Diese erstaunliche Effizienz bedeutet, dass weniger Energie verbraucht wird und die Lüfter leise laufen, selbst wenn Anwendungen wie Logic Pro anspruchsvolle Workflows durchlaufen, wie beispielsweise die Verarbeitung großer Mengen virtueller Instrumente, Audio-Plug-ins und Effekte.

Für besonders grafikintensive Anforderungen wie 3D Rendering und komplexe Bildverarbeitung verfügt der M1 Ultra über eine 64-Core GPU — 8-mal so groß wie die des M1 — und bietet damit eine schnellere Leistung als selbst die besten

verfügbaren PC-Grafikprozessoren, und das bei 200 Watt weniger Stromverbrauch.

Ebenfalls wichtig: gemeinsamer Speicher

Auch die Architektur des gemeinsamen Arbeitsspeichers von Apple ist mit dem M1 Ultra erweitert worden. Die Speicherbandbreite wurde auf 800 GB/s erhöht, mehr als das 10-fache des neuesten Chips eines Desktops, und der M1 Ultra kann mit bis zu 128 GB gemeinsamen Arbeitsspeicher konfiguriert werden. Mit maximal 48 GB bei den leistungsstärksten PC-Grafikkarten gibt es nichts Vergleichbares bei der Größe des Grafiksspeichers, das dem M1 Ultra das Wasser reichen kann. Die Menge an Speicher ist für GPU-intensive Workflows wie die Arbeit mit extremer 3D Geometrie oder dem Rendern riesiger Szenen von entscheidender Bedeutung.

Die 32-Core Neural Engine des M1 Ultra führt bis zu 22 Billionen Rechenoperationen pro Sekunde aus und beschleunigt so die anspruchsvollsten Aufgaben des maschinellen Lernens. Mit der doppelten Leistung der Media Engine des M1 Max bietet der M1 Ultra einen noch nie dagewesenen Durchsatz bei der Kodierung und Dekodierung von ProRes Video. Der neue Mac Studio mit dem M1 Ultra kann sogar bis zu 18 Streams 8K ProRes 422 Video wiedergeben — eine Leistung, die kein anderer Chip schafft.[4] Der M1 Ultra integriert auch spezielle Apple Technologien wie eine Display Engine, die mehrere externe Displays ansteuern kann, integrierte Thunderbolt 4 Controller und erstklassige Sicherheitsfunktionen, darunter Apples neueste Secure Enclave, Hardware-verifiziertes, sicheres Booten und Technologien zum Schutz vor Missbrauch während des Betriebs.

macOS und Apps skalieren auf M1 Ultra

Die tiefe Integration von Hardware und Software ist schon immer das Herz des Mac gewesen. macOS Monterey ist für Apple Chips entwickelt worden und nutzt die enormen Steigerungen bei CPU, GPU und Speicherbandbreite des M1 Ultra. Entwicklertechnologien wie Metal ermöglichen es Apps, den neuen Chip voll auszunutzen, und Optimierungen in Core ML nutzen die neue 32-Core Neural Engine, sodass Modelle für maschinelles Lernen schneller als je zuvor laufen.

Anwender haben Zugriff auf die größte Sammlung von Apps, die es je für den Mac gab, darunter iPhone- und iPad-Apps, die jetzt auch auf dem Mac laufen

können, sowie Universal Apps, die die volle Leistung der M1 Chipfamilie freisetzen. Apps, die noch nicht auf Universal aktualisiert worden sind, laufen reibungslos unter der Rosetta 2 Technologie von Apple.