Schieb Report

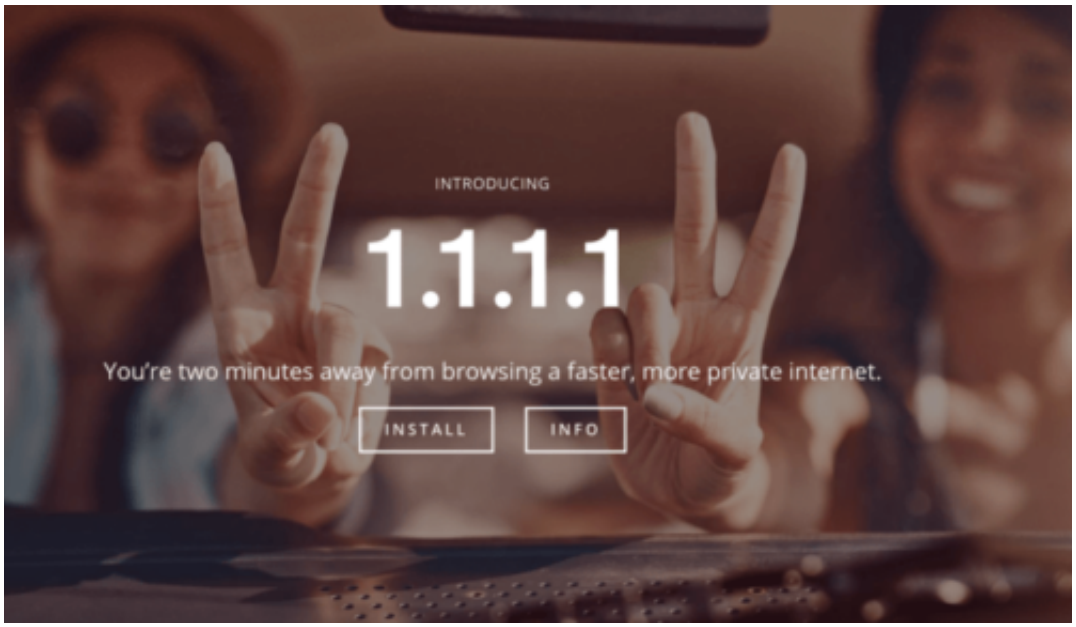
Ausgabe 2018.14

Schneller surfen mit 1.1.1.1 - aber auch sicherer?

Der US-Dienst Cloudflare hat einen kostenlosen öffentlich-zugänglichen Dienst unter der leicht einprägsamen Adresse 1.1.1.1 eingeführt. Ein Angtebot, das auch Privatnutzer in Anspruch nehmen können. Der Cloudflare-Dienst ist extre schnell - und kann so das Surfen beschleunigen. Aber was ist mit Sicherheitsbedenken?

Wenn wir im Netz Inhalte abrufen, etwa Webseiten, Bilder, Videos oder Grafiken, erfolgen Zugriffe auf den im Rechner oder Mobilgerät hinterlegten DNS-Server. DNS - das steht für "Domain Name System".

Er macht aus wdr.de zum Beispiel die IP-Adresse 149.219.205.51. Ohne DNS-Server könnten wir Domains wie schieb.de oder google.com einmotten. Sie haben nämlich ohne die "Übersetzung" in IP-Adressen keinerlei Bedeutung.



1.1.1.1 antwortet sehr schnell

Die meisten User wissen nichts von der Existenz des im Hintergrund arbeitenden DNS. Für gewöhnlich wird beim Einrichten der eigenen DSL-Leitung oder beim Installieren des Mobilgeräts irgendein öffentlich zugänglicher DNS-Server eingetragen. Manchmal die eigenen vom Provider, manchmal ganz andere. Man könnte das für belanglos halten. Ist es aber nicht. Denn der DNS-Server entscheidet, wie schnell wir auf Daten zugreifen können. Außerdem bekommt der DNS-Server eine Menge mit. Etwa, zu welchen Servern wir Kontakt herstellen. Auf diese Weise entstehen Nutzungsprofile.

Jetzt gibt es mit 1.1.1.1 einen neuen DNS-Dienst, den jeder kostenlos nutzen darf. Zur Verfügung gestellt von Cloudflare, einem US-Unternehmen, das auf die Optimierung der Zugriffsgeschwindigkeit im Netz spezialisiert ist. Und tatsächlich: Cloudflares DNS-Dienst 1.1.1.1 ist im Test doppelt so schnell wie die DNS-Server von Google (8.8.8.8) und Co. Das ist

wirklich beachtlich. Bedeutet nämlich konkret: Jedes einzelne Bild, jede Webseite, jedes Video wird deutlich schneller geladen.

https://vimeo.com/263126663

Wie vertrauensvoll ist ein amerikanischer DNS-Dienst?

Cloudflare verspricht darüber hinaus mehr Sicherheit. Auf Wunsch lassen sich die Domain-Abfragen nämlich verschlüsselt durchführen. Und: Die Logdateien des DNS-Servers werden angeblich nach 24 Stunden gelöscht. Damit wären dann alle Spuren der eigenen Nutzung verwischt. Freilich nur, wenn das stimmt - was wir nicht überprüfen können. Aus diesem Grund sind manche User zurückhaltend, einen DNS-Server zu nutzen, der technisch gesehen in den USA steht. (Wenngleich Kopien davon auch in Europa und Asien arbeiten.)

Dabei bieten öffentlich zugängliche DNS-Systeme wie 1.1.1.1 oder Quad9 (hier werden Webseiten mit Schadcode blockiert) einen weiteren Vorteil: Kommen sie in Ländern wie der Türkei zum Einsatz, lassen sich in der Regel auch gesperrte Inhalte abrufen. Denn das ist die einfachste Methode, um komplette Domains zu sperren: Sie aus dem DNS streichen.

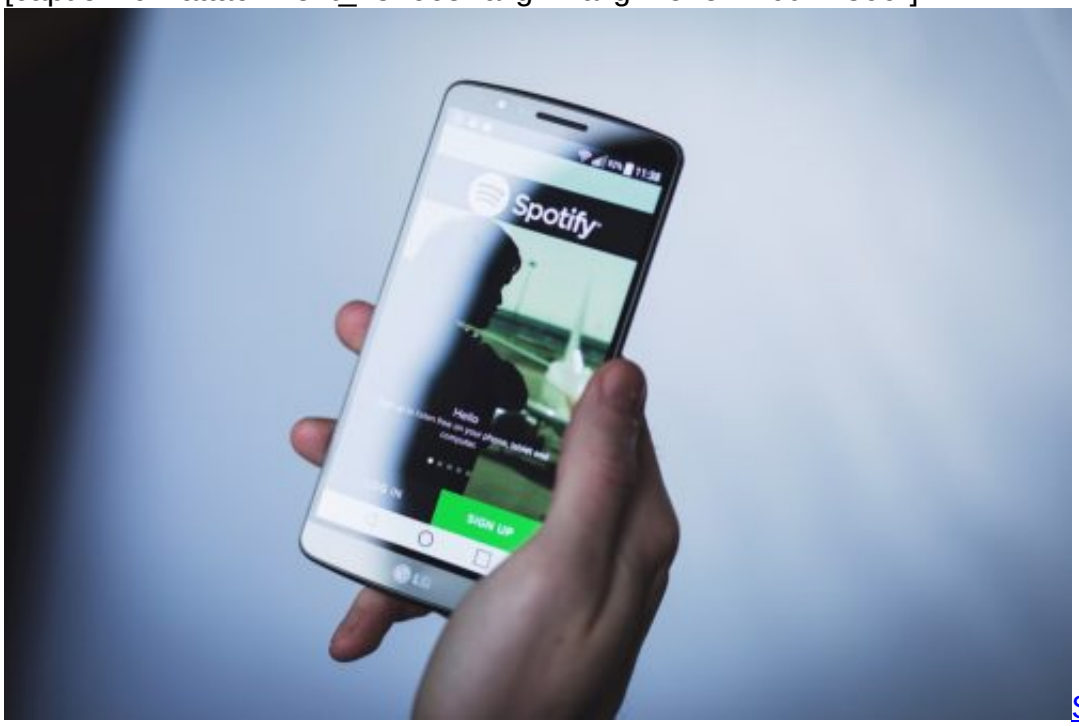
Wer 1.1.1.1 mal ausprobieren möchte, muss nur die IP-Adressen 1.1.1.1 und 1.0.0.1 (als Fallback) in die Netzwerkoptionen eintragen (siehe Video).

Spotify geht an die Börse - und dann?

Spotify geht an der Wallstreet an die Börse. Der Termin war bereits einmal verschoben worden. Jetzt ist es so weit. Der Streamingdienst sammelt Geld ein. Das ist auch dringend nöltig, wenn weiger investiert werden soll, da die Schweden nach wie vor erhebliche Verluste einfahren - obwohl Spotify der erfolgreichste Steamingdienst ist. Wie soll es weitergehen?

Wer wollte es bestreiten? Spotify hat definitiv die Art und Weise verändert, wie viele von uns heute Musik hören. Streaming statt CD - das ist die Idee des schwedischen Unternehmens. Viele sagen, Spotify hätte damit die Musikindustrie gerettet.

Lange Zeit sind die Umsätze der Musiklabels wegen der Piraterie im Netz eingebrochen. Doch die ständig wachsenden Umsätze der Streamingdienste haben den Musiklabels wieder festen Boden unter die Füße gegeben.

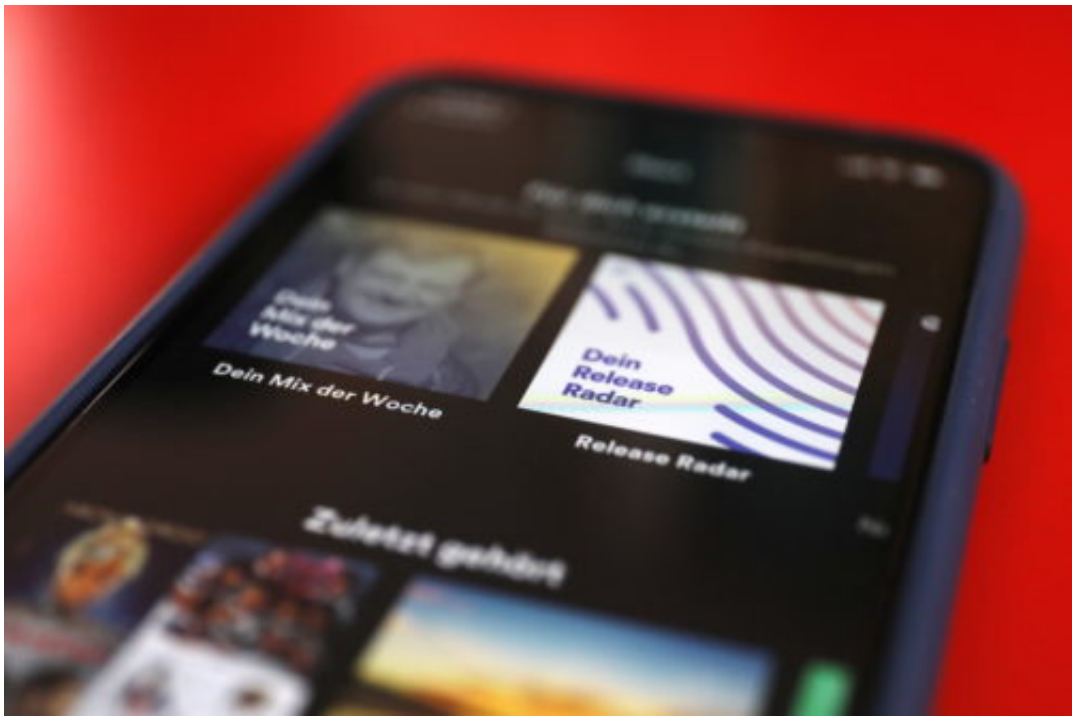
[caption id="attachment_757665" align="alignnone" width="500"]


StockSnap / Pixabay[/caption]

Werbung hören statt Bezahlen

Streaming ist ein interessantes Angebot: So viel Musik wie man möchte zu einem fairen Preis. Mittlerweile können Mitglieder bei Spotify auch Hörbücher und Podcasts hören. Das nutzen immer mehr Menschen.

Nicht nur bei Spotify, sondern auch bei Apple Music, Amazon Music, Deezer und anderen. Dienstag (03.04.2018) geht Spotify an die Börse. Das Unternehmen will Geld einsammeln, um sich weiterentwickeln zu können. Das ist auch dringend nötig, denn bislang fährt Spotify noch erhebliche Verluste ein.



Das Problem: Nur 71 Millionen Menschen aus 65 Ländern zahlen für den Streamingdienst. Doch 88 Millionen Menschen hören bei Spotify Musik, ohne dafür zu zahlen - indem sie Werbung erdulden. Für mich unverständlich: Wenn ich schon Musik hören will, dann doch bitte ohne lästige Werbung.

Außerdem ist es auch eine Frage der Wertschätzung: Brötchen und Bier gibt es auch nicht kostenlos. Wieso wird das bei Musik erwartet? Werbung anzuhören ist nicht nur lästig, sondern vor allem keine besondere Wertschätzung.

https://vimeo.com/257132999

Betrüger haben Spotify abgezogen: Millionen Euro für belanglose Musik

Es müssen eigene Inhalte her

Bis Ende 2018 will Spotify 208 Millionen Mitglieder haben. Das wäre ein großer Sprung. Allerdings hat Spotify ein Problem: Sollten Musiklabels den Stecker ziehen, hat Spotify keine Inhalte mehr. Vorbild Netflix zeigt, dass es auch anders geht: Eigene Inhalte produzieren. Doch das kostet. Spotify hat es mit selbst produzierten Podcasts und Videos probiert, allerdings nicht sonderlich erfolgreich.

Ich wünsche Spotify Erfolg. Denn sie waren die ersten, die den Streaminggedanken konsequent

aufgegriffen, entwickelt und ausgebaut haben. Apple und Amazon sind erst später auf den Zug aufgesprungen. Sie können allein durch ihre schiere Marktmacht Abonnenten gewinnen.

Spotify hat niemanden im Rücken, der ihm Kunden zuspielt. Deswegen ist es um so beeindruckender, was die Schweden geschafft haben. Allerdings muss Spotify nun Alleinstellungsmerkmale haben. Etwas, was sonst keiner hat - erst das hat Netflix zum Durchbruch verholfen.

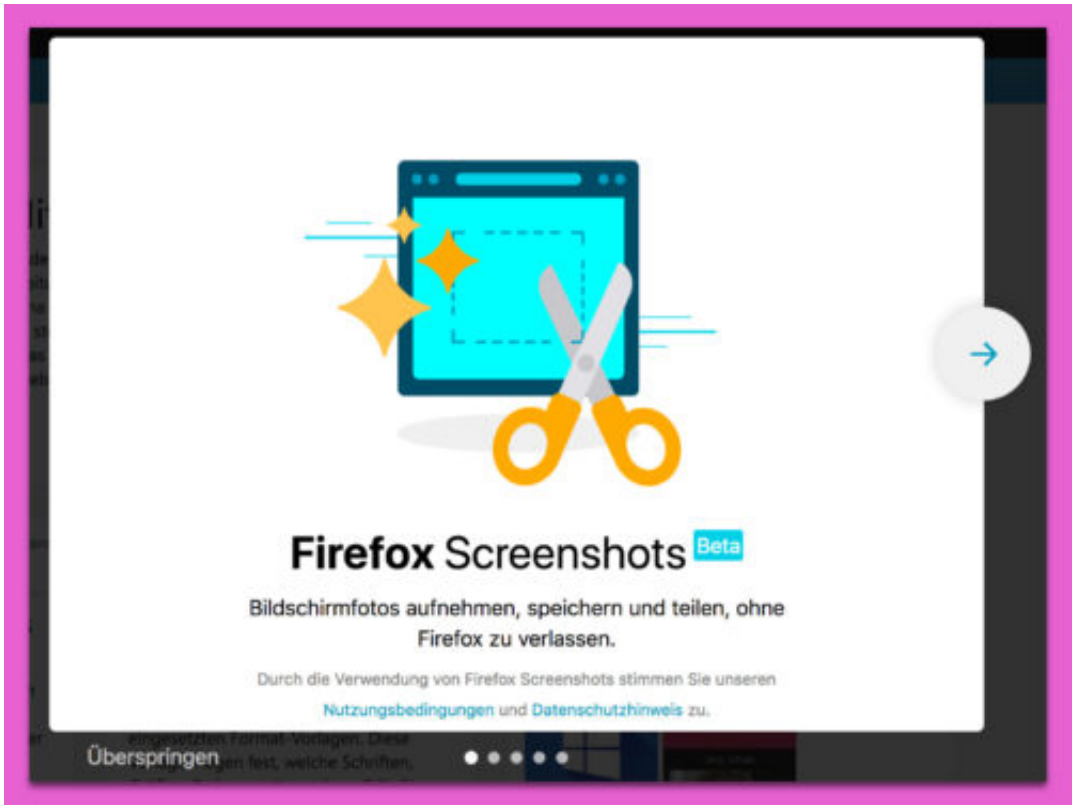
Firefox: Lange Webseiten fotografieren

Die meisten Seiten im Internet sind länger als das, was auf einen Bildschirm passt. Die Folge: Um die restlichen Inhalte zu sehen, muss nach unten gescrollt werden. Soll ein Foto einer Webseite angefertigt werden, müsste man mehrere Bilder zusammensetzen. Ab Firefox 56 geht das auch einfacher.

Waren früher noch Add-Ons nötig, die sich auf das Fotografieren von Webseiten spezialisiert haben, die länger sind als eine Monitor-Höhe, klappt dies nun auch gänzlich ohne Erweiterung:

Zunächst am Ende der Adressleiste auf den Button mit den drei Punkten klicken, dann die Funktion **Bildschirm-Foto aufnehmen, Gesamte Seite speichern**aufrufen. Beim ersten Mal stattdessen auf **Firefox Screenshots**klicken. Jetzt kann das Foto bei Bedarf übrigens auch noch zugeschnitten werden, oder man wählt den Bereich per Markierer aus, der hervorgehoben werden soll. Anschließend zur Bestätigung auf **Speichern**klicken.

Der Link zum geteilten Bild ist für 14 Tage gültig – danach wird er automatisch gelöscht.



Websites automatisch stumm schalten

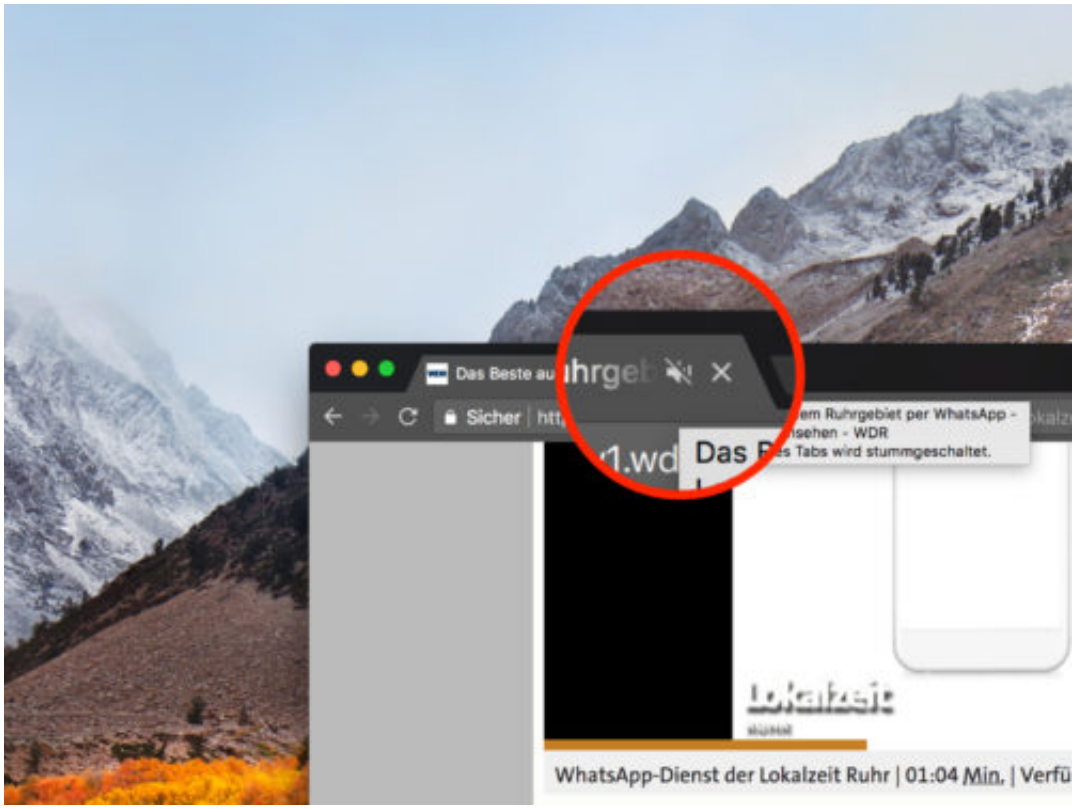
Chrome hat vor einiger Zeit eine Funktion eingeführt, mit der man Tabs stumm schalten kann. Welche Websites so stumm bleiben sollen, merkt sich der Browser in einer schwarzen Liste. Wer lieber grundsätzlich für Ruhe sorgen will, nutzt ein praktisches Chrome-Add-On.

AutoMute lässt sich aus dem Chrome Web Store installieren. Die Erweiterung macht sich sofort an die Arbeit, indem sie jeden einzelnen geöffneten Tab stummschaltet. Es schaltet Tabs wahllos stumm – dazu gehören auch Tabs, die Sound sehr wohl abspielen sollten, z. B. YouTube- und Facebook-Videos.

Die Stummschaltung für einen Tab lässt sich aufheben, indem auf den Lautsprecher auf dem Tab geklickt wird. Das Add-On-Menü hat auch Optionen zum Stummschalten aller Tabs, zum Stummschalten aller anderen Tabs und zum Freischalten der aktuellen Webseite.

Außerdem bietet AutoMute einen Whitelist-Modus, bei dem nur Seiten auf der Whitelist Audio abspielen dürfen, sowie einen Blacklist-Modus. Hier werden nur Webseiten auf der schwarzen Liste stummgeschaltet, während alle anderen Webseiten Audio abspielen dürfen.

https://chrome.google.com/webstore/detail/automute/kjcdcbhfpjkcjinohfaaihpcmpnpmpie



iCloud-Lesezeichen mit Firefox und Chrome

Wer unterwegs ist, will die gleichen Lesezeichen wie am Desktop nutzen – ungeachtet des Browsers. Die iCloud Bookmarks-Erweiterung ermöglicht das Speichern von Lesezeichen auf dem iPhone oder iPad und die automatische Übertragung mit den Desktop-Versionen von Chrome oder Firefox.

Zunächst die entsprechende Browser-Erweiterung für Chrome oder Firefox herunterladen und installieren. Ist iTunes bereits installiert, funktionieren beide Clients sofort. Falls nicht, erscheint eine Aufforderung, die eigenständige iCloud Control Panel App herunterzuladen und zu installieren.

Beide Browser-Erweiterungen funktionieren in Verbindung mit dem iCloud Control Panel und benötigen eine Apple ID, um Daten zwischen Ihrem Browser und der iCloud zu synchronisieren.

Die Synchronisierung für iCloud-Lesezeichen ist mit der Apple-ID verknüpft. Daher ist eine Anmeldung mit der eigenen Apple-ID und dem zugehörigen Passwort nötig, bevor die Einstellungen der iCloud-Lesezeichen angezeigt werden.

iCloud Bookmarks für Chrome

iCloud Bookmarks für Firefox

iCloud Control Panel

Interpreter eines Shell-Skripts ermitteln

Shell-Skripte sind praktisch – sie werden heruntergeladen und sind sofort einsatzfähig, denn sie können direkt über die Konsole aufgerufen werden. Soweit die Theorie. In der Praxis ist es besser, vorher einen Blick in den Code zu werfen.

In welcher Skript-Sprache ein Shell-Skript verfasst ist, kann der Nutzer dabei anhand der ersten Zeile im Skript erkennen. Denn hier erscheint die sogenannte „Shebang“.

Mit dieser einheitlichen Information weiß die Shell, welcher Interpreter, also welches Programm, das Skript ausführen kann. Damit das Skript dann aber auch tatsächlich gestartet werden kann, muss der passende Interpreter natürlich auch auf dem Server oder Computer installiert sein. Python-Skripts lassen sich beispielsweise nur dann starten, wenn auch die Python-Laufzeit installiert ist.

Wichtige Interpreter sind etwa #!/bin/bash – die Bash-Shell selbst, #!/...python, also die Python-Runtime, oder auch #!...perl für den Perl-Interpreter – quasi die Mutter aller Skript-Sprachen. Auch #!...php kommt recht häufig zum Einsatz.

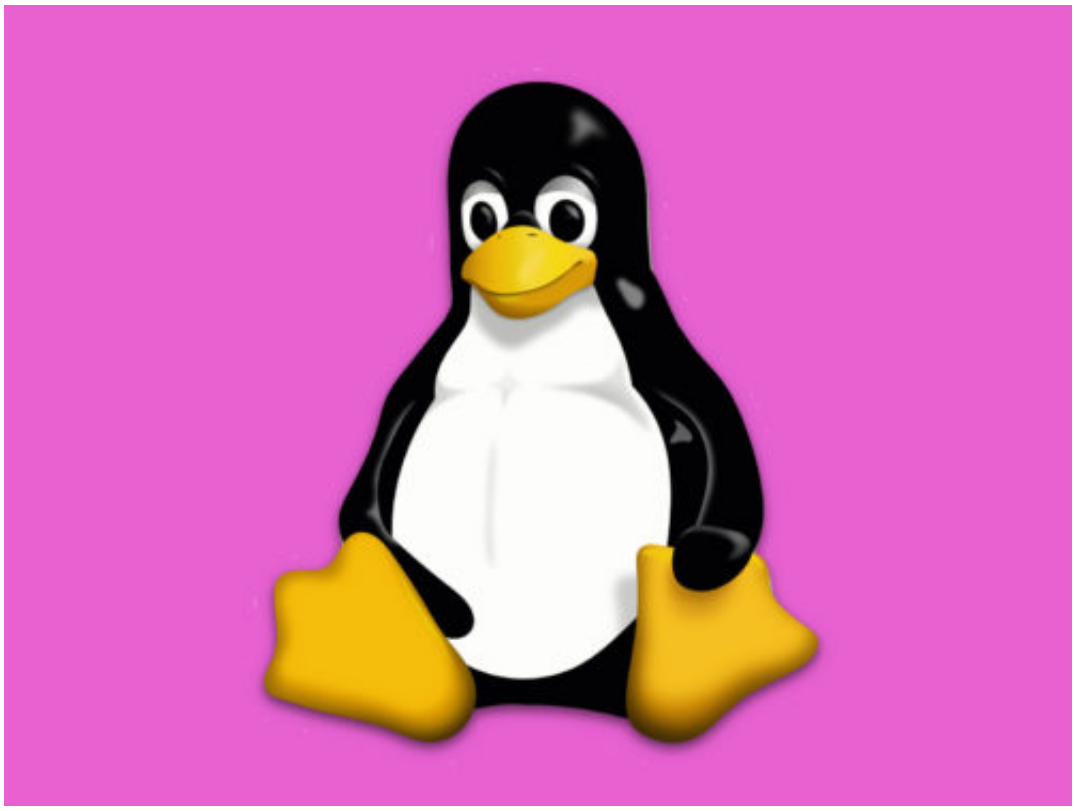
Linux-Ordner schneller öffnen

Jede Linux-Distribution bringt ihren eigenen Datei-Manager mit – der entspricht etwa dem Datei-Explorer von Windows oder dem Finder von macOS. Großer Vorteil von Datei-Managern unter Linux: Sie behandeln alles als URL, selbst lokale Ordner. Besondere Verzeichnisse sind dabei über Kürzel extra schnell aufrufbar.

Alle folgenden Kurz-URLs können durch Eingeben in die Adressleiste des Datei-Managers erreicht werden. Meist muss dazu anschließend noch [Enter] gedrückt werden:

- Datenträger und Laufwerke lassen sich mit **computer:///** aufrufen.
- Ebenso zeigt **network:///** eine Übersicht über alle Server, die sich im lokalen Netzwerk befinden. Dazu gehören auch Windows-PCs – **smb:///** startet dabei den Zugriff auf Windows-Freigaben.
- Der Papierkorb steht unter **trash:///** bereit.
- **fish:///**34.56.78 oder **sftp:///**12.34.56.78 öffnen einen SSH-Server.

Meist lassen sich auch ganz normale Internet-URLs in die Leiste eingeben. Für deren Aufruf startet das Linux-System dann den Browser.



Linux: USB-Stick sicher auswerfen

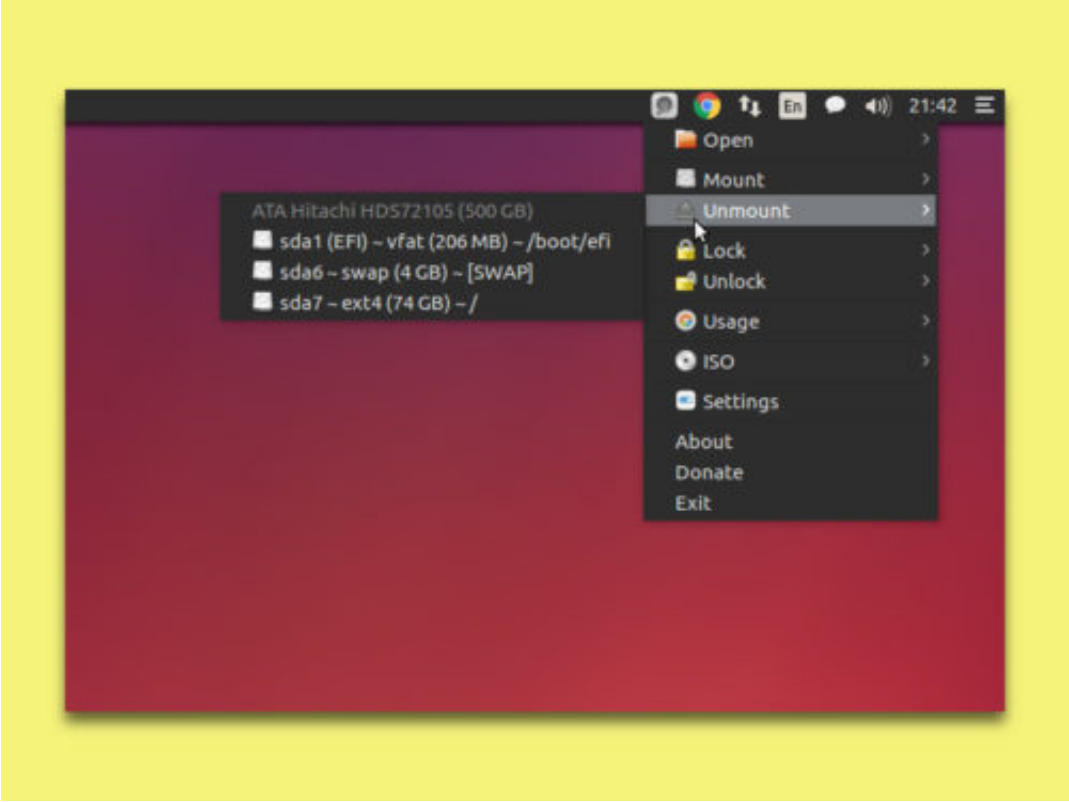
Einer der großen Vorteile von USB-Laufwerken ist, dass sie jederzeit auch im laufenden Betrieb ein- und ausgesteckt werden können. Windows blendet dazu neben der Uhrzeit ein Symbol ein, über das USB-Sticks und Festplatten sicher entfernt werden können. Mit einem Trick lässt sich diese Funktion auch für Linux nachrüsten.

„Indicator“ nennt sich diese Funktion, die es unter anderem auch für Ubuntu und verwandte Systeme gibt. Linux-typisch lässt sich das Feature bequem durch Installation eines zusätzlichen Pakets einspielen.

Dazu werden in der Shell folgende Befehle eingetippt:

sudo apt-add-repository ppa:teejee2008/ppa [Enter]
sudo apt update [Enter]
sudo apt install indicator-diskman [Enter]

Dadurch wird ein Icon installiert, mit dem sich sämtliche Datenträger mounten und unmounten lassen – nicht nur USB-Laufwerke.



Alte Safari-Downloads leeren

Wer mit dem Safari-Browser Dateien aus dem Internet lädt, erstellt dadurch automatisch eine Liste aller Downloads. Diese Liste steht per Klick auf das Download-Symbol oben rechts in jedem Safari-Fenster bereit. Wie lange der Browser sich die Dateien merken soll, kann auch geändert werden.

Die Verweildauer von Downloads im Safari-Verlauf kann zentral über die Browser-Optionen festgelegt werden. Dazu im Menü auf **Safari, Einstellungen …** klicken. Hier im Bereich **Allgemein** für die Option **Downloads aus der Liste entfernen** entweder **Nach einem Tag, Beim Beenden von Safari, Nach erfolgreichem Download** oder **Manuell** auswählen.

Wird hier **Manuell** eingestellt, leert der Browser die Liste der geladenen Dateien überhaupt nicht mehr automatisch. Soll die Liste zwischendurch manuell entsorgt werden, geht das mit zwei Schritten:

1. Im Safari-Fenster oben rechts auf den Download-Button klicken.
2. Hier den Button **Löschen** betätigen.

WLAN mit optimalem Empfang

Wer ein eigenes Haus hat, kann das WLAN nicht überall gleich gut empfangen. Zumindest nicht, wenn nur ein einzelner Router zum Einsatz kommt. Wer mehrere Router installiert und diese über einen Switch mit dem Internet vernetzt, kann den Empfang optimieren.

Automatisch funktioniert das WLAN-Roaming im eigenen Haus am besten, wenn beide Router die gleiche SSID anbieten. Dabei handelt es sich um den Namen des WLANs – so, wie er in Windows und auf mobilen Geräten zum Herstellen einer Verbindung angeboten wird. Die SSID lässt sich in den Einstellungen des Routers festlegen, etwa unter http://fritz.box.

Der Vorteil ist hierbei: Heißen die WLAN-Netzwerke gleich, ist der Wechsel zwischen den Routern nahtlos und für den Benutzer nicht festzustellen. Denn Windows misst im laufenden Betrieb stetig die Signalstärke aller WiFi-Netze, die sich in Reichweite befinden.

Das sorgt dafür, dass das System sich immer mit dem Netzwerk verbindet, das den besten Empfang bietet. Wichtig: Dies bezieht sich ausschließlich auf die WLAN-Stärke, nicht aber auf die Geschwindigkeit der Internet-Verbindung zwischen dem Router und dem Web. Es könnte ja sein, dass der Router im ersten Stock zwar besseren WLAN-Empfang bietet, dafür aber langsamer beim Surfen ist.

Word-Formate schneller anwenden

Professionell gestaltete Word-Dokumente basieren immer auf sorgfältig eingesetzten Format-Vorlagen. Diese Vorlagen legen fest, welche Schriften, Größen, Farben und sonstigen Stile für eine bestimmte Art von Text eingesetzt werden. Besonders schnell lässt sich eine Format-Vorlage anwenden, wenn sie direkt oben ins Menü integriert wird.

Klickt man oben in Word auf den Menü-Tab **Start**, erscheint im rechten Bereich der Leiste eine Übersicht mit besonders häufig genutzten Vorlagen. Welche Formate hier zur Auswahl stehen sollen, kann man auch selbst konfigurieren.

Soll eine neu erstellte Format-Vorlage in dieser Liste der Schnell-Format-Vorlagen angeboten werden, aktiviert man die entsprechende Option:

Dazu rechts im Menü den Bereich für Format-Vorlagen aufrufen. Jetzt auf den kleinen Pfeil neben der betreffenden Vorlage klicken, um diese zu bearbeiten. Hier die Option **Zur Liste der Schnell-Format-Vorlagen hinzufügen** aktivieren und mit **OK** bestätigen – fertig.

Auch die Post verhökert Daten - an FDP und CDU

Der Datenskandal um Cambidge Analytica und Facebook hat zweifellos die Sensibilität erhöht. Plötzlich hören wir genauer hin, wo wir vor einigen Wochen nur lässig mit den Achseln gezuckt hätten. Wie jetzt durch die Bild am Sonntag (BAMS) bekannt wurde, hat eine Tochterfirma der Post CDU und FDP mit Daten versorgt, die im Wahlkampf genutzt wurden. Dafür seien "fünfstellige Beträge" geflossen.

Nein, das ist von Dimension und Umfang natürlich nicht mal ansatzweise mit dem Cambridge Analytica Fall vergleichbar. Denn im Fall des Post-Deals wurden keine persönlichen Daten ermittelt und weitergegeben, sondern anonymisierte Daten. Die Post hat den Auftraggebern verraten, mit einem Wahrscheinlichkeitswert zwischen 1 und 100, wie die persönliche Gesinnung in einem Haushalt ist.

Aber nicht von einem konkreten Haushalt, sondern immer nur von mehrere Haushalten gleichzeitig - in der Regel voin 6,6 Haushalten. Doch dafür wurden viele Daten verarbeitet, unter anderem auch Daten, die vom Kraftfahrtbundesamt kommen. Angaben übrer Familiensituaion, Kaufkraft, Alter, Bildung, Wohnsituatuation und mehr.

[caption id="attachment_757636" align="alignnone" width="500"]


geralt / Pixabay[/caption]

Daten. anonymisiert

Das sind schon eine Menge Informationen. Und auch, wenn sie anonymisiert wurden, ist das

schon ziemlich konkret. Besonders neu ist das allerdings auch nicht, denn schon lange werden nach dem Konzept Bonitöt und Kaufkraft ermittelt - und auch bewertet, wenn jemand einen Antrag auf einen Mobilfunkvertrag stellt oder etwas kaufen möchte. Das Haus, in dem man wohnt, entscheidet (unter anderem), ob man ein gern gesehener Kunde ist oder nicht.

Das vergleichsweise milde Vergehen der Post macht aber deutlich, was heute nicht nur möglich, sondern selbstverständlich ist. Es wird aller höchste Zeit, sich darüber im Klaren zu werden, was man da OK findet und wo die Grenzen gezogen werden sollen. Politik gehört nicht hier her. Ganz sicher dürfen solche Daten aber nicht an Parteien gehen, denn die manipulieren die Menschen dann nur, anstatt sie zu informieren und aufzuklären.

[caption id="attachment_757637" align="alignnone" width="500"]


xresch / Pixabay[/caption]

Wie sicher sind eigentlich Sprachassistenten?

Erstaunlich, was die Sprachassistenten alles verstehen – und was sie teilweise auch können. Doch nicht wenige bezeichnen die Sprachassistenten als "Wanzen", die man sich freiwillig in die Wohnung holt. Potenzielle Schnüffler, die mitbekommen, was zu Hause los ist – oder unterwegs, wenn man die Assistenten auf einem Mobilgerät nutzt. Was können die Assistenten, was dürfen sie – und welche Daten fallen an?

Wenn wir das Codewort sprechen, das den Assistenten zum Leben erweckt, also "OK Google" oder "Alexa" oder "Siri", wird alles, was danach gesprochen wird, über das Internet an spezielle Server geschickt. Wohlgemerkt, die Sprachdatei, also das, was sie sagen.

Dort wird der gesprochene Text blitzschnell analysiert – und das Ergebnis kommt zurück, auch über das Internet. Etwa eine gesprochene Antwort, oder Musik, die angespielt werden soll und vieles andere mehr.

Es ist wirklich wichtig zu verstehen, dass rein gar nichts im Gerät selbst passiert. Das Gerät hat keine Spracherkennung. Die findet online statt. So kann das System lernen, etwa sich an die Aussprache der Nutzer gewöhnen, aber auch den Funktionsumfang ständig erweitern.

Hört mir denn so ein Sprachassistent ununterbrochen zu?

Grundsätzlich schon, denn sie müssen auf das Schlüsselwort zum Wecken reagieren. Deshalb ist das Mikro ständig offen, sofern es nicht explizit stummgeschaltet wurde (was durch

einfaches Antippen des entsprechenden Buttons geht). Was gesprochen wird, wenn der Assistent nicht direkt angesprochen wurde, bleibt unter normalen Umständen zu Hause.

Das wird nicht an die Server geschickt. Erst wenn der Weckbefehl gesprochen wurde, beginnt die Übertragung der Frage oder Anweisung an die Server des jeweiligen Betreibers. Bei Google kann man in seinem Google-Konto nachschauen – und sich auch anhören –, was man gefragt oder gesagt hat. Auch die Alexa-App bietet eine Übersicht über Fragen und Anweisungen.

Zeichnen Sprachassistenten Gespräche auf?

Niemand bemerkt, ob das Mikro offen ist, ob etwas mitgeschnitten wird. Wer sich so einen Sprachassistenten ins Haus holt, der muss also vertrauen. Theoretisch denkbar ist, dass Hacker ein Sicherheitsleck ausnutzen – und einfach mithören, was gesprochen wird.

Oder das Schnüffeldienste wie die NSA Sicherheitslecks ausnutzen und mithören. Das sollte man zumindest einkalkulieren, denn es ist denkbar und möglich – und wird deshalb auch früher oder später passieren. Mitunter aktiviert man als Benutzer sogar versehentlich die Mithörfunktion, etwa lange Zeit durch "OK Kuchen" oder "OK DU".

Das hat Google Home lange Zeit als "OK Google" verstanden – und das Mikro geöffnet. Jetzt nicht mehr. Bei Alexa reicht auch ein "Alexandra" für Alexa oder "Gecko" für Echo (Alexa kann man auf verschiedene Weisen ansprechen), um den Assistenten zu wecken.

Assistenten also vertrauen oder nicht?

Der TÜV hat kürzlich verschiedene Assistenten untersucht und auch die Schwachstellen mit den Ansprachen wie "OK Kuchen" gefunden. Die Prüfer haben festgestellt, dass die Geräte ständig Daten übertragen.

Da die Daten verschlüsselt sind, weiß man allerdings nicht, um welche Daten es sich handelt. Sie sind aber nicht nur dann aktiv, wann der User aktiv mit ihnen spricht. Das Datensicherheitsniveau entspreche aber dem Stand der Technik und wird als vergleichsweise hoch eingestuft.

Welche Daten fallen bei der Nutzung an?

Bislang sind die Assistenten kostenlos. Es ist nicht vorstellbar, dass Konzerne wie Amazon, Google oder Apple diese Dienste aus reiner Nächstenliebe anbieten. Amazon holt sich bei der Installation der Alexa-App die Erlaubnis, Cookies zu verwenden und Werbung zu präsentieren.

Bei Google ganz ähnlich: Hier ist nachgewiesen, dass Google Home sogar Daten mit Ad-Servern austauscht, also Servern, die mit der Auslieferung von Anzeigen beschäftigt sind. Es fallen jede Menge Daten an.

Die Anbieter erfahren nicht nur, welche Fragen wir haben und welche Themen uns interessieren, sie bekommen auch mit, welche Musik wir hören oder welche Nachrichten uns interessieren. Auch bekommen sie mit, wann wir wach sind, wann wir unser Smart Home per

Sprachbefehl steuern, wie viele Menschen im Raum sind – wenn mehrere die Systeme nutzen – und vieles andere mehr.

Ein Eldorado für die Datensammler. Sie bekommen mehr und vor allem andere Informationen als am Desktop-PC oder am Mobilgerät. Eine aus Sicht der Onlinedienste wunderbare Ergänzung. So ganz ohne scheint das nicht zu sein, denn Facebook hat nach dem Cambidge-Analytica-Skandal die geplante Vorstellung seines smarten Lautsprechers erst mal abgesagt und verschoben. Das sagt schon fast alles.

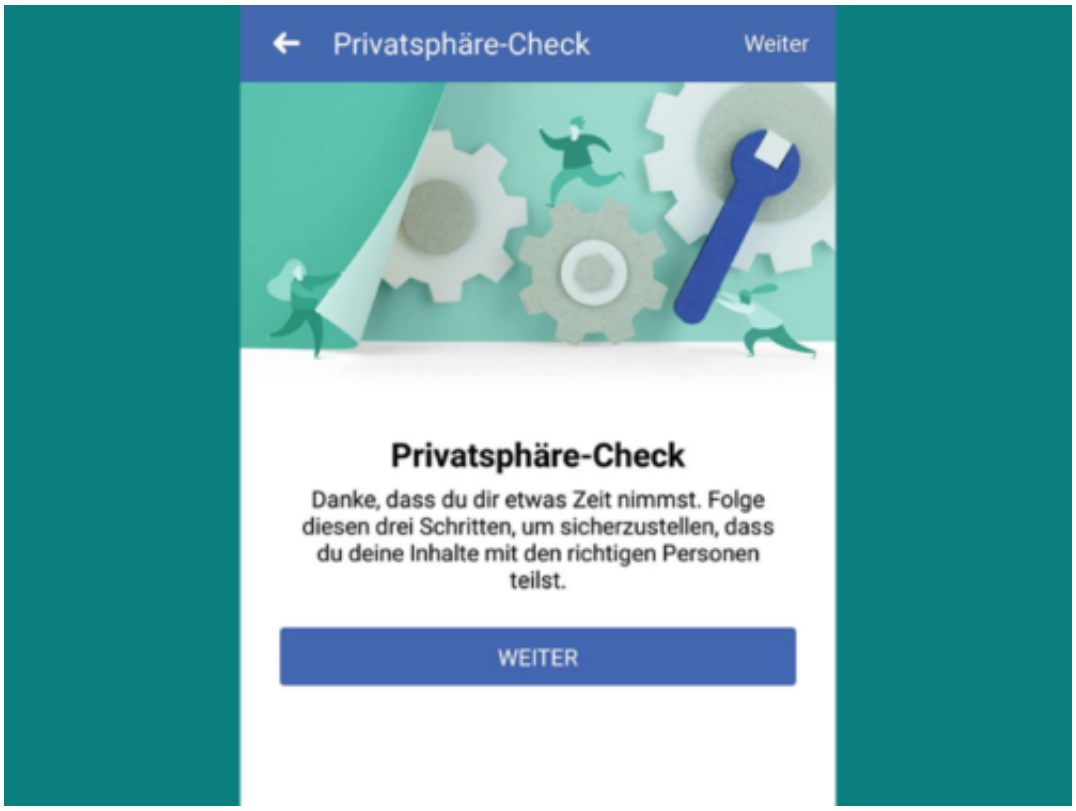
https://vimeo.com/248057554

Drittanbieter-Apps den Zugriff auf Facebook-Daten verwehren

Wer sich bei einem neuen Dienst, einem Portal oder einer App anmeldet, lässt sich schnell dazu verleiten, den “Mit Facebook anmelden”-Button zu klicken. Das geht zwar schnell, birgt aber auch einige Risiken. Denn: Was passiert mit den eigenen Daten?

Zugegeben, es ist ziemlich nervig und zeitaufwendig, sich ständig von Grund auf neu irgendwo anzumelden. Viele Portale bieten deshalb die Möglichkeit, sich mit nur einem Klick mit seinem Facebook-Account anzumelden. Mit diesem Klick gibt man allerdings in der Regel auch eine Menge Rechte und Zugriff ab. Um zu sehen, welchen Apps Sie welche Rechte eingeräumt haben, sollten Sie folgende Einstellungen vornehmen.

Zunächst die **Facebook-App** öffnen und über das Icon oben rechts das **Menü** öffnen. Hier nun etwas weiter herunterscrollen, bis zum Punkt **Kontoeinstellungen.** Über den Punkt **Privatsphäre** nun den Bereich **Sieh dir einige wichtige Einstellungen an** öffnen, um einen Privatsphäre-Check durchzuführen.

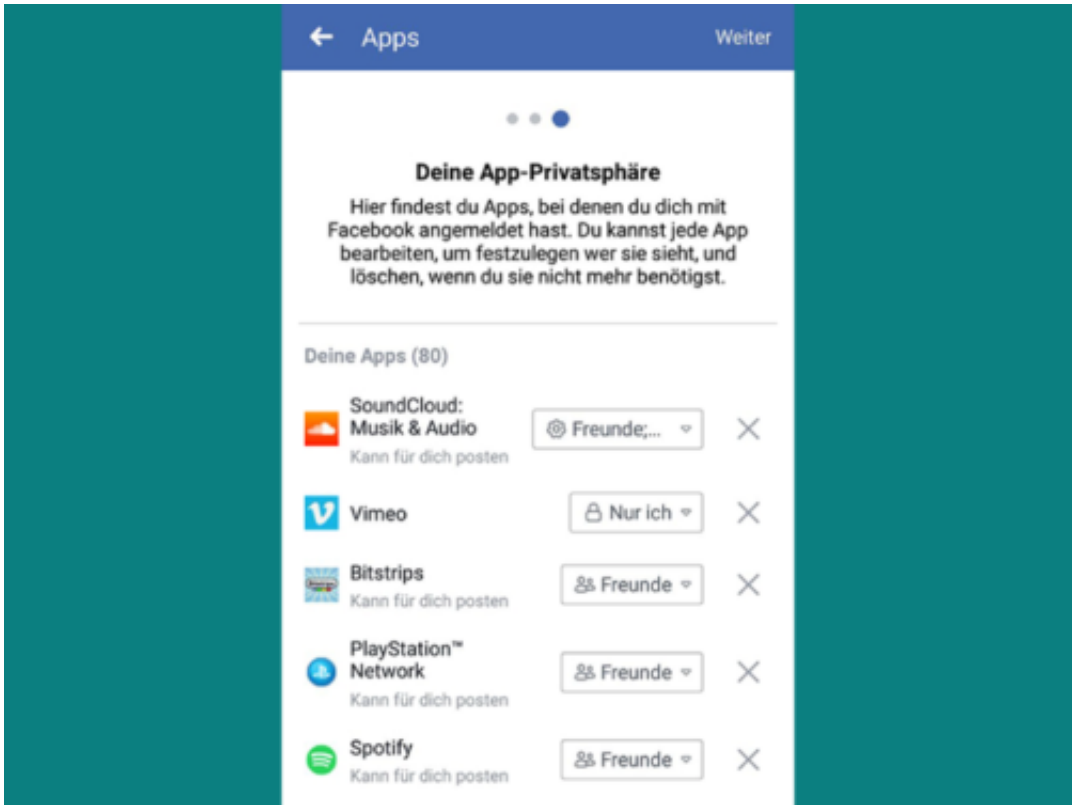


Keine Rechte für niemanden

Mit einem Tap auf **weiter** bekommen Sie drei Bereiche angezeigt, in denen sich verschiedene Einstellungen vornehmen lassen. Apps, in denen Sie sich mit Facebook angemeldet haben, finden Sie ganz rechts. Hier wird neben der entsprechenden App auch direkt angezeigt, welche

Rechte sie hat.

Um bestimmten Apps die Rechte und den Zugriff auf Ihr Facebook-Konto zu entziehen, genügt ein Tap auf das **X.** Wenn Sie eine App oder einen Dienst länger nicht genutzt haben, sollten Sie diesen aus der Liste löschen. Aber auch bei Anwendungen, die sich regelmäßig nutzen, sollten Sie genau schauen, wie viel Zugriff Sie tatsächlich zulassen.



Digitale Assistenten: Wirklich praktisch - oder eher lästig?

Digitale Assistenten wie Amazon Echo, Apples Homepod, Google Home oder Invoke von Microsoft (mit Cortana) sind derzeit total populär. Viele stellem sich solche Geräte ins Haus - und noch mehr Menschen nutzen Assistenten auf ihrem Smartphone. Doch was viele nicht wissen: Jede einzelne Anfrage landet in der Cloud. Ohne Wenn und Aber. Das macht die Assistenten durchaus zu einem Datenschutzproblem.

Auch Facebook wollte einen smarten Lautsprecher auf den Markt bringen. Als Alternative zu den Lautsprechern mit Assistenzfunktion wie Amazons Echo/Alexa - und Google mit Google Home, Microsoft mit Invoke (Cortana) und Apple mit dem HomePod. Mark Zuckerberg hat verstanden: Hier liegt die Zukunft.

Und für ein Datensammelunternehmen ist so ein Digitaler Assistent für zu Hause ganz weiß Feines. Nur: Der Datenskandal rund um Cambridge Analytica und Co. hat die Leute misstrauischer gemacht. Deshalb hat Facebook die Markteinführungen seiner Interpretation eines "Digitalen Assistenten" erst mal auf ungewisse Zeit verschoben.

Nutzer vertauen den Digitalen Assistenten blind

Vermutlich eine kluge Entscheidung. Denn eins sind die Digitalen Assistenten ganz gewiss: ein Datenschutzproblem. Schon aus psychologischen Gründen: Wer mit einer Maschine spricht, also nicht irgendwas eintippt oder auf dem Display wischt, der denkt noch weniger darüber nach, ob er vertrauliche Informationen preisgibt als ohnehin schon. Sprechen ist etwas ganz Natürliches. Und da man mit einer Maschine spricht, spricht man fast zu sich selbst. Vertrauen garantiert.

Aber haben die Digitalten Assistenten das Vertrauen verdient? Die Erfahrungen der Vergangenheit lehren uns: Wohl eher nicht. Alles, was nicht völlig undenkbar ist, das geschiebt

auch. Das hat uns die NSA gelehrt.

Also müssen wir davon ausgehen, dass es möglich ist, dass das eingebaute Mikro in solchen smarten Lautsprechern von Hackern (oder Geheimdiensten) gekapert werden kann. Zwecks Lauschaktion. Oder dass durch Pannen Gesprächsfetzen aufgezeichnet werden, die eigentlich gar nicht aufgezeichnet werden sollen.

https://vimeo.com/263408641

Die Onlinedienste merken sich genau, was wir unsere Assistenten gefragt haben - der Beweis

Klare Regeln nötig

Google Home reagiert(e) auf "OK Kuchen", Amszons Alexa auf "Alexandra" - nur zwei bekannte Beispiele. Und schon landen die nachfolgend gesprochenen Worte auf den Servern der Anbieter. Kann man sogar selbst überprüfen: Die Alexa App spielt einem auf Wunsch Gesprächsfetzen vor, die nicht richtig verstanden wurden. Bei mir sind das teilweise Telefongespäche.

Alles schon bedenklich genug. Dann kommen noch die Sachen dazu, die keine Unfälle sind, sondern geplant. Jedes Gespräch mit unserem Assistenten verrät etwas über uns. Ob wir zu Hause sind, in welchem Raum wir uns befinden, in welcher Stimmung wir sind (Kuschelrock, Jazz oder Hardrocj angefordert?), wann wir ins Bett gehen("Alexa: Licht aus") und vieles andere mehr. Ein Eldorado für Onlinedienste, die uns mit Vorliebe durchleuchten.

Man muss kein Hysteriker sein, um sich vorzustellen, welche Konsequenzen all das haben kann. Digitale Assistenten können sehr praktisch sein. Aber es braucht klare Regeln, was da überhaupt von verarbeitet werden darf. Die Standardeinstellung sollte laut Gesetzgeber lauten: NICHTS. Nur wenn ich unbedingt will und zustimmt, darf sich der Onlinedienst die ein oder andere Sache merken.

Windows-Version für Product Key ermitteln

Die meisten Windows-Lizenzen werden heute mit Hardware verkauft – ein neuer Laptop bringt seine Lizenz gleich mit. Dennoch lässt sich Windows 10 auch einzeln erwerben. Wer eine Lizenz vorliegen hat, aber nicht mehr weiß, für welche Windows-Variante sie gültig ist, kann dies leicht herausfinden.

Um herauszufinden, für welche Windows-Edition ein Produktschlüssel gedacht ist, kommt eine Anwendung namens ShowKeyPlus zum Einsatz. Dieses Tool kann Produktschlüssel lesen, die sich auf dem Motherboard befinden, d. h. OEM-Schlüssel, aber sie kann auch überprüfen, für welche Windows-Edition ein manuell eingegebener Schlüssel bestimmt ist.

Da es uns darum geht, herauszufinden, für welche Windows-Edition ein Produktschlüssel bestimmt ist, müssen wir auf die Registerkarte **Check Product Key** wechseln.

Geben Sie hier den Schlüssel ein, den Sie zur Hand haben, und es wird geprüft, ob der Produktschlüssel für Windows Home, Professional oder Education ist und ob es sich um eine OEM-Lizenz oder eine EULA-Lizenz (nicht an einen bestimmten Rechner gebunden) handelt und ob es sich um eine Volumenlizenz handelt oder nicht.

https://github.com/Superfly-Inc/ShowKeyPlus/releases